Отримано: 12 лютого 2024 р.

Прорецензовано: 28 лютого 2024 р.

Прийнято до друку: 03 березня 2024 р.

e-mail: a.ostapets@knute.edu.ua

e-mail: i.parasij-vergunenko@knute.edu.ua

ORCID-ідентифікатор: https://orcid.org/0000-0001-6506-6965

DOI: 10.25264/2311-5149-2024-32(60)-37-46

Остапець А. О., Парасій-Вергуненко І. М. Вплив ризику кіберзлочинності на діяльність технологічних підприємств. *Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал.* Острог : Вид-во НаУОА, березень 2024. № 32(60). С. 37–46.

УДК: 316.42:336.71]:338.14=111

JEL-класифікація: M21, M15, M41

Остапець Антон Олександрович,
аспірант кафедри фінансового аналізу та аудиту
Державного торговельно-економічного університету
Парасій-Вергуненко Ірина Михайлівна,
доктор економічних наук, професор, професор кафедри фінансового аналізу та аудиту
Державного торговельно-економічного університету

ВПЛИВ РИЗИКУ КІБЕРЗЛОЧИННОСТІ НА ДІЯЛЬНІСТЬ ТЕХНОЛОГІЧНИХ ПІДПРИЄМСТВ

У статті досліджено питання впливу ризиків кіберзлочинності на діяльність технологічних підприємств. Обґрунтовано доцільність врахування фактору кіберзлочинності як окремого ризику для діяльності технологічних підприємств і необхідність його аналізу та контролю на рівні з іншими ризиками. Розкрито сутність понять «кіберзлочинність» та «кіберзлочин». Проаналізовано вплив ризику кіберзлочинності на діяльність підприємств та доцільність аналізу та контролю наведеного ризику. Запропоновано долучити цей ризик до класифікації ризиків підприємств технологічної галузі, зокрема ІТ. Аналіз проблематики та узагальнення досліджень дали змогу визначити подальший напрям у процесах аналізу та контролю ризиків. Практична цінність статті полягає в тому, що вона знайомить читачів із питанням кіберзлочинності і важливістю аналізу та контролю за ризиками, пов'язаними з нею.

Ключові слова: *кіберзлочин, кіберзлочинність, хакер, ризик, технологічне підприємство, аналіз та контроль ризиків.*

Anton Ostapets,
Postgraduate Student at the Department of Financial Analysis and Audit
State University of Trade and Economics
Iryna Parasii-Verhunenko,
Doctor of Sciences (Economics), Professor, Professor at the Department of Financial Analysis and Audit
State University of Trade and Economics

THE IMPACT OF CYBERCRIME RISK ON TECHNOLOGICAL COMPANIES' ACTIVITIES

The article investigates the impact of cybercrime risks on technological enterprises' operations, highlighting the substantial losses incurred due to cyberattacks on computer systems, infrastructure, and personal data storage. It justifies considering cybercrime as a distinct risk factor and emphasizes the importance of analyzing and controlling this risk alongside others. The concept of «cybercrime» and «cybercriminal» is clarified based on Ukrainian, European, American, and global legislative perspectives. The article discusses how cybercrime risk influences enterprise activities and the relevance of managing this risk within business entities' risk management processes. It suggests integrating this risk into the risk classification of technological enterprises, particularly in the IT sector.

Additionally, the article examines the financial losses incurred by business entities as victims of major cybercrimes and classifies risks associated with cybercrime based on their impact on physical and legal entities. It proposes identifying key types of crimes that can cause significant losses to legal entities. The analysis and synthesis of related research underscore the importance of prioritizing cybercrime risks in the risk management processes of technological enterprises, including those in the IT industry.

The practical value of the article lies in familiarizing readers with cybercrime and its primary types, emphasizing the significance of analyzing and controlling associated risks.

Keywords: *cybercrime, cybercriminal, hacker, risk, technological enterprise, risk analysis and control.*

Постановка проблеми. Останні десятиліття розвитку людства визначаються значною цифровізацією усіх галузей суспільного життя і використанням сучасних цифрових технологій у веденні бізнесу та

повсякденні. Особливим драйвером використання цифрових технологій стала пандемія COVID-19 та повномасштабне військове вторгнення на територію нашої держави рф. Саме ці події послужили значним імпульсом використання цифрових технологій у галузі освіти, охорони здоров'я, системи розрахунків тощо. Багато компаній, які до початку вищезазначених подій не приділяли достатньої уваги питанням цифровізації бізнесу, зазнали значних збитків внаслідок неврахування причин необхідності впровадження негайних змін в своїх моделях ведення бізнесу. На поточний момент у всьому світі спостерігаються подальші процеси цифровізації всіх галузей життя, набувають все більшого розвитку такі галузі, як bigdata-аналітика, штучний інтелект тощо. Стратегією нашої держави передбачається подальша цифровізація процесів взаємодії з органами влади, галуззю освіти, охорони здоров'я, надання адміністративних послуг тощо. Всі ці процеси вимагають використання різноманітних програмних продуктів та зберігання великих масивів даних, що можуть викликати зацікавленість серед зловмисників, які засобами цифрового впливу можуть отримати несанкціонований доступ до персональних даних, використовувати їх для здійснення незаконних операцій з грошовими засобами, втручатись або ж повністю блокувати діяльність підприємств чи нанести непоправних втрат останнім. Враховуючи все вищезазначене, набуває актуальності питання впливу кіберзлочинності на діяльність підприємств та аналізу ризиків, пов'язаних з нею, та впровадження засобів протидії кіберзлочинам.

