Міністерство освіти і науки України
Миколаївський національний аграрний університет

Кваліфікаційна робота
на правах рукопису

**Заремба Микита Олегович**

УДК 336:330.46:004.056

# КВАЛІФІКАЦІЙНА РОБОТА

# КІБЕРБЕЗПЕКА В РОЗВИТКУ ФІНАНСОВОЇ СИСТЕМИ УКРАЇНИ

Спеціальність D2 Фінанси, банківська справа, страхування та фондовий ринок
Галузь знань D Бізнес, адміністрування та право

Подається на здобуття освітнього ступеня «Магістр»

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Науковий керівник: Сіренко Н. М., д-р екон. наук, професор
Завідувач кафедри: Сіренко Н. М., д-р екон. наук, професор

Миколаїв – 2026

# АНОТАЦІЯ

**Зарембо М. О.** Кібербезпека в розвитку фінансової системи України. Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня «Магістр» за спеціальністю D2 Фінанси, банківська справа, страхування та фондовий ринок у галузі знань D Бізнес, адміністрування та право. Миколаївський національний аграрний університет, Миколаїв, 2026.

У кваліфікаційній роботі обґрунтовано теоретичні засади та розроблено практичні рекомендації щодо підвищення рівня кібербезпеки фінансової системи України в умовах воєнного стану та поствоєнного відновлення. Уточнено співвідношення категорій «інформаційна безпека», «кібербезпека» і «кіберстійкість» стосовно фінансового сектору, систематизовано нормативно-правову базу та міжнародні стандарти кіберзахисту фінансових установ, виявлено розрив між темпами цифровізації фінансових послуг і зростання кіберзагроз та темпами оновлення законодавчої і наукової бази.

Проаналізовано структуру та тенденції цифровізації фінансової системи України, динаміку кіберінцидентів і платіжного шахрайства, класифіковано кіберзагрози й вразливості фінансового сектору, здійснено порівняльну оцінку кіберзахищеності фінансових установ різних категорій, яка засвідчила глибокий розрив між ними (інтегральний індекс 0,89 проти 0,24).

Запропоновано класифікацію кіберінцидентів із диференційованими строками звітування, гармонізованими з вимогами NIS2 і DORA, зміни до шести нормативно-правових актів, модель єдиного органу кіберстійкості фінансового сектору в структурі Національного банку України, яка усуває дублювання наглядових функцій і передбачає створення нових робочих місць для фахівців з кібербезпеки в період поствоєнної відбудови.

**Ключові слова:** кібербезпека, кіберстійкість, фінансова система, кіберінцидент, кіберризик, Національний банк України, цифровізація, NIS2, DORA, поствоєнне відновлення.

# ABSTRACT

**Zarembo M.O.** Cybersecurity in the Development of the Financial System of Ukraine. Qualification work, manuscript. Qualification work for the Master's degree in specialty D2 Finance, Banking, Insurance and Stock Market field of knowledge D Business, administration and law. Mykolaiv National Agrarian University, Mykolaiv, 2026.

The qualification work substantiates the theoretical foundations and develops practical recommendations for strengthening the cybersecurity of the financial system of Ukraine under martial law and during post-war recovery. The relationship between the categories of information security, cybersecurity and cyber resilience in the financial sector is clarified, the legal framework and international cybersecurity standards for financial institutions are systematised, and the gap between the pace of digitalisation of financial services and the growth of cyber threats, on the one hand, and the pace of updating the legislative and scientific base, on the other hand, is identified.

The structure and digitalisation trends of the financial system of Ukraine, the dynamics of cyber incidents and payment fraud are analysed; cyber threats and vulnerabilities of the financial sector are classified; a comparative assessment of the cyber protection of different categories of financial institutions is carried out, revealing a deep gap between them (integral index 0.89 versus 0.24).

The work proposes a classification of cyber incidents with differentiated reporting deadlines harmonised with NIS2 and DORA requirements, amendments to six legal acts, and a model of a single cyber resilience body for the financial sector within the National Bank of Ukraine that eliminates the duplication of supervisory functions and provides for the creation of new jobs for cybersecurity specialists during post-war reconstruction.

**Keywords:** cybersecurity, cyber resilience, financial system, cyber incident, cyber risk, National Bank of Ukraine, digitalisation, NIS2, DORA, post-war recovery.

**ЗМІСТ**

**АНОТАЦІЯ** ..... **2**

**ВСТУП** ..... **5**

**РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ФІНАНСОВОЇ СИСТЕМИ** ..... **9**

1.1 Сутність, понятійний апарат та складові кібербезпеки у фінансовій сфері ... 9

1.2 Нормативно-правове регулювання кібербезпеки фінансової системи ..... 16

1.3 Міжнародний досвід та стандарти забезпечення кібербезпеки фінансових систем ..... 26

**РОЗДІЛ 2 АНАЛІЗ СТАНУ ТА ЗАГРОЗ КІБЕРБЕЗПЕЦІ ФІНАНСОВОЇ СИСТЕМИ УКРАЇНИ** ..... **33**

2.1 Структура, особливості функціонування та тенденції цифровізації фінансової системи України ..... 33

2.2 Аналіз кіберзагроз, вразливостей та наслідків кібератак на фінансовий сектор України ..... 39

2.3 Оцінка рівня кіберзахищеності та готовності фінансових установ до протидії кіберзагрозам ..... 48

**РОЗДІЛ 3 НАПРЯМИ ВДОСКОНАЛЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВОЇ СИСТЕМИ УКРАЇНИ** ..... **56**

3.1 Удосконалення нормативно-правового та інституційного забезпечення кібербезпеки фінансового сектору ..... 56

3.2 Технологічні та організаційні заходи підвищення стійкості фінансової системи до кіберзагроз ..... 64

3.3 Стратегічні пріоритети розвитку кібербезпеки фінансової системи України в умовах воєнного стану та поствоєнної відбудови ..... 69

**ВИСНОВКИ** ..... **78**

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ** ..... **81**

**ДЕКЛАРАЦІЯ про використання/невикористання штучного інтелекту. 100**

**ДОДАТКИ** ..... **101**

# ВСТУП

**Актуальність теми дослідження.** Фінансовий сектор будь-якої держави належить до критично важливої інфраструктури, стабільність якої безпосередньо впливає на економічну безпеку в цілому. Упродовж останнього десятиліття Україна пережила стрімку цифровізацію банківських послуг, запровадження електронних платіжних інструментів і розширення дистанційного обслуговування клієнтів, що супроводжувалося зростанням обсягів конфіденційних даних у цифровому просторі. Воєнний стан, запроваджений 24 лютого 2022 року, докорінно змінив характер загроз: кібератаки на фінансові установи набули системного характеру, а їхні наслідки виходять за межі технічних збоїв і торкаються платіжної стійкості, довіри громадян та міжнародної інтеграції країни [33; 67, с. 5–7].

Актуальність дослідження зумовлена кількома чинниками. Насамперед це ескалація гібридної агресії, у якій фінансова інфраструктура стала однією з пріоритетних мішеней. Крім того, євроінтеграційний курс вимагає адаптації національних правил кібербезпеки до вимог Директиви NIS2 і Регламенту DORA [114; 144]. Нарешті, фінансовий ринок потребує стійкості до загроз, що швидко еволюціонують: фішинг залишається основним початковим вектором атак [117, с. 6, 8], а зловмисники дедалі частіше використовують генеративні інструменти штучного інтелекту [4, с. 244–255].

Питання кібербезпеки фінансового сектору активно досліджують вітчизняні та зарубіжні науковці, проте наукова і законодавча база розвивається повільніше, ніж інформаційні системи та арсенал зловмисників. Праці, зосереджені на стандартах NIST та ISO/IEC 27001, дають методологічну основу, але потребують адаптації до специфіки національного законодавства та воєнного періоду. Комплексних досліджень, які б поєднували аналіз нормативної бази, емпіричну оцінку динаміки кіберінцидентів і вразливостей фінансового сектору та модель інституційного забезпечення кіберзахисту в період поствоєнної відбудови, на сьогодні недостатньо, що й зумовило вибір теми.

**Мета кваліфікаційної роботи** полягає в обґрунтуванні теоретично-методичних засад та практичних рекомендацій щодо вдосконалення кібербезпеки у фінансовій системі України для подальшого соціально-економічного розвитку та захисту інтересів держави.

Для досягнення поставленої мети необхідно вирішити такі **завдання**:

а) розкрити сутність, понятійний апарат і складові кібербезпеки у фінансовій сфері;

б) систематизувати нормативно-правове забезпечення кібербезпеки фінансового сектору України та зіставити темпи його розвитку з темпами цифровізації і зростання кіберзагроз;

в) узагальнити міжнародний досвід і стандарти забезпечення кібербезпеки фінансових систем;

г) оцінити рівень кіберзахищеності та готовності фінансових установ різних категорій до протидії кіберзагрозам;

д) обґрунтувати напрями вдосконалення нормативно-правового, інституційного, технологічного та кадрового забезпечення кібербезпеки фінансової системи України.

**Об’єктом дослідження** є процеси забезпечення кібербезпеки фінансової системи України.

**Предметом дослідження** є теоретико-методичні засади та організаційно-правові, інституційні й технологічні механізми забезпечення кібербезпеки фінансової системи України.

**Методи дослідження.** У роботі застосовано методи аналізу і синтезу, абстрактно-логічний (уточнення понятійного апарату), системний, порівняльний (зіставлення національних моделей кіберзахисту), історичний (визначення часових лагів регуляторного реагування), статистичний з побудовою рядів динаміки (аналіз кіберінцидентів і платіжного шахрайства), табличний, SWOT-аналізу, бальної оцінки (оцінка кіберзахищеності установ), нормативного і сценарного розрахунку (кадрова потреба та очікуваний ефект), а також узагальнення.

**Інформаційною базою дослідження** стали закони України, укази Президента України, постанови Кабінету Міністрів і Національного банку України, звіти НБУ, Держспецзв'язку, НКЦК і CERT-UA, акти ЄС, міжнародні стандарти, звіти МВФ, ENISA, Ради з фінансової стабільності, праці науковців та інтернет-ресурси.

**Наукова новизна одержаних результатів** полягає в поглибленні теоретичних засад і розробленні практичних рекомендацій щодо забезпечення кібербезпеки фінансової системи України. Найбільш вагомі результати, що характеризують наукову новизну дослідження, полягають у такому:

*вперше:*

а) запропоновано модель єдиного органу кіберстійкості фінансового сектору в структурі Національного банку України, яка, на відміну від чинного розподілу функцій між кількома державними органами, закріплює за ним галузевий нагляд, прийом звітності про інциденти та координацію реагування, усуває дублювання вимог і передбачає поетапне створення робочих місць для фахівців з кібербезпеки в період поствоєнної відбудови з обґрунтуванням кадрової потреби сектору нормативним методом;

*удосконалено:*

б) класифікацію кіберінцидентів у фінансовому секторі за рівнями серйозності з диференційованими строками первинного, проміжного й остаточного повідомлення, гармонізованими з вимогами NIS2 і DORA, що забезпечує однозначність звітування для всіх учасників ринку;

в) методичний підхід до порівняльної оцінки кіберзахищеності фінансових установ різних категорій за сімома критеріями з бальним вимірюванням, що дає змогу кількісно визначити розрив між системно важливими банками та небанківськими установами і обґрунтувати пріоритети регуляторного втручання;

*набули подальшого розвитку:*

г) понятійний апарат кібербезпеки фінансової системи через розмежування категорій «інформаційна безпека», «кібербезпека» та «кіберстійкість» і обґрунтування положення про відставання темпів оновлення законодавчої та

наукової бази від темпів цифровізації фінансових послуг і зростання кіберзагроз з визначенням часових лагів регуляторного реагування;

д) пропозиції щодо внесення змін до законів України «Про основні засади забезпечення кібербезпеки України», «Про банки і банківську діяльність», «Про захист персональних даних», «Про платіжні послуги», Кримінального кодексу України та нормативно-правового акта Національного банку України з інформаційної безпеки, які деталізують обов'язки фінансових установ щодо звітування, тестування та відповідальності.

**Практичне значення одержаних результатів** полягає в тому, що його висновки можна застосовувати для вдосконалення системи кіберзахисту в банківському секторі в умовах постійного зростання кількості та складності цифрових загроз. Запропоновані в роботі підходи до виявлення, оцінювання та запобігання кіберзагрозам спрямовані на підвищення надійності фінансових операцій і збереження стабільності функціонування банківських установ. Матеріали роботи також можуть бути використані при розробці внутрішніх політик інформаційної безпеки та планів реагування на інциденти.

Практичну придатність результатів підтверджує Довідка АТ «Банк «Південний» №16/0301/15863/2026 від 28.10.2026. У ній зазначено, що тема дослідження є актуальною як з теоретичної, так і з практичної точки зору, а результати рекомендовано до розгляду та можливого впровадження в діяльність банку. Установа визначила такі напрями використання отриманих результатів:

удосконалення підходів до виявлення, оцінювання та запобігання кіберзагрозам у банківській діяльності для підвищення надійності фінансових операцій;

Окремо в довідці наголошено, що результати дослідження мають практичне значення для підвищення рівня кіберзахисту банку.

**Структура та обсяг роботи.** Кваліфікаційна робота складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел (154 найменування) і додатка. Загальний обсяг роботи становить 107 сторінок, обсяг основної частини становить 80 сторінок. Робота містить 32 таблиці та 1 рисунок, з них 26 в основній частині та 6 у додатку, а також дві формули.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ФІНАНСОВОЇ СИСТЕМИ

## 1.1 Сутність, понятійний апарат та складові кібербезпеки у фінансовій сфері

Трансформація фінансових послуг під впливом цифрових технологій створила принципово нове середовище функціонування банків, страхових компаній та інших учасників ринку. Перехід від паперових документів до електронних реєстрів, поширення мобільного банкінгу та впровадження хмарних обчислень змінили не лише технологічні процеси, а й характер ризиків, з якими стикається фінансова галузь. Традиційні загрози, як-от крадіжка готівки чи підробка документів, доповнюються атаками на інформаційні системи, компрометацією баз даних і дестабілізацією програмних комплексів. Ця трансформація зумовила появу окремого напряму досліджень, що отримав назву кібербезпеки фінансової системи [72, с. 90–96; 131, p. 466–483].

Еволюція терміна «кібербезпека» тісно пов’язана з розвитком інформаційних технологій та ускладненням архітектури комп’ютерних мереж. На початковому етапі науковці та практики оперували переважно поняттям інформаційної безпеки, під яким розуміли захист даних від несанкціонованого доступу, втрати або спотворення. З поширенням глобальних мереж, інтернету речей і хмарних сервісів сфера загроз вийшла за межі локальних корпоративних систем, тому сучасні підходи трактують кібербезпеку ширше: як захищеність інтересів особи, суспільства і держави в кіберпросторі, стійкість цифрової інфраструктури та неперервність бізнес-процесів. Основні підходи до визначення цього поняття в нормативних актах і міжнародних документах систематизовано в табл. 1.1.

Як видно з табл. 1.1, національне законодавство наголошує на захищеності життєво важливих інтересів і протидії загрозам національній безпеці, рекомендація МСЕ-Т X.1205 має інструментальний характер, ISO/IEC 27032 є ризик-орієнтованим, а Рада з фінансової стабільності визначає кібербезпеку через збереження конфіденційності, цілісності та доступності інформації і

доповнює її категорією кіберстійкості. Узагальнюючи ці підходи, під кібербезпекою фінансової системи доцільно розуміти стан захищеності фінансових установ, платіжної та ринкової інфраструктури, даних і коштів клієнтів у кіберпросторі, за якого забезпечуються конфіденційність, цілісність і доступність фінансових операцій, а також кіберстійкість, тобто здатність системи продовжувати виконання критичних функцій під час кібератак і швидко відновлюватися після них.

Таблиця 1.1 **Підходи до визначення понять «кібербезпека» і «кіберстійкість» у нормативних актах і міжнародних документах**

| Джерело | Визначення | Акцент підходу |
|---|---|---|
| Закон України «Про основні засади забезпечення кібербезпеки України» (2017) | «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» | Захищеність національних інтересів |
| Рекомендація МСЕ-Т X.1205 (2008) | Сукупність інструментів, політик, концепцій безпеки, заходів захисту, настанов, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можуть бути використані для захисту кіберсередовища, а також активів організації та користувачів | Інструментальний |
| ISO/IEC 27032:2023 | Захист людей, суспільства, організацій і держав від кіберризиків | Ризик-орієнтований |
| Рада з фінансової стабільності, Cyber Lexicon (2023) | Збереження конфіденційності, цілісності та доступності інформації та (або) інформаційних систем через кіберсередовище; можуть також охоплюватися автентичність, підзвітність, неспростовність і надійність | Властивості інформації |
| Рада з фінансової стабільності, Cyber Lexicon (2023): кіберстійкість | Здатність організації продовжувати виконання своєї місії, передбачаючи кіберзагрози та адаптуючись до них, протистоячи кіберінцидентам, стримуючи їх і швидко відновлюючись | Стійкість і безперервність |

Джерело: систематизовано автором за [58, ст. 1; 139; 127; 110, с. 10]; визначення з англомовних документів наведено в перекладі автора.

Кіберпростір у цьому контексті є глобальним динамічним середовищем, утвореним взаємопов’язаними інформаційно-комунікаційними системами, мережами та ресурсами. Він не має чітких географічних кордонів, що ускладнює правове регулювання та оперативне реагування на інциденти. Для фінансового сектору специфіка кіберпростору полягає в концентрації конфіденційних даних клієнтів, реальному характері транзакцій і необхідності миттєвої обробки

платіжних доручень. Банківська таємниця, персональні дані та комерційна інформація створюють привабливе середовище для зловмисників різного рівня: від окремих хакерів до організованих кримінальних груп і державних структур.

Інтеграція фінансових технологій у традиційну банківську екосистему породила додаткові вектори ризиків. Відкриті банківські інтерфейси дозволяють стороннім розробникам отримувати доступ до фінансових даних клієнтів за їхньою згодою, що розширює периметр захисту за межі корпоративної мережі банку. Безпека API-шлюзів, автентифікація сторонніх застосунків і контроль потоків даних між партнерами стають невід'ємною частиною кіберзахисту, а партнерство з платіжними агрегаторами, страховими брокерами та інвестиційними платформами формує ланцюжки довіри, у яких компрометація однієї ланки ставить під загрозу всю екосистему [83, с. 186–196].

Розмежування понять «інформаційна безпека» та «кібербезпека» залишається дискусійним, а в сучасних дослідженнях пропонують навіть замінити інформаційну складову економічної безпеки ширшою категорією цифрової безпеки [3, с. 234–246]. Інформаційна безпека зосереджена переважно на збереженні конфіденційності, цілісності та доступності даних незалежно від їхньої форми. Кібербезпека додає до цього протидію активним деструктивним впливам, розвідувальній діяльності в мережах і захист критичної інфраструктури від цілеспрямованих атак, а кіберстійкість переносить акцент із запобігання будь-якому проникненню на здатність зберігати критичні функції. Для фінансової галузі це розмежування має практичне значення, оскільки визначає структуру підрозділів безпеки, бюджетування та пріоритети інвестування.

Кіберзагроза як ключове поняття дослідження охоплює сукупність умов і чинників, що створюють небезпеку порушення функціонування інформаційних систем, витоку або спотворення даних. У фінансовій сфері кіберзагрози набувають специфічних форм. Розподілені атаки на відмову в обслуговуванні спрямовані на параліч каналів обслуговування клієнтів, фішингові кампанії використовують соціальну інженерію для отримання облікових даних, програми-вимагачі шифрують корпоративні бази даних і вимагають викуп, а цілеспрямовані персистентні загрози передбачають тривале приховане

перебування зловмисників у мережі. Окрему категорію становлять інсайдерські загрози, адже внутрішні суб’єкти мають легітимний доступ до критичних систем [31, с. 125–139].

Кіберінцидент фіксує факт реалізації загрози. Згідно із законом, це подія або ряд несприятливих подій ненавмисного характеру та (або) таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій і створюють імовірність порушення штатного режиму їх функціонування, тоді як кібератака охоплює навмисні дії в кіберпросторі, спрямовані на порушення конфіденційності, цілісності чи доступності електронних інформаційних ресурсів [58, ст. 1]. Рада з фінансової стабільності трактує кіберінцидент ширше, як кіберподію, що негативно впливає на кібербезпеку інформаційної системи незалежно від того, чи була вона результатом зловмисних дій [110, с. 10]. У фінансовому секторі класифікація інцидентів базується на масштабі наслідків: від локальних спроб несанкціонованого доступу до системних атак, що спричиняють тривале припинення обслуговування клієнтів. Реагування на кіберінцидент вимагає чітких процедур ідентифікації, локалізації, ліквідації наслідків і відновлення роботи систем, а тривалість простою прямо впливає на фінансові збитки та втрату довіри клієнтів.

Ключовою категорією управлінського підходу до кібербезпеки є кіберризик. Рада з фінансової стабільності визначає його як поєднання ймовірності виникнення кіберінцидентів та їхніх наслідків [110, с. 10], а Закон України «Про платіжні послуги» трактує кіберризик як ризик виникнення збитків або додаткових втрат фінансових установ і учасників платіжного ринку внаслідок реалізації кіберзагроз [59, ст. 66]. Національний банк окремо визначає системний кіберризик, тобто ризик порушення стабільності банківської системи внаслідок реалізації кіберзагроз щодо окремого банку через недоліки в його кіберстійкості [42, п. 7.33]. Саме концепція системного кіберризику пов’язує кібербезпеку окремої установи з фінансовою стабільністю держави: кіберризики здатні поширюватися між установами та секторами економіки, тому їх необхідно

інтегрувати в систему управління операційним ризиком і враховувати під час макропруденційного аналізу [31, с. 125–139; 90].

Кібербезпека фінансової системи тісно пов’язана з ширшою категорією фінансово-економічної безпеки. Цифровізація зумовлює заміну традиційної інформаційної складової економічної безпеки категорією цифрової безпеки, рівень якої залежить від інституційного середовища та масштабу діяльності суб’єкта [3, с. 234–246], а для фінансових установ кіберзагрози безпосередньо впливають на операційну діяльність, інформаційну та економічну безпеку, причому фінансовий сектор зазнає одних з найвищих втрат від кіберінцидентів [131, p. 466–483]. Отже, кібербезпеку доцільно розглядати як складову фінансової безпеки, що забезпечує збереження фінансових ресурсів, даних і довіри клієнтів у цифровому середовищі.

Фінансова стабільність як економічна категорія тісно пов’язана з рівнем кібербезпеки. Під фінансовою стабільністю розуміють стан фінансової системи, за якого вона здатна ефективно виконувати свої функції, протистояти шокам і адаптуватися до змін. Кібератака на системно важливий банк або платіжного оператора може спричинити ланцюгову реакцію: блокування рахунків, зрив виплат заробітної плати, порушення розрахунків за комунальні послуги. За оцінками Міжнародного валютного фонду, екстремальні втрати фінансових компаній від кіберінцидентів, які статистично очікуються раз на десять років, становлять близько 2,5 млрд дол. США, що здатне перерости в загрозу макрофінансовій стабільності [96, с. 7].

Критична інформаційна інфраструктура фінансового сектору охоплює об’єкти, робота яких безпосередньо впливає на національну безпеку: системи міжбанківських розрахунків, централізовані реєстри, автоматизовані банківські системи, інфраструктуру електронних платежів і системи дистанційного обслуговування. Порушення функціонування хоча б одного з цих елементів створює системні ризики для всього ринку, тому держава встановлює підвищені вимоги до їхнього захисту, включно з використанням засобів криптографічного захисту, що мають позитивний висновок експертизи, регулярним тестуванням на проникнення та обов’язковим інформуванням про інциденти [54; 40].

Складові кібербезпеки фінансової установи утворюють багаторівневу систему, в якій технічні засоби, організаційні процедури, правові норми та людський чинник взаємно доповнюють один одного. Технічна складова охоплює мережевий захист, криптографію, платформи керування інформацією про події безпеки та захист кінцевих точок. Організаційна складова визначає політики, розподіл ролей і рівнів доступу, плани безперервності бізнесу та аудит. Правова складова встановлює рамки відповідальності, вимоги регуляторів і стандарти, а людська складова визначає здатність персоналу розпізнавати атаки соціальної інженерії. Зміст і інструменти кожної складової узагальнено в табл. 1.2.

Дані табл.1.2 показують, що жодна складова не є самодостатньою. Технічні засоби втрачають ефективність без чітких процедур, організаційні заходи не працюють без правового забезпечення та механізмів відповідальності, а людський чинник вимагає постійного навчання. Окремо виділено стратегічну складову, оскільки сучасні регуляторні вимоги, зокрема DORA, покладають на органи управління фінансової установи безпосередню відповідальність за ризики у сфері інформаційно-комунікаційних технологій [144, ст. 5].

Правова складова кібербезпеки визначає рамки відповідальності та механізми регулювання. Національне законодавство встановлює вимоги до обробки персональних даних, критерії кваліфікації кіберзлочинів і повноваження спеціальних органів, міжнародні стандарти ISO/IEC 27001 і ISO/IEC 27002 надають методологію побудови системи управління інформаційною безпекою, а для фінансового сектору додатково діють галузеві нормативи: стандарт безпеки даних індустрії платіжних карток, вимоги міжнародних платіжних систем і регуляторні вимоги щодо управління операційними ризиками [124; 125; 140]. Регуляторний тиск на фінансові установи постійно зростає, а міжнародні органи, зокрема Комітет з платіжних та ринкових інфраструктур і Міжнародна організація комісій з цінних паперів, розробили принципи кіберстійкості фінансової інфраструктури, що закладають основи гармонізації підходів на глобальному рівні [120].

Таблиця 1.2 **Складові системи кібербезпеки фінансової установи**

| Складова | Зміст | Основні інструменти |
|---|---|---|
| Технічна | Захист мереж, систем, даних і кінцевих точок від несанкціонованого доступу та шкідливого коду | Міжмережеві екрани, системи виявлення та запобігання вторгненням, шифрування, SIEM, EDR/XDR, резервне копіювання |
| Організаційна | Процедурні механізми функціонування системи безпеки та управління кіберризиками | Політика інформаційної безпеки, управління доступом, плани безперервності бізнесу, аудит, управління інцидентами |
| Правова | Рамки відповідальності, вимоги регуляторів, порядок взаємодії з державними органами | Закони, нормативно-правові акти НБУ, стандарти ISO/IEC, PCI DSS, договірні вимоги до постачальників |
| Людська | Обізнаність, кваліфікація і поведінка персоналу та клієнтів | Навчання, імітаційні фішингові тести, тренінги з реагування, програми кібергігієни для клієнтів |
| Стратегічна (управлінська) | Інтеграція кіберризиків у корпоративне управління та ризик-апетит | Стратегія кібербезпеки, звітування наглядовій раді, бюджетування, персональна відповідальність керівництва |

Джерело: систематизовано автором на основі [136; 124; 47; 31, с. 125–139; p. 224–233].

