Міністерство освіти і науки України

Національний університет «Києво-Могилянська академія»

Факультет економічних наук

Кафедра фінансів

Магістерська робота

ОСВІТНІЙ СТУПІНЬ - МАГІСТР

на тему: «**КІБЕР-РИЗИКИ У ФІНАНСОВИХ СИСТЕМАХ: АНАЛІЗ, ОЦІНКА ТА ПІДХОДИ ДО ЗАХИСТУ**»

Виконав: студент 2-го року навчання,
Спеціальності
072 «Фінанси, банківська справа та страхування»

Янченюк Василь Васильович

Керівник: Камінський А.Б.
доктор економічних наук, професор

Рецензент: Джалладова І. А.
(прізвище та ініціали)

Магістерська робота захищена

з оцінкою

«_____»

Секретар ЕК _____
«____» _____ 2021 р.

Київ 2021

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Розвиток сучасної економіки, заснованої на використанні новітніх цифрових технологій, створення нових матеріалів, аналізі великих масивів даних, розробці нових систем управління, призводить до зміни ланцюгів виробничих відносин.

Однак, незважаючи на безумовні переваги цифровізації економіки – поява Big Data, штучного інтелекту, технології блокчейну, хмарних обчислень з’являються і новітні ризики, генеровані їх використанням, що можуть негативно впливати на економічних суб’єктів та результати їхньої діяльності.

Фінансовий сектор особливо вразливий по відношенню до кібер-атаки. Фінансові організації є привабливими об'єктами для атак через їх найважливішу роль як посередників у русі грошових коштів. Кібератака на одну організацію може швидко поширитися через вельми взаємопов'язану фінансову систему. Багато організацій все ще користуються застарілими системами, які, можливо, не є стійкими по відношенню до кібератак. Кібератака може мати прямі істотні наслідки у вигляді фінансових збитків, а також непрямих витрат, таких як погіршення репутації. Однак, зважаючи на недостатню активність потенційних потерпілих від наслідків кібер-ризиків розгляд сучасного стану та детермінант розвитку менеджменту кібер-ризиками є актуальним напрямом наукових досліджень.

Мета й завдання дослідження. Метою роботи є виявлення, класифікація, оцінка впливу цифрових ризиків для фінансового сектору України загалом, також її інститутів; надання рекомендацій стосовного ефективного менеджменту кібер-загроз на різних інституційних рівнях.

Завдання дослідження відповідно до поставленої мети:

– розглянути класифікацію кібер-загроз та представити їх основні типи для фінансових інститутів та споживачів;

– оцінити негативний вплив кібер-загроз насамперед для фінансового сектора України, порівняти його з іншими секторами економіки;

– представити різні методики оцінення втрат від кібер-загроз, порівняти їх позитивні негативні сторони;

– виявити наукові підходи до визначення, класифікації характеристики кібер-безпеки;

– розкрити мету, завдання та принципи різних типів боротьби з кібер-ризиками;

Об'єктами дослідження є кібер-загрози фінансового сектору, їх кількісний абсолютний і відносний вимір;

Предметом дослідження є теоретичні, методичні та практичні аспекти оцінки цифрових загроз для фінансових інституцій глобально та для різних країн, насамперед України, її інфраструктури загалом.

Методи дослідження. Дослідження виконувалось із застосуванням економічного, системного і порівняльного методів аналізу та синтезу. При обробці фактичних даних використовувались розрахунково-аналітичні, графічні, економіко-математичні методи, наприклад, економетричні моделі: кореляційний аналіз, лінійна регресія, VAR, симулювання випадкових значень, експертні оцінки.

Інформаційними джерелами дослідження слугували монографічна література та періодичні видання, дані статистичних Інтернет-сайтів, присвячених кібер-ризикам, прогнози та експертні оцінки провідних фінансових аналітиків та експертів, статистичні та аналітичні матеріали Національного банку України, Державної служби статистики України Світового банку та МВФ, Банку міжнародних розрахунків.

Наукова новизна отриманих результатів. Основні положення, які формують наукову новизну дослідження, полягають у тому, що набуло подальшого розвитку:

– уточнення змісту «кібер-ризик» як ризику, поява якого зумовлена діяльністю на електронному ринку та використанням ІТ-технологій, ідентифікація його специфіки;

– уточнення системи економічних та неекономічних факторів, що впливають на схильність фінансових організацій та громадян до цифрових загроз;

– вимір негативного впливу понесених прямих та непрямих (репутаційних) фінансових збитків від цифрових загроз для української економіки, насамперед її фінансово-банківського сектору;

– методичний підхід до прийняття рішення про доцільність оптимального способу упередження кібер-ризиків.

Практичне значення отриманих результатів полягає в тому, що в умовах переходу фінансового сектора у цифрову сферу зросла роль ІТ-інфраструктури, якими користуються індивіди та організації, і відповідно, зріс вплив цифрових загроз. Дана робота покликана вказати на ці загрози, оцінити їх вплив, а також надати рекомендації, як інституціям фінансового сектору оптимально та ефективно убезпечувати себе, зазначено необхідність ефективного регуляції на урядування з боку різних державних інститутів

Структура роботи. Для розуміння основних рушійних сил та взаємодій у першому розділі визначено основні цифрові загрози, розглянуто складність підходів розуміння та аналізу ризиків цифрової економіки, розмежовано принциповий поділ на прямий та систематичний кібер-ризик. А також проаналізовано вплив цифрового способу передачі інформації на рівень безпечності операційного бізнесу. У другому розділі проаналізовано статистичні аналітичні дані, які використовуются для моделювання виміру впливу кібер-ризику на фінансовий та інші сектори економіки, методи які використовуються, а також їх основні результати. Проаналізовано діяльність Національного банку України у розрізі оцінки, інформування та регуляції кібер-ризиків для фінансової індустрії. У третьому розділі представлений кількісний

аналіз агрегованих втрат фінансового сектору, використовуючи макроекономічну таблицю «Витрати-випуск», експертні оцінки та економетричні розрахунки для розробки моделі оцінки кібер-втрат для економіки. Також надано низку рекомендацій, як фінансовим інституціям та їх регуляторах справлятись із прямим та систематичним кібер-ризиком. Закінчується робота висновками, списком використаних джерел та додатками

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА ІДЕНТИФІКАЦІЯ КІБЕР-РИЗИКІВ У ФІНАНСОВИХ СИСТЕМАХ

1.1 Цифровізація економіки як основа підсилення кібер-загроз

Новітні ІТ-технології спричинили виникнення Індустрії 4.0, коли відповідно до категорій Д. Львова і С. Глазьєва людство загалом та Україна зокрема рухаються від четвертого технологічного устрою («ключові чинники IV техноустрою, - сукупність зв'язаних виробництв, що мають єдиний технічний рівень і розвиваються синхронно, — двигун внутрішнього згорання, конвеєрне виробництво, дротяний телефонний зв'язок, ядро устрою — автомобілебудування, літакобудування, нафтохімія» [12, 19-22]) до вищих. Тобто ядром є електронна промисловість, обчислювальна техніка, програмне забезпечення, телекомунікації, роботобудування для 5-го та, наприклад, наноелектроніка, молекулярна і нанофотоніка, наноматеріали, біотехнологія для 6-го. Ключовим аспектом техноустроїв після 4-го є «цифровізація» (чи «диджиталізація»).

Поширення цифрової інфраструктури, такої, як мобільні пристрої, бездротові мережі, персональні комп’ютери, сприяє інтеграції їх також в економічне та суспільно-політичне життя усіх розвинених країн. Це сформувало нові стратегії розвитку міжнародної економіки. Високорозвинені країни та країни перехідної економіки останніми роками намагаються активно зменшити частку традиційної економіки за рахунок збільшення частки цифрової економіки.

У середині минулого століття виник термін “диджитал-економіка” (digital economy). «Цифрову економіку» (Digitaleconomy) запропонував бізнес-аналітик Дон Тапскот. Його визначення пояснює цифрову економіку як

економічну діяльність, яка визначається через мережеву свідомість (networked intelligence) та залежить від віртуальних технологій. [13] Диджитал-економіка зазвичай ототожнюється із економікою знань, інформаційною або мережевою. [14, с. 33-57]. На думку Г. Коломійця, слушною є позиція, згідно з якою в основі диджиталізації лежить інформація, а саме «оцифрування значних обсягів знань і даних, що зумовлює якісні зміни в поведінці суб'єктів господарювання». [15, с. 140] Тобто відбувається інтеграція реальних господарських відносин у віртуальний простір.

Цифровізація та інші форми технологічних інновацій перевертають уявлення про функціонування сучасних фінансових ринків, створюють нові можливості для їхніх гравців, але також і продукують виклики для традиційних фінансових індустрій та їхніх регуляторів, наприклад, виникнення peer-to-peer кредитування, цифрового краудфандингу та інвойсів, інших альтернативних форм позичкового капіталу, а також пов'язаних із ними ризиків. Поряд із вищеперерахованими новими моделями на кредитних ринках, цифрові технології суттєво змінюють традиційні. Наприклад Великі дані широко використовуються для кредитного скорингу мікрофінансовими організаціями, а також банками. Зрозуміло, що банки заходяться під пильнішим наглядом регуляторів.

Диджиталізаційні процеси посилили ефективність фінансових інституцій і посилили фінансову інклюзію, але також створили сукупність принципово нових, малозрозумілих загроз, які швидко виникли та набули найрізноманітніших форм. Одними із ключових загроз супроти фінансових інституцій стали кібер-атаки, які з кожними днем стають все більш звичними та все більш складними. Кожного дня ми чуємо про витоки даних, і найбільш схильними до кібер-атак є саме фінансові організації, відповідно до висновків компанії Verizon Enterprise. [16]

1.2 Кібер-ризики як специфічний вид операційно-технологічних ризиків

Якщо оцінювати кібер-ризики з точки зору інвестора, він є складовою частиною систематичного ризику. Інвестопедія характеризує систематичний, або ж недиверсифікований ризик, ризик волатильності, як притаманний цілому ринку або його сегменту. Цей тип ризику одночасно слабко прогнозований та такий, якого важко уникнути через диверсифікацію, а лише можна хеджувати [5]. Або, як визначає Фредерік Мишкін: «Систематичний ризик - це ймовірність раптового, зазвичай неочікуваного випадку, що збурює інформацію на фінансових ринках, робить їх нездатними направляти фонди грошових коштів тим гравцям, які характеризуються найкращою інвестиційною привабливістю». Кібер-ризики відносяться до операційного ризику відповідно до протоколів Базелю, та у випадку банків із 2004 року Базель 2 вимагає покриття цих ризиків капіталом. Макропруденційні практики НБУ визначають операційний ризик як «імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі інформаційних систем банку або внаслідок впливу зовнішніх факторів». У свою чергу кібер-ризик визначається західними науковцями як «операційні ризики стосовно інформаційних та технологічних активів, що загрожують компрометацією даних: втрата конфіденційності, цілісності та доступу інформації або інформаційних мереж» [9]. Під «конфіденційністю» мається на увазі нерозголошення приватної внутрішньої інформації третім сторонам, під «цілісністю» - неможливість неправомірного використання інформації та інформаційних систем, під «доступом» - використання інформації під час звичних операційних процесів. [10, с.6]

У ризик-менеджменті інформаційної безпеки ризик визначається як композиція наслідків та ймовірності настання цих наслідків, у свою чергу ймовірність це функція рівня загрози, простоти неправомірного використання вразливостей та очікуваних наслідків: [10, с.12]

$$\text{Ризик} = f(\text{Загроза}, \text{Вразливісті}, \text{Наслідки}) \quad (1)$$

У даному контексті фінансові організації схильні до кібер-ризику внаслідок широкого набору факторів. Емануель Копп [11] показує і доводить, що загрози для фінансової індустрії високі внаслідок кіберзлочинності, хактивізму, інтернет-шпіонажу. Вразливостей теж багато, адже сучасна фінансова система включає інституції, залежні на поєднуючих мережах (платіжні системи, електронна пошта, SWIFT). Наслідки полягають як у прямих фінансових втратах, так і іншими процесами, пов’язаними з компрометацією даних.

Історично вважалося, що політики та протоколи кібер-захисту були спрямовані насамперед на «захист даних інвесторів від компрометації» [2], тобто втрати конфіденційності, цілісності та доступу. На сьогоднішній день захист даних залишається надзвичайно важливим, але новим викликом менеджменту кібер-ризиків стали атаки на самі інформаційні мережі та шляхи, які поєднують банки, фонди, біржі клірингові і платіжні системи тощо Це в свою чергу підриває стабільність роботи ринків і занурює їх у хаос. Ось чому спеціалісти з кібер-захисту, наприклад із Департамету фінансових послуг Нью-Йорка стверджують, що «хакінг є потенційно екзистенційною загрозою, що несе хаос у фінансову активність користувачів послуг». [6]

Американський регулятор фінансових послуг FINRA (Financial Industry Regulatory Authority) визначає «трикутник ризик-менеджменту цифрових

загроз», куди входять ендогенні загрози (працівники фірми, які можуть скомпрометувати персональні чи конфіденційні дані,), екзогенні загрози, які виникають від взаємодії з контрагентами та сторонніми інформаційними системами та систематичний ризик; та зазначає, що хоча усі три «сторони трикутника» є однаково важливими, фірма має особливо увагу приділяти саме ендогенним на екзогенним загрозам. [2]

З іншого боку Айзебах [34] показує, що природа і характеристика кібер-ризику для банківської системи відрізняють від операційного ризику, звертаючи увагу на те, що операційний ризик часто призводить насамперед до «втечі вкладників» (ризику ліквідності), натомість негативний вплив кібер-ризику значною мірою стосується порушення цілісності та конфіденційності даних, що можуть мати інші наслідки крім звичайної «втечі вкладників».

1.3 Характеристика систематичного кібер-ризику

Одним із найважливіших аспектів регулювання кібер-безпекової системи як з боку суверенних урядів, так і наднаціональних органів є (недиверсифікований) систематичний кібер-ризик. Світовий економічний форум визначає цей ризик наступним чином: «ризик, що кібер-подія (атака) чи інша несприятлива подія спрямована на окремий елемент критичної інфраструктури екосистеми спричинить затримку, відмову, поломку або втрату, так що вплив поширюється не лише на даний окремий компонент, а каскадно на логічно зв’язані компоненти, і в результаті призводить до значних негативних ефектів на публічне благополуччя, економічну чи національну безпеку. Несприятливі економічні та безпекові ефекти від реалізованого систематичного ризику, як правило, зазвичай розглядаються як такі, що виникають від значних порушень до довіри або визначеності стосовного певних

послуг, або такі, які стосуються цілісності даних, порушення роботи (систем та мереж) та знищення матеріальних цінностей» [24] Для фінансових інституцій такий ризик виникає, адже вони використовують програмне забезпечення третіх сторін, наприклад, операційні системи чи хмарні сервіси, і відповідно ці інституції можуть піддаватись впливу недиверсифікованого ризику, тобто тієї частини кібер-ризику, яка не може бути подолана за допомогою внутрішніх процесів кібер-гігієни, тобто немає різниці, наскільки добре інституції управляють власним ідеосинкратичним ризиком (див. Рис. 1.1). Як наслідок зовнішні екстерналії, спричинені інформаційними асиметричностями та розбіжністю стимулів різних агентів, ведуть до недоінвестування у кібер-безпеку.

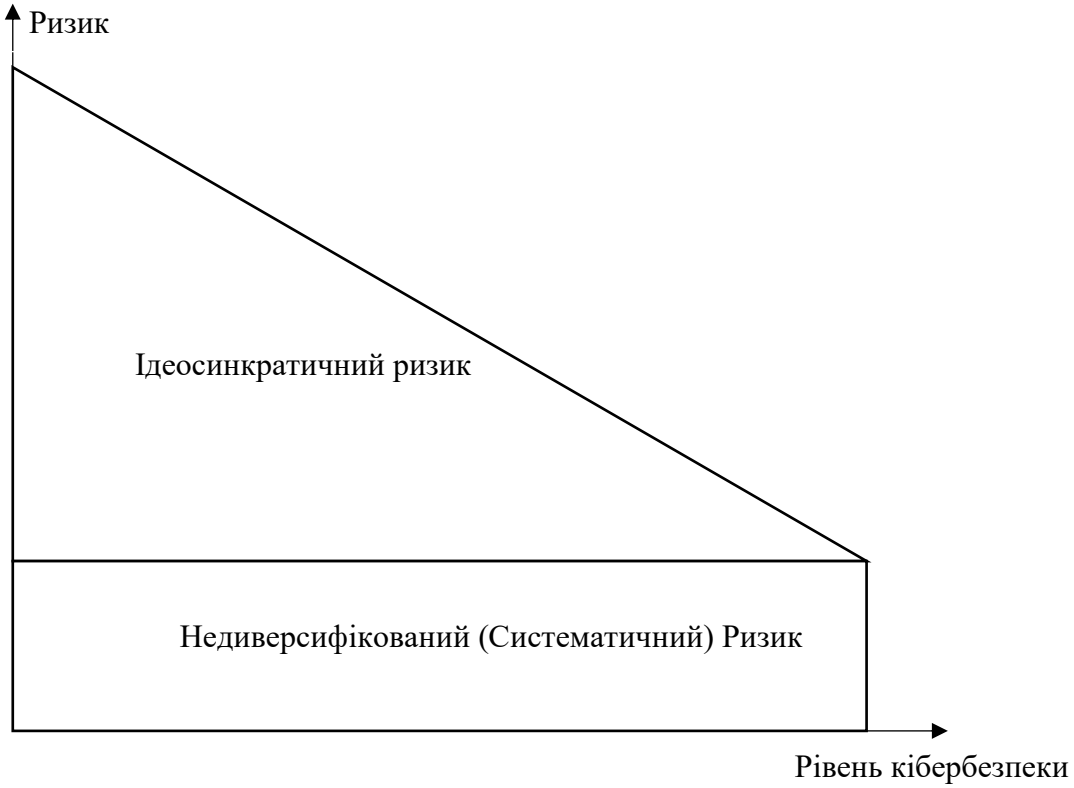

Рисунок 1.1 – Розподіл кібер-ризику для інституції на ідеосинкратичний та систематичний

Джерело: створено автором

Фінансові системи часто піддавалися кібер атаками, але багато хто має сумніви стосовно того, чи «тестувалась» стійкість фінансової системи у випадку значної широкомасштабної атаки. У той же час, так як зв’язок між кібер-середовищем та реальною економікою посилюється, - як і взаємозалежність та складність, - зростає також імовірність, що шок, який приймає фінансова система, стане системним. Окрім цього недостатня прозорість та доступність міжінституційних операцій та взаємозалежностей ускладнює оцінку ex-ante: насамперед кількісну оцінку системного кібер-ризику. Ба більше, даних недостатньо, і досить рідко кібер-ризик вимірюється з точки зору економічних втрат. Нарешті, методи моделювання, як ідеосинкратичного, так і систематичного ризику є менш прогресивними, ніж інші ризики, які покриваються, наприклад страхуванням, і потрібно провести складну роботу, щоб створити фундамент для даного моделювання.

Протягом довгого періоду часу кібер-ризик розглядався лише в його ідеосинкратичному прояві, нехтували його системною природою, яка випливає із взаємозалежності інституцій у сучасному кібер-просторі. Тобто внутрішні процеси ризик-менеджменту кібер-загроз мають бути розширені до охоплення тих ризиків, які походять від контр-агентів інституції та третіх сторін. На Рисунку 1.2 можна побачити джерела походження кібер-ризику та механізми його поширення. Під технологічними екстерналіями слід розуміти суміжні інфрастуктури: електропостачання, теле-, інтернет-комунікації, екосистема фінансових ринків тощо. Зрозуміло, що для конкретної бізнес одиниці можливості вплинути на такі процеси немає. Також до системних кібер-ризиків слід зараховувати нові проривні технології, які приходять на заміну старим, наприклад, нові покоління хмарних обчислень. Зовнішніми шоками можуть бути природні лиха та сучасні війни, відповідно вони потребують урядового

втручання для подолання. Такий системний кібер-ризик проявляється у одному із трьох сценаріїв:

- Сценарій операційного ризику високого ступеня впливу.
- Інфраструктурний сценарій.
- Сценарії зовнішнього шоку.

