ЕКОНОМІКА ТА ІННОВАЦІЙНИЙ РОЗВИТОК НАЦІОНАЛЬНОГО ГОСПОДАРСТВА

УДК 330:004 **DOI: 10.37332/2309-1533.2021.3-4.3**
JEL Classification: O20

Демчишак Н.Б.,
д-р екон. наук, професор, професор кафедри фінансів, грошового обігу і кредиту,
Шкиря А.С.,
студентка магістратури, спеціальність "Фінанси, банківська справа та страхування", Львівський національний університет ім. Івана Франка

УПРАВЛІННЯ РИЗИКАМИ У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ В УМОВАХ КІБЕРЗАГРОЗ І ПОСТПАНДЕМІЧНОГО ВІДНОВЛЕННЯ ЕКОНОМІКИ

Demchyshak N.B.
dr.sc.(econ.), professor, professor at the department of finance, money circulation and credit, Ivan Franko National University of Lviv,
Shkyria A.S.,
master student at the department of finance, money circulation and credit, Ivan Franko National University of Lviv

RISK MANAGEMENT IN THE FINANCIAL SECTOR OF UKRAINE IN THE CONTEXT OF CYBER THREATS AND POST-PANDEMIC ECONOMIC RECOVERY

Постановка проблеми. Сучасна глобалізована світова економіка характеризується значними обсягами інформаційних ресурсів та даних, якими володіють організації та підприємства, а також індивіди. У цьому контексті, зважаючи на інтенсифікацію процесів цифровізації, все більше уваги приділяється проблемам забезпечення захисту інформації, адже використання інформаційних технологій значно підвищує ефективність фінансових процесів й операцій на різних ринках. Водночас зростає кількість випадків шахрайства й злочинів через комп'ютерні мережі, що може завдати як матеріальної, так і нематеріальної шкоди. Зокрема суттєвою проблемою для малого та середнього бізнесу в Україні, з огляду на стрімке проникнення інформаційних та комп'ютерних технологій у всі сфери, у тому числі у фінансовий сектор, є кіберризики. Тому питання управління ними набуває особливої актуальності у контексті необхідності забезпечення постпандемічного відновлення економіки й гарантування національної безпеки.

Аналіз останніх досліджень і публікацій. Ризики у фінансовому секторі є об'єктом дослідження вітчизняних вчених, таких як: В. Біленька [9], В. Братюк [2], В. Бурячок [3], З. Варналій, І. Віннікова [4], С. Волосович [6], Н. Гребенюк [8], Я. Дропа [21], А. Іващенко, В. Толубко, О. Підхомний [20], В. Якушев [16] та ін. Не заперечуючи здобутків перелічених фахівців, потрібно відзначити, що проблематиці кіберзагроз в українській науці приділено недостатньо уваги, водночас однією із причин цього є відносна новизна цього поняття.

Постановка завдання. Метою статті є обґрунтування підходів вітчизняних та зарубіжних вчених до управління ризиками у фінансовому секторі України в умовах кіберзагроз та необхідності забезпечення національної безпеки і постпандемічного відновлення економіки.

Виклад основного матеріалу дослідження. Сучасний стан економіки України важко назвати стабільним. У 2021 році наша країна обтяжена численними загрозами та ризиками для своєї національноїх безпеки. Серед соціальних, економічних та фінансових ризиків України експерти усе частіше називають кібернетичні атаки. Наразі існує ціла система, яка оперує набором високотехнологічних інструментів, що дозволяють здійснювати кібератаки незалежно від стану захищеності. З розвитком «хмарних» технологій та ринку так званого «Інтернету речей» (IoT), зникає таке поняття, як мережевна захищеність підприємства. Відповідно, традиційний підхід до забезпечення кібербезпеки стає неефективним. Виклики, з якими стикається бізнес, – це складні цільові атаки (APT) з боку потужних хакерських об'єднань; застосування кіберзброї, яка здатна виводити з ладу об'єкти критичної інфраструктури, –призводять до вкрай негативних наслідків для економік окремих регіонів і держав світу. Зазначені факти, а також розповсюдження та постійне удосконалення механізмів кібератак та зростання завданої ними зумовлює необхідність у застосування технологій управління ризиками фахівцями у сфері кібербезпеки [1]. При цьому кібербезпеку необхідно розглядати як одну із ключових складових національної безпеки країни. На наш погляд, доцільність власне такої позиції щодо аналізу ризиків у фінансовому секторі, які мають цифровий характер, не у структурі фінансової безпеки, а загалом національної пояснюється їх різноманіттям та складністю ідентифікації приналежності чітко до конкретної сфери.

Загалом поняття «національна безпека» є неоднозначним й комплексним та характеризується різними сутнісними особливостями і критеріями, відмінність між якими полягає, зокрема, у відмінних позиціях вчених та практиків. Зрозуміло, що є розбіжності в розумінні сутності національної безпеки у фахівців-юристів порівняно із економістами, політологами та представниками військово-промислового комплексу тощо.

