УДК 330.131.7:004.946.5

ВОЛОСОВИЧ Світлана,
д. е. н., професор, професор кафедри фінансів
Київського національного торговельно-економічного університету

КЛАПКІВ Любов,
к. е. н., старший викладач кафедри фінансів
Київського національного торговельно-економічного університету

ДЕТЕРМІНАНТИ ВИНИКНЕННЯ ТА РЕАЛІЗАЦІЇ КІБЕРРИЗИКІВ

Виокремлено причинно-наслідковий, секторальний та інструментальний підходи до визначення дефініції кіберризиків. Запропоновано розглядати кіберризики у широкому та вузькому розумінні. Систематизовано кримінальні та некримінальні джерела кіберризиків. Проаналізовано явища кібератака та кіберінцидент як основні інструменти реалізації кіберризику. Виявлено кіберзагрози для зовнішньої торгівлі. Досліджено основні кіберінциденти глобального масштабу.

Ключові слова: кіберризик, кібератака, кіберзагроза, кіберінцидент.

Волосович С., Клапкив Л. Детерминанты возникновения и реализации киберрисков. *Выделены причинно-следственный, секторный и инструментальный подходы к определению дефиниции киберрисков. Предложено рассматривать киберриски в широком и узком смысле. Систематизированы уголовные и некриминальные источника киберрисков. Проанализированы явления кибератака и киберинцидент как основные инструменты реализации киберриска. Исследованы основные киберинциденты глобального масштаба.*

Ключевые слова: кибериск, кибератака, киберугроза, киберинцидент.

Постановка проблеми. Протягом останніх десятиліть розвиток інтернету спричинив революцію у сфері зв'язку та комунікації, що стало суттєвим чинником світового економічного зростання. З одного боку, це дало можливість суб'єктам господарювання та населенню в усьому світі отримати вигоди від ефективності, швидкості та зручності цифрових операцій та обміну інформацією, а з іншого, обумовило зростання ймовірності для підприємств отримання фінансових збитків, витоку даних та погіршення репутації через кіберзлочинні дії конкурентів та хакерів.

Проблема кіберризиків на світовому рівні була офіційно названа однією з п'яти ключових загроз людству, починаючи з 2012 р. В опрацюваннях Світового економічного форуму того року кібератаки посіли четверте місце в рейтингу загроз. Через п'ять років у подібному

рапорті було відзначено нові типи кіберзагрози – крадіжка і шахрайство з даними [1, с. 4]. Активізація цих процесів обумовила актуальність цього дослідження.

Аналіз останніх досліджень і публікацій. В сучасній науковій літературі економічним аспектам кіберризиків і методам управління ними присвячено незначну кількість праць. Варто відзначити, що темпи досліджень цієї проблеми у розвинутих країнах значно випереджають вітчизняні напрацювання. Такий розрив, з одного боку, пояснюється рівнем розвитку фінансової системи та залежністю її від інформаційних технологій. А з іншого – питання кіберризику об'єднує дві різні сфери: фінансову та інформаційну, що вимагає інтердисциплінарного підходу до його вивчення.

Істотну роль у дослідженні сутності кіберризиків відіграють приватні інституції: консалтингові, страхові компанії та компанії з інформаційного та програмного забезпечення, зокрема *AON, PricewaterhauseCoopers, Deloitte, Ernstand Young, Society of Actuaries, International Association, Allianz, Geneva Association*. Із зростанням кіберризику та негативних фінансових наслідків його реалізації все більшу увагу цій загрозі приділяють державні та комерційні установи, зокрема Федеральне Бюро розслідувань США, Банк міжнародних розрахунків.

У різних джерелах кіберризики розглянуто в таких аспектах як:

- систематичні ризики в діяльності фінансових установ та фінансових ринків [2];
- складова операційних ризиків компаній [3; 4];
- ймовірності настання подій у сфері інформаційних активів, комп'ютерних та комунікаційних ресурсів [5];
- ймовірні злочини, здійснені за допомогою мережі Інтернет [6].

Одним із найбільш повних теоретичних опрацювань вважається робота М. Елінга, де розглянуто 209 позицій з тематики кіберризику. При цьому автор виділив 7 сфер дослідження кіберризиків [7].

Серед вітчизняних науковців варто видіти праці В. Братюка, К. Семенової, К. Тарасової, Ю. Кожедуба, які приділили увагу страховому захисту від кіберризиків, проблемам їх менеджменту та аналізу документів з керування ними [8–10].

Не дивлячись, що в зазначених дослідженнях відображені окремі аспекти явища кіберризиків, в українській науковій літературі загалом поки що відсутнє цілісне комплексне дослідження з економічних проблем кіберризиків.

Метою статті є дослідження детермінантів виникнення кіберризиків та їх негативного впливу на світову та національну економіки.

Матеріали та методи. Теоретичним та методологічним підґрунтям статті стали праці вітчизняних та зарубіжних науковців. Застосування методів теоретичного узагальнення, порівняльного аналізу, аналізу та синтезу дозволило обґрунтувати детермінанти кіберризиків.

Результати дослідження. На основі аналізу наукової літератури та нормативно-правових актів можна виділити три підходи щодо розуміння дефініції кіберризику: причинно-наслідковий, секторальний та інструментальний.

Причинно-наслідковий підхід пов'язує наслідки реалізації кіберризиків та джерела їх виникнення. Згідно з ним, кіберризик – це будь-який ризик фінансових втрат, збоїв або шкоди репутації організації внаслідок відмови систем інформаційних технологій [11]. Робоча група Комітету з виплат і ринкової інфраструктури та Міжнародна організація комісій з цінних паперів Банку міжнародних розрахунків розглядають кіберризик як поєднання вірогідності події, що відбуваються у сфері інформаційних активів організації, комп'ютерних і комунікаційних ресурсів та наслідків цієї події для організації [5].

