DOI: https://doi.org/10.26642/sas-2025-1(7)-63-74
УДК 351

Дикий Анатолій
доктор економічних наук, доцент
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0002-5819-0236

Савіцький Владислав
кандидат економічних наук
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0003-4475-523X

Савчук Сергій
здобувач
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0007-7436-0702

Соха Артур
аспірант
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0009-8060-8350

Світові тенденції кіберзлочинності та загрози інформаційній безпеці держав

Анотація. Ця стаття визначає актуальні світові тенденції кіберзлочинності та загрози інформаційній безпеці держав, що впливає не лише на внутрішній розвиток окремих країн, але й є визначальною глобальною загрозою сучасності, враховуючи трансформації кібератак та масовість їх здійснення. Аналіз сучасного стану кіберзлочинності дозволить краще зрозуміти її динаміку, сприятиме обміну досвідом між країнами та формуванню міжнародних механізмів співпраці.

Автори провели глобальне дослідження сучасного стану кіберзлочинності за певними критеріями. Зокрема, визначили частку користувачів мережі «Інтернет» в окремих країнах, які коли-небудь стикалися з кіберзлочинами у 2022 р. Цей аналіз засвідчив, що кіберзлочинність залишається глобальною загрозою, яка впливає на користувачів незалежно від їхньої географічної локації. Проведений аналіз найпопулярніших у світі кіберзлочинів у мережі «Інтернет» за 2017–2022 рр. показав, що фішингові атаки та несплата податків зустрічаються найчастіше в цифровому середовищі. У 2023 р. спостерігалося збільшення кількості випадків платіжного шахрайства. Крім того, протягом 2015–2023 рр. у світі зростає кількість атак, пов'язаних із використанням зловмисного програмного забезпечення. Було встановлено, що до лідерів серед секторів промисловості у світі, на які найбільше нападає зловмисне програмне забезпечення, в період з листопада 2022 р. по жовтень 2023 р. належить освітній, професійний та розважальний сектори. Визначено частку організацій, які постраждали від атак програм-вимагачів у всьому світі протягом 2018–2023 рр., що становить 72,7 %, і є найвищим показником за останні роки дослідження. Отже, аналіз цих та інших показників довів, що обсяг та частота кібератак постійно зростають, що є головною загрозою для національної та міжнародної безпеки, а тому боротьба з кіберзлочинністю є глобальним викликом та вимагає злагодженої взаємодії різних країн та міжнародних організацій. Задля мінімізації виникнення кіберзагроз потрібно налагодити комунікацію між усіма можливими об'єктами кіберзагроз, підвищити рівень досліджень, ефективність наявних інструментів протидії кіберзагрозам.

Ключові слова: кіберзлочинність; інформаційна безпека; кібератака; кіберзлочин; інформаційні технології; фішинг; шахрайство.

Постановка проблеми. В епоху цифровізації та швидкого поширення інтернет-технологій суспільство зіштовхнулося з новими загрозами у сфері безпеки та правопорядку. Кіберзлочинність стала однією з найбільших загроз сучасного світу, яка впливає на всі сфери діяльності: економіку, освіту,

охорону здоров'я та критичну інфраструктуру. Кіберзлочинності притаманний широкий діапазон різних загроз: від конкретних атак у мережі «Інтернет» до постійних злочинів щодо фінансових систем і ресурсів державних структур та населення загалом. Трансформація кібератак та масовість їх здійснення стали головною темою для обговорення на міжнародному рівні та вимагають нових зусиль щодо їх попередження та усунення. Вивчення статистичних даних дозволяє не лише оцінити поточний стан кіберзлочинності, а й прогнозувати її розвиток, визначати вразливі сфери та розробляти ефективні стратегії захисту. Глобальний аналіз поширеності кіберзлочинності сприяє кращому розумінню динаміки злочинності, обміну досвідом між країнами та створенню міжнародних механізмів співпраці.

