ПРИКЛАДНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК,
БЕЗПЕКИ ТА МАТЕМАТИКИ, 2024, № 3

УДК 004.04

ТЕНДЕНЦІЇ РОЗВИТКУ ЗАГРОЗ КІБЕРБЕЗПЕЦІ

Кіндрат П.В. (ORCID: 0000-0003-0351-3349)
Рівненський державний гуманітарний університет

TRENDS OF CYBERSECURITY THREATES

Kindrat P.V.
Rivne State University of the Humanities

Abstract. To successfully counter information threats in the future, it is essential to understand the causes and trends in the development of cyberspace.Over the past years, there has been a noticeable increase in the diversity of cybersecurity threats. This trend is driven by both the widespread adoption of digital platforms in everyday life and the increasing role of social media as communication channels.

Social engineering remains a primary attack vector against both individuals and organizations. Enhancements in its techniques simplify the acquisition of critical information about potential targets and enable their exploitation through various communication channels.

At the national security level, cybersecurity threats are increasingly aimed at destabilizing social order and provoking conflicts within society. This reflects the challenge governments face in defending their national cyberspace.

The innovative changes that occurred in 2022-23 have significantly altered cybersecurity trends, as evidenced by statistics on the emergence and realization of information security threats.

Generative language models, while not directly threatening to cybersecurity, amplify the methods of social engineering and attacks that utilize them. The deployment of artificial intelligence in cybersecurity has shown particularly well results in network monitoring and encrypted traffic analysis.

Concurrently, the development of quantum computers threatens existing data encryption systems and prompts advancements in cryptography through the quantum transition.

Keywords: cybersecurity, cybersecurity threats, trends of cybersecurity, social engineering, artificial intelligence, quantum cryptography.

Вступ. Поняття «кібербезпеки» є доволі комплексним і може змінюватись в залежності від контексту. Попри те що виділення кібербезпеки як окремого напрямку забезпечення захисту суспільства і держави було вперше здійснено ще у 1987 році [1], вона все ще вважається молодою галуззю з глибокою історією. Не дарма тлумачення «кібербезпеки» доволі часто змінюються у відповідності до технологічного розвитку людства. Передумовою до цього є не лише самоочевидні чинники розвитку комунікаційних та обчислювальних засобів, а й розвиток суспільства як соціальної категорії, зростання ролі інформаційних технологій у повсякденному житті кожної людини та загальна низька підготовленість людства до викликів, які породжуються такими змінами.

Для уніфікації предмету дослідження будемо використовувати запропоноване Фурашевим В.М. [2] та розширене Барановим О.А. тлумачення поняття кібербезпеки як «такого стану захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації» [3] Відповідно, загрозами кібербезпеки (кіберзагрозам) може виступати будь-яке явище, дія чи подія, які можуть потенційно вплинути на зазначений стан.

Також важливо відмітити, що розвиток засобів забезпечення кібербезпеки на сьогодні є все ще доволі реактивним. Він в більшості випадків є відповіддю на виникнення та поширення різного роду кіберзагроз. Тому бажання змінити ситуацію і займати більш проактивну позицію щодо розвитку системи кібербезпеки спонукає багатьох дослідників займатись статистичним аналізом реалізованих кібератак та їх спроб. Метою таких досліджень є не лише вироблення розуміння засобів протидії загрозам, а й спроби виявити тенденції до їх розвитку в майбутньому. Накопичення та аналіз такого роду статистичних даних є критично важливим для покращення розуміння того які аспекти розвитку інформаційних технологій викликатимуть найбільше занепокоєння в майбутньому та завчасно підготуватись до їх викликів. Що відповідає і меті даного дослідження.

В світі дослідження тенденцій в розвитку кіберзагроз вже саме стає трендом і проводиться різноманітними організаціями починаючи від профільних [4, 5] і завершуючи фінансовими [6] та страховими [7] виданнями. Вони використовують різні критерії для оцінки впливу кіберзагроз на суспільство та оцінки потенційних ризиків які приносить такий вплив. Також слід відмітити спроби прогнозування майбутнього кібербезпеки [8] хоча вони мають здебільшого агітаційний характер і покликані звернути увагу на проблеми кібербезпеки ширшої аудиторії.

Аналіз і узагальнення статистичних звітів щодо динаміки розвитку кіберзагроз за 2022-23 роки є основним методом даного дослідження. Його результати дозволяють відмітити кореляцію між суттєвими змінами у спрямованості зловмисної діяльності та як новими технологічними інноваціями, так і модифікацією політичних і соціальних парадигм.

