КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.225236
УДК 004.56

Гайдук Олег Васильович
Старший викладач Кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID 0000-0003-4740-7759
o.hayduk@knute.edu.ua

Звєрєв Володимир Павлович
Кандидат технічних наук, старший науковий співробітник
Доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID 0000-0002-0907-0705
zvieriev_vp@knute.edu.ua

АНАЛІЗ КІБЕРЗАГРОЗ В УМОВАХ СТРІМКОГО РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Анотація. В епоху цифрових технологій кібербезпека стала невід'ємним аспектом нашого життя. Зі зростанням залежності від технологій та інтернету люди, організації та суспільство в цілому стикаються з безпрецедентним рівнем кіберзагроз. Кібератаки стають все частішими, витонченішими та результативнішими, ставлячи під загрозу конфіденційну інформацію та важливі об'єкти критичної інфраструктури. Тому вкрай важливо розуміти мінливий ландшафт кіберзагроз і розробляти ефективні стратегії для протидії. Розглядається поточний стан кібербезпеки та викликів, з якими вона стикається. Висвітлюються аспекти підвищення кількості кібератак та їхньої зростаючої складності, через що традиційним заходам безпеки важко встигати за ними. Також розглядаються різні типи кіберзагроз в тому числі програми-вимагачі та атаки на основі підбору паролів. Крім того, розглядаються мотиви цих атак, які можуть варіюватися від фінансової вигоди до комерційного та політичного шпигунства і кібервійни. Розглядаються аспекти впливу нових технологій на кібербезпеку, які пропонують величезні переваги, але вони також створюють нові вектори атак, якими можуть скористатися кіберзлочинці, експлуатуючи новітні потенційні вразливості та ризики. Аналізуються глобальні тренди розвитку IoT та кібербезпеки за 20 років з 2004 до 2024 року, а також розвиток загроз та атак програм-вимагачів, особливо під час пандемії Covid-19, а також кібератак на основі зламу паролів і їх значного підвищення в 2023 році. Стаття надає всебічний огляд поточного стану кібербезпеки та викликів, з якими вона стикається. Вона підкреслює важливість прийняття цілісного підходу до кібербезпеки, який поєднує технологічні рішення з освітою, обізнаністю та міжнародним співробітництвом. Крім того, підкреслюється необхідність для організацій і окремих осіб зберігати пильність і адаптуватися до нових загроз і технологій. Працюючи разом, ми можемо створити безпечніше і надійніше цифрове майбутнє для всіх.

Ключові слова: кіберпростір; кібербезпека; кіберзагроза; кібервійна; кіберризик; вплив; ризик; міжнародні комунікації.

ВСТУП

Постановка проблеми. Інтернет став невід'ємною частиною життя, охопивши мільярди людей. Кіберпростір перетворився на ключове середовище для більшості сучасних процесів, від економіки та політики до освіти та особистих стосунків. Зростання залежності від кіберпростору робить його мішенню для кіберзагроз, які

ставлять під загрозу конфіденційність, цілісність та доступність даних, а також створюють ризики для економіки, політики та суспільства [1, с. 12–13], [31].

Кібератаки мають більш широкий контекст, ніж традиційні інформаційні операції. Вони можуть бути спрямовані на крадіжку даних, порушення роботи систем, або поширення дезінформації. Кібератаки можуть мати значний вплив на економіку, політику та суспільство [2], [29], [31].

Оцінка впливу кібератак дозволяє класифікувати кіберінциденти за рівнем загрози. Поняття «ризик» є ключовим у сучасних дослідженнях кібербезпеки. Традиційне розуміння ризику як ймовірності негативної події є недостатнім. Потрібен новий підхід до аналізу ризиків, адаптований до реалій техногенної цивілізації [2].

Стрімкий технологічний прогрес сучасного світу, разом з позитивними досягненнями цивілізації, спричиняє до непередбачуваних викликів та загроз з кіберпростору. Швидкість розвитку технологій, зокрема в інформаційній сфері, відкриває нові можливості для суспільства та економіки, проте вона також приносить і значні проблеми і загрози [1]. Кіберпростір став полем боротьби для різних суб'єктів — від держав, їхніх розвідок і спецслужб до кримінальних груп, хакерів, та злочинців. Кібератаки можуть мати значні наслідки для інфраструктури, економіки і політики, а також для приватності та безпеки людей. Зловживання цифровими технологіями може призвести до крадіжок даних, дестабілізації фінансових систем, шпигунства і масового стеження, маніпулювання виборами, терористичних актів та інших серйозних проблем. Відповідно, забезпечення кібербезпеки стає важливим чинником для сучасного суспільства і вимагає спільних зусиль різних секторів, включаючи урядові органи, приватні компанії та громадянське суспільство [2].

В світі загальновизнано, що розвиток інформаційно-комунікаційних технологій призвів до формування глобального кіберпростору, який став невід'ємною частиною життя сучасного суспільства. Водночас залежність від кіберпростору породжує нові виклики і загрози безпеці — кіберзагрози [3].