Людський чинник залишається одним із найвразливіших елементів системи кібербезпеки. Технічні засоби можуть бути досконалими, проте помилка адміністратора, необережність працівника під час роботи з електронною поштою або навмисні дії інсайдера здатні нівелювати всі інвестиції в інфраструктуру. Тому фінансові установи спрямовують значні ресурси на програми підвищення обізнаності персоналу, імітаційні фішингові тести та тренінги з реагування на інциденти. Соціальна інженерія як метод маніпулювання людьми з метою отримання конфіденційної інформації постійно еволюціонує, тож навчання має бути безперервним процесом, а не разовою акцією [65, с. 331–347].

Модель CIA (конфіденційність, цілісність, доступність) лежить в основі більшості систем кіберзахисту. Конфіденційність гарантує доступ до інформації лише уповноваженим суб’єктам, цілісність передбачає захист даних від несанкціонованого редагування, доступність означає можливість отримання інформації та ресурсів у потрібний час. У банківській практиці ці принципи реалізуються через багатофакторну автентифікацію, контроль цілісності транзакцій, резервування каналів зв’язку та дублювання критичних систем. Рамкова модель NIST Cybersecurity Framework у версії 2.0 доповнила класичні функції ідентифікації, захисту, виявлення, реагування та відновлення функцією

управління (Govern), що підкреслює роль керівництва організації в управлінні кіберризиками [136, с. 3–5].

Економічний вимір кібербезпеки фінансового сектору виходить за межі прямих збитків від інцидентів. Вартість реагування на кібератаку зростає залежно від часу виявлення загрози, а витрати на юридичний супровід, компенсації клієнтам, аудит і оновлення інфраструктури часто перевищують суму вимаганого викупу. Непрямі збитки проявляються у відтоку клієнтів, зниженні капіталізації та подорожчанні страхування кіберризиків. За даними щорічних досліджень IBM, середня вартість витоку даних у фінансовій галузі стабільно перевищує середній показник за всіма галузями (детальніше див. 2.2) [103, с. 15; 107, с. 12–13]. Тому інвестиції в превентивний захист доцільно розглядати не як операційні витрати, а як складову капітальної вартості бізнесу.

Специфіка кібербезпеки у фінансовій сфері визначається поєднанням високої вартості даних, вимоги до миттєвості транзакцій та інтенсивної регуляторної уваги. Банк обслуговує сотні тисяч клієнтів одночасно, обробляючи мільйони операцій на добу, тому рішення в галузі кіберзахисту мають балансувати між рівнем захисту та зручністю користувача, між витратами на безпеку та операційною ефективністю. Надмірні обмеження доступу відштовхують клієнтів, тоді як недостатній захист відкриває вектори для атак.

Отже, кібербезпека фінансової системи має комплексний характер, а побудова стійкої системи кіберзахисту можлива лише за умови узгодженої взаємодії технічних, організаційних, правових, людських і управлінських ресурсів, скоординованих стратегією, визначеною на рівні керівництва установи та узгодженою з вимогами національного регулятора.

## 1.2 Нормативно-правове регулювання кібербезпеки фінансової системи

Правове регулювання кібербезпеки фінансового сектору України формувалося в умовах стислих строків адаптації національної правової системи до викликів цифрової економіки. Конституція України визначає забезпечення інформаційної безпеки однією з найважливіших функцій держави, гарантує

таємницю листування та іншої кореспонденції, недоторканність особистого життя і захист права власності [19, ст. 17, 31, 32, 41]. Ці положення, хоча й ухвалені до масового поширення цифрових фінансових послуг, стали основою для спеціальних норм, що регулюють обіг електронних даних у банківській і платіжній сферах. Банківська таємниця як складова права на недоторканність приватного життя трансформувалася в обов'язок фінансових установ забезпечувати конфіденційність не лише паперових документів, а й електронних реєстрів, журналів транзакцій і метаданих клієнтських сесій.

Законодавче поле має дворівневу структуру: загальні акти, що поширюються на всіх суб'єктів, і спеціальні норми, адресовані банкам, надавачам платіжних послуг та іншим учасникам фінансового ринку. До першої групи належить Закон України «Про інформацію», що закріпив поділ інформації на відкриту та з обмеженим доступом, до якої належать конфіденційна, таємна та службова інформація [53, ст. 20, 21]. Для фінансових установ ця класифікація має практичне значення, оскільки визначає коло осіб, яким дозволено доступ до критичних масивів даних, режим їхнього зберігання та передавання. Закон України «Про захист персональних даних» зобов'язує володільців і розпорядників персональних даних забезпечувати їх захист від випадкових втрати або знищення та від незаконної обробки, а також визначати структурний підрозділ або відповідальну особу, що взаємодіє з Уповноваженим Верховної Ради України з прав людини [52, ст. 24]. Водночас закон не містить обов'язку повідомляти контролюючий орган і суб'єктів даних про витоки персональних даних, що для банків з мільйонними клієнтськими базами є суттєвою прогалиною. Закон України «Про захист інформації в інформаційно-комунікаційних системах» встановлює вимоги до комплексних систем захисту інформації, що належить державі або вимога щодо захисту якої встановлена законом [51].

Центральне місце посідає Закон України «Про основні засади забезпечення кібербезпеки України», ухвалений у жовтні 2017 року, який вперше визначив на державному рівні поняття кібербезпеки, кіберзахисту, кібератаки та кіберінциденту, суб'єктів національної системи кібербезпеки та їхні

повноваження [58, ст. 1, 8]. Координацію в цій сфері здійснює Національний координаційний центр кібербезпеки як робочий орган РНБО, утворений у 2016 році [57], а Державна служба спеціального зв'язку та захисту інформації забезпечує формування і реалізацію політики щодо кіберзахисту державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, функціонування Державного центру кіберзахисту та урядової команди реагування CERT-UA [58, ст. 8]. Національний банк України, відповідно до п. 6 ч. 2 ст. 8 закону в редакції Закону «Про платіжні послуги», визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими учасниками ринків фінансових послуг, операторами та учасниками платіжних систем, здійснює контроль за їх виконанням, створює центр кіберзахисту НБУ і забезпечує оцінювання стану кіберзахисту на об'єктах критичної інфраструктури фінансового сектору [58, ст. 8]. Закон України від 27 березня 2025 року № 4336-IX суттєво оновив цю модель: запровадив систему національної, галузевих і регіональних команд реагування на кіберінциденти, обов'язок повідомляти про значні кіберінциденти та розширив координаційні повноваження НКЦК [35; 28, с. 7–11].

Закон України «Про критичну інфраструктуру» заклав засади захисту об'єктів, порушення функціонування яких загрожує життєво важливим інтересам держави, а Національний банк визначений секторальним органом у сфері захисту критичної інфраструктури у фінансовому секторі [54; 55, п. 2]. Закон України «Про Національний банк України» покладає на регулятор формування переліку об'єктів критичної інфраструктури та реєстру об'єктів критичної інформаційної інфраструктури, визначення критеріїв віднесення до них і забезпечення оцінювання стану кіберзахисту [56, ст. 7], а Закон України «Про електронну ідентифікацію та електронні довірчі послуги» визначає правові засади електронної ідентифікації клієнтів і кваліфікованих електронних підписів, які застосовуються під час дистанційного обслуговування [39]. Спеціальне фінансове законодавство формує додатковий рівень вимог. Закон України «Про банки і банківську діяльність» зобов'язує банки зберігати банківську таємницю та створювати комплексну систему внутрішнього

контролю і управління ризиками, проте прямо не згадує інформаційну безпеку, кіберзахист чи ризики інформаційно-комунікаційних технологій [32, ст. 44]. Закон України «Про платіжні послуги», що замінив Закон «Про платіжні системи та переказ коштів в Україні», вперше на рівні закону закріпив поняття кіберризику, обов'язок надавачів платіжних послуг затверджувати правила управління операційними ризиками, кіберризиками та ризиками безпеки і повідомляти Національний банк про істотні операційні інциденти, кіберінциденти та інциденти безпеки [59, ст. 66, 67]. Загальні законодавчі акти систематизовано в табл. 1.3.

Таблиця 1.3 **Загальні законодавчі акти України у сфері кібербезпеки**

| Нормативно-правовий акт | Ким і коли прийнято | Основний зміст щодо кібербезпеки |
|---|---|---|
| Конституція України | Верховна Рада України, 28.06.1996 | Інформаційна безпека як функція держави (ст. 17); таємниця кореспонденції (ст. 31); недоторканність особистого життя (ст. 32) |
| Закон України «Про інформацію» | Верховна Рада України, 02.10.1992 № 2657-XII | Режими доступу до інформації; інформація з обмеженим доступом |
| Закон України «Про захист інформації в інформаційно-комунікаційних системах» | Верховна Рада України, 05.07.1994 № 80/94-ВР | Комплексна система захисту інформації |
| Кримінальний кодекс України | Верховна Рада України, 05.04.2001 № 2341-III | Відповідальність за несанкціоноване втручання в роботу систем і мереж та інші діяння (ст. 361–363-1) |
| Закон України «Про захист персональних даних» | Верховна Рада України, 01.06.2010 № 2297-VI | Обов'язок захищати персональні дані; контроль Уповноваженого Верховної Ради України з прав людини |
| Закон України «Про основні засади забезпечення кібербезпеки України» | Верховна Рада України, 05.10.2017 № 2163-VIII | Понятійний апарат; суб'єкти національної системи кібербезпеки; повноваження НБУ щодо кіберзахисту фінансового сектору (п. 6 ч. 2 ст. 8) |
| Закон України «Про критичну інфраструктуру» | Верховна Рада України, 16.11.2021 № 1882-IX | Засади захисту критичної інфраструктури; секторальні органи |
| Закон України № 2149-IX | Верховна Рада України, 24.03.2022 | Посилення відповідальності за кіберзлочини в умовах воєнного стану |
| Закон України № 4336-IX | Верховна Рада України, 27.03.2025 | Галузеві та регіональні команди реагування; повідомлення про значні кіберінциденти; повноваження НКЦК |

Джерело: систематизовано автором за [19; 53; 51; 20; 52; 58; 54; 38; 35].

Отже, законодавча база охоплює всі рівні регулювання, проте спеціальні вимоги до кіберзахисту фінансових установ на рівні законів закріплено фрагментарно: у Законі «Про основні засади забезпечення кібербезпеки України» у вигляді повноважень НБУ та в Законі «Про платіжні послуги»

стосовно надавачів платіжних послуг. Основний масив вимог встановлено підзаконними актами Президента України, Кабінету Міністрів України та Національного банку України (табл. 1.5 і 1.6).

Таблиця 1.4 **Спеціальні законодавчі акти фінансового сектору з вимогами щодо кібербезпеки**

| Нормативно-правовий акт | Ким і коли прийнято | Основний зміст щодо кібербезпеки |
|---|---|---|
| Закон України «Про банки і банківську діяльність» | Верховна Рада України, 07.12.2000 № 2121-III | Банківська таємниця; система внутрішнього контролю й управління ризиками (без прямих вимог до кіберзахисту) |
| Закон України «Про Національний банк України» | Верховна Рада України, 20.05.1999 № 679-XIV | Повноваження НБУ щодо переліку об’єктів критичної інфраструктури та оцінювання стану кіберзахисту (ст. 7) |
| Закон України «Про платіжні послуги» | Верховна Рада України, 30.06.2021 № 1591-IX | Поняття кіберризику; управління операційними ризиками та ризиками безпеки; повідомлення НБУ про істотні інциденти (ст. 66–67) |
| Закон України «Про фінансові послуги та фінансові компанії» | Верховна Рада України, 14.12.2021 № 1953-IX | Вимоги до діяльності небанківських фінансових установ |
| Закон України «Про віртуальні активи» | Верховна Рада України, 17.02.2022 № 2074-IX | Правовий статус віртуальних активів (введення в дію пов’язане з податковими змінами) |
| Закон України «Про хмарні послуги» | Верховна Рада України, 17.02.2022 № 2075-IX | Засади надання хмарних послуг (без галузевих вимог для фінансового сектору) |

Джерело: систематизовано автором за [32; 56; 59; 63; 34; 64].

Серед документів, наведених у табл. 1.5, Стратегія кібербезпеки України 2021 року визначила пріоритетами стримування, кіберстійкість і взаємодію з міжнародними партнерами, а Кабінет Міністрів сформував організаційно-технічну модель кіберзахисту, загальні вимоги до кіберзахисту об’єктів критичної інфраструктури та у 2025 році затвердив Національний план реагування на кіберінциденти, кібератаки та кіберзагрози [62; 40; 46; 9]. Воєнний стан, запроваджений з 24 лютого 2022 року, змінив режим правового регулювання, розширивши повноваження органів сектору безпеки та оборони щодо захисту інформаційних ресурсів [33; 60].

Таблиця 1.5 **Акти Президента України та Кабінету Міністрів України у сфері кібербезпеки**

| Документ | Ким і коли затверджено | Основний зміст |
|---|---|---|
| Про Національний координаційний центр кібербезпеки | Указ Президента України від 07.06.2016 № 242/2016 | Утворення НКЦК як робочого органу РНБО |
| Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури | Постанова КМУ від 19.06.2019 № 518 | Базові вимоги до кіберзахисту об'єктів критичної інфраструктури |
| Стратегія національної безпеки України | Указ Президента України від 14.09.2020 № 392/2020 | Кібербезпека як складова національної безпеки |
| Деякі питання об'єктів критичної інформаційної інфраструктури | Постанова КМУ від 09.10.2020 № 943 | Організаційні питання функціонування об'єктів критичної інформаційної інфраструктури |
| Деякі питання об'єктів критичної інфраструктури | Постанова КМУ від 09.10.2020 № 1109 | Організаційні питання захисту об'єктів критичної інфраструктури |
| Система виявлення вразливостей і реагування на кіберінциденти | Постанова КМУ від 23.12.2020 № 1295 | Функціонування системи виявлення вразливостей і реагування |
| Стратегія кібербезпеки України | Указ Президента України від 26.08.2021 № 447/2021 | Пріоритети: стримування, кіберстійкість, взаємодія |
| Положення про організаційно-технічну модель кіберзахисту | Постанова КМУ від 29.12.2021 № 1426 | Організаційно-технічна модель кіберзахисту |
| Про введення воєнного стану в Україні | Указ Президента України від 24.02.2022 № 64/2022 | Правовий режим воєнного стану |
| Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози | Постанова КМУ від 26.11.2025 № 1533 | Національний план реагування на кіберінциденти |

Джерело: систематизовано автором за [57; 40; 61; 7; 8; 6; 62; 46; 33; 9].

Табл. 1.6 свідчить, що Національний банк сформував найрозвиненішу в Україні галузеву систему вимог до кіберзахисту. З 2018 року діє команда реагування на кіберінциденти в банківській системі CSIRT-NBU, що працює у складі Центру кіберзахисту НБУ і забезпечує інформаційний обмін, координацію дій та інформування банків про кіберзагрози [49, п. 2, 13; 108]. Банки зобов'язані інформувати Центр кіберзахисту про значні кіберінциденти протягом 24 годин (попереднє повідомлення), 72 годин (проміжне повідомлення) і не пізніше ніж через місяць (остаточний звіт) [41], а за порушення законодавства з питань кіберзахисту, що створили загрозу реалізації системного кіберризику, Національний банк може накласти на банк штраф у розмірі 0,01 % зареєстрованого статутного капіталу [42, п. 7.33]. З 2023 року до Положення про

систему управління ризиками включено окремі вимоги щодо ризиків інформаційно-комунікаційних технологій та інформаційної безпеки, а у 2025 році вимоги до кіберзахисту поширено на страховиків, кредитні спілки, фінансові компанії і ломбарди [37; 48].

Таблиця 1.6 **Нормативно-правові акти Національного банку України з питань кібербезпеки фінансового сектору**

| Нормативно-правовий акт | Дата і номер постанови Правління НБУ | Основний зміст |
|---|---|---|
| Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України | 28.09.2017 № 95 | Система управління інформаційною безпекою банку; періодичні тести на проникнення (п. 108) |
| Положення про організацію системи управління ризиками в банках України та банківських групах | 11.06.2018 № 64 (зі змінами від 30.03.2023 № 40) | Кіберризики у складі операційного ризику; вимоги до ризиків ІКТ та інформаційної безпеки |
| Положення про здійснення контролю за дотриманням банками вимог з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг | 16.01.2021 № 4 | Порядок перевірок кіберзахисту банків |
| Положення про захист інформації та кіберзахист учасниками платіжного ринку | 19.05.2021 № 43 | Вимоги до захисту інформації надавачів платіжних послуг; невідкладне повідомлення про кіберінциденти |
| Зміни до Положення про застосування НБУ заходів впливу | 04.08.2022 № 169 | Штраф за порушення у сфері кіберзахисту; поняття системного кіберризику |
| Положення про організацію кіберзахисту в банківській системі України | 12.08.2022 № 178 | Центр кіберзахисту НБУ, CSIRT-NBU, інформаційний обмін |
| Зміни з питань інформаційної безпеки та кіберзахисту | 25.02.2025 № 24 | Інформування про значні кіберінциденти: 24 год, 72 год, 1 місяць |
| Положення про критичну інфраструктуру фінансового сектору | 27.06.2025 № 69 | НБУ як секторальний орган у сфері захисту критичної інфраструктури |
| Положення про вимоги до системи управління ризиками надавача нефінансових платіжних послуг | 02.07.2025 № 73 | Негайне повідомлення НБУ про інциденти безпеки та кіберінциденти високого і критичного рівнів |
| Положення про відкритий банкінг в Україні | 25.07.2025 № 80 | Доступ надавачів нефінансових платіжних послуг до рахунків через API |
| Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг | 09.12.2025 № 143 | Поширення вимог на страховиків, кредитні спілки, фінансові компанії, ломбарди |

Джерело: систематизовано автором за [47; 50; 37; 45; 44; 42; 49; 41; 55; 43; 23; 48].

Правове регулювання кібербезпеки фінансового сектору неможливо розглядати ізольовано від міжнародних зобов’язань України. Угода про асоціацію з Європейським Союзом передбачає наближення національного законодавства до права ЄС, включно зі сферою електронних комунікацій і

захисту даних. Загальний регламент захисту даних не поширюється безпосередньо на територію України, проте створює стандарти, якими керуються міжнародні банки та платіжні системи під час обробки даних європейських клієнтів, а Директива NIS2 і Регламент DORA формують цільову модель регулювання, імплементація якої потребуватиме уточнення критеріїв ідентифікації суб'єктів, строків звітування та повноважень наглядових органів [143; 114; 144; 10, с. 46–51].

Незважаючи на значний обсяг нормативних актів, система правового регулювання містить низку прогалин і суперечностей. Закон «Про основні засади забезпечення кібербезпеки України» має рамковий характер і не враховує специфіки платіжних операцій та архітектури банківських інформаційних систем, а Закон «Про банки і банківську діяльність» у статтях 44 і 66 прямо не згадує інформаційну безпеку, кіберзахист чи ризики ІКТ. Повноваження Національного банку та Держспецзв'язку в частині об'єктів критичної інформаційної інфраструктури фінансового сектору частково дублюються, що створює ризики надмірного адміністрування або, навпаки, зон безконтрольності: НБУ зосереджений на операційних ризиках і фінансовій стабільності, Держспецзв'язку зосереджена на технічному захисті інформації та критичної інфраструктури, а критерії значного кіберінциденту і порядок обміну інформацією визначаються кожним органом окремо [41; 5; 2, с. 35–42]. Національний координаційний центр кібербезпеки прямо визнає наявність секторальних колізій у регулюванні, зокрема щодо фінансового сектору, який частково виведений із загального регуляторного поля [28, с. 12]. Відсутній єдиний механізм обміну інформацією про кіберзагрози між усіма учасниками фінансового ринку, а правова база не стимулює добровільне розкриття даних про інциденти, оскільки установи побоюються репутаційних втрат, а довіра між державою і бізнесом у сфері кібербезпеки залишається недостатньою [74, с. 355–358].

Кримінальне законодавство передбачає відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем і мереж, а

Закон № 2149-IX 2022 року посилив санкції за такі дії, вчинені під час дії воєнного стану [20, ст. 361–363-1; 38]. Проте кваліфікуючі ознаки не враховують специфіки атак на фінансову інфраструктуру, а правоохоронні органи стикаються з проблемами юрисдикції, анонімізації зловмисників і збирання цифрових доказів.

Окремої уваги потребує проблема відставання законодавчої та наукової бази від темпів розвитку інформаційних систем і кіберзагроз. Цифрові фінансові послуги і методи атак оновлюються щороку, тоді як ухвалення законів займає роки, а наукове осмислення нових явищ відбувається переважно після їх масового поширення. Співвідношення цих темпів за ключовими технологічними чинниками наведено в табл. 1.7.

Дані табл. 1.7 показують, що навіть у випадках, коли регуляторна відповідь в Україні вже сформована, її відставання від європейського законодавства становить від одного до шести років, з урахуванням фактичного запровадження (як у випадку відкритого банкінгу) сягає семи років, а від моменту масового поширення відповідної технології воно ще більше. Для чинників останніх п’яти років, зокрема залежності від хмарних постачальників, атак з використанням штучного інтелекту та квантової загрози криптографії, спеціального регулювання фінансового сектору поки немає, і розрив у 2–4 роки щороку збільшується. Водночас кількість кіберінцидентів, опрацьованих CERT-UA, лише за 2021–2025 роки зросла в 4,4 разів (див. табл. 2.4), а збитки від карткового шахрайства у 2022–2025 роках в 2,9 разів (див. табл. 2.5). Наукова база також реагує із запізненням: вітчизняні публікації ґрунтовно висвітлюють загальні питання фінансової безпеки та цифровізації банківських послуг [97, p. 355–369; 131, p. 466–483; 84, с. 273–280], тоді як спеціальних досліджень імплементації DORA, протидії атакам із застосуванням штучного інтелекту і переходу фінансових установ на постквантову криптографію небагато, і вони мають переважно технічний характер [21, с. 400–412; 29, с. 165–176].

Таблиця 1.7 **Співвідношення темпів розвитку інформаційних систем і кіберзагроз та темпів оновлення законодавчої і наукової бази**

| Технологічний чинник або загроза | Період масового поширення | Регуляторна відповідь ЄС | Регуляторна відповідь України | Лаг України, років | Наукове опрацювання в Україні |
|---|---|---|---|---|---|
| Дистанційний і мобільний банкінг, небанківські надавачі платіжних послуг | 2013–2016 | Директива PSD2 (2015, застосовується з 2018) | Закон «Про платіжні послуги» (2021, чинний з 01.08.2022) | 6 | Широке |
| Деструктивні атаки на критичну інфраструктуру | 2015–2017 | Директива NIS (2016) | Закон «Про основні засади забезпечення кібербезпеки України» (2017); Закон «Про критичну інфраструктуру» (2021) | 1–5 | Широке |
| Відкритий банкінг (доступ третіх сторін через API) | 2018–2019 | PSD2 і технічні стандарти автентифікації (2018) | Закон «Про платіжні послуги» (2021); Положення НБУ про відкритий банкінг (2025) | 3 (запровадження 7) | Помірне |
| Віртуальні активи | 2017–2021 | Регламент MiCA (2023, застосовується з 30.12.2024) | Закон «Про віртуальні активи» (2022), введення в дію пов’язане з податковими змінами | 3 | Помірне |
| Залежність від хмарних і ІКТ-постачальників | 2018–2022 | Регламент DORA (2022, застосовується з 17.01.2025) | Закон «Про хмарні послуги» (2022) без галузевих вимог для фінансового сектору | 4 | Фрагментарне |
| Атаки з використанням штучного інтелекту | 2023–2025 | Регламент про штучний інтелект (2024) | Спеціальне регулювання відсутнє | 2 | Початкове |
| Квантова загроза асиметричній криптографії | 2020-ті (перспективна загроза) | Рекомендація ЄС щодо переходу на постквантову криптографію (2024) | Рішення відсутні | 2 | Початкове |

Джерело: складено автором за [112; 113; 145; 144; 146; 102; 59; 58; 54; 34; 64; 23]. Лаг визначено як різницю між роками ухвалення акта ЄС та акта України, а для невирішених питань станом на 2026 р.; оцінку рівня наукового опрацювання здійснено автором за результатами аналізу публікацій.

Отже, проблема полягає не лише у прогалинах окремих норм, а в структурному розриві між швидкістю технологічних змін і швидкістю нормотворення, подолати який можна через делегування регулятору повноважень оперативно оновлювати технічні вимоги підзаконними актами та прискорену гармонізацію з правом ЄС.

Таким чином, нормативно-правове регулювання кібербезпеки фінансової системи України є багаторівневою, але недостатньо уніфікованою системою, у якій найбільш деталізовані вимоги встановлено підзаконними актами Національного банку, тоді як на рівні законів вони фрагментарні, а

повноваження органів частково дублюються. Головними завданнями на найближчу перспективу є закріплення статусу НБУ як галузевого органу кіберстійкості всього фінансового сектору, уніфікація правил звітування про інциденти, гармонізація з європейським законодавством і створення правових стимулів для обміну інформацією про загрози між учасниками ринку.

## 1.3 Міжнародний досвід та стандарти забезпечення кібербезпеки фінансових систем

Глобальна взаємопов’язаність фінансових ринків зумовлює транснаціональний характер кіберзагроз. Атака на інформаційну систему банку в одній країні може спричинити порушення розрахунків у кількох юрисдикціях, оскільки платіжні повідомлення, цінні папери та деривативи обертаються в інфраструктурі, що не визнає державних кордонів. Тому міжнародне співтовариство виробило уніфіковані підходи до кіберзахисту, які поєднують добровільні стандарти, галузеві вимоги та обов’язкове регулювання. Їхнє вивчення має практичне значення для України, адже інтеграція у світові фінансові потоки та євроінтеграційний курс потребують приведення національної системи кіберзахисту до рівня, сумісного з глобальними нормами [120; 10, с. 46–51; 99, p. 11–28].

Сполучені Штати Америки сформували одну з найдетальніших систем регулювання кібербезпеки фінансового сектору. Національний інститут стандартів і технологій розробив рамкову модель кібербезпеки, яка стала фактичною основою побудови систем захисту в банківській сфері багатьох країн. Модель побудована навколо функцій ідентифікації, захисту, виявлення, реагування та відновлення, а у версії 2.0, оприлюдненій у 2024 році, доповнена функцією управління, що охоплює стратегію, ризик-апетит і відповідальність керівництва [136, с. 3–5]. Модель має циклічний характер: кожен інцидент стає підставою для коригування всіх функцій, що забезпечує постійну адаптацію до змін ландшафту загроз.