В секторальному підході акцент ставиться на сферах реалізації кіберризиків. Кіберризик може бути визначений як загроза, пов'язана з онлайн-активністю, інтернет-торгівлею, електронними системами та технологічними мережами, а також зберіганням персональних даних [12].

В основі інструментального підходу покладено інструменти, за допомогою яких відбувається реалізація кіберризиків. Форум *Chief Risk Officers (CRO)* визначив кіберризики як будь-які ризики, що виникають при використанні електронних даних та їх передачі, включаючи технологічні інструменти, такі як інтернет та телекомунікаційні мережі. Це також містить у собі фізичний збиток, який може бути спричинений випадками порушення кібербезпеки; шахрайством, заподіяним зловживанням даними, будь-якою відповідальністю, що виникає внаслідок зберігання даних; а також доступності, цілісності та конфіденційності електронної інформації щодо приватних осіб, компаній чи урядів [13]. Всі підходи дають можливість стверджувати, що кіберризику притаманні ознаки операційного ризику. Слід зауважити, що середовищем виникнення кіберризиків є кіберпростір. Не дивлячись на існування множинності підходів до визначення кіберпростору, можна виділити його ознаки, присутні у всіх підходах. Кіберризик не може існувати без матеріальних елементів, він містить інформацію та є віртуальним [14]. Подібний підхід передбачає Федеральна служба розслідувань США і трактує кіберризики як ймовірні злочини, здійснені за посередництвом мережі Інтернет [6].

Поняття кіберризиків можна розглядати у вузькому і широкому значенні. У вузькому значенні кіберризики пов'язані з операційними загрозами інформаційним та технологічним активам, які негативно впливають на конфіденційність, доступність та цілісність інформації або інформаційної системи. Кіберризик – це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі. В широкому значенні кіберризики – це ймовірність загрози інтерактивним цифровим мережам, що використовуються для передачі, модифікації та зберігання інформації (кіберпростору).

Кіберзлочини поділяються на дві групи: кіберзалежні злочини та кіберможливі злочини.

Під кіберзалежними злочинами (*Cyber dependent crime*) розуміють злочини, які здійснюються лише з використанням пристроїв інформаційно-комунікаційних технологій, що є одночасно інструментом і метою злочину (наприклад, розробка та розповсюдження шкідливого програмного забезпечення для отримання фінансової вигоди, здійснення злому для крадіжки, пошкодження чи знищення даних та/або мережевої активності). Кіберможливі злочини (*Cyber-enabled crime*) – це традиційні злочини, що можуть бути збільшені в масштабі за допомогою комп'ютерів, комп'ютерних мереж або інших форм інформаційно-комп'ютерної техніки (наприклад, шахрайство з використанням кібертехнології та крадіжка даних) [15].

З огляду на проблему швидкої дифузії кіберзагроз і практично відсутність контролю за їх поширенням варто виділити рівні прояву кіберзлочинів:

- мікрорівень (рівень окремих домогосподарств і підприємств);
- макрорівень (рівень окремих галузей);
- мезорівень (рівень окремих країн чи їх об'єднань).

Відповідно до тривалості впливу наслідків ризику, можна виокремити довгострокову та короткострокову дію кіберзлочину.

Джерела виникнення операційних кіберризиків систематизували Й. Кебула і Л. Янг, виділивши чотири класи: дії людей, бездіяльність системи і технології, помилки у внутрішніх процесах та зовнішні події [4]. Кожен клас поділяється на підкласи, які в своєму складі мають різні елементи-чинники. З точки зору управління ризиками підкреслюється, що найбільше значення для фірми мають перебої (бездіяльність) в системах і технологіях *(рис. 1)*.

Одним із інструментів реалізації кіберризику є кібератака. Федеральна рада експертизи фінансових установ США *(Federal Financial Institutions Examination Council, FFIEC)* розрізняє поняття кібератаки та кіберінциденту. Під кібератакою розуміється спроба пошкодити, порушити або отримати несанкціонований доступ через кіберпростір до комп'ютера, комп'ютерної системи або електронної мережі зв'язку з метою порушення, виключення, знищення або зловмисного контролю над обчислювальним механізмом чи інфраструктурою; або знищення цілісності даних, або викрадення керованої інформації [16]. Кіберінцидент розглядається *FFIEC* як дії через використання комп'ютерних мереж, що призводять до фактичного або потенційно несприятливого впливу на інформаційну систему або інформацію. У доповіді британської спеціалізованої страхової компанії *«Hiscox»* за 2016 р. зазначено, що кіберзлочини завдали збитків світовій економіці у розмірі 450 млрд дол. США та було викрадено понад 2 млрд записів персональних даних [17]. У тому ж році шкідлива інтернет-активність завдала економіці США збитків від 57 до 109 млрд дол. США [18].

