МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені ВАДИМА ГЕТЬМАНА

ТРАНСФОРМАЦІЯ МЕНЕДЖМЕНТУ БІЗНЕС-ОРГАНІЗАЦІЙ: СУЧАСНІ ТРЕНДИ ТА ВИКЛИКИ

МОНОГРАФІЯ

з нагоди 115-річчя
Київського національного економічного університету
імені Вадима Гетьмана

за загальною редакцією
М. П. Сагайдака, Т. О. Соболєвої

КНЕУ 115 РОКІВ КИЇВ 2021

УДК 005.7:334.7
Т65

Рекомендовано до друку Вченою радою
ДВНЗ «Київський національний економічний університет
імені Вадима Гетьмана»
Протокол № 5 від 23.12.2021 р.

Рецензенти

Галушка З. І., д-р екон. наук, проф.
(Чернівецький національний університет імені Юрія Федьковича)

Карий О. І., д-р екон. наук, проф.
(Національний університет «Львівська політехніка»)

Скопенко Н. С., д-р екон. наук, проф.
(Національний університет харчових технологій)

Трансформація менеджменту бізнес-організацій: сучасні
Т65 тренди та виклики [Електронний ресурс] : монографія / за заг. ред. Сагайдака М.П., Соболєвої Т.О. Київ: КНЕУ, 2021. 378 с.
ISBN 978–966–926–399–5

В монографії розглянуті сучасні тренди і виклики трансформації менеджменту бізнес-організацій. В колі уваги авторів — глобальні тренди в управлінні бізнес-організаціями, стратегічні трансформації системи управління бізнес-організаціями, виклики інноваційного менеджменту та підприємництва, трансформація менеджменту на засадах сталого розвитку.

Для наукових та науково-педагогічних працівників, аспірантів, студентів економічних спеціальностей, керівників бізнес-організацій, підприємців, представників громадських організацій, усіх, хто цікавиться проблемами розвитку наукової думки та практики в сфері менеджменту.

УДК 005.7:334.7

ISBN 978–966–926–399–5

ЗМІСТ

КІБЕРБЕЗПЕКА В СИСТЕМІ ТРАНСФОРМАЦІЇ УПРАВЛІННЯ БІЗНЕС-ОРГАНІЗАЦІЄЮ

Полторак А.С., Сухорукова А.Л., Бурковська А.І.

Питання оцінювання кіберризику як ключової загрози фінансовій стабільності досліджувалося у працях А. Буверета[117], С. Байнерба, М. Елінга, Дж. Вирса[118], С. Толюпи, Є. Толюпи, Є. Агапової[119], О. Ясенко[120], В.Л. Бурячка[121], однак необхідно зазначити, що повні дані щодо кібератак у світі є дефіцитними, що суттєво ускладнює механізм оцінки та аналізу стану кібербезпеки, крім того, у будь-які офіційні дані включаються лише прямі збитки від кібератаки, тоді як непрямі витрати, у т. ч. на відновлення бізнесу та репутації, можуть становити понад 90 % від їх загального обсягу[122].

Ю. Безсусідня зазначає, що одним із посягань на інформаційну безпеку держави є здійснення «кібернетичних атак» та пропонує певні зміни до кримінального законодавства України[123].

Погоджуємось із думкою В.П. Шеломенцева[124], який розглядає кібератаку як процес пошуку та подальшого використання уразливості комп'ютерної системи з метою ефективної реалізації кібернетичної загрози, характер якої не встановлено.

---

[117] Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment; IMF Working Papers. 2018. URL: https://clck.ru/F2gS8 (Accessed 01 October 2021).

[118] Biener C., Eling M., Wirfs J. Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance: Issues and Practice.* 2015. Vol. 40. No. 1. pp. 131-158. DOI: 10.1057/gpp.2014.19.

[119]Толюпа С., Агапова Є. Вплив кібернетичних атак на інформаційну систему. *Педагогічні інновації: ідеї, реалії, перспективи.* 2017. Вип. 2. С. 83-87.

[120] Ясенко О. Бази даних як об'єкт кібертерористичних атак. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 95(2). С. 170-172.

[121] Бурячок В. Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу. *Інформаційна безпека.* 2013. № 1. С. 33-40.

[122] Mossburg E., Gelinne J., Calzada H. Beneath the Surface of a Cyberattack. Deloitte Development LLC, U.S.A. URL: https://clck.ru/F2gWs (Accessed 01 October 2021).

[123] Безсусідня Ю. Соціальна зумовленість криміналізації кібернетичних атак як суспільно небезпечного діяння проти національної безпеки України. *Підприємництво, господарство і право.* 2017. № 8. С. 149-153.

[124] Шеломенцев В. П. Поняття та сутність кібернетичної атаки. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2011. Вип. 25-26. С. 337-344.

Т. Гайдош[125] зазначає, що кіберзагрози глобальній фінансовій стабільності збільшуються навіть в умовах того, що пропозиція спеціалістів високого рівня у кіберпросторі не встигає за зростанням складності технологій, необхідних для здійснення ефективних кібератак на фінансовий сектор. Цей розрив заповнюється автоматизацією та сучасною інструментальною підтримкою, так, останні два десятиліття характеризуються стрімкими темпами розвитку інструментів, які використовуються для кібератак.

Відповідно до результатів опитування, опублікованих DTCC[126], серед головних ризиків глобальній фінансовій системі головними є: кіберризик, вплив нових вимог, геополітичні ризики. Крім того, у звіті наголошується на тому, що сектор фінансів, страхування та реальної економіки є більш вразливими до кібератак у порівнянні з іншими.

