Розділ 3
Забезпечення фінансової безпеки в контексті використання інструментарію фінансового та соціального секторів

3.1. Кібербезпека як системний імператив та елемент бізнес-моделей фінансової безпеки в умовах цифрової трансформації

(Я. В. Белінська, доктор економічних наук, професор, професор кафедри економічної політики, маркетингу та бізнес аналітики;
Р. І. Дюк, здобувач третього (освітньо-наукового) рівня вищої освіти, Державний податковий університет)

В умовах стрімкої цифровізації посилюються ризики кібератак на всіх рівнях фінансової системи, що потребує підвищеної уваги до безпекових проблем. Так, за останні 20 років фінансова індустрія зазнала збитків у розмірі 12 млрд дол. від кібератак, а кількість випадків шахрайства з ідентифікацією у фінтех-секторі зросла на 73 % у період з 2021 по 2023 роки, водночас викрадені дані використовуються для покупок, кредитів або відкриття нових рахунків (рис. 3.1.1).

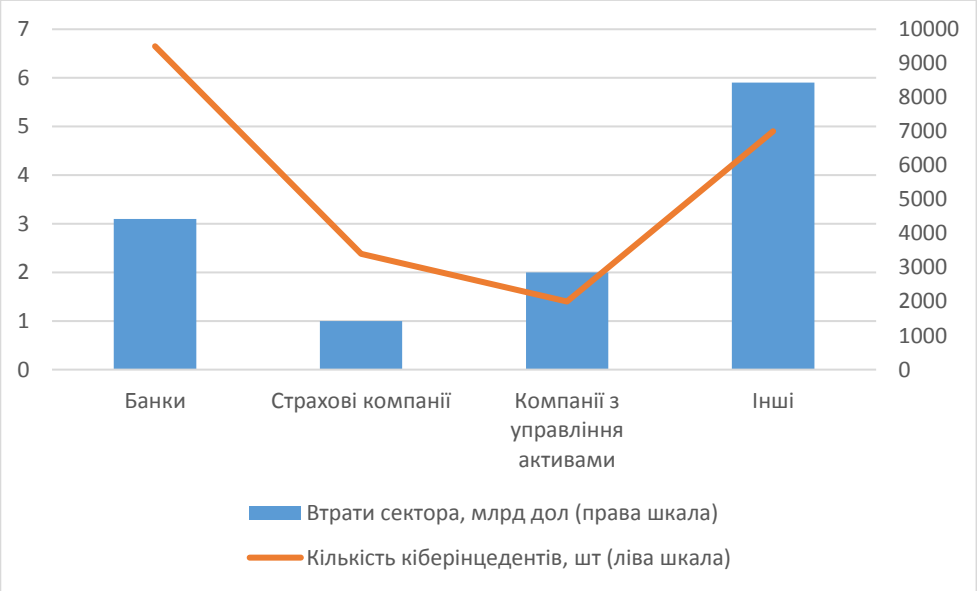

Рисунок 3.1.1 – Кількість кіберінцидентів та обсяг втрат від них фінансових установ упродовж 2004–2023 років

Джерело: [360; 361].

[360] Financial crime trends to watch out for in 2023. URL : https://fintech.global/2023/01/30/financial-crime-trends-to-watch-out-for-in-2023 (дата звернення: 07.10.2025).
[361] Traynor O. The Ultimate Guide to Financial Services Cybersecurity. November 18, 2024. URL : https://cybelangel.com/financial-services-cybersecurity-the-ultimate-guide/ (дата звернення: 07.10.2025).

Суттєво посилює негативні наслідки кібератак взаємопов'язаність фінансових систем, зокрема їхніх банківських секторів. У звіті про кіберризики Федерального резервного банку Нью-Йорка особливо наголошено на небезпеці «ефекту переливу» або «каскадного ефекту» кібератак. Фахівці банку змоделювали, як кіберінцидент може вплинути на фінансову систему США, і дійшли висновку, що атака на будь-який із п'яти провідних банків США вплине на майже 38 % національної фінансової системи та може спричинити різнопланові події – від зупинки онлайн-банкінгу до блокування торгових систем. Такі системні збої можуть призвести до мільйонних втрат, охоплюючи оцінювання можливості втрати даних і репутації надійного партнеру, підрив довіри клієнтів, регуляторні штрафи в разі витоку даних і, як наслідок, суттєві збитки, та створити серйозні незручності для клієнтів[362]. Тому дійсно надійна система кібербезпеки вимагає загальногалузевого обміну інформацією, скоординованих механізмів захисту й регуляторного нагляду, який сприяє колективній стійкості, розглядаючи кіберризик як ризик фінансової стабільності.

Відтак у сучасному глобалізованому світі кібербезпека у фінансовому секторі є не лише відповідальністю окремих фірм, а й колективним викликом для всієї фінансової екосистеми. Партнерство між фінансовими установами, центральними банками, компаніями з кібербезпеки та державними органами є життєво важливим для розробки проактивних механізмів захисту.

Для запобігання кіберризикам і мінімізації втрат від них формується система кібербезпеки, що представляє комплекс заходів, спрямованих на захист цифрових активів окремих суб'єктів, корпорацій і держав. У сучасному цифровому світі це стає фундаментальною умовою підтримки довіри клієнтів, захисту репутації постачальників послуг і забезпечення стабільності критичної інфраструктури. Кібербезпека охоплює всі аспекти, що стосуються безпеки інформації в цифровій площині функціонування фінансового сектору, починаючи від банківських платформ і закінчуючи фінансовими даними окремих установ, а саме:

інформаційна безпека, що полягає в запобіганні витокам даних і забезпеченні збереження цифрових активів;

[362] Eisenbach T. M., Kovner A., Lee M. J. Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis / Federal Reserve Bank of New York Staff Reports, no. 909. New York : Federal Reserve Bank of New York, 2020. (Revised May 2021). URL : https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf (дата звернення: 07.10.2025).