Американські регулятори деталізували загальні рамки на рівні галузевих вимог. Федеральна рада з перевірки фінансових установ (FFIEC) у 2015 році запровадила добровільний інструмент самооцінки кіберзахищеності банків, який з 31 серпня 2025 року виведено з ужитку, а окремий регуляторний акт штату Нью-Йорк (23 NYCRR 500), прийнятий у 2017 році та суттєво оновлений у 2023 році, зобов'язує фінансові установи призначати відповідальну особу за інформаційну безпеку, затверджувати політики на рівні ради директорів, проводити щорічні оцінки ризиків, тестування на проникнення та навчання персоналу, а також повідомляти регулятора про кіберінцидент протягом 72 годин [111, § 500.17; 150]. Цей досвід демонструє тенденцію до персоналізації відповідальності керівництва та жорстких строків звітування.

Велика Британія поєднує регуляторний тиск з галузевими ініціативами. Банк Англії як макропруденційний регулятор відповідає за стійкість фінансової системи в цілому, тоді як органи мікропруденційного нагляду контролюють окремі установи. Такий розподіл дозволяє розглядати кібербезпеку одночасно як питання індивідуальної стійкості банку і як загрозу системній стабільності. З 2014 року Банк Англії застосовує програму CBEST, яка передбачає тестування на проникнення на основі розвідданих про загрози, що імітує дії найдосконаліших зловмисників, зокрема державних кібергруп [95]. Результати тестування використовуються для оцінки здатності установи виявляти атаку, протидіяти їй і відновлюватися, а відмова від участі розглядається регулятором як негативний сигнал. На основі цього підходу Європейський центральний банк розробив рамкову програму TIBER-EU, яку застосовують центральні банки країн ЄС [152].

Європейський Союз виробив наймасштабнішу модель регулювання кібербезпеки, яка безпосередньо впливає на фінансовий сектор. Директива NIS 2016 року стала першим загальноєвропейським актом щодо операторів основних послуг, а досвід її імплементації виявив неузгодженість вимог у різних юрисдикціях і слабкі механізми санкцій. Директива NIS2, ухвалена у 2022 році, розширила коло суб'єктів, запровадила відповідальність органів управління за затвердження заходів з управління кіберризиками та триступеневе повідомлення

про значні інциденти: раннє попередження протягом 24 годин, повідомлення протягом 72 годин і остаточний звіт протягом місяця [114, ст. 20, 21, 23].

Для фінансового сектору ЄС ключовим став Регламент про цифрову операційну стійкість (DORA), що застосовується з 17 січня 2025 року. Він поширюється на кредитні та платіжні установи, установи електронних грошей, інвестиційні фірми, постачальників послуг у сфері криптоактивів, страхові компанії та інших учасників ринку і встановлює єдині вимоги до управління ризиками у сфері ІКТ, класифікації та звітування про інциденти, тестування цифрової операційної стійкості, включно з тестуванням на проникнення на основі загроз, а також до управління ризиками сторонніх постачальників ІКТ-послуг з наглядом за критичними постачальниками [144, ст. 2, 5, 17–19, 24–30; 101]. DORA демонструє перехід від захисту окремої установи до моделі колективної стійкості сектору, що особливо актуально для України, де фінансові установи діють в умовах системної агресії.

Міжнародні стандарти добровільного характеру відіграють не менш важливу роль, ніж обов’язкове регулювання. Стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою, яка може бути сертифікована незалежними органами, ISO/IEC 27002 містить каталог заходів контролю, а ISO/IEC 27005 присвячений управлінню ризиками інформаційної безпеки [124; 125; 126]. Для банків сертифікація за ISO/IEC 27001 часто є умовою встановлення ділових відносин з міжнародними партнерами. Стандарт PCI DSS встановлює дванадцять вимог до захисту даних власників платіжних карток, згрупованих у шість блоків, і є обов’язковим для банків-емітентів та еквайрів, що працюють з міжнародними платіжними системами [140]. Програма безпеки клієнтів SWIFT, запроваджена після інцидентів 2016 року, встановлює обов’язкові та рекомендовані заходи контролю для учасників мережі: у версії 2026 року рамка містить 32 заходи, з яких 26 є обов’язковими, а учасники щорічно підтверджують відповідність, ризикуючи в разі невиконання втратити доступ до мережі [151]. Для українських банків, що здійснюють міжнародні перекази, дотримання цих вимог є безальтернативною умовою участі в глобальній платіжній системі.

Узагальнену характеристику ключових міжнародних стандартів і настанов, що формують методологічну основу кіберзахисту фінансових установ, наведено в табл. 1.8.

Таблиця 1.8 **Міжнародні стандарти та настанови у сфері кібербезпеки фінансових установ**

| Документ | Розробник, рік | Предмет регулювання | Значення для України |
|---|---|---|---|
| ISO/IEC 27001:2022 | ISO, IEC, 2022 | Вимоги до системи управління інформаційною безпекою | Основа сертифікації банків і умова співпраці з міжнародними партнерами |
| ISO/IEC 27002:2022, ISO/IEC 27005:2022 | ISO, IEC, 2022 | Каталог заходів контролю; управління ризиками інформаційної безпеки | Методологія вибору заходів захисту та оцінки ризиків |
| ISO/IEC 27032:2023 | ISO, IEC, 2023 | Настанови з безпеки в інтернеті | Узгодження понятійного апарату кібербезпеки |
| NIST Cybersecurity Framework 2.0 | NIST, 2024 | Шість функцій управління кіберризиками, рівні реалізації | Шкала оцінки зрілості кіберзахисту установ |
| PCI DSS v4.0.1 | PCI SSC, 2024 | Захист даних власників платіжних карток | Обов’язковий для емітентів і еквайрів міжнародних карток |
| SWIFT CSCF v2026 | Swift, 2025 | 32 заходи контролю, з них 26 обов’язкових | Умова доступу до міжнародних розрахунків |
| Guidance on cyber resilience for FMIs | CPMI, IOSCO, 2016 | Кіберстійкість фінансових ринкових інфраструктур, відновлення за дві години | Орієнтир для НПС «ПРОСТІР» і системи електронних платежів НБУ |
| Principles for operational resilience | BCBS, 2021 | Операційна стійкість банків | Інтеграція кіберризиків в управління операційним ризиком |
| Cyber Lexicon; FIRE | FSB, 2023; 2025 | Єдина термінологія; формат обміну даними про інциденти | Гармонізація термінів і форм звітування |

Джерело: систематизовано автором за [124; 125; 126; 127; 136; 140; 151; 120; 141; 110; 119].

Дані табл. 1.8 свідчать, що міжнародні стандарти утворюють взаємодоповнювальну систему: стандарти ISO/IEC визначають процесну основу управління, рамкова модель NIST дає шкалу зрілості, галузеві вимоги PCI DSS і SWIFT встановлюють обов’язкові технічні заходи для учасників платіжних мереж, а документи Базельського комітету, CPMI-IOSCO і Ради з фінансової стабільності переносять акцент на стійкість і гармонізацію звітування.

Базельський комітет з банківського нагляду розглядає кіберризики як складову операційного ризику і в Принципах операційної стійкості 2021 року вимагає від банків здатності забезпечувати критичні операції під час руйнівних

подій, зокрема кібератак [141]. Комітет з платіжних та ринкових інфраструктур спільно з Міжнародною організацією комісій з цінних паперів розробив Керівні принципи кіберстійкості фінансових ринкових інфраструктур, які визнають неможливість абсолютного захисту і вимагають планувати безпечне відновлення критичних операцій протягом двох годин після руйнівного кіберінциденту [120, с. 16]. Ця філософія стійкості, а не непроникності, є важливим орієнтиром для українських регуляторів.

Наглядові органи дедалі частіше перевіряють не наявність засобів захисту, а здатність банків відновлюватися після успішної атаки. У 2024 році Європейський центральний банк провів стрес-тест кіберстійкості 109 банків, з яких 28 пройшли поглиблене тестування; сценарій передбачав, що всі превентивні заходи не спрацювали, а бази даних основних систем зазнали серйозного пошкодження. За результатами тесту ЄЦБ констатував, що банки мають рамки реагування та відновлення, проте зберігаються напрями для вдосконалення, а висновки врахував у процесі наглядової оцінки [115]. Паралельно Рада з фінансової стабільності у 2025 році затвердила формат обміну інформацією про інциденти (FIRE), покликаний зменшити фрагментацію вимог до звітування про кібер- та інші операційні інциденти в різних юрисдикціях [119]. Для України, де звітування про інциденти розпорошене між кількома органами, ця тенденція до уніфікації є особливо показовою.

Досвід Сінгапуру ілюструє модель активної ролі держави у формуванні екосистеми кібербезпеки. Монетарне управління Сінгапуру (MAS) встановило детальні вимоги до управління технологічними ризиками, вимагає повідомляти регулятора про відповідні інциденти не пізніше однієї години після їх виявлення, а з 2015 року в країні діє Агентство кібербезпеки, що координує національну політику кібербезпеки [88; 122; 137, п. 7–8]. В Ізраїлі, який перебуває під постійною безпековою загрозою, Банк Ізраїлю вимагає, щоб стратегію кіберзахисту затверджувала рада директорів, банк призначав керівника з кіберзахисту, а стратегія переглядалася не рідше одного разу на три роки [142, с. 6–7, 12]. Естонія після масштабних кібератак 2007 року, що вразили сайти органів влади та двох великих банків [109], створила розвинену систему захисту

цифрових сервісів під координацією Департаменту інформаційних систем, а в Таллінні у 2008 році засновано Центр передового досвіду НАТО з кібероборони [118; 89]. Японія з 2016 року проводить щорічні галузеві навчання фінансових установ «Delta Wall» і у 2024 році затвердила Настанови з кібербезпеки для фінансового сектору [121, с. 6–32]. Порівняльну характеристику моделей наведено в табл. 1.9.

Таблиця 1.9 **Порівняльна характеристика національних моделей забезпечення кібербезпеки фінансового сектору**

| Країна | Ключові органи | Основні документи | Особливості моделі |
|---|---|---|---|
| США | Федеральні банківські регулятори; Департамент фінансових послуг штату Нью-Йорк | NIST CSF 2.0 (2024); 23 NYCRR 500 (2017, ред. 2023) | Ризик-орієнтований підхід; щорічна сертифікація відповідності; повідомлення про інцидент не пізніше 72 год |
| Велика Британія | Банк Англії, органи пруденційного і поведінкового нагляду | Програма CBEST (2014) | Тестування на проникнення на основі розвідданих про загрози; поєднання макро- і мікропруденційного нагляду |
| ЄС | ЄЦБ, національні компетентні органи, європейські наглядові органи | DORA (застосовується з 17.01.2025); NIS2 (2022); TIBER-EU (2018, оновлено 2025) | Єдині вимоги до ризиків ІКТ; звітування про великі інциденти за схемою 4/24 год, 72 год, 1 місяць; нагляд за критичними постачальниками ІКТ |
| Сінгапур | Монетарне управління Сінгапуру (MAS); Агентство кібербезпеки (CSA, 2015) | Настанови з управління технологічними ризиками (2021) | Повідомлення регулятора не пізніше 1 год; призначення CISO; імітація дій противника |
| Ізраїль | Банк Ізраїлю (нагляд за банками) | Директива № 361 «Управління кіберзахистом» (2015, ред. 2021) | Стратегію кіберзахисту затверджує рада директорів; призначення керівника з кіберзахисту; перегляд стратегії не рідше разу на три роки |
| Японія | Агентство фінансових послуг (FSA) | Настанови з кібербезпеки для фінансового сектору (2024, ред. 2025) | Щорічні галузеві навчання Delta Wall з 2016 р.; управління ризиками третіх сторін |
| Естонія | Департамент інформаційних систем (RIA, 2011); фінансовий нагляд | Законодавство ЄС (NIS2, DORA) | Досвід протидії атакам 2007 р.; Центр передового досвіду НАТО з кібероборони в Таллінні (2008) |
| Україна | НБУ, Держспецзв'язку (CERT-UA), НКЦК при РНБО, СБУ, кіберполіція | Закон «Про основні засади забезпечення кібербезпеки України»; нормативно-правові акти НБУ | Розподіл функцій між кількома органами; відсутність обов'язкового тестування на основі загроз |

Джерело: систематизовано автором на основі [136; 111; 95; 144; 101; 152; 122; 137; 142; 121; 118; 89; 88; 58].

Тому міжнародні стандарти мають слугувати методологічною основою, яку необхідно доповнити національними механізмами протидії гібридним загрозам, географічним резервуванням систем, фізичним захистом центрів обробки даних і координацією з сектором безпеки та оборони. Україні належить виробити власну модель, що поєднуватиме імплементацію європейських норм, застосування міжнародних стандартів управління ризиками та специфічні механізми протидії загрозам воєнного періоду.

Аналіз табл. 1.9 дає змогу виокремити кілька орієнтирів для України. По-перше, у більшості країн фінансовий регулятор є головним наглядовим органом з кіберстійкості свого сектору, тоді як національні кіберагенції відповідають насамперед за міжсекторну координацію. По-друге, більшість розглянутих моделей (США, ЄС, Сінгапур) встановлюють чіткі строки повідомлення про інциденти, від однієї до сімдесяти двох годин. По-третє, розвинені юрисдикції використовують тестування на проникнення на основі розвідданих про загрози та галузеві центри обміну інформацією, що формує культуру колективної стійкості. По-четверте, важливу роль відіграє управління ризиками постачальників ІКТ-послуг, оскільки концентрація критичних функцій на кількох глобальних провайдерах створює системну вразливість.

Водночас стандарти ISO, NIST та вимоги ЄС розроблені для умов мирного функціонування ринків, тоді як Україна стикається з цілеспрямованими атаками державного рівня, фізичними загрозами інфраструктурі, перебоями з електропостачанням і міграцією кадрів.

# РОЗДІЛ 2
# АНАЛІЗ СТАНУ ТА ЗАГРОЗ КІБЕРБЕЗПЕЦІ ФІНАНСОВОЇ СИСТЕМИ УКРАЇНИ

## 2.1 Структура, особливості функціонування та тенденції цифровізації фінансової системи України

Фінансова система України є багаторівневою сукупністю інституцій, ринків, інфраструктури та регуляторів, що охоплює банківський сектор, ринки капіталу, страхові, лізингові та пенсійні установи, небанківські фінансові компанії, платіжні системи, а також органи державного регулювання і нагляду. Спільно вони забезпечують мобілізацію фінансових ресурсів, їхній розподіл між секторами економіки, безперервність платіжного обігу та захист прав вкладників і інвесторів. Архітектура системи формувалася впродовж трьох десятиліть незалежності, пройшовши шлях від централізованої моделі до ринкової системи, інтегрованої в глобальні фінансові потоки. Кожен сегмент має власну специфіку, регуляторні рамки та рівень технологічної зрілості, проте всі вони залежать від інформаційних систем, що робить кібербезпеку системно важливою для стабільності всього комплексу [14, с. 16–17; 94, p. 23–41; 154, p. 8–18].

Банківський сектор залишається провідною складовою фінансової системи України, концентруючи основну масу активів, зобов’язань і платіжних операцій. Протягом 2021–2025 років кількість діючих банків скоротилася внаслідок виведення з ринку неплатоспроможних установ, злиттів і поглинань, тоді як обсяг чистих активів сектору зріс більш ніж удвічі (табл. 2.1).

Дані табл. 2.1 свідчать, що за п’ять років кількість банків зменшилася на 13 установ, а чисті активи зросли в 2,2 разів, причому навіть у 2022 році, попри повномасштабну агресію, приріст активів становив 14,6 %. Консолідація ринку за зростання активів означає концентрацію фінансових ресурсів, даних і операцій у меншій кількості установ, а отже, зростання наслідків успішної кібератаки на кожну з них. Значну частку активів контролюють банки з державною часткою,

зокрема ПриватБанк, Ощадбанк, Укрексімбанк і Укргазбанк [27], тому компрометація державного банку матиме не лише фінансові, а й репутаційні наслідки для держави. Небанківський сектор налічував станом на 1 вересня 2026 року 717 установ, з них 378 фінансових компаній, 53 страховики, 76 кредитних спілок і 96 ломбардів [26], а його технологічна неоднорідність формує окремий вектор ризиків.

Таблиця 2.1 **Основні показники банківського сектору України з 2021 по 2026 рр.**

| Показник | 01.01. 2021 | 01.01. 2022 | 01.01. 2023 | 01.01. 2024 | 01.01. 2025 | 01.01. 2026 |
|---|---|---|---|---|---|---|
| Кількість діючих банків, од. | 73 | 71 | 67 | 63 | 61 | 60 |
| Чисті активи банківського сектору, млрд грн | 1 823 | 2 053 | 2 352 | 2 945 | 3 415 | 4 001 |
| Темп приросту чистих активів, % | – | 12,6 | 14,6 | 25,2 | 16,0 | 17,2 |

Джерело: побудовано і розраховано за даними НБУ [27, с. 4, 14].

Концентрація банківського ринку має двоїстий вплив на кібербезпеку. Великі банки мають більші ресурси для інвестування в захисні технології, спеціалізовані підрозділи та сертифікацію за міжнародними стандартами, однак їхній системний статус робить їх привабливішими мішенями: аналіз 319 кібератак на банки 53 країн засвідчив, що великі за активами банки частіше стають цілями атак [132]. Крім того, масштаб інфраструктури збільшує периметр захисту. Компрометація одного з системно важливих банків може спричинити ланцюгову реакцію платіжних збоїв і порушення розрахунків за державними програмами, зарплатними проєктами та комунальними платежами, тому Національний банк щороку визначає перелік системно важливих банків, до яких застосовуються підвищені вимоги щодо капіталу, ліквідності та управління ризиками; на 2026 рік такий статус мають 16 банків, серед яких ПриватБанк, Ощадбанк, Укрексімбанк, Укргазбанк, Райффайзен Банк і ПУМБ [25].

Небанківський фінансовий сектор за обсягом активів значно поступається банківському, проте забезпечує доступ до фінансових послуг тим верствам населення та бізнесу, які не обслуговуються банками. Технологічна зрілість кредитних спілок, ломбардів і частини фінансових компаній часто поступається

банківській, а фінансові компанії, що надають споживчі кредити онлайн, обробляють значні масиви персональних даних за недостатніх інвестицій у кіберзахист. З 1 липня 2020 року регулювання цього сегмента здійснює Національний банк, що створило передумови для поширення на нього вимог до інформаційної безпеки [36; 63]. Ринок цінних паперів характеризується відносно низькою капіталізацією, проте його інфраструктура, зокрема депозитарна система та торговельні платформи, потребує захисту на рівні критичної інфраструктури, оскільки порушення її роботи може призвести до некоректного обліку прав власності.

Платіжна інфраструктура забезпечує рух коштів між усіма суб'єктами економіки. Національна платіжна система «ПРОСТІР», створена Національним банком, функціонує поряд з міжнародними платіжними системами Visa і Mastercard, а надавачі платіжних послуг, зокрема фінтех-компанії та оператори електронних гаманців, розширили доступ до платежів для малого бізнесу та електронної комерції [59]. Розвиток миттєвих і безконтактних платежів збільшив обсяг даних, що обробляються в реальному часі, та поверхню атаки, адже кожна ланка платіжного ланцюжка, від емітента до процесингового центру, є потенційною вразливістю. Динаміку основних показників цифровізації платіжного ринку наведено в табл. 2.2.

Таблиця 2.2 **Показники розвитку безготівкових розрахунків з використанням платіжних карток в Україні**

| Показник | 2021 | 2023 | 2024 | 2025 |
|---|---|---|---|---|
| Кількість емітованих платіжних карток на кінець року, млн од. | – | 115,1 | 132,0 | 148,7 |
| Кількість активних платіжних карток, млн од. | 46,3 | 52,1 | 58,8 | 65,4 |
| Частка безготівкових операцій у загальній сумі операцій з картками, % | 61,0 | 65,0 | 64,5 | 65,4 |
| Частка безготівкових операцій у загальній кількості операцій з картками, % | 90,1 | 93,5 | 94,6 | 95,5 |

Джерело: побудовано за даними Національного банку України [11; 87; 1; 81]. Примітка. Порівнянні річні дані за 2022 р. в оглядах НБУ не наведено.

Як видно з табл. 2.2, кількість активних платіжних карток за 2021–2025 роки зросла на 41 %, а частка безготівкових операцій у загальній кількості

операцій з картками досягла 95,5 %. Фактично розрахунки населення перемістилися в цифрове середовище, і кожна така операція потребує захисту автентифікаційних даних, каналів передачі та процесингових систем. Отже, зростання безготівкового обігу безпосередньо розширює поверхню атаки і посилює залежність фінансової стабільності від кіберстійкості платіжної інфраструктури.

Особливості функціонування фінансової системи України визначаються насамперед воєнним станом. З перших днів повномасштабного вторгнення Національний банк забезпечив безперервність критичних операцій, запровадив тимчасові обмеження на валютні операції та транскордонний рух капіталу, а фінансові установи зіткнулися з необхідністю евакуації персоналу, перенесення центрів обробки даних і резервування каналів зв'язку. Попри це, банківський сектор зберіг операційну стабільність і високу ліквідність [94, p. 23–41]. Масовані удари по енергетичній інфраструктурі у 2022–2025 роках змусили банки інвестувати в автономні джерела живлення та географічно рознесені майданчики обробки операцій. Ці заходи безпосередньо пов'язані з кібербезпекою, оскільки відключення електроенергії створює умови для використання резервних, менш захищених каналів зв'язку. Міграція мільйонів громадян за кордон збільшила кількість транскордонних операцій і доступу до банківських застосунків з іноземних IP-адрес, що вимагало адаптації систем моніторингу аномальної активності.

Фінансова система України характеризується значною часткою операцій в іноземній валюті, що вимагає від банків підтримувати складні інформаційні системи обліку валютних позицій і управління валютними ризиками. Інтеграція з міжнародними кореспондентськими мережами, системою SWIFT і платіжними системами Visa та Mastercard зобов'язує українські банки дотримуватися міжнародних стандартів безпеки, проходити регулярні аудити та сертифікацію [140; 151]. Відповідно, кіберзахист систем, що забезпечують міжнародні розрахунки, стає умовою збереження доступу української економіки до світових

фінансових ринків, а його порушення може спричинити посилення моніторингу транзакцій або обмеження співпраці з боку іноземних контрагентів.

Тенденції цифровізації фінансової системи набули прискореного характеру, а воєнний стан став додатковим каталізатором переходу на дистанційні канали. Мобільний банкінг перетворився з додаткової опції на основний спосіб взаємодії банку з клієнтом, що супроводжувалося скороченням мережі відділень. Банки перетворюються на технологічні платформи, а модель загроз зміщується від фізичного доступу до кас і сховищ до вразливостей мобільних застосунків, API-інтерфейсів, хмарних сервісів і систем автентифікації [133, p. 143–150; 84, с. 273–280].

Наступним етапом цифрової трансформації стає відкритий банкінг. Закон України «Про платіжні послуги» передбачив доступ надавачів нефінансових платіжних послуг до рахунків клієнтів за їхньою згодою, що лежить в основі агрегації рахунків, персональних фінансових менеджерів і нових моделей кредитування [59; 23; 83, с. 186–196; 138]. Розширення екосистеми за межі банку створює мережу взаємозалежностей, у якій безпека кінцевого продукту залежить від надійності кожного учасника, а банк не завжди контролює, як сторонній фінтех-стартап зберігає токени доступу та захищає власні системи.

Проєкт цифрової гривні відкриває новий вимір для аналізу кібербезпеки. Пілотний випуск електронної гривні, здійснений Національним банком, продемонстрував технічну можливість реалізації цифрових грошей центрального банку, проте масове впровадження потребуватиме захисту криптографічних ключів емітента, забезпечення конфіденційності транзакцій за одночасної прозорості для регулятора та стійкості до атак найвищого рівня складності [70, с. 211–218; 69, с. 56–73; 130, p. 11–25]. Ринок віртуальних активів, попри незавершеність правового регулювання, пов’язаний з банківським сектором через сервіси обміну і платіжні шлюзи, що створює додаткові канали проникнення загроз [34; 145]. Впровадження штучного інтелекту для скорингу, виявлення шахрайства та протидії відмиванню коштів [92, p. 1–24; 76, с. 130–136] додає ризики отруєння даних, маніпулювання моделями і зловживання

генеративними інструментами з боку зловмисників [4, с. 244–255; 146]. Основні тенденції цифровізації та їхній вплив на вимоги до кібербезпеки систематизовано в табл. 2.3.

Таблиця 2.3 **Основні тенденції цифровізації фінансового сектору України та вимоги до кібербезпеки**

| Тенденція | Суть трансформації | Ключові наслідки | Вимоги до кібербезпеки |
|---|---|---|---|
| Масовий перехід на мобільний банкінг | Основний канал взаємодії банку з клієнтом перенесено у смартфон; скорочення мережі відділень | Зростання частки цифрових транзакцій; зменшення операцій у касах | Захист мобільних застосунків і API-шлюзів; багатофакторна автентифікація |
| Відкритий банкінг | Доступ сторонніх надавачів послуг до рахунків за згодою клієнта | Формування фінтех-екосистем; агрегація рахунків | Контроль доступу третіх сторін; аудит постачальників; захист токенів |
| Розвиток платіжної інфраструктури | Модернізація НПС «ПРОСТІР»; миттєві та безконтактні платежі | Швидша обробка платежів; зменшення залежності від готівки | Захист процесингових центрів; моніторинг аномалій у реальному часі |
| Цифрова гривня | Пілотний випуск цифрових грошей центрального банку | Нові форми грошей; програмовані платежі | Захист ключів емітента; стійкість до атак державного рівня |
| Штучний інтелект і великі дані | Машинне навчання для скорингу, виявлення шахрайства, персоналізації | Автоматизація рішень; зростання обсягів даних | Захист моделей від отруєння даних; контроль цілісності алгоритмів |
| Віртуальні активи | Зростання операцій з цифровими активами; інтеграція з платіжними шлюзами | Транскордонні перекази; поява локальних платформ | Контроль точок обміну; протидія відмиванню коштів |
| Цифровізація небанківського сектору | Електронний документообіг, віддалена ідентифікація у страховиків і фінансових компаній | Зростання кількості цифрових договорів | Уніфікація вимог до захисту даних; розширення нагляду |

Джерело: систематизовано автором на основі [59; 73; 72, с. 90–96; 83, с. 186–196].