В контексті сучасних викликів у сфері кібербезпеки важливо розглядати можливість ескалації ситуації та перехід від заходів усталеної протидії кіберзагрозам до концепції кібервійни. Зі зростанням технологічних можливостей кібератак та їхнього потенціалу викликати серйозні наслідки, держави повинні не лише удосконалювати свої системи кібербезпеки, але й розвивати стратегії протидії всупереч масовому наростанню інцидентів в кіберпросторі [3]. Хоча тематика кібервійни залишається ще недостатньо дослідженою, можна констатувати, що кібервійна є складним та багатогранним явищем і визначається як форма військового конфлікту із використанням кіберпростору, інформаційних технологій та електронних комунікаційних мереж для проведення військових операцій, включаючи шпигунство, саботаж, дискредитацію, дезінформацію та інші дії, які можуть призвести до серйозних наслідків для національної безпеки та стабільності [4] – [6].

Відсутність універсальної міжнародної системи класифікації кіберзагроз підкреслює різноманітність і багатоплановість цих загроз у сучасному цифровому середовищі. Кіберзагрози можна розділити на різні категорії, типи та сфери впливу [7], [8]. Важливі характеристики кіберзагроз включають глобальний масштаб, анонімність та складність виявлення джерела. Ця різноманітність і складність управління кіберзагрозами ставлять під загрозу безпеку та нормальне функціонування критичних інфраструктур, бізнесу та суспільства в цілому. Доцільно розглядати кіберзагрози як постійно еволюціонуючи, адаптивні вектори атак, які потребують постійного оновлення

та підвищення заходів захисту для забезпечення надійності та стійкості цифрового простору [8].

Аналіз останніх досліджень і публікацій. Завдяки інноваціям та здешевленню технологій, доступ до Інтернету значно розширився, що призвело до зростання кількості користувачів і продуктивності мережі. Сьогодні Інтернет охоплює більше 5 мільярдів людей у всьому світі [9] і ця кількість невпинно збільшується. Завдяки підвищенню доступності та зручності використання, Інтернет став невід'ємною частиною повсякденного життя для більшості людей. Кіберпростір став глобальною економічною площадкою, та генерує значну частину світової економіки [10]. Наразі більшість економічних, комерційних, наукових, освітніх, культурних, соціальних та урядових процесів на всіх рівнях — від окремих осіб, громадських організацій, бізнесу, наукової та освітньої спільноти, державних та міжнародних установ — відбувається у кіберпросторі. Інтернет став невід'ємним елементом взаємодії між країнами та різними суб'єктами міжнародних відносин. Тож можна констатувати, що сьогодні кіберпростір є ключовим середовищем для більшості сучасних процесів.

Доля прибутку, яку комерційний бізнес отримує в кіберпросторі, вносить все більший вклад у Валові Внутрішні Продукти (ВВП) країн світу. Серед критеріїв, що використовуються для визначення рівня розвитку, основні показники тепер пов'язані з кіберпростором [11], [31]. Велика частина матеріального та духовного надбання країн світу сьогодні генерується в кіберпросторі, і все більша частина матеріальних доходів та досягнень громадян отримується завдяки кіберпростору або має суттєвий вплив на кіберпростір [11], [12]. Низька вартість доступу, легкість маніпуляцій, анонімність, відсутність географічних кордонів в кіберпросторі, створили сприятливі умови для учасників всіх рівнів, включаючи як уряди, так і організовані терористичні групи, а також окремих осіб [11], [12], [32].

Разом із розвитком кіберпростору, у всьому світі стрімко зростають витрати на забезпечення кібербезпеки. Феномен пандемії Covid-19 і супутній йому карантин в багатьох країнах спричинив вибуховий ріст користування комп'ютерами разом із значною активізацією всіх форм кіберзагроз [13]. Щорічні витрати в світі на ці цілі сягнули трильйонів доларів і будуть тільки збільшуватися [14].

Інтернет речей (англійською «Internet of Things», скорочено — IoT) вперше було сформульовано в кінці XX-го століття, у 1999 році. Це концепція комунікації об'єктів («речей»), які використовують технології для взаємодії між собою та навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини. Таким чином, усі пристрої в будинках, в автомобілях та інших системах інфраструктури повинні виконувати обробку інформації, її аналіз та здійснювати обмін між собою і залежно від результатів приймати рішення та виконувати певні дії [15]. Використання систем IoT стрімко зростає, і сьогодні вони становлять все більшу частину кіберпростору і мають суттєвий взаємний вплив. Наріжне застосування цієї технології виходить далеко за рамки простого розуміння «Інтернету речей» і все більше дотичне як до кінетичної так і кібервійни [16].

Кіберпростір не має фізичних кордонів, відповідно кіберагресія та кібервійна не обмежуються одною постраждалою державою і часто впливають на значно більше коло суб'єктів [3], так само і агресія росії в кіберпросторі не обмежується Україною [17], [18].