Проаналізуємо стан та тенденції кіберінцидентів, що мали місце у фінансових установах різних країн. Зазначимо, що дані щодо кіберінцидентів є дефіцитними, відповідно, кількісного оцінювання кіберризику здійснено недостатньо, враховуючи відсутність єдиного стандарту обліку, стимулів для звітування, а також певних обмежень для міжнародного обміну даними щодо кібератак. У США ще у 2011 р. випущені інструкції щодо методики розкриття кіберризиків для підприємницького сектору, які у 2018 році були доповнені відомостями про алгоритм розкриття інформації про кібератаки та кіберінциденти інвесторам, тоді як в Україні аналогічних документів, які б сприяли розв'язанні наявних прогалин у сфері кібербезпеки, взагалі немає.

У Європейському Союзі положення про захист даних (*GDPR*), яке набрало чинності у 2018 р., засвідчує обов'язок підприємницьких структур повідомляти про порушення протягом 72 годин в компетентний наглядовий орган. Невиконання цього обов'язку може призвести до суттєвих штрафних санкцій для компаній (4 % of global annual turnover or EUR 20 Mn).

[125] Гайдош Т. Киберпреступность приобретает индустриальный характер. *Финансы и развитие.* 2018. С. 22-25.
[126] DTCC Systemic Risk Barometer : results overview. 2017. URL: https://clck.ru/F2gbJ (Accessed 01 October 2021).

Дж. Себула та Л. Янг[127] визначають кіберризик як операційний ризик активам, що мають наслідки доступності, конфіденційності та цілісності інформаційних систем. М. Елінг та Дж. Вифс[128] звертають увагу на те, що кіберризик у порівнянні з іншими видами ризиків пов'язаний і з відповідальністю, і з власністю.

Відповідно до даних ORX про кіберподії протягом 2009-2017 рр. офіційно зафіксовано 341 подію, пов'язану з кібератаками на фінансові установи, близько 1/3 з яких висвітлило дані про збитки. Спираючись на ці дані, з'ясовано, що 39 % успішних кібератак зафіксовано у США, 7 % – у Великобританії, 17 % – країнах BRICS (6 % – в Росії; 4 % – в Китаї; 3 % – в Індії)[129]. Так, протягом останніх кількох років згідно з повідомленнями в ЗМІ (англійською мовою) у понад 50 країн світу відбулись кібератаки на фінансові установи.

За наявними даними ORX, серед сукупності кібератак порушення даних (пов'язане з крадіжками інформації про банківські картки) та шахрайство (пов'язане з конкретними сумами збитків внаслідок незаконних грошових переказів) є найбільш розповсюдженими у порівнянні з іншими типами кіберінцидентів.

Е. Копп, Л. Каффенбергер, К. Вілсон[130] зазначають, що фінансові установи є вразливими до кібератак через те, що вони суттєво залежать від критичних інфраструктур, які містять торгові майданчики, системи оплати та розрахунків, та високо взаємопов'язаних мереж, крім того, у деяких фінансових установах використовуються застарілі нестійкі до кібератак системи.

Систематизуємо дані останніх років щодо кібератак на центральні банки країн світу в табл. 1.

[127] Cebula J. J., Young L. R. A taxonomy of Operational Cyber Security Risks. Software Engineering Institute, Carnegie Mellon University. 2010. URL: https://clck.ru/F2gRC (Accessed 01 October 2021).
[128] Eling M., Wirfs J. H. Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class. Institute of Insurance Economics, University of St. Gallen. 2016. URL: https://clck.ru/F2gdj (Accessed 01 October 2021).
[129] IMF cyber risk paper uses ORX News data. URL: https://managingrisktogether.orx.org/news-and-blogs/imf-cyber-risk-paper-uses-orx-news-data (Accessed 01 October 2021).
[130] Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability. IMF Working Paper. 2017. No. 17/185. URL: https://clck.ru/F2ghM (Accessed 01 October 2021).

Таблиця 1 – Систематизація кібератак на фінансовий сектор (центральні банки)

Тип атаки	Фінансова установа	Характеристика атаки
Порушення даних	Банк Італії	атака на поштові облікові записи двох колишніх керівників
	Банк Азербайджану	крадіжка інформації про тисячі банківських клієнтів
	Європейський Центральний банк	крадіжка інформації про 20 тисяч банківських клієнтів
	Федеральний резервний банк Сент-Луїса	анонімне оприлюднення інформації про 4 000 працівників банківських установ
	Федеральний резервний банк Нью-Йорка	крадіжка коду програмного забезпечення банку на загальну суму 9,5 млн.дол. США
	Федеральний резервний банк Клівленда	крадіжка інформації зі 122 тис. кредитних карток банківської установи
Шахрайство	Банк Бангладешу	повноваження центрального банку були використані для незаконного переказу 81 мільйонів доларів США
	Банк Росії	21 кібератаки призвели до втрати 22 мільйонів доларів США з кореспондентських банківських рахунків
	Центральний банк Свазіленду	крадіжка в розмірі 688 000 дол. США
	Центральний банк Еквадору	крадіжка в розмірі 13,3 млн. дол. США з банківського рахунку міста Ріобамба
Зрив бізнесу	Банк Норвегії	напад на сім великих фінансових установ призвів до проблем з обслуговуванням клієнтів

Джерело: Систематизовано авторами

Зауважимо, що кібератаки можуть бути використані з метою підриву довіри населення до фінансової установи, так, після розповсюдження інформації у червні 2014 р. стосовно наявних проблем з ліквідністю найбільшого банку Болгарії відтік депозитних вкладів склав близько 10 %.

Деякі кібератаки можуть бути засновані на системі обміну повідомленнями SWIFT, яка застосовується для здійснення фінансових операцій. Так, направлені хакерами шахрайські платіжні доручення до банківських рахунків, призвели до початкових збитків у 336 млн.дол. США. Кібератаки, що засновані на системі SWIFT, зафіксовано у банках Еквадору, Бангладешу, В'єтнаму, Туреччини, Тайваню, Непалу, Росії, Індії.