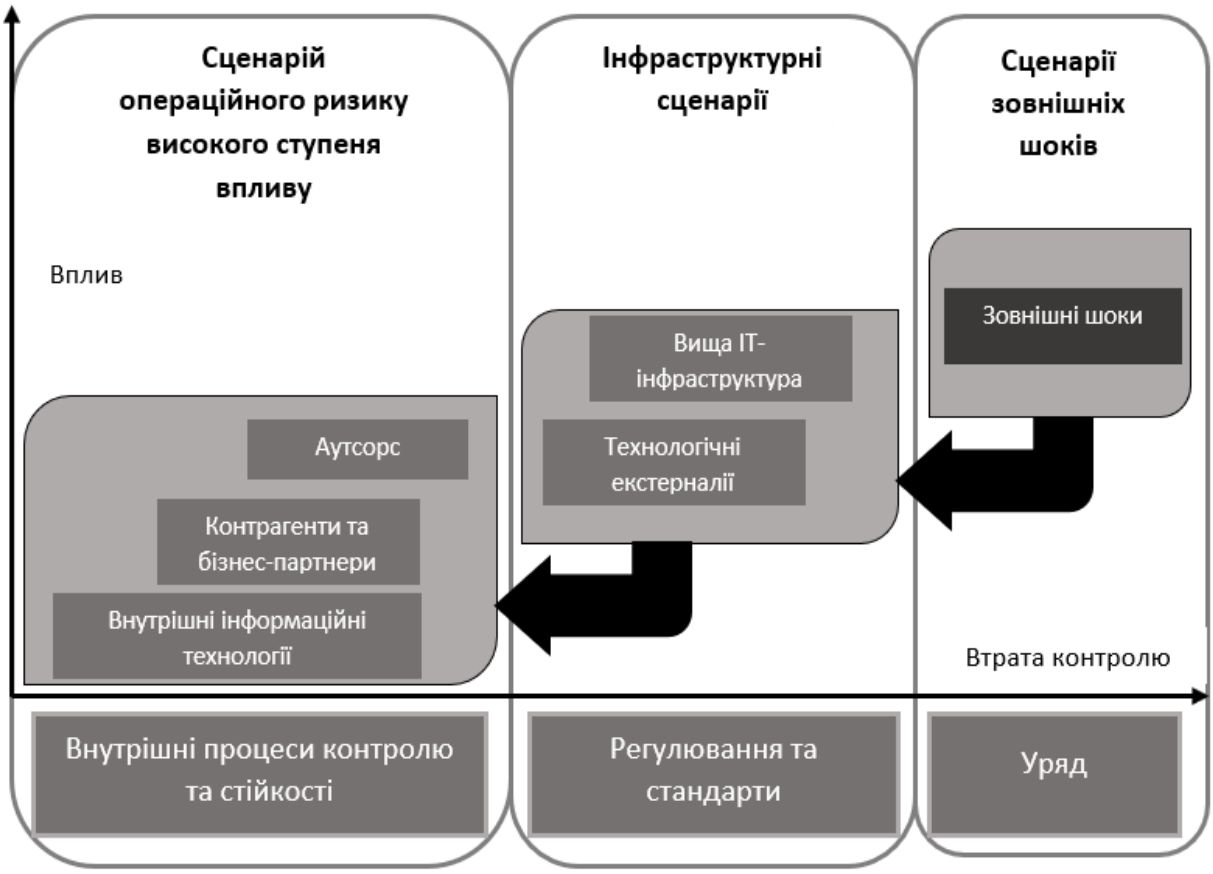

Рисунок 1.2 –Ключові сценарні типи кібер-ризику

Джерело: створено автором на основі [36]

Систематичний кібер-ризик слід зараховувати до системотворчих факторів фінансової стабільності. Наприклад, урядове бюро США «Офіс фінансових досліджень» зазначає, що такі головні трансмісійні механізми систематичного кібер-ризику як концентрація внаслідок недостатності замінності (одних інфрастуктур іншими), втрата довіри вналідок кореляцій ризиків, та підсилююча роль взаємозалежності (контагіозний ефект) можуть підірвати фінансову стабільність системи. [25]

- Ризик концентрації та недостатність можливості заміни. Систематичний кібер-ризик концентрується у ключових та системно важливих інституціїях ринкової інфраструктури: центральні клірингові платформи, SWIFT, найбільші банки та інші фонди фінансових ресурсів. Також мала кількість інституцій, особливо у розвинених ринках проводить левову частку усіх транзакцій через власні торгові системи. Наприклад, у дослідженні Айзенбаха засвідчено, що якщо 5 найбільших банків Америки зупинять свою діяльність на один операційний день, то це матиме ефект на 38 % банківської мережі і коштуватиме більше 210 млрд дол (більше ніж у 2.5 рази за одноденне ВВП). [34]
- Ризик кореляції та втрати довіри. Ідеосинкратичний кібер-шок на фінансову інституцію може спровокувати втрату довіри, відтік фондування, і, як наслідок, ризик ліквідності, ринковий ризик та ризик платоспроможності. Операційна неможливість прийняти платіж або розрахуватись по зобов'язанням може причинити кредитний ризик контрагента, - і далі по ланках фінансових взаємозв'язків. Шок ліквідності також може спонукати інституцію до продажу активів із значним дисконтом, що спричиняє переоцінку бізнесу ринком, зменшує власний капітал та збільшує ризик неплатоспроможності.
- Вразливості доступу. Фінансова система є однією із найбільш пов'язаних між собою у глобальній економіці, і інституції мають багато клієнтських сервісів, які повинні характеризуватись легкістю доступу будь-де, і будь-коли. А захист доступу настільки сильний, наскільки сильна його найслабша ланка.

Будь-яке значне або тривале порушення, що впливає на проведення платежів або кліринг торкається основних аспектів фінансового ризику, такі як:

- Кредитний ризик – дефолти по облігаціях та інших зобов'язання накладають прямі неочікувані збитки на інших учасників ринку;
- Ризик ліквідності – недостатня ліквідність для виконання платежів по зобов'язаннях.

- Ринковий та бізнесовий ризики – інші транзакційні ризики, які стосуються втрату доходу внаслідок зупинення дії платіжної послуги внаслідок неплатоспроможності чи припинення функціонування платежів та розрахунків.

1.4 Таксономія кібер-злочинів у фінансовому секторі

Кібер-атаки зростають експоненційно з року в рік. Як зазначає Крістін Джонсон: «Архітектура сучасних ринків базується на тому, що фінансові інституції є критичними для глобальної комерції та операцій на всіх рівнях: місцевому, державному та міжнародному. Індустрія фінансових інституцій надзвичайно широка: від традиційних акторів на зразок класичних банків, платформ для торгівлі цінними паперами та їх деривативами, інвестиційних, пенсійних чи хеджфондів до фінансових платформ та платіжних систем, створених фінтех-інженерами, наприклад Bitcoin. Внаслідок державних регуляцій та власних бізнес-моделей ці інституцій збирають, оброблюють та зберігають значні обсяги персональної інформації. Саме завдяки останнім властивостям фінансові інституції є високо привабливими для хакерів.

Кібер-загрози – це комплексне явище. Відповідно для розроблення та впровадження заходів боротьби з ним потрібно розуміти механізми, мотивації та процеси, які формують цей комплекс. Але методологічна література, яка стосується кібер-злочинності загалом, та кібер-злочинності у фінансовій індустрії зокрема залишається значною мірою теоретично недорозвиненою. Фрагментарним є саме розуміння кібер-злочинів, серед теоретиків та практиків відсутні єдині виключні визначення тих чи інших злочинів. У цьому підрозділі представлено кілька підходів до класифікації, які надають можливість більш інклюзивно зрозуміти кібер-злочинність, і відповідно ефективніше з нею справлятися. Із кібер-злочинністю потрібно боротися на різних інституційних

рівнях: державному правовому, галузевому, на рівні фірм і навіть спецслужб-військовому. Щоб ця боротьба була ефективною загалом потрібно відповісти на 5 запитань, запропоновані науковцем-теоретиком Моїтрою [4]:

1. Що для нас кібер-злочин?
2. Хто здійснює кібер-злочин?
3. Наскільки кібер-злочинність є поширеною?
4. Який вплив кібер-злочинів?
5. Як ми можемо реагувати своєчасно, ефективно та справедливо?

На кібер-інциденти можна дивитись із багатьох перспектив. Наприклад, наступна схема включає чотири основні категорії: причини (методи), актори, мотивації та наслідки:

Рисунок 1.3 – Сфери таксономічного поділу кібер-загроз

Джерело: створено автором на основі [32]

Існують різні типи та види кібер-атак: інциденти, тероризм, війни, злочини з метою наживи або із інших мотивів. Так як дані концепти у всіх давно

на слуху, їм можна дати багато різноманітних визначень. Відповідно і «кібератака» характеризується широким простором мотивацій акторів та дії. Науковці вирізняють кібернетичні дії у комп'ютерних мережах, які порушують законні стандарти як кібер-злочини, тобто це заборонена активність, яка вчинена «за сприяння або з використанням комп'ютерних мереж або апаратних засобів і направлена проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж або даних, рівно як і неправильне використання цих систем мереж або даних» (відповідно до конвенції Ради Європи [2]). Відповідно до методів та процесів таких активностей можна виділити 5 основних типів кібер-вторгнень:

1. Атаки «одиноких вовків», тобто індивідуальних хакерів, які намагаються скомпрометувати мережі, швидко проникнути у внутрішні системи, зазвичай з метою хвастощів.
2. Хактивізм, тобто кібер-атаки, які проводяться з метою привернення уваги до соціальних або політичних проблем.
3. Фрод і кримінальна активність, зазвичай проводиться тими, хто хоче неправомірно заволодіти інформацією для отримання власної вигоди. (напевно, саме цьому типові вторгнення найбільше піддаються фінансові інституції, адже такі структури володіють персональною чи конфіденційною інформацією у великих обсягах.
4. Промисловий шпіонаж, який часто проводиться «одинокими вовками», але характеризується довготривалим перебуванням у внутрішніх комп'ютерних мережах, системах чи базах даних, з метою отримання «інсайдерівської» інформації для ринкової боротьби.
5. Кібер-війни направленні на завдання втрат державним утворенням у рамках політичної чи військової кампанії; найчастіше такі атаки направлені на об'єкти критичної інфраструктури, у тому числі фінансові інституції. Подібні дії у сучасному світі можуть проводитись і недержавними акторами, і часто визначаються як кібертероризм.

Загалом кібер-атаки включають найрізноманітніші IT-загрози, починаючи від комп'ютерних вірусів, витоку даних і закінчуючи постійними загрозами підвищеної складності (англ. advanced persistent threat). Джеф Мельнік виділяє такі найактуальніші типи кібер-загроз відповідно до технічної природи здійснення атаки:

1. Denial-of -Service (DoS) & Distributed Denial-of -Service (DDoS) Attacks. DoS-атака, спрямована на перевантаження ресурсів IT-системи таким чином, щоб вони не могли виконувати своїх базових функцій відповіді на запити в Інтернеті. DDoS-атака діє загалом подібним чином, з урахування того факту, що координується із великої кількості заражених машин (бот-нетів, тобто інфікованих злочинним програмним забезпечення машин). На відмінну від більшості інших атак, це й тип не має на меті контролювати атаковану мережу, а лише призупинити звичайну діяльність, наприклад, е-комерцію, торговий термінал біржі тощо
2. Man-in-the-Middle (MitM) Attack. Зловмисник намагається перехопити поточну активну сесію між аутентифікованими клієнтом та сервером/програмою. Початкова IP-адреса користувача піддається DoS-атаці, в подальшому клієнтський IP підмінюється на IP зловмисника, і таким чином зловмисник керує поточною сесією, наприклад у онлайн-банкінгу.
3. Phishing & Spear-Phishing Attacks. За допомогою методів соціальної інженерії проводиться захоплення уваги жертв під час електронної розсилки таким чином, що б жертви повірили, що автор листа є легітимним, таким, що вартий довіри, і переходячи по гіперпосиланню або завантажуючи заражений файл, жертва «впускає» зловмисника у свою мережу. На відмінну від звичайного, spear-phishing має вузьке коло таргетних жертв, наприклад, працівників конкретного банку.

4. “Drive-by” Download Attacks не вимагає переходу по зараженому посиланню, щоб активувати атаку, адже злочинні скрипти можуть бути інтегровані у веб-ресурси, які виглядають безпечними. Звичним способом уникнення зараження атакою drive-by регулярне оновлення системи та браузера та уникнення надлишку надбудов у браузері.
5. Password Attack. Через аутентифікацію за допомогою пароля користувача зловмисник отримує доступ до комп’ютерних мереж та систем. Компрометуються паролі за допомогою методів соціальної інженерію, у простішому випадку – підгладжуються на робочому столі або записнику користувача. Неналежні за складністю паролі підбираються методом «буртфорса», тобто перебором. Ще у 2014 році координатор з кібер-безпеки Білого Дому Майкл Деніал зазначав, що «хотів би знищити паролі як основний метод захисту». На зміну сталим паролям приходять засоби біометрії: «райдужка» ока, відбитки пальців, ідентифікація лицем або голосом. Основним фактором стримування даної технології, є той факт що у разі компрометації біометричних даних їх не настільки легко замінити, як, наприклад, кредитні картки [3, с.86-87]
6. SQL Injection Attack – поширена атака, з використання SQL-запиту, впровадження в запит довільного SQL-коду
7. Cross-Site Scripting (XSS) Attack використовує веб-сайт третьої сторони, щоб запустити злоякісний код у браузері жертви, який викрадає кукі-файли і таким чином дає можливість перехопити поточну сесію
8. Eavesdropping Attack – перехоплення трафіку, у я кому можуть бути нешифровані дані: паролі, кредитні картки, інша конфіденційна інформація, яка передається онлайн
9. Birthday Attack. Даний тип атаки здійснюється проти алгоритмів шифрування, наприклад під час обміну повідомленнями. Таке повідомлення

створюється хеш-функцією, і в свою чергу продукує message digest. Завжди є ймовірність, що хеш-функція спродукує кілька messages digest, одним з яких може скористуватись хакер і підмінити повідомлення на своє.

10. Malware Attack. Небажана програмне забезпечення, яке може мати на меті повний спектр неправомірних дій є однією з найбільш значимих і популярних атак, наприклад, до цього типу відносять програми-вимагачі, трояни.

Висновок до Розділу 1

Насамперед показано цифровізацію виробничих процесів загалом, та у фінансовому посередництві зокрема як основу та джерело підсилення кібер-загроз для інституцій та індивідів. Представлено нові форми фінансового посередництва які уможливила диджиталізація та перехід на 5-ий технологічний уклад, у якому дані – персональні чи корпоративні – є новою «нафтою», і відповідно «ласим шматком» для акторів, які хочуть отримати неправомірну вигоду.

Важливим аспектом практичного ризик-менеджменту кібернетичних загроз у фінансовому секторі є ставлення до кібер-ризику як до операційного, - «ризик стосовно інформаційних та технологічних активів, що загрожують компрометацією даних: втратою конфіденційності, цілісності та доступу до інформації або інформаційних мереж», [9] або, як зазначає НБУ: «імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі інформаційних систем банку або внаслідок впливу зовнішніх факторів»

У ризик-менеджменті інформаційної безпеки ризик визначається як композиція наслідків та ймовірності настання цих наслідків, у свою чергу

ймовірність це функція рівня загрози, простоти неправомірного використання вразливостей та очікуваних наслідків. [10, с.12]

Протягом довгого періоду часу кібер-ризик розглядався лише в його ідеосинкратичному прояві, нехтували його системною природою, яка випливає із взаємозалежності інституцій у сучасному кібер-просторі. Як буде показано у наступних розділах розмір систематичного кібер-ризику, у тому числі у фінансовому секторі, часто переважає прямий ідеосинкаратичний ризик, тому роль регуляторів, творців законів і стандартів кібер-безпеки має надзвичайно велике значення, що не завжди зрозуміло окремим інституціям, наприклад, банкам, які вважають свою сферу «занадто зарегульованою». Дане дослідження покликане довести протилежне.

Кібер-злочинність – це комплексне явище. Відповідно для розроблення та впровадження заходів боротьби з ним на усіх інституційних рівня потрібно розуміти механізми, мотивації та процеси, які формують цей комплекс. Фрагментарним є саме розуміння кібер-злочинів, серед теоретиків та практиків відсутні єдині виключні визначення тих чи інших злочинів. Представлено кілька підходів до класифікації, які надають можливість більш інклюзивно зрозуміти кібер-злочинність, і відповідно ефективніше з нею справлятися. У розділі представлено основні сфери, базуючись на яких розробляється своя таксономія для тих чи інших політик кібер-безпеки. Представлено поділ кібер-загроз на типи відповідно до методів та загроз, а також технічної природи атаки.

РОЗДІЛ 2
ВИМІРЮВАННЯ РЕАЛІЗОВАНИХ КІБЕР-ВТРАТ ФІНАНСОВОЇ ІНДУСТРІЇ

2.1 Прямі банківські втрати від кібер-загроз та Var-оцінка

Як було зазначено у Розділі 1, у системі ризик-менеджменту банків кібер-загрози відносять до операційних. Ще 2003 року Базелем 2 було визначено операційний ризик як «втрати внаслідок неадекватних або помилкових внутрішніх процесів» [18]. Інакі Алдасоро та інші [17] зазначають, що, кібер-втрати мають малу часту серед усіх спричинених критичними операційними подіями, але кібер-капітал під ризиком (VaR) може спричинювати до третини усього операційного капіталу під ризиком.

Управління кібер-ризиком на рівні організації здійснюється у рамках операційного ризик-менеджменту, але зацікавленість операційним ризиком є критично малою у порівнянні з кібер-ризиком, як показує Google trends, хоча операційні процеси мають набагато ширший прояв.

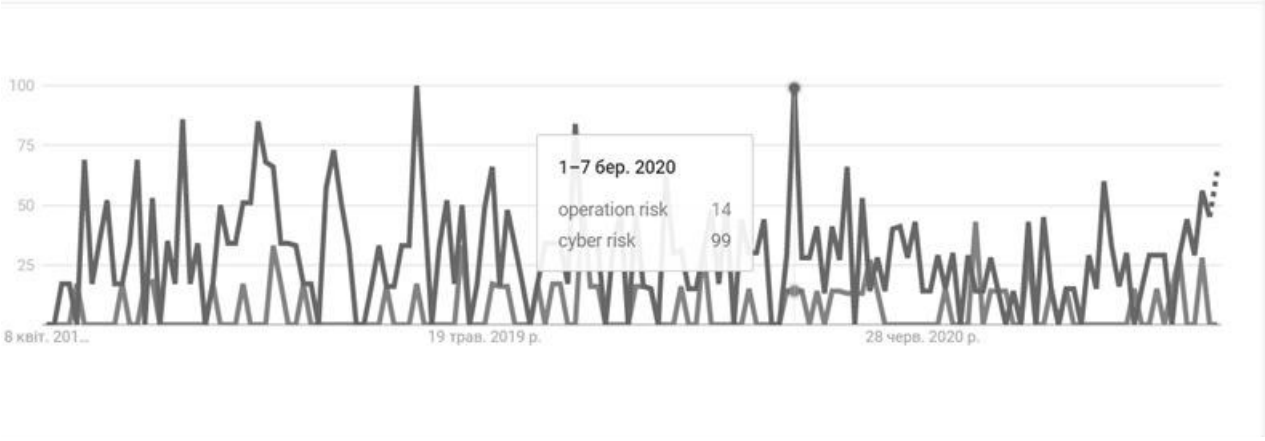

Рисунок 2.1 – Частотність пошукових запитів «operation risk» , «cyber risk» у категорії «Фінанси»

Джерело: Google trends {27]

Примітка: Кількість пошукових запитів для «операційний ризик» та «кібер-ризик» протягом останніх трьох років. Всесвітній аналіз пошукових запитів у категорії «Фінанси»

Хоча це напряму не стосується основного предмету дослідження роботи, для розуміння порядків розмірів кібер-втрат, звернемося до актуальних досліджень, які стосуються оцінок втрат у розрізі світової економічної системи. Загалом автори таких досліджень погоджуються, що надзвичайно важко порахувати із достатнім рівнем впевненості глобальні втрати від кібер-ризику, наприклад, протягом одного року, але це сотні мільярдів доларів. Наприклад, відома компанія-розробник антивірусного забезпечення McAfee називає цифру 375 млрд дол [28], Центр стратегічних та міжнародних студій – 575 млрд дол, натомість Juniper Reseach оцінює лише втрати від витоку даних у розмірі 2.1 трлн дол. [29]

Більшість науковців зазначать відсутність загально визнаних підходів до кількісної оцінки кібер-втрат, що в свою чергу спричинено відсутністю адекватної статистики відображення цього типу втрат у фінансовій звітності фінансових інституцій. Зазвичай втрати оцінюються з огляду на певні проксі-змінні. Наприклад Алдасаро та Бувере [17, 10] використовують дані найбільшого консорціуму банків у розрізі операційного ризику ORX, який класифікує події операційного ризику відповідного до стандартів Базелю. Дана статистика є однією з найбільших, зібраних за єдиним стандартом, баз даних, які стосуються операційних банківських втрат, що налічує близько 700 000 спостережень (подій операційного ризику, які призвели до відповідних втрат) протягом 2002-2019 років, при чому втрати менше 20 000 Євро не враховувались. [17] Серед цих подій може бути широкий спектр потенційних причин операційних втрат, таких як внутрішні чи зовнішні шахрайства, катастрофи, неправильна ділова практика пов’язана з клієнтами чи продуктами, пов’язана з IT. У свою чергу серед усього набору спостережень було виокремлено близько 14 000 подій, які стосуються кібер-ризику. У субкатегоріях стандартизованої звітності відповідно до вимог Базелю вони виглядали наступним чином:

Таблиця 2.1 Огляд типів подій операційного ризику

Клас події	Опис класу
ET0101	Несанкціоновна діяльність на фінансових ринках, шахрайський трейдинг
ET0102	Внутрішня крадіжка – підробка документів, вимагання, хабарі чи відкати
ET0103	Внутрішня безпека систем та мереж – навмисне пошкодження систем персоналом
ET0201	Зовнішні крадіжки чи шахрайство: грабіж, підробка платіжних документів
ET0202	Зовнішня безпека систем та мереж – навмисний збиток , злом обладнання, програного забезпечення, крадіжка даних

Джерело: представлено стандарти із роботи [17]

Уцілому частотність прямих операційних втрат (кількість подій реалізованого ризику) на 1 млрд Євро доходу представлено на Рисунку 2.2:

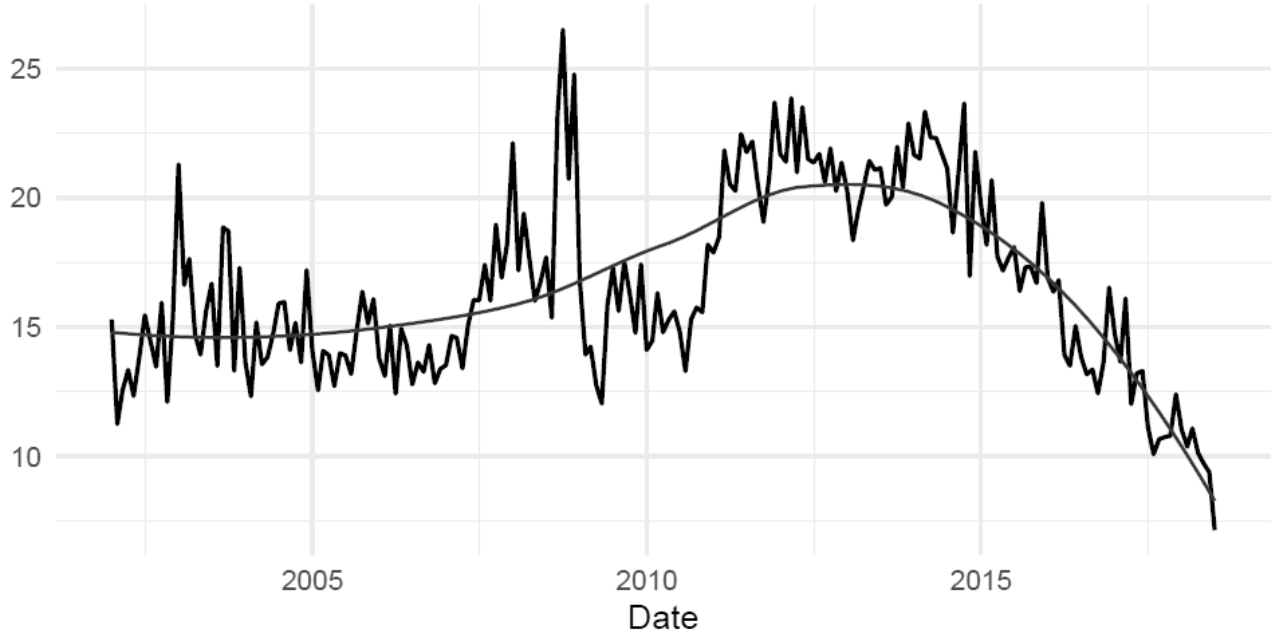

Рисунок 2.2 – Місячна частотність операційних втрат на 1 млрд Євро доходу

Джерело: представлено результати із роботи [17]

Як зазначають багато науковців, розмір операційного ризику є чутливим до фази ринку, а також монетарної політики. На рисунку видно різкі «спайки» під час Великої Фінансової кризи і чітку тенденцію до росту протягом наступних посткризових років, і, відповідно, починаючи із 2015 року події операційного ризику траплялися із меншою частотою. На противагу сумарному операційному, кібер-ризик не залежить ні від ринкового циклу, ні від класичної монетарної політики, як видно на наступному Рисунку 2.3, де частка подій кібер-ризику у операційному зростає якраз у некризові часи, у той час як втрати падають.