Мета статті. Метою статті є комплексне дослідження феномену кіберзагроз у контексті розвитку інформаційних технологій.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Кіберзагрози почали з'являтися з появою перших комп'ютерів у 1950–1960-х роках. Першим вірусом вважається Creeper, створений в 1971 році. У 1980-х роках з'явилися перші комп'ютерні віруси, що поширювалися через дискети та мережі [19].

У 1990-х роках з розвитком Інтернету кіберзагрози стали глобальним явищем. З'явилися перші хробаки, які самостійно поширювалися мережею, такі як Morris worm у 1988 році [19], [20].

У 2000-х роках стали популярними атаки типу DoS «відмова в обслуговуванні», що перевантажували сервери запитами. Також з'явилися перші ботнети — мережі заражених комп'ютерів для кібератак.

З 2010-х років кіберзагрози стали високотехнологічними та політично мотивованими. Поширилися APT-атаки на урядові та військові структури. З'явилися програми-вимагачі, що шифрують дані жертв. Триває боротьба з ботнетами та фішинговими атаками.

Кіберзагрози продовжують еволюціонувати, вимагаючи постійного вдосконалення кібербезпеки. Головною проблемою залишається людський фактор, оскільки більшість атак вимагають взаємодії з людиною [20], [30].

Переламним як з точки зору кібербезпеки, так і з боку технологій IoT, став 2014 рік [21]. Цей рік був названий «Роком кібератак», а 2015 рік деякі галузеві коментатори охрестили «Роком кібератак-2». Загальна картина полягає в тому, що кібератаки з цього періоду стають частішими, витонченішими і мають більш серйозні наслідки [21]. Крім того, спостерігається поступовий перехід до більш руйнівних, а також більш персональних атак [21], [30]. З цього року також почав суттєво зростати загальний інтерес до цих термінів в мережі Інтернет, що відобразилося в пошукових запитах. На діаграмі (рис. 1) представлені Google Тренди за пошуковими запитами «Кібербезпека» та «IoT» з початку 2004 року до лютого 2024 року.

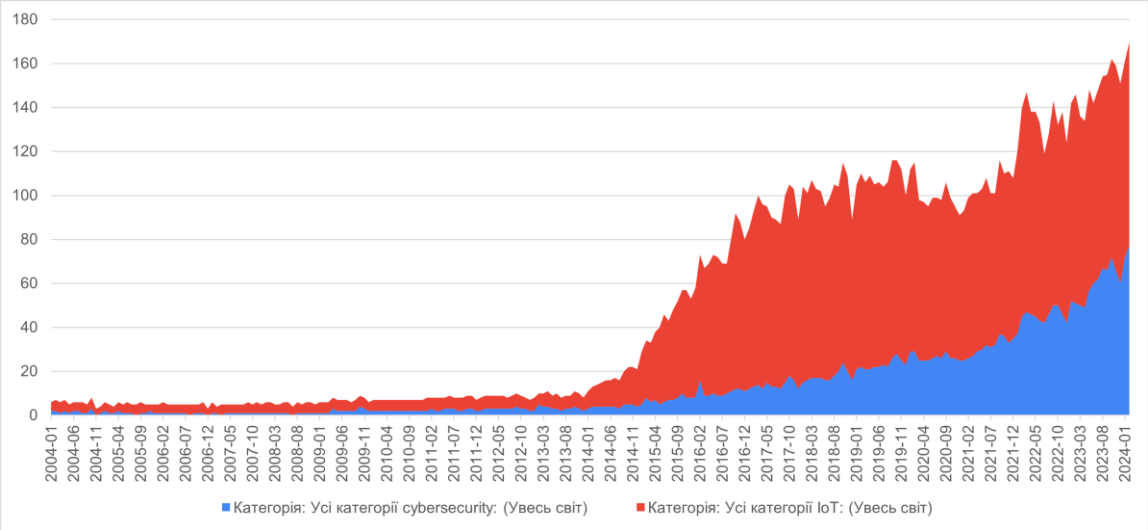

Рис. 1. Тренди пошукової системи Google за запитами «Кібербезпека» та «IoT»

Наведені дані свідчать не тільки про зростання глобального інтересу і кількості пошукових запитів за термінами «Кібербезпека» та «IoT» з 2014 року, а й про суттєве і наростаюче підвищення цього інтересу після спаду у 2019–2020 роках [22]. Враховуючи загальновідомі терміни розповсюдження Covid-19, яке розпочалося в 2019 році та

стрімко розвивалося і було оголошено пандемією в березні 2020 року, відслідковується глобальний вплив пандемії на ці фактори, що стало причиною зниження вказаних трендів в цей час [23]. Разом із цим, як видно із графіка, з початком 2021 року і до сьогодні йде постійне наростаюче підвищення цих показників. Загальновідомий факт, що з введенням карантину, населення майже всіх країн світу почало активніше використовувати комп'ютери, наслідком чого стало також значне підвищення негативної та деструктивної активності в кіберпросторі [22], [23]. Відповідно почав зростати інтерес людей до кібербезпеки та IoT, що ми і бачимо на рис. 1.