Аналіз останніх досліджень і публікацій. Дослідження щодо кіберзлочинності та загрози інформаційній безпеці здійснювали як вітчизняні, так і зарубіжні науковці: В.В. Аніщук, Р.В. Бараненко, О.А. Баранов, Ю.Бельській, В.Горлинський, Б.Горлинський, Д.О. Грицишен, В.В. Євдокимов, В.С. Павленко та інші. Проте вважаємо за доцільне розглянути більш детально світові тенденції кіберзлочинності та загрози інформаційній безпеці держав.

Мета статті полягає у дослідженні світових тенденцій кіберзлочинності та загроз інформаційній безпеці держав.

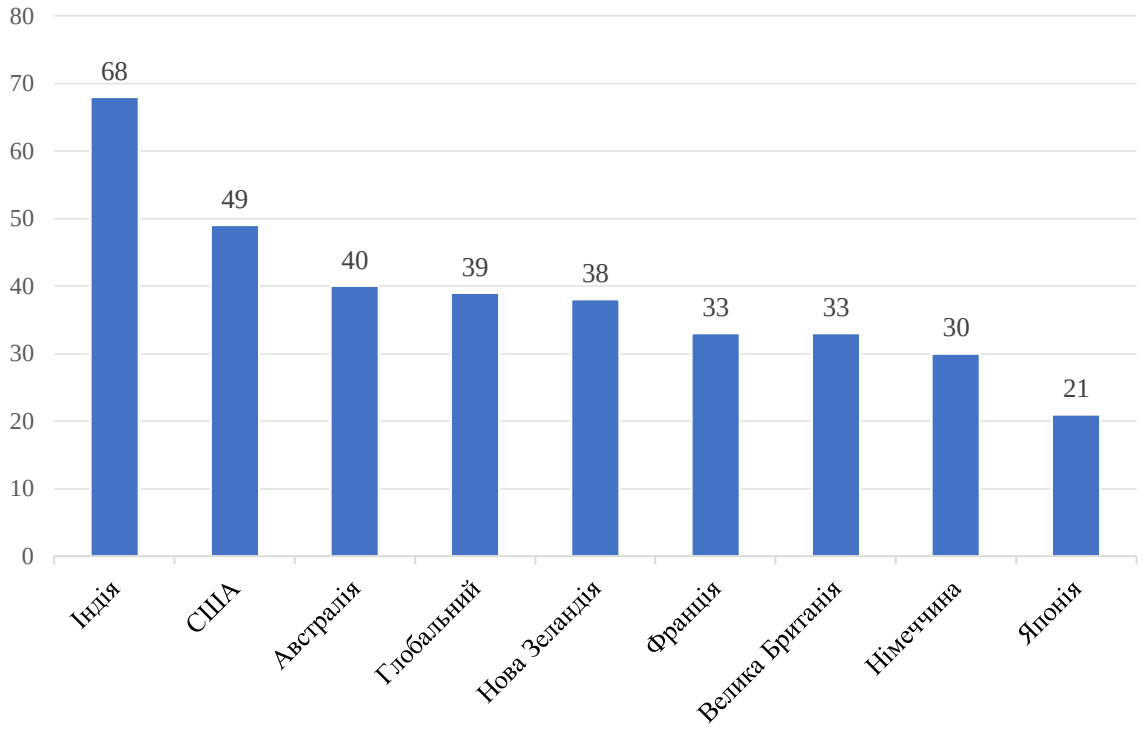
Викладення основного матеріалу. Інформаційні технології щодня змінюються зі стрімкою швидкістю, а саме: хмарні сервіси, блокчейн, Інтернет-речі. Це створює додаткові вразливі місця для злочинів щодо здійснення нових кібератак як в професійних, так і в особистих мережах. Кіберзлочинність може набувати різних форм: шахрайство з особистими даними, викрадення даних, атаки програм-вимагачів, кібератаки на критичну інфраструктуру або ж фішингові кампанії тощо.