Національна безпека, на думку вчених, – це система державно-правових і суспільних гарантій стабільності життєдіяльності та розвитку українського народу загалом та кожного громадянина зокрема, захист їхніх базових цінностей і законних інтересів, джерел духовного і матеріального добробуту від зовнішніх та внутрішніх загроз [5]. У свою чергу, згідно Закону України «Про національну безпеку» від 21 червня 2018 року, національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [12].

Традиційно розрізняють такі види безпеки, як: політична, екологічна, соціальна, військова, технологічна, екологічна, духовна, релігійна, інформаційна, соціокультурна, державна, генетична, продовольча, медична, демографічна, ядерна. Кібербезпеку як складову національної безпеки України часто розглядають в межах інформаційної, хоча, на наш погляд, активна цифровізація національних економік країн світу та вітчизняної зокрема дає аргументи для обґрунтування необхідності виокремлення кібербезпеки та її вивчення як окремої важливої складової національної безпеки. Доцільність цього також є наслідком тотальних трендів переходу в онлайн упродовж 2020–2021 рр., які стосуються надання послуг, організації роботи тощо. При цьому в умовах постпандемічного відновлення очевидно, що ці тенденції збережуться. Відтак, практично у всіх країнах має місце дефіцит дієвих управлінських рішень задля уникнення кіберзагроз та мінімізації ризиків власне у фінансовому секторі. Незважаючи на створення Міністерства цифрової трансформації України, роботу Державної служби фінансового моніторингу, департаментів із питань кіберзахисту в органах внутрішніх справ та інших інституціях, національна економіка є дуже вразливою до нових загроз, а громадяни й бізнес не готові їх сприймати й адекватно усвідомлювати рівень небезпеки.

Так, упродовж останнього десятиліття в середовищах систем управління в промисловості (Industrial Control Systems –ICS) все більше актуалізується питання національної безпеки, зокрема її кібер-складової. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека – це 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 [13]. Тобто у вітчизняній нормативно-правовій базі дається достатньо широке тлумачення кібербезпеки, з чим погоджуємось, враховуючи сутнісні характеристики цього поняття та складність формування чіткої дефініції.

У свою чергу, поява у науковому обігу та фінансовій практиці поняття «кіберризик» стала результатом усвідомлення у першу чергу бізнесом важливості кібербезпеки. Загалом підходи до його тлумачення принципово не відрізняються. Відтак, на наш погляд, «кіберризик» можна розглядати як ризик фінансових втрат (прямих і непрямих), повної або часткової зупинки роботи, а також ймовірності завдання збитків (матеріальних і нематеріальних) приватним особам чи бізнесу. Тобто, у цій дефініції робиться акцент на різні наслідки кіберзагроз, зокрема не лише матеріальні й суто фінансові, але й на моральні й репутаційні. При цьому, в умовах легкості доступу до інформації для потенційних клієнтів, наприклад, завдана шкода репутації певним бізнес-структурам часто може мати не менше значення для їх розвитку, ніж прямі фінансові втрати. Це власне і є аргумент на користь частково

обгрунтованого вище твердження, що поняття кібербезпеки ширше інформаційних систем і ресурсів. Адже будь-яка сфера діяльності індивідів і підприємств може бути охоплена чи «притягувати» певні загрози настання таких ризиків, наприклад, у процесі управління ресурсами компанії, роботи з персоналом, бізнес-партнерами, клієнтами тощо.

Можна виділити наступні ризики, пов'язані з використанням сучасних електронних технологій, що впливають на фінансовий сектор: кібератаки; ризики шахрайства в IT-сфері; ризики помилок в програмному забезпеченні; стратегічні ризики, пов'язані з швидким розвитком інформаційних технологій і зміною умов ведення бізнесу; ризики державного регулювання фінансових інновацій; ризик порушення функціонування складних інформаційних систем [7].

Становить науково-практичний інтерес запропонована вченими класифікація кіберризиків та їх групування за такими ознаками [4]: втрата або крадіжка носіїв інформації та мобільних пристроїв; доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ; ненавмисне розголошення співробітниками конфіденційної інформації; навмисні дії співробітників (інсайдерів); неконтрольоване копіювання даних співробітниками.

Такий підхід дозволив виокремити наступні види кіберризиків у фінансовому секторі: ризик втрати інформації під час злому паролю доступу або внаслідок DDoS атаки; ризик фінансових втрат від фішингових атак; ризик фінансових втрат через порушення роботи комп'ютерних систем; ризик фінансових втрат від кібер-шантажу або вірусного блокування комп'ютерних систем; ризик фінансових втрат через викрадення та розголошення персональних даних та інформації [4].

Проблему управління ризиками у фінансовому секторі України в умовах кіберзагроз доцільно розглядати безпосередньо у контексті управління кіберризиками як основи для будь-якої дії у сфері безпеки: чи то впровадження систем або інструментів, або побудова процесів і впровадження правил і політик. Погоджуємось із думкою фахівців, що проєкти з управління ризиками часто недооцінюють, проте саме грамотне визначення та управління кіберризиками дозволяє раціонально розподілити бюджет підприємств на кібербезпеку і грамотно підготуватися до атак і загроз заздалегідь [10].