Таким чином, з початком періоду пандемії Covid-19, який характеризується зростанням активності в кіберпросторі, уряди країн та транснаціональні компанії галузі IT і кібербезпеки почали фіксувати збільшення шкідливої та руйнівної активності в глобальній мережі.

Галузь програм-вимагачів (ransomware) являє собою діяльність великої кількості зловмисних учасників з усього світу. Аналіз цього сегменту свідчить, що для досягнення мети недостатньо тільки шкідливого програмного забезпечення, натомість викрита організована злочинна система з використанням соціальної інженерії та скоординованої бізнес-схеми подвійного вимагання з використанням як мережі даркнету, так і мережі сайтів на звичайних топ-доменах (як у відкритому Інтернеті) [23], [33]. Враховуючи, що «поріг доступу» з технічної компетенції в цей злочинний сегмент здається невисоким, це приваблює багатьох початківців і робить цю систему масовою і небезпечною.

Аналізуючи ситуацію випадків зіткнення корпоративних клієнтів з програмами-вимагачами у 2018–2021 роках за даними компанії Microsoft (рис. 2), можна побачити схожу картину помітного сплеску кількості таких випадків наприкінці 2019 року та у 2020 році на початку пандемії COVID-19.

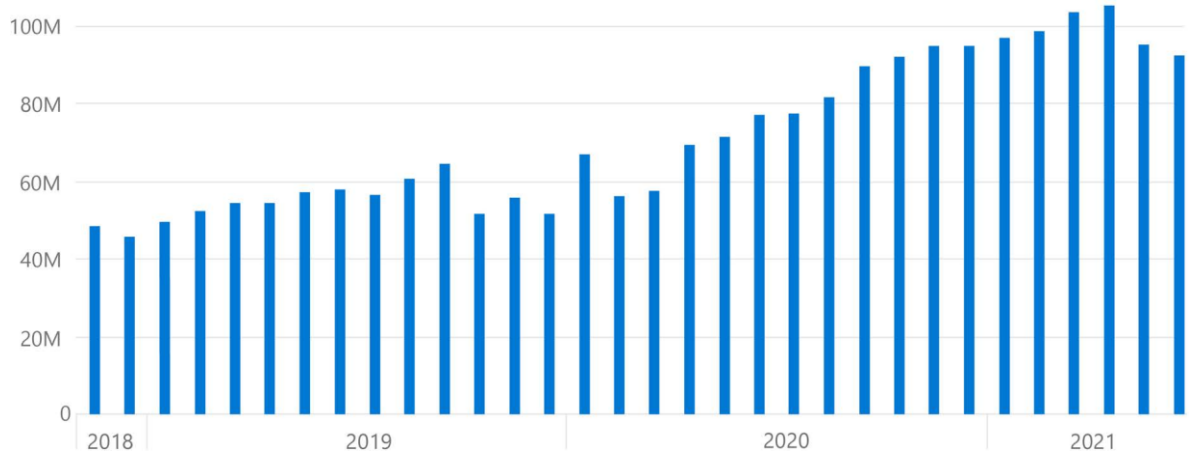

Рис. 2. Частота виявлення програм-вимагачів 2018–2021: Корпоративні клієнти

Аналіз телеметрії компанії Microsoft у 2022 і 2023 роках свідчить, що організації по всьому світу зіткнулися з подальшим збільшенням кількості атак програм-вимагачів, причому кількість атак, керованих людиною до кінця 2023 року зросла ще більш ніж на 200 відсотків з вересня 2022 року [23], [24], [33].

Аналіз кібератак на основі зламу паролів з 2020 по 2023 роки свідчить, що за даними Microsoft Entra, кількість спроб атак у безезні–квітні 2023 році зросла більш ніж у десять разів порівняно з середнім рівнем всього періоду 2020–2022 років, з приблизно 3 мільярдів на місяць до понад 30 мільярдів [24], [25]. Це означає, що у квітні відбувалося більше 11 000 атак на паролі в секунду.