Результати дослідження та їхнє обговорення. Загальною тенденцією в сфері кібербезпеки, яка спостерігається вже багато років є систематичне зростання кількості кіберінцидентів, підвищення рівня забезпечення та підготовленості кіберзлочинців і, як наслідок, складності і комплексності кібератак. Об'єктивними чинниками для цього є збільшення кількості цифрових платформ що знаходяться у повсякденному користуванні людини, а також зростання частки населення що систематично використовує соціальні мережі. Адже, у сукупності з розвитком методів соціальної інженерії, це дозволяє зловмисникам простіше збирати необхідну інформацію про потенційну жертву та використовувати різні канали впливу на неї.

Аналіз кіберпростору компанією Positive Technologies [9] показав що експлуатація вразливостей становила значну частку (37%) успішних атак на організації, причому зловмисники здебільшого використовували недоліки в популярних IT-рішеннях. Шкідливе програмне забезпечення використовувалось у 45% випадків, але ми спостерігали зниження частки програм-вимагачів. Соціальна інженерія залишалася найбільшою (92%) загрозою для приватних осіб та основним (37%) вектором атак на організації. Більше половини організацій (56%) зазнали витоку даних у результаті успішних атак, а порушення основних бізнес-функцій становило 36%.

В цьому контексті важливо відмітити спрямованість застосування соціальної інженерії як засобу впливу на фізичних осіб та організації, а також механізм який допомагає інфільтрувати шкідливе програмне забезпечення в інформаційну систему. По суті, соціальна інженерія – це один з методів реалізації кібератак який ґрунтується не на використанні складних технологічних рішень для прокламування системи безпеки ззовні. Її особливістю є акцент на визначенні методу та форми впливу на людину, як найбільш слабку ланку будь-якої системи захисту і спонукання її до явного чи неявного порушення регламентів кібербезпеки.

Так спроби атак з використанням поштових сервісів (87%) продовжували найчастіше використовувати методи соціальної інженерії для впливу на організації, в той час як для впливу на фізичних осіб частка таких атак становила лише 27%. Водночас, атаки із застосуванням соціальної інженерії іншими каналами комунікації (веб-сайти, соціальні мережі, месенджери тощо) більше орієнтовані на фізичних осіб. В більшості випадків, це обґрунтовано тим, що організації які дбають про свою кібербезпеку використовують локальні мережі з надійним фаєрволом і для них поштові сервери які є частиною інформаційної системи організації все ще залишаються Ахіллесовою п'ятою.

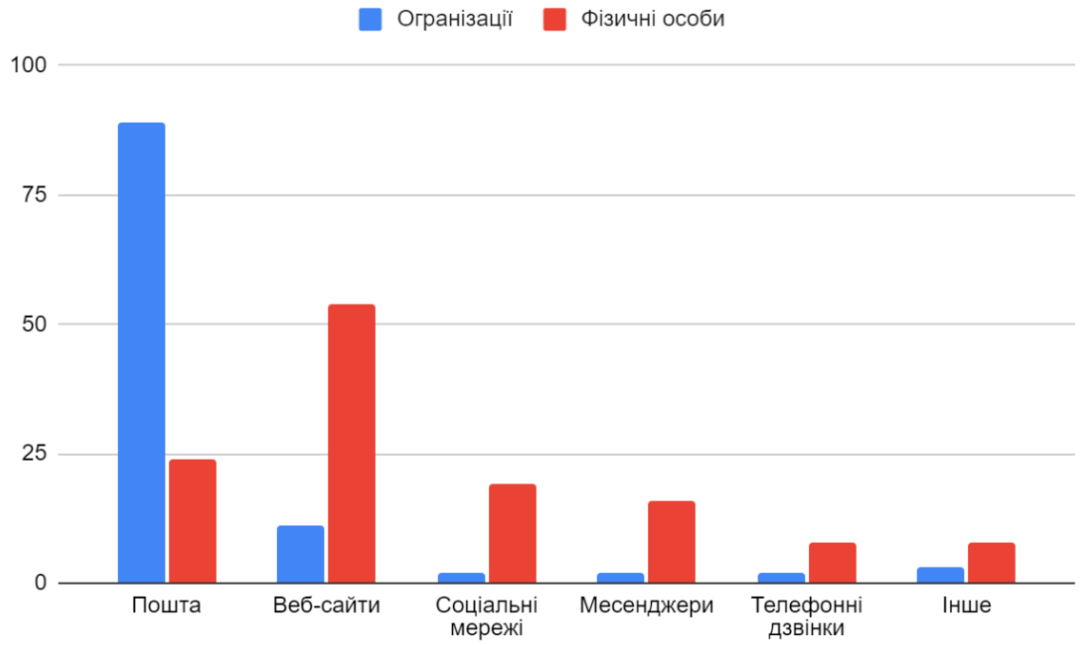

Рис. 1. Напрямки застосування соціальної інженерії для порушення кібербезпеки

Варто також звернути увагу на наявний аналіз успішних кібератак та їх спрямування. Так витік конфіденційних даних залишається найпоширенішим наслідком успішних атак на організації (56%) та приватних осіб (61%). Прямі фінансові втрати були другим за поширеністю наслідком (35%).

