правильно спрямовані фінансові інновації можуть стати потужним каталізатором для сталого економічного зростання та розвитку.

Список використаних джерел:

1. Бондар Ю.А., Легінькова Н.І. Інноваційні аспекти розвитку економіки. *Конкурентоспроможна модель інноваційного розвитку економіки України:* матеріали Міжнар. наук.-практ. конф., 14 квіт. 2020 р. Кропивницький, 2020. С. 71-73. https://www.kntu.kr.ua/doc/science/zahody/vikl/2020/2-tez.pdf; 2. Колінець Л.Б. Теоретичні концепти світового фінансового порядку. Інтелект XXI. 2017. № 2. С. 18–25; 3. Пантєлєєва Н.М. Фінансові інновації в умовах цифровізації економіки: тенденції, виклики та загрози. Приазовський економічний вісник. 2017. № 3. С. 68–73. URL: http://pev.kpu.zp.ua/journals/2017/3_03_uk/17.pdf

Буз А.О., здобувач вищої освіти ступеня доктора філософії [*]
Київський національний університет імені Тараса Шевченка,
м. Київ, Україна

Кіберризики як іманентна детермінанта атрибутів сучасних фінансових систем: приклад Сполучених Штатів Америки

Концепція кіберризику, яка відноситься до потенційних фінансових втрат через залежність від комп'ютерних систем та цифрових технологій, стає все більш помітною у фінансовому секторі. Кіберінциденти, особливо кібератаки, постійно ідентифікуються як основні ризики у дослідженнях, що оцінюють фінансову стабільність (ФС) як у США, так і в усьому світі [1]. Подібно до інших вразливостей у фінансовій сфері, кіберризики викликають стурбованість як на мікро-, так і на макрорівні. Незважаючи на значну увагу підвищенню технічної стійкості до кіберзагроз, оцінка наслідків кіберризиків для фінансової системи залишається на початковій стадії. Оскільки фінансова система зазнає дедалі більшої цифровізації, відповідно зростає і поширеність кіберризиків, про що свідчить зростання кіберінцидентів. Ця тенденція висунула на перший план відмітні характеристики кіберризику та його потенціал вплинути на ФС. Розуміння вразливостей ФС, що виникають в результаті кіберподій, має першорядне значення, враховуючи, що традиційні механізми, такі як капітал та ліквідність, не можуть пом'якшувати наслідки кіберподій так само ефективно, як вони зменшують фінансові втрати. Наприклад, хоча капітал і ліквідність можуть надати фінансові ресурси для усунення кіберінциденту, вони не можуть прискорити відновлення систем або даних.

Кіберризик схильний до прояву системних наслідків із більшою готовністю, ніж операційний ризик загалом [2]. Після кібершоку такі сценарії, як екстрені розпродажі активів, обмеження ліквідності та потенційні проблеми з

[*] Науковий керівник – Циганов С.А., д-р екон. наук, професор.

платоспроможністю можуть розвиватися по-іншому. Наприклад, якщо кіберподія ставить під загрозу дані фінансової установи, її здатність виконувати зобов'язання перед кредиторами може бути порушена. Хоча неможливість зняти кошти може пом'якшити наслідки вилучення коштів з банку для постраждалої установи, клієнти можуть ініціювати вилучення коштів з інших установ через побоювання щодо доступу до їхніх рахунків. Досягнення у наданні послуг, такі як продовження годин роботи платіжних систем та скорочення інтервалів клірингу та розрахунків, скоротили інтервали, доступні для відновлення операцій після кіберінциденту. Переважання перезакладання (вторинної, або повторної іпотеки) та використання складніших деривативів означає, що більший обсяг транзакцій залежить від миттєвого розповсюдження інформації. Неясність щодо характеру та масштабів кіберінциденту може спровокувати масові вилучення («набіги») у контрагентів, конкурентів чи незачеплених сегментах діяльності фірми. Атака програми-вимагача на Colonial Pipeline в 2021 році, хоч і не була націлена на фінансову організацію, ілюструє, як кібератака може спровокувати каскад подій (в даному випадку набіг на заправні станції), посилюючи наслідки, які набагато перевершують початковий шок (у даному випадку, про розподіл палива) [3]. Ще одним відмінним аспектом кіберризику є його схильність поширюватися через складні і часто випущені з уваги взаємозв'язки всередині фінансової системи, що охоплюють різні фірми. Ці зв'язки спричиняють вплив загальних технологій та сторонніх постачальників послуг, являючи собою додатковий рівень крім більш традиційних зв’язків, що встановлюються за допомогою фінансових платежів та ризиків, які зазвичай оцінюються за допомогою показників ризику контрагента [4].