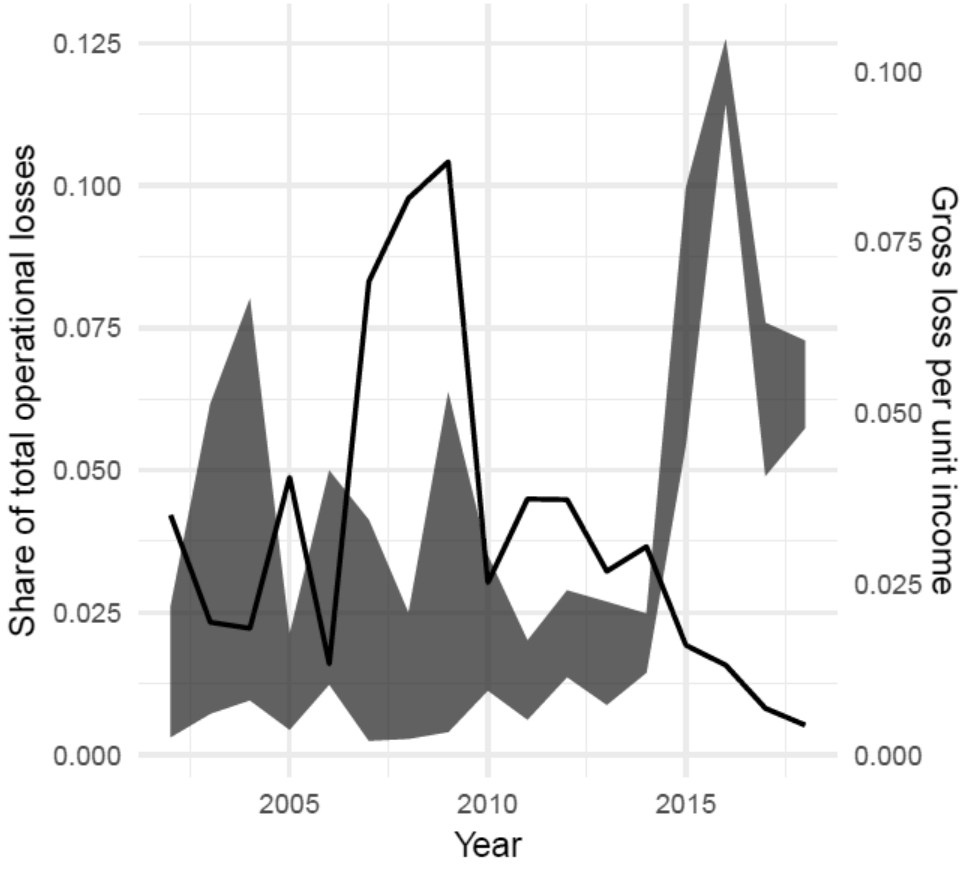

Рисунок 2.3 – Валові втрати та частка від кібер-подій

Джерело: представлено результати із роботи [17]

Примітка: Суцільною кривою зображено частка кібер-подій у межах операційних

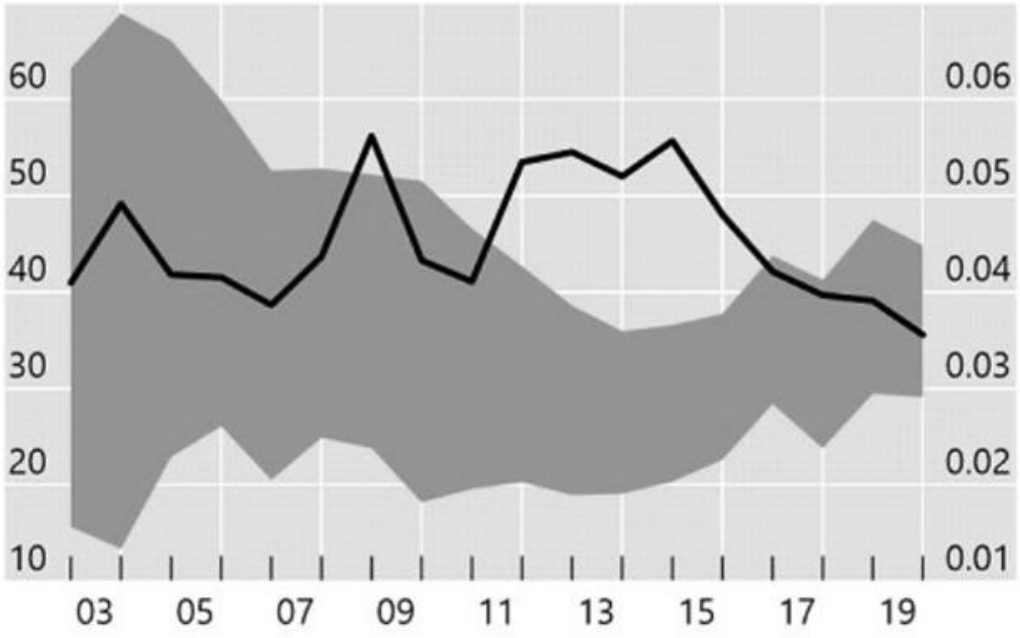

Рисунок 2.4 – Валові втрати та частка від кібер-подій

Джерело: побудовано із використання [32]

Примітка: Суцільною кривою зображено вцілому операційні втрати у млрд євро (ліва шкала), права шкала – ренж кібер-втрати у відсотка

Датасет ORX також показує цікаві «інсайти» стосовно регіонального розподілу реалізованого кібер-ризику у банках. Найчастіше і найбільш значимо дані події трапляються у банках країн Східної Європи, у тому числі і України:

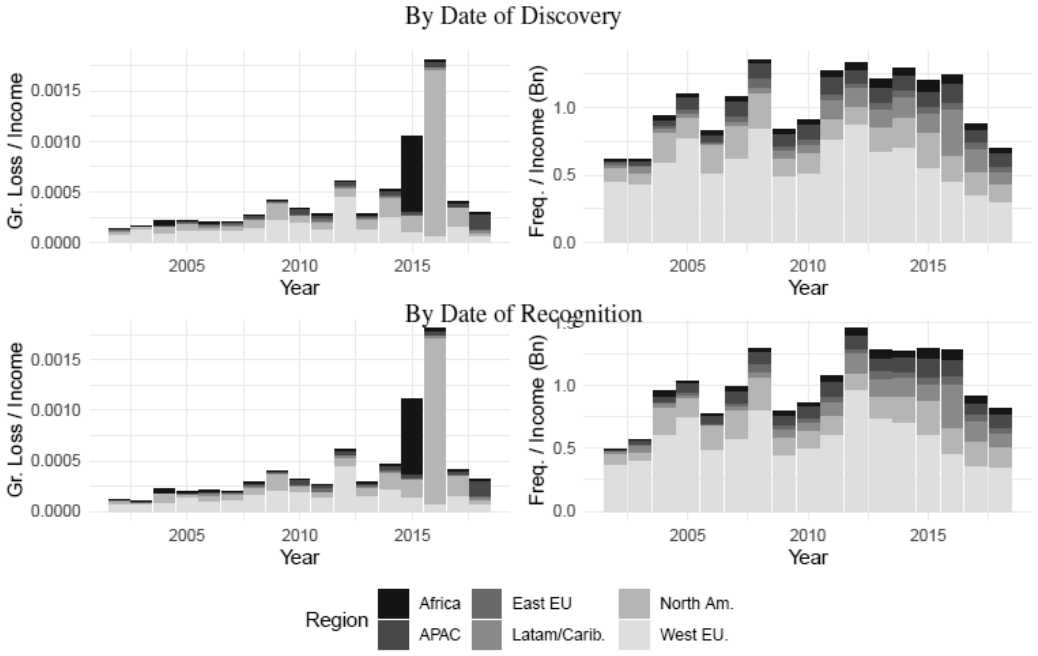

Рисунок 2.5 – Валові втрати у регіональному розрізі

Джерело: побудовано із використання [17]

Алтасаро [17] також порахував Value-at-Risk для операційного та в його межах кібер-ризику для банків консорціума ORX. Даний підхід відповідає Advanced Measurement Approach Базеля 2, і розраховує рівень регуляторного капіталу для страхування даних ризиків. Аналітично розрахований VaR для кібер-ризиків як фракцій операційних встановив, що значення капіталу під ризиком варіюються у межах 0.25-0.65% від валової валового прибутку банків, що відповідає всередньому 2.45-6.46 млрд Євро. Тим не менше стандартний підхід не враховує «товстих хвостів» розподілу кібер-втрат, яка відповідає самій природі кібер-ризику, а також тому факту, що звітування втрат від кібер-подій не завжди є бажаним для банку (в силу, наприклад, репутаційних причин), і не завжди обов'язковим з точки зору банківського нагляду та регулювання. Так, наприклад, у 2017 році лише 49 фінансових інституцій Великої Британії звітували своїм регуляторам про те, що пережили кібер-атаки. [31] У випадку врахування «товстих хвостів», VaR може «стрибнути» до рівня 4.2% валового прибутку, і відповідати третині цілого операційного Value-at-Risk, хоча, як було сказано раніше, частка кібер-подій у межах операційних незначна.

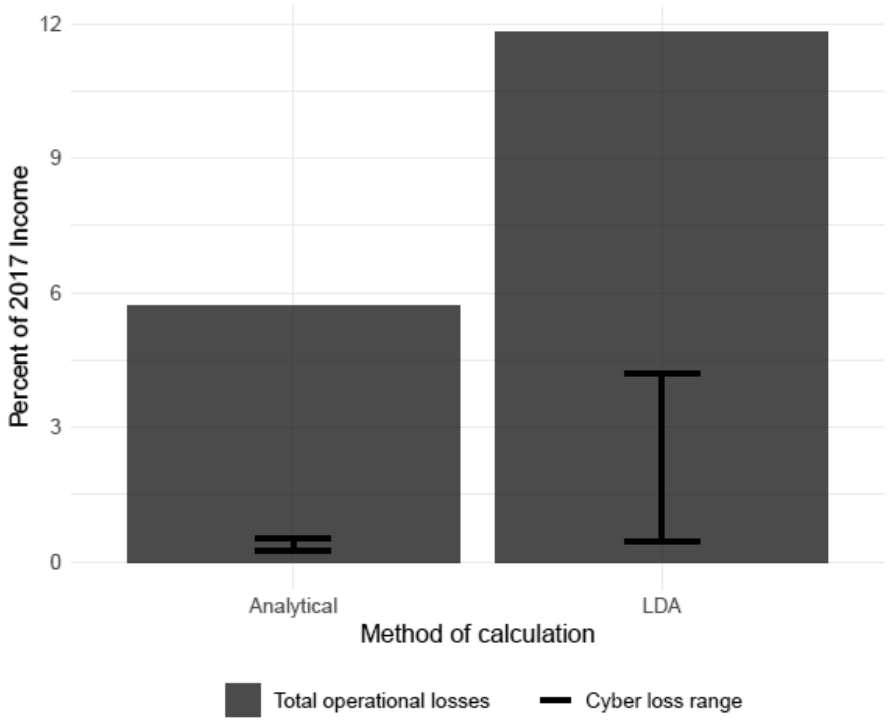

Рисунок 2.6 – Операційний та кібер капітал під ризиком для банків

Джерело: побудовано із використання [17]

Ще одне дослідження втрат банківської системи від кібер-подій проведене Бувере [10], який теж використовував дані ORX, але протягом 2011-2016 років (більше 5000 кібер-подій), і використовуючи метод симуляції Монте-Карло, екстраполював втрати на дохідність 7 947 банків по усьому світу. Розподіл втрат у даному датасеті виглядав наступним чином (див. Рисунок 2.7):

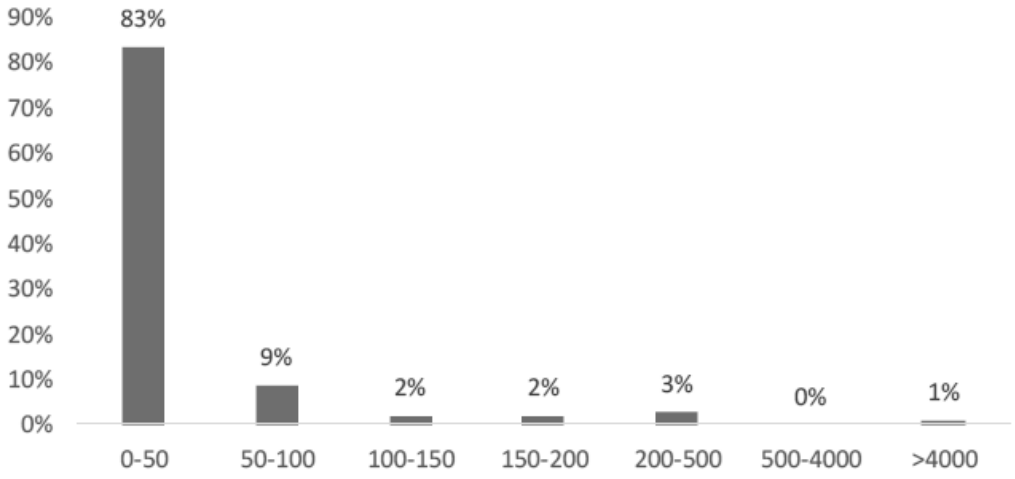

Рисунок 2.7 – Гістограма втрат – розподіл втрат у мільйонах доларів

Джерело: побудовано із використання [10]

Для побудуви і симуляції розподілу використовувався логномальний розподіл для «тіла» (83%), і узагальнений розподіл Парето для екстремальних значень правого «хвоста». Також Бувере увів у свої розрахунки «заразність поширення», тобто, що певна кібер-подія поширюється і на інші фінансові інституції та призводить до більших втрат, ба більше, чим вищі початкові втрати, тим більша можливість «поширення» - від 20% до 60%. Якщо у Алтасаро (76 банків консорціуму ORX) Var становив 4.2% відсотків прибутку, то у Бувере це 14% і більше. Також варто додати, що, наприклад, за розрахунками банківського регулятора Сінгапура в середньому кібер-атаки можуть знизити коефіцієнт адекватності капіталу до 0.4 відсоткових пункта. [33]

2.2 Драйвери збільшення кібер-втрат

Інформаційні технології стали критичним інструментом належного функціонування економіки. Відповідно зросла схильність фірм та інших інституцій до сприйняття кібер-ризиків, які ведуть до прямих фінансових втрат, зупинку звичного операційного функціонування або репутаційних втрат. Фірми активно інвестують у кібер-захист, але ефективність інвестицій важко підрахувати. Для фінансового сектора кібер-ризики є одними з ключових «відомих невідомих» «хвостових» ризиків, які потенційно є основною загрозою фінансовій стабільності. У 2017 своїм комюніке міністри фінансів держав G20 зазначили, що «зловмисне використання інформаційно-комунікаційних технологій може підривати функціонування надання фінансових послуг, що підриває національну на міжнародну фінансову стабільність, довіру та впевненість у фінансових інституціях» [26] Незважаючи на загальний консенсус щодо даних загроз, малодослідженим залишається основні драйвери

та пом’якшуючі фактори, які впливають на кількість фінансових втрат. Зацікавленими у розробці моделей, які пояснюють ціну кібер-інцидентів є регулятори, страхові компанії та самі фірми, які піддаються втратам. У академічному середовищі найбільш грунтовні і детальні розробки факторів-драйверів схильності до кібер-ризиків здійснили Романовскі, Алдасаро, Курті.

У праці «Drivers of cyber risk» статистично підтверджується, що «фінансовий сектор переживає найбільшу кількість кібер-інцидентів, у тому числі найбільше кібер-атак. Тим не менше, банки та страхові компанії піддаються меншим втратам відносно інших секторів завдяки позитивному впливу регуляторів, а також більших інвестицій у кібер-захист. Автори дослідження слідують прикладу Саші Романовського [21], і використовують датасет зібраний американською компанією Advisen, який також є одним з найбільш повних та великих. Advisen – це орієнтованй на прибуток аналітичний центр, який використовує власні методи збору та інтегрування даних із публічних джерел, - насамперед новинних агенств. Проблемою «парсингу» даних із публічного доступу є неповнота та неточність статистики, проблеми із інтеграцією і стандартизацією даних, відповідно розрахувати сукупні втрати із високим ступенем довіри до результатів надзвичайно важко. Генерацію статистики із наочним зображенням потенційно малої частки кібер-інцидентів у кінцевому датасеті можна побачити на наступному рисунку:

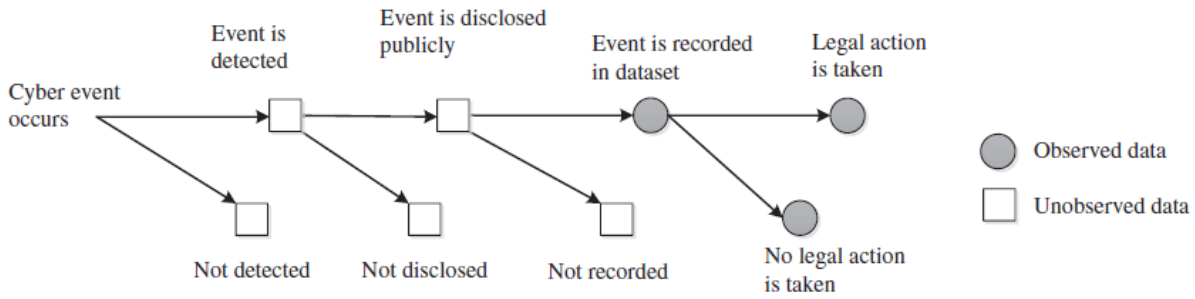

Рисунок 2.8 – Процес генерації даних методами парсингу публічних ресурсів

Джерело: представлено результати із роботи [21]

Найцікавішим аспектом описової статистики втрат від кібер-події відповідно до сектору економічної діяльності (стандарти NAICS) є той факт, що фінансовий сектор найчастіше піддається загрозам із боку кібер-середовища, але більші абсолютні втрати мають такі сектора як «Information and communication» та «Professional, scientific and technical» (див. Рисунок 2.9). У випадку природи наших даних більш релевантними метриками для порівняння секторів в розрізі їх вразливості до кібер-подій є середні втрати по галузі та стандартне відхилення втрат: 6 галузей мають одночасно більше стандартне відхилення на середні втрати за фінансовий сектор (див. Рисунок 2.10).

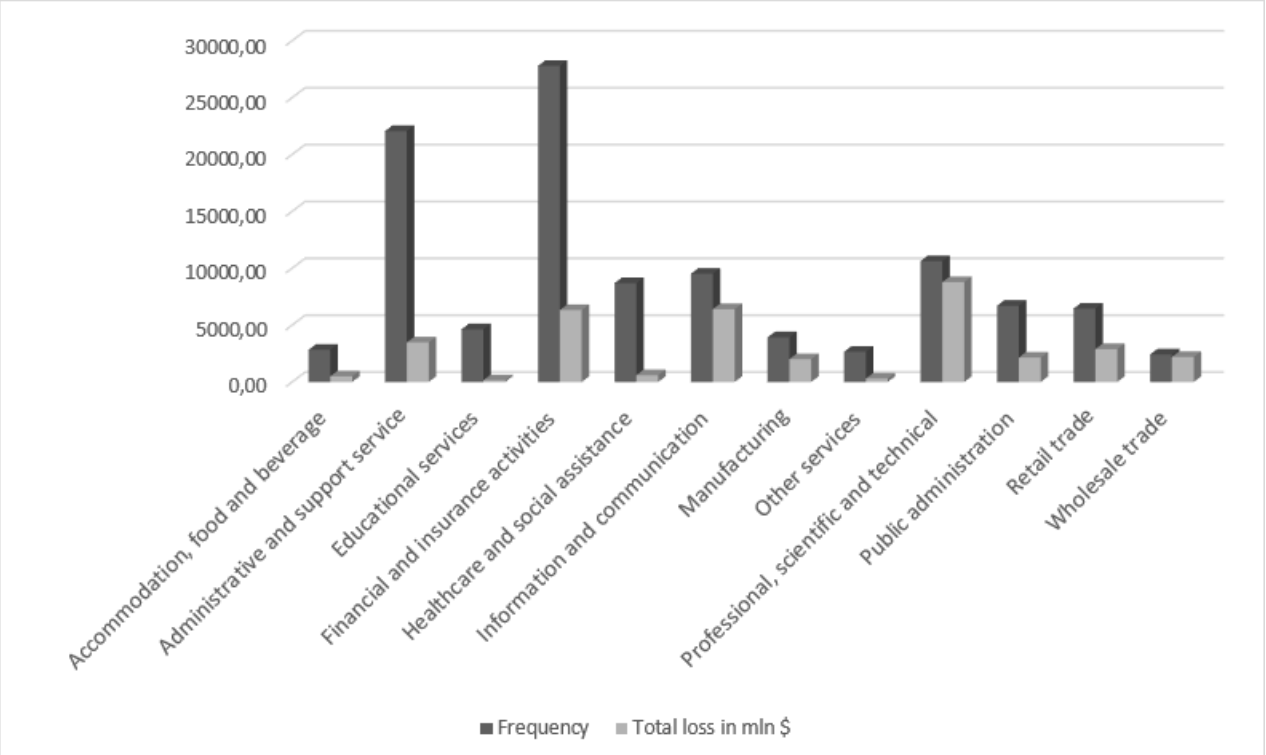

Рисунок 2.9 – Статистика сукупних втрат та частоти кібер-атак у секторальному розрізі

Джерело: Розроблено автором на основі даних із [17]

