DOI: [10.32702/2307-2105-2022.1.91](https://doi.org/10.32702/2307-2105-2022.1.91)

УДК 339.97

О. В. Дзяд,
к. е. н., доцент кафедри міжнародної економіки і світових фінансів,
Дніпровський національний університет імені Олеся Гончара
ORCID ID: 0000-0002-0869-599X
Д. С. Стародуб,
бакалавр, Дніпровський національний університет імені Олеся Гончара
ORCID ID: 0000-0001-8769-3222

ЕКОНОМІЧНІ ВТРАТИ ТА МЕХАНІЗМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ У СВІТОВОМУ ГОСПОДАРСТВІ

O. Dzyad
PhD in Economics,
Associate Professor of the Department of International Economics and World Finance,
Oles Honchar Dnipro National University
D. Starodub
Bachelor's student, Oles Honchar Dnipro National University

ECONOMIC LOSSES AND INTERNATIONAL METHODS AGAINST CYBERCRIMES AND WAYS TO OPPOSE CYBERCRIMES WORLDWIDE

У статті проаналізовано обсяги, динаміку, чинники зростання кіберзлочинності у світовому господарстві в період пандемії COVID-19, визначено та систематизовано економічні втрати від кіберзлочинності у розрізі країн (регіонів світу), причин виникнення, сфер діяльності та постачальників інформаційних технологій та ресурсів. Автори дослідили вже сформовані механізми кібербезпеки суб'єктів світового господарства на різних рівнях. Було встановлено, що цифровізація суспільства, з одного боку, створює простір для кіберзлочинності, з іншого боку, формує технології, методи, інструменти для протидії та її запобігання. Обґрунтовано необхідність міжнародної координації політики кібербезпеки між суб'єктами світового господарства, розробки та реалізації компаніями стратегій кібербезпеки з урахуванням прямих та непрямих витрат, підвищення обізнаності користувачів у питаннях кібербезпеки з одночасним запровадженням принципів глобальної кіберкультури.

The digitalization of society has become a real challenge and factor in the development of the world economy and its actors – international institutions, states, corporations and ordinary users. The authors have found that the digitalization of society, on the one hand, created space for cybercrime, on the other hand, formed technologies, methods, tools to combat and prevent it. The authors have analyzed the factors, volumes, dynamics of cybercrime growth in the world economy during the COVID-19 pandemic, identified and systematized economic losses from cybercrime by countries (regions of the world), causes, areas of activity and suppliers of information technology and resources. The proliferation of wireless devices with free access to the network, cloud technologies

provide new opportunities for cybercriminals. The cybercrime targets remain the healthcare, energy, finance, pharmaceuticals and technology industries of the industrialized world. Cybercrimes are in the nature of cyberattacks, committed not only for economic but also for political, ideological, terrorist reasons. It is the countries with high per capita incomes that suffer the most and spend the most on cybersecurity policies. During the COVID-19 coronavirus pandemic, employers are trying to improve the safety of their businesses and the work of their home-based workers, but human error remains an important cause of cybersecurity. The authors studied the already established mechanisms of cybersecurity of the world economy at various levels and substantiated the need for international coordination of cybersecurity policy between the world economy. The prospects of cybersecurity policy in the global economy will be related to the introduction of new effective practices to combat cyberattacks, strengthening the protection of sensitive data, development, adoption and implementation of cybersecurity strategies by participants at all levels. When developing corporate cybersecurity strategies for business, it is advisable to take into account the direct and indirect costs associated with the probable loss of data. Improving the general education of network users and implementing the principles of global culture can change the situation for the better.

Ключові слова: кіберзлочини; кібератака; системний злом баз даних; людська помилка; прямі та непрямі витрати компаній; суб'єкти світового господарства; кіберстратегії; глобальна кіберкультура

Keywords: *cybercrime; cyber attack; system database hacking; human error; direct and indirect costs of companies; global economic actors; cyber strategies; global cyberculture*

Вступ та постановка проблеми.

Прискорений розвиток ІТ сфери та цифровізація суспільства супроводжується, з одного боку, зростанням кількості кіберзлочинів, поширенням різноманітних методів та технологій кібератак, з іншого боку, надає можливість ефективніше від них захищатися. Пошук механізмів та інструментів забезпечення кібербезпеки (зокрема, розробка відповідних технологій) є актуальним і важливим напрямом діяльності компаній, країн, міжнародних організацій та світового господарства загалом [1, с. 82].

За даними звіту ВЕФ «Глобальне дослідження сприйняття ризиків 2021»[2], існують технологічні короткострокові загрози розвитку світового господарства, а саме: загрози кібербезпеки та «цифрової нерівності», про що зазначили 39% та 38% респондентів відповідно. У найближчі 3-5 років 53% респондентів вважають, що існує ризик зламу ІТ інфраструктури, ще 49% – прогнозують крах кібербезпеки, 48% – наголошують на збоях технологічного управління. На глобальні та серйозні проблеми, несприятливий вплив технологічного прогресу на розвиток суспільства вказують половина респондентів, що відбудеться у довгостроковому періоді.