аналіз загроз (Threat intelligence): проактивний моніторинг кіберзагроз з метою упередження хакерських атак;

управління зовнішньою поверхнею атаки (EASM) – розбудова кіберстійкості публічно доступних активів та фінансових систем.

Оскільки фінансові установи й фінтех-платформи активно нарощують свої пропозиції цифрових фінансових послуг, то зростає вартість і обсяг інформації, що робить їх привабливими мішенями для кіберзлочинців. Підвищена увага до кібербезпеки фінансових установ обумовлюється також специфікою цифрового фінансового простору, де довіра стає найважливішим активом фінансової індустрії: від фінансових установ клієнти очікують не лише зручності та персоналізації послуг, але й гарантій безпеки своїх фінансових операцій і захисту особистої інформації. Без надійної системи кібербезпеки зручність і персоналізація, пропоновані цифровою трансформацією, будуть нівельовані відсутністю довіри, що призведе до відтоку клієнтів – лише одне порушення спроможне підірвати суспільну довіру та спонукати клієнтів перевести свої активи до конкурентів. Відтак в умовах тотальної цифровізації фінансові установи продають не лише послуги, а й «довіру», що перетворює безпечність на основну характеристику продукту.

На практиці кіберризики реалізуються у формі кібератаки – це широкий термін, що охоплює будь-який навмисний злочинний напад на комп'ютерні пристрої, мережі чи інфраструктуру[363]. 2020 року кібератаки посіли одне із п'яти основних місць серед глобальних загроз, і щорічно хакери розробляють нові методи кібератак, використовуючи системні інформаційні вразливості фінансових установ у злочинних цілях. Для ілюстрації масштабу проблеми наведемо такі цифри: 67 % населення Америки зазнали кібератак; 2021 року було зафіксовано понад 623 мільйони атак-вимагачів, що вдвічі перевищує показник 2020 р., середній збиток від таких програм становив 812 тис. дол. США[364], а сукупні втрати від кібератак зросли в чотири рази, досягнувши приблизно 2,5 мільярда доларів прямих втрат з 2020 року.

[363] Різні типи кібератак та як не стати їх жертвою. URL : https://nordvpn.com/uk/blog/shcho-take-kiberataka/ (дата звернення: 07.10.2025).

[364] Traynor O. The Ultimate Guide to Financial Services Cybersecurity. November 18, 2024. URL : https://cybelangel.com/financial-services-cybersecurity-the-ultimate-guide/ (дата звернення: 07.10.2025).

Основною мотивацією для кіберзлочинних угруповань є отримання фінансової винагороди, адже банки, кредитні спілки та інші фінансові організації обробляють значні суми коштів. Кіберзлочинці легко можуть цим скористатися. Наприклад, вони можуть спробувати обійти контроль доступу та вимагати викуп за цінні дані або здійснювати шахрайські транзакції (табл. 3.1.1).

Таблиця 3.1.1 – Цілі, мотиви та суб'єкти кібератак

Суб'єкт кібератаки	Мотиви	Цілі	Приклад
Держави, групи, спонсовані урядом	Геополітичні, ідеологічні	Руйнування, пошкодження, загрози, фінансова вигода	Кіберкорупція, цілеспрямований фізичний злам систем, злам платіжної системи, шахрайські перекази, шпигунство
Кіберкримінал	Збагачення	Загроза / фінансова вигода	Тіньові потоки ліквідності, шахрайські перекази, наклеп, крадіжка облікових даних
Терористичні групи, хактивісти, внутрішня загроза	Ідеологічні, руйнування	Руйнація	Шахрайські перекази, витік інформації, хакерські атаки на кшталт «відмова в обслуговуванні»

Джерело: [365].

Поширеним видом кіберзлочинів у фінансовому секторі є крадіжка конфіденційних даних установ і клієнтів, які зловмисники можуть використовувати у власних інтересах. Наприклад, вони можуть продати конфіденційні дані іншим учасникам загроз, використати їх для крадіжки особистих даних або змусити організацію заплатити викуп за повернення даних.

До кібератак належать також маніпулятивні дії у формі «економічного шпигунства», що може дати змогу злочинним групам працювати на випередження ринків і маніпулювати цінами на акції та цінні папери. Так, 25 % фінансових лідерів виявили, що їхні ринкові дані були основною мішенню для кібератак.

[365] Traynor O. The Ultimate Guide to Financial Services Cybersecurity. November 18, 2024. URL : https://cybelangel.com/financial-services-cybersecurity-the-ultimate-guide/ (дата звернення: 07.10.2025).

Деякі кіберзлочинці прагнуть завдати шкоди репутації або дестабілізувати економіку. Наприклад, кібератака на національний банк країни може посилити нестабільність і підірвати суспільну довіру до фінансової установи. Деякі хакери зламують комп'ютерні системи відомих корпорацій лише з ціллю прославитися, використовуючи атаки на основі ШІ, шахрайство з використанням діпфейків та автоматизовані методи злому для обходу традиційних заходів безпеки. Наприклад, 2020 року було багато фішингових електронних листів, пов'язаних з COVID-19. Зловмисники розсилали інформацію від імені Всесвітньої організації охорони здоров'я, граючи на страху людей. Інші кіберзлочинці використовували клікбейт-заголовки, пов'язані з бізнесом, кредитами й політикою.