Ескалація концентрації ринку, викликана цифровою економією за рахунок масштабу або іншої ринкової динаміки, може призвести до виникнення одиничних або майже поодиноких точок збою, підвищуючи сприйнятливість фінансової системи до кібершоків. Наприклад, зростаюча концентрація банківського сектора США означає, що все більша кількість банківських ринків та продуктів обслуговується відносно невеликою кількістю банків. Крім того, феномен цифрової консолідації та супутні йому ризики помітні у наданні таких найважливіших послуг, як казначейський кліринг та розрахунки, а також у наданні хмарних послуг. Підвищений обсяг транзакцій, які проводяться через центральних клірингових контрагентів (ЦКА), також посилює ризик концентрації. Хоча ЦКА пом'якшили деякі вразливості, помітні під час фінансової кризи 2008-2009 років, за рахунок підвищення транспарентності та взаємозаліку, що супроводжується ефективністю капіталу та ліквідності, вони можуть одночасно підвищити кібервразливість за рахунок централізації діяльності в межах однієї організації, залежно від обсягу інвестицій у кіберстійкість [5]. Незважаючи на значні інвестиції у стійкість, фінансова система, як і раніше, схильна до кібератак, особливо у сценаріях, де скорочення штатів є недостатнім, що підкреслює вирішальну невідповідність між кіберризиками та іншими загрозами ФС – потенційний навмисний характер кіберподій. Хоча більшість кіберінцидентів, свідками яких стала фінансова система США, наприклад, досі були мотивовані отриманням прибутку,

зловмисники, які виношують зловмисні наміри, можуть вибірково атакувати одну або кілька фірм або критично важливі компоненти інфраструктури, стратегічно розраховуючи свої атаки на використання вразливостей і викликати системні наслідки.

Тим не менш, існують паралелі між кібершоками та іншими збоями у фінансовій системі. Кіберінциденти можуть призвести до одночасних втрат у кількох компаніях через взаємопов'язані ризики, які часто називають «ефектом попкорну», прикладом якого є випадки, коли кілька фірм встановлюють одне і те ж заражене шкідливим програмним забезпеченням (ПЗ) стороннє оновлення ПЗ. Понад те, взаємопов'язаність, властива фінансовій системі, означає, що збої у роботі однієї чи кількох фірм можуть поширитися інші, що відоме як «ефект доміно». Наприклад, кіберподія, що торкнулася одного банку, може порушити його здатність виконувати платежі, викликаючи каскадний вплив на ліквідність та операції інших банків. Нарешті, окремі фірми, зокрема які входять у ланцюжок поставок, можуть недостатньо інвестувати у власну стійкість, не зумівши повністю усвідомити наслідки своїх дій для стабільності системи і цим піднімаючи системний ризик за межі оптимального рівня.