Пандемія коронавірусу COVID-19 змусила компанії створювати віддалені робочі сили та працювати з хмарними платформами. Розгортання 5G зробило підключені пристрої ще більш залученими до мережі, ніж будь-коли. Серед компаній, для яких організація віддаленої роботи стала нормою, 70% зазначили, що вони збільшать бюджет на захист даних від злому, а 76% зауважили, що це збільшить час на виявлення та обмеження потенційних кіберінцидентів [3; с. 9]. Актуальність дослідження зумовлена появою низки новітніх загроз у системі міжнародної економічної безпеки, що потребує розробки ефективних механізмів протидії кіберзлочинності та координації спільних зусиль бізнесу, держав, міжнародних інститутів, і світової спільноти.

Аналіз останніх досліджень та публікацій.

Питання кіберзлочинності та кібербезпеки виступають предметом дослідження зарубіжних та вітчизняних науковців. Велику кількість наукових робіт присвячено сутності та технічним аспектам кіберзлочинності та кібербезпеки, серед яких: К. Бронкс, В. Х. Даттон, П. Естеве-Гонсалес, С. Кріз, Р. Шіллайр, О. Ткаченко, К. Ткаченко та інші. Організаційно-правові засади протидії кримінальним правопорушенням з використанням інформаційних технологій розглядали В. Болгов, Н. Гадіон, О. Гладун [6]. Міжнародно-правовим основам регулювання відносин у мережі присвячене дослідження К. Шахбазяна [7]. Кіберзлочинність в контексті забезпечення економічної безпеки країн розглянута в роботах О. Вівчар, А. Колеснікова, О. Олійницук, О. Погайдак [8]. Кіберзагрози у фінансовій сфері світового господарства представлені у роботі Т. Маурера, А. Нельсона [9]. Інформаційно-аналітичну оцінку ризиків кіберзлочинності, кібератак надають міжнародні інститути [3, 10].

Аналіз досліджень зазначених авторів дозволяє дійти висновку про високу актуальність питання техніко-технологічного, нормативно-правового та організаційного механізмів протидії кіберзлочинам.

Економічні втрати суб'єктів світового господарства в умовах «нової цифрової нормальності» в період пандемії COVID-19 залишаються недостатньо дослідженими, поза увагою авторів залишаються фінансово-економічні питання формування кіберстратегій суб'єктів світового господарства на всіх рівнях.

Мета роботи полягала у визначенні втрат від кіберзлочинності в умовах пандемії коронавірусу COVID-19 та ефективних механізмів кібербезпеки для суб'єктів світового господарства всіх рівнів.

Результати дослідження.

Існує багато визначень цифрової безпеки, проте у загальному розумінні кібербезпека – це набір методів та набір інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, навчання, найкращих практик, гарантії та технології, які можна використовувати для захисту кіберсередовища, організації, а також активів користувачів мережі інтернет [5; с. 214].

Передача та зберігання інформації в цифровому вигляді, разом із поширеністю мережових комп'ютерів, створили нові політичні та економічні виклики для світового господарства. Як «нова нормальність» – цифровізація суспільства в період пандемії COVID-19 супроводжується порушенням «цифрового простору» споживачів та виробників послуг та технологій – крадіжками, маніпулюванням, знищенням, несанкціонованим використанням електронних даних.

Питання інформаційної безпеки не нові. Під час холодної війни уряд США розробив складну систему систематизації інформації відповідно до якої друковані документи були чітко визначені за рівнем їх секретності. Дотримуючись парадигми індустріалізації, такі документи були закритими, а їх отримання потребувало спеціальних дій (проникнення в офіс, фотографування, передачу, розсекречення даних).

На початку розвитку ери комп'ютерної техніки, комп'ютерною безпекою в організації у більшості випадків займалася команда професіоналів з організації інформаційних систем та технологій (ІТ), яка часто мала досвід та засоби для забезпечення фізичного та електронного доступу до комп'ютерного обладнання та послуг. Оскільки комп'ютери перейшли до «систем спільного використання ресурсів», питання кібербезпеки потребують значних ресурсів, розробки відповідної стратегії, механізмів протидії кіберзлочинам та координації дій між різними суб'єктами ринку. Відповідальність за безпеку вийшла далеко за межі ІТ-команди будь-якої окремої організації. Вони можуть залучати різноманітні установи та окремих осіб у всьому світі, включаючи понад чотири з половиною мільярди користувачів Інтернету, що представляють більше половини населення світу [5; с. 215]. Більше того, підходи до забезпечення кібербезпеки більше не є переважно технічними, оскільки вони все більше охоплюють законодавчі та політичні питання, розраховані на певні навички та практики користувачів, сформовані різноманітністю культур і суспільств в Інтернеті та в усьому світі. Оскільки Інтернет став більш розповсюдженим в житті та на робочому місці, є все більше усвідомлення того, що кібербезпека не може бути просто реакцією на виникаючі проблеми, вона має попереджати загрози кіберзлочинів, щоб підвищити стійкість будь-яких систем.

Різноманітність поведінки користувачів комп'ютерів призвела до формування традиційних та появи нових форм кіберзлочинності. Традиційними формами кіберзлочинності можна вважати: кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг, соціальну інженерію, мальваре, протиправний контент, рефайлінг. Відносно новою формою є хактивізм, де хакерство поєднується з політичною активністю (створений неологізм хактивізм). Хактивізм переносить політичні демонстрації в мережі інтернет і часто «наслідує» діяльність, що спостерігається в нецифровому світі. З розвитком криптовалюти виникло поняття криптоджекінг. Його можна віднести до випадків, коли хакер захоплює комп'ютер для видобутку криптовалюти проти волі користувачів через веб-сайти або поки користувач ні про що не здогадується.