Аналіз табл. 2.3 свідчить, що цифровізація фінансової системи України є незворотним процесом, який підвищує ефективність фінансового посередництва, знижує витрати на обслуговування та розширює доступ до послуг. Водночас периметр, що потребує захисту, більше не збігається з корпоративним периметром банку: він охоплює мільйони мобільних пристроїв клієнтів, точки прийому платежів, хмарні середовища постачальників і API-партнерів. Особливістю українського контексту є поєднання швидкої цифровізації з обмеженими ресурсами значної частини учасників ринку:

найбільші банки можуть дозволити собі сучасні системи захисту та власні центри кіберрозвідки, тоді як середні та малі установи покладаються на аутсорсинг і типові рішення. Це формує двошвидкісну модель ринку, у якій вразливості менших гравців можуть бути використані для проникнення в екосистему великих банків через спільні платіжні шлюзи, бюро кредитних історій або корпоративних клієнтів.

## 2.2 Аналіз кіберзагроз, вразливостей та наслідків кібератак на фінансовий сектор України

Ландшафт кіберзагроз фінансовому сектору України набув особливої гостроти в період повномасштабної збройної агресії. Фінансові установи опинилися на передовій гібридної війни, оскільки дестабілізація платіжної системи, витік банківських даних або параліч цифрової інфраструктури завдають шкоди не лише окремій установі, а й довірі до держави в цілому. Сучасна атака на банк є багатоетапною операцією, що поєднує розвідку, проникнення, закріплення в мережі, збирання інформації, виконання основного завдання та приховування слідів, тому її виявлення можливе лише за наявності розвиненої системи моніторингу та аналітики загроз [31, с. 125–139].

Кількісне уявлення про інтенсивність загроз дає статистика урядової команди реагування на комп’ютерні надзвичайні події CERT-UA, що функціонує в складі Держспецзв’язку і опрацьовує кіберінциденти в органах влади, на об’єктах критичної інфраструктури та в інших секторах. Динаміку зареєстрованих кіберінцидентів за 2021–2025 роки наведено в табл. 2.4.

Аналіз табл. 2.4 показує, що кількість кіберінцидентів за 2021–2025 роки зросла в 4,4 разів, з 1 350 до 5 927. Найбільший приріст припав на 2024 рік (69,7 %, або 1 772 інциденти), значним він був і у 2022 році (62,5 %), коли розпочалася повномасштабна агресія, а у 2025 році зростання тривало (37,4 %). Водночас кількість інцидентів критичного та високого рівнів після піку 2022 року (1 048) скоротилася до 12 у 2025 році, а їхня частка зменшилася з 47,8 % до 0,2 %. З

урахуванням того, що методика класифікації інцидентів у звітах Держспецзв'язку різних років дещо відрізняється, ця динаміка свідчить про зростання спроможності системи кіберзахисту локалізувати атаки до того, як вони завдадуть значної шкоди, і про зміщення тактики зловмисників у бік масових атак: кількість фішингових інцидентів у 2025 році зросла до 1 727 проти 843 у 2024 році [79]. У першому півріччі 2026 року CERT-UA опрацювала 3 137 інцидентів, що на 8 % більше, ніж у другому півріччі 2025 року [80].

Таблиця 2.4 **Динаміка кіберінцидентів, зареєстрованих і опрацьованих CERT-UA, у 2021–2025 рр.**

| Показник | 2021 | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|---|
| Кількість кіберінцидентів, од. | 1 350 | 2 194 | 2 543 | 4 315 | 5 927 |
| Абсолютний приріст, од. | – | 844 | 349 | 1 772 | 1 612 |
| Темп зростання, % | – | 162,5 | 115,9 | 169,7 | 137,4 |
| Темп приросту, % | – | 62,5 | 15,9 | 69,7 | 37,4 |
| Інциденти критичного та високого рівнів, од. | 403 | 1 048 | 367 | 59 | 12 |
| Частка критичних і високих інцидентів, % | 29,9 | 47,8 | 14,4 | 1,4 | 0,2 |

Джерело: побудовано і розраховано за даними Державної служби спеціального зв'язку та захисту інформації України [67, с. 5–7; 66, с. 9; 17, с. 9].

Статистика CERT-UA не повною мірою відображає ситуацію у фінансовому секторі, оскільки більшість інцидентів у банках опрацьовує команда реагування Національного банку CSIRT-NBU [148, с. 22–23]. Міжнародні дані підтверджують високу вразливість галузі: за оцінками МВФ, майже п'ята частина всіх кіберінцидентів у світі стосується фінансових компаній, а їхні прямі втрати з 2004 року сягнули майже 12 млрд дол. США [96, с. 1, 3], тоді як серед 488 інцидентів у фінансовому секторі Європи за січень 2023 року – червень 2024 року 46 % припало на кредитні установи [116, с. 3, 8].

Суб'єктний склад загроз фінансовому сектору України надзвичайно розмаїтий. На одному полюсі перебувають кіберкримінальні угруповання, мотивовані фінансовою вигодою, які функціонують за моделлю організованої злочинності з чітким розподілом ролей: розробники шкідливого програмного забезпечення, постачальники інфраструктури для атак, фахівці з відмивання коштів і так звані грошові мули. На протилежному полюсі діють державні

кіберпідрозділи держави-агресора та пов’язані з ними угруповання, пріоритетом яких є дестабілізація економіки, підрив довіри до фінансової системи та збір розвідувальних даних. Між ними існує широкий спектр хактивістів і брокерів доступу, що продають доступ до скомпрометованих мереж. Отже, фінансові установи мають протистояти одночасно масовим автоматизованим атакам і цілеспрямованим операціям високої складності.

Розподілені атаки на відмову в обслуговуванні залишаються одним із найпоширеніших інструментів впливу на фінансові установи. У мирний період їх розглядали як відносно примітивний інструмент, що не призводить до втрати даних, однак воєнний час змінив цю оцінку. Показовими стали атаки 15 лютого 2022 року, коли напередодні вторгнення з використанням ботнетів Mirai і Meris було порушено доступність вебресурсів українських банків і державних органів, а громадянам розсилали фейкові SMS-повідомлення про нібито збої банкоматів державних фінансових установ [15]. Неможливість увійти до застосунку банку сприймається населенням як ознака фінансової нестабільності, тому технічна атака перетворюється на інструмент психологічного тиску. Сучасні атаки використовують ботнети з інфікованих пристроїв інтернету речей і протоколи ампліфікації, що змушує банки інвестувати в захист на рівні провайдера та розподілену архітектуру застосунків. Європейська статистика підтверджує домінування цього інструменту: за період з липня 2024 року по червень 2025 року DDoS-атаки становили близько 76,7 % зафіксованих інцидентів, а 83,5 % інцидентів у фінансовому секторі припали на хактивістські DDoS-атаки [117, с. 8, 16, 25]. У фінансовому секторі Європи 58 % DDoS-атак було спрямовано саме на кредитні установи [116, с. 3, 12].

Фішинг і соціальна інженерія експлуатують не технічні вразливості, а психологічні механізми людини. Фішингові листи, що імітують повідомлення від банку, державних органів чи міжнародних організацій, залишаються основним каналом первинного проникнення, а воєнний період породив нові сценарії: пропозиції гуманітарної допомоги, повідомлення про виплати, «підтвердження» отримання соціальних допомог. Цілеспрямований фішинг

націлений на керівників підрозділів, адміністраторів і операціоністів та ретельно персоналізується: листи містять відомості про структуру компанії, імена колег і посилання на реальні документи, отримані під час попередньої розвідки. Компрометація облікового запису одного працівника може відкрити доступ до внутрішньої кореспонденції, архітектурних схем мережі та баз даних клієнтів. Дослідження фішингових кампаній в українському кіберпросторі показують, що україномовні приманки та врахування демографічних характеристик аудиторії суттєво підвищують їхню успішність [65, с. 331–347]. За даними ENISA, фішинг залишається основним початковим вектором атак, на який припадає близько 60 % випадків [117, с. 6, 8]. Саме соціальна інженерія є основною причиною шахрайства з платіжними картками, динаміку якого наведено в табл. 2.5.

Таблиця 2.5 **Динаміка шахрайства з платіжними картками в Україні у 2022–2025 рр.**

| Показник | 2022 | 2023 | 2024 | 2025 | 2025 до 2022, разів |
|---|---|---|---|---|---|
| Кількість шахрайських операцій, тис. од. | 218 | 272 | 270 | 256 | 1,17 |
| Сума збитків, млн грн | 481 | 833 | ≈1 100 | ≈1 400 | ≈2,9 |
| Темп приросту збитків, % | 46 | 73 | 37 | 24 | – |
| Середня сума шахрайської операції, грн | 2 200 | 3 065 | 4 247 | 5 536 | 2,52 |
| Частка соціальної інженерії у сумі збитків, % | 53 | 80 | 84 | 90 | – |

Джерело: побудовано і розраховано за даними Національного банку України [24; 78; 13; 75; 30]. Примітка. Суми збитків за 2024–2025 рр. округлено в повідомленнях НБУ, тому темпи приросту наведено за даними НБУ, розрахованими за неокругленими сумами; темп за 2022 р. наведено порівняно з 2021 р.

За даними табл. 2.5, кількість шахрайських операцій з картками за 2022–2025 роки змінилася незначно, проте сума збитків зросла в 2,9 разів і досягла близько 1,4 млрд грн, а середня сума операції зросла в 2,5 разів. Частка соціальної інженерії в сумі збитків зросла з 53 до 90 %, а 83 % шахрайських операцій і 91 % збитків у 2025 році припали на інтернет-середовище [75]. Отже, технічний захист карткової інфраструктури загалом спрацьовує, а зловмисники переорієнтувалися на маніпулювання самими клієнтами, які розголошують реквізити карток, коди підтвердження та паролі до інтернет-банкінгу.

Програми-вимагачі становлять одну з найбільш руйнівних загроз для фінансових установ. Програма-вимагач проникає в корпоративну мережу, шифрує файли на серверах і робочих станціях та вимагає викуп, як правило, у криптовалюті. Для банку шифрування критичних баз даних означає неможливість обробки транзакцій, доступу до карткових реєстрів, формування звітності та обслуговування клієнтів у відділеннях, а відновлення навіть за наявності резервних копій може тривати дні або тижні. Сучасні угруповання застосовують подвійне вимагання: не лише блокують доступ до даних, а й викрадають конфіденційну інформацію, погрожуючи її оприлюдненням. Дослідження наслідків таких атак доводять, що, крім фінансових збитків, вони спричиняють переривання діяльності, репутаційні втрати та значну психологічну шкоду персоналу, тому атаку слід розглядати як кризу всієї організації, а не лише як проблему IT-підрозділу [135]. У європейському фінансовому секторі програми-вимагачі найчастіше уражали постачальників послуг (29 % випадків) і страховиків (17 %) [116, с. 3, 16].

Цілеспрямовані персистентні загрози (APT) становлять найвищий рівень складності та небезпеки. Такі кампанії зазвичай асоціюються з державними кіберпідрозділами або пов’язаними з ними угрупованнями і характеризуються тривалим, іноді багатомісячним, прихованим перебуванням у мережі жертви, використанням унікальних інструментів і ретельним приховуванням слідів. Для фінансового сектору APT-кампанія може мати на меті збір розвідувальних даних про структуру фінансової системи, ідентифікацію критичних вузлів, підготовку масштабної деструктивної атаки або використання скомпрометованої інфраструктури як плацдарму для атак на інші установи. Традиційні засоби захисту, орієнтовані на сигнатури відомих вірусів, проти таких інструментів неефективні, а атаки в одному секторі, за моделлю міжсекторного «зараження» кіберризиком, підвищують імовірність атак в інших [90].

Атаки на ланцюги постачання програмного забезпечення і послуг стали одним із найтривожніших трендів останніх років. Фінансові установи дедалі більше покладаються на комерційні програмні продукти, хмарні платформи,

аутсорсингові послуги та компоненти з відкритим кодом, що знижує витрати, але створює непрозорі зони ризику. Компрометація популярної бібліотеки коду, впровадження бекдору в оновлення комерційного продукту або захоплення облікового запису розробника можуть призвести до зараження тисяч організацій, включно з банками, адже оновлення програм традиційно сприймаються системами захисту як довірені. Для українського фінансового сектору ці ризики посилюються залежністю від іноземних технологічних рішень, зокрема хмарних сервісів, розміщених за межами країни, тому управління ризиками постачальників ІКТ-послуг стало окремим напрямом європейського регулювання [144, ст. 28–30].

Вразливості фінансового сектору України утворюють складну систему, що включає технічні, організаційні, інституційні та людські виміри. Технічна заборгованість є однією з найгостріших проблем: частина банківської інфраструктури побудована на застарілих платформах, що не підтримують сучасних протоколів шифрування, багатофакторної автентифікації та детального журналювання подій. Модернізація таких систем потребує значних інвестицій і зупинки критичних бізнес-процесів, тому часто відкладається, хоча для відомих вразливостей застарілого програмного забезпечення існують загальнодоступні експлойти [97, p. 355–369]. Дослідження мобільних фінансових застосунків також виявили, що основну частину ризику формують рідкісні, але критичні вразливості [91, p. 275–288].

Організаційні вразливості проявляються в недосконалості управління доступом, сегментації мереж і реагування на інциденти. Принцип мінімальних привілеїв часто порушується з операційних міркувань, а відсутність сегментації дозволяє зловмиснику, що проник через вразливу робочу станцію, рухатися горизонтально до критичних серверів і систем управління транзакціями. Через нерозвиненість центрів моніторингу атака нерідко виявляється не в момент проникнення, а в момент реалізації, тобто під час шифрування даних, виведення коштів чи публікації викраденої інформації.

Людський чинник посилюється хронічним стресом персоналу, пов’язаним з воєнним станом, міграцією і загрозами фізичній безпеці. Масова віддалена робота після лютого 2022 року створила нові вектори ризиків, оскільки працівники підключаються до корпоративних систем з домашніх мереж і персональних пристроїв. Інсайдерські загрози, хоча й становлять меншу частку інцидентів, здатні завдати максимальної шкоди, адже працівник із легітимним доступом може викрасти дані, здійснити несанкціоновані операції або передати зловмиснику інформацію про архітектуру захисту. Фізична інфраструктура виявилася вразливою до комбінованих загроз: ракетні удари по енергосистемі, пошкодження ліній зв’язку та переміщення обладнання створювали ситуації, коли системи кіберзахисту працювали в аварійному режимі з ослабленими процедурами контролю.

Наслідки кібератак на фінансовий сектор мають багаторівневий характер. Операційний рівень проявляється в недоступності цифрових каналів, блокуванні платіжних карток і зупинці еквайрингу, що для великої установи означає порушення повсякденного життя сотень тисяч людей. Фінансовий рівень охоплює викрадені кошти, виплати викупу, витрати на відновлення інфраструктури, юридичний супровід, компенсації клієнтам і штрафи, причому витрати зростають залежно від часу виявлення інциденту. Порівняння середньої вартості витоку даних у фінансовій галузі та в середньому за всіма галузями наведено в рис. 2.6.

Як видно з рис. 2.6, вартість інциденту у фінансовій галузі стабільно на 25–37 % перевищує середній рівень за всіма галузями і у 2024 році сягнула максимуму в 6,08 млн дол. США. Це зумовлено високою вартістю фінансових даних, жорсткими регуляторними вимогами і масштабом наслідків для клієнтів.

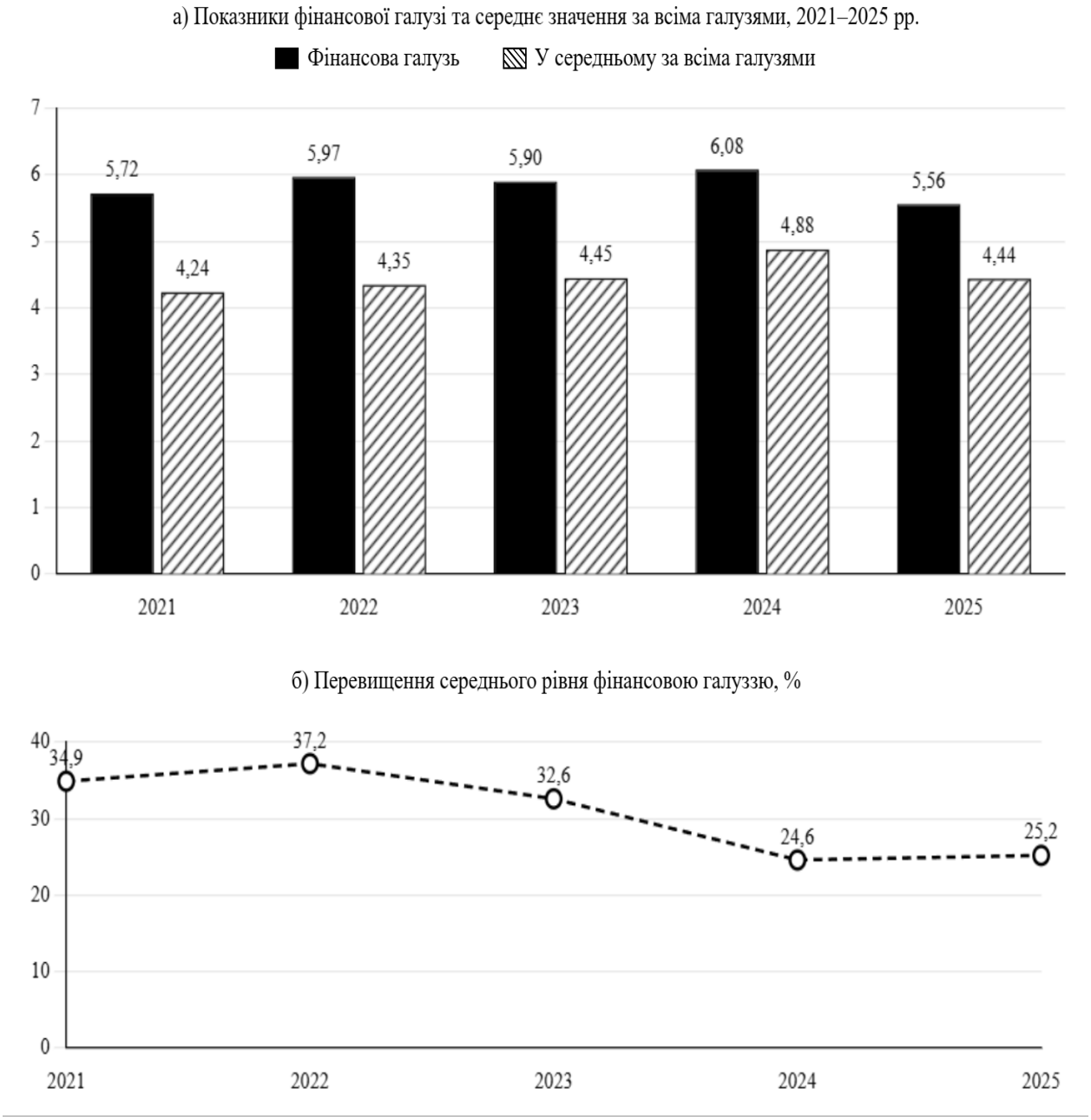



Рисунок 2.6 **– Середня вартість витоку даних у фінансовій галузі та в середньому у світі у 2021–2025 рр., млн дол. США**

Джерело: побудовано і розраховано за даними IBM [103, с. 12, 15; 104, с. 9, 11; 105, с. 10, 13; 106, с. 8, 10; 107, с. 10–13].

Репутаційний рівень пов’язаний з ерозією довіри, яка формується роками і руйнується за лічені години, а системний рівень виникає, коли атака на системно важливу установу, платіжну інфраструктуру або регулятора спричиняє каскадний ефект для всіх учасників ринку і загрожує фінансовій стабільності [96, с. 3, 7]. Узагальнену класифікацію загроз, вразливостей і наслідків наведено в табл. 2.7.

Таблиця 2.7 **Класифікація кіберзагроз, вразливостей та наслідків для фінансового сектору України**

| Категорія | Прояв | Механізм реалізації | Потенційні наслідки |
|---|---|---|---|
| Атаки на відмову в обслуговуванні (DDoS) | Масоване надходження трафіку на сервери, API-шлюзи, мобільні застосунки | Ботнети, ампліфікаційні атаки, флуд запитів | Недоступність цифрових каналів; паніка серед клієнтів; репутаційні втрати |
| Фішинг і соціальна інженерія | Імітація легітимних сервісів, маніпуляція персоналом і клієнтами | Шкідливі вкладення, підроблені сайти, дзвінки від імені банку | Викрадення облікових даних і коштів; первинне проникнення в мережу |
| Програми-вимагачі | Шифрування даних, подвійне вимагання | Фішинг, експлойти вразливостей, компрометація оновлень | Параліч операційної діяльності; витік даних клієнтів; регуляторні санкції |
| Цілеспрямовані персистентні загрози (APT) | Тривале приховане перебування в мережі, збір розвідданих | Унікальні інструменти, вразливості нульового дня, легітимні облікові дані | Компрометація стратегічної інформації; підготовка деструктивних атак |
| Атаки на ланцюги постачання | Компрометація програмного забезпечення, бібліотек коду, хмарних сервісів | Шкідливі оновлення, компрометація підрядників | Масове зараження; проникнення через довірені канали |
| Вразливості застарілих систем | Непідтримуване програмне забезпечення, застарілі протоколи | Експлуатація відомих вразливостей, слабка автентифікація | Несанкціонований доступ; неможливість аудиту |
| Організаційні вразливості | Надмірні привілеї, відсутність сегментації, слабкий моніторинг | Горизонтальне переміщення зловмисника, запізніле виявлення | Розширення зони інциденту; зростання збитків |
| Людський чинник та інсайдери | Помилки персоналу, навмисні дії, віддалена робота | Перехід за шкідливим посиланням, передача облікових даних, саботаж | Внутрішній доступ до критичних систем |
| Фізична вразливість інфраструктури | Перебої з електропостачанням, пошкодження ліній зв’язку, евакуація | Ракетні удари, аварії, переміщення обладнання | Відключення систем захисту; ослаблення контролю доступу |

Джерело: систематизовано автором на основі [116, с. 3, 8–16; 96, с. 1–7; 31, с. 125–139; 97, p. 355–369].

Табл. 2.7 дає змогу стверджувати, що загрози фінансовому сектору України мають не лише кількісну, а й якісну специфіку, яка відрізняє українську ситуацію від мирних юрисдикцій. Поєднання професійного кіберкримінал у, державних кіберпідрозділів, масових DDoS-атак як елемента інформаційної війни, фізичної деструкції інфраструктури та хронічного стресу персоналу формує унікальну комбінацію чинників. Кібератаки стали складовою комплексних операцій: інформація, зібрана в результаті кіберрозвідки, може використовуватися для планування фізичних ударів, а відключення

електроенергії після ракетного удару створює вікно можливостей для кібернетичних дій, оскільки резервні системи працюють у спрощеному режимі.

Кумулятивний ефект регулярних атак формує у фінансовому секторі стан хронічної оборони. Ресурси, які могли б бути спрямовані на розвиток продуктів і розширення доступу до фінансових послуг, перерозподіляються на підтримку базової безпеки. Цей стан стимулює інвестиції в кіберзахист і формує зрілішу культуру управління ризиками, але водночас створює ризик втоми, відтоку кваліфікованих кадрів і скорочення бюджетів на превентивні заходи. Подолання цього парадоксу вимагає системного підходу на рівні держави, регулятора та окремих установ, а його передумовою є об'єктивна оцінка рівня кіберзахищеності установ різних категорій.

## 2.3 Оцінка рівня кіберзахищеності та готовності фінансових установ до протидії кіберзагрозам

Оцінка рівня кіберзахищеності фінансових установ є багатовимірним завданням, що не зводиться до переліку встановлених засобів захисту. Кіберзахищеність є інтегральною характеристикою, яка відображає сукупний стан технічних, організаційних, кадрових і процедурних компонентів системи безпеки, їхню відповідність актуальним загрозам і здатність установи зберігати сталість функціонування в умовах деструктивних впливів. В українських умовах, ускладнених воєнним станом і атаками державного рівня, така оцінка набуває стратегічного значення, оскільки визначає не лише стійкість окремої установи, а й стійкість національної фінансової системи.

Методологічні підходи до оцінки кіберзахищеності базуються на поєднанні міжнародних стандартів, регуляторних вимог і галузевих практик. Рамкова модель NIST передбачає чотири рівні реалізації управління кіберризиками: частковий, поінформований про ризики, повторюваний і адаптивний [136, с. 7–8, 24–25]. На частковому рівні процедури реагування неформалізовані, а оцінка ризиків не проводиться систематично;

поінформований рівень означає визнання кіберризиків складовою загальної системи управління ризиками; повторюваний рівень передбачає стандартизацію процедур, центр моніторингу і планові тестування; адаптивний рівень характеризується використанням аналітики загроз, прогнозуванням нових векторів атак та інтеграцією в системи обміну інформацією. Оцінка за цією шкалою дозволяє не лише зафіксувати поточний стан, а й визначити траєкторію розвитку та пріоритетні інвестиції.

Стандарт ISO/IEC 27001 пропонує інший вимір оцінки, через систему управління інформаційною безпекою. Наявність сертифіката свідчить про документовану систему управління, проте не гарантує відсутності вразливостей, оскільки стандарт орієнтований на процеси, а не на конкретний технічний результат [124]. Тому фінансові установи доповнюють сертифікаційні аудити тестуванням на проникнення, а розвинені регулятори вимагають тестування командою атаки (red teaming), яке проводиться без попереднього інформування персоналу і дає об’єктивну картину технічних вразливостей, готовності команди захисту та якості процедур ескалації [152; 95].

Оцінка готовності до протидії кіберзагрозам фокусується на здатності установи діяти в умовах інциденту і включає організаційний компонент (ролі, плани реагування, процедури комунікації з регулятором, клієнтами та правоохоронними органами), технічний (інструменти виявлення і локалізації, резервні копії, резервні майданчики), людський (обізнаність і навченість персоналу, психологічна стійкість) та інституційний (інтеграція в галузеві та національні механізми обміну інформацією про загрози). Для оцінювання кожного компонента застосовують аналіз документів, спостереження за навчаннями, симуляції інцидентів і перевірку технічних рішень.