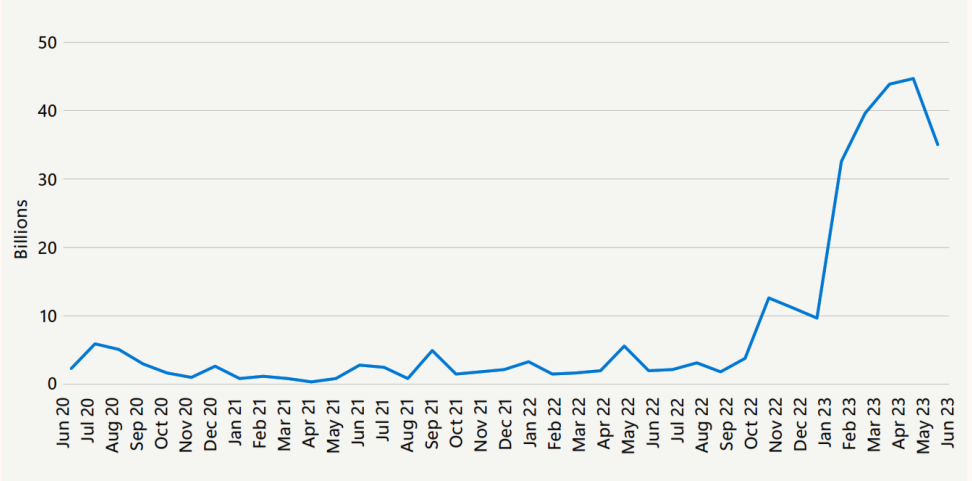

Рис. 3. Кількість атак на основі паролів 2020–2023 рр.

Компанія Microsoft вважає, що однією з головних причин, чому атаки на паролі настільки поширені, є низький рівень безпеки багатьох організацій, особливо в освітньому секторі. Разом із цим, надзвичайно важливим аспектом лишається криптозахист паролів [26], [28], [32], особливо у світлі останніх повідомлень про доведеність можливості використання штучного інтелекту для акустичного розпізнавання натискань клавіш на клавіатурі комп'ютера з телефону та інших пристроїв з мікрофонами, які знаходяться поруч [27], [28], [30], [33].

Основні ключові характеристики кіберзагроз в сучасних умовах:

- глобальний масштаб: кіберзагрози можуть впливати на системи та мережі в усьому світі, оскільки Інтернет не має кордонів. Це робить їх особливо складними для контролю та управління;
- анонімність: найчастіше атаки відбуваються через анонімні мережі або за допомогою фальшивих ідентичностей, що ускладнює виявлення та відстеження зловмисників;
- складність виявлення джерела атаки: як правило, зловмисники маскують свої зловмисні дії, використовуючи різноманітні техніки, такі як IP-підробка або розподілена атака з використанням ботнетів, ускладнюючи процес виявлення джерела атаки;
- використання новітніх технологій: зловмисники постійно вдосконалюють свої методи та використовують для цього новітні технології, такі як штучний інтелект, машинне навчання та криптографічні методи, щоб підвищити ефективність своїх атак і уникнути виявлення.

Ці характеристики роблять кіберзагрози особливо складними для боротьби з ними і вимагають постійного удосконалення технологій та стратегій кібербезпеки для захисту інформаційних систем та даних. Таким чином, в сучасних умовах вирішення означених проблем кібербезпеки доцільно проводити на основі наступного:

1) інтегрованого підходу до оцінки ризиків: запроваджувати більш ефективні методи оцінки ризиків від кіберзагроз у всіх сферах життєдіяльності суспільства, включаючи технологічний, економічний, політичний, правовий та екологічний виміри. Інтеграція цих факторів дозволить зробити більш детальний аналіз загроз і прийняти ефективні заходи для їх запобігання та управління;

2) подальшого розвитку теоретичних підходів: сучасні виклики у сфері кібербезпеки вимагають створення нових теоретичних підходів до поняття ризиків. Це включає аналіз сучасних тенденцій, вивчення характеристик загроз та їхніх можливих наслідків, а також розробку методологій для оцінки та управління кіберризиками;
3) розробки нових концепцій кібербезпеки: нові інциденти у сфері кібербезпеки потребують розробки нових концепцій та стратегій захисту. Це включає розробку технологічних інновацій, впровадження нових стандартів безпеки, підвищення кваліфікації кадрів у галузі кібербезпеки та забезпечення ефективного співробітництва між державами та приватним сектором;
4) комплексного підходу до захисту: кібербезпека потребує комплексного підходу, який охоплює технологічні, організаційні та правові аспекти захисту інформації. Це включає розробку та впровадження систем захисту, вдосконалення процесів управління безпекою, забезпечення відповідності з правовими вимогами та створення культури безпеки в організаціях і суспільстві в цілому.

Вирішення цих завдань вимагатиме конструктивної співпраці між різними галузями та структурами, від державних органів до приватного сектору та громадських організацій.

У сучасному світі кібербезпека стає все більш важливим елементом міжнародних відносин та комунікацій. Зростаюча взаємозалежність і цифровізація створюють нові виклики і загрози, які потребують адекватних стратегічних відповідей. Сьогодні управління кібербезпекою виходить за рамки простих технологічних рішень. Необхідно послідовно впроваджувати культурні зміни у підході до кібербезпеки, коли кожна людина розуміє свою відповідальність за власну безпеку в кіберпросторі. Це вимагає глобального навчання як фахових працівників, так і всіх громадян щодо кібергігієни, основ кібербезпеки та застосування найкращих практик.