Експерти німецької онлайн-платформи *Statista* оцінюють глобальні втрати від кіберзлочинів у 7,1 трлн дол. США у 2022 р. порівняно з 1,2 трлн дол. США у 2019 р. При цьому, згідно з даними *Chainalysis,* у 2021 і 2022 рр. різко зросли кібератаки на криптовалютні біржі та протоколи, зокрема з боку північнокорейської хакерської групи Lazarus, афілійованої з державою [5]. Згідно з дослідженнями, проведеними експертами антивірусної компанії McAfee разом із Центром стратегічних та міжнародних досліджень, глобальні збитки від хакерських атак щорічно становлять у середньому 600 млрд дол. США [4].

Світові організації вважають втрату особистої інформації клієнтів або співробітників одним із найнебезпечніших наслідків кібератак. Втрата конфіденційної інформації може мати серйозні наслідки для компаній, наприклад, призвести до погіршення репутації та збитків від недоотриманого прибутку. Криза COVID-19 призвела до того, що багато організацій зіткнулися з більшою кількістю кібератак через вразливість безпеки віддаленої роботи, а також через перехід до віртуалізованих IT-середовищ, таких як: інфраструктура, дані та мережа хмарних обчислень.

Дослідження, проведені у 2022 р. компанією PwC (PricewaterhouseCoopers), міжнародною мережею професійних послуг, показали високий рівень кіберзлочинності в світі. Зокрема, Індія має найвищий відсоток користувачів, які стали жертвами кіберзлочинів (68 %), тоді як у Сполучених Штатах цей показник становить 49 %. Це свідчить про те, що кіберзлочинність залишається глобальною загрозою, яка впливає на користувачів незалежно від їхньої географічної локації. З огляду на це, важливо підвищувати рівень обізнаності та захищеності користувачів в інтернеті, вдосконалювати кібербезпекові заходи та змінювати політику для запобігання цифровим атакам (рис. 1).

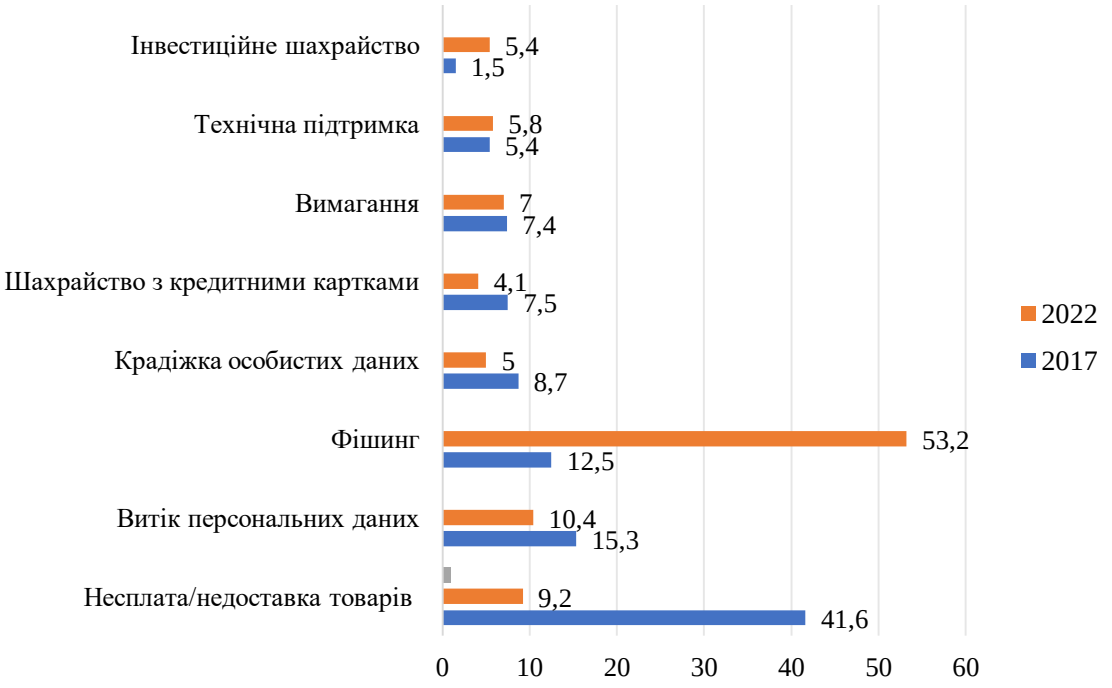
Слід зазначити, що фішингові атаки, які у 2022 р. становили більше половини всіх кіберзлочинів (53,2 %), є одними із найпоширеніших методів обману в цифровому середовищі. Їхня популярність пояснюється простою реалізацією та високою ефективністю введення жертви в оману для отримання конфіденційної інформації, такої як: паролі, дані кредитних карток або іншої чутливої інформації. Фішинг, зокрема, може здійснюватися через електронні листи, підроблені вебсайти чи повідомлення у соціальних мережах, що сприяє підвищенню уваги з боку користувачів і впровадження профілактичних заходів, таких як двофакторна аутентифікація.