Для держави підключення до глобальної інформаційної мережі також створює нові вразливі місця. Не кожна сторона, підключена до мережі, переслідує цілком доброзичливі інтереси. Корпорації бажають отримати знання про діяльність своїх конкурентів, тоді як спецслужби та служби безпеки прагнуть розкрити секрети своїх суперників. Будь-яке питання кібербезпеки пов'язане з новими технологіями створення, тиражування, передачі, зберігання інформації, має бути врегульовано відповідно до глобальних стандартів.

Простота, легкість, анонімність, доступність та економія часу – це основні переваги, які роблять інформаційні технології привабливими для людства. Безперечно, вони не могли не привернути увагу осіб, які займаються незаконною діяльністю. Збільшення кількості кіберзлочинів, постійне вдосконалення інформаційних технологій і, як наслідок, нові вдосконалені інструменти їх вчинення, створюють економічні загрози, супроводжуються втратами для глобальних інформаційних мереж та суспільства в цілому. Це зростання також є неминучим процесом, оскільки законодавче регулювання відносин у сфері інформаційних технологій не може ні випереджати їх розвиток, ні йти в ногу з ними. Погоджуємось з точкою зору авторів, які вважають, що подолання кіберзлочинності у суспільстві є основоположним фактором на шляху входження країни (конкретно України) у світовий інформаційний простір [8; с. 5].

До зловмисників, які стоять за кіберінцидентами, відносять держави, групи держав, бізнес та фізичні особи, які переслідують різні цілі. У таблиці 1 наведена класифікація кіберзлочинів за зловмисниками, їх намірами та цілями.

Таблиця 1.
Класифікації злочинів за зловмисниками, їх цілями та намірами [9]

Зловмисник	Наміри	Мета	Приклад
Держави, групи, спонсоровані державами	Геополітичні, ідеологічні	Дестабілізація, руйнування, заподіяння шкоди, крадіжка, шпигунство, фінансовий зиск	Незворотне порушення цілісності даних, цілеспрямоване фізичне ушкодження, порушення функціонування енергетичної системи, дезорганізація платіжної системи, шахрайські трансферти, шпигунство
Кіберзлочинці (представники бізнесу, фізичні особи)	Збагачення, економічні	Крадіжка/ фінансова вигода	Крадіжка коштів, шахрайські трансферти, крадіжка облікових даних
Терористичні групи, хактивісти, інсайдерські погрози	Ідеологічні, невдоволення	Дестабілізація	Витоки інформації, наклеп, атаки типу «відмова в обслуговуванні»

Інститут Понемона – провідний світовий центр, який досліджує політику конфіденційності, захисту даних та інформаційну безпеку у світовому господарстві. За даними IBM Security (Інститут Понемона), яка дослідила вартість втрачених даних серед 524 компаній та організацій й опитала понад 3200 респондентів з цих компаній у 17 країнах та регіонах світу, найбільша кількість кіберінцидентів у 2020 р. була зафіксована у США (63 інциденти). Топ-10 країн світу за кількістю кібератак та втратами даних у них наведений у таблиці 2.

Таблиця 2.
Топ-15 країн (регіонів світу) за кількістю кіберінцидентів у 2020 р. *

Країна / регіон	Кількість випадків, %	Середня загальна вартість втрачених даних, млн дол. США	Причини втрати даних, %		
			Зловмисна атака	Системний збій	Людська помилка
США	12	8,64	54	22	24
Індія	9	2,00	53	26	21
Великобританія	8	3,90	52	23	25
Німеччина	7	4,45	57	24	19
Франція	7	4,01	55	24	21
Японія	6	4,19	51	26	23
Середній Схід	6	6,52	59	24	17
Канада	5	4,50	42	35	23
Південна Корея	5	3,12	50	29	21
АСЕАН	4	2,71	48	22	30
Австралія	4	2,15	57	22	21
Скандинавія	4	2,51	48	30	22
Італія	4	3,19	52	19	29
Латинська Америка	4	1,68	56	26	18
Туреччина	4	1,77	50	25	25

*складено авторами за [3, с. 15, 23, 33]

Об'єктами для кібератак виступали першочергово розвинені країни світу (США, країни Європи та Сходу). На країни Азії хакерські напади були не такими частими (за виключенням Індії) та приводили до менших фінансових втрат.

Сфери, які зберігають цінну інформацію, такі як охорона здоров'я та фінанси, були найбільшою мішенню для хакерів, які хочуть вкрати номери карток соціального страхування, медичні записи та інші особисті дані. Вартість втрачених даних у медичній галузі у 2020 р. становила 7,13 млн дол. США, що на 10%

перевищило суму попереднього року (рис. 1), натомість середня вартість втрачених даних становила 3,86 млн дол. США.

Рисунок 1. Середня вартість втрачених даних від кіберінцидентів за сферами економіки (у млн дол. США) [3; с. 25]

Як видно з рис. 1, вартість втрачених даних в результаті кіберзлочинів у сферах охорони здоров'я, енергетики, фінансових послуг та фармацевтики була значно вищою, ніж у таких галузях, таких як готельна справа, медія та наукові дослідження. Організації державного сектору традиційно мають найнижчу вартість злому даних, оскільки вони не стикаються з проблемою втрати клієнтів у результаті кіберінцидентів. Протягом 2017-2020 рр. у понад 93% медичних організаціях відбувся злам баз даних. У галузі фінансових послуг було знайдено 352 771 конфіденційних файлів, які з'явилися у відкритому доступі. У сфері охорони здоров'я, фармацевтики та біотехнологій таких файлів було виявлено 113 491 [11; с. 20]. За даними Банку міжнародних розрахунків у 2020 р. фінансовий сектор посідає друге місце за кількістю кібератак, поступаючись лише сфері охорони здоров'я.