Головними ризиками для міжнародних комунікацій є атаки на урядову та корпоративну інфраструктуру, витік конфіденційної інформації, порушення роботи систем зв’язку та поширення дезінформації. Ефективна протидія цим загрозам потребує комплексного підходу, що включає оцінку ризиків, превентивні заходи, швидке реагування, міжнародну координацію та інвестиції в нові технології.

Інтернет речей став невід’ємною частиною сучасного життя, оскільки багато пристроїв підключено до інтернету, включаючи побутову техніку, автомобілі та промислове обладнання. Однак ця взаємопов’язаність створює нові вразливості, якими можуть скористатися зловмисники, що робить вкрай важливим забезпечення безпеки цих пристроїв.

Кібербезпека стає все більш важливою для організацій у всіх секторах, включаючи освіту, охорону здоров’я, фінанси та уряд, оскільки вони стикаються зі зростаючою кількістю витончених кібератак. Впроваджуючи надійні заходи кібербезпеки, організації можуть захистити свої системи та дані, мінімізувати час простою та зберегти довіру громадськості.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В сучасних умовах стрімкого розвитку інформаційних технологій найважливішим етапом в системі та управління кібербезпекою є аналіз і визначення трендів і тенденцій перебігу кіберзагроз, їхнього взаємного впливу, а також дії інших факторів, навіть не пов’язаних напряму з кіберпростором, які здатні внести суттєвий глобальний ефект в

розвиток комп'ютерних систем і мереж. Пошук нових типів ризиків та визначення їх ключових характеристик — це безперервний процес, який дозволяє зрозуміти сутність цих ризиків, проаналізувати їх та розробити ефективні методи управління ними. Подальший все більш глибокий аналіз цих даних може відкрити нові взаємозв'язки та взаємодію між кіберзагрозами та іншими чинниками. Це може призводити до виникнення поки що неідентифікованих ескалацій ризикових ситуацій та їх наслідків. Такий аналіз і спостереження можуть також бути потенційним джерелом викриття нових взаємозв'язків майбутніх ризикових ситуацій і суттєво покращити розуміння кіберпростору та управління кібербезпекою на національному та міжнародному рівнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Криворучко, В., & Костюк І. (2020) Стратегія безпеки інформації. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів. *Київський національний торговельно-економічний університет*.
2. Li, Y., & Liu, Q. (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent development. *Energy Reports, 7,* 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
3. Brantly A.F. (2016) *The decision to attack: military and intelligence cyber decision-making.* University of Georgia Press.
4. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation, 17(3),* 3–13. https://doi.org/10.15407/scine17.03.003
5. Dmytruk, Y., et al. (2022). Cyberwar as a Variety of Information Wars. Ukrainian Cyber Space Protection. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 4(16),* 28–36. https://doi.org/10.28925/2663-4023.2022.16.2836
6. Gillis, A. (2023). *Definition cyberwarfare*. TechTarget. https://www.techtarget.com/searchsecurity/definition/cyberwarfare
7. Laktionov, I., et al.. (2022). Research Tools for Protecting Internet Resources from Ddos-Attack During Cyberwar. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 1(17),* 91–111. https://doi.org/10.28925/2663-4023.2022.17.91111
8. Callejas, J., Afifi, A., & Lozinskiy, N. (2021). *Cybersecurity in the united nations system organizations.* United Nations. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf
9. *Digital 2023: Global Overview Report — DataReportal – Global Digital Insights.* (2023). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-global-overview-report
10. *Study Finds Internet Economy Grew Seven Times Faster Than Total U.S. Economy, Created Over 7 Million Jobs in the Last Four Years.* (2021). IAB. https://www.iab.com/news/study-finds-internet-economy-grew-seven-times-faster/
11. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation, 17(3),* 3–13. https://doi.org/10.15407/scine17.03.003
12. Li, Y., & Liu, Q., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7,* 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
13. Columbus, L. (2020). *2020 Roundup Of Cybersecurity Forecasts And Market Estimates*. Forbes magazine. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/
14. Fox, J. (2023). *Top Cybersecurity Statistics for 2024*. Cobalt: Offensive Security Services. https://www.cobalt.io/blog/cybersecurity-statistics-2024
15. O. V. Kryvoruchko, T. M. Morozova, A. M. Desyatko, (2021). The Internet of Things is a new stage of IT development. *Computer technologies of data processing.*
16. *Cybersecurity and the Internet of Things (IoT) | IDB.* (n.d.). Institute for Defense and Business. https://www.idb.org/cybersecurity-and-the-internet-of-things/
17. Boiko, V. (2022). *The global echo of the Russian-Ukrainian cyber confrontation*. National Institute for Strategic Studies. https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/svitove-vidlunnya-rosiysko-ukrayinskoho-kiberprotystoyannya