Необхідно зазначити, що нові технології особливо часто піддаються кібератакам, враховуючи те, що розширення меж застосовуваних технологій може призвести до збільшення діапазону входів у фінансову систему, на які націлюються дії кібератак[131]. Кібератаки на фінансові установи, які використовують нові технології Fintech, призвели з 2013 року принаймні до 1 450 млн. доларів США збитків від шахрайства.

Тісний взаємозв'язок між фірмами найчастіше призводить до швидких ефектів зараження. Так, атака на частину мережі може спричинити поширення на інші фірми. Модифікована кібератака вірусу «wannacry» (версія «cryptolocker»), що відбулась у червні 2017 р. в Україні, призвела до сумарних втрат у 1,3 млрд.дол. США (ця сукупна оцінка отримана за даними фінансових втрат, висвітлених у фінансових звітах компаній після атаки: Fedex TNT Express – 300 млн.доларів США; Saint Gobain – 350 млн.доларів США; Merck – 310 млн.дол. США; A.P. Møller-Mærsk – 200-300 млн.дол. США, Mondelez – 100 млн.дол. США).

Про цю атаку стало відомо від компанії ESET, що спеціалізується на розробці антивірусного програмного забезпечення[132], що на Україну припало більше ¾ систем, вражених вірусом Petya, від загальносвітової кількості (вірус загалом поширився майже в 100 країнах світу, у т. ч. в Англії, Росії, США, Індії, так, в цілому було інфіковано близько 75 тисяч комп'ютерів).

Гайдош Т.[133] звертає увагу на те, що сучасна кіберзлочинність – це фактично ціла індустрія, яка функціонує на принципах, які є дуже схожими з принципами законного бізнесу, який намагається отримати найвищий рівень прибутку. Так, ефективно знижувати рівень кіберзагроз як ключових загроз фінансовій безпеці держави означає систематично знищувати бізнес-модель, в якій в умовах невисокого ризику нескладні для застосування інструменти використовуються для отримання значних прибутків. Хакери кінця 1980-років, що здійснювали

[131] Полторак А.С., Баришевська І.В., Мельник О.І., Боднар О.А. Кібернетична безпека банківського сектора в системі фінансової безпеки держави. *Сучасні тенденції розвитку фінансово-кредитної системи: теорія та практика* : колективна монографія. Полтава : ПП «Астрая», 2019. С. 79-83.

[132] Безсусідня Ю. Соціальна зумовленість криміналізації кібернетичних атак як суспільно небезпечного діяння проти національної безпеки України. *Підприємництво, господарство і право.* 2017. № 8. С. 149-153.

[133] Гайдош Т. Киберпреступность приобретает индустриальный характер. *Финансы и развитие*. 2018. С. 22-25.

кібератаки лише для того, щоб продемонструвати рівень своєї майстерності, стали легендою. Починаючи з 1990-х років, кіберзлочинність має чітку направленість на отримання високих прибутків зі всіма атрибутами звичайного бізнесу, а саме: ринками, профільними операторами, біржами, інтегрованими ланцюжками постачань, постачальниками послуг на основі аутсорсингу та інше. Відповідно, окремі держави розробляють високоефективну зброю для фактично промислового шпіонажу, збирання даних розвідки та знищення інфраструктури кіберзлочинців, використовуючи аналогічні технології.

В оновленому законі України від 21.06.2018 р. № 2469-VIII «Про національну безпеку України» зазначено, що до системи загроз національній безпеці України включаються тенденції, явища і чинники, які реально чи потенційно ускладнюють або унеможливлюють збереження національних цінностей та реалізацію національних інтересів України.

На думку О.М. Підхомного[134], у процесі дослідження сутності та розроблення напрямів зміцнення фінансової безпеки держави важлива роль відводиться саме співвідношенню та розумінню змісту таких понять як «загроза», «виклик», «небезпека», «ризик». Зауважимо, що ці поняття дуже часто зустрічаються в дослідженнях проблем зміцнення фінансової безпеки та трактуються як синоніми. На нашу думку, ці поняття є близькими за змістом, однак, у різних ситуативних контекстах вони мають розумітися по-різному.

Загрози безпековим умовам розглядають як певні чинники або фактори, які формують небезпеку, а саме наявну та об'єктивну ймовірність негативного впливу на складну систему.

Найчастіше ризик розуміється як випадкова можливість отримати інший, у порівнянні з очікуваним, результат, тобто теоретично можна розглядати можливість як, наприклад, ризику збитків, так і ризику надприбутків, тоді як «загроза» – це чітко виражена ймовірність настання лише несприятливих наслідків для досліджуваної системи.

[134] Підхомний О.М. Фінансова безпека України: методологія аналізу та стратегічні орієнтири: дис. … д-ра екон. наук: 08.00.08 / Львівський національний університет імені Івана Франка. Львів, 2015. 455 с.

Погоджуємось із висновками О.І. Барановського[135], що загрози відрізняються від викликів певними унікальними характеристиками. Так, стосовно загроз не вжито своєчасних заходів впливу, відповідно, суперечності сторін у них значно сильніше загострені.

Трактування понять «виклик» та «загроза» систематизовано у табл. 2.

У Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» сформульовано визначення: «ризики – небезпека (загроза, уразливі місця) для суб'єктів первинного фінансового моніторингу бути використаними з метою легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму або фінансування розповсюдження зброї масового знищення під час надання ними послуг відповідно до характеру їх діяльності»[136], що підтверджує думку про те, що дуже часто поняття «загроза», «небезпека», «ризик» не розрізняють. На думку А.С. Марини[137], загрози фінансовій безпеці – це чинники і явища (потенційні або реальні) об'єктивного або суб'єктивного характеру, які формують умови для небезпеки розвитку та стабільності фінансової системи держави. О.М. Підхомний звертає увагу на те, що стратегічні інформаційні повідомлення, які на практиці можуть поширюватись формальними й неформальними способами, можуть виявлятись загрозою фінансовій безпеці, особливо це стосується негативного впливу деструктивних ідей, що поширюються в офіційному інформаційному просторі (реклама фінансових пірамід, популяризація боргової залежності, оприлюднення способів та варіантів ухилення від оподаткування, масове закликання до застосування криптовалют, розповсюдження інших теорій швидкого збагачення, псевдонаукові вчення, такі як фінансова нумерологія чи фінансова астрологія).