Аналіз останніх досліджень і публікацій. У світлі постійної цифровізації суспільства та всебічного використання засобів цифрових технологій, наведена тематика набуває все більшої значущості і привертає увагу закордонних та українських науковців. Питання класифікації кіберзлочинів, їх правової природи та засобів протидії досліджено такими українськими науковцями: В. Г. Кундеусом, В. В. Шемчук, М. В. Гребенюк, А. М. Черняк та М. І. Саєнко [1–4]. Окремі аспекти впливу на економіку та фінансову систему досліджено в роботах В. В. Боженко, В. В. Кайбічук, О. В. Дзяд та П. І. Пушкаренко [5–7]. Питання страхування ризиків, пов'язаних з кібербезпекою, розглянуто в роботах І. В. Ксьонжик, Н. А. Жовтої та А. І. Павліної [8]. Попри вагомість вкладу зазначених науковців в наведену проблематику, аналіз ризиків кібернебезпеки та їх вплив на економічну діяльність підприємств потребують подальшого дослідження та аналізу, оскільки з кожним днем з'являються нові види кіберзлочинів і масштаб потенційних збитків від них суттєво зростає.

Мета і завдання дослідження: розкрити поняття «кіберзлочинність» та провести аналіз її впливу на економічну діяльність закордонних та українських технологічних підприємств.

Виклад основного матеріалу дослідження. На тлі останніх світових подій і подальшого зростання рівня діджиталізації та використання цифрових технологій в різних сферах життя та бізнесу, а також появи таких понять, як війни у кіберпросторі, питання кіберзлочинності стає все більш актуальним, оскільки підприємства можуть зазнавати критичних збитків у випадку здійснення кіберзлочинів по відношенню до них.

Європейська комісія визначає поняття кіберзлочину як злочинні дії, вчинені в режимі онлайн з використанням електронних комунікаційних мереж та інформаційних систем [9]. Також Європейська комісія визначає кіберзлочинність як проблему безкордонного характеру і розподіляє кіберзлочини на такі категорії:

– злочини, специфічні для інтернету, як-от: атаки на інформаційні системи чи фішинг (наприклад, створення фальшивих веб-сайтів банків для збирання паролів та отримання доступу до банківських рахунків жертв);

– онлайн-шахрайство та фальсифікація: масштабне шахрайство, що може бути скоєне в інтернеті за допомогою таких інструментів: крадіжка ідентичності, фішинг, розсилання спаму та шкідливого коду;

– незаконний контент в інтернеті, зокрема матеріали з дитячою сексуальною експлуатацією, заклики до расової ненависті, заклики до терористичних актів і прославлення насильства, тероризму, расизму та ксенофобії.

У міжнародних документах поняттями «кіберзлочини», «кіберзлочинність» охоплюються різні види правопорушень. У п. 9 Доповіді Комітету II Десятого Конгресу ООН 2000 р. по попередженню злочинності і поводженню з правопорушниками було дано таке визначення поняттю «кіберзлочин» – злочин, який може бути скоєний за допомогою комп'ютерної системи чи мережі, у комп'ютерній системі чи мережі або проти комп'ютерної системи чи мережі [10]. В принципі, поняття кіберзлочину охоплює будь-який злочин, який можна вчинити в електронному середовищі. Також у п. 14 поняття «кіберзлочин» поділяють на дві категорії:

– кіберзлочин у вузькому сенсі («комп'ютерний злочин»): будь-яка незаконна поведінка, здійснена за допомогою електронних операцій, спрямована на безпеку комп'ютерних систем і даних, які ними обробляються;

– кіберзлочин у ширшому розумінні («злочини, пов'язані з використанням комп'ютерів»): будь-яка незаконна поведінка, вчинена за допомогою комп'ютерної системи або мережі або стосовно них, зокрема

такі злочини, як незаконне зберігання, пропозиція та розповсюдження інформації за допомогою комп'ютера, системи або мережі.

У п. 15 вищезазначеного документу зазначається, що кіберзлочинність стосується будь-якої незаконної поведінки, спрямованої проти безпеки системи та даних за допомогою електронних операцій. Комп'ютерні системи та безпеку даних можна описати трьома принципами: забезпечення конфіденційності, цілісності або доступності даних і функцій обробки. Згідно зі списком Організації економічного співробітництва та розвитку 1985 р. та більш детальною Рекомендацією Ради Європи 1989 р., порушення конфіденційності, цілісності та доступності охоплюють:

– несанкціонований доступ, тобто доступ без прав до комп'ютерної системи чи мережі з порушенням заходів безпеки;

– пошкодження комп'ютерних даних або комп'ютерних програм, що означає стирання, пошкодження, погіршення чи приховування комп'ютерних даних або комп'ютерних програм без права;

– комп'ютерний саботаж, що означає введення, зміну, видалення або придушення комп'ютерних даних чи комп'ютерних програм або втручання в комп'ютерні системи з наміром перешкодити функціонуванню комп'ютера чи телекомунікаційної системи;

– несанкціоноване перехоплення, що означає перехоплення, здійснене без дозволу та за допомогою технічних засобів, комунікацій до комп'ютерної системи чи мережі, з них та всередині них;

– комп'ютерне шпигунство, що означає придбання, розголошення, передачу або використання комерційної таємниці без дозволу чи законного обґрунтування з наміром завдати економічних збитків особі, яка має право на таємницю, або отримати незаконну вигоду для себе чи третьої особи.