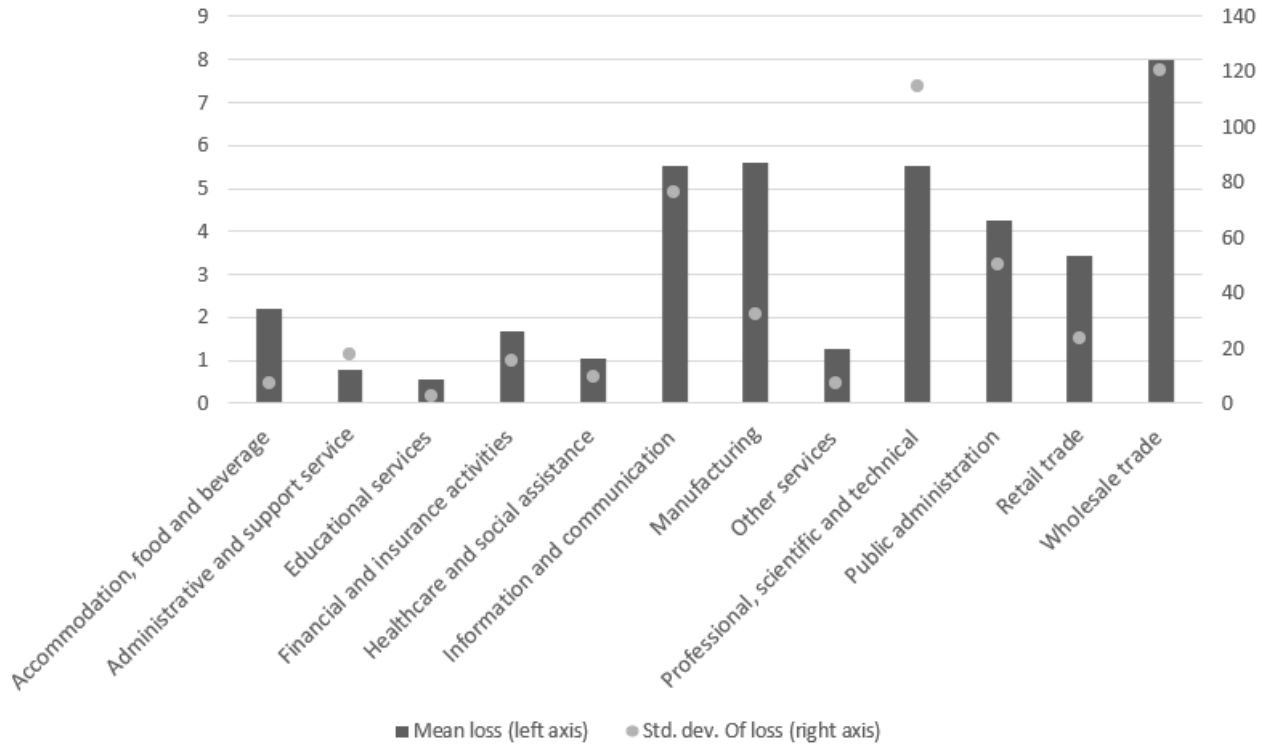

Рисунок 2.10 – Статистика середніх втрат та стандартного відхилення втрат від кібер-атак у секторальному розрізі

Джерело: Розроблено автором на основі даних із [17]

Вцілому для вражених фірм у середньому для усіх галузей ціна одного інциденту складала 2.6 млн дол. У той час як для фінансового сектору середні втрати нараховують 1.7 млн дол, хоча частотність більша майже у 2.5 разів. У середньому по галузях розподіл втрат за типом інцидентів виглядав наступним чином: 49% - шахрайство, 46% - витік даних, 5% - загальний операційний «дисконект» бізнесу; для фінансового сектору більшість складає все ж фінансовий фрод – відповідно 61%, 37%, 2%. [32]

Також важливим є аналіз, як змінились характеристики вразливості секторів внаслідок пандемії Covid-19, за умови, що значно зросла частка дистанційної роботи, що в свою чергу збільшили кібер-вразливості компаній. (див. Рисунок 2.7) Так лише за перші два місяці пандемії використання протоколів віддаленого доступу (RDP) та віртуальних приватних мереж (VPN) зросли на 41% і 33% відповідно, збільшивши вразливість інституцій до кібер-загроз. З іншого боку поширились методи соціальної інженерії, які

використовують страх для досягнення своїх цілей, наприклад, фішингові листи із зараженим вкладенням, які нібито стосуються Covid-19. Фінансовий сектор оцінено як один із таких, що найбільше перейшли на дистанційну роботу, а також він залишився одним із тих, що найчастіше піддаються кібер-загрозам.

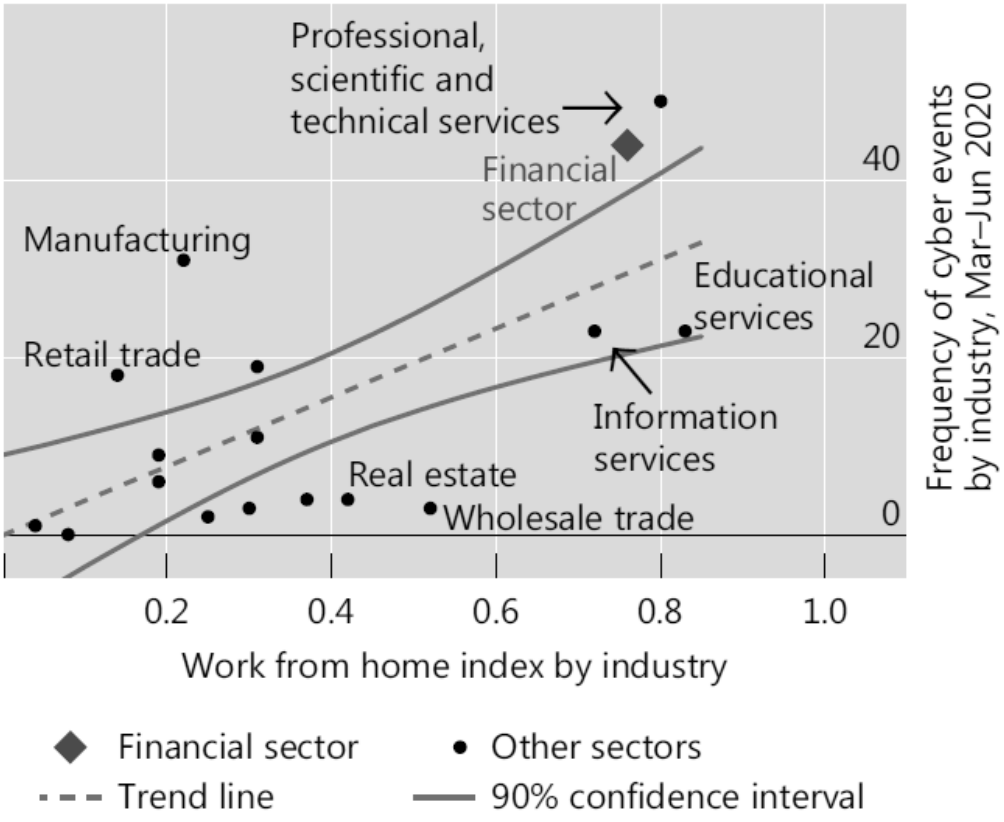

Рисунок 2.11 – Частотність кібер-подій versus індекс Work-From-Home

Джерело: використано результати із робіт [22, 17]

Як було зазначено на початку підрозділу, широке коло акторів зацікавлено у розробці моделей, які пояснюють ціну втрат від кібер-ризику. У науково-практичному середовищі для задоволення цієї потреби найчастіше використовують регресійні моделі. Так наприклад, Джейкобс регресував втрати на кількість скомпроментованих даних під час їх витоку [23]. Романовскі [21] розширив методологію, включивши ширший набір змінних у модель: розмір фірми, даммі змінну, чи є подія зловмисною (наприклад, хакерська атака чи продаж інсайдерівської інформації), даммі змінну, чи причинила подія втрати у кількох або багатьох фірмах, кількість скомпроментованих даних, ефект від

юридичних наслідків, якщо такі були. Алдасоро [20] ще більше розширив підхід, поетапно чи незалежно включаючи інші фактори: секторальність, даммі змінну, чи була подія хакерською, ефект від хмарних технологій та інвестицій в ІТ-безпеку. Наприклад, було побудовано три фактори, які пояснюють рівень ІТ-розвитку сектору:

1. Staff training – відсоток фірм у секторі, які проводять ІТ-тренінги для своїх робітників;
2. PC users, – відсоток робітників у кожному секторі, які використовують персональний комп'ютер у щоденній праці;
3. Specialist Staff, – відсоток фірм, які наймають висококваліфікованих у ІТ спеціалістів.

Таким чином модель, розроблена Алдасоро та іншими [20] в загальному вигляді має вигляд:

$$\log(Cost) = \beta_0 + \beta_1 FirmSize + \beta_2 Connections + \beta_3 HackerType + \beta_4 FE + u \quad (2.1)$$

де Cost – це загальна кількість втрат (вартість кібер-ризику);

FirmSize – логарифм валового доходу фірми;

Connections – кількість поширень однієї кібер-події (к-сть заражених фірм, що понесли втрати)

HackerType – даммі змінна, чи був інцидент зловмисний;

FE – фіксований ефект, яким може бути сектор події, тип (витік даних фішинг), рік

Внаслідок неможливості перевірки гіпотез моделі, наведеної вище, самостійно (закритість датасету), звернемося до результатів регресії, які отримав Алдасоро

Таблиця 2.2 Результати моделювання

Модель	I	II	III	IV
FirmSize	0.231*** (0.01)	0.259*** (0.02)	0.237*** (0.01)	0.227*** (0.01)
Connections	0.020*** (0.01)	0.018*** (0.01)	0.018*** (0.01)	0.022*** (0.01)
HackerType	-0.066 (0.12)	-0.323** (0.13)	-0.617** (0.29)	-0.511* (0.28)
Year	+	-	-	+
Sector	-	+	-	+
Incident Type	-	-	+	+
R2	0.177	0.125	0.125	0.199
Obs	3228	3228	3228	3228

Джерело: результати досліджень авторів [20]

Примітка: у стовпцях таблиці представлено результати моделей і з різними «фіксованими ефектами», у останньому стовпці включено усі ефекти

Із результатів моделювання можна чітко сказати про те, що драйвером втрат від кібер-ризику є розмір фірми. Результати регресій показують, що якщо фірма має виручку на 1% більше, тоді кібер-втрати більші на 0.23-0.27 %. Тому насамперед системно важливі фінансові інституції мають докладати відповідно потенційно більше зусиль для боротьби із кібер-ризиком. Тим не менше, вплив цього фактора саме для фінансової індустрії менший ніж загалом. Фактор Connections показує значення поширеності кібер-інциденту на кілька інституцій, тобто наскільки «заразність» підсилює втрати окремої бізнесової одиниці. Connections можна вважати мірилом системного кібер-ризику, про який йшлося у першому розділі. Чим більше інституції пов’язані, тим більший зв’язок, особливу у фінансовому секторі. Найбільш цікавими є той факт, що фактор HakerType має негативний знак, хоча вважається, що саме злочинні дії хакерів-нападників зазвичай мають більш значний вплив ніж кібер-події,

пов’язані наприклад, із переходом на іншу IT-інфраструктуру, або вцілому загальне відключення від кібер-простору.

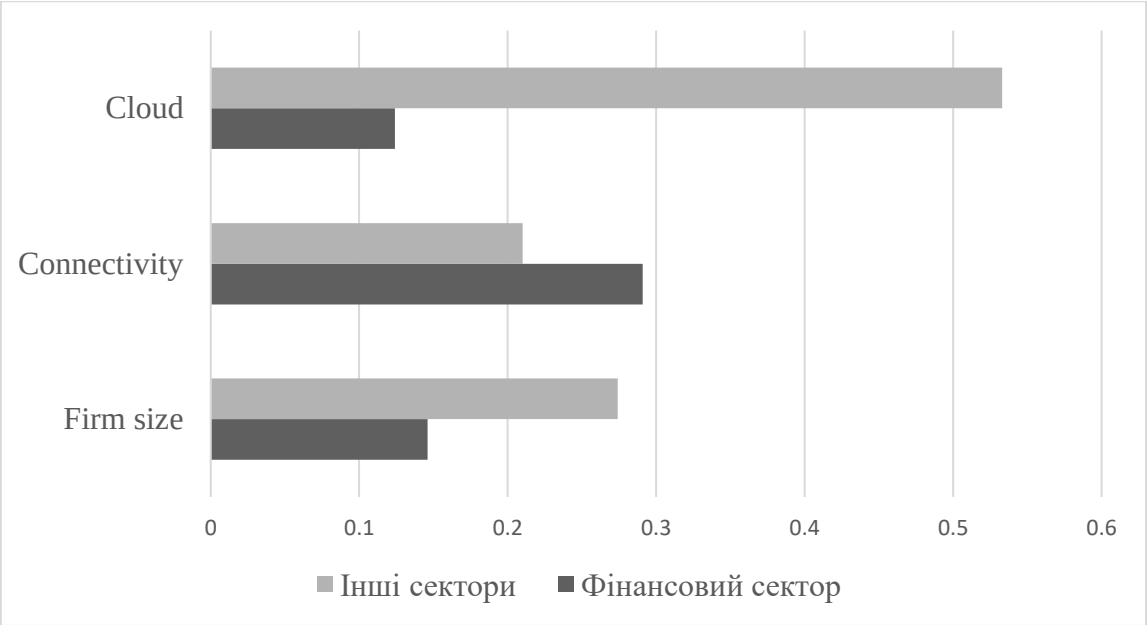

Рисунок 2.12 – Основні драйвери кібер-ризику

Джерело: розраховано автором на основі [31]

Протягом останніх років фінансові інституції почали широко використовувати хмарні технології для проведення ком’ютерних обчислень та зберігання даних, що надає фірмам гнучкості, зменшення ціни обробки і використання даних, а також зменшує споживання енергії. Як не дивно, цей процес сильно підсилила пандемія. Нові дослідження [35] засвідчують, що внаслідок пандемії 82% фірм посилили використання хмарних технологій, і 92% планують це зробити в найближчому майбутньому. Тим не менше, хмарні технології також породжують певні ризики насамперед надмірної концентрації у розрізі систематичного кібер-ризику. Адже близько половини компаній, які надають хмарні Infastructure-as-a-Service (IaaS) це такі IT-гіганти як Amazon, Microsoft, IBM, Google; хоча не можна відкидати того факту, що саме такі фірми мають найкращих спеціалістів з кібер-безпеки. Тим не менше, послуги останніх фірм є доступні інституціям із малими бюджетом, що однозначно має свій позитивний ефект.

Для дослідження потенційного впливу додаткових інвестицій на зменшення кібер-втрат Алдасоро додав фактор використання хмарних технологій у рівняння 2.1, а також ще один фактор (*Cloud*), де хмарні технології пов'язуються із тими кібер-подіями, які мали місце одночасно у кількох інституціях (*Cloud*×*Connections*):

$$\log(Cost) = \beta_0 + \beta_1 FirmSize + \beta_2 Connections + \beta_3 HackerType + \\ + \beta_4 Cloud \times Connections + \beta_5 FE + u \quad (2.1)$$

Результати моделювання підтверджують негативний та статистично значимий вплив залежності інституцій від хмарних технології на кількість кібер-втрат, навіть у випадку кібератаки, яка мала місце у кількох інституціях (систематичний кібер-ризик). Тому вцілому можемо говорити про використання хмарних технологій як про ефективний спосіб зменшення кібер-ризику, разом із іншими позитивними ефектами.

Таблиця 2.3 Результати моделювання із включенням факторів хмарних технологій

Модель	I	II	III
FirmSize	0.227 ***	0.223***	0.228***
	(0.01)	(0.02)	(0.01)
Connections	0.022 ***	0.022***	0.076***
	(0.01)	(0.01)	(0.01)
HackerType	-0.511	-0.527**	-0.572**
	(0.28)	(0.28)	(0.29)
Cloud		-0.015***	
		(0.00)	

Продовження Таблиці 2.3

	I	II	III
Cloud×Connections			-0.002*** (0.00)
Year	+	+	+
Sector	+	-	+
Incident Type	+	+	+
R2	0.199	0.191	0.203
Obs	3228	3228	3228

Джерело: результати досліджень авторів [20]

2.3 Регулятивні та наглядові аспекти систематичних кібер-ризиків у банківському секторі України

Загальнопоширеною та правильною є думка, що цифровізація стала новою нормою для усіх банків, пандемічні заходи пришвидшили ще більше зростання частки онлайн-платежів. Зрозуміло, що надалі цифрова трансформація покриватиме дедалі більше сфер обслуговування клієнтів. У даному випадку на перший план для забезпечення конкурентності банку стає швидкість розробки зручних віддаленних сервісів на різних платформах, відповідно кількість відділень буде зменшуватися:

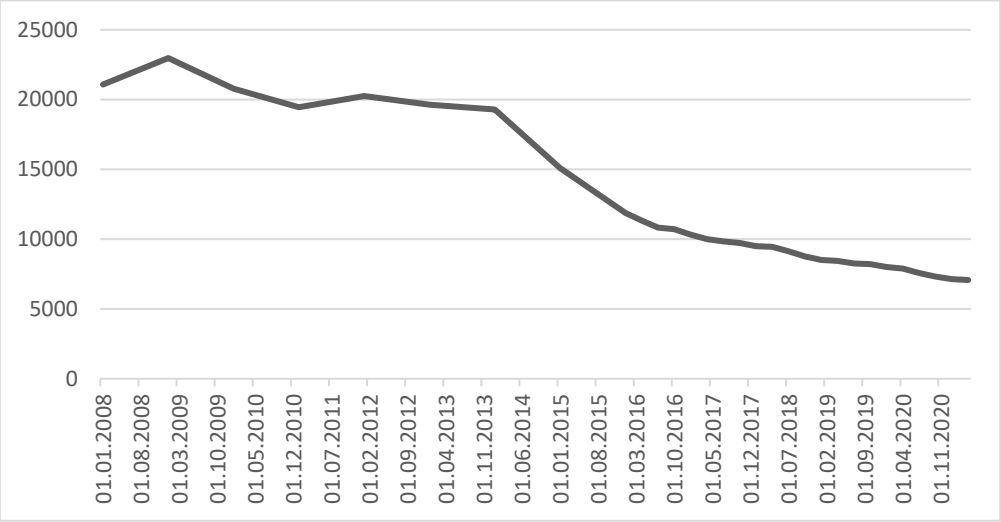

Рисунок 2.13 – Динаміка кількості структурних підрозділів українських банків

Джерело: розраховано автором на основі [46]

Розширення кола клієнтів, які користуються віддаленими системами доступу до банківських сервісів підвищує кібер-ризик як для окремих інституцій, так і для системи. У останньому «Опитуванні про системні ризики фінансового сектору» керівники фінустанов зазначають, що «фактор шахрайства та кібернетичних загроз стабільно входить до п’яти найбільших джерел ризику протягом всіх раундів опитування», [37] поступаючись лише ризикам політичної ситуації, корупції та діяльність правоохоронної системи (див. Рис. 2.9), хоча у передпандемічні часи роль оціненого кіберризику була набагато менша. Також результати опитування показали, що найбільше визначають рівень ризику як «Високий» саме ризик шахрайства та кібернетичних загроз: близько 65% респондентів, «Середній» - 35% респондентів

Рисунок 2.14 – Ранги найбільших факторів ризику у фінансовому секторі України

Джерело: побудовано автором на основі [37]

«Проблеми кібербезпеки винесено на державний рівень. 05 жовтня Верховна Рада України прийняла Закон України № 2163 "Про основні засади забезпечення кібербезпеки України" (набирає чинності 09.05.2018), де НБУ названо серед основних суб'єктів національної системи кібербезпеки. Відповідно до ухваленого закону НБУ визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки в банківській системі України; створює центр кіберзахисту Національного банку України.

Реагуючи на нові виклики, НБУ запропонував банкам комплексні рішення для мінімізації кібер-ризиків та усунення наявних кібер-загроз. 28 вересня 2017 року ухвалено постанову Національного банку України № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" (набирає чинності 01.03.2018). Положення встановлює обов'язкові мінімальні вимоги з організації заходів із забезпечення інформаційної безпеки та кібер-захисту; принципи

управління інформаційною безпекою та вимоги до інформаційних систем банку, що взаємодіють з інформаційними системами НБУ. Документ містить як комплексні настанови з розбудови системи інформаційної безпеки, так і вузькі технічні питання захисту банківської інформації.» [38, с.55]

Також у 2021 році Національний банк затвердив порядок планових та позапланових виїзних перевірок та безвиїзного нагляду інформаційної безпеки та кібер-захисту Постановою №4 «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кібер-захисту та електронних довірчих послуг». [47] Це Положення встановлює:

1) порядок організації та здійснення Національним банком України (далі – Національний банк) заходів контролю за дотриманням банками вимог законодавства, яке регулює відносини у сферах кібер-захисту
2) вимоги щодо проведення банком самооцінки стану інформаційної безпеки/кібер-захисту.

Відповідно до даної постанови зазначається, що «Національний банк має право проводити позапланову перевірку з метою термінового встановлення причин, обставин, масштабу негативного впливу на життєдіяльність банку та/або банківську систему в разі отримання документально підтвердженої інформації про:

1) інциденти інформаційної безпеки/кібер-інциденти, наслідком яких є реалізована загроза для безпеки інформації банку та його клієнтів;
2) інциденти інформаційної безпеки/кібер-інциденти, наслідки яких можуть спричинити системний ризик у банківській системі;
3) порушення вимог законодавства у сфері електронних довірчих послуг.»

«Банк зобов’язаний проводити щорічну самооцінку стану інформаційної безпеки/кібер-захисту шляхом складання щорічного Звіту з питань оцінювання ризиків інформаційної безпеки/кібер-ризиків із урахуванням відомостей за результатами періодичного проведення:

1) оцінювання ризиків інформаційної безпеки/кібер-захисту;

2) оцінювання результативності інформаційної безпеки та ефективності СУІБ;

3) зовнішнього аудиту інформаційної безпеки;

4) внутрішнього аудиту інформаційної безпеки/кібер-захисту (далі – внутрішній аудит).»

Висновок до Розділу 2

Інформаційні технології стали критичним інструментом належного функціонування економіки. Відповідно зросла схильність фірм та інших інституцій до сприйняття кібер-ризиків, які ведуть до прямих фінансових втрат, зупинку звичного операційного функціонування або репутаційних втрат. Фірми активно інвестують у кібер-захист, але ефективність інвестицій важко підрахувати. Для фінансового сектора кібер-ризики є одними з ключових «відомих невідомих» «хвостових» ризиків, які потенційно є основною загрозою фінансовій стабільності.

З огляду на результати робочих документів МФВ, Банку міжнародних розрахунків та академічних дослідників встановлено, що, кібер-втрати мають малу часту серед усіх спричинених критичними операційними подіями, але кібер-капітал під ризиком (VaR) може спричинювати до третини усього операційного капіталу під ризиком. Розрахований капітал під ризиком (VaR) для кібер-загроз як частки операційних встановив, що значення капіталу під ризиком варіюються у межах 0.25-0.65% валового прибутку. Тим не менше стандартний підхід не враховує «товстих хвостів» розподілу кібер-втрат, яка відповідає самій природі кібер-ризику, а також тому факту, що звітування втрат від кібер-подій не завжди є бажаним для банку, і не завжди обов’язковим з точки зору банківського нагляду та регулювання. А із врахуванням «товстих хвостів» - 14% і більше від прибутку банку. [10] Також у першому пункті

другого розділу показано, що на противагу сумарному операційному, кібер-ризик не залежить ні від ринкового циклу, ні від класичної монетарної політики.