[135] Барановський О.І. Загрози фінансовій безпеці фондового ринку. *Фінанси України.* 2016. № 3. С. 15-33.
[136] Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: закон України від 14.10.2014 р. № 1702-VII / Верховна рада України. 2014. URL: http://zakon.rada.gov.ua/laws/card/1702-18 (дата звернення: 01.10.2021).
[137] Марина А.С. Фінансова безпека країни в умовах фінансової інтеграції: концептуальні положення. *Вісник Одеського національного університету. Економіка.* 2013. Т. 18, Вип. 2(1). С. 22-25.

Таблиця 2 – Трактування понять «виклик» та «загроза»

Виклики	Загрози
Вимога, спонукання до будь-яких дій, відносин; заклик до змагання, участі в будь-чому; категорична, різка пропозиція вступити в боротьбу, поєдинок[138]	Соціальне, природне чи техногенне явище з прогнозованими, але не контрольованими небажаними подіями, що можуть статись у певний момент часу в межах даної території, спричинити смерть людей або завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків, погіршити стан довкілля[139]
Проблема, котра з певних причин і в конкретний час набула сильного звучання та загострено сприймається політичною елітою, й має, на її погляд, важливе, пріоритетне значення[140]	Зовнішні і внутрішні потенційно можливі чи реальні події, процеси, обставини або дії осіб, навмисні чи ненавмисні, які призводять до втрати власного капіталу підприємства або виникнення умов його банкрутства[141]
Зачатковий ступінь формування загрози[142]	Явище, чинник (сукупність чинників), що здатні реально створити умови чи стати причиною повної або часткової неможливості реалізації інтересів
Сукупність обставин не обов'язково загрозливого характеру, але, безумовно, таких, що вимагають реагування на них[143]	Одна з форм небезпеки[144]
Протидія здійсненню захисту, перешкода на шляху до безпечного розвитку[145]	Потенційно можливе заподіяння шкоди суб'єкту господарювання з боку окремих чинників, зумовлених характером економічної діяльності й оточенням[146]
	Найвищий ступінь імовірності перетворення небезпеки з можливості на дійсність, висловлений намір певних суб'єктів завдати шкоди іншим, демонстрація готовності вдатися до насилля для заподіяння шкоди[19]

Джерело: Систематизовано авторами

[138] Великий тлумачний словник сучасної української мови / уклад. і гол. ред. В. Т. Бусел. К. ; Ірпінь : ВТФ «Перун», 2005. 1728 с.

[139] Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи ; Ін-т проблем нац. безпеки. Київ, 2004. 472 с.

[140] Бодрук О.С. Структура воєнної безпеки: національний та міжнародний аспекти : монографія; Рада нац. безпеки і оборони України, Нац. ін-т проблем міжнар. безпеки. К., 2001. 300 с.

[141] Кириченко О. А., Кім Ю. Г. Методологічні основи економічної безпеки суб'єктів господарювання в трансформаційній економіці. *Актуальні проблеми економіки.* 2008. № 12. С. 53-65.

[142] Брега А. В. Риск в системе категорий, характеризующих антитезу национальной безопасности. Национальная безопасность: научное и государственное управленческое содержание : материалы Всерос. науч. конф., 4 дек. 2009 г., Москва. М. : Науч. эксперт, 2010. С. 737-753.

[143] Сергунин А. А. Международная безопасность: новые подходы и концепты. *Политические исследования.* 2005. № 6. С. 126-138.

[144] Єрмошенко М. М., Горячева К. С., Ашуєв А. М. Економічні та організаційні засади забезпечення фінансової безпеки підприємства : препринт наук. доп.; Нац. акад. упр. ; за наук. ред. М. М. Єрмошенка. Київ, 2005. 80 с.

[145] Різник Н. С. Теоретичні засади формування системи діагностики економічної безпеки банку. *Вісник Харківського національного технічного університету сільського господарства. Серія : економічні науки.* 2007. Вип. 66. С.118-123.

[146] Орлов П. І., Духов В. Є. Основи економічної безпеки фірми. Харків : Прометей-Прес, 2004. 284 с.

Зауважимо, що у сфері кібербезпеки фінансового сектору проблемами пострадянських країн є: недостатня кількість галузевих центрів кібербезпеки; недостатній рівень стандартизації для суб'єктів господарювання; міжвідомча взаємодія; механізми стимулювання галузі. Показники NCSI розроблялися з урахуванням кіберзагроз (рис. 1).