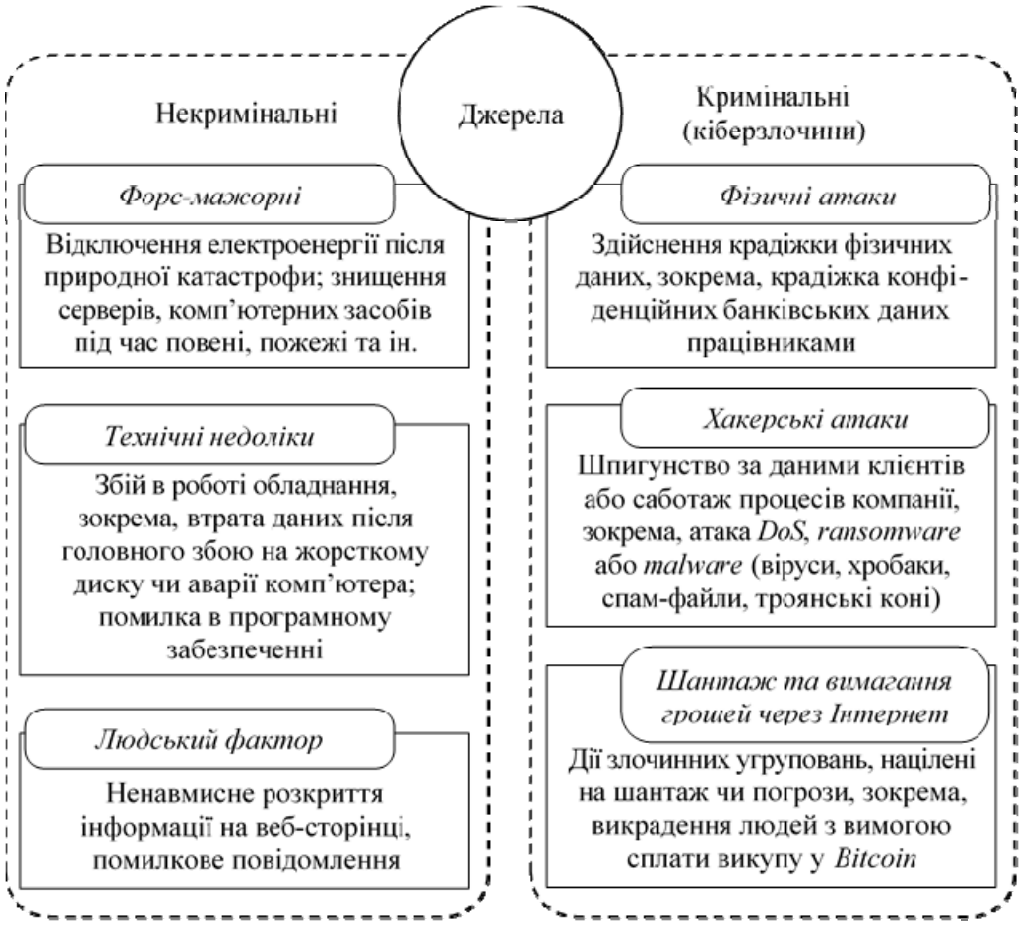


Рис. 1. Класифікація джерел кіберризиків

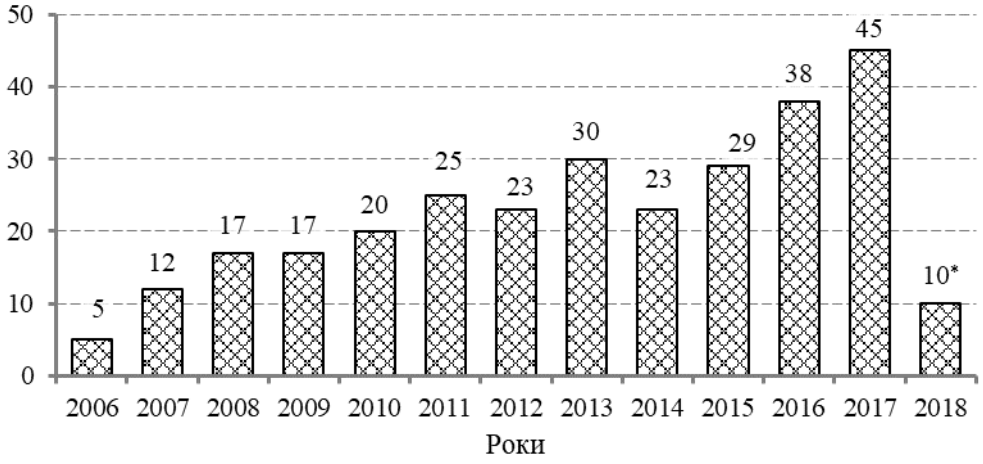
Джерело: складено авторами на основі [15, с. 146].

Слід зазначити, що 43 % кібератак у США спрямовується на малий бізнес [19]. Згідно з даними уряду Великої Британії, опрацьованих разом із фірмою *Pricewaterhausecooper*, збитки від кібератак для малого і середнього бізнесу країни в 2015 р. становили від 75 тис. до 310 тис. фунтів і від 1,46 млн до 3,41 млн фунтів – для великого [20].

До переліку форм реалізації кіберризику варто додати третю категорію – кібертероризм. Особливістю кібертероризму є мотивація, яка полягає у деструктивному впливі на соціально важливу інфраструктуру (наприклад, систему електропостачання, залізничного сполучення) [21]. Четвертою категорією, яку варто розглядати як найважчу форму прояву кіберризиків, є кібервійна, характерною особливістю якої є використання інформаційних технологій однією країною з метою руйнації та створення нестабільності в іншій [22]. Ключовий критерій поділу на такі форми – це мотивація кібервтручання та механізм його впливу на інформаційні системи. На практиці такий поділ досить складний, оскільки дуже часто важко визначити основну мотивацію злочинної кібердії.

Консалтингова компанія *Phenomenon* провела опитування серед 2168 фірм в країнах Європи, Південної Америки, Азії та Африки, які запровадили управління кіберризиками як складову системи управління ризиками. Відповіді респондентів показали, що 46 % мали досвід з кібератаками, причому вони носили різний характер – пов'язані з руйнуванням бізнесу та IT-процесів – 46 %, пошкодженням або крадіжками конфіденційних даних фірми (наприклад інтелектуальну власність) – 34 %, з крадіжками конфіденційної інформації приватних осіб – 26 % [23, с. 13]. Згідно з дослідженнями страхової компанії *Allianz*, до кіберризиків, що найбільше впливали на діяльність компаній, належать переривання бізнес-процесів, крадіжка інтелектуальної власності та кібервимагання [24].

За даними Центру стратегічних та міжнародних досліджень (*Senter for Strategic&International Studies, CSIS*) кількість значних кіберінцидентів практично щороку зростає. При цьому спостерігається чітка тенденція до їх зростання впродовж 2014–2017 р. Водночас уже у 2018 р. було зафіксовано 11 значних кіберінцидентів (*рис. 2*).