Відтак, управління ризиками як процес має безперервний та ітеративний характер. Грунтуючись на традиційних підходах, у межах цього процесу можна виділити три етапи (рис. 1): ідентифікація ризиків, їх мінімізація, оцінка та моніторинг ризиків.

Рис. 1. Цикл управління кіберризиками на підприємстві

Джерело: удосконалено авторами на основі [1]

Тобто в рамках першого етапу необхідно визначити ризик та його складові. У першу чергу йдеться про загрози та ймовірність їх настання в межах конкретної сфери роботи підприємства, відповідні сутнісні характеристики таких загроз. Потрібно провести аналіз впливу таких загроз і, як результат чіткої ідентифікації, сформувати опис та дати оцінку наслідків реалізації ризику і його значимості для роботи.

На наступному етапі приймаються конкретні рішення на рівні менеджменту підприємства щодо комплексу інструментів управління ризиками і заходів з їх мінімізації. Останні можуть мати адміністративно-правовий характер, організаційно-процедурний, або ж суто технічний. Відтак розпочинається робота над мінімізацією ризиків, при цьому акцентується увага на ключових ризиках, оскільки важливими є витрати на їх мінімізацію для підприємства. Тобто реалізація відповідних заходів спрямована на протидію виявленим чи потенційним ризикам чи контроль за ними у межах визначеної процедури й послідовності управління.

Після імплементації заходів починається етап оцінки ризиків і їх постійного моніторингу. Водночас аналізується ефективність заходів підприємств. Критерієм успішності управління при цьому є ситуація, коли ризик зменшується до допустимого для підприємства рівня, що був заздалегідь визначений. Особливе значення в умовах стрімкого розвитку цифрових технологій, на наш погляд,

має збір інформації для використання у випадку появи типових кіберзагроз задля економії ресурсів. У свою чергу, із появою нових ризиків цикл запускається заново.

Очевидно, що сьогодні ключовим фактором конкурентоспроможності індивідів та підприємств є діджиталізація і впровадження ІТ та фінансових технологій (фінтех) у всіх сферах діяльності. Тому організація управління кіберризиками у системі національної безпеки країни однозначно повинна базуватись на підходах, сформованих на розумінні невідворотності діджиталізації різних сфер життєдіяльності в Україні у громадському та бізнес-секторі. Зазначені процеси будуть лише інтенсифікуватись, водночас, з іншого боку, вони зумовлюються крайньою необхідністю у зв'язку із карантинними обмеженнями, а також потребою у відновленні національної економіки у постпандемічний період, тобто першочергово йдеться про 2021–2022 рр.

Відзначимо, що у широкому розумінні під діджиталізацією (цифровізацією) прийнято розуміти трансформацію й проникнення цифрових технологій у всі бізнес-процеси та надання послуг й використання нових інструментів, наслідком чого є підвищення продуктивності та покращення комунікаційної взаємодії учасників фінансово-економічних та суспільних відносин. Тобто діджиталізація – це перехід інформаційного простору у цифровий. Зокрема фінансовий сектор є складовою національної економіки, яка першочергово цифровізуватиметься в Україні, процес чого по суті уже активно триває упродовж 2019–2021 рр.

У контексті зазначеного вище необхідно акцентувати особливу увагу на ринок фінансових послуг, який зазнає по суті найглибших структурних змін в частині виникнення нових цифрових сервісів, а також модернізації існуючих. Водночас, саме цей ринок є базисом для забезпечення конкурентоспроможності країни, адже дозволяє спрямувати інвестиційні потоки у ті чи ніші сегменти економіки, сприяючи у такий спосіб стійкому економічному зростанню. Ринок фінансових послуг структурно включає ринки банківських, страхових, інвестиційних послуг, операцій з цінними паперами тощо, у межах яких здійснюється обіг фінансових активів та надаються конкретні сервіси. Відтак, окрім безпосередньо послуг, у найближчі роки в Україні модернізуватимуть й підходи до їх надання, імплементуватимуться технологічні рішення в частині організації надання послуг та маркетингу. Клієнтам також необхідно буде бути готовими до нових способів супроводу, зокрема використання чат-ботів і штучного інтелекту банківськими установами тощо. Поширення таких фінансових технологій (фінтех) значно інтенсифікувалось у період пандемії, при цьому потреба у фінансових послугах аж ніяк не знизилась ні в Україні, ні у світі. У цьому контексті важливо не стати об'єктом шахрайства й кіберзлочинів для громадян і бізнесу, які ще не достатньо адаптовані до нових реалій.