Ці мотиви можуть бути притаманними різним суб'єктам – від хакерів до національних держав і навіть простежуватися в інсайдерських загрозах, наприклад від незадоволених співробітників. Відтак, крім зовнішніх, суттєвими є внутрішні загрози, що походять від колишніх або нинішніх співробітників чи партнерів, які мають авторизований доступ до баз даних, і можуть вчинити крадіжки даних, зловживання та шахрайські дії. Загрози кібератаки посилюються за рахунок ризиків, пов'язаних з третіми сторонами, оскільки багато фінансових установ покладаються на сторонніх постачальників, постачальників хмарних послуг та інтеграції API.

Варто зазначити, що основним чинником кібератак унаслідок їхньої інформаційної природи залишається людський фактор. Аналіз випадків шахрайства свідчить про те, що 68 % випадків були пов'язані з людськими помилками та зловмисними діями інсайдерів[366]. Як співробітники, так і клієнти можуть несвідомо піддавати фінансові системи кіберризикам через низький рівень обізнаності щодо правил кібербезпеки. Нині існує глобальний дефіцит фахівців із кібербезпеки (за експертними оцінками, приблизно 4 мільйони), а понад половини державних організацій називають брак ресурсів і навичок кібербезпеки своєю найбільшою проблемою в підвищенні кіберстійкості. Тому поряд із технологічними рішеннями кібербезпеки потрібні значні інвестиції в розвиток людського капіталу, комплексне навчання співробітників, провадження програм підвищення обізнаності з кібербезпеки.

[366] Ozarslan S. Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. URL : https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (дата звернення: 07.10.2025).

Щодо об’єктів кібератаки, то ними можуть бути:

індивідуальні користувачі інтернету в частині їхніх особистих пристроїв, даних та облікових записів;

підприємства й корпорації, а саме корпоративні мережі, бази даних, інтелектуальна власність, фінансові активи;

державні установи, урядові мережі, критична інфраструктура, конфіденційні державні дані;

організації охорони здоров’я, зокрема медичні записи пацієнтів, інфраструктура лікарень, дослідницькі дані;

освітні установи – дані студентів, результати досліджень, мережева інфраструктура;

телекомунікаційні мережі, зокрема інфраструктура зв’язку, послуги передачі даних;

центри обробки даних, серверні потужності, хмарні сховища, клієнтські дані.

Зважаючи на різноманіття об’єктів атаки, важливим поняттям у кібербезпеці є «зовнішня поверхня атаки», що охоплює всі онлайн-об’єкти фінансової установи, видні зовнішньому світу: публічні вебсайти, мобільні додатки, портали для клієнтів, API, хмарні сервери, до яких потенційно може отримати доступ будь-хто, хто має підключення до інтернету. Зовнішня поверхня атаки у фінансовій індустрії постійно розширюється. Ця тенденція особливо посилилася після пандемії COVID-19, коли фінансові організації пройшли масштабну цифрову трансформацію для адаптації до дистанційних режимів роботи. Кожне додавання нового інструменту, програми чи сервера призводить до збільшення поверхні атаки фінансових послуг. З часом деякі з цих активів – особливо застарілі системи або тіньові ІТ (несанкціоноване, некероване програмне забезпечення) – можуть залишитися поза сферою моніторингу. Якщо ці «забуті» активи залишаються незахищеними, вони стають легкими мішенями для зловмисників. Водночас кіберзлочинці постійно вдосконалюють свою тактику, використовуючи передові методи для злому фінансових систем.

Для кібератак хакери використовують чотири основні категорії: пасивні, активні, інсайдерські, зовнішні атаки та їхні види (рис. 3.1.2).

Рисунок 3.1.2 – Суб’єкти, об’єкти та типи кібератак

Джерело: складено автором за [367].

[367] Cybersecurity Threats to Digital Banking and How to Guard Against Them. URL : https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them (дата звернення: 07.10.2025).

У сучасному глобальному світі регулярне повторення кібератак набуває форми такого явища, як кібертероризм. На відміну від типових кіберзлочинців, які шукають швидкої наживи, кібертерористи можуть атакувати фінансові установи, щоб дестабілізувати національні економіки, спричинити суспільну паніку або зробити політичні заяви.

Основними формами кібертероризму є:

державно-спонсовані атаки, які використовуються для підриву фінансової стабільності в конкуруючих державах і можуть бути надзвичайно складними. Наприклад, 2016 року Центральний банк Бангладеш зазнав державно-спонсованої кіберкрадіжки (ймовірно, здійсненої Північною Кореєю), що призвело до втрати 81 мільйона доларів[368];

хактивізм: хактивісти часто атакують великі фінансові компанії, щоб привернути увагу до таких проблем, як екологічна політика, соціальні питання або економічна нерівність. Їхньою метою може бути витік конфіденційних даних або спотворення вебсайтів, а не пряме отримання прибутку від атаки. Наприклад, 2010 року хактивістська група Anonymous здійснила атаки на декілька фінансових установ, включно із Visa та Mastercard[369].