* станом на I квартал 2018 р.

Рис. 2. Кількість кіберінцидентів у світі

Джерело: складено авторами на основі [25].

Спільні дослідження *CSIS* та компанії *McAfee* свідчать, що щорічна вартість кіберзлочинів у глобальному масштабі становить 445–600 млрд дол. США. Це складає приблизно 1 % світового ВВП [26]. У структурі мотивацій кібератак станом на січень 2018 р. найбільшу частку займають кіберзлочини (*cyber crime*) – 81,7 %. Водночас частка кібершпигунства (*cyber espionage*) склала 12,2 %, кібервійн (*cyber warfare*) – 4,3 %, хактівізму (*hacktivism*) – 1,7 % [27]. За векторами дії кібератак станом на січень 2018 р. переважали шкідливі програми – 43,5 %. При цьому частка викрадення облікових записів склала 14,8 %, невідомих – 13 %, цільових атак – 9,6 %, *DDoS* – 6,1 % [27].

Найбільш потужними кіберінцидентами у 2017 р. стали *WannaCry*, *Petya*, *Dragonfly* 2.0 *Equifax*, *Deloitte LLP*, коротку характеристику яких описано у *табл. 1*.

Таблиця 1

Характеристика найбільших кіберінцидентів у 2017 році

Назва	Період	Програмне забезпечення	Масштаби поширення	Розмір збитків
WannaCry	Травень, 2017 р., чотири дні	*Ransomware.* Врахував вразливість *EternalBlue* у *Microsoft Windows XP* та *Windows Server 2003*	Кількість країн охоплення – 150. Кількість жертв – близько 200 тис. [28]	Близько 4 млрд дол. США
NotPetya	Вперше зявився як *Petya* у 2016 р. *NotPetya* – червні 2017 р.	*Malware.* Врахував вразливість *Eternal Blue* та *Eternal Romancey Microsoft Windows XP* та *Windows Server* 2003. В Україні була пов'язана із бухгалтерським програмним забезпеченням «*MeDoc*»	Кількість країн охоплення: понад 60 [29]. **Україна:** урядові організації, банки, державні енергетичні установи та залізничні компанії, аеропорти «Бориспіль» та «Жуляни», автозаправки, організації водопостачання, телефонні компанії, метрополітен м. Києва, сайт Львівської міської ради, система радіаційного моніторингу на Чорнобильській атомній станції була переведена у «ручний» режим управління. **Нідерланди:** судноплавна компанія *TNT Express*, дочірня компанія *FedEx*. **Великобританія:** рекламна компанія. **Данія:** конгломерат з транспорту та логістики Maersk. **Іспанія:** транснаціональні компанії. **Австралія:** юридична фірма *DLA Piper*, авіалінії «*Qantas*»	Невідомий
Dragonfly 2.0	Перша половина 2017 р.	Троянські програми віддаленого доступу, замасковані під оновлення *Flash: Backdoor.Goodor*, *Backdoor.Dorshe*l і *Trojan. Karagany.B*	Орієнтована на критичні галузі енергетики **США, Туреччини та Швейцарії**	Невідомий
Equifax	Вересень 2017 р.	Порушення даних (*data breaches*)	Британське відділення американського кредитно-рейтингового агентства *Equifax* визнала, що майже 700 тисяч британських споживачів мали доступ до своїх особистих даних після кібер-атаки, що набагато вище, ніж вважалося раніше [30]	27, 3 млн дол. США. Загальні операційні витрати *Equifax* зросли на 15 %. Додатково витрати на надання безкоштовного кредитного моніторингу – 56 млн дол. США [31]
Deloitte LLP	Березень 2017 р.	Порушення даних (*data breaches*)	*Deloitte* – одна з найбільших приватних фірм Нью-Йорку, що зареєстрована в Лондоні. Вона надає консультації з питань аудиту, оподаткування, кібербезпеки для найбільших банків світу, міжнародних компаній, медіа підприємств, фармацевтичних фірм та державних установ. Гіпотетично могли бути викрадені дані з 5 млн листів, що знаходяться у хмарі [32]. Проте офіційно було заявлено, що лише 350 клієнтів можуть опинитися під загрозою [33]	Невідомий

Джерело: складено авторами за [28–33].

Нині спостерігається активізація впливу ринку криптовалют на реалізацію кібератак [34, с. 90]. Національне агентство зі злочинності Великобританії (*National Crime Agency, NCA*) визначає, що криптовалюти допомагають кіберзлочинцям отримати платіж від жертви, сприяють зростанню кіберзлочинності як послуги, полегшують фінансові потоки у кіберзлочинному світі [35].

Під час опитування ризик-менеджерів фінансових послуг, проведеного компанією *Depository Trust&Clearing Corporation* (*DTCC*), 70 % респондентів зазначили, що кіберризик має найсуттєвіший вплив на функціонування глобальної фінансової системи. Водночас до п'ятірки ризиків, що загрожують функціонуванню глобальної фінансової системи, також належать географічний ризик (50 %), вплив нових регуляторних вимог (41 %), економічний спад (33 %), монетарна політика (31 %) [36]. Проте сфера фінансових послуг та глобальна фінансова система не є винятками для кіберзагроз. Їх потужного впливу також зазнають сфери комунальних послуг, транспорту, охорони здоров'я, нафтогазова індустрія, урядові органи. У грудні 2015 р. в Туреччині відбулись кібератаки на мережі, якими користувались банки, уряд та засоби масової інформації [37]. В тому ж році в Україні кібератаки зазнала українська система дистрибуції електроенергії, тимчасово позбавивши майже 230 тис. громадян доступу до електрики [38]. Серед суб'єктів господарювання найбільш чутливими сферами до кіберзагроз є телекомунікації, логістика та виробництво.