Провідні ризики кібератак пов'язані з фінансовою дестабілізацією у світі, причому питання стоїть не в тому «чи буде атака?», а «коли буде зроблена атака?». У квітні 2020 р. Рада фінансової стабільності МВФ застерігала про те, що «великий кіберінцидент, якщо він не буде належним чином стриманий, може серйозно порушити функціонування фінансових систем, у тому числі критично важливої фінансової інфраструктури, та спричинити масштабні наслідки для фінансової стабільності» [9; с. 25]. Потенційні економічні витрати суб'єктів міжнародних економічних відносин на кібербезпеку можуть бути великими, а збитки, завдані довірі та впевненості громадськості, – значними. Цей ризик посилюється двома тенденціями. По-перше, глобальна фінансова система зазнає безпрецедентних цифрових трансформацій, які прискорюються пандемією COVID-19. Банки конкурують з компаніями галузі інформаційних технологій (ІТ) та навпаки. У той же час, пандемія збільшила попит на фінансові послуги у режимі онлайн та зробила віддалену роботу нормою. Центральні банки країн у всьому світі повністю чи частково підтримують цифрові валюти та модернізацію платіжних систем. За принципом доміно один кіберінцидент може легко підірвати довіру, звести нанівець інновації у фінансовій сфері, роль кібербезпеки у фінансових установах постійно зростає. По-друге, зловмисники використовують цифровізацію задля «розхитування фінансової стабільності та цілісності» фінансової системи.

Провідними причинами кіберінцидентів виступали зловмисна атака, людська помилка та системний збій. Дані табл. 2 вказують на різне співвідношення причин серед країн світового господарства. Кожен другий інцидент розглядався як зловмисна атака, майже кожен четвертий – як системний збій, кожен п'ятий – як людська помилка. За результатами опитування IBM 52% кіберінцидентів у 2020 р. були кібератаками. Зміна середньої вартості втрати даних від кіберінцидентів за причинами наведена на рис. 2.

Протягом 2019 р. вартість втрачених даних від кіберзлочинів зросла за всіма причинами. На кінець 2020 р. з причини зловмисної атаки даних було втрачено на 4,27 млн дол. США, втрати від системних збоїв та людської помилки становили 3,38 та 3,33 млн дол США відповідно. Співвідношення вартості втрачених даних за причинами втрат залишилось незмінним.

Рисунок 2. Зміна середньої загальної вартості втрати даних за причинами кіберінцидентів у світі у період 2016-2020 рр. (у млн дол. США) [3; с. 32]

За оцінками М. Кукієра, асистента професора машинобудування школи Кларк і філією Центру ризиків і надійності школи Кларк та Інституту системних досліджень, хакери атакують кожні 39 секунди, що складає у середньому близько 2244 рази на день [12].

Згідно зі звітом Risk Based Security (RBS), світового лідера у сфері аналізу даних про кіберзлочини та вразливості, у третьому кварталі 2020 р. кількість втрачених чи скомпрометованих записів була безпрецедентно високою. Динаміка втрачених записів наведена на рис. 3.

Рисунок 3. Кількість втрачених записів, про які повідомлялося в третьому кварталі у період 2017-2020 рр. (млн) [13; с. 10]

Тільки за третій квартал 2020 р. додатково з'явилося 8,3 мільярда записів, за три квартали року кількість таких записів досягла 36 мільярдів. Оцінки свідчать, що найбільше даних втрачено / зіпсовано за рахунок зломів (хакерських атак), нерозкритих причин, вірусних програм та на веб-сторінках (найменше). Постачальники інформаційних технологій та ресурсів за ймовірністю втрати даних розподілялись наступним чином: Dell (найвища), Intel, Microsoft, Google (найнижча) [14].

Все більше суб'єктів світового господарства серйозно ставляться до питань кібербезпеки та нараховують бюджети для її забезпечення. Динаміка витрат для протидії кібератакам у США наведена на рис.4.

Рисунок 4. Динаміка витрат на кібербезпеку в США протягом 2010-2018 рр., (у млрд дол. США)

Саме США несуть найбільші збитки від кіберзлочинів, їх втрати від злому баз даних становили 8,64 млн дол. США у 2020 р., країн Близького Сходу – 6,52 млн дол США. Витрати на протидію кіберзлочинам у США протягом 2010-2018 рр. зросли до 66 млн дол. США або у 2,4 рази порівняно з 2010 р. IBM Security зазначають, що середній загальний бюджет на кібербезпеку зріс у 12 з 16 країн або регіонів, де проводились дослідження як у 2019 р., так і в 2020 р., причому найбільше зростання відбулося у Бразилії – на 29% [3; с. 12].

У сфері міжнародної інформаційної безпеки досі не сформований універсальний міжнародний договір, який би визначав права, обов'язки та механізм суб'єктів міжнародних економічних відносин з питань кібербезпеки. Проте, склався комплекс норм soft law, закріплений у резолюціях ГА ООН, які дозволяють визначити риси, окреслити контури, а у певних випадках і елементи майбутнього механізму міжнародно-правового регулювання міжнародної інформаційної безпеки [7]. Задля протидії кіберзлочинності компанії та держави дотримуються двох головних орієнтирів – нормативно-правових правил, сформованих у міжнародних інститутах та державах, та запроваджують кращі практики кібербезпеки.