Основним наслідком кібератак є значні фінансові втрати, які можуть досягати мільйонів доларів і складатися з витрат на ідентифікацію кіберзлочину, відновлення втрачених даних або систем, інформування клієнтів і зацікавлених сторін про кіберінцидент, а також покращення стандартів безпеки за результатами вразливостей. Прямі витрати охоплюють витрати на відновлення даних та ІТ, виплати викупів і юридичні та регуляторні штрафи. Публічні компанії зазнають значного падіння цін на акції (у середньому на 7,5 %) після витоку, що відображає занепокоєння інвесторів щодо майбутньої безпеки й прибутковості компанії. Непрямі витрати охоплюють втрату довіри споживачів, зменшення лояльності клієнтів і зниження продажів. Втрата репутації внаслідок витоку конфіденційних даних може значно зашкодити бізнесу та його клієнтам з фінансовими наслідками, що перевищують витрати на відновлення.

Аналіз показує, що кібервразливість може негативно впливати на вартість компанії та доходи інвесторів, відповідно, компанії з вищим рівнем ризику демонструють нижчі показники на фондовому

[368] Хакери зламали вебсайт Mastercard / BBC news Україна. 2010. 9 жовтня. URL : https://www.bbc.com/ukrainian/news/2010/12/101209_wikileaks_mastercard_attack_er

[369] Там само.

ринку. Однак ці ризики не повністю відображаються в цінах акцій, особливо у фірмах з менш досвідченими інвесторами. Це вказує на ринкову неефективність, де кіберризик систематично недооцінюється, що призводить до потенційно неправильного розподілу капіталу й наражає акціонерів на непередбачені втрати. Ця недооцінка кіберризиків у поєднанні з глибокими міжсекторальними зв'язками в цифровому ланцюжку поставок і потенціалом системної ескалації свідчить про те, що кіберврразливість окремих фірм є системним ризиком для всієї фінансової економіки, створюючи негативні зовнішні ефекти для суспільства.

Звіт IBM за 2024 рік показав, що фінансова індустрія має другу за величиною вартість витоків даних, поступаючись лише сектору охорони здоров'я (рис. 3.1.3).

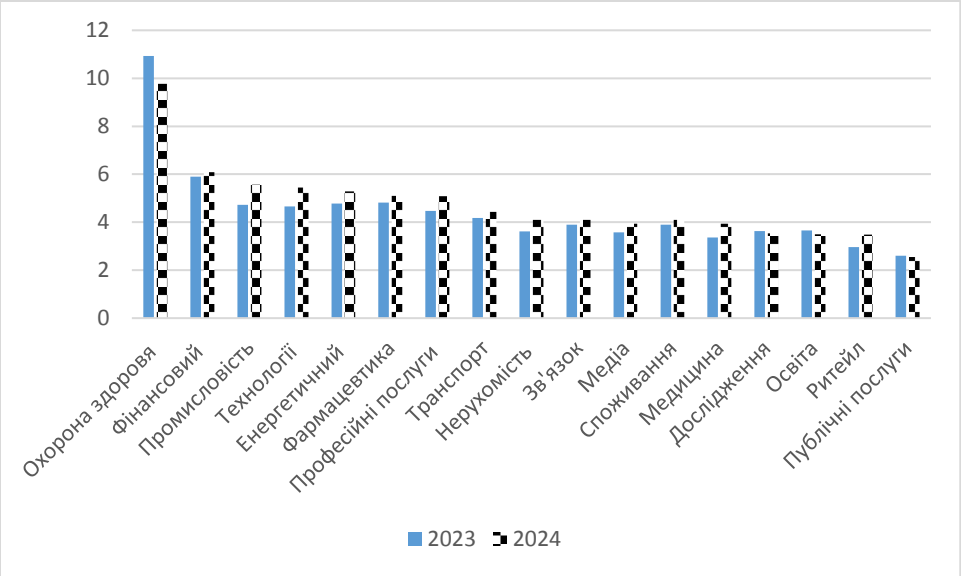

Рисунок 3.1.3 – Втрати від витоку даних унаслідок кібератак у різних сферах економіки

Джерело: [370].

В умовах глобальної фінансиалізації та стрімкого поширення мобільного банкінгу, цифрових гаманців і децентралізованих фінансів (DeFi) питання полягає вже не в тому, чи станеться кібератака, а в тому, коли вона станеться та наскільки вчасно фінансові організації зможуть її виявити, ефективно відреагувати й відновитися після неї. Така ситуація вимагає оновлення парадигми управління кіберризиками, де акцент зміщується з профілактичних заходів і простого реагування

[370] Traynor O. The Ultimate Guide to Financial Services Cybersecurity. November 18, 2024. URL : https://cybelangel.com/financial-services-cybersecurity-the-ultimate-guide/ (дата звернення: 07.10.2025).

на кіберінциденти до забезпечення безперервного моніторингу кіберзагроз і підвищення стійкості фінансової установи до наслідків кібератак. Водночас фінансові установи повинні виходити з того, що атаки й періодичні витоки інформації неминучі, що виводить на перше місце завдання розвитку засобів їхнього швидкого виявлення, локалізації та відновлення захисту організації після атаки. Тобто в умовах цифрової фінансиалізації система кібербезпеки як сукупності заходів щодо управління й захисту від кіберризиків стає фундаментальною складовою бізнес-моделі фінансового сектору.