Не є винятком впливу кіберризиків і сфера міжнародної торгівлі, підґрунтям поширення якої є інтернет, інформаційні та комунікаційні технології. Перш за все це стосується транскордонної е-комерції, частка якої вже нині становить біля 7 % загального обсягу е-комерції [39]. Використання сучасних технологій обумовило не лише потужне зростання е-комерції, але й активізацію кіберзагроз у вигляді несанкціонованого доступу до персональних даних споживачів, їх використання чи модифікації. Це стосується зараження комп'ютерів шкідливими програмами, зокрема вірусами, хробаками, троянськими конями; хактівізму; кібершпигунства шляхом доступу до незахищеної інформації через *Wi-Fi*, підробки *IP*-адрес та сканування портів. Також кібершпигунство є інструментом отримання конкурентних переваг на міжнародному ринку. При цьому часто фінансування кібершпигунства здійснюються урядами. Яскравим прикладом є взаємне обвинувачення Китаю та США у кібершпигунстві та застосування на цьому підґрунті взаємних санкцій.

Значного впливу кібератаки завдають об'єктам глобального постачання. Прикладом є кібератака на гіганта судноплавства «*Maersk*» влітку 2017 р., що здійснює міжнародні перевезення товарів, зокрема нафти. Вона спричинила значну перерву в роботі компанії під час вимкнення комп'ютерів за допомогою шкідливого програмного забезпечення та збитки близько 300 млн дол. США [40]. Хоча подібні інциденти можуть обумовити серйозніші наслідки для глобальної економіки.

Варто зазначити, що наслідки (в економічному контексті – втрати) від реалізації кіберризиків поділяються на прямі та непрямі [2, с. 9]. Прямі втрати пов'язані з експертизою, розслідуванням, правовим захистом, інформуванням клієнтів, зміцненням системи захисту даних клієнтів та компанії. Непрямі витрати менш помітні, але довготриваліші та складніші в оцінці. У *табл. 2* показано основні негативні наслідки реалізації кіберризику.

Таблиця 2

Наслідки реалізації кіберризиків

Прямі	Опосередковані
Втрата власних даних компанії (комерційних таємниць, конфіденційної інформації)	Відкликання продукту з ринку
Втрата клієнтів	Розірвання контрактів
Санкції від державних органів	Кадрові зміни
Активізація технічних досліджень	Зростання страхових премій
Регуляторне доповнення	Зростання витрат на обслуговування позик
Посилення громадських зв'язків	Вплив операційного підриву чи руйнування
Покращення кібербезпеки	Знецінення торгової марки
Повідомлення про злам даних клієнтів	Втрата інтелектуальної власності
Захист клієнтів від зламу	Вартість втрати доходу за контрактом
Виплати на адвокатські гонорари та судові збори	Втрата цінності зв'язку з клієнтом
Витрати, пов'язані з виплатою компенсацій клієнтам	Втрата репутації та часу на її відновлення

Джерело: авторська розробка за [39].

У 2016 р. шкідлива активність в інтернеті була за масштабами другим у світі типом економічної злочинності, яка торкнулася 32 % організацій. В Індії за десять років до 2014 р. рівень злочинності в інтернеті збільшився в 19 разів, водночас вона наразі посідає третє місце після США та Китаю за кількістю джерел шкідливої онлайн-діяльності. У Великобританії за 2016 р. одне з кожних п'яти підприємств зазнало нападу, і лише 24 % британських компаній стверджують, що вони мають безпеку для захисту від зламу [41, с. 3]. У США кібератак зазнавала у 2017 р. одна з кожних п'яти компаній. При цьому дві третини підприємств країни вважають кіберризик фундаментальним викликом для свого бізнесу [42, с. 5–6]. Наслідки від кібератак стають відчутнішими через застосування кіберзлочинцями нових технологій, що сприяють цьому виду злочинної діяльності, зокрема «чорних ринків» та цифрової валюти.

Висновки. Кіберризик є динамічним ризиком, в основі якого лежить втручання та порушення цілісності інформаційного забезпечення. Кіберризик найчастіше проявляється через кібератаки, наслідки

яких можуть бути як прямі, так і опосередковані, що значно ускладнює процес оцінки фінансових втрат. Крім того, фінансові втрати від реалізації кіберризиків не обмежені в часі, тобто можуть проявитись набагато пізніше після ліквідації шкоди.

Щороку відмічається стрімкий зріст кількості кіберінцидентів і їх вартості. Об'єктом кібератак можуть бути фізичні й юридичні особи, які є суб'єктами зовнішньоекономічної діяльності, окремі галузі економіки чи ціла країна. Найбільш загрозливою формою прояву кіберризику є кібервійна, яка може охоплювати всю країну. Для попередження реалізації кіберризиків кіберпростір має регулюватися певними правилами та нормами поведінки. Національні органи кібербезпеки мають отримувати від суб'єктів національної економіки своєчасні та точні звіти про кіберподії. Стандарти для кіберризику повинні передбачати надання внутрішніх даних фінансовими установами, що автоматизовано оброблятимуться. На першому етапі це має здійснюватися на періодичній основі, а у подальшому – в режимі реального часу. При цьому здійснюватиметься перевірка надійності даних.

Враховуючи кримінальну природу кібератак, органи нагляду за ринками фінансових послуг повинні взаємодіяти з відповідними правоохоронними органами на основі двостороннього надання інформації. Для швидкої адаптації до мінливих кіберзагроз регуляторні правила для фінансових установ мають бути гнучкими.