Система моніторингу ФС, встановлена Федеральною резервною системою (ФРС), розмежовує шоки (потрясіння) та вразливості фінансової системи. У цьому контексті шоки відносяться до раптових і, як правило, непередбачених змін у фінансових або економічних умовах, тоді як уразливості розвиваються поступово з часом і є аспектами фінансової системи, які схильні викликати проблеми в періоди стресу [3]. Потрясіння, пов'язані з кіберризиками, виявляються у вигляді кіберподій — інцидентів, що відбуваються в інформаційній системі чи мережі, незалежно від того, чи вони є зловмисними чи ні. Ці події можуть виникати як ззовні, і всередині. Подібно до будь-якого економічного чи фінансового шоку, кіберподія не обов'язково впливає на ФС. Більшості кіберзлочинів, спрямованих проти фінансових установ, запобігають суворі заходи контролю та захисту, такі як регулярні оновлення ПЗ та надійні мережеві брандмауери. Щоб кіберподія становила загрозу ФС, вона повинна використовувати вразливості на рівні компанії, тим самим переходячи від події до інциденту, що завдає шкоди фірмі. Вразливості на рівні компанії включають слабкі місця в інфраструктурі кібербезпеки компанії і її здатність відновлюватися після кіберподії до того, як буде завдано істотних збитків [4]. Потенційні несприятливі наслідки лише на рівні компанії включають фінансову втрату чи втрату даних, пошкодження даних, збої у роботі і пов'язані з цим грошові чи репутаційні витрати.

Уразливості на рівні системи відносяться до характеристик фінансової системи, які можуть посилити та поширити кіберінцидент, що призведе до збоїв у роботі системи. Приклади таких вразливостей включають взаємопов'язаність, що виникає через фінансові та цифрові ризики, залежність від даних та операцій, ринки, в яких домінують кілька ключових гравців з обмеженими альтернативами для критично важливих послуг, чутливість платіжних процесів до часу та ступінь довіри у фінансових відносинах. Кіберінциденти, здатні суттєво порушити функціонування фінансової системи, справді можуть поставити під загрозу ФС.

Потенційні наслідки включають відсутність чи недоступність найважливіших послуг, даних чи фінансування; зниження довіри, що веде до втечі та розпродажу активів; або збої в потоках платежів чи механізмах визначення цін. Навіть менш серйозні кіберінциденти можуть вплинути на ФС, взаємодіючи та посилюючи інші уразливості фінансової системи, такі як кредитне плече та ризики [5]. Цей сценарій ще більше посилюється потенційно навмисним характером кіберподій.

Є два найважливіші аспекти кіберризиків і ФС, які також заслуговують на розгляд. По-перше, ФРС займає ключову позицію на фінансових ринках та в платіжній системі, забезпечуючи необхідну інфраструктуру, що підтримує і те, й інше. Отже, будь-які операційні збої, у тому числі спричинені кіберподіями, можуть завдати значної шкоди. По-друге, вразливість ФС може виникнути в результаті технологічних інновацій. Оскільки криптовалюти та інші фінтех-рішення продовжують розвиватися, можуть виникнути нові наслідки для ФС через підвищену залежність від технологій та потенційне скорочення надмірності — факторів, які потребують ретельного вивчення. Крім того, слід врахувати дискусію навколо зусиль компаній і галузі, спрямованих на зниження кіберризиків, які можуть не бути безпосередньо пов'язані з проблемами ФС, незважаючи на те, що вони сприяють зниженню кібервразливості [2]. Наприклад, мікропруденційна політика може сприяти зниженню кіберризиків, а боротьбі з кіберризиками приділяється значна увага органів нагляду. Крім того, різні галузеві групи поряд з офіційними регулюючими органами беруть активну участь в обміні інформацією про кіберінциденти і співпрацюють у реагуванні на зниження пов'язаних з ними ризиків.