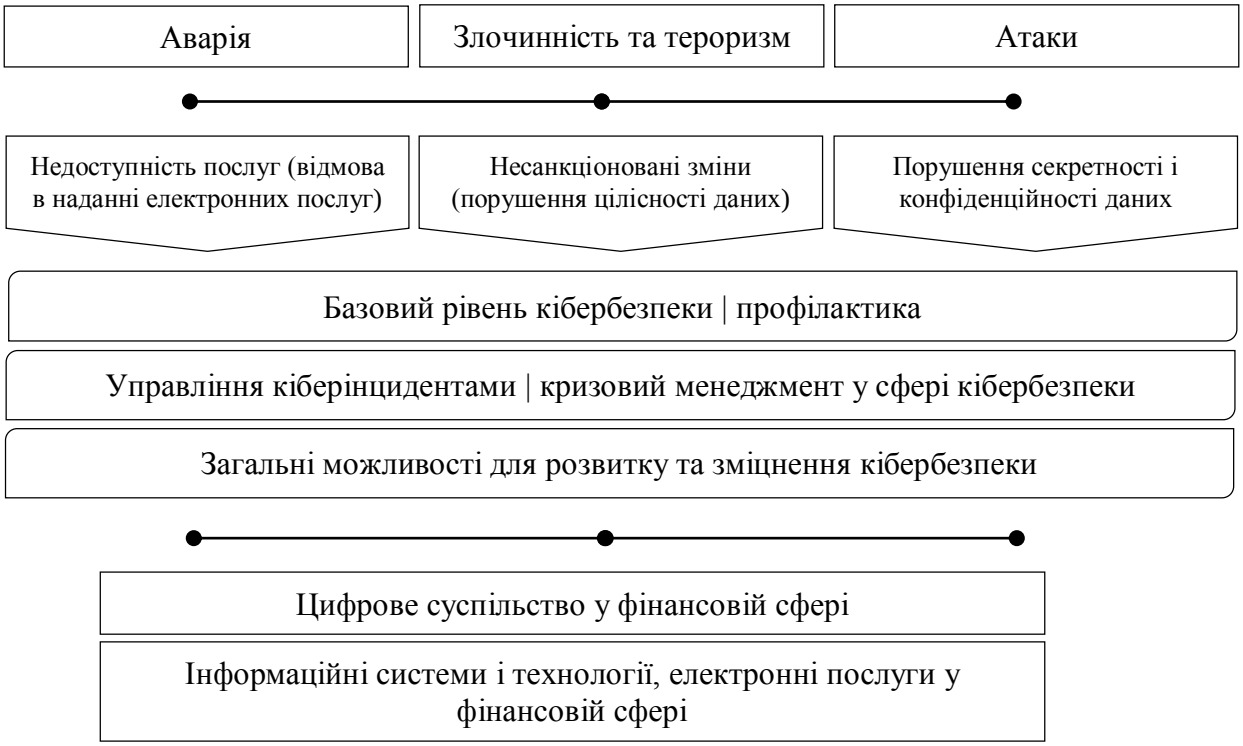

Рисунок 1. Основні кіберзагрози фінансовій безпеці держави та необхідні можливості для управління ними

Джерело: адаптовано авторами до специфіки дослідження на основі[147]

Система фінансової безпеки держави в умовах глобалізації не може характеризуватися оптимальним рівнем без необхідного рівня кібербезпеки фінансового сектору, так, на нашу думку, саме кібернетичну безпеку фінансового сектору необхідно розглядати та аналізувати як важливу підсистему фінансової безпеки держави.

Кібернетичний ризик має найвищі кількісні показники й показники зростання у динаміці в системі ризиків глобальній фінансовій системі, що

[147] e-Governance Academy Foundation. National Cyber Security Index, URL: https://ncsi.ega.ee/.

підтверджується результатами міжнародних опитувань, численними дослідженнями міжнародних фахівців, в т. ч. представниками поважних фінансових установ, показниками глобального індексу кібербезпеки для країн світу (Україна з показником 0,501 посідає 59 місце серед досліджуваних країн світу) та національного індексу кібербезпеки (National Cyber Security Index).

В останні роки активно розвивається законодавчо-нормативна база країн у сфері протидії кіберзлочинності, розкриття інформації про кібератаки, захисту даних (в т. ч. *GDPR*, яке набрало чинності у 2018 р. у Європейському Союзі). Протягом 2017 р. за даними НБУ банки України зафіксували 77,6 тисячі випадків шахрайства із банківськими картками (для порівняння у 2016 р. – 95 тис.). Сума збитків досягає 163,7 млн.гривень.

Річні втрати фінансових організацій від кібернетичних атак відповідно до розрахунків, проведених спеціалістами МВФ, можуть становити в середньому декілька сот мільярдів доларів[148]. Кібернетичні атаки останніх років підтверджують, що ця загроза є реальною для фінансового сектору. Так, серед останніх випадків кібератак на фінансові організації: крадіжка 500 млн доларів на біржі криптовалюти Coinchec; злом системи *Equifax*, який призвів до порушення конфіденційності 143 млн. користувачів у сфері кредитної інформації; крадіжка з банку Бангладешу 81 млн.дол. США.

Особливо небезпечно те, що зломи систем окремих фінансових організацій можуть спричинити негативні ефекти доміно для інших компаній (як фінансової, так і нефінансової сфери), створюючи системний ризик. Крім того, у багатьох випадках інформація про успішні кібератаки розкривається лише через місяці, або навіть роки після інциденту з побоювань шкоди для репутації, відповідно, як зазначає Т. Гайдош[149], кількісно оцінити кіберризик дуже важко.

Наявні дані щодо збитків, отриманих внаслідок кібератак на фінансовий сектор, є неповними та ненадійними через те, що стимули повного висвітлення

[148] Лагард К. Оценка кибер-риска для финансового сектора / Кристин Лагард ; IMFBlog. 2018. URL: https://goo.gl/1zGYrB (дата звернення: 21.06.2018).
[149] Гайдош Т. Киберпреступность приобретает индустриальный характер. *Финансы и развитие.* 2018. С. 22-25.

інформації про успішні кібератаки, особливо за умови відсутності страхування від кіберризиків, відсутні. Крім того, характер кіберзагроз швидко змінюється, що призводить до зниження важливості даних щодо минулих кіберінцидентів для можливого прогнозування майбутніх загроз фінансовому сектору. Моделювання на основі сценаріїв, у процесі якого визначаються втрати для економіки конкретних країн, пов'язані з конкретним кіберінцидентом, надає оцінку в десятки або навіть сотні млрд доларів. Так, фірма Lloyd's оцінює у 53 млрд.доларів збитки від відключення на 2,5-3 дні хмарного сервісу у країнах з розвиненою економікою. Моделювання, виконане спеціалістами МВФ, свідчить, що у базовому сценарії середні сукупні річні збитки, пов'язані з кіберінцидентами, складають 97 млрд.доларів, у найгіршому – 250 млрд.доларів.