Важливо, що на державному рівні є концептуальне розуміння того, що фінансовий ринок завжди був індикатором стану економіки та ефективності її реформування. Враховуючи це, задля розвитку цифрової економіки в Україні на початку 2020 року Національний банк України, Національна комісія з цінних паперів та фондового ринку та Міністерство фінансів України підготували важливий програмний документ – Стратегію розвитку фінансового сектору України до 2025 року, що була оновлена у березні 2021 року. Стратегія передбачає розвиток фінансового сектору за п'ятьма основними напрямами: зміцнення фінансової стабільності; сприяння макроекономічному розвитку та зростанню економіки; розвиток фінансових ринків; розширення фінансової інклюзії; впровадження інновацій у фінансовому секторі [14].

На наш погляд, успішна реалізації цієї стратегії у період постпандемічного відновлення національної економіки буде можливою лише за умови активної роботи над мінімізацією кіберзагроз, які з кожним роком лише зростають. Аналітична компанія Canalys провела дослідження щодо ситуації в сфері кіберзахисту та зробила негативні висновки – число успішних кібератак зростає з величезною швидкістю. Статистика 2020 року показує, що за цей період було зламано більше записів, ніж за минулі 15 років [17] (рис. 2).

Як видно з даних рис. 2, збитки від кібератак у 2020 р. склали понад 30 млрд дол. США та більш ніж вдвічі перевищують збитки за підсумками 2019 р. На кількість зламів суттєво вплинули спеціальні віруси-вимагачі, у яких основною метою були лікарні та інші організації охорони здоров'я з появою пандемії. Через такі атаки великим і дрібним компаніям довелося закритися. Ті, хто змогли пережити атаки, екстрено впроваджували нові стратегії щодо захисту даних. Але, як показує практика, швидкі рішення в сфері кіберзахисту можуть привести до виникнення нових вразливостей в системі [17].

Водночас, світова практика підтверджує, що впровадження фінтеху є цікавим як безпосередньо розробникам продукту-стартапам, так і банківським установам. Найбільшу вигоду від його розвитку мають клієнти банківських та небанківських установ. Однією із основних причин стрімкого поширення фінтеху в Україні стала фінансова криза 2008 р., внаслідок чого значно скоротилась кількість працюючих банків, ці тренди продовжились зокрема у 2015–2019 рр. Відповідно, зросло навантаження на діючі банки зі сторони юридичних та фізичних осіб. У свою чергу, виникла потреба у певній альтернативі традиційним фінансовим послугам. Це змусило клієнтів банків віддавати перевагу дистанційному доступу до банківських операцій (перекази коштів, офердрафт-кредити на банківську картку), з другої сторони, змусило банки змінювати технології й підходи для забезпечення кінцевого позитивного фінансового результату.

Рис. 2. Кількість кібератак (млн) та збитки від кібератак (млрд дол. США) за 2005–2020 рр. у світі

Джерело: побудовано авторами на основі [17]

Неоднозначну роль у стрімкому зростанні фінтех-сектору зіграла світова криза, зумовлена пандемією короновірусу у світі й Україні. Згідно зі статистикою Mastercard, у першому кварталі 2020 року українці почали розраховуватися на 7% частіше безконтактно і на 8% частіше онлайн. Кількість оплат в e-commerce також зросла на 8%. Рітейл почав ще більш активно освоювати і використовувати діджитал-канали для продажів: кількість онлайн-оплат у продуктовому ритейлі по картках Mastercard зросла на 12% за вказаний період, купівля техніки і електроніки – на 44% [15]. Самі ці започатковані тренди в частині переходу до безготівкової економіки та діджиталізації послуг, вважаємо, повинні стати підґрунтям оздоровлення фінтех-сектору та фінансового ринку України в цілому. Певна безвихідь як зі сторони надавачів послуг, так і клієнтів у зв'язку із пандемією та в період відновлення, вочевидь відіграє позитивну роль і дасть змогу значно пришвидшити процес цифровізації національної економіки, який був би за попередніх умов суттєво повільнішим. Однак такі швидкі темпи діджиталізації формують нові виклики в частині управління ризиками у фінансовому секторі й потребують у першу чергу від фінансових установ й надавачів послуг оперативної роботи й реакції на кіберзагрози й махінації, що почастішали в Україні у 2020–2021 рр.

Потрібно відзначити, що кінцевою метою реалізації згаданої вище Стратегії розвитку фінтеху в Україні до 2025 року є створення повноцінної фінтех-системи з інноваційними фінансовими сервісами та доступними цифровими послугами. Результатом впровадження Стратегії розвитку фінтеху має бути [14]: більшість гравців ринку перейдуть на стандарти відкритого банкінгу та інструменти віддаленої ідентифікації та верифікації; кількість безготівкових платежів – 85%; кількість протестованих у запущеній регуляторій пісочниці інноваційних продуктів – в межах 16–20 на рік; збалансований розвиток усіх ніш фінтеху; поширене використання інноваційних технологій у наглядових та регуляторних процесах; входження Національного банку України до «глобальної пісочниці» – Глобальної мережі фінансових інновацій (GFIN); розвинуте академічне середовище з підготовки спеціалістів з цифрових фінансів.