18. Vityuk, I. (2023). *How the SBU uses the latest technologies to protect the country's cyber security*. Ua.news. https://ua.news/ua/technologies/yak-sbu-zastosovuye-novitni-tehnologiyi-dlya-zahystu-kiberbezpeky-krayiny-poyasnyuye-nachalnyk-departamentu-kiberbezpeky-sbu-illya-vityuk
19. Alam, S. (2022). *Cybersecurity: past, present and future*. ResearchGate. https://www.researchgate.net/publication/361765615_Cybersecurity_Past_Present_and_Future
20. Tarhan, K. (2022). *International Islamic University Malaysia, Historical development of cybersecurity studies: a literature review and its place in security studies*. http://studiastrategiczne.amu.edu.pl/wp-content/uploads/2023/02/ps-2023-15-21.pdf
21. Weber, R., & Studer, E. (2016). Cybersecurity in the internet of things: legal aspects. *Computer Law & Security Review, 32(5),* 715–728. https://doi.org/10.1016/j.clsr.2016.07.002
22. Katagiri, N. (2022). Explaining cyberspace dynamics in the covid era. *Global Studies Quarterly, 2(3).* https://doi.org/10.1093/isagsq/ksac022
23. Microsoft Didital Defence Report 2021.
24. Microsoft Didital Defence Report 2022.
25. Microsoft Didital Defence Report 2023.
26. Kuznetsov, O., et al. (2018) . Periodic properties of cryptographically secure pseudorandom sequences. *Applied Radio Electronics: Sci. J. 17(3, 4),* 96–103.
27. Harrison, J., Toreini, E., & Mehrnezhad, M. (2023), A practical deep learning-based acoustic side channel attack on keyboards. *Cornell University.*
28. Hulak, H., et al. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
29. Shevchenko, S., et al. (2022). Insiders and Insider Information: Essence, Threats, Activities and Legal Responsibility. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 3(15),* 175–185. https://doi.org/10.28925/2663-4023.2022.15.175185
30. Skitsko, O., et al. (2023). Threats and Risks of the Use of Artificial Intelligence. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 2(22),* 6–18. https://doi.org/10.28925/2663-4023.2023.22.618
31. Sokolov, V., & Skladannyi, P. (2023). Methodology for Assessing Comprehensive Damages from an Information Security Incident. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 1(21),* 99–120. https://doi.org/10.28925/2663-4023.2023.21.99120
32. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative Analysis of Solutions to Provide Control and Management of Privileged Access in the it Environment. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 4(16),* 98–112. https://doi.org/10.28925/2663-4023.2022.16.98112
33. Hulak, H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 2(10),* 6–28. https://doi.org/10.28925/2663-4023.2020.10.628

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Oleg Gaiduk
Senior Lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID 0000-0003-4740-7759
o.hayduk@knute.edu.ua

Volodymyr Zverev
Candidate of Technical Sciences, Senior Researcher
Associate Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID 0000-0002-0907-0705
zvieriev_vp@knute.edu.ua

ANALYSIS OF CYBER THREATS IN THE CONTEXT OF RAPID DEVELOPMENT OF INFORMATION TECHNOLOGY

Abstract. In the digital age, cybersecurity has become an integral aspect of our lives. With the growing dependence on technology and the Internet, individuals, organizations and governments face unprecedented levels of cyber threats. Cyberattacks are becoming more frequent, sophisticated, and malicious, putting confidential information and critical infrastructure at risk. Therefore, it is crucial to understand the changing nature of cyber threats and develop effective strategies to counter them. The current state of cybersecurity and the challenges it faces are analyzed. It highlights aspects of the increasing number of cyberattacks and their growing complexity, which makes it difficult for traditional security measures to keep up. The different types of cyber threats, including ransomware and password guessing attacks, are also discussed. In addition, the motives for these attacks are discussed, which can range from financial gain to commercial and political espionage and cyberwarfare. The impact of new technologies on cybersecurity is considered, which offer tremendous benefits, but they also create new attack vectors that can be used by cybercriminals to exploit the latest potential vulnerabilities and risks. The paper analyzes global trends in IoT and cybersecurity over the 20 years from 2004 to 2024, as well as the development of ransomware threats and attacks, especially during the Covid-19 pandemic, as well as password cracking cyberattacks and their significant increase in 2023. Provides a comprehensive overview of the current state of cybersecurity and the challenges it faces. It emphasizes the importance of adopting a holistic approach to cybersecurity that combines technological solutions with education, awareness and international cooperation. It also emphasizes the need for organizations and individuals to remain vigilant and adapt to new threats and technologies. By working together, we can create a safer and more secure digital future for all.

