А саме: 1) як поширення технології сек'юритизації на сферу страхування і створення принципово нового типу сек'юритизації – сек'юритизації ризиків катастроф, що сприятиме збільшенню грошових потоків та ємності ринку; 2) новий механізм фінансування збитків, що зменшує навантаження на бюджет (емітентом можуть виступати державні установи); 3) як новий клас фінансових активів, що формує новий сегмент ІФР; 4) як можливий напрям розширення можливостей портфельної диверсифікації, оскільки його дохідність практично не корелює з ринками традиційних фінансових активів, крім того їх ціноутворення і ризик дефолту прямо не пов'язані з кредитним та процентним ризиком; 5) як екзотичний інструмент соціально-відповідальних інвестицій, оскільки їх різновидом є благодійні облігації катастроф. За даними Financial Times станом на початок вересня 2018 року загальний обсяг таких облігацій постійно зростає і досяг рівня у 30 млрд дол., а емісія за 2018 рік становила 11,08 млрд дол. США.

Цей спосіб, на нашу думку, буде все більше поширюватися на фінансовому ринку, враховуючи те, що він дозволяє інвестору диверсифікувати ризики. Вважаємо, що потреба в такому методі буде тільки зростати зважаючи на посилення турбелентності розвитку економіки, небезпеки шоків, особливо актуально в умовах коли посилюється ефект перетікання волатильності на фінансових ринках.

Перелік джерел посилання:

1. *Журнал Nature* [Електронний ресурс]. Режим доступу: http://www.nature.com/nclimate/journal/v6/n7/full/nclimate2972.html

2. Краснова І.В. Концепція сталого розвитку та вихід на ринки «сталих інвестицій. *Ринок цінних паперів України*. 2012. № 10. С. 17-24.

3. Kampa Ch. *Alternative Risk Transfer: The Convergence of The Insurance and Capital Markets*. A Three Part Series / ISI. 2010. 19th July. URL: http://www.insurancestudies.org/wp-content/uploads/2010/07/ISI_Insurance-Convergence-Series-Part-I.pdf

Лавренюк В.В.
к.е.н., доцент кафедри банківської справи та страхування
ДВНЗ «КНЕУ імені Вадима Гетьмана»

КЛЮЧОВІ ДРАЙВЕРИ КІБЕР-РИЗИКІВ ФІНАНСОВИХ УСТАНОВ

За останнє десятиліття високорозвинена ІТ-індустрія стала одним із найважливіших компонентів економіки та лежить в основі забезпечення економічного зростання. Організації будь-якого розміру, державного чи приватного сектору, стають все більше взаємопов'язаними та залежними від сучасних ІТ-продуктів і послуг, зокрема хмарних технологій. Це провокує підвищення схильності до кібер-ризиків, що вимагає відповідної адаптації політик ризик-менеджменту фінансових установ.

Лише віднедавна фінансові установи активно почали розвивати менеджмент кібер-ризиків та інвестувати у кібербезпеку. Проте існує проблема кількісної

оцінки кібер-збитків. Кібер-ризики у фінансовому секторі вже давно мають статус «відомих невідомих» хвостових ризиків та несуть суттєву загрозу фінансовій стабільності. Багато науковців вважають, що для окремих секторів економіки кібер-ризики можуть мати катастрофічні наслідки набуваючи системних характеристик, що автоматично переводить питання управління кібер-ризиками у площину національної безпеки [1, 2]. Однак, незважаючи на значну актуальність проблеми менеджменту кібер-ризиків, інформація щодо драйверів, збитковості та пом'якшуючих факторів кіберінцидентів досить обмежена.

Зазвичай, у широкому розумінні під кібер-ризиком розуміють «ймовірність фінансових витрат, порушень або збитків у результаті збоїв роботи IT-систем» [1, 2]. В українській банківській практиці немає чіткого визначення поняття «кібер-ризик», однак у Постанові НБУ №64 [3] є визначення інформаційного ризику та ризику інформаційно-комунікаційних технологій, як складових операційного ризику. Спільним у підходах до визначення кібер-ризику є акцент на кіберінцидентах (англ. cyber events, кібер-події), які передбачають зловмисні кібератаки, що можуть завдати значних збитків (атаки шахраїв, витік конфіденційної інформації, DoS-атаки тощо).