Джерело: сформовано на основі [3]

Рис. 1. Частка користувачів мережі «Інтернет» в окремих країнах, які коли-небудь стикалися з кіберзлочинами у 2022 р., %

Водночас, хоча інвестиційне шахрайство залучає найменшу кількість учасників (5,4 %), його наслідки можуть бути особливо руйнівними. Обман інвесторів, пов'язаний із неправдивою інформацією щодо надання акцій, зобов'язань чи інших фінансових інструментів, завдає шкоди не лише окремим особам ринку, а й фінансовій стабільності в цілому. Крім спричинення матеріальних втрат, такі злочини підривають довіру до фінансових установ і ринкових механізмів. Це вимагає посилення регуляторного контролю, вдосконалення системи виявлення шахрайства та підвищення фінансової грамотності серед громадян, що є головними завданнями під час боротьби з подібними злочинами.

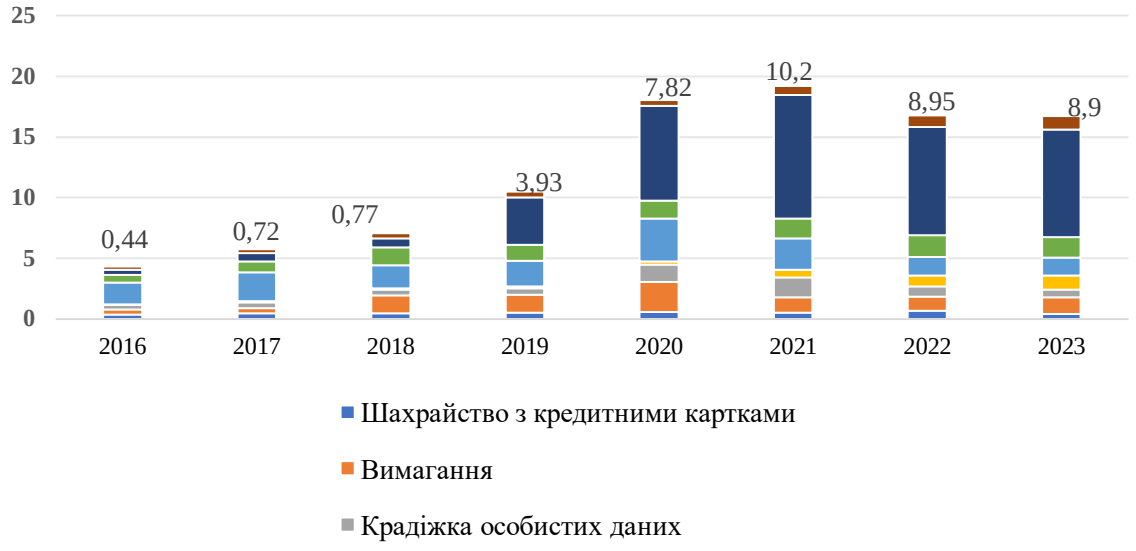


Джерело: сформовано на основі [6–8]