У цьому аспекті актуальним питанням є визначення основних проблем розвитку фінансового сектору з метою обґрунтування конкретних механізмів та інструментів реалізації сформульованих у згаданій стратегії пріоритетів. Адже фінансові аналітики зазначають, що ключова проблема банківської системи України – це дефіцит довіри клієнтів, зокрема громадян, що пов'язано із економічною нестабільністю та банкрутством багатьох банків упродовж 2015–2020 рр. При цьому на неприпустимо низькому рівні є рівень довіри до небанківських фінансових посередників. У свою чергу ризик полягає в тому, що цифровізація поступово «стирає» будь-які межі між власне банківською діяльністю та роботою небанківських фінансових посередників. Більше того, саме небанківське бізнес-середовище швидше пристосовується до змін у використанні платіжних інструментів, необхідності надання послуг принципово нової якості, що часто є непосильним для традиційного банківського сектору у зв'язку із громіздкими апаратами управління й довготривалими процедурами ухвалення рішень у банках. З іншого боку, потужні банки мають, як правило, більші фінансові ресурси для того, щоб адаптуватись до нових стандартів якості, водночас вони в змозі профінансувати роботу відповідних підрозділів із кіберзахисту та сформувати ефективну систему управління ризиками.

Упродовж 2019–2020 рр. різні фахівці усе частіше з-поміж ключових проблем розвитку фінансового сектору виділяють зростання рівня кіберзлочинності. Кібератаки є основною причиною значних фінансових втрат, особливо для банків. Якщо проводити аналіз програмних продуктів-вірусів, які завдали найбільших збитків малому та середньому бізнесу в 2017–2019 рр., як в Україні, так і в світі, то можна виділити наступні кіберзагрози (табл. 1).

Таблиця 1

Топ-10 кіберризиків у 2017–2019 роках в Україні

№	Назва	Опис
1	Petya	програма-вимагач, яка шифрує дані
2	Blueborne	вразливість – у протоколі Bluetooth
3	NotPetya	програма, яка знищує дані на ПК
4	Wannacry	програма-шифрувальник, що вимагає викуп за дешифрування
5	KRACK	критична уразливість мереж Wi-Fi
6	EternalBlue	програма для одержання віддаленого доступу до системи
7	Bad rabbit	вірус-шифрувальник, розроблений для ОС сімейства Windows
8	Loki / Locky	Android-шкідливий / шифрувальник Windows
9	Reaper	вірус, спрямований на IoT-пристрої
10	Критична вразливість у доступі під root користувачем в MacOS	

Джерело: систематизовано на основі [16]

Тому кібербезпека має бути стратегічним пріоритетом в контексті підвищення стійкості фінансових систем, при цьому її забезпеченням мають займатись комплексно як на загальнодержавному, тобто інституційному рівні, так і на рівні конкретних підприємницьких структур, а також в частині формування цифрової грамотності.

Зокрема, в Україні активно розвиваються фінансові інститути, які пропонують банківські послуги на основі мобільних додатків та через інтернет (всі великі банки дають змогу клієнтам користуватись інтернет-банкінгом: privat24, my.ukrsibbank, web-банкінг «Ощад 24/7»). Саме вони стикаються дедалі частіше з проникненням шкідливих програм, випадками фішингу і шахрайських дій. При цьому загалом в Україні немає високоякісної системи управління інформаційною безпекою. Розуміння необхідності цього у контексті забезпечення національної безпеки в цілому з'явилось на інституційному рівні порівняно недавно, відтак є загрози того, що українські банки можуть стати «майданчиком» для апробації вірусів з боку кібер-злочинності. Створені департаменти і інші структурні підрозділи для кіберзахисту, зокрема в структурі Міністерства внутрішніх справ, поки що не справляються із власними функціями та не в змозі оперативно реагувати на загрози. Водночас, потрібно відзначити, що у 2021 р. в Україні створено Бюро економічної безпеки України, що відповідатиме за боротьбу з економічними злочинами. Відтак, координація дій між Бюро, МВС, іншими інституціями сприятиме зміцненню національної безпеки країни у тому числі у напрямі стримування кібер-злочинності.

Згідно національного індексу кібербезпеки (National Cybersecurity Index), Україна у 2020 році піднялась на 4 позиції порівняно з 2019 р. та зайняла 25 місце з 160 країн [19]. Під час розробки даного рейтингу експерти аналізували напрямки та показники, зазначені в табл. 2.