Враховуючи вищевикладене, вважаємо необхідним розглядати кібернетичну безпеку як важливу складову фінансової та, відповідно, національної безпеки держави.

Погоджуємось із думкою Т. Гайдоша, що кіберзлочинність спричиняє виникнення системного ризику, який по-різному відбивається на різних сферах економіки, однак, є найвищим у фінансовому секторі. Намагаючись дестабілізувати фінансову сферу, кіберзлочинці розглядають найбільш перспективні напрями. Інфраструктура фінансового ринку, враховуючи її важливу роль на світових фінансових ринках, є найбільш вразливою. Масштабні ефекти послідовної ланцюжкової реакції дефолтів внаслідок кібератак на фінансовий сектор можуть мати системні наслідки саме через те, що фінансовий сектор залежить від невеликого набору технічних систем. Крадіжка конфіденційної інформації, дезорганізація клірингової, платіжної або розрахункової системи, враховуючи тісний взаємозв'язок суб'єктів фінансового сектору, очікувано призведуть до масштабних вторинних ефектів та, відповідно, стануть реальною загрозою для фінансової безпеки.

Ефективний розвиток інструментів, які використовуються у процесі кібератак, особливо співвідношення ризику та потенційної винагороди, є

аргументом та фактично поясненням різкого розвитку кіберзлочинності у фінансовому секторі, її трансформацію в цілу індустрію.

У ситуації, якщо кібератака буде успішно проведена у напрямі інфраструктури фінансового ринку, або, наприклад, спричинить неможливість ефективно збирати податки, результатом можуть стати суттєві потрясіння з системними фінансовими наслідками, що потенційно є небезпекою для держави та її населення. У цій потенційній ситуації сукупний ризик для економіки може суттєво перевищувати загальну суму ризиків для окремих осіб, враховуючи національний характер структур реагування, глобальний характер мереж та платформ інформаційних технологій, неефективність міжнародного співробітництва.

В.М. Панченко[150] трактує поняття «кібернетична безпека» як безпеку об'єктів, які безпосередньо пов'язані із комп'ютерними технологіями, що забезпечують зв'язок між комунікаторами, комп'ютерами, смартфонами, тобто обчислювальними пристроями та звертає увагу на те, що кібербезпека є складовою інформаційної безпеки, яка, у свою чергу, є ширшим поняттям. В.М. Фурашев[151] обґрунтовує, що кібербезпека – стан спроможності держави, суспільства і людини запобігання та уникнення спрямованого, несвідомого, негативного впливу інформації, однак, детальний аналіз, проведений автором, дозволив зробити висновок, що порівняння понять «інформаційна безпека» та «кібернетична безпека» показує їх тотожність через те, що кіберпростір – це складова інформаційного простору, відповідно, вони мають єдині об'єкт, суб'єкти, процеси та спрямованість.

У 2017 р. незаконні дії з платіжними картками в Україні становили 0,0077 % від сукупного обсягу операцій з платіжними картками на загальну суму 163,7 млн.грн., для порівняння у 2016 році – 0,011%. Так, за даними НБУ на 1 млн.грн. видаткових операцій з платіжними картками припадає 77 грн.

[150] Панченко В. М. Співвідношення понять: інформаційна та кібернетична безпека. *Інформаційна безпека людини, суспільства, держави.* 2013. № 2. С. 20-23.
[151] Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162-169.

незаконних операцій (у 2016 р. – 110 грн.). У середньому близько 2 100 грн. припадає на одну незаконну операцію 2017 року. Зазначимо, що у 2017 р. 38 банків повідомили про шахрайські дії. Серед останніх тенденцій у сфері кібербезпеки є збільшення кількості незаконних операцій, які здійснюються через Інтернет (у 2017 р. – 84,1 млн.грн.), що пояснюється фахівцями Нацбанку тим, що шахраї змінюють фокус уваги з технологічних методів на методи соціальної інженерії, відповідно, усім учасникам платіжного ринку у першу чергу необхідно підвищувати свою фінансову грамотність. Найчастіше шахрайські випадки відбуваються у великих містах України та найбільших областях.

На думку В. Ліпкана та І. Діордіци[152], кібербезпека – це певний стан захищеності в кібернетичному просторі інтересів громадянина, суспільства та держави, в якому можливе безперешкодне збирання, створення, одержання, використання, зберігання, поширення, а також захист та охорона інформації.

Відповідно до закону України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України»[153] кібербезпека – це «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі», а індикатори кіберзагроз – це показники, які використовуються для виявлення та реагування на них.

Зазначимо, що міжнародне співробітництво у сфері кібербезпеки суттєво відстає від системного глобального характеру цієї загрози. Найкращим напрямом боротьби з кіберзлочинністю є атака на її бізнес-модель, особливістю якої є специфічне співвідношення рівня ризику та потенційного прибутку, винагороди, що пов’язано з неефективністю судового переслідування. Так,

[152] Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. № 5. С. 174-180.
[153] Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. 2017. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 23.07.2019).

необхідно суттєво збільшити ризик у сфері кіберзлочинів, що можливо лише в умовах тісного міжнародного співробітництва.

Регулюючі органи фінансового сектору мають ефективніше встановлювати вимоги, забезпечені правовою санкцією, розробляти стандарти оцінки, цільові орієнтири, підтримувати обмін інформацією між регулюючими органами та фінансовими компаніями. Органи банківського регулювання мають систематично проводити перевірку інформаційних технологій, у процесі якої у стрес-тестах, плануванні врегулювання та нагляді за стійкістю та надійністю, шляхом імітаційного моделювання кібератаки має оцінюватись стійкість до атаки та спроможність протистояти кіберінцидентам. Сучасні тенденції кіберпростору вимагають від фінансового сектору збільшення інвестицій у забезпечення кібербезпеки, забезпечення її рівня шляхом управління ризиками, перенесення ризиків завдяки страхуванню від кіберризику.