Міжнародне бачення проблем майбутнього інституту інформаційної безпеки відображено в резолюціях ООН [17]. Генеральна Асамблея ООН відзначила, що ефективність кібербезпеки залежить не тільки від дій державних або правоохоронних органів, а й повинна досягатися превентивними заходами і мати підтримку в усьому суспільстві. Її не можна забезпечити за допомогою однієї тільки технології, плануванням і управлінням кібербезпекою, її забезпеченням у всьому суспільстві має бути пріоритетним завданням.

Починаючи з 2000 р., прийняті найважливіші міжнародні правові акти, передусім Окінавська хартія глобального інформаційного суспільства. Підсумкові документи Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства в грудні 2003 р. в Женеві та в листопаді 2005 р. в Тунісі, спрямовані на прискорення формування постіндустріальних тенденцій в економічній, соціально-політичній і духовній сферах життя суспільства. Декларація принципів із питань інформаційного суспільства, прийнята в Женеві в 2003 р., проголосила побудову інформаційного суспільства глобальним завданням у новому тисячолітті і визначила ключову роль принципу забезпечення підвищення довіри і безпеки під час використання інформаційних технологій [16; с. 165].

Міжнародна політика кібербезпеки включає в себе: взаємодію суб'єктів (держав, компаній) для боротьби із кіберзлочинністю, участь у міжнародних організаціях, що сприяє цій взаємодії. Серед міжнародних та регіональних організацій слід вказати наступні:

1. ООН. Регулятивна діяльність ООН у сфері кібербезпеки полягає в ухваленні резолюцій, наприклад, «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» (2019), в якій підтверджується необхідність створення мирного інформаційного середовища, розширення можливостей держав щодо співпраці і заохочення використання високих технологій, що сприятимуть зменшенню ризику виникнення конфліктів, і яка є суттєво важливою для забезпечення міжнародної безпеки [17];

2. НАТО. НАТО визначила кібербезпеку як один з пріоритетів діяльності. Організація заснувала передові центри у країнах-членах як багатонаціональні інститути для розробки доктрини кібербезпеки,

вдосконалення міждержавної взаємодії, обміну досвідом кіберзахисту фахівців. Наразі Центр кібербезпеки НАТО функціонує в Естонії [18];

3. ОБСЄ. В ОБСЄ було сформульовано основні напрямки роботи у сфері інформаційної безпеки: розробка теоретичної бази понять у даній сфері; створення механізмів попередження, виявлення й знешкодження загроз; використання чинних норм міжнародного права; активізація співробітництва; підвищення довіри до мережі Інтернет на основі міжнародного управління нею [19];

4. ОЕСР. Рекомендація ОЕСР 2015 р. щодо управління ризиками цифрової безпеки для економічного та соціального процвітання включає вісім принципів високого рівня для вирішення проблеми цифрової безпеки без перешкоджання економічному та соціальному процвітання [20];

5. ЄС. Діюча директива ЄС про гарантії достатнього рівня кібербезпеки, захисту персональних даних та конфіденційності користувачів певних категорій бездротових пристроїв, які використовують радіотехнології поширюється на таке обладнання [21]:

- пристрої, здатні працювати у мережі – смартфони, планшети, електронні камери; телекомунікаційне обладнання. Через недостатню безпеку такі пристрої створюють ризик того, що треті сторони можуть отримати доступ до особистих даних та поділитися ними, у тому числі з метою шахрайства, або що таке обладнання буде використано для шкоди мережі;

- іграшки та обладнання для догляду за дітьми. Іграшки та радіоняні можуть бути вразливими до загроз кібербезпеці, які відстежують або збирають інформацію про дітей. Таким чином, захист прав дитини є суттєвим елементом цього законодавства;

- пристрої для носіння. Такі пристрої, як розумні годинники та фітнес-трекери, все частіше присутні в нашому житті і збирають біометричні дані.

Серед неурядових організацій питаннями кібербезпеки опікуються:

1. Міжнародний форум управління Інтернетом (Internet Governance Forum – IGF). IGF – глобальна багатостороння платформа, яка сприяє обговоренню питань державної політики, що стосуються Інтернету. На щорічних зборах делегати обговорюють, обмінюються інформацією та діляться передовим досвідом. IGF полегшує загальне розуміння того, як максимізувати використати можливості Інтернету, скоротити ризики та розв'язати проблеми, які виникають [22];

2. Міжнародний альянс із захисту кібербезпеки (International Cyber Security Protection Alliance – ICSPA) був створений, щоб фінансувати, проводити експертизу та надавати допомогу безпосередньо правоохоронним підрозділам з кіберзлочинності на внутрішньому та міжнародному ринках [23];

3. Інтернет-суспільство (Internet society – IS) – глобальна некомерційна організація, яка намагається сприяти довірі до інформаційних технологій: допомагає розвивати мережу Інтернет, щоб уникнути цифрового розриву, виступає за його надійність [24];