Таблиця 2

Україна у Національному індексі кібербезпеки 2020

Основні напрямки	Оцінка України у 2020 році	Максимальна оцінка
1. Загальні показники кібербезпеки		
Розробка законодавства у сфері кібербезпеки	7	7
Аналіз кіберінцидентів	4	5
Освіта у сфері кібербезпеки	8	9
Внесок у глобальну кібербезпеку	2	6
2. Базові показники кібербезпеки		
Забезпечення захисту цифрових послуг	1	5
Забезпечення захисту основних послуг	5	6
Електронна ідентифікація та довірчі послуги	8	9
Захист персональних даних	4	4
3. Показники управління інцидентами		
Заходи із реагування на кіберінциденти	4	5
Заходи із керування на кіберінциденти	0	5
Боротьба із кіберзлочинністю	9	9
Військові кібер-операції	1	6

Джерело: складено авторами на основі [19]

Покращити позиції Україні вдалося завдяки ухваленим протягом останнього року законодавчим актам у галузі кібербезпеки та кіберзахисту. Так, прийнята НБУ Постанова «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України», що визнає інформаційну безпеку як складову операційного ризику, котрий впливає на діяльність банку, стан його капіталу та якість менеджменту банку при визначенні рейтингової оцінки, беззаперечно, відповідає світовим стандартам ведення банківського бізнесу, але навряд чи стане дієвим інструментом практичного захисту особистої інформації клієнтів та фінансових даних самих банків [11]. При цьому під власне інформаційною безпекою розуміють багаторівневу систему збору, зберігання, обробки, передачі та захисту інформації, що циркулює як у банку, так і зовні та може впливати на прийняття управлінських рішень відносно діяльності банку. У відповідності до значущості та наслідків розголошення інформацію можна умовно поділити на інформацію front-офісів та interior-офісів. Інформація front-офісів зосереджена на даних клієнтів, на кількості та сутності послуг, що надає банк як в установі, так і за допомогою мобільного чи інтернет-банкінгу. Інформація interior-офісів – це аналітичні дані, що безпосередньо стосуються діяльності самого банку: його фінансові звіти, посадові інструкції, специфіка відносин з різними клієнтами та контрагентами, фінансові плани, бюджети, стратегії розвитку та ін. Найчастіше ціллю кібер-атак є інформація front-офісів, за допомогою якої вони крадуть кошти клієнтів, тим самим наносячи шкоду не лише їм, але й репутації банку [8].

Важливою є адаптація зарубіжного досвіду управління кіберризиками. Так, відомий англійський фінансовий аналітик, віце-президент компанії Business Computing World UK Марк Рівз обґрунтував п'ять базових напрямів запобігання кібератакам на front-офіси, які можуть бути корисними і для українських фінустанов і компаній [18]:

1. Систематичне оцінювання ризиків онлайн-транзакцій на відповідність чуттєвості зміни інформації (тип клієнту, обсяг операції, якість обслуговування, мобільний засіб та ін.).
2. Підвищення стандартів аутентифікації інформації. Відмовитися від розповсюджених дворівневих методів ідентифікації прізвище-пароль на користь передових систем виявлення шахрайства на основі поведінки, які можуть автоматично виявляти транзакції або веб-сайт навігацій аномалії в реальному часі.
3. Застосування багаторівневого підходу до перевірки даних: нашарування різних, що доповнюють один одного технологій безпеки, таких, як сувора аутентифікація, поведінкове виявлення шахрайства поза зоною перевірки транзакції, мобільна перевірка справжності, розширена перевірка персоніфікації, SSL цифрові сертифікати.
4. Впровадження передових методів аутентифікації: перевірка мобільного на основі транзакцій, аутентифікації динамічних пристроїв – в тому числі одноразові сеансові куки і цифрові відбитки пальців та ін.
5. Підвищення рівня обізнаності та освіти клієнтів. Частину коштів банки повинні витрачати на розробку доступних освітніх проектів для своїх клієнтів. Це має подвійні наслідки: підвищення рівня безпеки та створення з клієнтами довготермінових партнерських відносин.

Ці підходи також можна застосовувати при захисті стратегічно важливої інформації для роботи банку та небанківських фінансових установ. Тобто, очевидним є акцент провідних зарубіжних фахівців на пріоритетах застосування технологій штучного інтелекту для ідентифікації випадків шахрайства, що вітчизняними фінустановами активно почали використовуватись лише упродовж останніх років. У свою чергу, проблеми цифрової грамотності також стали об'єктом уваги на загальнодержавному рівні по суті тільки у 2019–2020 рр. після створення Міністерства цифрової трансформації України. Отже, вважаємо, ці передові підходи у зарубіжній практиці повинні бути імплементовані у процесі формування механізмів управління кіберризиками у вітчизняній фінансовій системі.

Висновки з проведеного дослідження. Формування ефективної системи управління ризиками у фінансовому секторі України, враховуючи імплементацію цифрових технологій у всіх галузях і секторах економіки, має відбуватись у контексті загальнодержавних підходів до гарантування національної безпеки та базуватись на кращих зарубіжних практиках. Необхідно при цьому враховувати, що сучасні тенденції зміни фінансового середовища спричиняють ситуацію, коли загрози постійно розширюються, трансформуються, виникають принципово нові кіберризики та спостерігається кумулятивний ефект від їх впливу.

Управління кіберризиками, на наш погляд, повинно відбуватись у межах відповідного циклу, що має включати етапи ідентифікації, мінімізації, а також оцінки та моніторингу таких ризиків. При цьому запропоновано тлумачити «кіберризик» як ризик фінансових втрат (прямих і непрямих), повної або часткової зупинки діяльності, а також ймовірності завдання збитків (матеріальних і нематеріальних) приватним особам чи бізнесу. У дефініції зроблено акцент на різні наслідки кіберзагроз, зокрема не лише матеріальні й суто фінансові, але й на моральні й репутаційні.