Статистично підтверджується, що фінансовий сектор переживає найбільшу кількість кібер-інцидентів, у тому числі найбільше кібер-атак. Тим не менше, банки та страхові компанії піддаються меншим втратам відносно інших секторів. Також у другому пункті другого розділу представлено оцінки деяких факторів, які є драйверами кібер-ризику. Тобто збільшують фінансові втрати інституцій. Такими факторами є розмір фірми, якщо фірма має виручку на 1% більше, тоді кібер-втрати більші на 0.23-0.27%, Connections показує значення поширеності кібер-інциденту на кілька інституцій, тобто наскільки «заразність» підсилює втрати окремої бізнесової одиниці, фактор теж має позитивний знак. Найбільш цікавими є той факт, що фактор HakerType має негативний знак, хоча вважається, що саме злочинні дії хакерів-нападників зазвичай мають більш значний вплив. Також досліджено використання хмарних технологій: доведено негативний та статистично значимий вплив залежності інституцій від хмарних технології на кількість кібер-втрат. Тому вцілому можемо говорити про використання хмарних технологій як про ефективний спосіб зменшення кібер-ризику, разом із іншими позитивними ефектами.

Основний регулятор фінансового сектору України НБУ усвідомлює системну важливість кібер-ризиків для фінансової стабільності і протягом останніх кількох років почав здійснювати суттєві кроки стосовно нагляду за ним, а також упередження. У останньому «Опитуванні про системні ризики фінансового сектору» керівники фінустанов зазначають, що «фактор шахрайства та кібернетичних загроз стабільно входить до п’яти найбільших джерел ризику протягом всіх раундів опитування. Також результати опитування показали, що найбільше визначають рівень ризику як «Високий»

саме ризик шахрайства та кібернетичних загроз: близько 65% респондентів, «Середній» - 35% респондентів.

РОЗДІЛ 3
КІЛЬКІСНИЙ АНАЛІЗ КІБЕР-ВТРАТ ІНСТИТУТІВ ФІНАНСОВО-БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

3.1 Загальна структура моделі секторальних кібер-втрат для економіки України. Прямі втрати

Останнім роками зростає частота і вартість кібер-інцидентів, причому в по деяким з них втрати складають сотні мільйонів доларів. Існує помітна різноманітність серед досліджень щодо вивчення передбачуваних прямих і системних витрат від кібер-інциденти. У багатьох випадках порівняння досліджень ускладнюється відсутністю прозорості в методологіях, закладених припущень і використовуваних даних. Враховуючи результати досліджень, описаних у попередньому розділі як припущення моделі у Розділі 3 описано модель, за допомогою якою розраховуються втрати від реалізованого кібер-ризику (кібер-атак) для економіки України у розрізі секторів економіки (насамперед нас цікавить фінансово-банківський сектор), поділу на прямий та систематичний кібер-ризик, макроекономічний поділ на секторальний випуск та частку ВВП та інші аспекти.

За основу структури моделі було взято розробки Паула Дреєра та інших спеціалістів аналітичного центру RAND «Estimating the Global Cost of Cyber Risk. Methodology and Examples». [41] Мета цього дослідження полягала в тому, щоб розробити прозору і адаптовану методологію для оцінки поточних і майбутніх глобальних, національних та секторальних витрат на кібер-ризик, яка визнає закладання невизначеності у частотах і вартості кібер-інцидентів.

Щоб включити невизначеність у модель, багато параметрів є оціненими точково або розподілами ймовірностей. У модель включено рівномірний,

трикутний, трапецієвидний, узагальнений бета- да Дельфі розподіли (останнє включає набір розподілів-запитів кількох профільних експертів).

Дреєр та інші зазначають: «Ми виявили, що в результаті оцінені значення дуже чутливі до вхідних параметрів; наприклад, з використанням трьох вхідних необхідних для моделі наборів параметрів з існуючих досліджень і нашого власного аналізу даних, ми виявили, що кіберзлочинність має прямі витрати на валовий внутрішній продукт (ВВП) від 275 млрд. дол. США до 6,6 трлн. дол. США у всьому світі і загальні ВВП-витрати (прямі плюс системні) від 799 до 22,5 трильйонів доларів (1,1-32,4 відсотка ВВП, - верхньою межею є розрахунки Value-at-Risk-моделі)» [41 с.8]

Для побудови цієї моделі спочатку визначимо наступні чотири структурних набори, які є описовими і, таким чином, не мають одиниць вимірювання:

Країни: $c \in C$

Сектори індустрій: $i \in I$

Економічні втрати: $e \in E$

Загрози: $p \in P$

Набори галузевих секторів та загроз є взаємовиключні і колективно вичерпні. У нашому аналізі ми пов'язуємо вартість інциденту з втратою ВВП в конкретних галузях промисловості. Зокрема, витрати поділяються на:

1. втрати продукції, що відчуваються кожним сектор i в кожній країні c (прямі втрати - d_{cg})
2. макроекономічні наслідки для виробництва, що відчувається іншими секторами через прямий збиток кожного сектору і в кожній країні с (системні втрати - s_{cg}).

У цьому визначенні прямі витрати включають витрати, які безпосередньо оплачуються сектором до, під час і після події, в тому числі відшкодування

збитків у формі штрафів, витрат на розслідування, а також перерв у роботі підприємств, які відбуваються в секторі, який був атакований, а також судові витрати, які можуть бути понесені третіми сторонами, але отримують компенсацію від фірми, яка зазнала нападу. [40] Прогін моделі або створює очікуване значення витрат з урахуванням базових розподілів вхідних даних, або використовує велику кількість базових розподілів для оцінки функції розподілу витрат.

Насамперед визначається w_{ci}, як частка i-го сектора ВВП в країні c. Таким чином, $w_{ci} * GDP_c$ є додана вартість (внесок у ВВП) сектора i в країні c. Крім того, ми визначаємо O_{ci}, як випуск сектора i в країні c. Потім, и визначаємо вартість Y_{cie}, що є часткою випуску продукції галузі, еквівалентна на суму грошей під ризиком від кожного типу (e) фінансової експозиції, незалежно від того, чи можуть вони постраждати від кібер-атаки. Нарешті, ми визначаємо вартість X_{ciep}, що є часткою фінансової експозиції під ризиком в країні (c), і тип (e) впливу, який буде успішно зруйнований, вкрадений через загрозу (p). Таким чином, Y_{cie} і X_{ciep} обчислює фракційний вплив кожної кібер небезпеки (p) на випуск та/або додану вартість кожного сектора i пов'язаний з кожною експозицією e.

Тому ми можемо визначити прямі втрати випуску кожного сектора i в країні c, просумувавши Y_{cie} і X_{ciep} для всіх загроз p і експозицій e. Відповідно результат помножений на продукцію сектора i в країні c (O_{ci}), дає сукупні прямі витратам сектора:

$$d_{cio} = O_{ci} \sum_{e \in E} \sum_{p \in p} Y_{cie} X_{ciep} \quad \forall i \in I, c \in C \qquad (3.1)$$

де, O_{ci} - секторальний випуск для країни c і сектору i;

Y_{cie} - частка від $w_{ci} * G_c$, яка еквівалентна сумі грошей під ризиком

від кожного типу експозиції (e);

X_{ciep} *- частка експозиції під ризиком в країні c, секторі і і схильності до ризику типу експозиції (e), що буде успішно знищено, вкрадено чи іншим чином втрачено через певну кібер-загрозу(p).*

Якщо змінюється обсяги виробництва в певному секторі, змінюється обсяг втрат сектора ВВП:

$$d_{cig} = w_{ci} G_c \sum_{e \in E} \sum_{p \in p} Y_{ciep} X_{ciep} = \frac{w_{ci} G_c}{O_{ci}} d_{cio} \quad \forall i \in I, c \in C \qquad (3.2)$$

Агреговані секторальні втрати дозволяють визначити прямі сумарні втрати випуску секторів та втрати ВВП $d_{co} = \sum_{i \in I} d_{cio}$; $d_{cg} = \sum_{i \in I} d_{cig}$.

Через складність вимірювань і невизначеності в сценаріях кібератак, важливо визначити, як різні модельні припущення впливають на кількість $w_{ci} * G_c$, ВВП країни c. Отримана оцінка буде значною мірою залежати від факторів ризику, експозицій, секторів і їх взаємозв'язків. Оцінка впливу ризиків на вплив є значною проблемою. Хоча надалі розглядаються підходи до визначення цих взаємозв'язків, зберігаються значні невизначеності.

3.2 Від прямих до систематичних втрат

Основна перевага нашого моделювання перед багатьма попередніми оцінками кібер-втрат, це те, що розраховуються не лише прямі втрати, які несе той чи інший сектор економіки, а й дає кількісну оцінку тому що, в першому розділі визначено як систематичний кібер-ризик, тобто, під час кібер-атаки втрати несе не лише таргетна інституція, а присутній ширший макроекономічний ефект по усьому ланцюгу поставок, - що включає інші

сектори економіки, - або ж інших контрагентів інституції. Важливою рисою моделі є те, вхідними даними моделі є леонтієвська таблиця типу «витрати-випуск», відповідно аналіз проводиться на секторальному рівні, а не на рівні окремих ринкових гравців, адже зв’язки на рівні секторів набагато більше очевидні та доступні, в той час як усі зв’язки між інституціями врахувати неможливо.

Загалом є два способи реалізувати теоретичну модель типу нашої: використовуючи таблицю «витрати-випуск», або ж калібровану модель загальної рівноваги (CGE); кожна з яких має свої переваги та недоліки. Обидва підходи враховують поширення змін у попиті та пропозиції на пов’язані сектори, але «витрати-випуск» не враховує ефекту заміщення, тобто впливи одного сектору на інший здійснюється лінійно, натомість калібровану модель загальної рівноваги цей ефект враховує, а попит на продукти та послуги є функцією від ціни. Якщо продукція стає дорожчою, замінники використовуються у виробничому процесі. Подальші розрахунки будуть використовувати метод «витрати-випуск».

Як зазначено в інформаційних ресурсах Мінекономрозвитку: «Таблиці "витрати-випуск" (міжгалузевого балансу) являють собою систему взаємопов'язаних таблиць (матриць) пропозиції ресурсів та їх використання, що відображають склад витрат і формування ресурсів (пропозиції) кожного виду товарів та послуг та використання (попит) товарів та послуг у виробничому споживанні (підприємствами для виробництва), кінцевому споживанні (домашніми господарствами, загальним державним управлінням), валовому нагромадженні (основного капіталу, зміні запасів), експорті. Ці таблиці дають розгорнуту характеристику процесів відтворення та ілюструють взаємозв'язки між виробниками і споживачами та взаємозалежність між видами економічної діяльності».

Для моделювання як методом «витрати-випуск», так і CGE використовується Матриця соціального обліку (Social accounting matrix - SAM). Social Accounting Matrix - це всеосяжна загальноекономічна база даних, що записує дані про всі операції між економічними агентами в конкретній економіці за певний період часу. SAM розширює класичну структуру витрати-випуск, включаючи повний циклічний потік доходів в економіці. Є два важливих аспект SAM: вона є стандартною базою даних для більшості моделей економіки вцілому, оскільки надає дані для економічного моделювання (багатогалузеві лінійні моделі або більш складні обчислювані моделі загальної рівноваги - CGE), і вони показують повний, але інтуїтивно зрозумілий знімок економіки. [41]

Як вже було зазначено, модель типу «витрати-випуск» ґрунтується на розумінні взаємозв'язків в межах економіки. Для того, щоб задовільнити кінцевий попит для усіх продуктів, економіка повинна продукувати більше за кінцевий попит, адже певні продукти використовуються як витрати для виробництва інших продуктів.

Припустимо, що V_c – рівень виробництва в країні c, F_c – вектор кінцевого попиту, A_c – матриця «витрати-випуск», як визначає як відбувається виробництво. Так як рівень виробництва має задовільняти як проміжний попит на витрати на виробництво, а також кінцевий попит споживачів, економіка у рівновазі відповідає рівнянню $V_c = A_c V_c + F_c$. Ми можемо трансформувати рівняння спочатку у $I_n V_c - A_c V_c = F_c$, а тоді – $V_c = (I_n - A_c)^{-1} F_c$, де I_n – одинична матриця. $(I_n - A_c)^{-1}$ є інверсійна матриця Леонтьєва, яка показує, як змінюється випуск в залежності від змін у попиті. Кожне значення у інверсійній матриці Леонтьєва пояснює, як зміни випуску однієї галузі впливає на випуск у іншій галузі. [41] Інверсійна матриця Леонтьєва показує коефіцієнти (економічні множники), що вимірюють послідовний вплив на економіку в

результаті початкового збільшення виробництва певної галузі економічної діяльності. Іншими словами, якщо збільшення виробництва спочатку вимагає більш високого попиту на проміжне споживання для його здійснення, проміжне споживання, у свою чергу, проводиться іншими галузями за рахунок використання нового проміжного споживання тощо. Це те, що відомо як побічний ефект, який виникає між різними галузями діяльності економіки.

Наш підхід розрахунку систематичного кібер-ризику (систематичні втрати випуску s_{cio}) у розрізі понесених втрат різними галузями, насамперед фінансово-банківського, але й економікою вцілому ґрунтується на використанні прямих втрат як зміну витрат у моделі «витрати-випуск»:

$$s_{cio} = \sum_{j \in I} z_{cij} d_{cio} \quad \forall i \in I, c \in C \qquad (3.3)$$

де, z_{cij} – значення інверсійної матриці $(I_n - A_c)^{-1}$, i-та строкам та j-та колонка.

Так як у моделі типу «витрати-випуск» секторальні витрати та витрати ВВП змінюється лінійно, систематичні втрати для певного сектора у структурі ВВП будуть мати значення: $s_{cig} = s_{cio} \frac{w_{ci} G_c}{O_{ci}} \quad \forall i \in I, c \in C.$ Агреговані секторальні втрати дозволяють визначити систематичні сумарні втрати випуску секторів та втрати ВВП $s_{co} = \sum_{i \in I} s_{cio}; \; s_{cg} = \sum_{i \in I} s_{cig} \quad c \in C.$ Отже, тоді сукупні втрати, - тобто прямі і систематичні, - випуску від кібер-загроз для певної країни будуть мати значення $d_{co} + s_{co}$

3.2 Параметри моделі

Попередній пункт зазначав загальні характеристики моделі, реалізованої в Excel. Також потрібно специфікувати певні набори параметрів для запуску

моделі. Дреєр та інші [41] брали за основну економічну статистику дані по 63 країнах OECD, використовуючи Structural Analysis Database. [42] Натомість для цього дослідження використано матриця «витрати-випуск», опублікована Державною службою статистики за 2019 рік, [43] але модифікована під формат OECD. Відповідно із матриці «витрати-випуск» групи випуску ВВП були поєднанні для формування меншої кількості агрегованих секторів необхідних для моделювання (детальніше дивитись Додаток Б).

Для операційного ризик-менеджменту, наприклад, мікро- або макропруденційного нагляду характерно основним «таргетним» показником є дохід компанії, через нього насамперед визначають ступінь впливу ризику. Але протягом звітного періоду і не тільки негативний вплив не обмежується доходом. Точки негативного впливу ризику у нашому випадку є фінансовими експозиціями, і їх у моделі 3:

- Капітальні активи: фізична власність фірми, така як земля, будівлі, комп'ютерне обладнання. Припускається, що кібер-ризик може вплинути на капітальні активи, і таким чином вплинути на дохідність компанії.
- Інтелектуальна власність: власні ідеї, бізнесові практики, патенти, торгові марки та інші процеси, якими володіє фірма. Інтелектуальна власність дозволяє фірмі відмежувати свої продукти від інших. Тому передбачається, що кібер-ризики можуть негативно вплинути на інтелектуальну власність фірми, що також зменшує дохідність внаслідок втрати конкурентних переваг.
- Чистий дохід, тобто розрахований валовий дохід за виключенням валових витрат.

Модель має певні обмеження, які стосуються попереднього набору факторів, стосовно оцінення ступеня впливу ризику: виключення репутаційних втрат напряму, хоча передбачається, що вони входять до «капітальних активів»; відсутність розрахунків на індивідуальному рівні, або на рівні окремих фірм.

Для того що розрахувати кібер-втрати для окремих секторів, потрібно закласти параметри фінансових експозицій для кожного сектора, - насамперед нас цікавить фінансово-банківський сектор, тобто у рамках ймовірносних розподілів задати фактор Y_{cie} - частка від $w_{ci} * G_c$, яка еквівалентна сумі грошей під ризиком від кожного типу фінансової експозиції (e). Тобто можна інтерпретувати Y_{cie} як частку доходу кожного сектору, що еквівалентно сумі грошових коштів репрезентованих кожною фінансовою експозицією, що може піддаватись кібер-атакам.

Для розрахунку впливу експозицій на дохідність і випуск кожного сектору було використано регресійну модель:

$$\log(\text{Валовий дохід}) = b_0 + b_1(\text{Чистий прибуток (Збиток)}X_1) + b_2(\text{Інтелектуальна власність}) + b_3(\text{Загальні Активи}) \quad (3.4)$$

Насамперед нас цікавить калібрування основної моделі для українського банківського сектору. Для розрахунків параметрів із використанням вищенаведеної регресії було використані Балансові залишки 73 діючих українських банків. [46] Потрібно зазначити, що як проксі-змінну для "Інтелектуальна власність" вибрано «Нематеріальні активи», а для "Загальні Активи" – «Загальні активи, усього» за винятком «Основні засоби та нематеріальні активи», «Дебіторська заборгованість щодо поточного податку на прибуток», «Інвестиційна нерухомість», «Інвестиції в асоційовані та дочірні компанії», «Цінні папери, які обліковуються за справедливою та амортизаційною вартістю через інший сукупний дохід, що рефінансуються НБУ», «Кошти в інших банках», адже останні не підпадають напряму під операційний ризик.

Таблиця 3.1 Розрахунок параметру Y_{cie} для фінансового сектору України

N=73	Regression Summary for Dependent Variable: Всього доходів R= .96476834 R?= .93077795 Adjusted R?= .92776830 F(3,69)=309.26 p<0.0000 Std.Error of estimate: 0.20					
	b*	Std.Err.	b	Std.Err.	t(69)	p-value
Intercept			0.245188	0.185288	1.323280	0.190110
Нематеріальні активи	0.193255	0.057482	0.203469	0.060520	3.361995	0.001265
Всього активів	0.559209	0.064693	0.443299	0.051284	8.643983	0.000000
Прибуток/(збиток)	0.278612	0.052904	0.216312	0.041074	5.266414	0.000001

Джерело: власні розрахунки на основі даних [46]

Таким чином логарифмовані значення залежної та нежалежних змінних дають можливість інтерпретувати коефіцієнти біля змінних як відсоткову зміну у експозиціях, що спричиняє відсоткову змінну дохідності (випуску) сектору. Тобто у моделі припускається, що зменшення/знецінення нематеріальних активів на 1% спричинить падіння дохідності на 0.2%, зменшення сукупних активів, які підпадають під операційний ризик, - на 0.4%, недоотримання прибутку – на 0.2%.

Внаслідок того, що метою моделювання є розрахунок прямих системних та загальних втрат саме для фінансового сектору України, а також відсутність відкритих даних стосовно інших секторів виокремлених у моделі, оцінено Y_{cie} лише для банківського сектору, а параметри інших секторів використані ті, що розраховані Дреєром. [41] Останній використав фінансові звітності 4 447 публічних американських компаній протягом 2013-2016 років. Регресійні результати із точкових оцінок також потрібно перевести у інтервальні, використавши розраховане стандартне відхилення. Результати розрахованого для банківського сектору параметру Y_{cie}, а також використані параметри інших секторів подано у наступній таблиці:

Таблиця 3.2 Параметри Y_{cie} моделі для усіх секторів

Sector-Exposure	Capital Assets	Intellectual Property	Net Income
Asset Management and Pensions	U(0.89, 0.92)	U(0, 0.04)	U(0.03, 0.06)
Banking	U(0.35, 0.47)	U(0, 0.4)	U(0.15, 0.27)
Business and Professional Services	U(0.69, 0.93)	U(0.07, 0.30)	U(0, 0.11)
Consumer Goods	U(0.93, 0.97)	U(0, 0.6)	U(0.04, 0.09)
Defense and Aerospace	U(0.91, 0.93)	U(0, 0.03)	U(0.02, 0.05)
Healthcare and Insurance	U(0.89, 0.91)	U(0, 0.05)	U(0.02, 0.06)
Media	U(0.90, 0.95)	U(0, 0.03)	U(0.03, 0.06)
Oil, Gas, and Chemicals	U(0.65, 0.76)	U(0.10, 0.20)	U(0.09, 0.27)
Public	U(0.79, 1)	U(0, 0.08)	U(0, 0.32)
Technology and Electronics	U(0.9, 0.99)	U(0, 0.09)	U(0, 0.09)
Telecom	U(0.85, 0.95)	U(0.09, 0.25)	U(0, 0.03)
Transportation	U(0.89, 1.23)	0	U(0, 0.29)
Utilities	U(0, 1.39)	U(0, 1.39)	U(0,1.21)
Wholesale and Retail	U(0.90, 0.94)	U(0, 0.04)	U(0.03, 0.06)
Other	U(0.93, 0.96)	U(0, 0.02)	U(0.04, 0.06)

Джерело: власні розрахунки автора на основі даних [46], а також результати із [41]

Примітка: U(a,b) – це неперервний рівномірний розподіл

Попередньо було визначено p як загрозу у межах набору загроз P, яка класифікує дію кібер-нападника, що призводить до понесених втрат. Таксономія загроз може бути представлена багатьма способами, як показано у Розділі 1. У моделі використано інший метод для виявлення загроз: використовуючи ланцюжок «кібер-вбивств», розроблений Lockheed Martin. [44] Фази ланцюжки «кібер-вбивств» включають розвідку, вепонізацію (підготовка злочинного програмного забезпечення), доставку, експлуатацію вразливостей системи, установку (злочинного коду), управління та кінцеві дії на таргентий об’єкт. Ми фокусуємося на розумінні остаточних дій на цілі, де витрати реалізуються захисником. Визначено набір взаємовиключних дії щодо цілей як перелік кібер-злочинів (p):

- ексфільтрація даних компанії (наприклад, внутрішніх даних, інтелекуальної власності або комерційної таємниці); витрати включають збитки через витік даних, які належать компанії;

- ексфільтрація даних клієнтів (наприклад, втрата персональної ідентифікуючої інформації); втрати включають витрати на повідомлення клієнів і компенсацію збитків;
- деградація, знищення і пошкодження даних і систем, включаючи кібер-фізичні системи;
- зупинка функціонування бізнесу внаслідок порушення роботи систем і активів, а також атак типу "відмова в обслуговуванні".