Регуляторна оцінка кіберзахищеності фінансового сектору України здійснюється Національним банком і Державною службою спеціального зв’язку та захисту інформації, причому кожен орган наголошує на власній сфері повноважень. НБУ проводить перевірки дотримання банками вимог з питань інформаційної безпеки та кіберзахисту за окремим положенням, оцінює

управління операційними ризиками і ризиками ІКТ, плани безперервності бізнесу та якість управління інформаційними технологіями, а за порушення, що створили загрозу реалізації системного кіберризику, застосовує фінансові санкції [45; 50; 42, п. 7.33]. Держспецзв'язку зосереджується на захисті об'єктів критичної інформаційної інфраструктури, аудиті інформаційної безпеки на таких об'єктах та своєчасності звітування про інциденти [58, ст. 8; 40]. Розмежування функцій змушує частину установ проходити дві паралельні оцінки за різними методиками, що потребує значних ресурсів. На наявність секторальних колізій у регулюванні фінансового сектору вказує і Національний координаційний центр кібербезпеки (див. 1.2).

Фактичний стан кіберзахищеності фінансових установ України характеризується вираженою диференціацією за розміром, формою власності та сегментом ринку. Системно важливі банки та установи з іноземним капіталом демонструють найвищий рівень зрілості: вони мають виділені підрозділи інформаційної безпеки, власні центри моніторингу, що працюють цілодобово, сертифікацію за ISO/IEC 27001, регулярне тестування на проникнення та інтеграцію в міжнародні системи обміну інформацією про загрози, а відповідальність за інформаційну безпеку покладена на рівень правління. Середні банки з переважно вітчизняним капіталом мають формалізовані політики і штатних фахівців, проте їхні підрозділи безпеки обмежені кількісно, тестування на проникнення проводиться епізодично, а центри моніторингу часто працюють у денному режимі або з аутсорсинговою підтримкою вночі. Такі установи, за узагальненням автора, здатні протистояти масовим загрозам, але мають обмежені можливості протидії цілеспрямованим кампаніям.

Малі банки, кредитні спілки, страхові компанії та інші небанківські фінансові установи демонструють найнижчий рівень кіберзахищеності. Штатні підрозділи безпеки в них часто відсутні або складаються з одного-двох фахівців, які поєднують функції системного адміністрування та захисту, резервне копіювання проводиться нерегулярно або зберігається в тій самій інфраструктурі, а плани реагування мають формальний характер. Через спільних

клієнтів і спільну інфраструктуру такі установи стають потенційними ланками проникнення загроз у більш захищені сегменти ринку.

Готовність до протидії кіберзагрозам вимірюється здатністю реалізувати плани в критичній ситуації. Масовані кібератаки, що супроводжували повномасштабне вторгнення, змусили банки активувати плани безперервності бізнесу, перевести критичні функції на резервні майданчики та посилити моніторинг. Сильними сторонами виявилися загальна стійкість платіжної системи, оперативна координація з боку Національного банку і високий рівень мобілізації IT- та безпекових команд, а слабкими стали залежність від єдиних точок відмови в ланцюгах постачання, недостатня підготовленість до тривалих перебоїв з електропостачанням і труднощі з фізичною безпекою центрів обробки даних у регіонах, що зазнавали обстрілів [128, p. 224–233; 94, p. 23–41].

Управління інцидентами як процес охоплює підготовку, виявлення, аналіз, локалізацію, ліквідацію наслідків, відновлення та аналіз після інциденту, тому оцінка готовності вимагає перевірки кожного з цих етапів. На етапі підготовки важливими є класифікатор інцидентів, матриця ескалації, контактні списки, шаблони комунікацій і резервні канали зв’язку. На етапі локалізації критичною є здатність ізолювати скомпрометовані сегменти мережі без зупинки бізнес-процесів, що неможливо за відсутності належної сегментації. Етап відновлення вимагає перевірених резервних копій та ізольованого середовища для відновлення, а дослідження відмовостійкості інформаційного середовища банку показують, що ручне перемикання на резервний майданчик може не відповідати нормативному часу відновлення найкритичніших сервісів [68, с. 304–311]. Аналіз після інциденту в умовах операційної напруги часто ігнорується, хоча саме він дає змогу вилучити уроки та вдосконалити систему захисту.

Ключовим індикатором готовності є центри моніторингу та реагування (SOC). У найбільших банках вони функціонують як аналітичні центри, що використовують платформи SIEM, інтегровані з міжнародними джерелами даних про загрози, і проводять активне полювання на загрози. Середні установи часто користуються аутсорсинговими SOC, що знижує витрати, але створює

залежність від постачальника та сповільнює реагування, а малі установи взагалі не мають централізованого моніторингу. Чим довше зловмисник непомітно перебуває в мережі, тим більших збитків завдає інцидент, тому скорочення часу виявлення атаки є головним показником ефективності центру моніторингу [107].

Кадрове забезпечення кібербезпеки фінансового сектору перебуває в стані системного дефіциту: попит на фахівців перевищує пропозицію, кваліфіковані кадри зосереджені в найбільших банках, а воєнний стан посилив дефіцит через мобілізацію та еміграцію. Ринок потребує фахівців, що поєднують розуміння банківських бізнес-процесів з володінням сучасними технологіями, тоді як освітні програми часто відстають від темпів еволюції загроз [123; 93, p. 1–17; 16, с. 188–197]. Глобальний дефіцит фахівців з кібербезпеки у 2024 році оцінювався в 4,76 млн осіб і зріс за рік на 19,1 % [123], а систематичні огляди підтверджують, що саме брак кваліфікованих кадрів і слабка підтримка керівництва є головними бар'єрами для впровадження в банках інструментів кіберзахисту на основі штучного інтелекту [93, p. 1–17]. Внутрішні програми підготовки великих банків частково заповнюють цей розрив, але їхній масштаб недостатній для покриття потреб усього сектору, особливо небанківських установ. Додатковим викликом є технологічна залежність від іноземних постачальників автоматизованих банківських систем, антифрод-рішень і хмарних сервісів, що створює непрозорі зони ризику через неможливість повного аудиту коду та ризик припинення підтримки. Міжнародна інтеграція сектору створює додаткові критерії оцінки: банки, що працюють з міжнародними платіжними системами, зобов'язані проходити аудити на відповідність PCI DSS, а учасники SWIFT щорічно підтверджують виконання обов'язкових заходів контролю, невідповідність яким загрожує відключенням від міжнародних платіжних магістралей [140; 151]. Отже, міжнародні стандарти фактично є мінімальним порогом допуску до глобальної фінансової інфраструктури. Порівняльну оцінку рівня кіберзахищеності та готовності установ різних категорій узагальнено в табл. 2.8.

Таблиця 2.8 **Порівняльна оцінка рівня кіберзахищеності та готовності фінансових установ України**

| Критерій оцінки | Системно важливі банки та банки з іноземним капіталом | Середні банки з вітчизняним капіталом | Малі банки, кредитні спілки, небанківські фінансові установи |
|---|---|---|---|
| 1. Управління кіберризиками на рівні стратегії | Інтегровано в систему управління ризиками; відповідальність правління; регулярне інформування наглядової ради | Формалізовано на рівні політик; участь правління епізодична | Окрема стратегія відсутня; кіберризики делеговані IT-підрозділу |
| 2. Технічний захист інфраструктури | Багаторівневий захист; поведінкова аналітика; шифрування; сегментація | Базовий набір засобів; часткова сегментація | Мінімальний захист; типові рішення; сегментація відсутня |
| 3. Моніторинг і реагування | Власний SOC 24/7; активне полювання на загрози; автоматизоване реагування | Аутсорсинговий SOC або частковий моніторинг; реагування в робочий час | Централізований моніторинг відсутній; запізніле виявлення |
| 4. Кадрове забезпечення | Штатні команди з десятків фахівців; внутрішнє навчання; сертифікація | Малі штатні групи; зовнішні тренінги; плинність кадрів | Один-два фахівці або суміщення з системним адмініструванням |
| 5. Тестування на проникнення та аудити | Регулярне тестування командою атаки; щорічні незалежні аудити | Епізодичне тестування зовнішнього периметра; аудити на вимогу регулятора | Тестування відсутнє; формальні звіти |
| 6. Управління інцидентами | Детальні процедури; регулярні тренінги; перевірені резервні копії | Плани наявні; нерегулярні тренінги; відсутність практичного апробування | Формальні плани; ненадійне резервування |
| 7. Сертифікація та відповідність стандартам | ISO/IEC 27001; PCI DSS; SWIFT CSCF | Часткова сертифікація; окремі стандарти | Сертифікація відсутня; формальна відповідність |

Джерело: узагальнено автором на основі [47; 124; 140; 151].

Табл. 2.8 показує, що за кожним із семи критеріїв характеристики установ різних категорій якісно відрізняються, причому малі банки та небанківські установи за більшістю критеріїв мають лише формальні елементи системи захисту. Для кількісного вимірювання розриву якісні характеристики переведено в бали експертним методом автора за п’ятибальною шкалою: 1 бал відповідає відсутності елемента системи захисту, 2 бали частковому рівню реалізації за класифікацією NIST (неформалізовані, епізодичні заходи), 3 бали рівню, поінформованому про ризики (затверджені політики без регулярної перевірки), 4 бали повторюваному рівню (стандартизовані процедури, регулярні перевірки), 5 балів адаптивному рівню (аналітика загроз і безперервне вдосконалення); проміжні значення позначено половиною бала. Інтегральний індекс

кіберзахищеності розраховано як відношення середнього бала до максимально можливого (табл. 2.9).

Таблиця 2.9 **Бальна оцінка рівня кіберзахищеності фінансових установ України за критеріями**

| Критерій оцінки | Системно важливі банки та банки з іноземним капіталом | Середні банки з вітчизняним капіталом | Малі банки і небанківські установи |
|---|---|---|---|
| 1. Управління кіберризиками на рівні стратегії | 4,5 | 3,0 | 1,5 |
| 2. Технічний захист інфраструктури | 4,5 | 3,0 | 1,5 |
| 3. Моніторинг і реагування | 5,0 | 2,5 | 1,0 |
| 4. Кадрове забезпечення | 4,0 | 2,5 | 1,0 |
| 5. Тестування на проникнення та аудити | 4,5 | 2,0 | 1,0 |
| 6. Управління інцидентами | 4,0 | 2,5 | 1,5 |
| 7. Сертифікація та відповідність стандартам | 4,5 | 2,5 | 1,0 |
| Середній бал | 4,43 | 2,57 | 1,21 |
| Інтегральний індекс кіберзахищеності | 0,89 | 0,51 | 0,24 |
| Рівень кіберзахищеності | Високий | Середній | Низький |

Джерело: розраховано автором на основі табл. 2.8 та шкали рівнів реалізації [136, с. 7–8, 24–25].

Результати табл. 2.9 показують, що інтегральний індекс кіберзахищеності системно важливих банків у 3,7 разів перевищує відповідний показник малих банків і небанківських установ, а індекс середніх банків у 1,7 разів. Найбільший розрив спостерігається за критеріями моніторингу і реагування (4,0 бала), тестування на проникнення та сертифікації (по 3,5 бала), тобто саме за тими напрямами, які потребують значних фіксованих витрат і дефіцитних фахівців. Оскільки загальний рівень кіберзахищеності фінансової системи визначається не середнім значенням, а найслабшою ланкою, вразливості менших учасників можуть бути використані як плацдарм для атак на великі банки через спільні інформаційні системи, платіжні шлюзи, корпоративних клієнтів або ланцюги постачання. Тому подолання розриву вимагає не лише зусиль окремих установ, а й системних заходів регулятора, спрямованих на підвищення мінімально допустимого рівня захисту для всіх учасників ринку.

Узагальнення результатів аналізу дає змогу сформувати SWOT-матрицю кібербезпеки фінансової системи України (табл. 2.10).

Таблиця 2.10 **SWOT-аналіз кібербезпеки фінансової системи України**

| **Сильні сторони** | **Слабкі сторони** |
|---|---|
| Високий рівень кіберзахисту системно важливих банків; досвід функціонування в умовах війни; Центр кіберзахисту НБУ і CSIRT-NBU; вимоги НБУ до звітування про значні інциденти; зниження частки інцидентів критичного та високого рівнів у загальнонаціональній статистиці CERT-UA до 0,2 % (2025 р.) | Розрив у рівні захищеності між категоріями установ (індекс 0,89 проти 0,24); дублювання функцій органів; відсутність прямих вимог до кіберзахисту в Законі «Про банки і банківську діяльність»; кадровий дефіцит; залежність від іноземних постачальників |
| **Можливості** | **Загрози** |
| Імплементація DORA і NIS2; міжнародна технічна допомога; програми відновлення; розвиток галузевих сервісів моніторингу; повернення фахівців і перекваліфікація ветеранів | Атаки державного рівня; зростання соціальної інженерії (90 % збитків); атаки з використанням штучного інтелекту; квантова загроза криптографії; удари по енергетичній інфраструктурі |

Джерело: складено автором на основі результатів аналізу, наведених у 2.1–2.3.

SWOT-аналіз показує, що сильні сторони фінансової системи зосереджені переважно в сегменті системно важливих банків і регуляторних вимог НБУ, тоді як слабкі сторони мають інституційний і кадровий характер. Можливості, пов’язані з євроінтеграцією та міжнародною допомогою, здатні компенсувати слабкі сторони лише за умови усунення дублювання функцій і поширення єдиних вимог на весь фінансовий ринок, що й визначає логіку пропозицій розділу 3.

Отже, перспективи підвищення рівня кіберзахищеності фінансового сектору України залежать від вирішення кількох ключових завдань: створення механізмів підтримки малих і середніх установ через галузеві центри моніторингу, спільні програми тестування та типові політики безпеки; розвитку національної системи кіберосвіти; посилення вимог до управління ризиками ланцюгів постачання; стимулювання обміну інформацією про інциденти та подолання культури замовчування. Обґрунтуванню цих напрямів присвячено розділ 3.

# РОЗДІЛ 3
# НАПРЯМИ ВДОСКОНАЛЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВОЇ СИСТЕМИ УКРАЇНИ

## 3.1 Удосконалення нормативно-правового та інституційного забезпечення кібербезпеки фінансового сектору

Аналіз чинного нормативно-правового поля, проведений у попередніх розділах, дає підстави констатувати, що система регулювання кібербезпеки фінансового сектору України перебуває в стані кількісного насичення за одночасної якісної фрагментації. Законодавство про захист інформації, кібербезпеку, банківську діяльність, платіжні послуги та персональні дані утворює багатошарову, але недостатньо узгоджену архітектуру, у якій відсутній акт, що комплексно врегулював би специфіку кіберзагроз саме для фінансової галузі. Через це регулятори та учасники ринку змушені інтерпретувати загальні норми через призму галузевої специфіки, що породжує неоднозначність правозастосування, надмірне адміністрування в одних сферах і правові прогалини в інших [58; 2, с. 35–42; 74, с. 355–358].

Фінансовий сектор не є лише одним із сегментів критичної інфраструктури поряд з енергетикою чи транспортом. Він виконує функцію кровоносної системи економіки, де будь-яке порушення цілісності чи доступності даних безпосередньо трансформується в економічні збитки, втрату довіри громадян і загрозу національній безпеці. Тому стратегічним завданням є розроблення спеціального закону про кібербезпеку фінансового сектору, який інтегрував би розрізнені норми, усунув суперечності та встановив єдині правила для банків, небанківських фінансових установ, надавачів платіжних послуг, страховиків, професійних учасників ринків капіталу, бюро кредитних історій, операторів платіжних систем, а також постачальників критичних ІКТ-послуг, без яких неможливе функціонування фінансової інфраструктури. Закон має закріпити класифікацію інформаційних систем за рівнями критичності з

диференційованими вимогами залежно від масштабу операцій і системної важливості установи: для системно важливих банків і операторів критичної платіжної інфраструктури вимоги мають відповідати міжнародним стандартам кіберстійкості фінансових ринкових інфраструктур, для менших установ слід передбачити пропорційну модель, яка зберігає непорушність базових принципів захисту клієнтських даних і неперервності послуг [120; 144, ст. 4].

Ключовим елементом закону має стати єдиний правовий режим звітування про кіберінциденти. Нині правила істотно різняться залежно від виду установи та органу: банки з 2025 року інформують Центр кіберзахисту НБУ про значні кіберінциденти протягом 24 годин, 72 годин і одного місяця [41], учасники платіжного ринку повинні повідомляти Національний банк про кіберінциденти «невідкладно», без визначення строку в годинах [44, п. 45], небанківські надавачі фінансових послуг лише проходять перехідний період до нових вимог [48], Закон № 4336-IX запровадив загальний обов'язок повідомляти про значні кіберінциденти [35], а Держспецзв'язку у 2026 році затвердила власні критерії значного кіберінциденту і порядок обміну інформацією [5]. Через це одна установа може бути зобов'язана повідомляти про той самий інцидент кільком адресатам за різними критеріями та в різні строки. Пропонується встановити єдину градацію інцидентів за рівнями серйозності для всіх учасників фінансового ринку з чіткими строками звітування, гармонізованими з вимогами DORA і NIS2 (табл. 3.1).

Запропонована в табл. 3.1 класифікація, на відміну від чинного порядку, поширюється на всіх учасників фінансового ринку, поєднує кількісні критерії з вимогою до змісту та строків кожного звіту, запроваджує для критичних інцидентів чотиригодинний строк первинного повідомлення після класифікації за моделлю DORA і визначає одного адресата первинного повідомлення, який автоматично передає інформацію CERT-UA та правоохоронним органам. Закон має також гарантувати конфіденційність відомостей про інцидент на етапі розслідування, щоб уникнути передчасного розголошення, здатного спровокувати паніку серед клієнтів.

Таблиця 3.1 **Запропонована класифікація кіберінцидентів у фінансовому секторі України та строки звітування**

| Рівень | Критерії віднесення | Первинне повідомлення | Проміжний звіт | Остаточний звіт | Адресат |
|---|---|---|---|---|---|
| I. Критичний | Ураження системно важливої установи або платіжної інфраструктури; недоступність критичних послуг понад 2 год; ураження понад 10 % клієнтів; ознаки атаки державного рівня; транскордонний вплив | Не пізніше 4 год після класифікації і 24 год після виявлення | 72 год | 1 місяць | Єдиний орган кіберстійкості (НБУ) з передачею CERT-UA і СБУ протягом 1 год |
| II. Значний | Витік персональних даних чи банківської таємниці; недоступність послуг від 30 хв до 2 год; прямі втрати понад встановлений поріг | 24 год після виявлення | 72 год | 1 місяць | Єдиний орган кіберстійкості; Уповноважений ВРУ з прав людини не пізніше 72 год (у разі витоку персональних даних) |
| III. Помірний | Локальні збої без витоку даних і без впливу на клієнтів понад 30 хв | 72 год (спрощена форма) | Не подається | У квартальному звіті | Єдиний орган кіберстійкості |
| IV. Незначний | Спроби атак, заблоковані засобами захисту | Не подається | Не подається | Квартальна статистика | Єдиний орган кіберстійкості (для аналітики загроз) |

Джерело: розроблено автором з використанням [144, ст. 18–19; 101; 114, ст. 23].

Правове регулювання має встановити вимоги до управління кіберризиками на корпоративному рівні. Наглядова рада фінансової установи повинна затверджувати стратегію кібербезпеки, щорічно переглядати політики управління ризиками, контролювати бюджет на інформаційну безпеку та отримувати регулярні звіти про стан кіберзахисту. Члени правління та керівники підрозділів ризиків, інформаційних технологій і безпеки мають нести персональну відповідальність за грубий недогляд у сфері кіберзахисту, що відповідає підходу NIS2 [114, ст. 20]. Водночас законодавство має захищати керівників, які діяли добросовісно та в межах затвердженої стратегії, щоб

управління кіберризиками не перетворилося на формальне відпрацювання процедур.

Інституційне забезпечення кібербезпеки фінансового сектору потребує перебудови архітектури відповідальності між державними органами. Сьогодні функції регулювання, нагляду, реагування та розслідування розподілені між Національним банком України з його Центром кіберзахисту та командою CSIRT-NBU, Державною службою спеціального зв'язку та захисту інформації з урядовою командою CERT-UA, Національним координаційним центром кібербезпеки при РНБО, Службою безпеки України та Національною поліцією [58, ст. 8; 49]. Банк, що є оператором об'єкта критичної інформаційної інфраструктури, може отримувати вимоги щодо одного й того самого об'єкта від НБУ як фінансового регулятора і секторального органу, від Держспецзв'язку як органу державного контролю за кіберзахистом критичної інформаційної інфраструктури та від правоохоронних органів у межах кримінального провадження, причому кожен орган використовує власні форми звітності, методики оцінки й термінологію. Чинний і запропонований розподіл функцій наведено в табл. 3.2.

Як видно з табл. 3.2, оптимальним рішенням є визначення Національного банку України головним органом кіберстійкості всього фінансового сектору з відповідними повноваженнями щодо об'єктів критичної інформаційної інфраструктури фінансових установ. НБУ вже виконує функції галузевого регулятора кібербезпеки фінансового сектору, має Центр кіберзахисту і команду реагування CSIRT-NBU [28, с. 6], тому розширення цих повноважень дозволить створити єдине вікно для фінансових установ і усунути дублювання. Держспецзв'язку має зберегти повноваження щодо загальнодержавних стандартів криптографічного захисту, експертизи засобів захисту та роботи CERT-UA, а РНБО через НКЦК має виконувати функції стратегічної координації. Такий поділ відповідає моделям розвинених країн, розглянутим у 1.3, де саме фінансовий регулятор несе основну відповідальність за

кіберстійкість піднаглядних установ. Організаційну модель єдиного органу та її кадрове забезпечення в період поствоєнної відбудови обґрунтовано в 3.3.

Таблиця 3.2 **Чинний і запропонований розподіл функцій у сфері кібербезпеки фінансового сектору України**

| Функція | Чинний розподіл | Проблема | Запропонований розподіл |
|---|---|---|---|
| Встановлення вимог до кіберзахисту фінансових установ | НБУ (банки, надавачі платіжних і фінансових послуг); Держспецзв'язку (об'єкти КІІ, захист інформації) | Паралельні вимоги до одних і тих самих систем | НБУ як єдиний галузевий регулятор; Держспецзв'язку визначає загальнодержавні стандарти та криптографію |
| Нагляд і перевірки кіберзахисту | НБУ (перевірки банків); Держспецзв'язку (державний контроль і аудит на об'єктах КІІ) | Подвійні перевірки, різні методики | Єдиний орган кіберстійкості в структурі НБУ; спільні перевірки за єдиною методикою |
| Прийом повідомлень про інциденти | Центр кіберзахисту НБУ (банки); НБУ (учасники платіжного ринку); CERT-UA; правоохоронні органи | Кілька каналів, різні критерії значного інциденту та строки | Єдине «вікно» повідомлень у єдиному органі з автоматичною передачею CERT-UA, СБУ та кіберполіції |
| Реагування на інциденти | CSIRT-NBU (банки); CERT-UA; СБУ; НКЦК (координація) | Небанківські установи поза галузевою командою реагування | Галузева команда реагування всього фінансового сектору на базі CSIRT-NBU, взаємодія з CERT-UA |
| Розслідування кіберзлочинів | Кіберполіція, СБУ | Затримка отримання даних від установ | Регламент обміну даними через єдиний орган |
| Обмін інформацією про загрози | Двосторонні контакти, неформальні мережі | Культура замовчування інцидентів | Галузевий центр обміну інформацією з режимом конфіденційності |

Джерело: розроблено автором з використанням [58, ст. 8; 54; 49; 41; 44; 5; 74, с. 355–358].

Необхідним елементом інституційної архітектури є галузевий центр обміну інформацією про загрози, який функціонував би на засадах державно-приватного партнерства за участю найбільших банків, платіжних систем, асоціацій учасників ринку та державних органів за зразком галузевих центрів обміну інформацією (ISAC), що діють у розвинених фінансових системах. Законодавство має створити умови для довірливого обміну даними, гарантуючи, що інформація, надана установою для попередження інших учасників, не буде використана як підстава для санкцій, якщо установа своєчасно виявила інцидент, вжила заходів для його локалізації та діяла добросовісно. Водночас технічні деталі атаки, індикатори компрометації та заходи захисту можуть поширюватися

в закритому режимі, тоді як відомості про наслідки для клієнтів і витоки персональних даних підлягають обов’язковому розкриттю.

Невід’ємною складовою правового забезпечення є вдосконалення кримінального законодавства. Чинні норми про несанкціоноване втручання в роботу інформаційних систем і створення шкідливих програмних засобів не враховують специфіку атак на фінансову інфраструктуру [20, ст. 361–363-1]. Доцільно запровадити кваліфікуючі ознаки для кіберзлочинів проти систем електронних платежів, масової компрометації платіжних інструментів, маніпуляцій з банківськими базами даних і цілеспрямованого блокування роботи системно важливих установ. Окремої уваги потребує регулювання обігу віртуальних активів, адже незавершеність введення в дію правил щодо діяльності постачальників послуг у цій сфері створює канали легалізації коштів, отриманих унаслідок кібератак, і виплати викупу програмам-вимагачам [34; 145].

Гармонізація національного законодавства з європейськими стандартами зумовлена євроінтеграційними прагненнями України. Директива NIS2 та Регламент DORA встановлюють нову планку вимог до фінансових установ, імплементація якої потребує не технічного перекладу норм, а інституційної реформи: визначення компетентних органів, механізмів транскордонного обміну інформацією, узгодження строків звітування та критеріїв класифікації інцидентів. Це створить передумови для взаємного визнання українських сертифікатів, спрощення доступу банків до європейських ринків та інтеграції української фінансової інфраструктури в європейський простір кібербезпеки [114; 144; 21, с. 400–412; 99, p. 11–28; 133, p. 143–150].

Ступінь готовності національної нормативної бази до імплементації Регламенту DORA можна оцінити, зіставивши його ключові вимоги з чинними актами Національного банку (табл. 3.3).

Таблиця 3.3 **Відповідність нормативно-правової бази НБУ ключовим вимогам Регламенту DORA**

| Напрям DORA | Вимога DORA | Чинне регулювання в Україні | Розрив і пропозиція |
|---|---|---|---|
| Управління ризиками ІКТ | Рамка управління ризиками ІКТ, відповідальність органу управління (ст. 5–16) | Глава щодо ризиків ІКТ та інформаційної безпеки в Положенні № 64 (з 2023 р.) | Закріпити обов'язки ради банку на рівні закону (додаток А) |
| Звітування про інциденти | Первинне повідомлення 4/24 год, проміжне 72 год, остаточне 1 місяць (ст. 19) | Для банків 24 год, 72 год, 1 місяць (з 2025 р.); для платіжного ринку «невідкладно» | Єдина класифікація і строки для всіх учасників (табл. 3.1) |
| Тестування цифрової операційної стійкості | Щорічне тестування; тестування на основі загроз раз на 3 роки для значущих установ (ст. 24–27) | Періодичні тести на проникнення без визначеної періодичності (п. 108 Положення № 95) | Щорічні тести і тестування на основі загроз для системно важливих банків |
| Ризики третіх сторін ІКТ | Управління ризиками постачальників, нагляд за критичними постачальниками (ст. 28–44) | Вимоги до управління ризиком третіх сторін для банків, надавачів платіжних послуг і страховиків діють з 01.07.2026 | Поширити вимоги на інших учасників ринку; реєстр і нагляд за критичними постачальниками |
| Обмін інформацією | Добровільний обмін даними про кіберзагрози (ст. 45) | Інформаційний обмін через Центр кіберзахисту НБУ (банки) | Галузевий центр обміну інформацією для всього фінансового сектору |

Джерело: складено автором за [144; 101; 50; 37; 41; 44; 47, п. 108; 22; 49, п. 13].