В Україні питання кібербезпеки регламентується Законом України від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України», в якому, зокрема, дається таке визначення поняттю «кіберзлочин»: суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [11].

Основні кіберзлочини і їх фінансовий вплив наведені в табл. 1.

Таблиця 1

Основні види кіберзлочинів і їх фінансові наслідки

Злочин	Фінансові наслідки
Вимагання викупу	Такий вид кіберзлочину передбачає шифрування даних жертви та вимагання викупу за їх розблокування. Фінансові наслідки можуть коливатися від тисяч до мільйонів доларів, враховуючи вартість викупу, витрати на відновлення даних та період простою
Компрометація бізнес-пошти (BEC)	BEC передбачає компрометацію бізнес-поштових облікових записів для здійснення шахрайських транзакцій або отримання доступу до конфіденційної інформації. Фінансові збитки можуть бути значними, часто включаючи шахрайство з переказами, із втратами, які сягають мільйонів доларів
Витік даних	Витік даних може призвести до розголошення конфіденційної інформації, що призводить до фінансових втрат через штрафи за порушення регуляторних вимог, витрати на юридичне обслуговування, витрати на оповіщення та погіршення репутації організації
Шахрайство з платіжними картками	Злочинці можуть вкрасти інформацію стосовно кредитних карток для несанкціонованих транзакцій, що призводить до фінансових втрат як для фізичних осіб, так і для підприємств. Витрати включають в себе вартість відшкодування, заходи з виявлення/попередження шахрайства та шкоду репутації
Крадіжка особистості	Крадіжка особистості може призвести до фінансових втрат для осіб через використання вкрадених ідентифікаційних даних для шахрайських дій, таких як відкриття банківських рахунків, отримання кредитів або здійснення несанкціонованих покупок
Фішингові атаки	Фішинг передбачає обман осіб з метою отримання конфіденційної інформації. Фінансові втрати можуть виникнути через крадіжку облікових даних, несанкціонований доступ та можливі шахрайські дії проти осіб та організацій
Атаки шкідливих програм	Зараження програмами може призвести до витрат через крадіжку даних, знищення інформації та витрати на відновлення систем і впровадження заходів кібербезпеки
Шахрайство в інтернет-банкінгу	Злочинці можуть використовувати різні методи для отримання несанкціонованого доступу до інтернет-банкінгу та рахунків, що призводить до фінансових втрат для осіб та банків. Це може включати несанкціоновані перекази, захоплення рахунків та шахрайські транзакції
Криптовалютний джекінг	Криптовалютний джекінг передбачає несанкціоноване використання ресурсів комп'ютера для видобутку криптовалюти. Фінансові наслідки включають в себе зростання витрат на енергію, погіршення роботи систем та можливе пошкодження обладнання
Крадіжка інтелектуальної власності	Крадіжка інтелектуальної власності, включаючи патенти, торгові секрети та конфіденційну інформацію, може призвести до значних фінансових втрат для підприємств через втрату конкурентної переваги та можливі правові дії по відношенню до них

Джерело: складено та систематизовано авторами на основі [12].

Враховуючи вищенаведені види кіберзлочинів, є доцільним розглянути вплив кожного з них на діяльність підприємств. Злочини, пов'язані з вимаганням викупу за вкрадені дані, набувають все більшого поширення в світі. За даними звіту компанії Sophos, яка займається питаннями кібербезпеки, у 2023 р. відбулось значне зростання кількості кібератак на підприємства фінансової галузі [13]. Відповідно до проведеного опитування, 64 % компаній зазнали впливу цього виду злочину, що на 9 % більше порівняно з 2022 р. і майже вдвічі вище за рівень 2021 р. (34 %). Також варто зазначити, що, окрім компаній фінансового сектору, 66 % респондентів, що належать до усіх галузей виробництва та суспільного життя, доповіли про те, що зазнали атак на дані їх компаній з вимогою викупу. Найбільшій кількості атак підлягли галузь вищої освіти (79 %), будівництва (71 %), федеральні урядові організації (70 %), мас-медіа та сфера розваг (70 %), місцеві урядові організації (69 %) та рітейлери (69 %). У 43 % випадків організації фінансового сектору надають перевагу виплаті викупу за повернення даних, що на 3 % менше середнього показника по всіх галузях. За даними дослідження, проведеного Sophos, середня сума виплати серед фінансових організацій становила 1,6 млн дол. США у 2023 р., що майже у шість разів вище за показник 2022 р. і на 100 тис. дол. США вище за середньостатистичну суму по всіх галузях. Середня кількість витрат фінансових організацій, необхідних для повного відновлення від злочину, склала 2,23 млн дол. США. Витрати на повне відновлення після атак в організаціях, що мала система резервування та відновлення даних, в середньому склали 375 тис. дол. США, а в організацій, що погодились на сплату викупу, середній показник склав 3 млн дол. Здебільшого організації не розповсюджують інформацію про атаки з вимогою викупу. Серед прикладів технологічних компаній, що зазнали подібних атак у минулі роки, варто зазначити такі: HTC Global Services, Cloud Nordic, Reddit, Nvidia, Cisco, Acer, Quanta Computer.