Рис. 2. Найпопулярніші кіберзлочини в мережі «Інтернет» у світі, 2017–2022 рр., %

Слід зазначити, що у 2017 р. лідером серед кіберзлочинів була несплата або ж недоставка товарів, проте за останні роки ситуація дещо змінилася, і у 2022 р. найпопулярнішими кібератаками стали фішингові атаки (рис. 2), їхня кількість становила понад 53,2 % від загальної частки всіх кіберзлочинів. Найменшу частку при цьому займає інвестиційне шахрайство, яке становить 5,4 % від загальної частки кіберзлочинів, що по суті є обманом, який змушує інвесторів ухвалювати рішення про купівлю або ж продаж цінних паперів на основі неправдивої інформації, наслідком таких дій є порушення чинного законодавства та матеріальні втрати.

Кіберзлочини з кожним роком набувають нових видів та форм, вони швидко адаптуються до технологічних змін. На рисунку 3 наведено показники кібератак, здійснених протягом 2016–2023 рр. у розрізі їх видів.

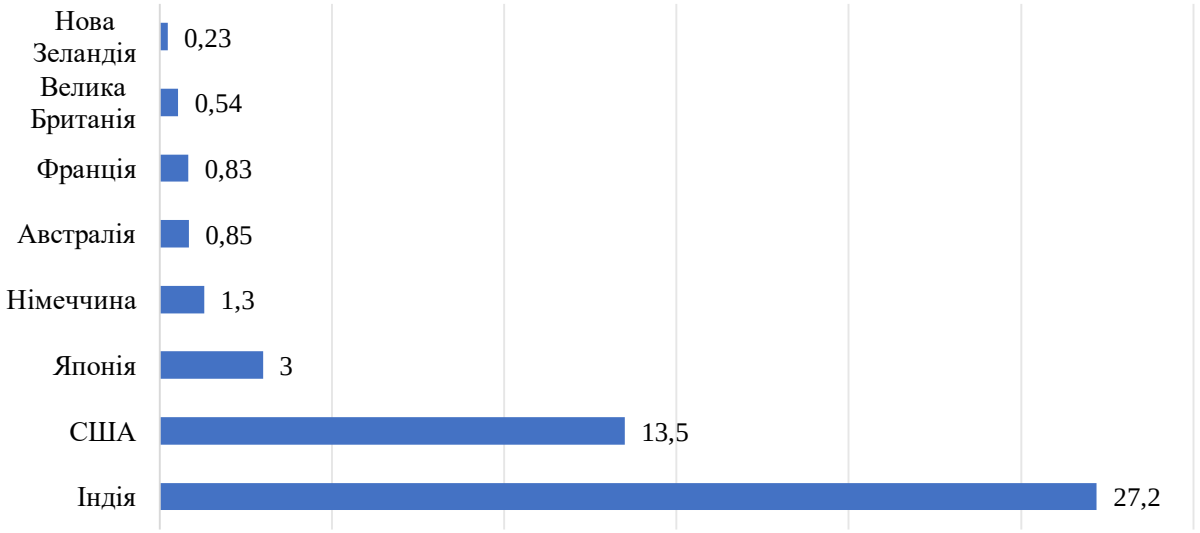


Джерело: сформовано на основі [9]

Рис. 3. Динаміка кібератак у світі в розрізі їх видів, 2016–2023 рр., млн шт. [1]