Як видно з табл. 3.3, найближчими до європейських стандартів є вимоги НБУ щодо звітування банків про значні кіберінциденти та управління ризиками ІКТ, тоді як найбільші розриви стосуються тестування на основі загроз, нагляду за критичними постачальниками ІКТ-послуг і поширення вимог на небанківських учасників ринку. Саме ці напрями відображено в запропонованих змінах до законодавства.

Конкретні пропозиції щодо змін до чинних нормативно-правових актів, які випливають із проведеного аналізу, наведено в додатку А. Вони стосуються шести актів: Закону України «Про основні засади забезпечення кібербезпеки України» (закріплення статусу НБУ як органу кіберстійкості фінансового сектору і єдиного вікна звітування), Закону України «Про банки і банківську діяльність» (вимоги до управління ризиками ІКТ і кіберстійкості на рівні закону), Закону України «Про захист персональних даних» (обов'язок повідомляти про витоки персональних даних), Закону України «Про платіжні послуги» (строки

повідомлення про інциденти та тестування стійкості), Кримінального кодексу України (кваліфікуюча ознака кіберзлочинів проти фінансової інфраструктури) та Положення НБУ про організацію заходів із забезпечення інформаційної безпеки в банківській системі (тестування на проникнення на основі загроз). Для кожного акта наведено чинну редакцію норми, запропоновану редакцію та пояснення необхідності змін.

Правове регулювання має передбачати і механізми державної підтримки фінансових установ у сфері кібербезпеки. Воєнний стан обмежує можливості середніх і малих банків інвестувати в дороговартісні системи захисту, тому доцільними є програми часткового відшкодування витрат на засоби криптографічного захисту, резервні центри обробки даних і підготовку персоналу, податкові стимули у вигляді прискореної амортизації обладнання та програмного забезпечення кіберзахисту, а також розвиток кіберстрахування. Страховики, проводячи власні аудити перед укладенням договорів, стають додатковим контролером рівня захищеності, а установи з кращими системами безпеки отримують нижчі премії [85, с. 98–106; 149].

Інституційні зміни мають супроводжуватися розвитком міжнародного правового співробітництва, адже кіберзлочинність у фінансовій сфері має транскордонний характер. Ефективне розслідування потребує використання механізмів Європолу, Євроюсту та Інтерполу, спрощення процедур міжнародної правової допомоги та оперативного доступу до даних на іноземних серверах. Технічні вимоги доцільно встановлювати підзаконними актами регулятора з обов’язковим громадським обговоренням і перехідними періодами, що забезпечить гнучке реагування на нові загрози без постійних змін до закону.

Таким чином, удосконалення нормативно-правового та інституційного забезпечення кібербезпеки фінансового сектору України потребує системних змін на кількох рівнях. На законодавчому рівні необхідні спеціальний акт і точкові зміни до чинних законів, що встановлюють чіткі правила звітування про інциденти, персональну відповідальність керівництва та механізми колективного захисту. На інституційному рівні потрібно розмежувати

повноваження між НБУ та Держспецзв'язку і створити єдиний орган кіберстійкості з галузевим центром обміну інформацією. На міжнародному рівні слід забезпечити імплементацію NIS2 і DORA, а на економічному слід запровадити стимули для інвестування в кіберзахист.

## 3.2 Технологічні та організаційні заходи підвищення стійкості фінансової системи до кіберзагроз

Підвищення стійкості фінансової системи до кіберзагроз вимагає відмови від концепції абсолютного захисту на користь моделі стійкості, яка передбачає здатність витримувати атаки, швидко виявляти проникнення, локалізувати його наслідки та відновлювати критичні функції в мінімальні строки. У сучасних умовах жоден периметр не є непроникним, тому пріоритет зміщується з попередження будь-якого проникнення на мінімізацію часу перебування загрози в мережі, обмеження зони її впливу та забезпечення неперервності бізнесу. Реалізація цієї моделі потребує поєднання технологічних рішень, що створюють багаторівневий захист, та організаційних механізмів, які забезпечують управління цими рішеннями і компетентність персоналу. В українських умовах технологічні засоби мають працювати під час перебоїв з електропостачанням, фізичної небезпеки для персоналу та можливої ізоляції окремих сегментів інфраструктури [141; 68, с. 304–311; 100].

Архітектурною основою сучасного технологічного захисту фінансових установ стає концепція нульової довіри (Zero Trust). Традиційна модель безпеки будувалася навколо чіткого периметра: всередині корпоративної мережі перебували довірені користувачі, а зовні потенційні загрози. Ця модель втратила адекватність у світі хмарних сервісів, віддаленої роботи, мобільних застосунків і партнерських API. Концепція Zero Trust відкидає припущення про довіру до будь-якого суб'єкта чи пристрою незалежно від його розташування: кожен запит на доступ підлягає верифікації, кожна сесія автентифікується, а рішення про доступ ухвалюється з урахуванням контексту, тобто часу, геолокації, стану

пристрою та історії операцій [147]. Застарілі банківські системи ускладнюють перехід до цієї архітектури, проте навіть поступова міграція суттєво звужує поверхню атаки та ускладнює горизонтальне переміщення зловмисника.

Шифрування як фундаментальний механізм захисту конфіденційності та цілісності даних потребує постійного вдосконалення. Розвиток квантових обчислень ставить під загрозу асиметричні криптографічні алгоритми, що лежать в основі протоколів захищеного з'єднання, цифрових підписів та обміну ключами. Фінансовий сектор, який зберігає архіви транзакцій і довгострокові зобов'язання, має вже зараз планувати перехід на постквантову криптографію: у 2024 році Національний інститут стандартів і технологій США затвердив перші стандарти постквантових алгоритмів [134]. Впровадження гібридних схем, що поєднують класичне та постквантове шифрування, а також управління життєвим циклом ключів у апаратних модулях безпеки дозволять забезпечити захищений перехідний період [129, p. 145–154; 29, с. 165–176].

Багатофакторна автентифікація стала мінімально допустимим стандартом доступу до критичних систем фінансових установ і передбачена вимогами НБУ до інформаційної безпеки банків [47], оскільки парольна автентифікація вразлива до фішингу, підбору та витоків баз даних. Для адміністраторів критичних систем доцільно запроваджувати апаратні токени з підтримкою протоколів FIDO2, які унеможливлюють фішинг облікових даних, а біометричні шаблони клієнтів мобільного банкінгу слід зберігати на пристрої, а не в хмарі. Централізоване управління ідентифікацією та доступом дає змогу оперативно відкликати права в разі звільнення працівника чи підозри на компрометацію та виявляти аномалії, зокрема одночасний вхід з різних географічних точок.

Системи моніторингу та реагування на події безпеки є ядром кіберзахисту фінансової установи. Платформи SIEM агрегують дані міжмережевих екранів, систем виявлення вторгнень, антивірусного захисту, систем управління доступом, застосунків і баз даних, а кореляція подій дозволяє виявляти багатоетапні атаки, що проявляються як ланцюжок аномалій. Поведінкова аналітика на основі машинного навчання будує профілі нормальної активності

користувачів і пристроїв, а платформи автоматизованого реагування виконують сценарії блокування облікового запису чи ізоляції пристрою [82, с. 704–716; 77, с. 203–209; 4, с. 244–255]. Надмірна автоматизація несе ризик помилкових спрацювань, що блокують легітимні операції, тому баланс між автоматичними діями та людським контролем потребує постійного налаштування. Захист кінцевих точок еволюціонував від сигнатурних антивірусів до платформ EDR і XDR. Традиційні рішення, засновані на сигнатурному аналізі, неефективні проти цілеспрямованих атак з унікальними інструментами або легітимними системними утилітами, тоді як EDR відстежує активність процесів, їхні взаємозв'язки, зміни у файловій системі та мережеві з'єднання на кожній робочій станції і сервері, а XDR об'єднує дані кінцевих точок, мережі, хмари та електронної пошти в єдине поле видимості для аналітика. Для фінансових установ з віддаленими працівниками і партнерськими доступами такі платформи разом з управлінням мобільними пристроями, шифруванням корпоративних даних і можливістю віддаленого очищення пристрою стають необхідним інструментом контролю розширеного периметра.

Резервування даних і можливість відновлення після катастрофічних подій є технологічним і організаційним фундаментом стійкості. Програми-вимагачі довели, що резервні копії не гарантують відновлення, якщо вони зберігаються в тій самій інфраструктурі або зловмисник встиг їх зашифрувати. Сучасна стратегія передбачає правило трьох копій на двох типах носіїв з однією копією, фізично відокремленою від мережі, незмінність резервних копій та регулярне тестування відновлення. Для українського фінансового сектору воєнний стан додав вимогу географічної рознесеності резервів, захищених від одночасного фізичного ураження.

Організаційні заходи підвищення стійкості починаються з сегментації мережі та мікросегментації критичних зон, що узгоджується з вимогами НБУ до захисту периметра мережі банку [47]. Плоска мережа дозволяє зловмиснику вільно переміщуватися після проникнення, тоді як поділ на зони з різними рівнями довіри (публічна, корпоративна, адміністративна, критична зона баз

даних і процесингу) обмежує поширення атаки. Принцип мінімальних привілеїв має реалізовуватися в операційній практиці через періодичний перегляд прав, автоматичне відкликання доступу та тимчасове надання підвищених прав адміністраторам лише на час виконання конкретного завдання з журналюванням усіх операцій у незмінному сховищі.

Щодо персоналу, програми підвищення обізнаності мають виходити за межі разових лекцій: ефективними є імітаційні фішингові кампанії з миттєвим зворотним зв'язком і практичні тренінги з реагування на інциденти. Культура безпеки формується керівництвом, яке дотримується процедур і підтримує ініціативи підрозділу захисту. В умовах хронічного стресу персоналу під час воєнного стану завдання формування такої культури ускладнюється, але не втрачає актуальності [65, с. 331–347; 71, с. 90–97].

Ефективність управління інцидентами (див. 2.3) визначається не обсягом документації, а якістю апробації, а для фінансового сектору особливо важливою є своєчасна комунікація з клієнтами, оскільки затримка породжує чутки та паніку. Управління ланцюгами постачання технологій і послуг передбачає перевірку постачальників перед укладенням договорів, включення вимог до кібербезпеки в договори, регулярний аудит і плани на випадок припинення підтримки, що для українських банків має і геополітичний вимір через юрисдикцію постачальника [144, ст. 28–30].

Забезпечення безперервності бізнесу поєднує технологічні та організаційні компоненти. Безперервність бізнесу передбачає не лише резервування даних, а й здатність продовжувати критичні операції в умовах часткової втрати інфраструктури: наявність географічно рознесених майданчиків обробки даних, резервних каналів зв'язку, незалежних від основного провайдера, і можливість роботи персоналу з альтернативних локацій. Плани відновлення мають бути деталізовані до рівня окремих бізнес-процесів з визначенням цільового часу відновлення та допустимих втрат даних, а їхня працездатність перевірятися симуляціями відмови основного центру обробки даних, оскільки апробація на реальних георозподілених середовищах банків виявляє приховані дефекти

конфігурації, непомітні під час формальних перевірок [68, с. 304–311]. В українських умовах плани безперервності враховують сценарії масованих ракетних ударів, тривалих відключень електроенергії, евакуації персоналу та ізоляції регіонів, а фізична безпека центрів обробки даних стала невід'ємною частиною кібербезпеки. Пріоритетність заходів для установ різних категорій узагальнено в табл. 3.4.

Таблиця 3.4 **Пріоритетні технологічні та організаційні заходи підвищення кіберстійкості фінансових установ України**

| Захід | Зміст | Системно важливі банки | Інші банки і небанківські установи | Очікуваний ефект |
|---|---|---|---|---|
| Архітектура Zero Trust | Поетапна верифікація кожного запиту на доступ, мікросегментація | Високий (до 3 років) | Середній (через хмарні сервіси) | Обмеження горизонтального переміщення зловмисника |
| Багатофакторна автентифікація | FIDO2-токени для адміністраторів, MFA для всіх працівників і клієнтів | Високий (негайно) | Високий (негайно) | Нейтралізація більшості фішингових атак на облікові записи |
| Моніторинг і реагування (SIEM, EDR/XDR, SOC) | Цілодобовий моніторинг, автоматизовані сценарії реагування | Високий (власний SOC) | Високий (галузевий або аутсорсинговий SOC) | Скорочення часу виявлення і локалізації атак |
| Захищене резервування | Правило 3-2-1, незмінні та географічно рознесені копії | Високий | Високий | Відновлення після атак програм-вимагачів і фізичних уражень |
| Постквантова криптографія | Інвентаризація криптографії, гібридні схеми, апаратні модулі безпеки | Середній (план до 2030 р.) | Низький | Захист довгострокових архівів і транзакцій |
| Навчання персоналу | Імітаційні фішингові кампанії, практичні тренінги | Високий | Високий | Зменшення ризику успішної соціальної інженерії |
| Управління постачальниками ІКТ | Перевірка, договірні вимоги, аудит, плани виходу | Високий | Середній | Зниження ризиків ланцюга постачання |
| Тестування на основі загроз | Тестування на проникнення за моделлю TIBER-EU/CBEST | Високий (раз на 3 роки) | Не обов'язкове | Перевірка реальної готовності до складних атак |

Джерело: розроблено автором з використанням [144; 152; 136; 68, с. 304–311].

З табл. 3.4 випливає, що частина заходів, зокрема багатофакторна автентифікація, захищене резервування і навчання персоналу, має високий пріоритет для всіх установ незалежно від розміру та не потребує значних

інвестицій, тоді як власні центри моніторингу і тестування на основі загроз доцільно вимагати від системно важливих банків, а для інших учасників забезпечувати через галузеві сервіси. Синергія технологічних та організаційних заходів полягає в тому, що жоден інструмент не є самодостатнім: система захисту кінцевих точок вимагає кваліфікованого аналітика, шифрування втрачає сенс за недосконалого управління ключами, а резервні копії корисні лише за наявності перевірених процедур відновлення. Тому ефективність кожної інвестиції в кіберзахист має вимірюватися не кількістю встановлених продуктів, а зростанням реальної здатності установи витримувати атаки та відновлюватися.

## 3.3 Стратегічні пріоритети розвитку кібербезпеки фінансової системи України в умовах воєнного стану та поствоєнної відбудови

Кібербезпека фінансової системи перестає бути суто технічною функцією окремих установ і стає стратегічним елементом національної безпеки. Стійкість банківського сектору, платіжних систем і ринків капіталу безпосередньо визначає здатність держави фінансувати оборону, виконувати соціальні зобов’язання та зберігати довіру громадян. Стратегічний підхід вимагає виходу за межі тактичного реагування на окремі інциденти і формування довгострокового бачення, яке поєднує заходи забезпечення живучості в умовах воєнного стану з перетвореннями, необхідними для інтеграції в європейський простір і відбудови економіки [62; 73].

Першочерговим пріоритетом воєнного періоду є живучість фінансової інфраструктури, тобто її здатність виконувати критичні функції під час кібератак, ракетних ударів по енергетичних об’єктах, перебоїв зі зв’язком або евакуації персоналу. Реалізація цього пріоритету вимагає переходу від централізованого захисту периметра до архітектури розподіленої стійкості: критичні системи мають бути географічно розосереджені й здатні до автономної роботи, резервні центри обробки даних розміщені в локаціях, захищених від одночасного ураження, а протоколи перемикання на резервні майданчики

відпрацьовані на регулярних навчаннях. Особливого захисту потребують системи електронних платежів і міжбанківських розрахунків, порушення яких має негайний каскадний ефект для економіки.

Другий пріоритет полягає в збереженні та розвитку людського капіталу. Технології можна придбати, інфраструктуру відновити, проте кваліфікований фахівець, що поєднує розуміння банківських процесів, володіння сучасними методами захисту та здатність діяти в кризі, є ресурсом, який неможливо швидко замінити. Мобілізація, еміграція і перехід фахівців до оборонного сектору чи іноземних компаній поглибили кадровий дефіцит, який за оцінками ISC2 має глобальний характер [123]. Держава спільно з фінансовими установами має сформувати національну екосистему підготовки кадрів, що охоплює освітні програми закладів вищої освіти, синхронізовані з потребами сектору, програми перекваліфікації, гранти для студентів, бронювання ключових фахівців і умови для повернення спеціалістів після завершення воєнного стану [16, с. 188–197; 18, с. 504–511].

Третім пріоритетом є поглиблення міжнародної співпраці. Воєнний стан засвідчив, що Україна не може самотужки протистояти кіберзагрозам державного рівня, тому технічна допомога партнерів, обмін індикаторами компрометації та консультаційна підтримка регуляторів ЄС стали чинниками стійкості фінансової системи. Стратегічною метою є практична інтеграція в європейський простір кібербезпеки через угоди про обмін даними між галузевими центрами, участь у спільних навчаннях і стажування українських фахівців у європейських наглядових органах. Ця співпраця має бути двосторонньою, адже Україна набула унікального досвіду протистояння масштабним гібридним атакам.

Поствоєнна відбудова фінансової системи не має обмежуватися відновленням довоєнного стану. Воєнний період прискорив цифровізацію, і цей досвід створює підґрунтя для якісного стрибка на основі гармонізації з NIS2 і DORA: єдиної системи нагляду за кіберстійкістю, обов’язкового тестування на основі загроз, чітких процедур звітування та персональної відповідальності

керівництва. Відбудова має передбачати інвестиції не лише в житловий фонд та інфраструктуру, а й у цифрову стійкість фінансової системи [86, с. 392–400; 12, с. 214–223].

Найважливішою перспективною ініціативою поствоєнного періоду, на нашу думку, є створення єдиного органу кіберстійкості фінансового сектору, який замінить нинішню розпорошену модель (див. 1.2 і табл. 3.2). Дублювання вимог і перевірок з боку кількох державних органів, різні форми звітності та відсутність галузевої ланки реагування не дозволяють сформувати єдину, надійну і зрозумілу для учасників ринку систему. Пропонується утворити Центр кіберстійкості фінансового сектору як відокремлений структурний підрозділ Національного банку України на базі наявного Центру кіберзахисту та команди CSIRT-NBU зі статусом галузевої команди реагування на кіберінциденти всього фінансового сектору, передбаченим Законом № 4336-IX [35], який об’єднає функції регулювання і нагляду, єдиного вікна повідомлень про інциденти, галузевого центру моніторингу, обміну інформацією про загрози, тестування стійкості та підготовки кадрів. Держспецзв’язку і CERT-UA взаємодіятимуть з Центром на підставі меморандуму, а правоохоронні органи отримуватимуть дані про інциденти через регламентований канал. Організаційну структуру та кадрове забезпечення Центру наведено в табл. 3.5.

Таблиця 3.5 **Організаційна структура і кадрове забезпечення Центру кіберстійкості фінансового сектору**

| Структурний підрозділ | Основні функції | Етап II (кінець першого року відбудови), осіб | Етап III (кінець третього року відбудови), осіб |
|---|---|---|---|
| Управління регулювання та нагляду | Розроблення вимог і методик, перевірки кіберзахисту установ, оцінка відповідності | 15 | 25 |
| Галузева команда реагування (CSIRT-FIN) | Єдине вікно повідомлень, координація реагування, цілодобове чергування | 20 | 35 |
| Галузевий центр моніторингу (SOC як послуга) | Моніторинг подій безпеки для малих банків і небанківських установ на договірних засадах | 25 | 60 |
| Центр обміну інформацією про загрози (FIN-ISAC) | Аналітика загроз, поширення індикаторів компрометації, взаємодія з CERT-UA та партнерами ЄС | 10 | 20 |
| Відділ тестування стійкості | Організація тестування на проникнення на основі загроз за моделлю TIBER-EU, кібернавчання сектору | 8 | 15 |
| Навчально-сертифікаційний центр | Програми підготовки та перекваліфікації, зокрема для ветеранів, сертифікація фахівців | 7 | 15 |
| Регіональні представництва | Взаємодія з установами в регіонах, виїзне реагування | 10 | 25 |
| Адміністративне забезпечення | Правове, фінансове, кадрове забезпечення | 10 | 15 |
| Разом | – | 105 | 210 |

Джерело: розроблено автором.

Етапи формування Центру узгоджено з дорожньою картою (див. табл. 3.8): чисельність на етапі II наведено станом на кінець першого року після завершення воєнного стану, коли Центр формується на базі наявних підрозділів НБУ з кіберзахисту, а на етапі III станом на кінець третього року, коли запрацює повноцінний галузевий центр моніторингу як послуга для малих учасників ринку. Отже, на етапі III чисельність Центру становитиме 210 осіб, зокрема фахівців з кібербезпеки, аналітиків загроз, юристів і викладачів; кількість нових робочих місць дорівнюватиме різниці між цим показником і чисельністю працівників наявних підрозділів НБУ з кіберзахисту, які увійдуть до Центру. Водночас запровадження єдиних вимог до кіберзахисту формує ширший попит на фахівців у самих фінансових установах. Мінімальну нормативну потребу сектору в таких фахівцях пропонується визначати за формулою:

$$N = \sum_{i=1}^{k} n_i \times s_i \quad (3.1)$$

де N – мінімальна нормативна потреба фінансового сектору у фахівцях з кібербезпеки, осіб;

$n_i$ – кількість фінансових установ і-ї категорії, од.;

$s_i$ – нормативна чисельність фахівців з кібербезпеки на одну установу і-ї категорії, осіб;

k – кількість категорій фінансових установ.

Нормативи чисельності обґрунтовано складом мінімально необхідних функцій. Для системно важливого банку з власним цілодобовим центром моніторингу потрібні п’ять змін по три аналітики (15 осіб), а також керівник з інформаційної безпеки, інженери захисту, фахівці з аналізу загроз, тестування, управління доступом і навчання персоналу (10 осіб), разом 25 осіб. Для інших банків, які отримують нічний моніторинг як послугу, норматив становить 6 осіб: керівник з інформаційної безпеки, два аналітики, інженер захисту, фахівці з управління доступом і з комплаєнсу та навчання. Для страховиків прийнято 2 особи (відповідальна особа та інженер), для фінансових компаній 1 особу, для кредитних спілок і ломбардів 0,5 штатної одиниці за умови підключення до галузевого центру моніторингу. Результати розрахунку наведено в табл. 3.6.

Розрахунок, наведений у табл. 3.6, показує, що мінімальна нормативна потреба фінансових установ становить 1 234 фахівці з кібербезпеки, а разом із Центром кіберстійкості 1 444 робочі місця. Із потреби фінансових установ 570 осіб (46 %) припадає на небанківський сектор, де сьогодні такі посади здебільшого відсутні або поєднуються з функціями системного адміністрування. Враховуючи глобальний дефіцит фахівців з кібербезпеки, який у 2024 році перевищив 4,7 млн осіб [123], створення цих робочих місць потребує конкурентного рівня оплати праці, державного замовлення на підготовку фахівців за спеціальністю «Кібербезпека та захист інформації» і практичної підготовки на базі Центру. Саме тому навчально-сертифікаційний центр включено до структури органу: він дасть змогу перекваліфіковувати ІТ-фахівців,

ветеранів і внутрішньо переміщених осіб, а також підтримувати єдиний рівень кваліфікації персоналу всього сектору.

Таблиця 3.6 **Розрахунок мінімальної нормативної потреби фінансового сектору України у фахівцях з кібербезпеки**

| Категорія фінансових установ | Кількість установ ($n_i$), од. | Норматив чисельності ($s_i$), осіб | Потреба ($n_i \times s_i$), осіб |
|---|---|---|---|
| Системно важливі банки | 16 | 25 | 400 |
| Інші банки | 44 | 6 | 264 |
| Страховики | 53 | 2 | 106 |
| Фінансові компанії | 378 | 1 | 378 |
| Кредитні спілки | 76 | 0,5 | 38 |
| Ломбарди | 96 | 0,5 | 48 |
| Разом у фінансових установах | 663 | – | 1 234 |
| Центр кіберстійкості фінансового сектору (етап III) | 1 | – | 210 |
| Усього | – | – | 1 444 |

Джерело: розраховано автором за формулою (3.1) на основі даних [27, с. 4; 25; 26]. Примітка. Кількість банків наведено станом на 01.01.2026, небанківських установ станом на 01.09.2026 без страхових брокерів і колекторських компаній; норматив 0,5 означає часткову зайнятість або спільного фахівця за умови підключення установи до галузевого центру моніторингу.

Очікуваний економічний ефект від запровадження запропонованих заходів доцільно оцінити через зменшення збитків від шахрайства з платіжними картками, основну частину яких формує соціальна інженерія (див. табл. 2.5). Обов’язкове повідомлення клієнтів про витоки персональних даних, галузевий обмін індикаторами шахрайських ресурсів, моніторинг для малих установ і програми кібергігієни безпосередньо спрямовані на цей вид втрат. Річний ефект пропонується розраховувати за формулою:

$$E = L_{ce} \times d \tag{3.2}$$

де E – очікуване зменшення річних збитків, млн грн;

$L_{ce}$ – річні збитки від шахрайства із застосуванням соціальної інженерії, млн грн;

d – очікувана частка зменшення збитків, частки одиниці.

За даними 2025 року збитки від шахрайства з платіжними картками становили близько 1 400 млн грн, з них 90 % припало на соціальну інженерію, тобто $L_{ce}$ = 1 400 × 0,9 = 1 260 млн грн. Значення d є припущенням автора: як орієнтир використано результати моделювання для сервісів відкритого банкінгу, за якими жорсткіші вимоги до підключення та краще виявлення аномалій зменшують граничні операційні втрати на 20–30 % [138], а помірний сценарій (10 %) відображає консервативну оцінку. Результати розрахунку за трьома сценаріями наведено в табл. 3.7.