Наступним поширеним кіберзлочином є компрометація електронної пошти. За даними звіту Центру скарг щодо інтернет-злочинності Федерального Бюро Розслідувань Сполучених Штатів Америки, втрати від цього виду цього виду злочину склали 43 млрд дол. США. Такий вид шахрайства було зареєстровано в усіх штатах США і 177 країнах, при цьому понад 140 країн отримували шахрайські перекази [14]. Основними пунктами призначення шахрайських коштів були банки в Тайланді, Гонконзі, КНР, Мексиці та Сінгапурі. Відповідно до даних звіту, за період з червня 2016 р. по грудень 2021 р. було зареєстровано 241 206 внутрішніх та міжнародних інцидентів, загальна сума збитків від яких сягнула позначки в 43,3 млрд дол. США. Статистика скарг потерпілих за період з жовтня 2013 р. по грудень 2021 р. свідчить про понад 116 тис. потерпілих в США і 5,3 тис. потерпілих поза США, які зазнали загальної суми збитків в 16 млрд дол. США. Серед найбільших злочинів по відношенню до технологічних компаній варто відзначити випадок, що стався в проміжку між 2013 р. та 2015 р., жертвами якого стали технологічні гіганти Google та Facebook. Загальна сума втрат від злочину склала понад 120 млн дол. США [15]. Також у 2015 р. жертвою злочинців стала IT-компанія Uniquiti, яка зазнала збитків в розмірі 46,7 млн дол. США [16], а у 2019 р. жертвою шахраїв стала японська компанія Toyota, яка зазнала збитків у розмірі 37 млн дол. США [17].

Втрати, які отримують компанії у разі витоку даних, здебільшого пов'язані зі штрафами, накладеними на них регуляторами різних країн. Найбільшого штрафу за виток даних зазнала китайська прокатна компанія Didi Global за порушення закону про безпеку даних та закону про захист особистої інформації. Загальна сума накладеного штрафу склала 1,19 млрд дол. США. Серед технологічних гігантів найбільших збитків зазнали компанії Amazon (штраф у розмірі 877 млн дол. США від влади Люксембургу за порушення умов GDPR влітку 2021 р.), Instagram (штраф у розмірі 403 млн дол. США від Комісії з захисту даних Ірландії за порушення умов GDPR стосовно конфіденційності особистих даних неповнолітніх у вересні 2022 р.), Tiktok (штраф у розмірі 370 млн дол. США від Комісії з захисту даних Ірландії за порушення умов GDPR стосовно конфіденційності особистих даних неповнолітніх у вересні 2023 р.), T-Mobile (компенсація в розмірі з 350 млн дол. США постраждалим від витоку інформації за умовами мирової угоди в липні 2022 р. та зобов'язання інвестувати 150 млн дол. США в засоби безпеки даних та відповідні технології протягом 2022–2023 рр.), Meta (Facebook) (штраф у розмірі 277 млн дол. США від Комісії з захисту даних Ірландії за невідповідність до умов GDPR, спричинену компрометацією особистих даних 500 млн користувачів мережі у вересні 2022 р.), Whatsapp (штраф у розмірі 255 млн дол. США від Комісії з захисту даних Ірландії за порушення правил GDPR в серпні 2021 р.) [18].

Наступним видом кіберзлочину є шахрайство з платіжними картами. Останнім часом в нашій державі цей вид кіберзлочину набуває все більшого поширення. В той же час, Європейський Центральний Банк у своєму звіті про шахрайство з платіжними картами повідомляє про тенденцію до зниження кількості подібних злочинів у 2021 р. порівняно з минулими роками. Зокрема, загальні втрати від шахрайства по картках, виданих в країнах ЄС, склали 1,2 млрд євро, що на 12 % менше ніж за 2020 р. В той же час,

такий вид шахрайства є найбільш розповсюдженим серед злочинів, пов'язаних з використанням кредитних карток і складає 87 % випадків [19].

Крадіжка особистості є видом кіберзлочину, який здебільшого стосується фізичних осіб, а не організацій, оскільки жертвами здебільшого є персональні дані. На організації може здійснюватися вплив у репутаційній площині. Серед найбільших злочинів, пов'язаних з крадіжкою особистості, були справа Філіпа Каммінгса, Абрахама Абдали та Амара Сінгха. У 2001 р. Філіп Каммінгс, співробітник служби підтримки американської ІТ-компанії, здійснив крадіжку понад 33 тис. кредитних звітів з метою перепродажу їх шахраям за суму в 30 дол. США за кожен запис. В результаті неправомірних дій шахраїв, понад 30 тис. громадян США зазнали сумарних втрат від 50 до 100 млн дол. США. Абрахам Абдала протягом півроку мав доступ до брокерських рахунків та номерів кредитних карт. За цей час потенційними постраждалими від його оборудки могли стати 217 осіб, серед яких такі відомі особистості: Уорен Баффет, Опра Уінфрі та Стівен Спілберг – і зазнати сумарних втрат у 22 млн дол. США, однак злочинця було вчасно заарештовано і він не зміг провести фінансові операції. Амар Сінгх і його дружина Нехі Пунджані-Сінгх використовували RFID-сканери для отримання інформації про кредитні картки споживачів у закладах роздрібної торгівлі чи харчування, а також на незаконних веб-сайтах. Отримані з оборудок кошти використовувались для купівлі товарів у Apple та Bestbuy, з подальшим їх перепродажем. До моменту затримання в жовтні 2011 р., злочинці назбирали 14 млн дол. у вигляді викрадених грошей [20].