Зважаючи на посилення складності кіберзагроз упродовж усього життєвого циклу фінансової організації формування її системи кібербезпеки має відбуватися на основі підходу «безпека за задумом», де заходи кібербезпеки інтегровані в бізнес-модель ще на етапі проєктування (підхід «shift-left»). Саме «вбудовування» заходів кібербезпеки в бізнес-модель на початкових етапах її формування дає змогу формувати найбільш ефективні засоби виявляти шахрайство на основі ШІ та захищати конфіденційні дані для безпечного впровадження інноваційних технологій і нових бізнес-моделей, як-от онлайн-банкінгі відкритий банкінг. Це дасть змогу клієнтам користуватися перевагами цифровізації, відчуваючи себе в безпеці та не стикаючись із надмірними регуляторними перешкодами. Водночас кібербезпека за допомогою таких технологій, як біометрія та багатофакторна автентифікація (MFA), певною мірою стає «невидимою» завдяки інтеграції в діяльність фінансових установ, тим самим формуючи довіру клієнтів і стимулюючи впровадження нових цифрових послуг. У такий спосіб реалізується принцип «безперешкодної безпеки», де заходи безпеки покращують взаємодію з користувачем, а не перешкоджають їй.

Сучасні системи кібербезпеки базуються на концепції «нульової довіри» (ZTA), яка орієнтована на стратегії ідентифікації ризиків через мікросегментації та передбачає, що жодна подія й елемент – всередині чи зовні мережі – не повинна автоматично вважатися надійною.

Для ідентифікації та моніторингу кіберризиків, забезпечення безпеки активів фінансові організації мають використовувати відповідний інструментарій. Наприклад, кіберангел (CybelAngel) – це інструмент управління поверхнею зовнішньої атаки (EASM), який спеціалізується на захисті цифрової діяльності від кібератак і витоків даних. Його функціонал охоплює:

ідентифікацію вразливих цифрових активів до того, як їх виявлять хакери;

виявлення будь-яких витоків даних до того, як вони стануть проблемою;

запобігання захопленню й продажу викрадених облікових даних на Dark Web;

відстеження кіберзлочинної діяльності темного вабу (Dark Web) для запобігання атакам;

зняття зловмисних сайтів до того, як вони завдадуть шкоди репутації бренду або клієнтам.

На жаль, фінансові організації не можуть повністю покласти відповідальність за кібербезпеку лише на IT-відділ. Це ключова складова загальної стратегії компанії, і провідну роль у ній відіграє головний фінансовий директор (далі – CFO). Саме CFO має знайти баланс між інвестиціями в кібербезпеку та досягненням широких фінансових цілей компанії. Зокрема, CFO повинен:

розпізнавати фінансові кібербезпекові загрози й забезпечувати наявність ресурсів та інструментів, як-от CybelAngel, для їхнього усунення;

контролювати дотримання організацією всіх фінансових і регуляторних норм щодо захисту даних;

тісно співпрацювати з головними офіцерами з інформаційної безпеки (CISO) для визначення пріоритетних напрямів зусиль у сфері кібербезпеки.

Розпочинати формування ефективної системи кібербезпеки Американське Агентство з кібербезпеки та інфраструктурної безпеки (CISA) рекомендує, спираючись на такі чотири «стовпи»:

1. Визнання ключовим пріоритетом обмін інформацією між організаціями, сторонніми постачальниками й керівними органами, водночас комунікація має бути «своєчасною та дієвою».

2. Дотримання найкращих практик щодо управління ризиками на основі рекомендацій Національного інституту стандартів і технологій (NIST) Cybersecurity Framework, зокрема для забезпечення безпеки операцій зі сторонніми постачальниками.

3. Створення планів реагування на інциденти й алгоритмів відновлення в процесі співпраці банків і фінансових установ з керівними органами та правоохоронними органами для відновлення після будь-яких кіберінцидентів, використовуючи скоординовані плани реагування.

4. Постійне вдосконалення регуляторних рамок щодо дотримання кібербезпеки.

У міжнародній практиці вже існує досить розвинена нормативно-правова база, основні акти якої наведені в таблиці 3.1.2.

Таблиця 3.1.2 – Міжнародні нормативно законодавчі акти, що регулюють сферу кіберризиків

Назва	Зміст
Рамка кібербезпеки NIST (NIST CSF)	Широко прийнята, гнучка й комплексна рамка, що надає стандарти, рекомендації та найкращі практики для управління кіберризиками. Вона зосереджена на п'яти «стовпах»: ідентифікація, захист, виявлення, реагування, відновлення. Багато великих світових організацій використовують NIST CSF
GDPR (Загальний регламент про захист даних ЄС)	Обов'язковий для підприємств, що обробляють дані, пов'язані з громадянами ЄС, зі значними штрафами за недотримання
SOX (Закон Сарбейнса-Окслі)	Обов'язковий для всіх публічних компаній у США, що визначає найкращі практики безпеки для запобігання шахрайським фінансовим операціям і вимагає регулярних аудитів
PCI DSS (Стандарти безпеки даних індустрії платіжних карток)	Стандарти для зменшення шахрайства з кредитними картками та захисту даних власників карток
DORA (Закон про цифрову операційну стійкість)	Європейський регламент, що зосереджується на цифровій операційній стійкості фінансових установ
Директиви AML та вимоги KYC	Закони, що вимагають від фірм виявляти й повідомляти про підозрілі фінансові операції та перевіряти особи клієнтів для запобігання шахрайству й відмиванню грошей

Джерело: [371; 372].

Хоча дотримання загальноприйнятих нормативних вимог (GDPR, SOX, DORA тощо) є важливою умовою під час вибору заходів кібербезпеки, акцент на «проактивних, керованих розвідкою стратегіях безпеки», «безперервному моніторингу та виявленні загроз» і менталітеті «коли, а не якщо» свідчить про вихід фінансових установ за межі простого дотримання рекомендованих вимог щодо непорушення кібербезпеки. Це означає, що фінансові установи еволюціонують від

[371] Traynor O. The Ultimate Guide to Financial Services Cybersecurity. November 18, 2024. URL : https://cybelangel.com/financial-services-cybersecurity-the-ultimate-guide/ (дата звернення: 07.10.2025).