Таблиця 3.7 **Сценарна оцінка очікуваного ефекту від зниження збитків від шахрайства з платіжними картками**

| Показник | Помірний сценарій | Базовий сценарій | Оптимістичний сценарій |
|---|---|---|---|
| Річні збитки від соціальної інженерії ($L_{ce}$), млн грн | 1 260 | 1 260 | 1 260 |
| Частка зменшення збитків (d) | 0,10 | 0,20 | 0,30 |
| Очікуваний річний ефект (E), млн грн | 126 | 252 | 378 |
| Ефект за п’ять років за незмінної бази, млн грн | 630 | 1 260 | 1 890 |

Джерело: розраховано автором за формулою (3.2) на основі даних [75]; частку d прийнято за припущенням автора з урахуванням [138].

Навіть за помірного сценарію щорічне зменшення збитків клієнтів фінансових установ становитиме близько 126 млн грн, а за базового сценарію сягне 252 млн грн, які залишаються у клієнтів і фінансових установ і знижують навантаження на систему розгляду скарг та правоохоронні органи. Крім прямого ефекту, запропоновані заходи знижують імовірність витоків даних, середня вартість яких у фінансовій галузі у світі перевищує 5,5 млн дол. США (див. табл. 2.6).

Фінансування Центру доцільно здійснювати за рахунок кошторису НБУ, внесків піднаглядних установ за послуги галузевого моніторингу та програм міжнародної технічної допомоги на відновлення України. Соціальний ефект ініціативи полягає у створенні якісних робочих місць, зменшенні відтоку кваліфікованих кадрів за кордон, залученні ветеранів, які набули досвіду кібероперацій, через програми перекваліфікації, а також у формуванні центру

компетенцій, здатного надавати експертні послуги країнам, що стикаються з аналогічними гібридними загрозами.

Технологічна стратегія поствоєнного періоду має бути зосереджена на побудові адаптивних систем, здатних еволюціонувати разом із загрозами: модульних мікросервісних архітектур, які ізолюють компрометацію окремого компонента, власних компетенцій у сфері штучного інтелекту для виявлення аномалій і стійкої інфраструктури цифрової гривні, адже управління інформаційними системами за міжнародними нормами цифрової безпеки є основою цифрового суверенітету [98, p. 7–11]. Паралельно має відбуватися модернізація національної платіжної системи та її інтеграція з європейськими платіжними інфраструктурами, що вимагатиме відповідності їхнім стандартам кіберстійкості [153; 69, с. 56–73].

Відновлення довіри населення та міжнародних партнерів є пріоритетом, що виходить за межі технічних аспектів. Прозорість у питаннях кібербезпеки, своєчасне інформування клієнтів про інциденти та чітка комунікація щодо компенсаційних механізмів формують довгострокову лояльність, а для міжнародних партнерів довіра формується через відповідність стандартам, відкритість до аудитів і участь у галузевих ініціативах. Кіберзахист має розглядатися як капітальна інвестиція в стійкість бізнесу та економічну безпеку держави, а багатоканальна модель його фінансування може поєднувати цільові програми відбудови, кіберстрахування, податкові стимули та міжнародні гранти. Узагальнену дорожню карту реалізації стратегічних пріоритетів наведено в табл. 3.8.

Відповідно до табл. 3.8, стратегічні пріоритети воєнного та поствоєнного періодів не протиставляються одне одному, а утворюють континуум розвитку. Георозподілена інфраструктура, створена для протистояння ракетним ударам, одночасно підвищує стійкість до кібератак, культура швидкого реагування стає конкурентною перевагою, а досвід протистояння державним кіберпідрозділам формує компетенції, у яких зацікавлені партнери.

Таблиця 3.8 **Дорожня карта розвитку кібербезпеки фінансової системи України**

| Етап | Ключові заходи | Індикатори досягнення |
|---|---|---|
| I. Воєнний стан | Географічне резервування критичних систем; обов'язкова багатофакторна автентифікація; єдина форма повідомлення про інциденти; галузеві кібернавчання | Частка установ з MFA для привілейованих облікових записів 100 %; первинне повідомлення про критичні інциденти не пізніше 4 год |
| II. Перші два роки відбудови | Утворення Центру кіберстійкості фінансового сектору; ухвалення змін до законодавства (додаток А); запуск FIN-ISAC і SOC як послуги | Не менше 105 фахівців у Центрі; пілотний запуск SOC як послуги |
| III. Інтеграційний (до п'яти років) | Повна імплементація NIS2 і DORA; тестування на основі загроз для системно важливих банків; план переходу на постквантову криптографію | Усі системно важливі банки пройшли тестування на основі загроз; 210 фахівців у Центрі; підключення до SOC як послуги більшості малих установ; взаємне визнання з наглядовими органами ЄС |

Джерело: розроблено автором з використанням [62; 144; 114].

Кожен крок, спрямований на забезпечення безперервності сьогодні, наближає момент, коли українська фінансова система вийде з війни не ослабленою, а зміцненою та готовою до повноцінної інтеграції в європейський економічний простір.

# ВИСНОВКИ

Проведене дослідження дало змогу обґрунтувати теоретичні засади та розробити практичні рекомендації щодо вдосконалення рівня кібербезпеки фінансової системи України для подальшого соціально-економічного розвитку та захисту інтересів держави і сформулювати такі висновки.

1. Кібербезпека фінансової системи перетворилася з вузькоспеціалізованої функції інформаційних технологій на стратегічний вимір національної безпеки. Узагальнення нормативних і міжнародних підходів дозволило визначити її як стан захищеності фінансових установ, платіжної та ринкової інфраструктури, даних і коштів клієнтів у кіберпросторі, за якого забезпечуються конфіденційність, цілісність і доступність фінансових операцій та кіберстійкість системи. Кібербезпека фінансової установи інтегрує технічну, організаційну, правову, людську та стратегічну складові, жодна з яких не є самодостатньою, а кіберзагрози у фінансовому секторі мають каскадний характер, коли локальний інцидент здатен перерости в загрозу стабільності всієї системи.

2. Нормативно-правове регулювання кібербезпеки фінансового сектору України є багаторівневим, але фрагментарним: загальні закони про кібербезпеку, захист інформації та критичну інфраструктуру не враховують специфіки платіжних операцій, а повноваження Національного банку України та Держспецзв’язку щодо об’єктів критичної інформаційної інфраструктури частково дублюються. Найдеталізованіші вимоги встановлено нормативно-правовими актами Національного банку, зокрема щодо інформування про значні кіберінциденти протягом 24 годин, 72 годин і одного місяця, тоді як Закон «Про банки і банківську діяльність» у статтях про внутрішній контроль і регулювання прямо не згадує кіберзахисту, а критерії значного інциденту та порядок звітування визначаються різними органами окремо. Зіставлення темпів розвитку технологій і регулювання засвідчило, що відставання українського законодавства від актів ЄС становить від одного до шести років, а з урахуванням фактичного запровадження сягає семи років. Для залежності від хмарних

постачальників, атак з використанням штучного інтелекту та квантової загрози спеціального регулювання фінансового сектору поки немає; наукова база також реагує на нові загрози із запізненням.

3. Міжнародний досвід засвідчує відсутність універсальної моделі кіберзахисту, проте виявляє спільні риси: провідну роль фінансового регулятора в нагляді за кіберстійкістю, чіткі строки повідомлення про інциденти (від однієї до сімдесяти двох годин), тестування на проникнення на основі розвідданих про загрози (CBEST, TIBER-EU) та галузеві центри обміну інформацією. Регламент DORA і Директива NIS2 формують для України цільову модель регулювання, яку необхідно доповнити механізмами протидії гібридним загрозам воєнного періоду.

4. Фінансова система України функціонує в умовах прискореної цифровізації та консолідації: кількість діючих банків за 2021–2025 роки скоротилася з 73 до 60, чисті активи зросли в 2,2 раза, а частка безготівкових операцій у кількості операцій з платіжними картками досягла 95,5 %. Кількість кіберінцидентів, опрацьованих CERT-UA, зросла з 1 350 у 2021 році до 5 927 у 2025 році, тобто в 4,4 раза, за одночасного скорочення частки критичних і високих інцидентів з 47,8 % у 2022 році до 0,2 % (з урахуванням змін методики класифікації), що свідчить про зростання спроможності кіберзахисту і перехід зловмисників до масових атак. Збитки від шахрайства з платіжними картками за 2022–2025 роки зросли в 2,9 раза, до близько 1,4 млрд грн, а частка соціальної інженерії в них досягла 90 %. Вартість витоку даних у фінансовій галузі у світі стабільно на 25–37 % перевищує середній рівень. Особливістю українського контексту є поєднання кіберзагроз з фізичною деструкцією інфраструктури та хронічним стресом персоналу.

5. Порівняльна оцінка кіберзахищеності за сімома критеріями засвідчила глибоку диференціацію фінансових установ: інтегральний індекс становить 0,89 для системно важливих банків, 0,51 для середніх банків і 0,24 для малих банків і небанківських установ, тобто розрив сягає 3,7 раза. Найбільше відставання спостерігається за критеріями моніторингу і реагування, тестування на

проникнення та сертифікації. Оскільки стійкість системи визначається найслабшою ланкою, вразливості менших учасників створюють системний ризик для всього сектору.

6. Обґрунтовано комплекс напрямів удосконалення кібербезпеки фінансової системи України. Запропоновано єдину класифікацію кіберінцидентів для всіх учасників фінансового ринку з чотирма рівнями серйозності та строками первинного повідомлення про критичні інциденти не пізніше 4 годин після класифікації і 24 годин після виявлення, проміжного звіту протягом 72 годин і остаточного звіту протягом місяця, а також модель розподілу функцій, за якою Національний банк стає єдиним органом кіберстійкості фінансового сектору. Розроблено зміни до шести нормативно-правових актів (додаток А), визначено пріоритетні технологічні та організаційні заходи для установ різних категорій. Як перспективну ініціативу поствоєнного відновлення запропоновано утворити Центр кіберстійкості фінансового сектору на базі Центру кіберзахисту НБУ, що усуне дублювання функцій і матиме кадровий склад 210 осіб, частину з яких становитимуть працівники наявних підрозділів НБУ, а мінімальну нормативну потребу фінансових установ у фахівцях з кібербезпеки обґрунтовано на рівні 1 234 осіб; разом це 1 444 робочі місця у секторі, реалізація яких передбачена дорожньою картою з трьох етапів.

Отримані результати доводять, що кібербезпека фінансової системи України не може бути ефективною за умови ізольованих зусиль окремих установ і потребує системного підходу, який поєднує законодавче врегулювання, інституційну реформу, технологічну модернізацію, розвиток людського капіталу та міжнародну інтеграцію. Подальші дослідження доцільно зосередити на механізмах імплементації DORA в українське законодавство, моделях економічної оцінки ефективності заходів кіберзахисту та сценаріях еволюції загроз в умовах розвитку квантових обчислень і штучного інтелекту.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Безготівкові розрахунки у 2024 році суттєво переважали серед операцій з картками. Дебет-Кредит. 2025. 4 берез. URL: https://news.dtkt.ua/finance/bank-system/96562-bezgotivkovi-rozraxunki-u-2024-roci-suttjevo-perevazali-sered-operacii-z-kartkami.

2. Богом'я В., Галунько В. Правове регулювання кібербезпеки в контексті захисту критичної інфраструктури. Information Technology: Computer Science, Software Engineering and Cyber Security. 2024. № 4. С. 35–42. DOI: https://doi.org/10.32782/it/2024-4-5.

3. Боднар О. А. Модернізація фінансово-економічної безпеки підприємства в умовах цифровізації. Наукові перспективи. 2023. № 2(32). С. 234–246. DOI: https://doi.org/10.52058/2708-7530-2023-2(32)-234-246.

4. Ваврик Ю., Опірський І. Штучний інтелект: кібербезпека нового покоління. Безпека інформації. 2024. Т. 30, № 2. С. 244–255. DOI: https://doi.org/10.18372/2225-5036.30.19235.

5. Держспецзв'язку визначила порядок обміну інформацією про кіберінциденти та критерії визначення значного кіберінциденту. Урядовий портал. 2026. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-vyznachyla-poriadok-obminu-informatsiieiu-pro-kiberintsydenty-ta-kryterii-vyznachennia-znachnoho-kiberintsydentu.

6. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : постанова Кабінету Міністрів України від 23.12.2020 № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-п.

7. Деякі питання об'єктів критичної інформаційної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п.

8. Деякі питання об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п.

9. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-п.

10. Дрига Д. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського Союзу. Вісник Хмельницького національного університету. Економічні науки. 2024. Т. 334, № 5. С. 46–51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7.

11. «єПідтримка»: у грудні-2021 зафіксовано рекордний приріст платіжних карток. Мінфін. 2022. 17 лют. URL: https://minfin.com.ua/ua/2022/02/17/81183088/.

12. Єрмак В. О. Банківська система України у період повоєнного відновлення: виклики та шляхи розвитку. Державне будівництво. 2023. № 2(34). С. 214–223. DOI: https://doi.org/10.26565/1992-2337-2023-2-18.

13. Збитки від шахрайських операцій з картками у 2024р зросли на 37% за скорочення їх кількості на 1% – НБУ. Інтерфакс-Україна. 2025. 12 трав. URL: https://interfax.com.ua/news/economic/1071169.html .

14. Звіт про фінансову стабільність. Червень 2025 року. Київ : Національний банк України, 2025. URL: https://bank.gov.ua/admin_uploads/article/FSR_2025-H1.pdf

15. Інформація щодо кібератак 15 лютого 2022 року : повідомлення CERT-UA. Дебет-Кредит. 2022. 21 лют. URL: https://news.dtkt.ua/finance/bank-system/75022-informaciia-shhodo-kiberatak-15-liutogo-2022-roku .

16. Кальченко В., Любчак В., Ободяк В., Пугач І. Формування компетентностей майбутніх фахівців кібербезпеки завдяки ініціативі «Студентські кібербригади». Кібербезпека: освіта, наука, техніка. 2025. Т. 3, № 31. С. 188–197. DOI: https://doi.org/10.28925/2663-4023.2025.31.1006.

17. Кіберзагрози: Україна. Аналітика за II півріччя 2025 року. Київ : Державна служба спеціального зв'язку та захисту інформації України, 2026. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=74645 .

18. Кіцель Н., Борисенко О. Розробка лабораторного практикуму з аналізу та виявлення програм-вимагачів для освітніх програм з кібербезпеки. Кібербезпека: освіта, наука, техніка. 2026. Т. 1, № 33. С. 504–511. DOI: https://doi.org/10.28925/2663-4023.2026.33.1145.

19. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр .

20. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 .

21. Курій Є., Сусукайло В., Єрофеєва А., Нестерюк М. Аналіз впливу вимог Digital Operational Resilience Act (DORA) на процес безпечної розробки програмного забезпечення. Кібербезпека: освіта, наука, техніка. 2025. Т. 4, № 28. С. 400–412. DOI: https://doi.org/10.28925/2663-4023.2025.28.852.

22. НБУ встановив вимоги щодо управління ризиком третіх сторін для банків. Дебет-Кредит. 2026. 3 лип. URL: https://news.dtkt.ua/finance/bank-system/112544-nbu-vstanoviv-vimogi-shhodo-upravlinnia-rizikom-tretix-storin-dlia-bankiv .

23. НБУ затвердив Положення про відкритий банкінг в Україні. Дебет-Кредит. 2025. 28 лип. URL: https://news.dtkt.ua/finance/bank-system/101521-nbu-zatverdiv-polozennia-pro-vidkritii-banking-v-ukrayini .

24. НБУ назвав суму збитків від шахрайства з платіжними картками за останній рік. Finance.ua. 2023. 4 трав. URL: https://news.finance.ua/ua/nbu-nazvav-sumu-zbytkiv-vid-shahraystva-z-platizhnymy-kartkamy-za-ostanniy-rik .

25. НБУ оприлюднив список системно важливих банків на 2026 рік. Finance.ua. 2026. 17 черв. URL: https://news.finance.ua/ua/nbu-oprylyudnyv-spysok-systemno-vazhlyvyh-bankiv-na-2026-rik .

26. Небанківський фінринок за місяць втратив 10 учасників – НБУ. Mind.ua. 2026. URL: https://mind.ua/news/20309759-nebankivskij-finrinok-za-misyac-vtrativ-10-uchasnikiv-nbu .

27. Огляд банківського сектору. Лютий 2026 року. Київ : Національний банк України, 2026. URL: https://bank.gov.ua/admin_uploads/article/Banking_Sector_Review_2026-02.pdf .

28. Огляд національної системи кібербезпеки України 2025 : аналіт. дослідж. / Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Київ, 2026. URL: https://rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf .

29. Олексійчук Ю. Емпіричне дослідження продуктивності постквантових криптографічних алгоритмів ML-KEM, ML-DSA та SLH-DSA у різних версіях JDK. Кібербезпека: освіта, наука, техніка. 2026. Т. 1, № 33. С. 165–176. DOI: https://doi.org/10.28925/2663-4023.2026.33.1210.

30. Платіжне шахрайство під час великої війни: кількість випадків та суми збитків. Слово і діло. 2026. 6 трав. URL: https://www.slovoidilo.ua/2026/05/06/infografika/finansy/platizhne-shaxrajstvo-velykoyi-vijny-kilkist-vypadkiv-ta-sumy-zbytkiv .

31. Приходько Б. Кіберризики фінансового сектору в умовах цифрової трансформації. Вісник Хмельницького національного університету. Економічні науки. 2025. Т. 340, № 2. С. 125–139. DOI: https://doi.org/10.31891/2307-5740-2025-340-20.

32. Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III. URL: https://zakon.rada.gov.ua/laws/show/2121-14 .

33. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022. URL: https://www.president.gov.ua/documents/642022-41397 .

34. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20 .

35. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20 .

36. Про внесення змін до деяких законодавчих актів України щодо удосконалення функцій із державного регулювання ринків фінансових послуг : Закон України від 12.09.2019 № 79-IX. URL: https://zakon.rada.gov.ua/laws/show/79-20 .

37. Про внесення змін до деяких нормативно-правових актів Національного банку України : постанова Правління Національного банку України від 30.03.2023 № 40. URL: https://bank.gov.ua/admin_uploads/law/30032023_40.pdf .

38. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20 .

39. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19 .

40. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п .

41. Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту : постанова Правління Національного банку України від 25.02.2025 № 24. URL: https://bank.gov.ua/admin_uploads/law/25022025_24.pdf .

42. Про затвердження Змін до Положення про застосування Національним банком України заходів впливу : постанова Правління Національного банку України від 04.08.2022 № 169. URL: https://bank.gov.ua/admin_uploads/law/04082022_169.pdf .

43. Про затвердження Положення про вимоги до системи управління ризиками надавача нефінансових платіжних послуг та внесення зміни до Положення про вимоги до системи управління надавача фінансових платіжних послуг : постанова Правління Національного банку України від 02.07.2025 № 73. URL: https://bank.gov.ua/admin_uploads/law/02072025_73.pdf .

44. Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку : постанова Правління Національного банку України від 19.05.2021 № 43. URL: https://bank.gov.ua/admin_uploads/law/19052021_43.pdf .

45. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг : постанова Правління Національного банку України від 16.01.2021 № 4. URL: https://bank.gov.ua/admin_uploads/law/16012021_4.pdf .

46. Про затвердження Положення про організаційно-технічну модель кіберзахисту : постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п .

47. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : постанова Правління Національного банку України від 28.09.2017 № 95. URL: https://bank.gov.ua/admin_uploads/law/28092017_95.pdf .

48. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг : постанова Правління Національного банку України від 09.12.2025 № 143. URL: https://bank.gov.ua/admin_uploads/law/09122025_143.pdf .

49. 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 12.08.2022 № 178. URL: https://bank.gov.ua/admin_uploads/law/12082022_178.pdf .

50. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : постанова Правління Національного банку України від 11.06.2018 № 64. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18 .

51. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр .

52. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 .

53. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 .

54. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 .

55. Про критичну інфраструктуру фінансового сектору : постанова Правління Національного банку України від 27.06.2025 № 69. URL: https://bank.gov.ua/admin_uploads/law/27062025_69.pdf .

56. Про Національний банк України : Закон України від 20.05.1999 № 679-XIV. URL: https://zakon.rada.gov.ua/laws/show/679-14 .

57. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://www.president.gov.ua/documents/2422016-20141 .

58. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 .

59. Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20 .

60. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19 .

61. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ

Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 .

62. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 .

63. Про фінансові послуги та фінансові компанії : Закон України від 14.12.2021 № 1953-IX. URL: https://zakon.rada.gov.ua/laws/show/1953-20 .

64. Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20 .

65. Прокопович-Ткаченко Д., Бакута А., Звєрєв В., Козаченко І., Черкаський О. Моделювання фішингових сценаріїв у кіберпросторі України: аналітичний підхід з використанням Grafana-дошки. Кібербезпека: освіта, наука, техніка. 2025. Т. 1, № 29. С. 331–347. DOI: https://doi.org/10.28925/2663-4023.2025.29.881.

66. Російські кібер-операції. Аналітика за І півріччя 2025. Київ : Державна служба спеціального зв'язку та захисту інформації України, 2025. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=71278 .

67. Російські кібероперації. Аналітика за ІІ півріччя 2024 року. Київ : Державна служба спеціального зв'язку та захисту інформації України, 2025. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=68752 .

68. Роскладка А., Кузін О. Моделювання відмовостійкої конфігурації інформаційного середовища банку. Кібербезпека: освіта, наука, техніка. 2026. Т. 3, № 35. С. 304–311. DOI: https://doi.org/10.28925/2663-4023.2026.35.1395

69. Савлук С., Пасічний М. Цифрова валюта як новий інструмент монетарної політики. Фінанси України. 2026. № 3. С. 56–73. DOI: https://doi.org/10.33763/finukr2026.03.056.

70. Свічкар Н. М., Андреєва І. Г., Андреєва К. О. Потенційний вплив е-гривні на платіжну систему, фінансову стабільність та клієнтський досвід.

Цифрова економіка та економічна безпека. 2025. № 6(21). С. 211–218. DOI: https://doi.org/10.32782/dees.21-33.

71. Сергєєва О. С. Фінансова безпека банків на ринку платіжних карток України. Науковий вісник Одеського національного економічного університету. 2023. № 9(310). С. 90–97. DOI: https://doi.org/10.32680/2409-9260-2023-9-310-90-97.

72. Сіренко Н. М., Мікуляк К. А. Імперативи розвитку банківської системи України в умовах цифровізації та ринкових трансформацій. Modern Economics. 2022. № 34. С. 90–96. DOI: https://doi.org/10.31521/modecon.V34(2022)-13.

73. Стратегія розвитку фінансового сектору України / Національний банк України, Міністерство фінансів України, Національна комісія з цінних паперів та фондового ринку, Фонд гарантування вкладів фізичних осіб, Міністерство економіки, довкілля та сільського господарства України. Оновл. ред. Київ, 2025. URL: https://mof.gov.ua/storage/files/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F_%D1%84%D1%96%D0%BD%D1%81%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D1%83_%D0%BF%D1%83%D0%B1%D0%BB%D1%96%D1%87%D0%BD%D0%B0_%D1%83%D0%BA%D1%80.pdf .

74. Студзінський Р. В. Роль державно-приватного партнерства у забезпеченні кібербезпеки в Україні. Інвестиції: практика та досвід. 2025. № 22. С. 355–358. DOI: https://doi.org/10.32702/2306-6814.2025.22.355.

75. Сума збитків від шахрайських дій з платіжними картками зросла на чверть за рік – НБУ. Економічна правда. 2026. URL: https://epravda.com.ua/finances/zbitki-vid-shahraystva-z-platizhnimi-kartkami-v-ukrajini-zrosli-na-24-u-2025-820539/ .

76. Тищенко С. І., Пархоменко О. Ю., Дармосюк В. М. Моделювання та аналіз ризиків кібератак на фінансові установи з використанням методів математичної статистики та Python. Modern Economics. 2024. № 48. С. 130–136. DOI: https://doi.org/10.31521/modecon.V48(2024)-16.

77. Тищенко С. І., Пархоменко О. Ю., Ємельянов С. І., Богатєнкова О. Є., Хилько І. І. Застосування методів глибокого навчання для виявлення та класифікації кіберзагроз у фінансових мережах на базі набору даних NSL-KDD. Modern Economics. 2025. № 52. С. 203–209. DOI: https://doi.org/10.31521/modecon.V52(2025)-28.

78. Торік кількість шахрайських дій з картками зросла на чверть – Нацбанк. Укрінформ. 2024. 6 квіт. URL: https://www.ukrinform.ua/rubric-economy/3849295-torik-kilkist-sahrajskih-dij-z-kartkami-zrosla-na-cvert-nacbank.html .

79. У 2025 році кількість ворожих кібератак зросла на 37%: кого атакують найчастіше. Dev.ua. 2026. 8 січ. URL: https://dev.ua/news/u-2025-rotsi-kilkist-kiberatak-zrosla-na-37-1767858414 .

80. У першому півріччі 2026 року кількість кіберінцидентів в Україні зросла на 8%: які сектори атакують найчастіше. Dev.ua. 2026. 30 верес. URL: https://dev.ua/news/u-pershomu-pivrichchi-2026-roku-kilkist-kiberintsydentiv-v-ukraini-zrosla-na-8-1790769498 .

81. Українці у 2025 році майже повністю перейшли на безготівкові розрахунки – НБУ. Mind.ua. 2026. 16 лют. URL: https://mind.ua/news/20301081-ukrayinci-u-2025-roci-majzhe-povnistyu-perejshli-na-bezgotivkovi-rozrahunki-nbu .

82. Усік П., Смірнова Т., Буравченко К., Смірнов О., Улічев О., Смірнов С. Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2025. Т. 1, № 29. С. 704–716. DOI: https://doi.org/10.28925/2663-4023.2025.29.930.

83. Чайковський Я. І., Чайковський Є. Я. Відкритий банкінг і фінтех-екосистема як чинники трансформації банківського бізнесу в цифровій економіці. Наукові записки Національного університету «Острозька академія». Серія «Економіка». 2026. № 41(69). С. 186–196. DOI: https://doi.org/10.25264/2311-5149-2026-41(69)-186-196.

84. Шлапак А. Наглядовий потенціал фінансових установ у протидії кіберзлочинам та інформаційним асиметріям в умовах зростання ролі FinTech і Big Techs на цифровізованих ринках капіталу. Вісник Хмельницького

національного університету. Економічні науки. 2022. Т. 304, № 2(2). С. 273–280. DOI: https://doi.org/10.31891/2307-5740-2022-304-2(2)-43.

85. Шолойко А. С. Актуалізація кіберстрахування в умовах цифровізації економіки. Науковий вісник Одеського національного економічного університету. 2023. № 9(310). С. 98–106. DOI: https://doi.org/10.32680/2409-9260-2023-9-310-98-106.