Останнім часом серйозного поширення набув такий вид кіберзлочину, як фішингові атаки. Найбільш серйозною фішинговою атакою була NotPetya, що мала місце у червні 2017 р. Спочатку NotPetya розпочався як атака на ланцюг поставок на українські компанії через оновлення від невеликої української компанії, що займається бухгалтерським програмним забезпеченням. Однак він швидко поширився на понад 60 країн, вразивши комп'ютерні системи тисяч транснаціональних компаній. Зловмисне програмне забезпечення здійснювало шифрування даних на ПК з подальшої можливістю відновити доступ до них після сплати певної суми коштів. В пастку атаки NotPetya потрапило багато міжнародних компаній, включаючи Maersk, фармацевтичного гіганта Merck, європейську дочірню компанію FedEx TNT Express, Saint-Gobain, Mondelez і Reckitt Benckiser. Грошовий збиток, завданий шкідливим програмним забезпеченням, оцінюється у понад 10 млрд дол. США – це найзначніші збитки в історії кібератак. Також серед прикладів впливу фішингу можна зазначити подію, що мала місце у грудні 2015 р. в Україні, коли шляхом фішингової атаки зловмисники отримали доступ до управління енергомережою компаній «Київобленерго», «Чернівціобленерго» та «Прикарпаттяобленерго», результатом чого стало відключення електроенергії у понад 225 тис. споживачів Київської, Чернівецької та Івано-Франківської областей протягом декількох годин [21].

Наступним видом кіберзлочину є атака ПК шкідливими програмами. Такий вид злочину все ще є розповсюдженим, незважаючи на сучасні заходи протидії. До останніх прикладів подібних атак належать такі: Emotet Trojan, CovidLock, атаки на Colonial Pipeline, Microsoft Exchange Server та технологічного гіганта NVIDIA [22]. Одним із найвідоміших прикладів зловмисного програмного забезпечення за останні роки є троян Emotet. Ця надзвичайно складна форма зловмисного програмного забезпечення спочатку з'явилася приблизно у 2014 р. як банківський троян, призначений для викрадення фінансових даних. Проте з роками він перетворився на більш універсальну загрозу. Основним способом роботи Emotet є надсилання фішингових електронних листів жертвам. Ці електронні листи зазвичай містять зловмисне вкладення або посилання, яке під час відкриття дозволяє зловмисному програмному забезпеченню проникнути в систему жертви. Потрапивши всередину, Emotet може спричинити різноманітні проблеми: від крадіжки конфіденційної інформації до пошкодження програмного забезпечення. За звітом Американської Агенції Кібербезпеки, відновлення після кожного інциденту, пов'язаною з атакою Emotet, коштувало місцевим урядовим організаціям в середньому 1 млн дол. США [23]. CovidLock є ще одним прикладом злоякісного програмного забезпечення, яке було поширене під час пандемії COVID-19 і представляло собою додаток, який був схожий на той, що був запропонований урядами різних країн з метою відстежування пересування осіб підчас карантинного режиму. Після встановлення додатку користувачі отримували повідомлення з вимогою сплатити 100 дол. США у біткоїнах на рахунок шахраїв для відновлення доступу для пристрою. Здебільшого від CovidLock постраждали користувачі платформи Android [24]. У травні 2021 р. група програм-вимагачів, відома як DarkSide, здійснила атаку на компанію Colonial Pipeline, один із найбільших паливних трубопроводів у Сполучених Штатах. Результатом атаки була зупинка газопроводу на кілька днів, внаслідок чого виникли масовий дефіцит палива і зростання цін на нього. Компанія була вимушена сплатити викуп у розмірі приблизно 4,4 млн дол., щоб відновити контроль над своїми системами.

На початку 2021 р. корпорація Майкрософт повідомила, що виявила атаку шкідливого програмного забезпечення, що використовувалось для нанесення шкоди локальним версіям Microsoft Exchange

Server. Зловмисник, якого Microsoft вважає групою під назвою Hafnium, зміг отримати доступ до облікових записів електронної пошти та встановити додаткове шкідливе програмне забезпечення для тривалого доступу до середовища жертви. Атака торкнулася десятків тисяч організацій по всьому світу, що підкреслює потенційний масштаб таких загроз кібербезпеці. У лютому 2022 р. – провідний розробник графічних процесорів, американська компанія NVIDIA. Атака, яка, ймовірно, була здійснена групою програм-вимагачів, призвела до крадіжки конфіденційної інформації та спричинила значний збій у роботі компанії.

Ще одним видом кіберзлочинності є злочини, здійснені шляхом отримання доступу до сервісів інтернет-банкінгу. Цей тип шахрайства відбувається, коли шахрай отримує доступ до рахунку банку жертви через інтернет-банкінг з використанням скомпрометованих особистих даних та паролів та здійснює несанкціонований переказ грошей. Згідно до звіту організації UK Finance, за період з 2018 по 2022 рр. було зафіксовано понад 285 тис. випадків такого виду злочину, а загальні втрати склали понад 860 млн фунтів [25]. Варто зазначити, що жертвами цього виду злочину можуть стати як фізичні, так і юридичні особи.