Щодо кращих практик, їх список поповнюється щоразу при знаходженні нового вразливого місця в системи залежно від типу кібератаки. Суттєві негативні наслідки несуть кіберзлочини з так званими делікатними файлами (інформацію про кредитну картку, медичні записи, або особисту інформацію, що підпадає під дію нормативних актів, таких як GDPR, HIPAA та PCI). Однією з найбільших проблем сучасної інформаційної безпеки є незахищений або недостатньо захищений обліковий запис працівника-користувача, відсутність постійної ротації паролів. 38% усіх опитаних користувачів мають пароль з безстроковим терміном дії і 61% компаній з чисельністю співробітників / споживачів понад 500, які не змінюють їх [10]. Користувачі з безстроковими паролями дають зловмисникам велике часове вікно, щоб зламати їх за допомогою brute force (викриття паролів шляхом перебору всіх можливих варіантів ключа). У цьому контексті кращими практиками компаній та установ для протидії кіберзлочинам виступають:

- заборона IT-відділом використання паролів, що не мають терміну дії, і встановлення для всіх користувачів терміну дії пароля через певні проміжки часу;
- використання довгого, складного і випадкового ключа, щоб захистити акаунт від атак brute force;
- використання корпоративними менеджерами паролів, двофакторної автентифікації, а також моніторинг та попередження про підозрілі, невдалі спроби входу до облікового запису.

Слід наголосити, що для досягнення кібербезпеки не лише весь світ і регіон має протидіяти кіберзлочинам, а й кожна держава та компанія має впроваджувати власну стратегію, вживати конкретних дій та заходів. Так, сучасна Стратегія кібербезпеки Фінляндії, прийнята у жовтні 2019 р., базується на таких принципах [25]:

1. Міжнародне співробітництво. Стратегія (Програма розвитку) кібербезпеки покликана вийти за державні кордони, сприяти перерозподілу ресурсів та покращити співпрацю для цілей протидії кіберзлочинам. Таким чином, національна політика буде посилена, з'явиться краще розуміння проєктів кібербезпеки, програм досліджень і розробок;

2. Покращена координація управління кібербезпекою, планування та готовності протидії кіберзлочинам. Для координації питань кібербезпеки буде створена спеціальна посада директора з кібербезпеки у Міністерстві транспорту та зв'язку країни;

3. Технології для забезпечення кіберстійкості. Для протистояння цифровим збоям широкий спектр технологій кіберстійкості доповнений кібергігієною. Національний центр кібербезпеки (NCSC-FI) забезпечує і підтримує сенсорну мережу під назвою HAVARO, об'єднує урядові організації та компанії, які забезпечують

національну безпеку (фінанси, енергетика, логістика, цифровізація). Центр відстежує інтернет-потік даних ключових організацій національних кіберактивів, сповіщає власника мережі, з якої походять оповіщення. Ця послуга є доповненням до власної відповідальності організацій за моніторинг своїх мереж;

4. Культура безпеки як міцна база для технології безпеки. Стійкість до кібератак пов'язана з культурою безпеки, де обізнаність та освіта про неї формує позитивний досвід користувача. Стійкість культури безпеки можлива тільки в тому випадку, коли перевірка безпеки стає активною на етапах проектування, розробки, тестування та впровадження програмного забезпечення, тобто стає невід'ємною частиною процесу його розробки відповідно до концепції DevSecOps;

5. Відокремлені системи. Ізоляція секретної інформації в окремі мережі та системи гарантує, що атака мінімізована і неможлива через мережу Інтернет. Складне шифрування, аутентифікація мереж поєднані з моніторингом та швидким реагуванням забезпечить додатковий рівень захисту інформаційних даних.

Система кібербезпеки Фінляндії побудована таким чином, що у разі кібератаки перше повідомлення про неї надходить або від цільового інтернет-оператора, NCSA-FI, або при обміні даних між службами кіберрозвідки різних країн. Сигнал про атаку може надходити також від незалежного джерела, такого як ЗМІ, хакера або користувача.

Пандемія коронавірусу COVID-19 створила нові виклики для бізнесу, оскільки підприємства прискорюють цифрову трансформацію, а робота з дому стала « новою нормальністю ». Якщо компанії будуть нехтувати ризиками кібербезпеки, це може мати суттєві негативні наслідки для репутації, іміджу, результатів діяльності, їх позицій на ринку. Середній строк виявлення та локалізації кібератаки у 2020 р. становив 280 днів, причому для користувачів хмарних сервісів він скорочується на 77 днів. Економічна складова стратегії кібербезпеки компаній має враховувати прямі та приховані витрати бізнесу на попередження, виявлення, локалізацію, протидію та подолання негативних наслідків кібератак. До прямих витрат компаній можна віднести витрати на технічне розслідування, повідомлення клієнтів, забезпечення подальшого захисту клієнтів, відповідність нормативним вимогам, підтримання зв'язків з громадськістю, гонорари адвоката та судові розгляди, покращення кібербезпеки. Приховані витрати пов'язані зі збільшенням страхового внеску, підвищення вартість залучення боргу, наслідки операційного збою або руйнування виробничої діяльності, втрата цінності відносин із клієнтами, вартість втраченого доходу за контрактом, девальвація торговельної назви/бренду, втрата інтелектуальної власності (ІВ).