Для організацій третім найпоширенішим наслідком було порушення основних бізнес-функцій (36%). Попри значний відсоток ця частка суттєво зменшилася у порівнянні з 2022. Аналітики відмічають, що це пов'язано, в першу чергу, зі зниженням використання шифрування даних програмами-вимагачами. Причиною ж називають як покращення якості системної протидії такого типам загроз, так і зниження інтересу кіберзлочинців до такого виду діяльності, та концентрація саме на викраденні інформації, про що скажемо нижче.

На додачу до особистісного та корпоративного рівня кіберзагроз спостерігається суттєве зростання рівня загроз національній безпеці, які зорієнтовані на дестабілізацію соціальної обстановки та провокування конфліктів в середині суспільства. В Україні аналітики сходяться на думці, що кібервійна є лише продовженням конвенційних військових дій на полі бою. Проте в світовому масштабі відмічається неспроможність урядів ефективно захищати свій кіберпростір як технологічному так і в правовому контексті, що робить його важливим місцем для проведення кібероперацій для

державних спецслужб та афільованих з ними груп. Це, в свою чергу, призводить до зростання кількості кіберзлочинців які отримують державне фінансування – по суті зародження та бурхливий розвиток кіберкаперства.

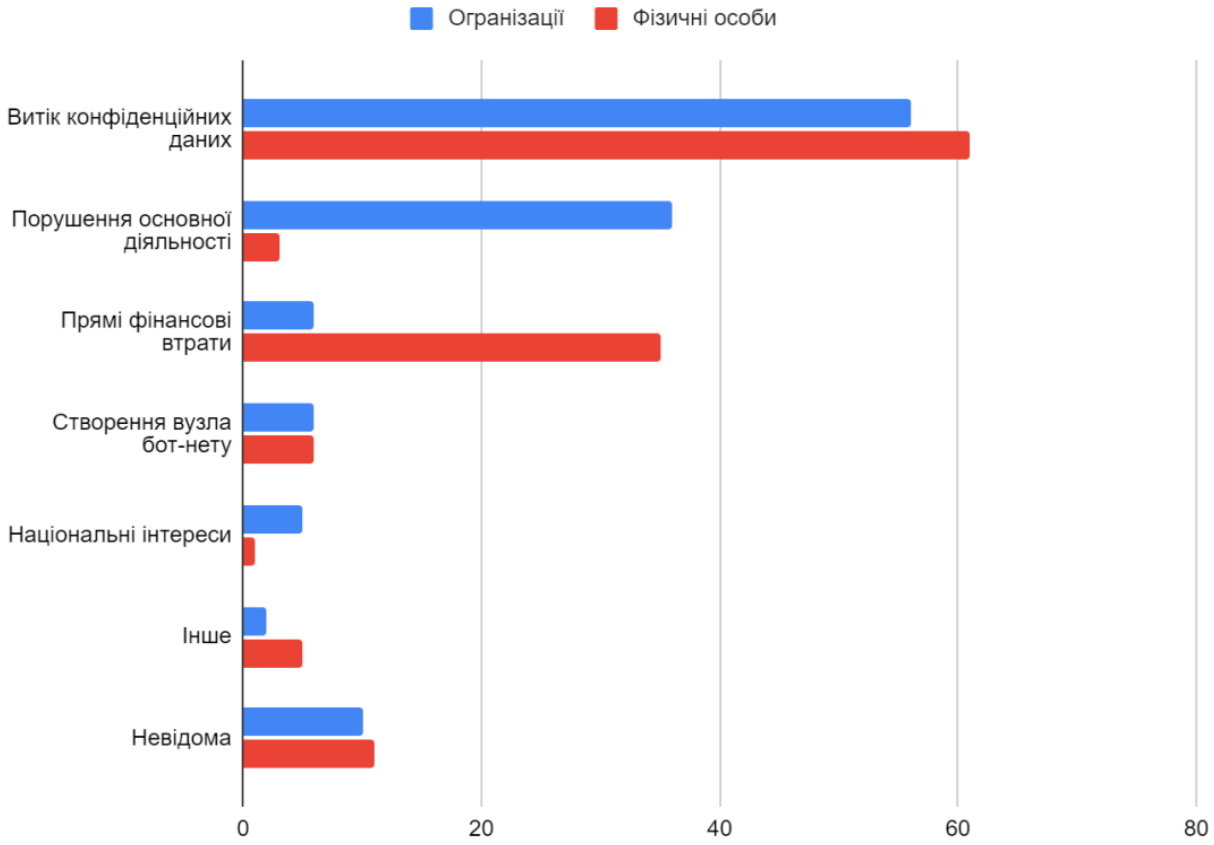

Рис. 2. Спрямованість успішних кібератак

Окремо для розуміння тенденцій у сфері кібербезпеки вартує відмітити дві ключові інновації, які мали вагомий вплив як на способи веденя кібероперацій, так і на засоби протидії їм.

Основною інновацією яка вплинула на сферу кібербезпеки стало представлення широкій публіці генеративних мовних моделей, які відобразили значний прогрес у розвитку штучного інтелекту. Хоч сама технологія не несе безпосередньої загрози кібербезпеці, вона може широко застосовуватись в удосконаленні та підвищенні ефективності методів соціальної інженерії та атак що використовують ці методи.

Похідним наслідком представлення штучних інтелектів (ШІ) також стрімкий розвиток та здешевлення апаратних рішень для їх навчання та підтримки, що зробило технологію більш доступною для широкого вжитку. Це, створило новий інструмент, який активно використовується обома сторонами в кібепротистоянні. Адже саме на штучний інтелект покладаються великі надії щодо здійснення моніторингу підозрілої активності мережевих за стосунків та користувачів.

Так компанія Cisco повідомляє, що на 2024 рік штучний інтелект отримав найбільше впровадження саме в моніторингу мережевої діяльності (40% від успішних впроваджень) та аналізу шифрованого трафіку. [8] Зокрема найвищі показники якості впровадження штучного інтелекту мають хост-брандмауери які забезпечують захист динамічного навантаження від вразливостей. Це може свідчити про потенційне