Наявна ситуація у сфері кібербезпеки фінансового сектору України залишається децентралізованою та різнорідною. Ризики усуваються та розглядаються як часткові поодинокі проблеми, відсутні системні механізми співробітництва регулюючих органів фінансового сектору. Для ефективного забезпечення підвищеної стійкості фінансового сектору до кіберризику необхідні дієві превентивні міри на рівні регулювання, технологій в різних галузях, затвердження та виконання мінімальних стандартів кібербезпеки, забезпечених правовою санкцією регулюючих органів.

Також потрібні сучасні кадри для підвищення рівня інформованості стосовно кібербезпеки, що позитивно вплине на рівень захищеності від технічних недоліків базового рівня, помилок користувачів, які є джерелом переважної більшості кібератак. В умовах забезпечення кібербезпеки також важливим є те, наскільки оперативно система може повернутися до стійкого стану і звичайного режиму функціонування та ефективно відреагувати на кіберінциденти.

Отже, аналізуючи методичні засади систематизації фінансової безпеки держави, узагальнено ключові ознаки її оптимального стану, серед яких:

ефективність та стабільність фінансової системи; конкурентоспроможність та фінансова незалежність; захищеність інтересів у фінансовій сфері; достатність фінансових ресурсів; розвиток фінансової системи держави.

Виділено особливий структурний елемент категорії «фінансова безпека», визначений відповідно до об'єкта захисту, а саме фінансова безпека об'єднаного світового фінансового простору, яке розглядається автором як умови розвитку глобальної фінансової системи, за яких наслідки глобалізації не спричиняють негативних процесів в інтеграційному процесі та не обмежують можливості створення сприятливих фінансових умов щодо розвитку світового фінансового простору, сприяють ідентифікації, якісній оцінці та гарантуванню передумов до забезпечення фінансової безпеки держав світу.

Удосконалено теоретичний підхід до трактування категорії «податкова безпека держави», що, на відміну від загальновживаних, розглядається як умови функціонування податкової системи України, які надають змогу оптимально поєднати стабільність наповнення дохідної частини бюджету для повного і своєчасного задоволення потреб суспільства та стимулювання підприємницької активності в країні й інтереси платників податків, своєчасно виявляти та запобігати загрозам і ризикам у сфері оподаткування, а також характеризує здатність податкової системи України до збалансованого розвитку.

Проаналізовано динаміку значень глобального індексу кібербезпеки (global protection index), що розраховується за п'ятьма основними показниками: організаційний і технічний потенціали; законодавча база; кооперація; темпи нарощування потенціалу, та національного індексу кібербезпеки (National Cyber Security Index), який визначається з метою оцінки здатності країн управляти кіберінцидентами та запобігати кіберзагрозам. З'ясовано, що високий рівень індексів мають переважно розвинені держави, тоді як держави з низьким та середнім рівнем розвитку характеризуються нижчими значеннями індексів кібербезпеки. Доведено, що позитивна різниця між NCSI-індексом та індексом цифрового розвитку (DDL), що є узагальненим показником розвитку інформаційно-комунікаційних технологій та індексу мережевої готовності,

свідчить, що розвиток кібербезпеки окремих держав (Словаччина, Чехія, Польща, Угорщина, Україна) випереджає або відповідає її цифровому розвитку, тоді як від'ємний результат означає, що цифрове суспільство певних країн (Білорусь, Румунія, Болгарія, Молдова) є більш розвиненим у порівнянні з національною сферою кібербезпеки.

Зафіксовано активний розвиток законодавчо-нормативної бази країн у сфері протидії кіберзлочинності, розкриття інформації про кібератаки, захисту даних, що підтверджує особливу увагу фахівців до зростання загрози від кіберзлочинів для фінансового сектору. В окремих країнах світу випущені інструкції щодо методики та алгоритмів розкриття кіберризиків для підприємницького сектору й затверджено штрафні санкції за їх невиконання, тоді як в Україні аналогічних заходів, які сприяли б розв'язанню наявних прогалин у сфері кібербезпеки, і досі бракує. Зазначено, що міжнародне співробітництво у сфері кібернетичної безпеки суттєво відстає від системного глобального характеру цієї загрози.

З'ясовано, що у 2017 р. за даними НБУ банківські установи України зафіксували 77,6 тисячі випадків шахрайства із банківськими картками на загальну суму збитків у 163,7 млн.грн., крім того, 38 банків повідомили про шахрайські дії. Річні втрати фінансових організацій від кібернетичних атак відповідно до розрахунків спеціалістів МВФ можуть становити в середньому декілька сотень мільярдів доларів.

Враховуючи те, що кібератаки складають все більшу загрозу фінансовій безпеці України в умовах глобалізації, зміцнення кібернетичної безпеки фінансового сектору стає важливою проблемою сучасності. Технологія блокчейн може бути застосована для її успішного розв'язання та, відповідно, захисту інформації від кібератак. Кожен з користувачів має можливість додавати необхідну інформацію в блокчейн, захищений криптографією, та зобов'язаний перевіряти весь обсяг нової інформації на достовірність (*proof of work*) до моменту, коли вона буде додана в ланцюг. Відповідно, весь цей процес відбувається за допомогою трьох ключів (приватного, публічного, ключа одержувача), які дозволяють перевіряти інформацію кожному учаснику ланцюга.

Судова інформаційна служба в Нідерландах вже успішно використовує технологію *Guardtime KSI Blockchain* для ефективного забезпечення цілісності електронних послуг, забезпечення прозорості, можливості аудиту та забезпечення безпеки інформації, яка оброблюється в державних системах. Ще з 2012 р. Міністерство юстиції Естонії застосовує технологічні рішення блокчейн з метою ефективного моніторингу та забезпечення цілісності, так, сьогодні такі технологічні рішення впроваджено в багатьох електронних послугах: реєстр електронних ділових операцій; земельна книга; державна газета, що містить інформацію про прийняті закони й т. д.