Протягом досліджуваного періоду стає помітно, що фішингові атаки мають найбільшу тенденцію до розповсюдження у глобальному просторі. Так у 2023 р. було зафіксовано більше ніж 9 млн випадків атак у світі, а вже у першому кварталі 2024 р. кількість унікальних фішингових сайтів становила понад 1 млн. Друге місце посідає такий вид кіберзлочинності, як порушення персональних даних, їх кількість у 2022 р. становила понад 1,66 млн кіберінцидентів. На третьому місці знаходиться недоставка або несплата товарів, що трапляється у 1,5 млн випадків. За допомогою підробленого листування, яке надходить на електронну пошту або в соціальні мережі, жертв фішингу спрямовують на перехід до спеціально створених фішингових сайтів. Ці сайти збирають персональні дані користувачів, які згодом використовуються для онлайн-шахрайства або викрадення особистої інформації. Крім того, посилання в таких підроблених повідомленнях нерідко слугують точкою доступу для проникнення зловмисного програмного забезпечення в систему.

Дослідження, проведені компанією PwC у 2022 р. серед респондентів у вибраних країнах, які коли-небудь ставали жертвами крадіжки особистих даних, свідчать, що Індія стала лідером серед досліджуваних держав – дані понад 27,2 млн дорослих були вкрадені зловмисниками (рис. 4). Наступною країною за кількістю потерпілих від втрати даних є Сполучені Штати Америки (орієнтовно 13,5 млн осіб). На третьому місці знаходиться Японія, де показник жертв крадіжки особистих даних становить понад 3 млн випадків [3].

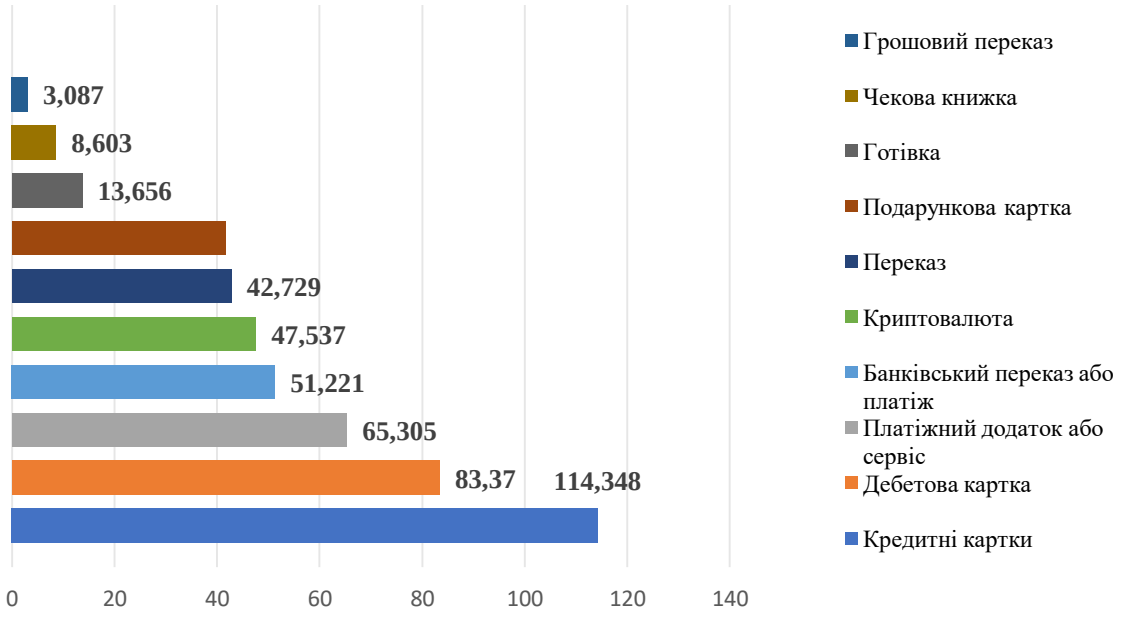


Джерело: сформовано на основі [3]

Рис. 4. Кількість дорослих, які стали жертвами крадіжки персональних даних у 2022 р., млн осіб [2]

У 2023 р. шахрайства, пов'язані з платежами, були основними загрозами у кіберпросторі. Значна частина таких злочинів була спрямована на крадіжку платіжних даних через електронні гаманці, банківські рахунки або використання скімінгових пристроїв. Одним із поширених методів є соціальна інженерія, яка надає можливість зловмисникам шляхом обману змусити жертву розкрити банківські реквізити або підтвердити транзакції. У 2023 р. значне зростання таких злочинів було зафіксовано в електронній комерції.