зниження ефективності DDOS-атак, так як штучний інтелект зможе ефективніше здійснювати відсікання підозрілого трафіку.

Проте, попри початок активного впровадження ШІ в процеси моніторингу кібербезпеки та протидії загрозам, можна стверджувати, що на сьогодні деструктивний вплив ШІ є вищим ніж конструктивний. А зважаючи на динаміку розвитку ШІ подолати цей розрив в найближчій перспективі буде важко. Якщо розглядати еволюцію протистояння в сфері кібербезпеки як класичну дилему еволюції розвитку щита і меча, то представлення та стрімке розповсюдження сфери застосування ШІ можна порівняти з появою вогнепальної зброї на полі бою. Попри те що поки існуючий захист все ще може виконувати свої базові функції для успішного протистояння атакам із застосуванням ШІ необхідно буде змінити не так засоби, як саму парадигму їх застосування.

Іншою технологічною інновацією, яка проте не мала такого публічного ефекту як ШІ стала демонстрація діючих квантових комп'ютерів, що ознаменувало відчутний прогрес у розвитку квантових обчислень. На відміну від ШІ, який сам по собі не несе безпосередньої загрози кібербезпеці, квантові комп'ютери першочергово орієнтовані саме на підпилювання одного з ключових стовпів кіберзахисту – шифрування даних. Тому їх представлення, актуалізувало і прискорило перехід до використання алгоритмів пост-квантової криптографії. Адже попри те, що теоретичні розробки та окремі стандарти в цій галузі існують вже певний час, стандартизація протоколів пост квантового шифрування і їх застосування в програмному забезпеченні до недавнього часу не отримало широкого вжитку.

Збільшення зацікавленості компаній-постачальників інформаційних послуг у впровадженні відповідних алгоритмів у свої продукти спричинило у 2023 році зміщення фокусу кібератак зі спроб отримання фінансової вигоди шляхом використання крипто вимагачів (падіння кількості успішних атак на 60%) [9] чи заволодіння фінансовою інформацією (падіння кількості успішних атак на 40%), на заволодіння корпоративною чи персональною інформацію що зберігається, навіть у зашифрованому вигляді (зростання кількості атак на понад 50%). Кіберзлочинці впроваджують на практиці методику SNDL (steal now decryp later) і намагаються заволодіти як найбільшою кількістю доступної інформації до завершення пост квантового переходу, щоб в майбутньому, при наявності більш доступних квантових комп'ютерів, мати можливість розшифрувати накопичені дані і отримати від них вигоду.