Постпандемічне відновлення національної економіки буде неможливим без реалізації очікувань клієнтів щодо підвищення якості та адаптації до нових умов банківських й небанківських установ. Важливо, щоб кожен банк в Україні мав відповідні програмні продукти для упізнання, класифікації, прогнозування та стримування потенційних загроз. Така система має характеризуватись автоматизацією рішень з мінімальними можливостями ручного втручання, вбудованими передовими

аналітичними моделями, налагодженою співпрацею з клієнтами, стійкістю до зміни правової бази, а також до недобросовісної конкуренції. Передусім, на наш погляд, необхідно враховувати кращі зарубіжні практики в частині використання технологій штучного інтелекту для попередження випадків кіберзлочинів й розширення аналітичного інструментарію управління ризиками у фінансовому секторі.

Успішна діджиталізація фінансового простору України можлива за умови комплексних підходів до управління кіберризиками в державі. Окрім безпосереднього застосування конкретних інструментів такого управління банківськими й небанківськими установами, державою тощо, важливим у контексті гарантування національної безпеки у довгостроковій перспективі є підвищення рівня цифрової і власне фінансової грамотності громадян. Вирішення цієї проблеми можливе лише за умови інституційних зусиль і заходів на рівні держави із використанням потенціалу Міністерства цифрової трансформації України та злагодженої співпраці із бізнесом і громадським сектором. Необхідний рівень знань й розуміння нових можливостей матиме стратегічно важливе значення для подальшого розширення використання цифрових технологій в Україні та пришвидшить постпандемічне відновлення економіки.

Література

1. Алєксєєв М. М. Аналіз методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки. *Протиборство у кібернетичному просторі*. 2019. №1(34). С. 109-114.
2. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9. С. 421-427.
3. Бурячок В. Л., Толубко В. Б., Хорошко В. О. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.
4. Віннікова І. І., Марчук С. В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. *Східна Європа: економіка, бізнес та управління*. 2018. № 5(16). С. 110-114.
5. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук. праці. Київ : НІСД, 2016. 528 с.
6. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кібер-ризиків. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 3. С. 101-115.
7. Гаряга Л. О. Ризики фінансової безпеки в умовах цифровізації економіки. *Збірник наукових праць ΛΌГОΣ*. 2020. С. 47-48. DOI: 10.36074/21.08.2020.v1.18. URL: https://doi.org/10.36074/21.08.2020.v1.18 (дата звернення: 12.04.2021).
8. Гребенюк Н. О. Фінансова безпека банків: система розпізнавання загроз та усунення ризиків. *Вісник Харківського національного університету імені В. Н. Каразіна.* 2016. № 91. С. 53-64.
9. Демчишак Н. Б., Біленька В. А. Розвиток технологічних платформ як інструмент реалізації інноваційного потенціалу в Україні. *Економіка та суспільство*. 2018. № 16. С. 731-738.
10. Кібер-ризики: як розуміти та управляти. URL: https://10guards.com/ua/articles/cyber-risks/ (дата звернення: 12.04.2021).
11. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України : Постанова Правління НБУ від 28 жовтня 2010 року № 474. URL: https://zakon.rada.gov.ua/laws/show/v0474500-10#Text (дата звернення: 12.04.2021).
12. Про національну безпеку : Закон України від 21.06.2018 № 2469-VIII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.04.2021).
13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VI (зі змінами). URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.04.2021).
14. Стратегія розвитку фінансового сектору України до 2025 року. URL: https://mof.gov.ua/storage/files/Strategija_/financovogo_sectoru_ua.pdf (дата звернення: 12.04.2021).
15. Україна обирає цифрові та безконтактні оплати як найбільш зручні й безпечні – експерти Mastercard. URL: https://newsroom.mastercard.com/eu/uk/news briefs/online_contactless_payments/ (дата звернення: 12.04.2021).
16. Якушев В. Кібербезпека-2018: чого чекати бізнесу? URL: https://mind.ua/openmind/20180414-kiberbezpeka-2018-chogo-chekati-biznesu (дата звернення: 12.04.2021).
17. Canalys: Cybersecurity investment grows in 2020, but organizations face record data breaches. 2020. URL: https://www.canalys.com/newsroom/cybersecurity-investment-2020 (дата звернення: 12.04.2021).
18. Mark Reeves. Top 5 Security Practices for Financial Institutions to Defeat Online Identity Attacks. URL: https://www.entrust.com/top-5-security-practices-financial-institutions-defeat-online-identity-attacks/ (дата звернення: 12.04.2021).
19. NCSI. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 12.04.2021).
20. Pidkhomnyi O., Demchyshak N., Dropa Ya. Confidence as the national economy pricing factor: the case of Ukraine. *Espacios.* 2019. № 40(20). P. 21-22. URL: http://www.revistaespacios.com/a19v40n20/19402021.html (дата звернення: 12.04.2021).