Keywords: cyberspace; cybersecurity; cyber threat; cyber warfare; cyber risk; impact; risk; international communications.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kryvoruchko, V., & Kostyk I. (2020). Information security strategy. Cyberhygiene. Cubersecurity. State security: materials of scientific seminars. *Kyiv National Unoversity of Trade and Economics.*
2. Li, Y., & Liu, Q. (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent development. *Energy Reports, 7,* 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
3. Brantly A.F. (2016) *The decision to attack: military and intelligence cyber decision-making.* University of Georgia Press.
4. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation, 17(3),* 3–13. https://doi.org/10.15407/scine17.03.003

5. Dmytruk, Y., et al. (2022). Cyberwar as a Variety of Information Wars. Ukrainian Cyber Space Protection. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 4(16),* 28–36. https://doi.org/10.28925/2663-4023.2022.16.2836
6. Gillis, A. (2023). *Definition cyberwarfare*. TechTarget. https://www.techtarget.com/searchsecurity/definition/cyberwarfare
7. Laktionov, I., et al.. (2022). Research Tools for Protecting Internet Resources from Ddos-Attack During Cyberwar. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 1(17),* 91–111. https://doi.org/10.28925/2663-4023.2022.17.91111
8. Callejas, J., Afifi, A., & Lozinskiy, N. (2021). *Cybersecurity in the united nations system organizations.* United Nations. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf
9. *Digital 2023: Global Overview Report — DataReportal – Global Digital Insights.* (2023). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-global-overview-report
10. *Study Finds Internet Economy Grew Seven Times Faster Than Total U.S. Economy, Created Over 7 Million Jobs in the Last Four Years.* (2021). IAB. https://www.iab.com/news/study-finds-internet-economy-grew-seven-times-faster/
11. Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation, 17(3),* 3–13. https://doi.org/10.15407/scine17.03.003
12. Li, Y., & Liu, Q., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7,* 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
13. Columbus, L. (2020). *2020 Roundup Of Cybersecurity Forecasts And Market Estimates*. Forbes magazine. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/
14. Fox, J. (2023). *Top Cybersecurity Statistics for 2024*. Cobalt: Offensive Security Services. https://www.cobalt.io/blog/cybersecurity-statistics-2024
15. O. V. Kryvoruchko, T. M. Morozova, A. M. Desyatko, (2021). The Internet of Things is a new stage of IT development. *Computer technologies of data processing.*
16. *Cybersecurity and the Internet of Things (IoT) | IDB.* (n.d.). Institute for Defense and Business. https://www.idb.org/cybersecurity-and-the-internet-of-things/
17. Boiko, V. (2022). *The global echo of the Russian-Ukrainian cyber confrontation*. National Institute for Strategic Studies. https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/svitove-vidlunnya-rosiysko-ukrayinskoho-kiberprotystoyannya
18. Vityuk, I. (2023). *How the SBU uses the latest technologies to protect the country's cyber security*. Ua.news. https://ua.news/ua/technologies/yak-sbu-zastosovuye-novitni-tehnologiyi-dlya-zahystu-kiberbezpeky-krayiny-poyasnyuye-nachalnyk-departamentu-kiberbezpeky-sbu-illya-vityuk
19. Alam, S. (2022). *Cybersecurity: past, present and future*. ResearchGate. https://www.researchgate.net/publication/361765615_Cybersecurity_Past_Present_and_Future
20. Tarhan, K. (2022). *International Islamic University Malaysia, Historical development of cybersecurity studies: a literature review and its place in security studies*. http://studiastrategiczne.amu.edu.pl/wp-content/uploads/2023/02/ps-2023-15-21.pdf
21. Weber, R., & Studer, E. (2016). Cybersecurity in the internet of things: legal aspects. *Computer Law & Security Review, 32(5),* 715–728. https://doi.org/10.1016/j.clsr.2016.07.002
22. Katagiri, N. (2022). Explaining cyberspace dynamics in the covid era. *Global Studies Quarterly, 2(3).* https://doi.org/10.1093/isagsq/ksac022
23. Microsoft Didital Defence Report 2021.
24. Microsoft Didital Defence Report 2022.
25. Microsoft Didital Defence Report 2023.
26. Kuznetsov, O., et al. (2018) . Periodic properties of cryptographically secure pseudorandom sequences. *Applied Radio Electronics: Sci. J. 17(3, 4),* 96–103.
27. Harrison, J., Toreini, E., & Mehrnezhad, M. (2023), A practical deep learning-based acoustic side channel attack on keyboards. *Cornell University.*
28. Hulak, H., et al. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
29. Shevchenko, S., et al. (2022). Insiders and Insider Information: Essence, Threats, Activities and Legal Responsibility. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 3(15),* 175–185. https://doi.org/10.28925/2663-4023.2022.15.175185

30. Skitsko, O., et al. (2023). Threats and Risks of the Use of Artificial Intelligence. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 2(22),* 6–18. https://doi.org/10.28925/2663-4023.2023.22.618
31. Sokolov, V., & Skladannyi, P. (2023). Methodology for Assessing Comprehensive Damages from an Information Security Incident. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 1(21),* 99–120. https://doi.org/10.28925/2663-4023.2023.21.99120
32. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative Analysis of Solutions to Provide Control and Management of Privileged Access in the it Environment. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 4(16),* 98–112. https://doi.org/10.28925/2663-4023.2022.16.98112
33. Hulak, H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 2(10),* 6–28. https://doi.org/10.28925/2663-4023.2020.10.628