Висновки. Попри різноманітні прогнози та очікування сповільнення темпів розвитку інформаційних технологій, «кінця історії» все ще не трапилося і в найближчий час його очікувати не варто. Натомість стрімкий технологічний прогрес кидає нові виклики у сфері кібербезпеки зміщуючи акценти та розвертаючи тенденції її розвитку які спостерігались в 2015-2021 роках.

Нові можливості ШІ зорієнтовані на здійснення пошуку зв'язків і аналізу великої кількості інформації очікувано призведуть до зростання кількості і якості фішингових атак. Ця ж технологія може активно використовуватись для атак фальсифікації особистості, що, в свою чергу, актуалізує проблематику забезпечення надійної аутентифікації особи.

Зважаючи на особливості організації та функціонування відповідних програмно-апаратних рішень відбувається зростання кількості атак спрямованих на її знищення, а також підтримуючої інформаційної інфраструктури. Для протидії цьому активно розвиваються хмарні технології та інтеграція в них ШІ для моніторингу мережевого трафіку. Що, потенційно, може також знизити ефективність окремих видів кібератак.

Відновлення інтересу кіберзлочинців до заволодіння конфіденційною інформацією актуалізує необхідність у використанні надійних методів шифрування інформації не лише при її передачі через канали зв'язку, а й при її зберіганні в інформаційних системах.

Слід зважати на те, що на побутовому і значною мірою на корпоративному рівні соціальна інженерія залишається одним з ключових методів реалізації загроз кібербезпеці. Тому можна констатувати, що ми лише починаємо вивчати і системно розуміти закономірності функціонування кіберпростору, методів розповсюдження в ньому інформації та маніпулювання нею. А поява нових інструментів та засобів маніпулювання і генерації інформації лише ускладнює цей процес.

Бібліографія

1. The History of Cyber Security: A Detailed Guide URL: https://www.knowledgehut.com/blog/security/history-of-cyber-security (Дата звернення: 10.06.2024)
2. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності //Інформація і право. – 2012. – №. 2 (5). – С. 162-169. DOI: https://doi.org/10.37750/2616-6798.2012.2(5).271955
3. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» //Правова інформатика. – 2014. – Т. 2. – №. 42. – С. 54-62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf
4. Steve Morgan. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics URL: https://cybersecurityventures.com/cybersecurity-almanac-2023/ (Дата звернення: 10.06.2024)
5. Calibrating Expansion. 2023 Annual cybersecurity report URL: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/calibrating-expansion-2023-annual-cybersecurity-threat-report (Дата звернення: 10.06.2024)
6. Mariah St. John, Brenna Swanston Cybersecurity Stats: Facts And Figures You Should Know URL: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/ (Дата звернення: 10.06.2024)
7. Cyber security trends 2023. The latest threats and risk mitigation best practice – before, during and after a hack URL: https://commercial.allianz.com/news-and-insights/reports/cyber-security-trends-2023.html (Дата звернення: 10.06.2024)
8. 2024 Cisco Cybersecurity Readiness Index URL: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf (Дата звернення: 10.06.2024)
9. Cybersecurity threatscape: Q3 2023 URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/ (Дата звернення: 10.06.2024)

References

1. The History of Cyber Security: A Detailed Guide URL: https://www.knowledgehut.com/blog/security/history-of-cyber-security (Date of inquiry: 10.06.2024)
2. Furashev V.M. Cyber space and information space, cybersecurity and information security: essence, definitions, differences // Information and Law. – 2012. – No. 2 (5). – P. 162-169. DOI: https://doi.org/10.37750/2616-6798.2012.2(5).271955
3. Baranov O.A. On the interpretation and definition of the concept of "cybersecurity" // Legal Informatics. – 2014. – Vol. 2. – No. 42. – P. 54-62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf
4. Steve Morgan. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics URL: https://cybersecurityventures.com/cybersecurity-almanac-2023/ (Date of inquiry: 10.06.2024)
5. Calibrating Expansion. 2023 Annual cybersecurity report URL: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/calibrating-expansion-2023-annual-cybersecurity-threat-report (Date of inquiry: 10.06.2024)
6. Mariah St. John, Brenna Swanston Cybersecurity Stats: Facts And Figures You Should Know URL: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/ (Date of inquiry: 10.06.2024)
7. Cyber security trends 2023. The latest threats and risk mitigation best practice – before, during and after a hack URL: https://commercial.allianz.com/news-and-insights/reports/cyber-security-trends-2023.html (Date of inquiry: 10.06.2024)
8. 2024 Cisco Cybersecurity Readiness Index URL: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf (Date of inquiry: 10.06.2024)
9. Cybersecurity threatscape: Q3 2023 URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/ (Date of inquiry: 10.06.2024)