21.Pidkhomnyi O., Demchyshak N., Dropa Ya. Population financial activity in the formation of indicators for public confidence level and shadow economy risks: the case of Ukraine. *Espacios.* 2019. № 40(38). P. 16-17. URL: https://www.revistaespacios.com/a19v40n38/19403816.html (дата звернення: 12.04.2021).

References

1. Aleksieiev, M.M. (2019), "Analysis of methodological approaches to the application of risk management technology in the field of cybersecurity", *Protyborstvo u kibernetychnomu prostori*, no. 1(34), pp. 109-114.

2. Bratiuk, V.P. (2015), "The essence of cybercrime and insurance protection against cyber risks in Ukraine", *Aktualni problemy ekonomiky*, no. 9, pp. 421-427.

3. Buriachok, V.L., Tolubko, V.B. and Khoroshko, V.O. (2015), *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* [Information and cybersecurity: social and technical aspect], high school textbook, DUT, Kyiv, Ukraine, 288 p.

4. Vinnikova, I.I. and Marchuk, S.V. (2018), "Cyber risks as one of the types of modern risks in the activities of small and medium-sized businesses and their management", *Skhidna Yevropa: ekonomika, biznes ta upravlinnia*, no. 5(16), pp. 110-114.

5. Vlasiuk, O.S. (2016), *Natsionalna bezpeka Ukrainy: evoliutsiia problem vnutrishnoi polityky : Vybrani naukovi pratsi* [National Security of Ukraine: the evolution of domestic policy problems: Selected Scientific Papers], NISD, Kyiv, Ukraine, 528 p.

6. Volosovych, S. and Klapkiv, L. (2018), "Determinants of the emergence and implementation of cyber risks", *Zovnishnia torhivlia: ekonomika, finansy, pravo*, no. 3, pp. 101-115.

7. Hariaha, L.O. (2020), "Risks of financial security in the conditions of digitalization of economy", *Zbirnyk naukovykh prats LOGOS*, pp. 47-48, DOI: 10.36074/21.08.2020.v1.18, available at: https://doi.org/10.36074/21.08.2020.v1.18 (access date April 12, 2021).

8. Hrebeniuk, N.O. (2016), "Financial security of banks: threat recognition and risk elimination system", *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina*, no. 91, pp. 53-64.

9. Demchyshak, N.B. and Bilenka, V.A. (2018), "Development of the technological platform as instrument of innovative potential implementation in Ukraine", *Ekonomika ta suspilstvo*, no. 16, pp. 731-738.

10."Cyber risks: how to understand and manage", available at: https://10guards.com/ua/articles/cyber-risks/ (access date April 12, 2021).

11.The National Bank of Ukraine (2010), Resolution of the Board of the NBU "On the entry into force of standards for information security management in the banking system of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/v0474500-10#Text (access date April 12, 2021).

12.The Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On National Security" dated 21.06.2018 no. 2469-VIII, available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text (access date April 12, 2021).

13.The Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On the basic principles of cybersecurity of Ukraine" dated 05.10.2017 no. 2163-VI, available at: http://zakon.rada.gov.ua/laws/show/2163-19 (access date April 12, 2021).

14."Strategy for the development of the financial sector of Ukraine until 2025", available at: https://mof.gov.ua/storage/files/Strategija_/financovogo_sectoru_ua.pdf (access date April 12, 2021).

15."Ukraine chooses digital and contactless payments as the most convenient and secure – Mastercard experts", available at: https://newsroom.mastercard.com/eu/uk/news briefs/online_contactless_payments/ (access date April 12, 2021).

16.Yakushev, V. "Cybersecurity-2018: what to expect from business?", available at: https://mind.ua/openmind/20180414-kiberbezpeka-2018-chogo-chekati-biznesu (access date April 12, 2021).

17.Canalys: Cybersecurity investment grows in 2020, but organizations face record data breaches, 2020, available at: https://www.canalys.com/newsroom/cybersecurity-investment-2020 (access date April 12, 2021).

18.Mark Reeves. Top 5 Security Practices for Financial Institutions to Defeat Online Identity Attacks, available at: https://www.entrust.com/top-5-security-practices-financial-institutions-defeat-online-identity-attacks/ (access date April 12, 2021).

19.NCSI, available at: https://ncsi.ega.ee/ncsi-index/ (access date April 12, 2021).

20.Pidkhomnyi, O., Demchyshak, N. and Dropa, Ya. (2019), "Confidence as the national economy pricing factor: the case of Ukraine", *Espacios,* no. 40(20), pp. 21-22, available at: http://www.revistaespacios.com/a19v40n20/19402021.html (access date April 12, 2021).

21.Pidkhomnyi, O., Demchyshak, N. and Dropa Ya. (2019), "Population financial activity in the formation of indicators for public confidence level and shadow economy risks: the case of Ukraine", *Espacios,* no. 40(38), pp. 16-17, available at: https://www.revistaespacios.com/a19v40n38/19403816.html (access date April 12, 2021).