[372] Cost of a Data Breach Report 2025 / IBM. URL : https://www.ibm.com/reports/data-breach (дата звернення: 07.10.2025).

дотримання мінімальних регуляторних стандартів до побудови всебічної кіберстійкості, яка може адаптуватися до динамічних загроз і забезпечувати безперервну діяльність навіть під час атаки. Інакше кажучи, спостерігається стратегічний перехід від статичного, заснованого на правилах підходу кібербезпеки до динамічного, адаптивного до ризиків.

Для науково обґрунтованого й методологічно виваженого вибору ефективних методів протидії кіберінцидентам критично важливим є методика аналізу кіберзагроз. Аналіз кіберзагроз – це процес систематизації інформації, спрямований на підвищення стійкості фінансових установ і організацій підвищити свою стійкість до кібератак. Він спирається на фактологічні дані й аналітичні висновки, що надають уявлення про ландшафт загроз. Це зі свого боку дає змогу приймати обґрунтовані рішення щодо підготовки до кібератак, їхнього раннього виявлення та ефективного реагування. Аналітично-структурована інформація про поведінку кіберзлочинців, їхні інструменти й методи, цільові вразливості та нововиявлені загрози допомагає організації обрати найбільш ефективні методи й інструменти забезпечення кібербезпеки.

У сучасному світі обробка значних обсягів даних щодо нових або вже відомих кіберзагроз здійснюється на аналітичних платформах. Основними джерелами даних для аналізу кіберзагроз є:

використання публічно доступної інформації з відкритих джерел;

інформаційні канали, що охоплюють потоки спеціалізованих даних від постачальників інформації;

внутрішні дані, зібрані всередині самої організації.

Хоча канали даних про кіберзагрози містять значний обсяг інформації про кіберінциденти, проте для вирішення завдання безпосереднього визначення й оцінювання загроз і внутрішніх вразливостей фінансових установ та розробки плану дій залучається людина-аналітик. Водночас сучасні аналітичні технології активно використовують інструменти на основі штучного інтелекту й машинного навчання з розширеними можливостями, як-от оркестрація безпеки, автоматизація та реагування (SOAR), керування інформацією та подіями безпеки (SIEM), розширене виявлення й реагування (XDR). Це дає змогу автоматично блокувати шкідливі файли та IP-адреси в разі виявлення ознак кібератаки.

Так, фірма Банц (Bunq) використовує ШІ-платформу Nvidia для перевірки 520 атрибутів платежів на предмет шахрайства. Рішення Mastercard для аналізу рішень сканує трильйон точок даних у реальному часі для виявлення справжності транзакцій, підвищуючи ефективність виявлення шахрайства до 300 %. Фірма Клоуз бразер (Close Brothers) використовує UiPath для автоматизації обробки платежів, зменшуючи затримки й помилки. Інноваційні технології забезпечують безпечний цифровий онбординг: наприклад, система SmartServe від HSBC, що використовує ШІ, машинне навчання та біометричну верифікацію, дає змогу відкривати нові рахунки та проходити процедуру KYC (Знай свого клієнта) віддалено за лічені хвилини, покращуючи клієнтський досвід і забезпечуючи безпеку. Це не тільки запобігає втратам, але й прискорює обробку транзакцій, оскільки роботизація та автоматизація процесів (RPA) заощаджує час і зменшує кількість помилок за умови, що автоматизовані процеси захищені від маніпуляцій. Сьогодні в умовах постійного потоку інформації нові загрози складно визначити, що є дійсно актуальним і вимагає негайних дій.

Щоденна агрегація глобальних даних та їхній аналіз на основі наукових принципів для фільтрації хибних спрацювань і пріоритизації ризиків, безперебійність і зручність цифрових процесів забезпечує прийняття швидких та раціональних рішень і дає змогу перейти від реактивного реагування до проактивного запобігання кібератакам, а саме:

ефективно планувати заходи реагування на інциденти, що забезпечує швидку локалізацію атаки, відновлення системи та зв’язок із зацікавленими сторонами під час кіберінцидентів, мінімізуючи час простою та захищаючи репутацію установи;

безперервний моніторинг і розвідка кіберзагроз: цілодобові послуги моніторингу забезпечують виявлення загроз у реальному часі, збір розвідувальних даних про загрози, хоча часто її неформальний, має вирішальне значення для випередження загроз, що розвиваються;

безпека «shift-left»: інтеграція безпеки на ранніх етапах циклу розробки зменшує обсяг переробок, технічний борг і вплив на бізнес. Автоматизований безперервний аналіз безпеки коду та ШІ в технологіях безпеки коду прискорюють пріоритизацію вразливостей.

Ключові заходи в системі кібербезпеки наведені в таблиці 3.1.3.