Основними інструментами забезпечення кібербезпеки учасників транскордонної е-комерції є аутентифікація клієнтів, антивірусне програмне забезпечення, шифрування, цифровий підпис. Оскільки боротьба з кіберзлочинцями реальна та постійна, технології (такі як токенізація**,** біометрія, штучний інтелект) допомагають ідентифікації клієнтів, безпечності транзакцій та мінімізації збитків від шахрайства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Global Economic Forum, The Global Risks Report 2017. 12th Edition. URL : http://wef.ch/risks2017.
2. Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability. Working Paper, 2017. International Monetary Fund. URL : https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx.
3. Peters Gereth W., Shevchenko P. V., Cohen D. R., Maurice D. Understanding Cyber Risk and Cyber Insurance, FinTech: Growth and Deregulation. URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065635.
4. Cebula J. J., Young L. R. A Taxonomy of Operational Cyber Security Risks, Carnegie Mellon University. URL : https://www.sei.cmu.edu/reports/10tn028.pdf.
5. Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures. June 2016. URL : https://www.bis.org/cpmi/publ/d146.htm.
6. Federal Bureau of Investigation, Internet Crime Report. 2016. URL : https://pdf.ic3.gov/2016_IC3Report.pdf.
7. Eling M. What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance. 2017. Iss. 5. P. 474–491.

8. Братюк В. П. Сутність кіберризиків та страховий захист від кіберризиків в Україні. Актуальні пробл. економіки. 2015. № 9 (171). С. 421–427.
9. Семенова Е. Д., Тарасова К. И. Становление нового цифрового мира и проблемы менеджмента кибер-рисков. Маркетинг і менеджмент інновацій. 2017. № 3. С. 236–244.
10. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. Information Technology and Security. 2017. Vol. 5. № 1. С. 82–95.
11. Institute of Risk Management. URL : https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk.
12. Olsen T. Cyber risk insurance. 18.06.2013. URL : https://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf.
13. CRO Forum. The Cyber Risk Challenge and the Role of Insurance. December 2014. URL : http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance.
14. Rajnovic D. Cyberspace – What is it? Cisco Blogs. July 2012. URL : https://blogs.cisco.com/security/cyberspace-what-is-it.
15. Eling M., Wirfs J. H. Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class Institute of Insurance Economics Universitat St. Gallen. 2016, 174 p. URL : www.ivw.unisg.ch.
16. Lloyds Banking Group. Understanding the interactions between cyber-crime and fraud prevention. URL : https://www.cefpro.com/0506ri-understanding-the-interactions-between-cyber-crime-and-fraud-prevention.
17. FFIEC. Cybersecurity Assessment Tool Glossary. June 2015. URL : http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.
18. Киберпреступления обошлись мировой экономике в $450 миллиардов в 2016 году. URL : http://biz.censor.net.ua/news/3020281/kiberprestupleniya_oboshlis_mirovoyi_ekonomike_v_450_milliardov_v_2016_godu.
19. CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy. February 16, 2018. URL : https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy.
20. Rob Starr.7Types of Cyber Attacks Are Threatening Your Small Business Right Now. May 8, 2017. URL : https://smallbiztrends.com/2017/05/types-of-cyber-attacks-small-business.html.
21. PricewaterhouseCooper. 2015 Information Security Breaches Survey. Department for Business, Innovation and Skills. URL : www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.
22. Hua J., Bapna S. The economic impact of cyber terrorism. The Journal of Strategic Information Systems. 2013. № 22 (2). P. 175–186.
23. Ponemon Institute LLC. Global Cyber Risk TransferComparison Report. 2017. URL : http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp.
24. Allianz Global Corporate and Speciality. A Guide to Cyber Risks. URL : https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
25. Significant Cyber Incidents Since 2006: Center for Strategic&International Studies. URL : https://csis-prod.s3.amazonaws.com/s3fs-public/180308_Significant_Cyber_Events _List.pdf?Szs5ZuZShJAIfgcUXRsvB5T8C76PJR0y.
26. Lewis J. Economic Impact of Cybercrime No Slowing Down. URL : https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_ CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-b9303ae70.
27. Passeri P. Cyber Attacks Statistics. January 2018. Nextgen Network Monitor. URL : https://www.hackmageddon.com/2018/02/22/january-2018-cyber-attacks-statistics.
28. WannaCry Ransomware – A Wake-Up Call for Cybersecurity and Data Management. URL: http://en.finance.sia-partners.com/20170609/wannacry-ransomware-wake-call-cybersecurity-and-data-management.

29. Вірус petya.a вразив мережі у 60 країнах світу. Reuters. URL : https://www.5.ua/svit/virus-petyaa-vrazyv-merezhi-u-60-krainakh-svitu-reuters-149124.html.
30. Personal details of almost 700,000 Britons hacked in cyber-attack https://www.theguardian.com/technology/2017/oct/11/personal-details-of-almost-700000-britons-hacked-in-cyber-attack.
31. Surane J. Equifax Is Haunted By Its Costly Cyber Attack. URL : https://www.bloomberg.com/news/articles/2017-11-09/equifax-haunted-by-cyber-attack-as-costs-jump-lawsuits-abound.
32. Deloitte hit by cyber-attack revealing clients' secret email. URL : https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.
33. The Biggest Cybersecurity Threats of 2017: The Need to Prepare. 24.10.2017. URL : http://en.finance.sia-partners.com/20171024/biggest-cybersecurity-threats-2017-need-prepare.
34. Волосович С. Державне регулювання ринку криптовалют: зарубіжний досвід. Зовнішня торгівля: економіка, фінанси, право. 2018. № 1. С. 97–108.
35. UK national risk assessment of money laundering and terrorist financing. URL : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.
36. Reagan J., Raghavan A., Thomas A. Quantifying risk: What can cyber risk management learn from the financial services industry?. Deloitte Review. Iss. 19. July 25, 2016. URL : https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/quantifying-risk-lessons-from-financial-services-industry.html.
37. Snyder C. How Attackers Can Disrupt the Global Internet, Why it Matters, And What We Can Do About It. Harvard University Belfer Center for Science and International Affairs. May 2017. URL : https://www.belfercenter.org/publication/too-connected-fail.
38. Zetter K. Inside the cunning, unprecedented hack on Ukraine's power grid. March 3, 2016. URL : https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.
39. 5 ways to make global e-commerce easier for everyone. December, 2017. URL : https://www.weforum.org/agenda/2017/12/ecommerce-trade-wto-growth-opportunity.
40. Bahar M., Satnick T. Cyber Kinks in the Global Supply Chain. URL : http://www.globaltrademag.com/global-trade-daily/commentary/cyber-kinks-global-supply-chain.
41. Payment cybersecurity: Be prepared. Be protected. London: Worldpay 2017. URL : http://offers.worldpayglobal.com/rs/850-JOA-856/images/Worldpay_Security_Whitepaper_v10.1.pdf?mkt_tok=eyJpIjoiTXpsa05EZ3hOR1F3TlRRNSIsInQiOiJGWlVjTDVDZjdGOUVTa1BwNHlWYXExNUl4WXJQVTlpM2NHRmtNOU5vZDJJcGlTWWlTRDZGcFBibUkwakxpNVpTZ2VScFF0MllEclV0b2FBOUtMQ21qdHhacU1MXC9VYVMyQ01zdWQrUm9PWlFzT0k3T21YUXQ0R01OWlIyQ2todDAifQ%3D%3D.
42. Willis Towers Watson. Cyber Risk Survey Report 2017. URL : https://www.willistowerswatson.com/en/insights/2017/06/2017-cyber-risk-survey-report.