Частота кіберінцидентів зростала у геометричній прогресії до 2016 року, проте в останні 5 років спостерігається уповільнення динаміки. Це скорочення пояснюється збільшенням інвестицій у кібербезпеку, однак необхідно враховувати і часовий лаг пов'язаний із розкриттям відповідної інформації щодо кібер-інцидентів (в т.ч. звітування). Водночас середня збитковість кібер-подій постійно зростала протягом останніх 10 років [1, 2]. Зауважимо, що певні сектори економіки виявляють більшу стійкість до кіберінцидентів, наприклад, фінансовий сектор зазнав вищої частоти кіберінцидентів, однак збитки від них були одними із найнижчих. Зокрема банки і страхові компанії несуть менші збитки у порівнянні з іншими учасниками фінансового ринку, у більшості випадків через посилене регулювання діяльності і вищі інвестиції у власну кібербезпеку.

Багато науковців практиків доходять висновку, що збитки від кіберінцидентів залежать від *розміру та бізнес-моделі фінансової установи*. Розмір фінансової установи позитивно корелює із розміром її операційних збитків (в т. ч. збитків від кібер-ризиків). Специфіка бізнес-моделі, а також і операційної моделі впливає на схильність до ризику (ризик-апетит) фінансової установи. Це пояснюється тим, що: 1) збитки сильно залежать від масштабу діяльності, видів, складності операцій фінансової установи; 2) великі за розміром установи мають відповідну інституційну складність і взаємопов'язаність; 3) можливе нарощення морального ризику, що є наслідком реалізацією принципу «too-big-to-fail».

Важливим драйвером кібер-ризиків є взаємопов'язаність між кіберінцидентами, що провокує ефект зараження. Кібер-події, які вплинули на певну кількість установ, можуть призвести до нарощення обсягу збитків в абсолютному виразі. Однак, за достатньо ефективного рівня ризик-менеджменту та наявності відповідних буферів безпеки, витрати можуть бути розподілені рівномірно між «ураженими» установами.

Особливу увагу серед драйверів кібер-ризиків займають саме *зловмисні* за характером події. В цілому кіберінциденти передбачають широкий набір подій,

які можна поділити на: зловмисні та стохастичні (випадкові, що не мають злого умислу). Серед великої кількості науковців існує припущення, що зловмисні кіберінциденти несуть більші та масштабніші збитки, на відміну від ненавмисних (без злого умислу) [2]. З іншого боку, інформація щодо особливостей більшості зловмисних кібер-інцидентів поширюється засобами ЗМІ та постійно вивчається спеціалістами із кібербезпеки. З огляду на це, відповідне програмне забезпечення здатне протистояти відомим, зловмисним кіберінцидентам. У такому ракурсі, стохастичні кібер-інциденти (баги, технічні збої, ненавмисні помилки персоналу тощо) можуть нести більші збитки. До ключових інцидентів, що підвищують концентрацію кібер-ризиків можна віднести: 1) інциденти щодо порушення безпеки (несуть загрозу або порушують роботу ІТ-систем (конкретних комп'ютерів, комп'ютерних мереж)); 2) інциденти витоку корпоративних даних (навмисне / ненавмисне розголошення інформації (випадкове публічне розголошення конфіденційних даних клієнтів, неналежне відчуження інформації тощо) та/або крадіжка техніки, що містить персональну інформацію співробітників / клієнтів; 3) інциденти імплементації ІТ-систем (несправне обладнання або програмне забезпечення, що призводить до збоїв і збитків); 4) інциденти фішингу /скіммінгу (відправка електронних листів, отриманих від авторитетних компаній, з метою отримання конфіденційної, таємної або службової інформації); 5) інциденти порушення конфіденційності (несанкціонований збір даних телефонів, GPS-пристроїв, файлів cookie, веб-браузингу або фізичного переміщення); 6) інші кіберінциденти (пов'язані із збитками події, що не відносяться до попередніх категорій).