Формування міжнародних правових засад, розробка та реалізація міжнародної, національних та корпоративних стратегій кібербезпеки, на нашу думку, має відбуватися паралельно з формуванням глобальної культури кібербезпеки у всіх суб'єктів. Основними елементами цієї культури мають бути [15]: обізнаність (поінформованість) учасників про необхідність безпеки інформаційних систем і мереж і про те, що вони можуть зробити для підвищення безпеки; відповідальність за безпеку інформаційних систем і мереж згідно з роллю кожного з них; вчасне попередження, виявлення та реагування на кіберінциденти; етика учасників; дотримання та гарантування цінностей демократичного суспільства, включаючи свободу обміну думками, ідеями, вільний потік інформації, конфіденційність інформації та комунікації, належний захист інформації особистого характеру, відкритість і гласність; оцінка ризиків, загроз та факторів уразливості кіберзлочинності; проектування, впровадження засобів та управління забезпеченням кібербезпеки; моніторинг та оновлення політики, практики, заходів та процедур відповідно до нових ризиків, загроз та чинників уразливості.

Висновки. Цифровізація суспільства стала справжнім викликом та чинником розвитку світового господарства та його суб'єктів – міжнародних інститутів, держав, корпорацій та звичайних користувачів. Розвиток інформаційних технологій, поширення мережі інтернет, зростання кількості користувачів спричинили як зростання кіберзлочинності так і розвиток технологій та практик, які здатні дати їй відсіч. Поширення бездротових пристроїв з вільним доступом до мережі, хмарних технологій надають нові можливості для кіберзлочинців, формують нові виклики інтернет-спільноти, компаній та міжнародних організацій. Об'єктом вчинення кіберзлочинів залишаються сфери охорони здоров'я, енергетика, фінанси, фармацевтика та технологічна галузь промислово розвинені країни світу, причому, першочергово злочини носять характер кібератак, здійснюються не тільки за економічними, а й за політичними, ідеологічними, терористичними мотивами. Саме країни з високими доходами на душу населення зазнають найбільших збитків та найбільше витрачають на політику кібербезпеки. У період пандемії коронавірусу COVID-19 роботодавці намагаються поліпшити безпеку бізнесу та роботу своїх працівників, що працюють вдома, але людська помилка все ж таки залишається важливою причиною кібернебезпеки.

Перспективи політики кібербезпеки у світовому господарстві будуть пов'язані з запровадженням нових ефективних практик протидії кібератакам, посиленням захисту делікатних даних, розробкою, прийняттям та реалізацією стратегій кібербезпеки учасниками на всіх рівнях. При розробці корпоративних стратегій кібербезпеки бізнесу доцільно враховувати прямі та непрямі витрати, пов'язані з ймовірною втратою даних. Підвищення загальної освіченості користувачів мережі та запровадження принципів глобальної культури зможуть змінити ситуацію на краще.

Список використаних джерел.

1. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: Проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. №1. С.75-86.

2. The Global Risks Report 2021. WEF. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата звернення 10.12.2021)
3. IBM Security. Cost of a Data Breach Report. 2020. URL: <https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf> (дата звернення 10.10.2021)
4. Bronk Ch. Hacking the Nation-State: Security, Information Technology and Policies of Assurance. *Information Security Journal: A Global Perspective*. 2008. Vol.17, № 3. pp.132-142.
5. Creese S., Dutton W. H., Esteve-González P., Shillair R. Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy*. 2021. Vol. 6, №2. pp.214-235.
6. Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / В. М. Болгов, Н. М.Гадіон, О. З. Гладун та ін. К. : Національна академія прокуратури України, 2015. 202 с.
7. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: автореф. дис.... канд. юрид. наук: 12.00.11. Київ, 2009. 19с.
8. Вівчар О., Олінійчук О., Погайдак О. Сучасні тенденції кіберзлочинності в контексті економічної безпеки дослідили. *Вісник Дніпровського університету. Серія «Світове господарство і міжнародні економічні відносини»*. 2017. №9 (25), С. 3-17.
9. Маурер Т., Нельсон А. Глобальная киберугроза. *Финансы и развитие*. 2021. Март. С.24-27.
10. Global Data Risk Report. Varonis. 2019. URL: <https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf>. (дата звернення 01.11.2021)
11. Cybersecurity Statistics for 2021. Varonis blog. URL: <https://www.varonis.com/blog/cybersecurity-statistics/>. (дата звернення 20.12.2021).
12. Study: Hackers Attack Every 39 Seconds [Електронний ресурс]. URL: <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>. (дата звернення 10.11.2021)
13. Risk Based Security. 2020 Q3 Report Data Breach QuickView. 2020. URL: <https://pages.riskbasedsecurity.com/en/en/2020-q3-data-breach-quickview-report-0> (дата звернення 01.12.2021)
14. Data Breach QuickView. 2021. November. URL: <https://www.riskbasedsecurity.com/2021/12/06/data-breach-quickview-november-2021/> (дата звернення 11.01.2022)
15. Створення глобальної культури кібербезпеки. Резолюція ГА ООН №57/239 від 20 грудня 2001 р. URL: <https://undocs.org/ru/A/RES/57/239> (дата звернення 20.12.2021)
16. Полякова Т. А. Информационная безопасность в условиях построения информационного общества. М.: РПА Минюста России, 2007. 165 с.
17. Developments in the field of information and telecommunications in the context of international security. UN Resolution from 12 December 2019. URL: <https://undocs.org/en/A/RES/74/29> (дата звернення 12.11.2021)
18. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: <https://www.cybersecurityintelligence.com/nato-cooperative-cyber-defence-centre-ccdcoe-395.html> (дата звернення 12.11.2021)
19. Organization for Security and Co-operation in Europe – OSCE. URL: <https://www.osce.org/whatistheosce> (дата звернення 12.11.2021)
20. Digital security risk management, OECD. 2015. URL: <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf> (дата звернення 05.11.2021)
21. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance). Consolidated text. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0053-20180911> (дата звернення 17.11.2021)
22. Internet Governance Forum – IGF. URL: <https://www.intgovforum.org/>. (дата звернення 12.11.2021)
23. International Cyber Security Protection Alliance – ICSPA. URL: <https://icspa.org/about-us/>. (дата звернення 12.11.2021)
24. Internet society. URL: <https://www.internetsociety.org/>. (дата звернення 12.11.2021)
25. Finland's cyber security strategy 2019. URL: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf. (дата звернення 12.11.2021)

References.