Стаття надійшла до редакції 25.04.2018.

Volosovych S., Klapkiv L. Determinants of the cyber-risks arise and realization.

Background. *Over the past decades, the development of the Internet has revolutionized the communication area, which has become a major factor in global economic growth, but has led to cyber-risk arise.*

Analysis of recent research and publications. *In modern scientific literature the small number of jobs is devoted to the economic aspects of cyber-risks and methods of managing them. The pace of research on this problem in developed countries leaves*

significantly behind the domestic developments. This gap, on the one hand, is explained by the level of development of the financial system and the degree of its dependence on information technology. On the other hand, the issue of cyber risk combines two different areas: financial and informational, requiring an interdisciplinary approach to its study.

Private institutions play a key role in the study of the essence of cyber-risks: consulting, insurance companies and information and software companies, such as AON, PricewaterhouseCoopers, Deloitte, Ernstand Young, Society of Actuaries, International Association, Allianz, and Geneva Association. With the growing of cyber risk and the negative financial implications of its implementation, state and commercial institutions, such as the Federal Bureau of Investigation in the USA, the Bank for International Settlements, are increasingly paying attention to this threat.

Among domestic scientists it is worth to highlight the works of V. Bratiuk, E. Semenova, and Yu. Kozhedub, that paid attention to insurance protection against cyber-risks, to problems of their management and analysis of documents on their management.

*The **aim** of the article is to study the determinants of cyber-risk and their negative impact on world and national economies.*

***Materials and methods.** The works of domestic and foreign scholars have become the theoretical and methodological basis of the article. The research was carried out using the methods of theoretical generalization, comparative analysis, analysis and synthesis.*

***Results**. Based on the analysis of scientific literature and normative legal acts, the causal, sequential, and instrumental approaches to understanding the definition of cyber risk are identified. It is proposed to consider the concept of cyber-risk in a narrow and broad sense. In the narrow sense, cyber-risk is associated with operational threats to information and technology assets that adversely affect the confidentiality, availability and integrity of information or information systems. Cyber-risk is an operational risk, which is to obtain direct or indirect damage by economic agents as a result of their operation in cyberspace. In the broad sense, cyber-risks are the likelihood of a threat to interactive digital networks used to transmit, modify, and store information.*

***Conclusion.** To prevent cyber-risk implementation, cyberspace should be governed by certain rules of behavior. National cyber-security agencies should receive timely and accurate cyber-crime reports from national economic agents. Cybersecurity standards should include the provision of internal cyber-risk data by financial institutions that will be automated.*

Keywords: cyber-risk, cyber-attack, cyber-threat, cyber-incident.

REFERENCES

1. Global Economic Forum, The Global Risks Report 2017. 12th Edition. URL : http://wef.ch/risks2017.
2. Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability. Working Paper, 2017. International Monetary Fund. URL : https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx.
3. Peters Gereth W., Shevchenko P. V., Cohen D. R., Maurice D. Understanding Cyber Risk and Cyber Insurance, FinTech: Growth and Deregulation. URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065635.
4. Cebula J. J., Young L. R. A Taxonomy of Operational Cyber Security Risks, Carnegie Mellon University. URL : https://www.sei.cmu.edu/reports/10tn028.pdf.
5. Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures. June 2016. URL : https://www.bis.org/cpmi/publ/d146.htm.
6. Federal Bureau of Investigation, Internet Crime Report. 2016. URL : https://pdf.ic3.gov/2016_IC3Report.pdf.