Обгронувавши чим є наші кібер-загрози на фінасові ексозиції, повернімося до Формули 1.1, щоб задати параметр X_{ciep} - частка експозиції під ризиком в країні c, секторі i і схильності до ризику типу експозиції (e), що буде успішно знищено, вкрадено чи іншим чином втрачено через певну кібер-загрозу(p)

Без прив'язки до секторів взаємозв'зок загроз та фінансових експозицій, тобто на що конкретно при оцінці ці загрози мають свій негативний вплив, - частка від сукупного продукту виробленого секторами економіки показано у наступній таблиці у вигляді трикутних ймовірносних розподілів.

Таблиця 3.3 Взаємодія кібер-загроз на фінансових експозиції (X_{ciep})

Сектори	Загрози-фінансові експозиції	Капітальні активи	Інтелектуальна власність	Чистий дохід
Усі сектри	ексфільтрація даних компанії	T(0,0.0043,0.021)	T(0,0.00012,0.00096)	T(0,0.0015,0.0032)
Усі сектри	ексфільтрація даних клієнтів	T(0,0.0043,0.021)	T(0,0.00012,0.00096)	T(0,0.0015,0.0032)
Усі сектри	деградація, знищення і пошкодження даних	T(0,0.0083,0.041)	T(0,0.00025,0.0021)	T(0,0.0031,0.0079)
Усі сектри	зупинка функціонування бізнесу	T(0,0.0083,0.041)	T(0,0.00025,0.0021)	T(0,0.0031,0.0079)

Джерело: розраховано автором на основі [Dreyer, 45]

Щоб побудувати попередню таблицю використане компексне дослідження Deloitte [45], пристосувавши їхню таксономію до використаної в моделі (див. Таблицю 3.4):

Таблиця 3.4 Пристосування загроз Deloitte до загроз моделі

Загрози Deloitte	Загрози моделі			
	ексфільтрація даних компанії	ексфільтрація даних клієнтів	деградація, знищення і пошкодження даних	зупинка функціонування бізнесу
Кібер-фізична			X	
Витік даних	X	X		
Знищення або видалення даних			X	X
Шкідливе програмне забезпечення	X	X		X
Програма-вимагач	X	X		X
Саботаж			X	X

Джерело: розраховано автором на основі [Dreyer, 45]

3.3 Результати моделі

Якщо провести моделювання із закладеними у попередньому розділі параметрами X_{ciep} та Y_{cie}, то секторальні втрати у абсолютних і відносних числах від кібер-загроз у розрізі прямих та системачних втрат у 2019 році (за матрицею «витрати-випуск» Держстату) будуть складати (див. Рисунок 3.1):

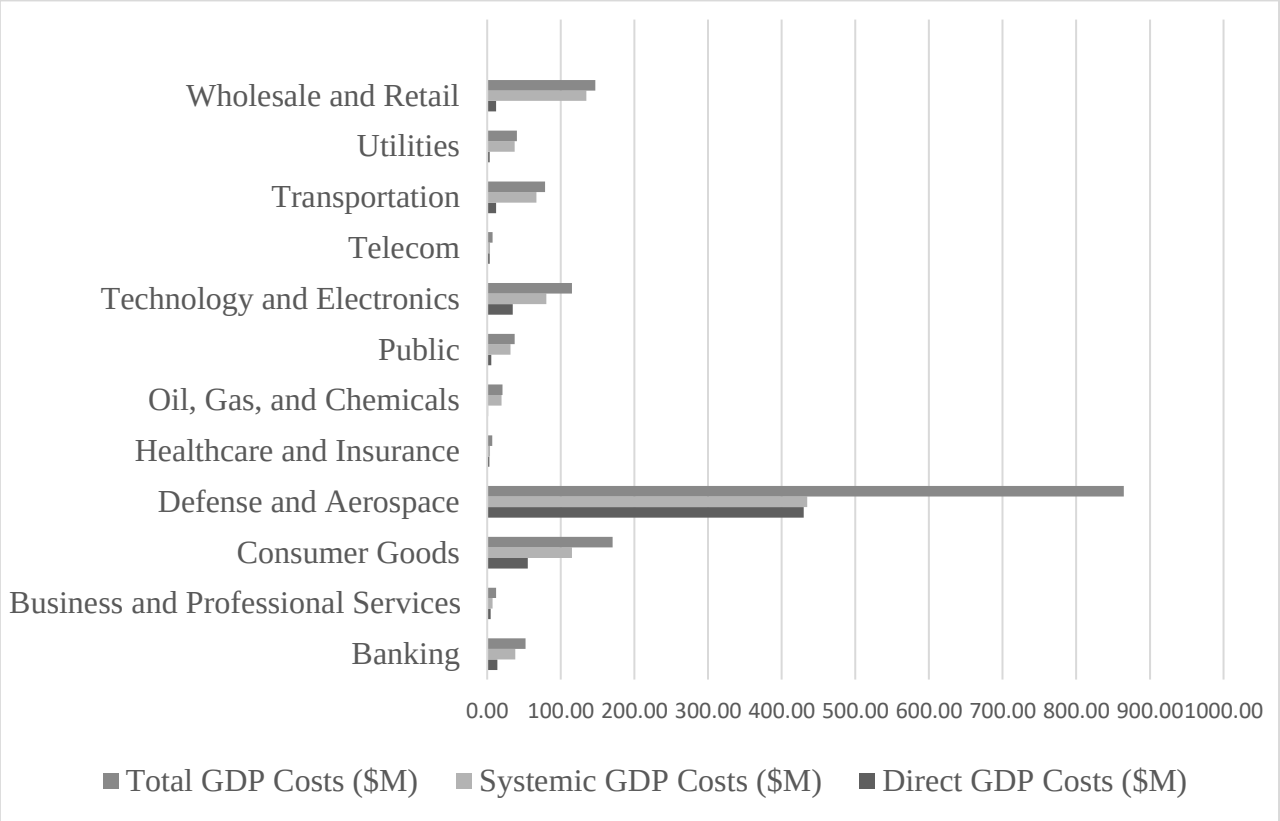

Рисунок 3.1 – Секторальні втрати від кібер-подій у розрізі прямих, систематичних та сукупних втрат

Джерело: власні розрахунки на основі даних [43, 45, 46]

Добуток X_{ciep} та Y_{cie}, що покриває фінансові експозиції (в якій мірі «страждають» активи компаній за заданого рівня впливу ризиків), дає можливість розрахувати мультиплікатори, які накладаються на випуск сектору відповідно до матриці «витрати-випуск» і отримуються секторальні втрати від кібер-ризику в Україні. За розрахунками моделі 4 сектори мають більші втрати за фінансово-банківський: «Defense and Aerospace», «Technology and Electronics», «Consumer Goods» та «Transportation». Прямі втрати від кібер-ризику для українського фінансово-банківського сектору складають 14.05 млн дол, систематичні 38.03 млн дол, що свідчить про значну концентрацію ризиків внаслідок високої значимості системно важливих інституцій та кореляцію ризиків, наприклад, витік персональної ідентифікаційної інформації є систематичною загрозою.

Рисунок 3.2 показує що за усередненого сценарію банківський сектор щорічно втрачає близько 1 % свого випуску внаслідок кібер-втрат, що є середнім значенням серед інших виокремлених секторів, тому не доводиться фіксувати особливу вразливість фінансового сектору порівняно з іншими. До того ж 0.7% це систематичні втрати, що стосуються насамперед дій регулятора НБУ та нормативних вимог (див. Рисунки 3.5-3.5):

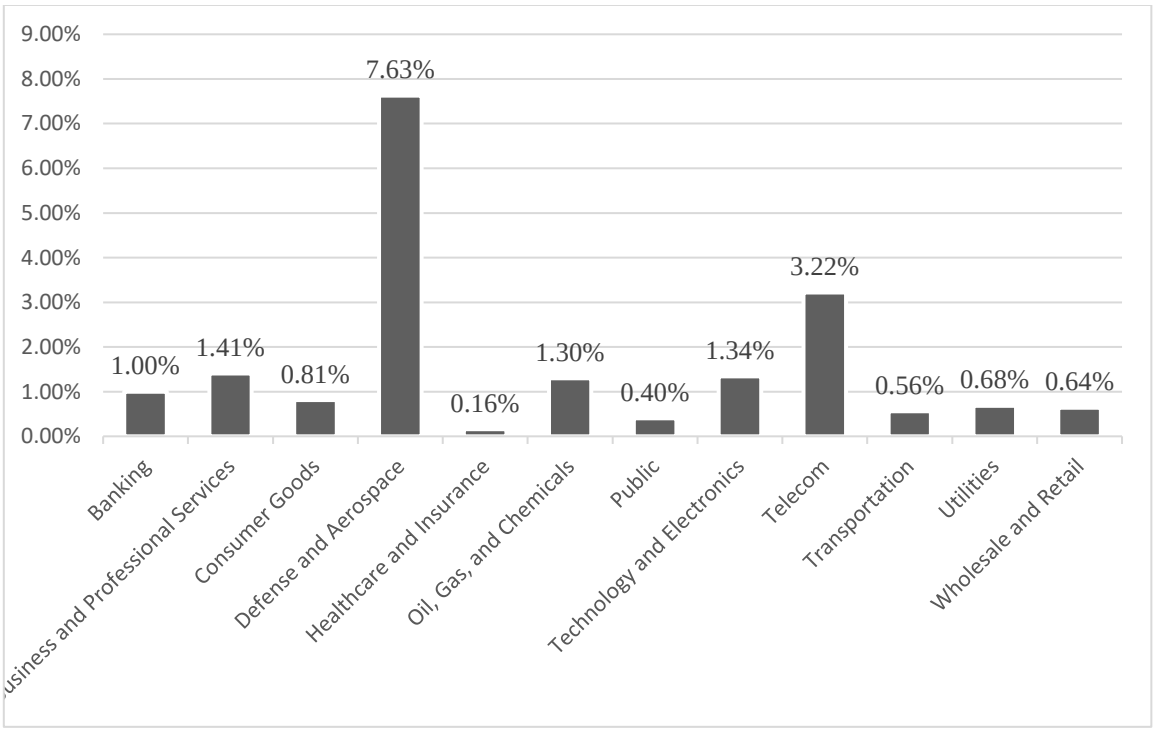

Рисунок 3.2 – Сукупні втрати по кожному секторів у вигляді % від кожного сектора

Джерело: власні розрахунки на основі даних [43, 45, 46]

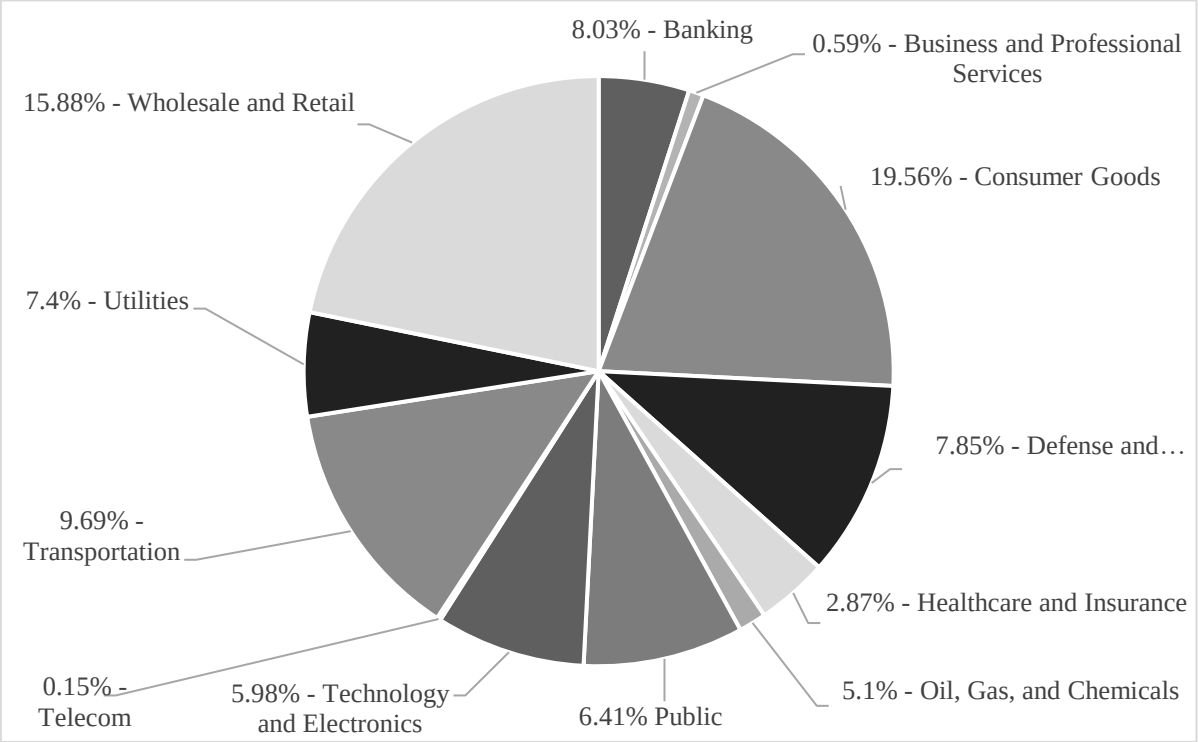

Рисунок 3.3 – Розподіл ВВП на сектори

Джерело: власні розрахунки на основі даних [43, 45, 46]

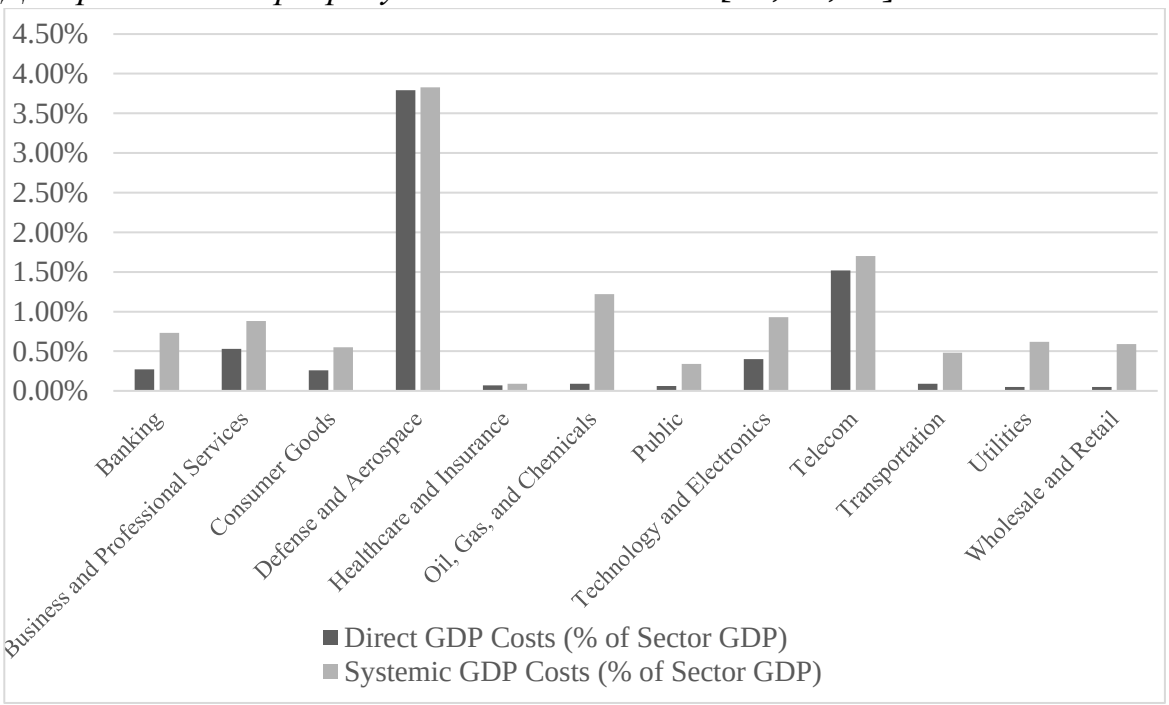

Рисунок 3.4 – Відсоткові втрати в межах внеску сектора у ВВП

Джерело: власні розрахунки на основі даних [43, 45, 46]

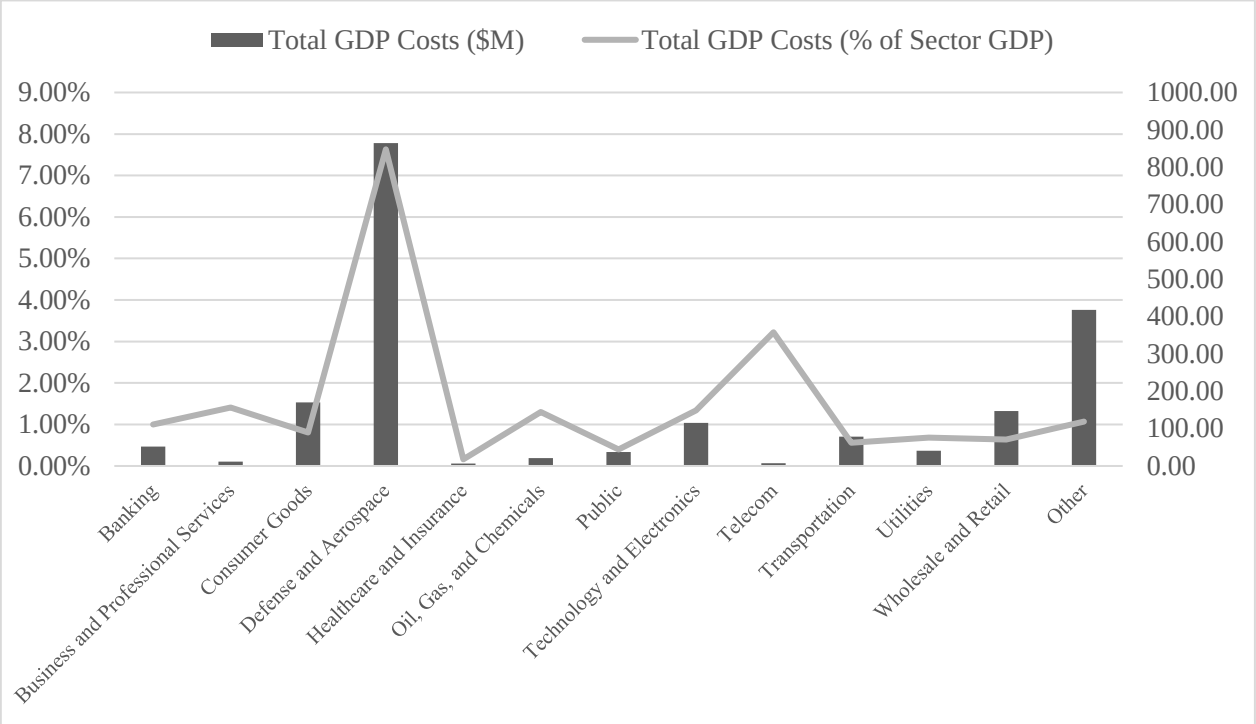

Рисунок 3.5 – Кібер-втрати в межах внеску сектора у ВВП

Джерело: власні розрахунки автора на основі даних [43, 45, 46]

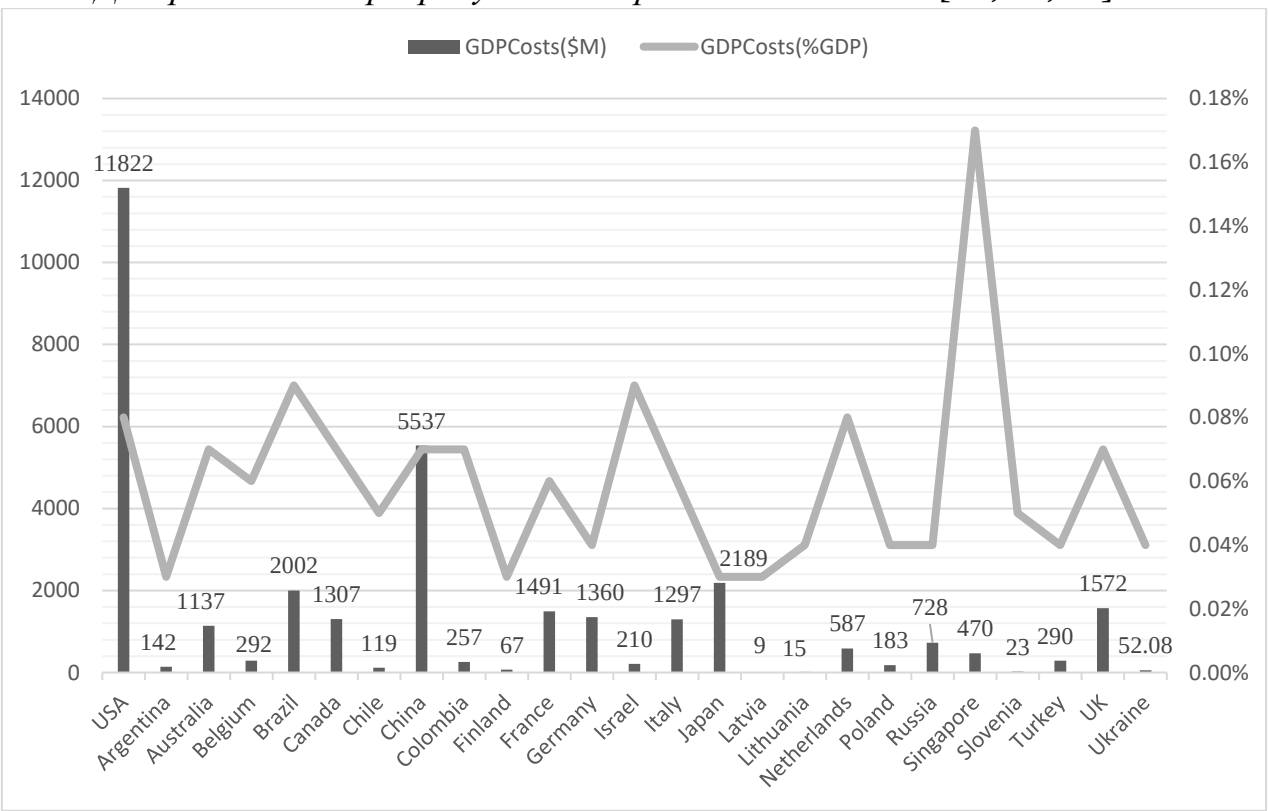

Рисунок 3.6 – Кібер-втрати фінансово-банківського сектору серед країн

Джерело: власні розрахунки автора на основі даних [43, 45, 46]