Відносно новим видом кіберзлочину є криптовалютний джекінг, сутність якого полягає в тому, що зловмисники вдаються до дистанційного злому серверів і пристроїв різноманітних організацій та використовують їх ресурси шляхом встановлення шкідливого програмного забезпечення, що змушує обладнання майнити криптовалюти та біткойни без відома власників. За звітом провідної американської компанії зі сфери кібербезпеки SonicWall, останніми роками відбувається значне зростання випадків криптоджекінгу. За перше півріччя зафіксовано понад 330 млн випадків криптоджекінгу, що 2,4 рази більше за увесь 2022 р. і спостерігається подальша тенденція до зростання. Найбільша кількість випадків зафіксована в Сполучених Штатах Америки, Данії, Німеччині, Франції та Об'єднаних Арабських Еміратах [26]. На жаль, нині питання оцінки збитків від цього виду злочину є досить складним, оскільки у корпоративному середовищі ефект може бути посилений, якщо для криптоджекінгу використовуються кілька пристроїв одночасно. Головним чином, захоплення контролю за обладнанням з метою майнингу криптовалют може призвести до серйозних втрат продуктивності обладнання, потенційних втрат та витоків інформації і відповідних фінансових наслідків. Крім того, компанії можуть понести додаткові витрати на вирішення проблем безпеки та відновлення нормальної роботи обладнання.

Останнім, але не менш значущим видом кіберзлочину є крадіжка інтелектуальної власності. Інтелектуальна власність є джерелом життя будь-якої сучасної економіки, за даними Бюро патентів і товарних знаків Сполучених Штатів, станом на 2019 р. на інтелектуальну власність припадає понад 7 трлн дол. ВВП США, тому крадіжка інтелектуальної власності завдає значних витрат не лише економіці США, але й світовій економіці [27]. Крадіжка інтелектуальної власності проявляється в різних формах, кожна з яких має свої відмінні характеристики та наслідки. Нижче наведено чотири основні типи крадіжки ІВ:

– порушення авторських прав: використання без дозволу законного власника захищених авторським правом матеріалів, як-от: музика, літературні твори чи програмний код. Несанкціоноване використання позбавляє творців їхніх належних роялті та контролю над тим, як їхні творіння розповсюджуються чи використовуються;

– підробка товарних знаків: несанкціоноване використання зареєстрованих товарних знаків. Ця шахрайська практика вводить споживачів в оману щодо походження або якості товарів і паплюжить репутацію справжніх брендів;

– порушення патенту: несанкціоноване використання, продаж або виготовлення запатентованих винаходів. Цей вид злочину підриває суть патентів, яка полягає в наданні винахідникам виняткових прав на їхні винаходи, заохочення інновацій;

– крадіжка комерційної таємниці: несанкціоноване отримання та використання конфіденційної ділової інформації. Викрадена інформація, яка часто має вирішальне значення для конкурентної переваги бізнесу, може бути використана конкурентами несправедливо, порушуючи ринкову динаміку та цілісність.

До найпоширеніших методів, за допомогою яких зазвичай відбувається крадіжка комерційної таємниці, належать:

– несанкціонований доступ: отримання доступу до комерційних секретів підприємств шляхом кібератак хакерів;

– неправомірне привласнення інформації: розкриття певної комерційної інформації третім особам. Кіберзлочинці або недобросовісні організації можуть використовувати ці розкриття для отримання конкурентної переваги;

– зловживання працівниками: неправомірне привласнення комерційної таємниці, викликане внутрішнім невдоволенням або зовнішніми спокусами, внаслідок чого комерційні секрети можуть бути використані конкуруючими підприємствами, що винаймають таких співробітників;

Згідно до звіту 301 Торгової Палати США за 2023 р. до списку країн, в яких спостерігається недостатній захист прав інтелектуальної власності і які підлягають першочерговому спостереженню, входять Аргентина, Чилі, Китай, Індія, Індонезія, росія та Венесуела [28].

Серед найбільш резонансних злочинів по відношенню до інтелектуальної власності варто виділити конфлікт між технологічними гігантами Apple і Samsung, які були втягнуті в тривалу судову тяганину через порушення компанією Samsung декількох патентів на дизайн пристроїв, власником яких була корпорація Apple. У 2012 р. суд США постановив, що Samsung має відшкодувати збитки у розмірі 1 млрд дол. Відтоді між компаніями тривають суперечки щодо питань інтелектуальної власності й судові процеси в різних країнах світу.

На основі приведених вище видів кіберзлочинів вважаємо доцільним провести класифікацію ризиків, пов'язаних з ними, з точки зору ступеню притаманності суб'єктам господарювання. Запропонована авторами класифікація наведена на рис. 1.

Рис. 1. Класифікація ризиків кіберзлочинів за суб'єктами господарювання

Джерело: побудовано авторами.

Кіберзлочинність, як і інформаційні технології в цілому останніми роками набуває все більшого поширення, починаючи зі злочинів зі зламу сторінок в соціальних мережах фізичних осіб з метою розсилання шкідливих повідомлень та отримання коштів на рахунок шахраїв, отримання доступу до банківських рахунків шляхом здійснення маніпуляцій з номерами телефонів, асоційованих з ними, і закінчуючи комбінованими хакерськими атаками з використанням різноманітних методів соціальної інженерії, що можуть призвести до повної зупинки діяльності підприємства.

Висновки. На поточний момент в умовах війни, яка розповсюджується в тому числі і на кіберпростір, питання кібербезпеки стають все більш актуальними і ризики, пов'язані з кібербезпекою повинні мати найбільш високий пріоритет під час процесів аналізу та контролю. Як показали останні події, що стались у грудні 2023 р. з найбільшими українським оператором стільникового зв'язку Kyivstar, мережа якого була

атакована хакерським угрупуванням, недостатнє приділення уваги кібербезпеці може призвести до значних збитків (до 8 % річної виручки) і повного припинення діяльності підприємства на декілька днів до її повного відновлення. Враховуючи наведене у статті, темою подальших досліджень буде аналіз та контроль ризиків, пов'язаних із кіберзлочинами, що здійснюються по відношенню до підприємств технологічної галузі.