У Великобританії впроваджено платформу персональних даних із застосуванням блокчейн для понад 30 млн. пацієнтів Національної Служби охорони здоров'я Великобританії (*NHS*), які мають доступ до смартфона. Платформа, яка запущена *Guardtime* та партнерами *Healthcare Gateway, Instant Access Medical*, дозволяє покращити дотримання правил приймання ліків користувачами. Потенційна економія від застосування цієї платформи складає близько 800 млн. фунтів стерлінгів у Великобританії, а також 290 млрд.доларів США у США.

У Китаї у 2019 р. розпочато застосування платформи *HSX Guardtime,* яка використовує технологію блокчейн, у великій приватній лікарні провінції Фуцзянь (*Putian Hospital Group*). Ця платформа очікувано підвищить рівень довіри, транспарентності та цілісності лікарняних інформаційних систем, дозволить прискорити доступ до лікування, співпрацювати з третіми сторонами, розширювати дослідження здоров'я населення, сприятиме доступу пацієнтів до певних додатків для більш ефективного управління своїм здоров'ям.

Також технологія блокчейн може застосовуватися у процесі запобігання атак на відмову в обслуговуванні (*distributed denial of service* (DDoS-атаки)), принцип роботи яких полягає в т. ч. у відправленні великої кількості запитів на сайт, внаслідок чого суттєво збільшується трафік, а сайт виходить з ладу. Теоретично, за оцінками експерта *Cisco* по інформаційній безпеці В. Ілібмана, на певний час з ладу може вийти будь-який сайт державної структури України.

Кожне відомство повинно мати комплексний захист, однак, багато державних структур не враховує поточні ризики.

Застосування блокчейн-технології може децентралізувати *DNS* (головний центр, в якому концентрується основний масив інформації), а інформацію розподілити серед вузлів мережі, що фактично захистить від хакерських атак систему. Це впровадження дозволить користувачам створювати доменні імена, однак, вносити зміни в домени зможуть виключно авторизовані користувачі. Враховуючи те, що дані теоретично будуть зберігатися на різних комп'ютерах, а у кожного з користувачів буде копія загального масиву інформації на блокчейн, система стає захищеною.

Окремі компанії вже успішно запроваджують блокчейн-технологію для запобігання *DDoS*-атак. *Blockstack* повністю децентралізує *DNS*, прибираючи треті сторони від управління серверами, базами даних і ID системами. Англійська компанія *MaidSafe* також намагається повністю децентралізувати мережу шляхом шифрування, фрагментації та розподілу між користувачами кожного файлу, розміщеного на сервері, у результаті чого тільки власник інформації має доступ до неї. Отже, запровадження шифрування та системи розподілу протоколів у мережі фактично може гарантувати захист інформації від зловмисників.

Отже, характер кіберзагроз швидко змінюється, що призводить до зниження важливості даних щодо минулих кіберінцидентів для можливого прогнозування майбутніх загроз фінансовому сектору. Особливо це стосується негативного впливу деструктивних ідей, що поширюються в офіційному інформаційному просторі (реклама фінансових пірамід, популяризація боргової залежності, оприлюднення способів та варіантів ухилення від оподаткування, масове закликання до застосування криптовалют, розповсюдження інших теорій швидкого збагачення, псевдонаукові вчення, такі як фінансова нумерологія чи фінансова астрологія).

Крім того, нами обґрунтовано доцільність розширення системи фінансової безпеки держави в умовах глобалізації особливою підсистемою – кібербезпека

фінансового сектору. Запропоновано трактування поняття «кібернетична безпека фінансового сектору», що, на відміну від наявних, розглядається як умови, в яких функціонує фінансова система держави, за яких дія внутрішніх та зовнішніх загроз у кібернетичному просторі не спричиняє негативних процесів у даній складній системі та не заважає створенню сприятливих фінансових умов для її сталого розвитку в умовах діджиталізації, безперешкодного формування, зберігання, використання, поширення та захисту інформації, що сприятиме удосконаленню науково обґрунтованої термінології та розвитку економічної науки.

На підставі експертних оцінок, запропоновано наступні індикатори стану кібернетичної безпеки України: питома вага незаконних дій з платіжними картками у сукупному обсязі операцій з платіжними картками; середня вартість 1 незаконної операції у кіберпросторі; кількість незаконних операцій, які здійснюються через Інтернет; міжнародний глобальний індекс кібербезпеки; питома вага витрат на забезпечення кібербезпеки у загальному обсязі витрат зведеного бюджету України; питома вага витрат на страхування кіберзагроз у загальному обсязі витрат на страхування.

Poltorak Anastasiia, DSc, Assosiate Professor, Head of Department of Management and Marketing, Mykolayiv National Agrarian University, Ukraine, https://orcid.org/0000-0002-9752-9431
Полторак Анастасія Сергіївна, доктор економічних наук, доцент, завідувач кафедри менеджменту та маркетингу Миколаївського національного аграрного університету, Україна, https://orcid.org/0000-0002-9752-9431

Sukhorukova Anna, Candidate of Sciences in Public Administration, Associate Professor of Management and Marketing, Mykolayiv National Agrarian University, Ukraine, https://orcid.org/0000-0002-6170-4955
Сухорукова Анна Леонідівна, кандидат наук з державного управління, доцент кафедри менеджменту та маркетингу Миколаївського національного аграрного університету, Україна, https://orcid.org/0000-0002-6170-4955

Burkovska Anna, Assistant at the Department of Management and Marketing, Mykolayiv National Agrarian University, Ukraine, https://orcid.org/0000-0003-0563-6967
Бурковська Анна Іванівна, асистент кафедри менеджменту та маркетингу Миколаївського національного аграрного університету, Україна, https://orcid.org/0000-0003-0563-6967