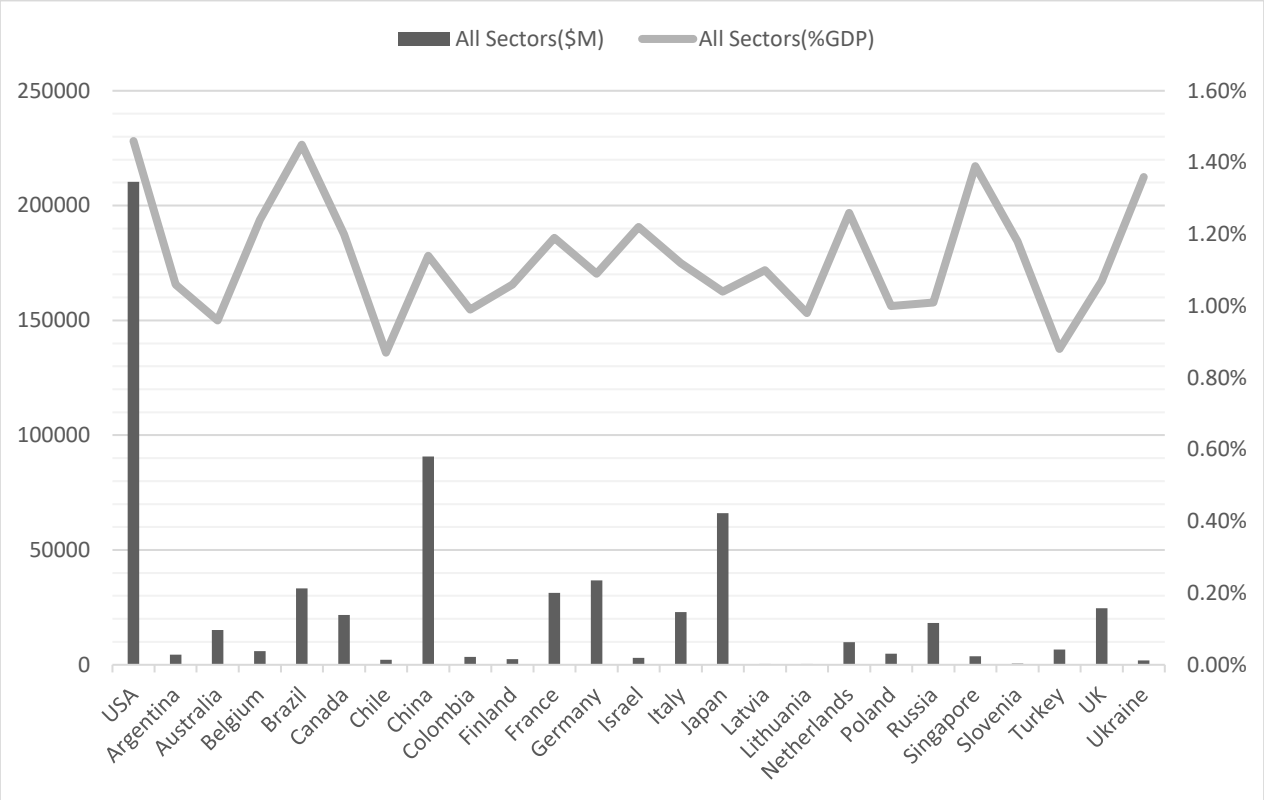

Рисунок 3.7 – Кібер-втрати усіх секторів серед країн

Джерело: власні розрахунки автора на основі даних [43, 45, 46]

Якщо порівнювати фінансово-банківський сектор України на предмет вразливості до кібер-ризиків серед інших країн, то можна сказати, що він нижче середнього рівня - 0.04% ВВП, як і в Росії, Польщі, Німеччині (див. Рнисунок 3.7). Натомість закономірно, що цей показник вищий серед країн, де фінансове посередництво займає високі відносні та абсолютні показники випуску: США - найбільше, адже саме там наймасштабніша і найбільш розгалужена система фінансових інститутів, - Японія, Сінгапур, Велика Британія, Китай.

У той же час, хоча втрати фінансового сектору України серед інших порівняно незначні, в цілому усі сектори «коштують» випуску економіки 1.4% на рівні із Сінгапуромом, США.

3.4 Рекомендації стосовно менеджменту та регуляції кібер-загроз

Ідентифікація, аналіз та оцінка кібер-ризиків це складова процесів ідентифікації загроз, і нею потрібно керувати за допомогою загальноприйнятих та специфічних методів управляння ризиками. Активний менеджмент є критично важливим для вжиття заходів, пов’язаних із кібер-безпекою. У цьому пункті надані певні рекомендації, як упереджувати кібер-ризик на рівні бізнесової одиниці, як національні регулятивні органи можуть зменшити системний кібер-ризик, та які розроблені міжнародні стандарти для цього розроблені. Основними заходами є уникнення, зменшення та перенесення ризику:

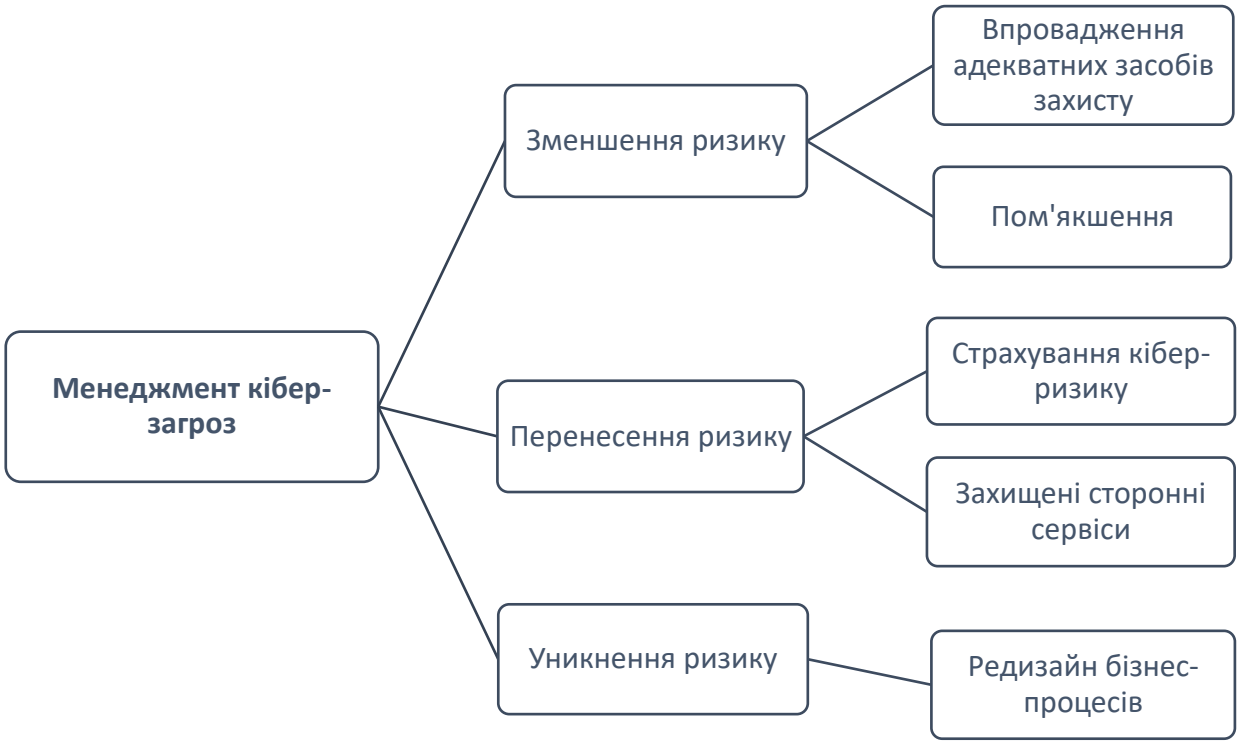

Рисунок 3.8 – Основні заходи менеджменту кібер-загроз

Джерело: розроблено автором

Зменшення ризику. Ризик може бути зменшений через активні попередні (ex-ante) заходи ризик-менеджменту через виміряння і приведення

ймовірності та вартості ризику до рівня, що є співмірними із визначеним для компанії профілем ризиків. Даний процес передбачає реалізацію спектру захисних заходів, що можуть бути як фізичними (паркани, замки), так і цифровими (захисне програмне забезпечення: файєрволи, криптування даних тощо), або ж із задіянням працівників (тренінги із цифрової безпеки, доступ до інформації через складну систему погоджень).

Уникнення ризику. Більш фундаментальний підхід до управління схильністю до кібер-ризиків стосується трансформації операційних бізнес-процесів: реалізацію чи зміну бізнес-моделі, процесингу платежів тощо. Тим не менше, цей динамічний процес із новими технологіями сам створює нові вразливості, що цілком можуть бути зрозумілими лише з часом.

Перенесення ризику. Даний спосіб управління ризиком передбачує купівлю страхових продуктів або ж перенесення операційних ризиків контрагенту третій стороні.

Незалежно від розміру фінансової установи, існує кілька основних заходів, які фірми можуть вжити для вирішення ідіосинкратичного (недиверсифікованого) кібер-ризику. Незважаючи на величезні технологічні темпи за останні десятиліття рецепти та рекомендації були відносно постійними. Різні експерти з комп'ютерної безпеки фактично пропонують майже однакові списки дій, які включають:

- Білий список додатків (запускайте лише попередньо затверджене програмне забезпечення на комп’ютерах фірм);
- Використання стандартизованих конфігурацій системи захисту (оскільки складні конфігурації більше важко захищати);
- Наявність процесів для виправлення (ремонту) системного та прикладного програмного забезпечення протягом короткого періоду.

- Обмеження кількості осіб, які мають права адміністратора у комп’ютерних системах;
- Використання хмарних інфраструктур як сервісів. [49]

Банки розраховують нормативні вимоги до капіталу як суму очікуваних і непередбачених збитків. Рамки операційних ризиків включають необхідність кількісної оцінки хвостових ризиків при розрахунку регулятивного капіталу. Нормативи регулятивного капіталу вимагають, щоб банки відкладали капітал на операційний ризик з метою поглинання непередбачених збитків. Невід'ємною частиною цього підходу має бути використання сценарного аналізу із закладеними критичними наслідками реалізації кібер-ризиків у поєднанні із зовнішніми даними для оцінки хвостового ризику. Сюди входить оцінка потенційних втрат, що виникають в результаті декількох одночасних операційних втрат. З часом такі оцінки необхідно перевіряти і переглядати шляхом зіставлення з фактичними втратами. Сценарний аналіз може допомогти установам зрозуміти потенційні ризики, те, як вони можуть передаватися, де необхідно здійснювати інвестиції і як найкраще реагувати на порушення. Інформація із сценарного аналізу може допомогти поліпшити фінансове планування і планування на випадок непередбачених обставин, але спочатку необхідно зменшити асиметрію інформації за рахунок обміну даними. Великі банківські холдингові компанії (BHC) матимуть найдосконаліші обороноздатні можливості і зможуть оговтатися від будь-якої атаки протягом двох годин. З 2013 року вони включають кібер-ризики та операційні ризики в сценарії, які вони подають у свої щорічні стрес-тести. У США банки готують ці сценарії як частину стрес-тестів, необхідних відповідно до закону Додда-Франка. Для української банківської системи врахування врахування кібер-ризиків під час стрес-тестування могло би теж бути корисною рекомендацією.

Регулювання сектора фінансових послуг спрямоване на сприяння довгостроковому економічному зростанню і мінімізування витрат і негативних зовнішніх наслідків фінансової нестабільності. Однак, щоб залишатися ефективним, регулювання може потребувати адаптації до нових технологічних досягнень і факторів ризику, такі як кібер-ризик.

Як було доведено раніше систематичний кібер-ризик переважає для фінансової індустрії (згідно з моделлю близько 70%), отже явну роль виконують державні регулятори та нормотворці у визначені пов'язаних з цифровими загрозами термінів і стандартів, цифрового нагляду, збиранні інформації, об' єднанні її для збереження конфіденційності. [11]

По-перше, для забезпечення узгодженості класифікації кібер-заходів між фірмами та країнами, необхідно розробити загальну термінологію та ідентичні визначення термінів кібер-ризиків. Загальні рамки та приклади такої класифікації подані у першому розділі.

По-друге, слід інституціоналізувати обмін інформацією між правоохоронними органами, наглядовими органами, регулюючими органами та приватним сектором. Систематичний збір і обмін кібер-даними, в тому числі про частоту і фінансовий вплив кібер-подій, допоможе поліпшити розуміння розміру і характеру кібер-подій. Надійна система звітування про кібер-ризики має вирішальне значення. Національні органи влади та нормативні акти повинні забезпечувати правильні стимули для забезпечення своєчасного та точного повідомлення про кібер-події. Стандарти кібер-ризику повинні вимагати, щоб фінансові установи надавали внутрішні дані про кібер-ризики спочатку періодично, а згодом і в режимі реального часу. Перевірка надійності даних та автоматизована обробка будуть відповідальністю установників стандартів. Основною дослідницькою проблемою у цій роботі, а також проаналізованих більшість інших. Є відсутність, недосконалість або неповність

даних пов’язаних із кібер-втратами, що робить недосконалими і ненадійними для практичного менеджменту моделі оцінки кібер-ризиків.

По-третє, щоб подолати стурбованість галузі щодо обміну інформацією та потенційних наслідків для репутації, інформація окремих фірм повинна бути анонімізована і/або агрегована до рівня, який дає достатнє розуміння фінансових наслідків кібер-атак і порушень при збереженні конфіденційності інформації.

По-четверте, необхідно забезпечити публічний доступ до інформації і даних, з тим щоб фірми, наглядові органи та регулюючі органи могли використовувати ці джерела в якості вхідних даних для своїх моделей управління ризиками та вдосконалювати механізми спостереження і раннього попередження.

Також через кримінальний характер кібератак регуляторам потрібно буде координувати роботу з відповідними правоохоронними органами. Мають бути підписані офіційні домовленості про двосторонній обмін інформацією між правоохоронними органами та регуляторними органами.

У тісно глобально взаємопов'язаній ІТ- та фінансовій системі вирішальне значення матиме ефективна координація на національному та міжнародному рівнях. Урядам необхідно забезпечити, щоб різні установи співпрацювали один з одним. Оскільки кібер-ризик не обмежується політичними або географічними бар'єрами, необхідна також міжнародна координація політики. Міжнародні організації, такі як Банк міжнародних розрахунків, Рада з фінансової стабільності або МВФ, можуть відігравати ключову роль у сприянні координації, підтримці обміну інформацією. Агрегація кіберризиків занадто складна для управління на рівні окремих фірм, галузей або навіть країн, як було показано у першому розділі. Це глобальне джерело системного ризику, яке необхідно вирішувати на наднаціональному рівні.

Стандарти управління ризиками для пов'язаних з IT ризиків розробляються міжнародними органами встановлення стандартів і застосовуються на секторальній основі. Для фірм, що займаються фінансовими послугами, органи встановлення стандартів створили нормативну рамку, що встановлює мінімальні стандарти для заохочення більш ефективного управління ризиками та виділення капіталу на неочікувані збитки, включаючи кібер-ризики. Стандарти застосовуються в розбивці по секторах (див. малюнок 7). Існуюча рамка для банків складається з різних стандарті, напри клад, «Basel Core Principles», [50] «the Principles for the Sound management of Operational Risk», [51] підкріплені «Basel Capital Accord». [52]

У зв 'язку з високою залежністю від технологій на ринках цінних паперів і деривативів були впроваджені чіткі стандарти кіберстійкості. Операційні ризики, пов'язані з платежами та розрахунками, можуть поширитися на фінансові ринки в цілому. Спільний документ Комітету з платіжних і ринкових інфраструктурах і Ради Міжнародної організації з цінних паперів має назві "Управління кіберстійкістю для інфрастуктур фінансових ринків" [53]. Керівництво двох згаданих організацій розробників стандартів вимагає високих стандартів управління операційними ризиками для систем платежів, клірингу та розрахунків.

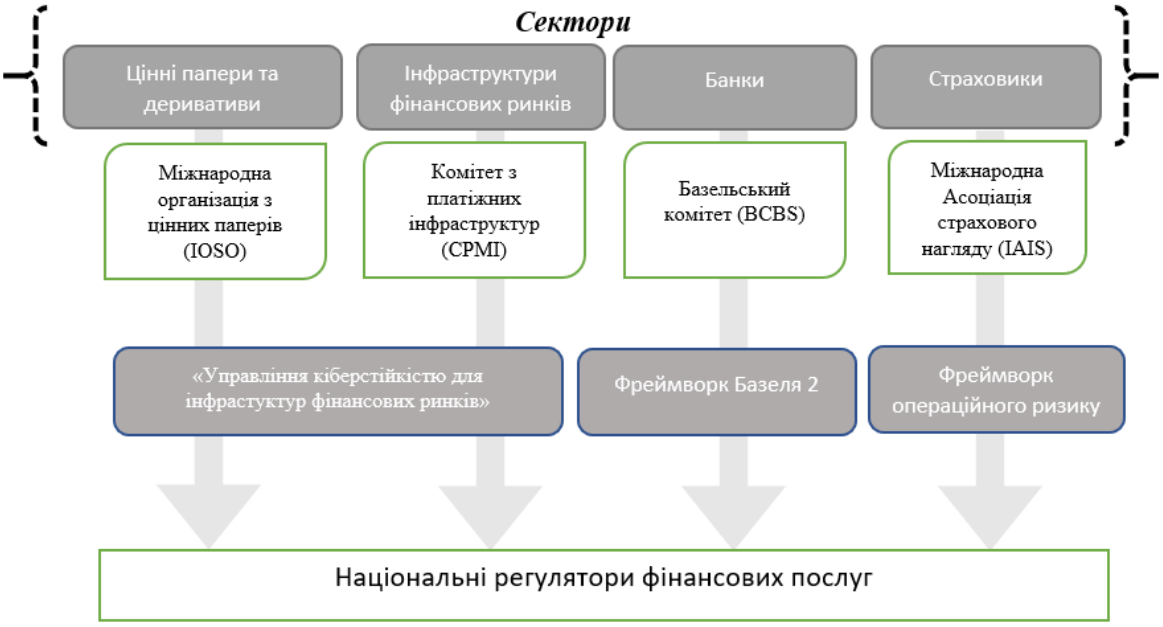

Рисунок 3.9 – Міжнародні стандарти кіберстійкості

Джерело: розроблено автором

Група держав G7 зробила перший крок до стандартизованих вимог до кібер-ризику. G7 розробила набір основних елементів високого рівня, призначених для приватних та державних структур фінансового сектору. Елементи є будівельними блоками, на основі яких інституція може розробляти та реалізовувати свою стратегію кібер-безпеки та операційну систему. Державні органи в межах і між юрисдикціями можуть використовувати ці елементи, а також спрямовувати свою державну політику, регулятивні та наглядові практики. Елементи включають:

1. Елемент 1: Стратегія та рамки кібер-безпеки.

«Розробити та підтримувати стратегію та основи кібер-безпеки з урахуванням конкретних кібер-ризиків та належним чином враховувати міжнародні, національні та галузеві стандарти та керівні принципи.» [48]

2. Елемент 2: Урядування.

«Визначити та сприяти виконанню ролей та відповідальності персоналу, який впроваджує, керує та контролює ефективність стратегії та рамок кібер-

безпеки для забезпечення підзвітності; і забезпечити належні ресурси, відповідні повноваження та доступ до керівного органу.» [48]

3. Елемент 3: Оцінка ризиків та контролю.

«Визначте функції, види діяльності, продукти та послуги - включаючи взаємозв’язки, залежності та треті сторони - визначте пріоритет їх відносної важливості та оцініть відповідні кібер-ризики. Визначити та впровадити засоби контролю - включаючи системи, політику, процедури та навчання - для захисту від цих ризиків та управління ними в межах допуску, встановленого керівним органом.» [48]

4. Елемент 4: Моніторинг.

«Встановити систематичні процеси моніторингу для швидкого виявлення кібер-інцидентів та періодичної оцінки ефективності виявлених засобів контролю, в тому числі шляхом моніторингу мережі, тестування, аудиту.» [48]

5. Елемент 5: Відповідь.

«Своєчасно (a) оцінювати характер, масштаби та вплив кібер-інциденту; (b) стримувати інцидент та пом'якшувати його вплив; (c) повідомляти внутрішніх та зовнішніх зацікавлених сторін (таких як правоохоронні органи, регуляторні органи та інші органи державної влади, а також акціонерів, сторонніх постачальників послуг та замовників); та (d) координувати за необхідністю спільні заходи реагування. В рамках оцінки ризиків та контролю суб'єкти господарювання повинні впроваджувати політику реагування на аварії та інші засоби контролю, щоб сприяти ефективному реагуванню на аварії.» [48]

6. Елемент 6: Відновлення.

«Відновити операції, дозволяючи при цьому продовжувати санацію, в тому числі шляхом (a) усунення шкідливих залишків інциденту; (b) відновлення систем та даних до нормального стану та підтвердження нормального стану; (c) виявлення та пом'якшення всіх вразливих місць, які

були використані; (г) усунення вразливостей для запобігання подібним інцидентам; та (е) належним чином проведення комунікації.» [48]

7. Елемент 7: Поширення інформації.

«Залучати до своєчасного обміну надійною, ефективною інформацією щодо кібер-безпеки з внутрішніми та зовнішніми зацікавленими сторонами (включаючи суб'єкти та органи державної влади у фінансовому секторі та за його межами) щодо загроз, вразливостей, інцидентів та реакцій для підвищення захищеності, обмеження збитків, підвищення ситуаційної обізнаності.» [48]

Висновок до Розділу 3

У Розділі 3 описано модель, за допомогою якою розраховуються втрати від реалізованого кібер-ризику (кібер-атак) для економіки України у розрізі секторів економіки (насамперед нас цікавить фінансово-банківський сектор), поділу на прямий та систематичний кібер-ризик, макроекономічний поділ на секторальний випуск та частку ВВП та інші аспекти. Вхідними даними моделі є леонтієвська таблиця типу «витрати-випуск», відповідно аналіз проводиться на секторальному рівні, а не на рівні окремих ринкових гравців.

Для того що розрахувати кібер-втрати для окремих секторів, потрібно закласти параметри фінансових експозицій для кожного сектора. Для цього побудовано економетричну модель. Відповідно у основну мудель включається наступні значення фактору фінансових експозицій для українського фінансово-банківського сектору: що зменшення/знецінення нематеріальних активів на 1% спричинить падіння дохідності на 0.2%, зменшення сукупних активів, які підпадають під операційний ризик, - на 0.4%, недоотримання прибутку – на 0.2%.

Результати моделювання подані у третьому пункті розділу. Прямі втрати від кібер-ризику для українського фінансово-банківського сектору складають

14.05 млн дол, систематичні 38.03 млн дол, що свідчить про значну концентрацію ризиків внаслідок високої значимості системно важливих інституцій та кореляцію ризиків, наприклад, витік персональної ідентифікаційної інформації є систематичною загрозою. Банківський сектор щорічно втрачає близько 1% свого випуску внаслідок кібер-втрат, на рівні і Сінгапуром, США, що є середнім значенням серед інших виокремлених секторів. До того ж 0.7% це систематичні втрати, що стосуються насамперед дій регулятора НБУ та нормативних вимог.