Література:

1. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну: матеріали науково-практичної конференції, присвяченої пам'яті віце-президента Кримінологічної асоціації України, професора, ОМ Литвака (м. Харків, 23 квіт. 2020 р.)*. 2020. С. 44–45. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content

Kundeus, V. G. (2020). Poniattia ta vydy kiberzlochyniv. [Concepts and types of cybercrimes]. *Derzhava i zlochynnist'. Novi Vyklyky v epohu postmodernu: materialy naukovo-praktychnoii conferenciii, prysviachenoii pam`iati vice-prezydenta Kryminologichnoii asociaciii Ukraiiny, profesora O.M. Lytvaka (m. Kharkiv, 23 kvitnia 2020 r.)* [State and crime. New challenges in the postmodern era: collection of theses of science and practice conference, in memory of the vice-president of the Criminological Association of Ukraine, professor, OM Litvak (Kharkiv, April 23, 2020)], 44-45 [in Ukrainian]

2. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки.* 2018. № 29 (68), 6. С. 119–124.

Schemchuk, V.V. (2018). Kiberzlochynnist' iak pereshkoda rozvytku informatsiynoho suspil`stva v Ukraiini. [Cybercrime as an obstacle to the development of the information society in Ukraine]. *Vcheni zapysky Tavriys`koho nacional`noho universytetu imeni V. I. Vernads`koho. Seriia: Iurydychni nauky*. [Academic notes of the Tavri National University named after V.I. Vernadskyi. Series: Legal Sciences],(29 (68), 6), 119-124. [in Ukrainian]

3. Гребенюк М., Черняк А. Проблеми протидії організованій злочинності у сфері цифрової економіки. *Підприємництво, господарство і право.* 2019. № 3. С. 297–303.

Grebeniuk, M., Cherniak, A. (2019). Problemy protydii orhanizovaniy zlochynnosti u sferi cyfrovoii ekonomiky. [Problems of combating organized crime in the field of digital economy]. *Pidpryiemnytstvo, hospodarstvo i pravo* [Entrepreneurship, economy and law], 3, 297-303.

4. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2021. № 64. С. 386–391.

Saiienko, M.I., Savela, I. A., Topolians`kyy, I.I. (2021). Mizhnarodnyy dosvid protydiii kiberzlochynnosti ta kibershakhraistvu. [International experience in combating cybercrime and cyberfraud]. *Naukovyy visnyk Uzhhorods`koho nacional`noho universytetu. Seriia: Pravo.* [Scientific Bulletin of the Uzhhorod National University. Series: Law], 64, 386-391. [in Ukrainian]

5. Боженко В. В., Койбічук В. В., Габенко М. М. Вплив кібершахрайств на фінансову систему на прикладі країн Євросоюзу. *Вісник Сумського державного університету. Серія: Економіка*. 2021. № 2. С. 47–52.

Bozhenko, V. V., Koybichuk, V. V., Habenko, M. M. (2021). Vplyv kibershakhraystv na finansovu systemu na prykladi kraiin Ievrosoiuzu. [The impact of cyber fraud on the financial system on the example of the countries of the European Union]. *Visnyk Sums`koho derzhavnoho universytetu. Seriia: ekonomika* [Bulletin of Sumy State University. Series: economy], 2, 47-52 [in Ukrainian]

6. Дзяд О. В., Стародуб Д. С. Економічні втрати та механізми протидії кіберзлочинності. *Ефективна економіка*. 2022. № 1. URL: http://www.economy.nayka.com.ua/pdf/1_2022/93.pdf (дата звернення: 21.01.2024).

Dziad, O.V., Starodub, D.S. (2022). Ekonomichni vtraty ta mekhanizmy protydiii kiberzlochynnosti. [Economic losses and cybercrime prevention mechanisms]. *Efektyvna ekonomika* [Effective economy], 1 < http://www.economy.nayka.com.ua/pdf/1_2022/93.pdf > (21 January 2024). [in Ukrainian]

7. Пушкаренко П. І. Кіберзлочинність як новітній феномен тіньової економіки. *Проблеми і перспективи розвитку банківської системи України.* 2006. № 17. С. 75–82.

Pushkarenko P. I. (2006). Kiberzlochynnist` iak novitniy fenomen tin`ovoii ekonomiky. [The cybercriminal as a new phenomenon of the shadow economy], *Problemy i perspektyvy rozvytku bankivs`koii systemy Ukraiiny: zbirnyk naukovykh prac'* [Problems and prospects of the development of the banking system of Ukraine: a collection of scientific papers], 17, 75-82. [in Ukrainian]

8. Ксьонжик І., Жовта Н., Павліна А. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. *Економіка та суспільство*. 2021. № 34.