Отже, вищенаведений аналіз дає три основні висновки: по-перше, кіберризики можуть бути інтегровані у структуру ФС національних центральних банків, але традиційні засоби зниження ризику, такі як капітал та ліквідність, можуть вимагати додаткових заходів для стримування системних наслідків кібершоків. По-друге, необхідні подальші дослідження, щоб зрозуміти шляхи передачі кібервразливостей та визначити ефективні засоби їх пом'якшення. Значні проґалини в даних ускладнюють оцінку та пом'якшення кібервразливостей як усередині самої фінансової системи, так і серед її постачальників послуг. Хоча підвищення стійкості окремих фірм до кіберзагроз, як і раніше, має вирішальне значення, ми наголошуємо на важливості вирішення проблем кіберризиків у контексті ФС та їх потенційного посилення через фінансову систему, а не зосередження уваги виключно на мікропруденційному нагляді. Разом з тим, спільні зусилля в рамках офіційного сектору, а також партнерські відносини за участю промисловості та наукових кіл відіграють вирішальну роль у покращенні розуміння системних аспектів кіберризиків. Координаційні прагнення сприяють глибшому розумінню того, як кіберподії можуть посилюватися у фінансовій системі, та потенційних шляхів пом'якшення їх побічних ефектів, особливо в контексті валютної інтернаціоналізації та значущості для світової економіки таких міжнародних валют як долар США зокрема. Така співпраця сприяє виробленню комплексного підходу до вирішення проблем кіберризиків та підвищення стійкості фінансового сектора.

Список використаних джерел

1. Bank of Canada (Banque du Canada). Financial System Survey highlights – 2023. Ottawa: Bank of Canada, 2023. URL: https://www.bankofcanada.ca/2023/05/financial-system-survey-highlights-2023/; 2. Afonso G., Curti F., Mihov A. Coming to Terms with Operational Risk. *Liberty Street Economics*, Federal Reserve Bank of New York, 2019. URL: https://libertystreeteconomics.newyorkfed.org; 3. Implications of Cyber Risk for Financial Stability / D. Brando та ін. *FEDS Notes.* 2022. Т. 2022, № 3077. URL: https://doi.org/10.17016/2380-7172.3077; 4. Bank of England. Systemic Risk Survey Results - 2023 H2. London: Bank of England, 2023. URL: https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h2; 5. Maurer T., Nelson A. The Global Cyber Threat. *Finance & Development.* 2021. № 1. URL: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

Валявка О. Я., Мельник Р. А., здобувачі вищої освіти ступеня доктора філософії*
Державний біотехнологічний університет, Україна

Логістичне забезпечення та цифрова трансформація агробізнесу: теоретичні аспекти

Система логістичного забезпечення агробізнесу в умовах євроінтеграції передбачає комплексну організацію процесів збору, зберігання, переробки та доставки сільськогосподарської продукції від виробника до кінцевого споживача з урахуванням вимог та стандартів Європейського Союзу [1, 2]. Це включає оптимізацію ланцюгів постачання, впровадження інноваційних технологій для зберігання та транспортування продукції, а також забезпечення якості і безпеки продуктів. Умови євроінтеграції вимагають від агробізнесу адаптації до норм і стандартів ЄС у сфері сільського господарства, зокрема, щодо застосування пестицидів, ветеринарних препаратів, стандартів якості продукції та екологічних норм. Також важливою є інтеграція інформаційних систем для управління логістикою, що дозволяє здійснювати ефективний контроль за переміщенням товарів, а також забезпечувати прозорість і слідування всього ланцюга поставок від поля до столу споживача. Особлива увага в системі логістичного забезпечення агробізнесу приділяється питанням екологічної стійкості та відповідального використання природних ресурсів, що відповідає зростаючим вимогам європейських споживачів та законодавства. Це передбачає інвестиції в сучасні технології, розробку та впровадження інноваційних рішень для підвищення ефективності виробництва і логістики, а також зменшення впливу на довкілля. Таким чином, система логістичного забезпечення агробізнесу в умовах євроінтеграції є ключовим елементом для успішної конкуренції на

* Наукові керівники – А. В. Кучер, д-р екон. наук, старш. досл.; В. Є. Мещеряков, канд. екон. наук, доцент.