В останні роки популярності в усіх сферах почала набувати технологія блокчейн. Пов'язані з нею види діяльності, мають обмежене регулювання та пов'язані із підвищеними збитками. Віднедавна, спостерігається позитивна кореляція між ціною біткоїна та інтенсивністю впровадження пов'язаних з блокчейн кіберзаходами. Зі стрімким зростанням ціни на біткоїн у 2020-2021 рр. з'явився підвищений стимул кібератак на криптобіржі, оскільки саме вони є найвразливішим структурним елементом екосистеми обігу криптоактивів. Саме тому посилення регулювання діяльності фінансових посередників, які працюють на ринках криптоактивів є необхідним, так як очікувані збитки від кібер-ризиків є найвищими або й взагалі катастрофічними.

В цілому розвиток технологічних навичок допомагає фінансовим установам мінімізувати збитки за кібер-ризиками, а також більше опиратися не на власні ІТ-системи, а хмарні послуги спеціалізованих провайдерів. Однак і цей підхід має бути виваженим. Оскільки від міри інтеграції ІТ-систем до хмарних сервісів залежить рівень системної важливості провайдерів хмарних послуг, що може призвести до збільшення концентрації кібер-ризиків. Також, чиста вигода від впровадження хмарних технологій залежить від рівня взаємопов'язаності та масштабу куіберінцидентів.

Важливо зауважити, що досі не існує підходів до оцінки системних кібер-ризиків для різних секторів економіки. Результати таких досліджень могли б сприяти ефективності політик регулятора фінансового сектору щодо підвищення кіберстійкості. Посилення кіберстійкості в Україні повинно бути одним із

пріоритетних завдань для держави, бізнесу та суспільства і базуватися на власній експертизі та міжнародній співпраці. Значне порушення кіберстійкості може викликати кібер-кризу. Мінімізацію наслідків кібер-кризи можна звести до належного управління кіберінцидентами до, під час та після їхнього виникнення. Для стримування та управління кризовими ситуаціями необхідна координація численних функцій та вмінь спеціалістів і керівників різного рівня. Ефективна підготовка до кризи виходить за межі реагування на кіберінцидент і охоплює повний життєвий цикл управління кризою: готовність, реагування та відновлення. Під готовністю мається на увазі не лише цілодобовий моніторинг, але також і підготовка персоналу до діяльності під час інциденту чи кризи. Рішучі і скоординовані дії у відповідь на кібер-інцидент локалізують збої та збитки.

Отже, сучасне економіка характеризується стрімкою мінливістю різноманітних кібер-загроз, що є викликом для фінансових установ, фокус уваги яких не повинен обмежуватися лише шахрайством та крадіжками. Оскільки атаки стають дедалі більш організованими, спрямованими на припинення надання послуг, знищення даних, вимагання, то й і виклики, пов'язані з кібер-ризиками, стають більш складними. А штрафи, відшкодування збитків, втрата довіри та репутації стають частиною цього рівняння. Тому фінансовим установам необхідно постійно оцінювати кібер-ризики та інвестувати у кібербезпеку, що дозволить стримувати кіберінциденти, мінімізувати збитки і забезпечити належний рівень кіберстійкості.

Перелік джерел посилання:

1. Aldasoro I. & Gambacorta L. & Giudici P. & Leach T. Operational and cyber risks. Bank for International Settlements. BIS Working Papers №840. URL: https://www.bis.org/publ/work840.pdf

2. Aldasoro I. & Gambacorta L. & Giudici P. & Leach T. The drivers of cyber risk. Bank for International Settlements. BIS Working Papers №865. URL: https://www.bis.org/publ/work865.pdf

3. Постанова НБУ №64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах». Положення, Перелік, Класифікація від 11.06.2018 № 64. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18/print

4. Brenner J. 2017. Keeping America safe: Toward more secure networks for critical sectors. Report on a series of mit workshops. MIT Internet Policy Research Initiative.

Мартінович П.Г.
аспірант (PhD) ОНП «Економіка»,
Черкаський державний технологічний університет, м. Черкаси
Науковий керівник –д.е.н, професор,
завідувач кафедри економіки та управління
Манн Р.В.

ВПЛИВ СМАРТ-ЕКОНОМІКИ РЕГІОНІВ НА РОЗВИТОК УКРАЇНИ