Активний менеджмент є критично важливим для вжиття заходів, пов’язаних із кібер-безпекою. В останньому пункті розділу надані певні рекомендації, як упереджувати кібер-ризик на рівні бізнесової одиниці, як національні регулятивні органи можуть зменшити системний кібер-ризик, та які розроблені міжнародні стандарти для цього розроблені. Основними заходами є уникнення (фундаментальна зміна бізнес-процесів), зменшення (тренінги для працівників, стрес-тести) та перенесення (купівля страхових продуктів) ризику. Представлено кілька беззаперечних рекомендацій, що зроблять інституцію кібер стійкішою: білий список додатків, використання стандартизованих конфігурацій системи захисту, обмеження кількості осіб, які мають права адміністратора у комп’ютерних системах; використання хмарних інфраструктур як сервісів. Також надано низку рекомендацій для регуляторів фінансового сектору:

- необхідно розробити загальну термінологію та ідентичні визначення термінів кібер-ризиків;
- слід інституціоналізувати обмін інформацією між правоохоронними органами, наглядовими органами, регулюючими органами та приватним сектором. Систематичний збір і обмін кібер-даними, в тому числі про

частоту і фінансовий вплив кібер-подій, допоможе поліпшити розуміння розміру і характеру кібер-подій;

- стандарти кібер-ризику повинні вимагати, щоб фінансові установи надавали внутрішні дані про кібер-ризики спочатку періодично, а згодом і в режимі реального часу. По-третє, щоб подолати стурбованість галузі щодо обміну інформацією та потенційних наслідків для репутації, інформація окремих фірм повинна бути анонімізована і/або агрегована до рівня, який дає достатнє розуміння фінансових наслідків кібер-атак і порушень при збереженні конфіденційності інформації,
- необхідно забезпечити публічний доступ до інформації і даних, з тим щоб фірми, наглядові органи та регулюючі органи могли використовувати ці джерела в якості вхідних даних для своїх моделей управління ризиками;
- регуляторам потрібно буде координувати роботу з відповідними правоохоронними органами. Мають бути підписані офіційні домовленості про двосторонній обмін інформацією між правоохоронними органами та регуляторними органами.

Наприкінці розділу представлено найважливіші міжнародні стандарти щодо забезпечення кібер-стійкості фінансового сектору. Для фірм, що займаються фінансовими послугами, органи встановлення стандартів створили нормативну рамку, що встановлює мінімальні стандарти для заохочення більш ефективного управління ризиками та виділення капіталу на неочікувані збитки, включаючи кібер-ризики.

ВИСНОВКИ

Кібер-атаки зростають експоненційно з року в рік. Архітектура сучасних ринків базується на тому, що фінансові інституції є критичними для глобальної комерції та операцій на всіх рівнях: місцевому, державному та міжнародному. Індустрія фінансових інституцій надзвичайно широка: від традиційних акторів на зразок класичних банків, платформ для торгівлі цінними паперами та їх деривативами, інвестиційних, пенсійних чи хеджфондів до фінансових платформ та платіжних систем, створених фінтех-інженерами, наприклад Bitcoin. Внаслідок державних регуляцій та власних бізнес-моделей ці інституцій збирають, оброблюють та зберігають значні обсяги персональної інформації клієнтів-фізосіб, а також інших даних про своїх клієнтів, контр-агентів, та власну діяльність. Саме завдяки останнім властивостям фінансові інституції є високо привабливими для хакерів, а також вразливими з точки зору операційно-технологічного менеджменту.

Статистично підтверджується, що фінансовий сектор переживає найбільшу кількість кібер-інцидентів, у тому числі найбільше кібер-атак. Тим не менше, банки та страхові компанії піддаються меншим втратам відносно інших секторів. Також у другому пункті другого розділу представлено оцінки деяких факторів, які є драйверами кібер-ризику. Кібер-втрати мають малу часту серед усіх спричинених критичними операційними подіями, але кібер-капітал під ризиком (VaR) може спричинювати до третини усього операційного капіталу під ризиком для банківських установ. Розрахований капітал під ризиком (VaR) для кібер-загроз як частки операційних встановив, що значення капіталу під ризиком варіюються у межах 0.25-0.65% валового прибутку. А із врахуванням «товстих хвостів» - 14% і більше від прибутку банку. [10]

Одним із найважливіших аспектів регулювання кібер-безпекової системи як з боку суверенних урядів, так і наднаціональних органів є (недиверсифікований) систематичний кібер-ризик, - ризик, що кібер-подія спрямована на окремий елемент критичної інфраструктури екосистеми спричинить затримку, відмову, поломку або втрату, так що вплив поширюється не лише на даний окремий компонент, а каскадно на логічно зв'язані компоненти, і в результаті призводить до значних негативних ефектів на публічне благополуччя. Систематичний кібер-ризик слід зараховувати до системотворчих факторів фінансової стабільності, який має такі головні трансмісійні механізми: концентрація внаслідок недостатності замінності (одних інфраструктур іншими), втрата довіри внаслідок кореляцій ризиків, та підсилююча роль взаємозалежності (контагіозний ефект), які можуть підірвати фінансову стабільність системи. Моделювання показало, прямі втрати від кібер-ризику для українського фінансово-банківського сектору складають 14.05 млн дол, систематичні - 38.03 млн дол, що свідчить про значну концентрацію ризиків внаслідок високої значимості системно важливих інституцій та кореляцію ризиків. За усередненого сценарію банківський сектор щорічно втрачає близько 1% свого випуску внаслідок кібер-втрат, що є середнім значенням серед інших виокремлених секторів, тому не доводиться фіксувати особливу вразливість фінансового сектору порівняно з іншими. До того ж 0.7% це систематичні втрати, що стосуються насамперед дій регулятора НБУ та нормативних вимог. Уцілому усі сектори внаслідок реалізованого кібер-ризику «коштують» економіці 1.4% ВВП, схожий ризик-профіль наявний у Сінгапура та США.

Активний менеджмент є критично важливим для вжиття заходів, пов'язаних із кібер-безпекою. В останньому пункті розділу надані певні рекомендації, як упереджувати кібер-ризик на рівні бізнесової одиниці, як національні регулятивні органи можуть зменшити системний кібер-ризик, та які міжнародні стандарти для цього розроблені. Основними заходами ризик-

менеджменту є уникнення (фундаментальна зміна бізнес-процесів), зменшення (тренінги для працівників, стрес-тести) та перенесення (купівля страхових продуктів) ризику. Тим не менше основною проблемою розроблення страхових продуктів, які би покривали ІТ-безпеку фірми є належний незалежний аудит інформаційних систем, політик і практик. Останнє в Україні поки що є в зародковому стані, хоча в 2021 році НБУ висунув обов'язковою умовою для банків проведення такого незалежного аудиту. Також представлено кілька беззаперечних порад, що зроблять інституцію кібер- стійкішою, таких як білий список додатків, обмеження кількості осіб, які мають права адміністратора у комп'ютерних системах, використання хмарних сервісів та інше. Також надано низку рекомендацій для регуляторів фінансового сектору, наприклад, слід інституціоналізувати обмін інформацією між правоохоронними органами, наглядовими органами, регулюючими органами, приватним сектором та широким загалом зацікавлених осіб для проведення досліджень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) Sarah Gordon & Richard Ford, On the Definition and Classification of Cybercrime, 2 J. Computer Virology 13, 14 (2006);

2) Fin. Indus. Regulatory Auth [Електронний ресурс] . supra note 83 – URI: https:.core.ac.uk/download/pdf/72835234.pdf

3) Taplin R. Managing Cyber Risk in the Financial Sector / Ruth Taplin. – New York,, 2016. 196 с.

4) Moitra, S. Developing policies for cybercrime, European Journal of Crime, Criminal Law and Criminal, 13(3): 2005, с. 435–64.

5) Amy F. Systematic Risk [Електронний ресурс] / Fontinelle Amy. Investopedia. 2020. URI: https:.www.investopedia.com/terms/s/systematicrisk.asp

6) Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments [Електронний ресурс] . Press Release, N.Y. Dep't of Fin. Servs. 2014. URI: http:.www.dfs.ny.gov/about/press/pr1412101.htm.

7) Frederic S. M. Systemic risk and the international lender of last resort [Електронний ресурс] / Mishkin Frederic S. BIS. 2007. URI: https:.www.bis.org/review/r071003f.pdf.

8) J M. Top 10 most common types of cyber attacks [Електронний ресурс] / Melnick J . Netwrix.com. 2018. URI: https:.blog.netwrix.com/2018/05/15/top-10-most-com mon-types-of-cyber-attacks/.

9) Cebula J. A taxonomy of Operational Cyber Security Risks / J. Cebula, L. Young. Software Engineering Institute, Carnegie Mellon University. 2010. с. 25.

10) Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment / Antoine Bouveret. IMF Working Paper. –2018.

11) Kopp E. Cyber Risk, Market Failures, and Financial Stability / E. Kopp, L. Kaffenberger, C. Wilson. . IMF Working Paper. 2017. №17.

12) Глазьев С.Ю., Харитонов В.В. Нанотехнологии как ключевой фактор нового технологического уклада в экономике. - Монографія, 2009. 304 с.

13) Tapscott D. The Digital Economy / Tapscott. – New York: McGraw-Hill, 1995. 342 с

14) Бажал Ю. Інформаційна економіка. Роль інформації у формуванні ринкової економіки: монографія / Ю. Бажал, В. Бакуменко, І. Бондарчук та ін.; за заг. ред. І. Розпутенка. Київ : К.І.С., 2004. С. 33–57.

15) Коломієць Г. М., Глушач Ю. С. Цифрова економіка: контроверсійність змісту і впливу на господарський розвиток. Бізнес Інформ, 2017. № 7. С. 137–143.

16) Data Breach Investigations Report 2016 [Електронний ресурс] . Verizon Enterprise, 2016. URI: http:.www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

17) Aldasoro I. Operational and cyber risks in the financial sector / I. Aldasoro, L. Gambacorta, P. Giudici. BIS Working Papers, 2020. №840.

18) The new Basel capital accord. Consultation. Basel Committee on Banking Supervision. 2003.

19) ORX News [Електронний ресурс]. 2020. URI: https:managingrisktogether.orx.org/orx-news.

20) Aldasoro I. The drivers of cyber risk / I. Aldasoro, L. Gambacorta, P. Giudici. . BIS Working Papers Monetary and Economic Department. 2020. №865.

21) Romanosky S. Examining the costs and causes of cyber Incidents / Sasha Romanosky. Journal of Cybersecurity, 2016. с. 1–15.

22) Dingel J. How many jobs can be done at home? / J. Dingel, B. Neiman. Journal of Public Economics, 2020. №189.

23) Jacobs J. Analyzing ponemon cost of data breach / Jacobs. Data Driven Security. 2014. №11.

24) World Economic Forum (WEF), Understanding Systemic Cyber Risk, Global Agenda Council on Risk & Resilience, White Paper, October 2016.

25) Office of Financial Research (OFR), Cybersecurity and Financial Stability: Risks and Resilience, OFR Viewpoint 17-01, 2017.

26) Communiqué: G20 Finance Ministers and Central Bank Governors Meeting [Електронний ресурс] . G20 Information Centre. 2020. URI: http:.www.g20.utoronto.ca/2020/2020-g20-finance-1014.html.

27) Частотність пошукових запитів «operation risk» , «cyber risk» [Електронний ресурс] . Google Trends. 2021. URI: https:.trends.google.com/trends/explore?cat=7&date=2018-04-03%202021-04-04&q=operation%20risk,cyber%20risk.

28) McAfee. Net Losses: Estimating the Global Cost of Cybercrime [Електронний ресурс] / McAfee, Center for Strategic and International Studies. McAfee, 2018. URI: https:.csis-prod.s3.amazonaws.com/s3fs-public/legac

29) Juniper Research. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation / Juniper Research. 2015

30) Cimpanu C. RDP and VPN use skyrocketed since coronavirus onset [Електронний ресурс] / Catalin Cimpanu. ZDNet. 2020. URI: https:.www.zdnet.com/article/rdp-and-vpn-use-skyrocketed-since-coronavirus-onset/.

31) Butler M. Effective global regulation in capital markets / Butler.ICI Conference, London, 2017. №5.

32) Aldasoro I. Cyber risk in the financial sector [Електронний ресурс] / I. Aldasoro, J. Frost, L. Gambacorta. The European Money and Finance Forum, 2020. URI: https:www.suerf.org/policynotes/18421/cyber-risk-in-the-financial-sector.

33) Financial Stability Review. Monetary Authority of Singapore. 2019.

34) Eisenbach T. Cyber risk and the U.S. financial system: a pre-mortem analysis / T. Eisenbach, A. Kovner, M. Lee. Federal Reserve Bank of New York. 2019.

35) Haugh C. Study: How the ‘New Normal’ is Changing Cloud Usage and Strategy [Електронний ресурс] / Ciri Haugh. Snow, 2020. URI:

https:.www.snowsoftware.com/blog/how-new-normal-changing-cloud-usage-and-strategy.

36) Beyond Data Breaches: Global Interconnections of Cyber Risk.. Zurich Insurance Group, Risk Nexus, Atlantic Council. 2014.

37) Національний банк України. Опитування про системні ризики фінансового сектору [Електронний ресурс] / Національний банк України. Травень. 2020. URI: https:.bank.gov.ua/admin_uploads/article/Risk_Survey_2020-H1.pdf?v=4.

38) Національний банк України. Звіт про фінансову стабільність [Електронний ресурс] / Національний банк України, 4. 2017. URI: https:.bank.gov.ua/admin_uploads/article/FSR_2017-H2.pdf?v=4#page=54.

39) Мінекономіки: Інформаційні ресурси. Загальна характеристика таблиць "витрати-випуск" (міжгалузевого балансу) як економіко-математичної моделі економіки [Електронний ресурс] / Мінекономіки Інформаційні ресурси. 2006. URI: https:.www.me.gov.ua/Documents/Print?lang=uk-UA&id=b0e5c176-f2c4-4b47-9478-ad73f5d48915.

40) Mainar-Causapé A. J., Ferrari E., McDonald S. Social Accounting Matrices: basic aspects and main steps for estimation. Technical report by the Joint Research Centre (JRC), the European Commission’s science and knowledge service, 2018.

41) Dreyer P. Estimating the Global Cost of Cyber Risk. Methodology and Examples [Електронний ресурс] / P. Dreyer, T. Jones, K. Klima . RAND Corporation. 2020. – URI: Estimating the Global Cost of Cyber Risk: Methodology and Examples.

42) OECD. Input-Output Tables [Електронний ресурс] / OECD. 4, 2021. URI: https:.www.oecd.org/sti/ind/input-outputtables.htm.

43) Державна служба статистики України. Таблиця "витрати-випуск" [Електронний ресурс] / Державна служба статистики України. Статистичний збірник «Таблиця "витрати–випуск" України у цінах споживачів». 2019. URI: http:.ukrstat.gov.ua/druk/publicat/kat_u/publ3_u.htm.

44) Lockheed Martin. the Cyber Kill Chain [Електронний ресурс] / Lockheed Martin. URI: https:.www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

45) Deloitte. Cyber Value at Risk in the Netherlands [Електронний ресурс] / Deloitte, 2016. URI: https:.www.thehaguesecuritydelta.com/images/deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf

46) Національний банк України. Дані наглядової статистики [Електронний ресурс] / Національний банк України. URI: https:.bank.gov.ua/ua/statistic/supervision-statist/data-supervision#4.

47) Правління Національного банку України. П о с т а н о в а № 4 Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кібер-захисту та електронних довірчих послуг [Електронний ресурс] / Правління Національного банку України. 16. URI: https:.bank.gov.ua/admin_uploads/law/16012021_4.pdf.

48) U.S. Department Of The Treasury. G7 Fundamental Elements Of Cybersecurity For The Financial Sector [Електронний ресурс] / U.S. Department Of The Treasury. URI: https:.www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf.

49) World economic forum. White Paper: Global Agenda Council on Cybersecurity [Електронний ресурс] / World economic forum. URI: http:.www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

50) The Basel Committee on Banking Supervision (BCBS). Core principles for effective banking supervision [Електронний ресурс] / The Basel Committee on Banking Supervision (BCBS). 2012. URI: https:.www.bis.org/publ/bcbs230.pdf

51) The Basel Committee on Banking Supervision (BCBS). Principles for the Sound Management of Operational Risk [Електронний ресурс] / The Basel Committee on Banking Supervision (BCBS). 2011. URI: https:.www.bis.org/publ/bcbs195.pdf

52) The Basel Committee on Banking Supervision (BCBS). Basel Committee on Banking Supervision, International Convergence of capital Measurement and Capital

Standards [Електронний ресурс] / The Basel Committee on Banking Supervision (BCBS). 2006. URI: https:.www.bis.org/publ/bcbs118.pdf

53) Committee on Payments and Market Infrastructures. Guidance on cyber resilience for financial market infrastructures [Електронний ресурс] / Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions. 2016. URI: https:.www.bis.org/cpmi/publ/d146.pdf.

54) Камінській А.Б., Кияк А.Т. Ідентифікація, аналіз та управління операційними ризиками в українських банках// Вісник Національного банку України. – 2005.–№ 10.–С. 7-11.

55) Джалладова І. А. Політика інформаційної безпеки: науково-прикладні аспекти і проблеми підготовки фахівців / І. А. Джалладова // Моделювання та інформаційні системи в економіці : зб. наук. пр. /КНЕУ. – Київ : КНЕУ, 2015. – Вип. 91. – С. 57–75.

ДОДАТКИ

Додаток А Витрати за секторами

Таблиця А.1 Future Direct EV + Systemic EV Costs + GDP (by Sector) (початок)

	Direct Output Costs ($M)	Direct GDP Costs ($M)	Direct GDP Costs (% of Sector GDP)	Systemic Output Costs ($M)	Systemic GDP Costs ($M)	Systemic GDP Costs (% of Sector GDP)
Banking	55.06	27.63	0.27%	149.08	74.81	0.73%
Business and Professional Ser	21.22	8.94	0.53%	34.89	14.70	0.88%
Consumer Goods	406.21	108.42	0.26%	849.90	226.85	0.55%
Defense and Aerospace	1 857.31	845.55	3.79%	1 878.00	854.97	3.83%
Healthcare and Insurance	13.94	5.77	0.07%	18.56	7.68	0.09%
Oil, Gas, and Chemicals	18.39	2.68	0.09%	259.97	37.93	1.22%
Public	23.61	11.07	0.06%	132.92	62.33	0.34%
Technology and Electronics	194.25	68.52	0.40%	448.86	158.34	0.93%
Telecom	14.37	6.64	1.52%	16.06	7.42	1.70%
Transportation	57.44	23.48	0.09%	321.03	131.25	0.48%
Utilities	18.84	6.31	0.05%	218.48	73.20	0.62%
Wholesale and Retail	56.21	24.21	0.05%	614.33	264.55	0.59%
Other	0.00	0.00	0.00%	2 348.98	822.82	1.07%
Total	2 736.86	1 139.24		7 291.05	2 736.86	

Додаток А Витрати за секторами

Таблиця А.2 Future Direct EV + Systemic EV Costs + GDP (by Sector) (кінець**)**

	Total Output Costs ($M)	Total GDP Costs ($M)	Total GDP Costs (% of Sector GDP)	Sector GDP ($M)	Sector GDP (% of Total GDP)
Banking	204.14	102.44	1.00%	10 289.85	1.84%
Business and Professional Services	56.10	23.64	1.41%	1 674.77	0.30%
Consumer Goods	1 256.11	335.27	0.81%	41 452.97	7.42%
Defense and Aerospace	3 735.31	1 700.52	7.63%	22 299.89	3.99%
Healthcare and Insurance	32.51	13.45	0.16%	8 164.60	1.46%
Oil, Gas, and Chemicals	278.37	40.61	1.30%	3 113.78	0.56%
Public	156.52	73.39	0.40%	18 224.04	3.26%
Technology and Electronics	643.11	226.87	1.34%	16 981.87	3.04%
Telecom	30.43	14.07	3.22%	436.82	0.08%
Transportation	378.47	154.74	0.56%	27 521.46	4.92%
Utilities	237.31	79.51	0.68%	11 760.92	2.10%
Wholesale and Retail	670.55	288.76	0.64%	45 109.60	8.07%
Other	2 348.98	822.82	1.07%	77 081.01	13.79%
Total	10 027.91	3 876.10	20.22%	284 111.58	100.00%

Додаток Б Сектори економіки в моделі

Таблиця Б.1 Перетворення груп ВВП у сектори (початок)

Sector-Category (Enter X to map a GDP Category to an Industry Sector)	Agriculture, hunting, forestry and fishing	Mining and quarrying	Food products, beverages and tobacco	Textiles, textile products, leather and footwear	Wood and products of wood and cork	Pulp, paper, paper products, printing	Coke, refined petroleum products and nuclear fuel	Chemicals and chemical products	Rubber and plastics products	Other non-metallic mineral products	Basic metals	Fabricated metal products
Asset Management and Pensions												
Banking												
Business and PServices												
Consumer Goods			X	X	X				X	X		X
Defense and Aerospace												
Healthcare and Insurance												
Media												
Oil, Gas, and Chemicals							X	X				
Public												
Technology and Electronics												
Telecom												
Transportation												
Utilities												
Wholesale and Retail												
Other	X	X				X					X	

Додаток Б Сектори економіки в моделі

Таблиця Б.2 Перетворення груп ВВП у сектори (продовження)

Sector-Category	Machinery and equipment, nec	Computer, Electronic equipment	Electrical machinery and apparatus, nec	Motor vehicles, trailers and	Other transport equipment	Manufacturing nec; recycling	Electricity, gas and water supply	Construction	Wholesale and retail trade; repairs	Hotels and restaurants	Transport and storage	Post and telecommunications
Asset Management												
Banking												
Business Professio Services												
Consumer Goods						X						
Defense Aerospace												
Healthcare and Insurance												
Media												
Oil, Gas, and Chemicals												
Public												
TechnologyElectronics	X	X	X									
Telecom												X
Transport				X	X						X	
Utilities							X					
Wholesale									X			
Other								X		X		

Додаток Б Сектори економіки в моделі

Таблиця Б.3 Перетворення груп ВВП у сектори (кінець)

Sector-Category	C65T67: Financial intermediation	C70: Real estate activities	C71: Renting of machinery and equipment	C72: Computer and related activities	C73T74: R&D and other business activities	C75: Public administration and defence; compulsory social security	C80: Education	C85: Health and social work	C90T93: Other community, social and personal services	C95: Private households with employed persons
Asset Management										
Banking	X									
Business Professio Services					X					
Consumer Goods										
Defense Aerospace						X				
Healthcare and Insurance								X		
Media										
Oil, Gas, and Chemicals										
Public							X		X	
TechnologyElectronics				X						
Telecom										
Transport										
Utilities										
Wholesale										
Other		X	X							X