7. Eling M. What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance. 2017. Iss. 5. P. 474–491.
8. Bratjuk V. P. Sutnist' kiberryzykiv ta strahovyj zahyst vid kiberryzykiv v Ukrai'ni. Aktual'ni probl. ekonomiky. 2015. № 9 (171). C. 421–427.
9. Semenova E. D., Tarasova K. I. Stanovlenie novogo cifrovogo mira i problemy menedzhmenta kiber-riskov. Marketing i menedzhment innovacij. 2017. № 3. S. 236–244.
10. Kozhedub Ju. Analiz dokumentiv z keruvannja ryzykom kiberbezpeky. Information Technology and Security. 2017. Vol. 5. № 1. S. 82–95.
11. Institute of Risk Management. URL : https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk.
12. Olsen T. Cyber risk insurance. 18.06.2013. URL : https://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf.
13. CRO Forum. The Cyber Risk Challenge and the Role of Insurance. December 2014. URL : http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance.
14. Rajnovic D. Cyberspace – What is it? Cisco Blogs. July 2012. URL : https://blogs.cisco.com/security/cyberspace-what-is-it.
15. Eling M., Wirfs J. H. Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class Institute of Insurance Economics Universitat St. Gallen. 2016, 174 p. URL : www.ivw.unisg.ch.
16. Lloyds Banking Group. Understanding the interactions between cyber-crime and fraud prevention. URL : https://www.cefpro.com/0506ri-understanding-the-interactions-between-cyber-crime-and-fraud-prevention.
17. FFIEC. Cybersecurity Assessment Tool Glossary. June 2015. URL : http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.
18. Kiberprestuplenija oboshlis' mirovoj jekonomike v $450 milliardov v 2016 godu. URL : http://biz.censor.net.ua/news/3020281/kiberprestupleniya_oboshlis_mirovoyi_ekonomike_v_450_milliardov_v_2016_godu.
19. CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy. February 16, 2018. URL : https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy.
20. Rob Starr.7Types of Cyber Attacks Are Threatening Your Small Business Right Now. May 8, 2017. URL : https://smallbiztrends.com/2017/05/types-of-cyber-attacks-small-business.html.
21. PricewaterhouseCooper. 2015 Information Security Breaches Survey. Department for Business, Innovation and Skills. URL : www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.
22. Hua J., Bapna S. The economic impact of cyber terrorism. The Journal of Strategic Information Systems. 2013. № 22 (2). P. 175–186.
23. Ponemon Institute LLC. Global Cyber Risk TransferComparison Report. 2017. URL : http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp.
24. Allianz Global Corporate and Speciality. A Guide to Cyber Risks. URL : https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
25. Significant Cyber Incidents Since 2006: Center for Strategic&International Studies. URL : https://csis-prod.s3.amazonaws.com/s3fs-public/180308_Significant_Cyber_Events _List.pdf?Szs5ZuZShJAIfgcUXRsvB5T8C76PJR0y.
26. Lewis J. Economic Impact of Cybercrime No Slowing Down. URL : https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-b9303ae70.
27. Passeri P. Cyber Attacks Statistics. January 2018. Nextgen Network Monitor. URL : https://www.hackmageddon.com/2018/02/22/january-2018-cyber-attacks-statistics.

28. WannaCry Ransomware – A Wake-Up Call for Cybersecurity and Data Management. URL: http://en.finance.sia-partners.com/20170609/wannacry-ransomware-wake-call-cybersecurity-and-data-management.
29. Virus petya.a vrazyv merezhi u 60 krai'nah svitu. Reuters. URL : https://www.5.ua/svit/virus-petyaa-vrazyv-merezhi-u-60-krainakh-svitu-reuters-149124.html.
30. Personal details of almost 700,000 Britons hacked in cyber-attack https://www.theguardian.com/technology/2017/oct/11/personal-details-of-almost-700000-britons-hacked-in-cyber-attack.
31. Surane J. Equifax Is Haunted By Its Costly Cyber Attack. URL : https://www.bloomberg.com/news/articles/2017-11-09/equifax-haunted-by-cyber-attack-as-costs-jump-lawsuits-abound.
32. Deloitte hit by cyber-attack revealing clients' secret email. URL : https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.
33. The Biggest Cybersecurity Threats of 2017: The Need to Prepare. 24.10.2017. URL : http://en.finance.sia-partners.com/20171024/biggest-cybersecurity-threats-2017-need-prepare.
34. Volosovych S. Derzhavne reguljuvannja rynku kryptovaljut: zarubizhnyj dosvid. Zovnishnja torgivlja: ekonomika, finansy, pravo. 2018. № 1. S. 97–108.
35. UK national risk assessment of money laundering and terrorist financing. URL : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.
36. Reagan J., Raghavan A., Thomas A. Quantifying risk: What can cyber risk management learn from the financial services industry?. Deloitte Review. Iss. 19. July 25, 2016. URL : https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/quantifying-risk-lessons-from-financial-services-industry.html.
37. Snyder C. How Attackers Can Disrupt the Global Internet, Why it Matters, And What We Can Do About It. Harvard University Belfer Center for Science and International Affairs. May 2017. URL : https://www.belfercenter.org/publication/too-connected-fail.
38. Zetter K. Inside the cunning, unprecedented hack on Ukraine's power grid. March 3, 2016. URL : https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.
39. 5 ways to make global e-commerce easier for everyone. December, 2017. URL : https://www.weforum.org/agenda/2017/12/ecommerce-trade-wto-growth-opportunity.
40. Bahar M., Satnick T. Cyber Kinks in the Global Supply Chain. URL : http://www.globaltrademag.com/global-trade-daily/commentary/cyber-kinks-global-supply-chain.
41. Payment cybersecurity: Be prepared. Be protected. London: Worldpay 2017. URL : http://offers.worldpayglobal.com/rs/850-JOA-856/images/Worldpay_Security_Whitepaper_v10.1.pdf?mkt_tok=eyJpIjoiTXpsa05EZ3hOR1F3TlRRNSIsInQiOiJGWlVjTDVDZjdGOUVTa1BwNHlWYXExNUl4WXJQVTlpM2NHRmtNOU5vZDJJcGlTWWlTRDZGcFBibUkwakxpNVpTZ2VScFF0MllEclV0b2FBOUtMQ21qdHhacU1MXC9VYVMyQ01zdWQrUm9PWlFzT0k3T21YUXQ0R01OWlIyQ2todDAifQ%3D%3D.
42. Willis Towers Watson. Cyber Risk Survey Report 2017. URL : https://www.willistowerswatson.com/en/insights/2017/06/2017-cyber-risk-survey-report.