1. Tkachenko, O. and Tkachenko, K. (2018), "Cyberspace and cybersecurity: Problems, prospects, technologies", *Tsyfrova platforma: informatsiini tekhnologii v sotsiokulturnii sferi*, vol.1, pp.75-86.
2. WEF (2021), "The Global Risks Report", available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (Accessed 10 December 2021)
3. IBM Security (2020), "Cost of a Data Breach Report", available at: <https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf> (Accessed 10 October 2021)

4. Bronk, Ch. (2008), "Hacking the Nation-State: Security, Information Technology and Policies of Assurance", *Information Security Journal: A Global Perspective*, vol.17, no 3, pp. 132-142.
5. Creese, S., Dutton, W. H., Esteve-González, P. and Shillair, R. (2021), "Cybersecurity capacity-building: cross-national benefits and international divides", *Journal of Cyber Policy*, Vol.6, no 2, pp.214-235.
6. Bolgov, V. Gadion, N.M. and Gladun, O.Z. (2015), *Orhanizatsiino-pravove zabezpechennia protydivi kriminalnym pravoporushenniam, shcho vchyniautsia z vykorystanniam informatsiinykh tekhnolohii: nauk.-prakt. posib* [Organizational and legal support of counteraction to criminal offenses committed with the use of information technology], National Academy of the Prosecutor's Office of Ukraine, Kyiv, Ukraine.
7. Shahbazyan, K. S. (2009), "International legal bases of regulation of relations on the Internet", Ph.D. Thesis of law science, Kyiv, Ukraine.
8. Vivchar, O., Oliniitsuk, O. and Pogaidak, O. (2017), "Modern tendencies of cybercrime in the context of economic security have been studied", *Bulletin of Dnipro University. Series. World Economy and International Economic Relations*, vol.9, no 25, pp. 3-17.
9. Maurer, T. and Nelson, A. (2021), "Global Cyrebug Threat", *Finance and development*, March, pp. 24-27.
10. Varonis (2019), "Global Data Risk Report", available at: <https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf>. (Accessed 01 November 2021)
11. Varonis blog (2021), "Cybersecurity Statistics for 2021", available at: <https://www.varonis.com/blog/cybersecurity-statistics/>. (Accessed 20 December 2021).
12. Cukier, M. (2007), "Study: Hackers Attack Every 39 Seconds", available at: <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds> (Accessed 10 November 2021)
13. Risk Based Security (2020), "Q3 Report Data Breach QuickView", available at: <https://pages.riskbasedsecurity.com/en/en/2020-q3-data-breach-quickview-report-0> (accessed 01 December 2021)
14. Risk Based Security (2021), "Data Breach QuickView", available at: <https://www.riskbasedsecurity.com/2021/12/06/data-breach-quickview-november-2021/> (Accessed 11 January 2022)
15. UN General Assembly (2001), Resolution "The creation of a global culture of cybersecurity", available at: <https://undocs.org/ru/A/RES/57/239> (Accessed 20 December 2021)
16. Polyakova, T. A. (2007), *Ynformatsyonnaia bezopasnost v usloviakh postroeniya ynformatsyonnoho obshchestva* [Information security in the context of building an information society], RPA Ministry of Justice of Russia, Moscow, Russia.
17. UN (2019), Resolution "Developments in the field of information and telecommunications in the context of international security", available at: <https://undocs.org/en/A/RES/74/29> (Accessed 12 November 2021)
18. NATO Cooperative Cyber Defence Centre (CCDCOE), (2021), available at: <https://www.cybersecurityintelligence.com/nato-cooperative-cyber-defence-centre-ccdcoe-395.html> (Accessed 12 November 2021)
19. Organization for Security and Co-operation in Europe – OSCE, (2021), available at: <https://www.osce.org/whatistheosce> (Accessed 12 November 2021)
20. OECD (2015), "Digital security risk management", available at: <https://www.oecd.org/digital/ieconomy/digital-security-riskmanagement.pdf> (Accessed 05 November 2021)
21. EU of the European Parliament and of the Council (2014), Directive "2014/53/EU of the European Parliament and of the Council of 16 April on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance). Consolidated text", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L_0053-20180911 (Accessed 17 November 2021)
22. Internet Governance Forum – IGF (2021), available at: <https://www.intgovforum.org/>. (Accessed 12 November 2021)
23. International Cyber Security Protection Alliance – ICSPA (2021), available at: <https://icspa.org/about-us/>. (Accessed 12.11.2021)
24. Internet society (2021), available at: <https://www.internetsociety.org/>. (Accessed 12 November 2021)
25. Turvallisuuskomitea Puolustusministeriö (2019), "Finland's cyber security strategy", available at: https://turvallisuuskomitea.fi/wpcontent/uploads/2019/10/Kyberturvallisuus_strategia_A4_ENG_WEB_031019.pdf (Accessed 12 November 2021).

Стаття надійшла до редакції 20.01.2022 р.