86. Штерма Т. В., Гончарук Я. М., Урбанович А. В., Бура М. М. Перспективи інтеграції фінансового сектора України у світовий ринок після війни. Бізнес Інформ. 2025. № 2. С. 392–400. DOI: https://doi.org/10.32983/2222-4459-2025-2-392-400.

87. Як змінились обсяги безготівкових розрахунків у другий рік війни? Дебет-Кредит. 2024. 7 берез. URL: https://news.dtkt.ua/finance/bank-system/89307-iak-zminilis-obsiagi-bezgotivkovix-rozraxunkiv-u-drugii-rik-viini .

88. The 3rd Annual Billington International Cybersecurity Summit: keynote address by CE / Cyber Security Agency of Singapore. URL: https://www.csa.gov.sg/news-events/speeches/the-3rd-annual-billington-international-cybersecurity-summit-keynote-address-by-ce/ .

89. About us / NATO Cooperative Cyber Defence Centre of Excellence. Tallinn : CCDCOE. URL: https://ccdcoe.org/about-us/ .

90. Agosto A., Giudici P. Cyber Risk Contagion. Risks. 2023. Vol. 11, No. 9. Art. 165. DOI: https://doi.org/10.3390/risks11090165.

91. AL Hawatmah Z. M., Bader A., Zoubi M. Quantitative modeling of cyber risks in Gulf banks and FinTech platforms. Banks and Bank Systems. 2026. Vol. 21, No. 2. P. 275–288. DOI: https://doi.org/10.21511/bbs.21(2).2026.19.

92. Ali A., Abd Razak S., Othman S. H., et al. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences. 2022. Vol. 12, No. 19. Art. 9637. 24 p. DOI: https://doi.org/10.3390/app12199637.

93. Ali A., Shah M. What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector. Information. 2024. Vol. 15, No. 12. Art. 760. 17 p. DOI: https://doi.org/10.3390/info15120760.

94. Arzhevitin S., Bortnikov G., Bublyk Ye., Lyubich O. Impact of martial state on the performance of the Ukrainian banking sector. Financial and Credit Activity: Problems of Theory and Practice. 2023. Vol. 1, No. 48. P. 23–41. DOI: https://doi.org/10.55643/fcaptp.1.48.2023.3966.

95. Bank of England launches new framework to test for cyber vulnerabilities : news release, 10 June 2014 / Bank of England. URL: https://www.bankofengland.co.uk/-/media/boe/files/news/2014/june/boe-launches-new-framework-to-test-for-cyber-vulnerabilities .

96. Barbosa R., Chen B., Khadarina O., Okuda T., Rangachary R., Shao E., Suntheim F., Tsuruga T. Cyber Risk: A Growing Concern for Macrofinancial Stability. Global Financial Stability Report. Washington, DC : International Monetary Fund, 2024. April. Chapter 3. URL: https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf .

97. Biliavska Yu., Biliavskyi V., Shestak Ya., Dyeyeva N., Kolesnyk M., Tryvailo A. Monitoring of cyber risks in the financial sector of the economy. Financial and Credit Activity: Problems of Theory and Practice. 2025. Vol. 3, No. 62. P. 355–369. DOI: https://doi.org/10.55643/fcaptp.3.62.2025.4702.

98. Burkovska A. Strategic Prospects for Managing Computer Networks and Information Systems in the Context of Digital Transformation and Global Cyberspace Integration. Modern Economics. 2025. No. 52. P. 7–11. DOI: https://doi.org/10.31521/modecon.V52(2025)-01.

99. Buttigieg C. P., Brunelli Zimmermann B. The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. ERA Forum. 2024. Vol. 25, No. 1. P. 11–28. DOI: https://doi.org/10.1007/s12027-024-00793-w.

100. Chanon R. D., Habahbeh L., Klumpes P. J. M., Mann S. Operational resilience in the UK financial sector: practical guidance. British Actuarial Journal. 2025. Vol. 30. Art. e25. DOI: https://doi.org/10.1017/S1357321725100202.

101. Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the

Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats. Official Journal of the European Union. 2025. L 2025/301. URL: https://eur-lex.europa.eu/eli/reg_del/2025/301/oj .

102. Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. Official Journal of the European Union. 2024. L 2024/1101. URL: https://eur-lex.europa.eu/eli/reco/2024/1101/oj .

103. Cost of a Data Breach Report 2021 / IBM Security, Ponemon Institute. Armonk, NY : IBM, 2021. URL: https://www.ibm.com/reports/data-breach .

104. Cost of a Data Breach Report 2022 / IBM Security, Ponemon Institute. Armonk, NY : IBM, 2022. URL: https://www.ibm.com/downloads/cas/3R8N1DZJ .

105. Cost of a Data Breach Report 2023 / IBM Security, Ponemon Institute. Armonk, NY : IBM, 2023. URL: https://www.ibm.com/downloads/cas/E3G5JMBP .

106. Cost of a Data Breach Report 2024 / IBM, Ponemon Institute. Armonk, NY : IBM, 2024. URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec .

107. Cost of a Data Breach Report 2025: The AI Oversight Gap / IBM, Ponemon Institute. Armonk, NY : IBM, 2025. URL: https://www.ibm.com/reports/data-breach .

108. CSIRT-NBU : team directory entry / Trusted Introducer. URL: https://trusted-introducer.org/trusted-introducer/directory/teams/csirt-nbu-ua/ .

109. Cyber attacks against Estonia (2007) / NATO Cooperative Cyber Defence Centre of Excellence. Cyber Law Toolkit. URL: https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007) .

110. Cyber Lexicon : Updated in 2023 / Financial Stability Board. Basel : FSB, 2023. URL: https://www.fsb.org/uploads/P130423-3.pdf .

111. Cybersecurity Requirements for Financial Services Companies : 23 NYCRR Part 500 (as amended effective November 1, 2023) / New York State

Department of Financial Services. URL: https://www.law.cornell.edu/regulations/new-york/23-NYCRR-500.17 .

112. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Official Journal of the European Union. 2015. L 337. P. 35–127. URL: https://eur-lex.europa.eu/eli/dir/2015/2366/oj .

113. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. 2016. L 194. P. 1–30. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj .

114. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. P. 80–152. URL: http://data.europa.eu/eli/dir/2022/2555/oj .

115. ECB concludes cyber resilience stress test : press release, 26 July 2024 / European Central Bank. URL: https://www.banque-france.fr/system/files/2024-07/ECB-concludes-cyber-resilience-stress-test.pdf .

116. ENISA Threat Landscape: Finance Sector. January 2023 – June 2024. Athens : European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf .

117. ENISA Threat Landscape 2025. Athens : European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf .

118. Estonian Informatics Centre became Estonian Information System Authority / Riigi Infosüsteemi Amet. 2011. URL: https://ria.ee/en/news/estonian-informatics-centre-became-estonian-information-systems-authority .

119. Format for Incident Reporting Exchange (FIRE) : Final report / Financial Stability Board. Basel : FSB, 2025. URL: https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/ .

120. Guidance on cyber resilience for financial market infrastructures / Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions. Basel : Bank for International Settlements, 2016. 32 p. URL: https://www.bis.org/cpmi/publ/d146.htm .

121. Guidelines on Cybersecurity for the Financial Sector : provisional translation / Financial Services Agency. Tokyo : FSA, 2024. URL: https://www.fsa.go.jp/common/law/cybersecurity_guideline_en.pdf .

122. Guidelines on Risk Management Practices – Technology Risk / Monetary Authority of Singapore. Singapore : MAS, 2021. URL: https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines .

123. ISC2 Cybersecurity Workforce Study 2024. Alexandria, VA : ISC2, 2024. URL: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf .

124. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. 3rd ed. Geneva : ISO, 2022. 19 p. URL: https://www.iso.org/standard/27001 .

125. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. 3rd ed. Geneva : ISO, 2022. 152 p. URL: https://www.iso.org/standard/75652.html .

126. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. 4th ed. Geneva : ISO, 2022. 62 p. URL: https://www.iso.org/standard/80585.html .

127. ISO/IEC 27032:2023. Cybersecurity – Guidelines for Internet security. 2nd ed. Geneva : ISO, 2023. 28 p. URL: https://www.iso.org/standard/76070.html .

128. Izha M., Pachomova T., Lypach O., Yakubovskyi O., Akhlamov A. Modeling the cybersecurity of the socio-economic system under martial law. Financial

and Credit Activity: Problems of Theory and Practice. 2023. Vol. 3, No. 50. P. 224–233. DOI: https://doi.org/10.55643/fcaptp.3.50.2023.4075.

129. Jančiūtė L. Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework. International Cybersecurity Law Review. 2025. Vol. 6, No. 2. P. 145–154. DOI: https://doi.org/10.1365/s43439-025-00135-7.

130. Koziuk V., Ivashuk Yu., Haida Yu. Privacy preferences and trust in central banks: heterogeneity in case of CBDC. Financial and Credit Activity: Problems of Theory and Practice. 2025. Vol. 3, No. 62. P. 11–25. DOI: https://doi.org/10.55643/fcaptp.3.62.2025.4734.

131. Kudinova A., Maslii O., Smokvina V., Tsyhanenko K. The impact of digitalization on the financial institutions' economic security in the face of growing cyber threats. Financial and Credit Activity: Problems of Theory and Practice. 2025. Vol. 4, No. 63. P. 466–483. DOI: https://doi.org/10.55643/fcaptp.4.63.2025.4790.

132. Kurowski Ł., Smaga P. Does bank's financial standing influence the risk of a cyberattack? Journal of Cybersecurity. 2026. Vol. 12, No. 1. Art. tyag033. DOI: https://doi.org/10.1093/cybsec/tyag033.

133. Melnyk L. V., Trusova N. V. State Regulatory Policy for the Development of the Payment Segment Fintech Sector. Modern Economics. 2026. No. 57. P. 143–150. DOI: https://doi.org/10.31521/modecon.V57(2026)-19.

134. Module-Lattice-Based Key-Encapsulation Mechanism Standard : Federal Information Processing Standards Publication 203. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 47 p. DOI: https://doi.org/10.6028/NIST.FIPS.203.

135. Mott G., Turner S., Nurse J. R. C., Pattnaik N., MacColl J., Huesch P., Sullivan J. 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. Journal of Cybersecurity. 2024. Vol. 10, No. 1. Art. tyae013. DOI: https://doi.org/10.1093/cybsec/tyae013.

136. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 32 p. (NIST CSWP 29). DOI: https://doi.org/10.6028/NIST.CSWP.29.

137. Notice FSM-N07 : Notice on Technology Risk Management / Monetary Authority of Singapore. Singapore : MAS, 2024. URL: https://www.mas.gov.sg/-/media/mas-media-library/regulation/notices/trpd/notice-fsm-n07/mas-notice-fsm-n07.pdf .

138. Ojehomon O. G., Cichorska J., Michnik J. Cyber Risk Management of API-Enabled Financial Crime in Open Banking Services. Entropy. 2026. Vol. 28, No. 2. Art. 163. DOI: https://doi.org/10.3390/e28020163.

139. Overview of cybersecurity : Recommendation ITU-T X.1205. Geneva : International Telecommunication Union, 2008. URL: https://www.itu.int/rec/T-REC-X.1205-200804-I/en .

140. Payment Card Industry Data Security Standard : Requirements and Testing Procedures. Version 4.0.1. Wakefield : PCI Security Standards Council, 2024. URL: https://www.pcisecuritystandards.org/document_library/ .

141. Principles for operational resilience / Basel Committee on Banking Supervision. Basel : Bank for International Settlements, 2021. 12 p. URL: https://www.bis.org/bcbs/publ/d516.htm .

142. Proper Conduct of Banking Business Directive No. 361 «Cyber Defense Management» / Bank of Israel, Supervisor of Banks. Jerusalem, 2021. URL: https://boi.org.il/media/422h2aed/361_et.pdf .

143. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj .

144. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014,

(EU) No 909/2014 and (EU) 2016/1011. Official Journal of the European Union. 2022. L 333. P. 1–79. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj .

145. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Official Journal of the European Union. 2023. L 150. P. 40–205. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj .

146. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj .

147. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg, MD : National Institute of Standards and Technology, 2020. 59 p. DOI: https://doi.org/10.6028/NIST.SP.800-207.

148. Russia's Cyber Tactics: Lessons Learned 2022 / State Service of Special Communications and Information Protection of Ukraine. Kyiv : SSSCIP, 2023. URL: https://nsarchive.gwu.edu/sites/default/files/documents/s9zfme-rssdn/2023-03-08-SSSCIP-Russia%E2%80%99s-Cyber-Tactics-Lessons-Learned-2022-via-website.pdf .

149. Skeoch H. R. K., Ioannidis C. The barriers to sustainable risk transfer in the cyber-insurance market. Journal of Cybersecurity. 2024. Vol. 10, No. 1. Art. tyae003. DOI: https://doi.org/10.1093/cybsec/tyae003.

150. Sunset of the FFIEC Cybersecurity Assessment Tool : Financial Institution Letter FIL-61-2024 / Federal Deposit Insurance Corporation. 2024. URL: https://www.fdic.gov/news/financial-institution-letters/2024/sunset-ffiec-cybersecurity-assessment-tool .

151. Swift Customer Security Programme : Customer Security Controls Framework v2026. La Hulpe : Swift, 2025. URL: https://www.swift.com/myswift/customer-security-programme-csp .

152. TIBER-EU Framework updated to align with DORA / European Central Bank. 2025. 11 February. URL: https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html .

153. Yoon J., Kim Y. Offline Payment of Central Bank Digital Currency Based on a Trusted Platform Module. Journal of Cybersecurity and Privacy. 2025. Vol. 5, No. 2. Art. 14. DOI: https://doi.org/10.3390/jcp5020014.

154. Zarutska O., Ponomarova O., Pavlov R., Pavlova T., Levkovich O. Changes in Ukrainian banks' business models in times of military crisis. Financial and Credit Activity: Problems of Theory and Practice. 2022. Vol. 6, No. 47. P. 8–18. DOI: https://doi.org/10.55643/fcaptp.6.47.2022.3923.

# ДЕКЛАРАЦІЯ

## про використання / невикористання штучного інтелекту

Я, Зарембо Микита Олегович

(прізвище, ім'я, по батькові)

здобувач(ка) освіти / науковий(а) працівник(ця) другого (магістерського) рівня вищої освіти заочної форми здобуття освіти

(рівень освіти, науковий ступінь, посада)

повідомляю, що під час підготовки:

**Назва та вид роботи:**

**Кваліфікаційної роботи на тему: «Кібербезпека в розвитку фінансової системи України»**

☐ **1. Штучний інтелект не використовувався**

Підтверджую, що під час підготовки зазначеної наукової роботи інструменти штучного інтелекту не застосовувалися.

☑ **2. Штучний інтелект використовувався**

**Інформація про використаний інструмент штучного інтелекту:**

| № з/п | Мета використання штучного інтелекту | Назва ШІ | Назва чату | Посилання на чат |
|---|---|---|---|---|
| 1 | Переклад іноземних джерел | Claude | 12 | https://claude.ai/share/35568f83-9d08-4185-9de6-346c5c726c7e |

*(Допустимі цілі використання штучного інтелекту з дотриманням вимог академічної доброчесності: мовне та стилістичне редагування авторського тексту; орфографічна і граматична перевірка; переклад без зміни змісту; структурування вже наявного матеріалу; уточнення термінології; допомога у формуванні плану або логіки викладу; генерація прикладів загального характеру, що не містять наукової новизни; технічна допомога з оформлення таблиць, схем і переліків.)*

Підтверджую, що під час підготовки наукової роботи застосовувалися інструменти штучного інтелекту **виключно як допоміжні засоби**, без передачі їм функцій авторства, наукового аналізу, інтерпретації результатів чи формування висновків.

## ПІДТВЕРДЖЕННЯ

Я усвідомлюю, що:

- відповідальність за наукову новизну, достовірність даних, висновки та інтерпретацію результатів **повністю несу особисто**;
- використання штучного інтелекту не звільняє від дотримання принципів академічної доброчесності;
- приховування або викривлення інформації про використання ШІ може розглядатися як порушення академічної етики.

Дата: «05» листопада 2026р. Підпис: _____

# ДОДАТКИ

# ДОДАТОК А

## Пропозиції щодо внесення змін до нормативно-правових актів у сфері кібербезпеки фінансового сектору України

У додатку наведено порівняльні таблиці чинних і запропонованих редакцій норм шести нормативно-правових актів (табл. А.1–А.6), необхідність зміни яких обґрунтовано в 1.2 і 3.1. Для кожного акта подано чинну редакцію відповідного структурного елемента, запропоновану редакцію та пояснення.

### 1. Закон України «Про основні засади забезпечення кібербезпеки України»

Таблиця А.1 **Пропозиції щодо змін до пункту 6 частини другої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»**

| Чинна редакція | Запропонована редакція |
|---|---|
| «6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, … забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об’єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, …» | «6) Національний банк України є органом кіберстійкості фінансового сектору, який визначає порядок, вимоги та заходи із забезпечення кіберзахисту, інформаційної безпеки та цифрової операційної стійкості осіб, зазначених у цьому пункті, здійснює контроль за їх виконанням, у тому числі щодо об’єктів критичної інформаційної інфраструктури фінансового сектору; утворює Центр кіберстійкості фінансового сектору, який виконує функції галузевої команди реагування на кіберінциденти, галузевого центру моніторингу та обміну інформацією про кіберзагрози; приймає від зазначених осіб повідомлення про кіберінциденти та не пізніше однієї години після отримання передає інформацію про значні і критичні кіберінциденти урядовій команді реагування на комп’ютерні надзвичайні події України CERT-UA; організовує тестування на проникнення на основі розвідданих про загрози; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об’єктах критичної інфраструктури фінансового сектору.» |

Джерело: чинну редакцію наведено за [58, ст. 8] у редакції, що діяла на 05.06.2024, запропоновану редакцію розроблено автором.

**Пояснення.** Зміна закріплює за НБУ статус єдиного органу кіберстійкості фінансового сектору і єдиного адресата повідомлень про кіберінциденти, у тому числі для фінансових установ, що є операторами об’єктів критичної інформаційної інфраструктури. Це усуває паралельне звітування за різними критеріями до кількох органів (див. табл. 3.2) і зберігає інформованість CERT-

UA через обов’язкову передачу даних про значні інциденти. Поняття цифрової операційної стійкості запозичене з Регламенту DORA, що сприятиме подальшій гармонізації з правом ЄС [144, ст. 3].

**2. Закон України «Про банки і банківську діяльність»**

Таблиця А.2 **Пропозиції щодо змін до статті 44 Закону України «Про банки і банківську діяльність»**

| Чинна редакція | Запропонована редакція |
|---|---|
| «1. Банк створює комплексну, адекватну та ефективну систему внутрішнього контролю, що включає систему управління ризиками та внутрішній аудит, згідно з вимогами, установленими Національним банком України. 2. Система внутрішнього контролю банку має забезпечувати: 1) досягнення банком довгострокових цілей, зокрема прибутковості його діяльності; 2) здійснення банківської діяльності з урахуванням ризиків; … 5) чіткий розподіл обов’язків, функцій та повноважень між радою банку та правлінням банку, а також між підрозділами банку; …» | Частину другу доповнити пунктом такого змісту: «ефективне управління ризиками інформаційно-комунікаційних технологій та інформаційної безпеки, кіберстійкість банку і безперервність надання банківських послуг у разі кіберінцидентів та інших руйнівних подій». Доповнити статтю частиною такого змісту: «Рада банку затверджує стратегію кібербезпеки банку, не рідше одного разу на рік розглядає звіт про стан кіберзахисту та забезпечує достатність ресурсів для управління ризиками інформаційно-комунікаційних технологій.» |

Джерело: чинну редакцію наведено за [32, ст. 44], запропоновану редакцію розроблено автором.

**Пояснення.** Чинна редакція ст. 44 не згадує інформаційну безпеку, кіберзахист чи ризики ІКТ, і відповідні вимоги до банків існують лише на рівні нормативно-правових актів НБУ [50; 37]. Закріплення їх у законі підвищує правовий статус вимог, а покладення на раду банку обов’язку затверджувати стратегію кібербезпеки відповідає підходам NIS2 і DORA до відповідальності органів управління [114, ст. 20; 144, ст. 5].

## 3. Закон України «Про захист персональних даних»

Таблиця А.3 **Пропозиції щодо доповнення Закону України «Про захист персональних даних» статтею 24¹**

| Чинна редакція | Запропонована редакція |
|---|---|
| «Стаття 24. Забезпечення захисту персональних даних у базах персональних даних. 1. Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. …» Обов'язок повідомляти про порушення безпеки персональних даних відсутній. | «Стаття 24¹. Повідомлення про порушення безпеки персональних даних. 1. У разі порушення безпеки персональних даних, що може створити ризик для прав і свобод суб'єктів персональних даних, володілець персональних даних без невиправданої затримки, але не пізніше 72 годин після того, як йому стало відомо про порушення, повідомляє про нього Уповноваженого Верховної Ради України з прав людини. 2. Якщо порушення може створити високий ризик для прав і свобод фізичних осіб, володілець без невиправданої затримки повідомляє про нього суб'єктів персональних даних і рекомендує заходи для зменшення можливих негативних наслідків. 3. Банки та інші особи, державне регулювання діяльності яких здійснює Національний банк України, одночасно інформують Національний банк України в порядку, встановленому для повідомлення про кіберінциденти.» |

Джерело: чинну редакцію наведено за [52, ст. 24], запропоновану редакцію розроблено автором з використанням [143, ст. 33, 34].

**Пояснення.** Відсутність обов'язку повідомляти про витоки персональних даних позбавляє клієнтів фінансових установ можливості вчасно заблокувати картки, змінити паролі та захиститися від соціальної інженерії, частка якої в збитках від карткового шахрайства у 2025 році сягнула 90 % (див. табл. 2.5). Запропонована норма відтворює підхід Загального регламенту ЄС про захист даних і узгоджується зі строками звітування про кіберінциденти.

## 4. Закон України «Про платіжні послуги»

Таблиця А.4 **Пропозиції щодо змін до статті 66 Закону України «Про платіжні послуги»**

| Чинна редакція | Запропонована редакція |
|---|---|
| «2. Надавачі платіжних послуг зобов'язані повідомляти Національний банк України у встановленому ним порядку про істотні операційні інциденти, кіберінциденти та інциденти безпеки, пов'язані з наданням ними платіжних послуг (виконанням платіжних операцій).» Частина четверта відсутня. | «2. Надавачі платіжних послуг зобов'язані повідомляти Національний банк України про істотні операційні інциденти, кіберінциденти та інциденти безпеки, пов'язані з наданням ними платіжних послуг (виконанням платіжних операцій): первинним повідомленням про критичні інциденти не пізніше 4 годин з моменту класифікації і не пізніше 24 годин з моменту виявлення, про інші істотні інциденти не пізніше 24 годин з моменту виявлення, проміжним звітом не пізніше 72 годин з моменту первинного повідомлення та остаточним звітом не пізніше одного місяця з моменту подання проміжного звіту. Форму та порядок повідомлення встановлює Національний банк України.» «4. Надавачі платіжних послуг, визначені Національним банком України як значущі, не рідше одного разу на три роки проводять тестування на проникнення на основі розвідданих про загрози та забезпечують управління ризиками, пов'язаними із залученням постачальників послуг у сфері інформаційно-комунікаційних технологій, у порядку, встановленому Національним банком України.» |

Джерело: чинну редакцію наведено за [59, ст. 66], запропоновану редакцію розроблено автором з використанням [101, ст. 5; 144, ст. 26, 28].

**Пояснення.** Чинна норма не визначає строків повідомлення, а підзаконні акти встановлюють для учасників платіжного ринку лише вимогу повідомляти «невідкладно» [44, п. 45]. Закріплення в законі строків, ідентичних вимогам DORA, усуває неоднозначність і готує платіжний ринок до інтеграції з європейським, а тестування на основі загроз і управління ризиками постачальників ІКТ відповідають сучасним вимогам до цифрової операційної стійкості.

## 5. Кримінальний кодекс України

Таблиця А.5 **Пропозиції щодо змін до статті 361 КкУ**

| Чинна редакція | Запропонована редакція |
|---|---|
| «1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж – карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років, або обмеженням волі на той самий строк.» Спеціальної кваліфікуючої ознаки щодо фінансової інфраструктури немає. | Доповнити статтю після частини третьої новою частиною такого змісту: «Дії, передбачені частиною першою або другою цієї статті, вчинені щодо систем і мереж Національного банку України, банків, інших надавачів фінансових чи платіжних послуг або операторів платіжних систем, якщо вони призвели до порушення надання фінансових чи платіжних послуг або до витоку інформації, що становить банківську таємницю, караються позбавленням волі на строк від п’яти до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.» |

Джерело: чинну редакцію наведено за [20, ст. 361], запропоновану редакцію розроблено автором.

**Пояснення.** Атаки на фінансову інфраструктуру мають підвищену суспільну небезпеку через каскадний вплив на платіжну систему і довіру до держави (див. 2.2). Запропонована кваліфікуюча ознака диференціює відповідальність за об’єктом посягання і за санкцією займає проміжне місце між частиною третьою (від трьох до восьми років) та частиною четвертою (від восьми до дванадцяти років) статті 361 [20, ст. 361; 38].

## 6. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України

Таблиця А.6 **Пропозиції щодо змін до пункту 108 Положення, затвердженого постановою Правління НБУ від 28.09.2017 № 95**

| Чинна редакція | Запропонована редакція |
|---|---|
| «108. Банк зобов'язаний виконувати перевірку ефективності заходів щодо захисту периметра мережі банку шляхом виконання періодичних тестів на проникнення.» | «108. Банк зобов'язаний виконувати перевірку ефективності заходів щодо захисту периметра мережі та критичних інформаційних систем банку шляхом виконання тестів на проникнення не рідше одного разу на рік, а також після суттєвих змін в інформаційній інфраструктурі. Системно важливий банк додатково не рідше одного разу на три роки проходить тестування на проникнення на основі розвідданих про загрози за методикою, затвердженою Національним банком України та гармонізованою з рамковою програмою TIBER-EU, із залученням незалежних тестувальників.» |

Джерело: чинну редакцію наведено за [47, п. 108], запропоновану редакцію розроблено автором з використанням [152; 144, ст. 26].

**Пояснення.** Чинна норма не встановлює ні періодичності тестування, ні його глибини, тоді як міжнародна практика (CBEST, TIBER-EU, DORA) передбачає для значущих установ регулярне тестування, що імітує дії реальних зловмисників (див. 1.3). Запропонована редакція визначає мінімальну періодичність і запроваджує тестування на основі загроз для системно важливих банків, перелік яких щороку визначає Національний банк.