Ks`onzhyk, I., Zhovta, N., Pavlina, A. (2021). Strahuvannia ryzykiv kiberbezpeky diial`nosti sub`iektiv hospodariuvannia v suchasnomu informatsiynomu prostori. [Monitoring of cyber security risks of business entities in the modern information space]. *Ekonomika ta suspil`stvo* [Economy and society], 34

9. Cybercrime. (European Comission) < https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en > (2024, січень, 21)

Cybercrime. (European Comission) < https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en > (21 January 2024)

10. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna, 10-17 April 2000. (United Nations) < https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf > (2024, січень, 21)

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna, 10-17 April 2000. (United Nations) < https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf > (21 January 2024)

11.Закон України Про основні засади забезпечення кібербезпеки України. 2017 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.01.2024).

Zakon Ukraiiny Pro osnovni zasady zabezpechennia kiberbezpeky Ukraiiny. 2017 (Verkhovna Rada Ukraiiny). [The Law of Ukraine On the Basic Principles of Ensuring Cyber Security of Ukraine. 2017 (Verkhovna Rada of Ukraine)]. Oficiyniy sayt Verkhovnoii Rady Ukraiiny [Official website of the Verkhovna Rada of Ukraine] < https://zakon.rada.gov.ua/laws/show/2163-19#Text > (21 January 2024)

12. What is Cybercrime? Types, Examples, and Prevention (Cyber Talents) < https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention > (2024, січень, 21)

What is Cybercrime? Types, Examples, and Prevention (Cyber Talents) < https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention > (21 January 2024)

13. Ransomware attacks in finance hit new high (2024 report) (Invenio IT) < https://invenioit.com/continuity/ransomware-attacks-finance/ > (2024, січень, 21)

Ransomware attacks in finance hit new high (2024 report) (Invenio IT) < https://invenioit.com/continuity/ransomware-attacks-finance/ > (21 January 2024)

14. FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud (FBI) < https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view > (2024, січень, 21)

FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud (FBI) < https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view > (21 January 2024)

15. Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme (United States Attorney's Office) < https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business > (2024, січень, 21)

Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme (United States Attorney's Office) < https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business > (21 January 2024)

16. Current report pursuant to Section 13 or 15(d) of the securities exchange aco of 1934 (United States Securities and Exchange Comission) < https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm > (2024, січень, 21)

Current report pursuant to Section 13 or 15(d) of the securities exchange aco of 1934 (United States Securities and Exchange Comission) < https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm > (21 January 2024)

17. Toyota Subsidiary Loses $37 Million Due to BEC Scam (CPO Magazine) < https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/ > (2024, січень, 21)

Toyota Subsidiary Loses $37 Million Due to BEC Scam (CPO Magazine) < https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/ > (21 January 2024)

18. The biggest data breach fines, penalties, and settlements so far (CSO) < https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html > (2024, січень, 21)

The biggest data breach fines, penalties, and settlements so far (CSO) < https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html > (21 January 2024)

19. Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures (European Central Bank) < https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html > (2024, січень, 21)

Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures (European Central Bank) < https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html > (21 January 2024)

20. The biggest ID fraud cases of all time: lots of money and damage (Techradar Pro) < https://www.techradar.com/how-to/the-biggest-id-fraud-cases-of-all-time-lots-of-money-and-damage > (2024, січень, 21)

The biggest ID fraud cases of all time: lots of money and damage (Techradar Pro) < https://www.techradar.com/how-to/the-biggest-id-fraud-cases-of-all-time-lots-of-money-and-damage > (21 January 2024)

21. The Worst Phishing Attacks in History (Graphus) < https://www.graphus.ai/blog/worst-phishing-attacks-in-history/ > (2024, січень, 21)

The Worst Phishing Attacks in History (Graphus) < https://www.graphus.ai/blog/worst-phishing-attacks-in-history/ > (21 January 2024)

22. 10 Malware Examples and 6 World Famous Attacks (Perception Point) < https://perception-point.io/guides/malware/10-malware-examples-and-6-world-famous-attacks/ > (2024, січень, 21)

10 Malware Examples and 6 World Famous Attacks (Perception Point) < https://perception-point.io/guides/malware/10-malware-examples-and-6-world-famous-attacks/ > (21 January 2024)

23. Emotet Malware (Cybersecurity & Infrastructure Security Agency) < https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware > (2024, січень, 21)

Emotet Malware (Cybersecurity & Infrastructure Security Agency) < https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware > (21 January 2024)

24. CovidLock ransomware exploits coronavirus with malicious Android app (TechRepublic) < https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/ > (2024, січень, 21)

CovidLock ransomware exploits coronavirus with malicious Android app (TechRepublic) < https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/ > (21 January 2024)

25. Annual Fraud Report. The definitive overview of payment industry fraud in 2022 (UK Finance) < https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf > (2024, січень, 21)

Annual Fraud Report. The definitive overview of payment industry fraud in 2022 (UK Finance) < https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf > (21 January 2024)

26. 2023 SONICWALL CYBER THREAT REPORT (Sonicwall) < https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2023-cyber-threat-report.pdf > (2024, січень, 21)

2023 SONICWALL CYBER THREAT REPORT (Sonicwall) < https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2023-cyber-threat-report.pdf > (21 January 2024)

27. Top IP theft statistics and stories in 2023 (Cyberhaven) < https://www.cyberhaven.com/guides/top-ip-theft-statistics > (2024, січень, 21)

Top IP theft statistics and stories in 2023 (Cyberhaven) < https://www.cyberhaven.com/guides/top-ip-theft-statistics > (21 January 2024)

28. 2023 Special 301 Report (Office of the United States Trade Representative) < https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf > (2024, січень, 21)

2023 Special 301 Report (Office of the United States Trade Representative) < https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf > (21 January 2024)