Таблиця 3.1.3 – Ключові заходи кібербезпеки у фінансовому секторі

Захід / Технологія кібербезпеки	Опис	Пряма вигода для цифрової трансформації / бізнес-моделі
Багатофакторна автентифікація (MFA)	Вимагає кілька форм ідентифікації для доступу, значно зменшуючи ризик несанкціонованого доступу	Підвищення довіри клієнтів та безпечне цифрове онбординг, мінімізація крадіжки облікових даних
Виявлення шахрайства на основі ШІ	Використання штучного інтелекту та машинного навчання для аналізу даних і виявлення аномальних транзакцій у реальному часі	Покращена операційна ефективність завдяки автоматичному виявленню та запобіганню шахрайству, зменшення фінансових втрат
Шифрування даних	Перетворення даних на закодований формат для захисту конфіденційної інформації від несанкціонованого доступу	Забезпечення конфіденційності даних і відповідності нормативним вимогам, захист даних під час передачі та зберігання
Планування реагування на інциденти	Розробка структурованих протоколів для швидкого реагування на кіберінциденти, локалізації та відновлення	Безперервність бізнесу й захист репутації, мінімізація часу простою та наслідків витоків
Рамка кібербезпеки NIST (NIST CSF)	Комплексний набір стандартів і рекомендацій для управління кіберризиками, що охоплює ідентифікацію, захист, виявлення, реагування та відновлення	Цілісне управління ризиками та адаптивність, масштабована й гнучка основа для програм безпеки
Безпека «shift-left»	Інтеграція заходів безпеки на ранніх етапах циклу розробки програмного забезпечення	Швидші й безпечніші інновації, зменшення технічного боргу та витрат на виправлення вразливостей

Джерело: складено автором за [373].

Серед методів, що дають змогу оперативно ідентифікувати потенційні кіберзагрози та мінімізувати їхні наслідки, виділяють такі:

1. Мережевий моніторинг, який є ключовим інструментом для відстеження й аналізу обміну даними в мережі та призначений для виявлення аномальної мережевої активності, що може свідчити про спроби зловмисників здійснити атаку. Предметом аналізу є обсяги трафіку, типи з'єднань, портів і протоколів, що дає змогу вчасно виявити відхилення від нормальної поведінки.

[373] Financial crime trends to watch out for in 2023. URL : https://fintech.global/2023/01/30/financial-crime-trends-to-watch-out-for-in-2023 (дата звернення: 07.10.2025).

2. Аналіз поведінки систем і користувачів як потужний метод ідентифікації нетипових змін у їхній роботі. Системи поведінкового аналізу здатні виявляти аномалії в динаміці, як-от нехарактерні години активності, незвичайні обсяги завантажень або доступ до нетипових ресурсів. Це дає нагоду фахівцям з кібербезпеки отримувати своєчасні сповіщення про підозрілі дії та реагувати на них.

3. Управління журналами подій (Log Management) за рахунок збору, зберігання й аналізу даних із системних журналів, які містять детальну інформацію про дії користувачів і систем у реальному часі, що є критично важливим для постінцидентного аналізу. Завдяки цій системі в разі атаки можна відновити хронологію подій, ідентифікувати джерело та вектор атаки, а також виявити підозрілі дії, що передували інциденту.

4. Регулярні тести на проникнення (Penetration Testing), проведення яких є проактивним підходом до забезпечення кібербезпеки. Ці тести імітують атаки реальних зловмисників на систему, даючи змогу виявити слабкі місця та вразливості до того, як їх використають кіберзлочинці. Результати таких тестів допомагають удосконалювати захисні механізми й розробляти ефективніші плани реагування на інциденти.

5. Використання штучного інтелекту (ШІ), який разом із алгоритмами машинного та глибокого навчання дає змогу аналізувати значні обсяги даних у режимі реального часу, виявляючи підозрілі дії та аномалії, які можуть вказувати на шахрайство або кібератаки. Центри операцій з безпеки (SOC), керовані ШІ, використовують автоматизацію для виявлення та нейтралізації загроз до їхньої ескалації. Ці моделі постійно вдосконалюються, навчаючись на попередніх спробах шахрайства, що дає нагоду фінансовим установам діяти пруденційно щодо нових кіберзагроз.

6. Технологію блокчейн, що забезпечує децентралізований підхід до безпеки цифрових фінансів, зменшуючи залежність від централізованих систем, які є більш вразливими до кібератак. Незмінний реєстр блокчейну забезпечує цілісність фінансових транзакцій, запобігаючи спотворенню даних. Смарт-контракти дають змогу укладати безпечні й автоматизовані фінансові угоди без потреби в посередниках. Крім того, системи верифікації ідентифікації на основі блокчейну підвищують автентифікацію та зменшують крадіжку ідентифікаційних даних.

7. Децентралізовані фінанси (DeFi), які забезпечують підвищену фінансову доступність послуг та їх прозорість, вони також стикаються з унікальними проблемами безпеки, як-от вразливості смарт-контрактів, маніпуляції оракулами й флеш-кредити атаки. Щоб усунути ці ризики, платформи DeFi впроваджують розширені аудити безпеки, методи формальної верифікації та децентралізовані рішення для управління ідентифікацією.

Для підвищення кібербезпеки й зменшення шахрайства фінансові установи все частіше впроваджують біометричні та поведінкові методи автентифікації, як-от сканування відбитка пальця, розпізнавання обличчя та голосу. Ці технології забезпечують додатковий рівень захисту, що виходить за межі традиційних паролів і PIN-кодів, вимагаючи кількох методів верифікації, зокрема:

багатофакторна автентифікація (MFA) та біометрія є критично важливими для запобігання несанкціонованому доступу й мінімізації крадіжки облікових даних / токенів, на які припадає значна частина витоків даних. Безпарольні підходи, як-от FIDO, є новими стандартами в цій сфері;

шифрування та токенізація потрібні для захисту конфіденційної фінансової інформації як у стані її зберігання, так і під час передачі, забезпечуючи, що навіть у разі перехоплення даних вони залишаться нечитабельними;

брандмауери, системи виявлення / запобігання вторгненням (IDS / IPS), брандмауери вебдодатків (WAF) та системи запобігання DDoS-атакам, що є вирішальними для захисту фінансової інфраструктури;

рішення щодо управління ідентифікацією та доступом (IAM), охоплюючи фреймворки з нульовою довірою та принцип найменших привілеїв, які дають змогу запобігти несанкціонованому доступу до критично важливих систем і даних.

Під час побудови системи кібербезпеки зазначені технології інтегруються в банківські додатки, банкомати та платформи мобільних платежів з метою поглибленого аналізу поведінки користувачів (швидкість набору тексту, рухи миші та жести на сенсорному екрані) для виявлення аномалій, що можуть вказувати на шахрайську діяльність. Такий підхід підвищує безпеку, не впливаючи на користувацький досвід. Отже, експертний аналіз загроз у поєднанні із цифровими

інструментами їх виявлення та запобігання, що спираються на ШІ й машинне навчання, суттєво підвищує ефективність протидії кіберзагрозам через:

викриття ймовірних зловмисників та їхніх мотивів;

виявлення тактики, методів і процедур противника;

аналіз потенційного впливу різних атак на бізнес;

визначення загальних індикаторів компрометації;

формування алгоритму відповідних дій банку, ефективних під час кібератаки;

автоматичне блокування атак;

формування бази даних про загрози для формування стратегій безпеки й тактичних заходів;

отримання контексту для оцінювання загроз та їхнього співвідношення з іншими діями для визначення оптимальної та найефективнішої відповіді;

глибше розуміння вразливостей, заходів протидії їм і методів, які зловмисники використовують для компрометації систем;

визначення релевантних для фінансової організації загроз для надання обґрунтованих рекомендацій щодо бюджету системи кібербезпеки.

На практиці в останні роки НБУ значно посилив контроль за дотриманням банками заходів кібербезпеки та інформаційної безпеки у сфері переказу коштів. Ще 2021 року було ухвалено Положення про організацію кіберзахисту в банківській системі України[374]. 2025 року проєкт постанови Правління НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків» оприлюднено на сайті для громадського обговорення[375]. Цей документ розроблено на виконання вимог Закону України «Про основні засади забезпечення кібербезпеки України», згідно з яким Національний банк України має визначити порядок, вимоги та заходи із забезпечення кіберзахисту й інформаційної безпеки для суб'єктів переказу коштів, а також здійснювати контроль за їхнім виконанням.

[374] Про затвердження Положення про організацію кіберзахисту в банківській системі України / Національний банк України. URL : https://bank.gov.ua/admin_uploads/article/proekt_2021-11-04.pdf (дата звернення: 07.10.2025).

[375] Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг : постанова НБУ. URL : https://bank.gov.ua/admin_uploads/article/proekt_2025-03-10.pdf (дата звернення: 07.10.2025).

Загальною метою цього посиленого нагляду є підвищення стійкості та безпеки банківських операцій на тлі все більш складних сучасних кіберзагроз. Для досягнення цього постанова запровадила нові категорії контролю, що охоплюють як виїзні перевірки, так і дистанційний нагляд, які ретельно проводяться спеціалізованими експертами НБУ у сферах кібербезпеки й інформаційної безпеки. Крім того, банки тепер зобов'язані проводити щорічні самооцінки стану своєї інформаційної безпеки та кібербезпеки. Вони також повинні готувати та подавати до НБУ комплексний річний звіт, що деталізує їхнє оцінювання ризиків інформаційної безпеки та кіберризиків.

Зобов'язуючи проводити ретельні самооцінки та здійснюючи всебічний регуляторний нагляд, НБУ стратегічно позиціонує кібербезпеку не просто як пункт у списку відповідності банку, а як фундаментальний і беззаперечний елемент довгострокової життєздатності, цілісності та надійності цифрових фінансових послуг. Цей акцент є особливо критичним, враховуючи поточний геополітичний контекст, де кіберзагрози часто спонсоруються державою та є високотехнологічними.

Провідні фінансові установи в Україні, як-от Райффайзен Банк Україна, своїми діями підтверджують, що безпека клієнтських даних є першочерговим пріоритетом. Вони демонструють це, дотримуючись суворих міжнародних стандартів, зокрема ISO 27001:2022, впроваджуючи системи безперервного моніторингу, призначені для виявлення нетипової поведінки й підозрілих подій у своїй інфраструктурі. Вони також використовують передові інструменти, спеціально розроблені для виявлення та запобігання шахрайським діям, тим самим захищаючи кошти, довірені їм клієнтами. Додатково НБУ також встановив конкретні вимоги до надання певних обмежених платіжних послуг (набрали чинності 28 грудня 2022 року), що стосуються таких операцій, як платежі за цифровий контент і благодійні внески. Їхня мета полягає в підвищенні безпеки користувачів і проактивному запобіганні шахрайським операціям, пов'язаним з цими видами цифрових платежів.

Підсумовуючи, кібербезпека є не просто технічною вимогою, а невід'ємним стратегічним імперативом функціонування установ в умовах цифрової трансформації фінансового сектору. Вона є основою, на якій будуються сучасні бізнес-моделі, забезпечуючи інновації, сприяючи довірі клієнтів і гарантуючи операційну стійкість у все більш взаємопов'язаному та загрозливому цифровому ландшафті.