Крім того, активізувалися атаки, спрямовані на компанії, які обробляють великий обсяг платіжних операцій. Зловмисники використовують методи зламування систем, які забезпечують електронні платежі, для вилучення коштів або компрометації даних клієнтів. Така діяльність створює значні ризики не тільки для компаній, але й для споживачів, які стикаються з фінансовими втратами та порушенням конфіденційності. Враховуючи ці тенденції, боротьба з платіжним шахрайством у 2023 р. вимагала підвищення рівня кібербезпеки у всіх сферах, а також впровадження технологій штучного інтелекту для виявлення аномалій у транзакціях, покращення шифрування даних і посилення законодавчих заходів. На рисунку 5 наведено показники шахрайства, пов'язані з платежами у 2023 р.

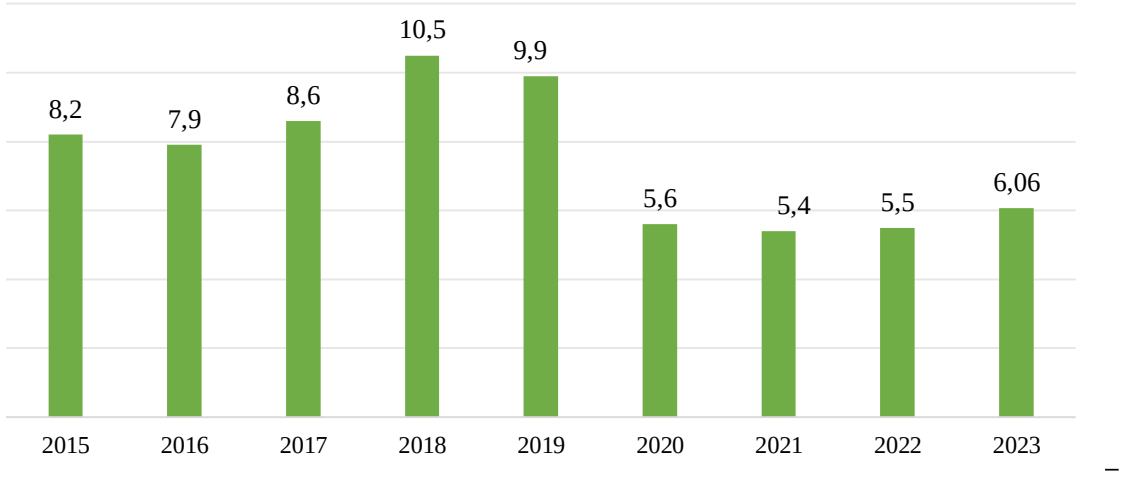


Джерело: сформовано на основі [10]

Рис. 5. Динаміка кількості випадків шахрайства, пов'язана з платежами у 2023 р., тис. одиниць

Ключовими чинниками збільшення кількості платіжного шахрайства є поширення методів соціальної інженерії, фішингових атак та використання вразливостей у цифрових платіжних системах. Зростання обсягів онлайн-транзакцій під час пандемії COVID-19 також сприяло активізації шахрайства. У 2023 р. було найбільше зафіксовано повідомлень про шахрайство з кредитними картками – близько 114 348 тис. випадків. На другому місці були звернення щодо шахрайства з дебетовими картками, а на третьому – випадки шахрайства, пов'язані з платіжними додатками.

На рисунку 6 наведено показники атак із використанням зловмисного програмного забезпечення у світі протягом 2015–2023 рр.



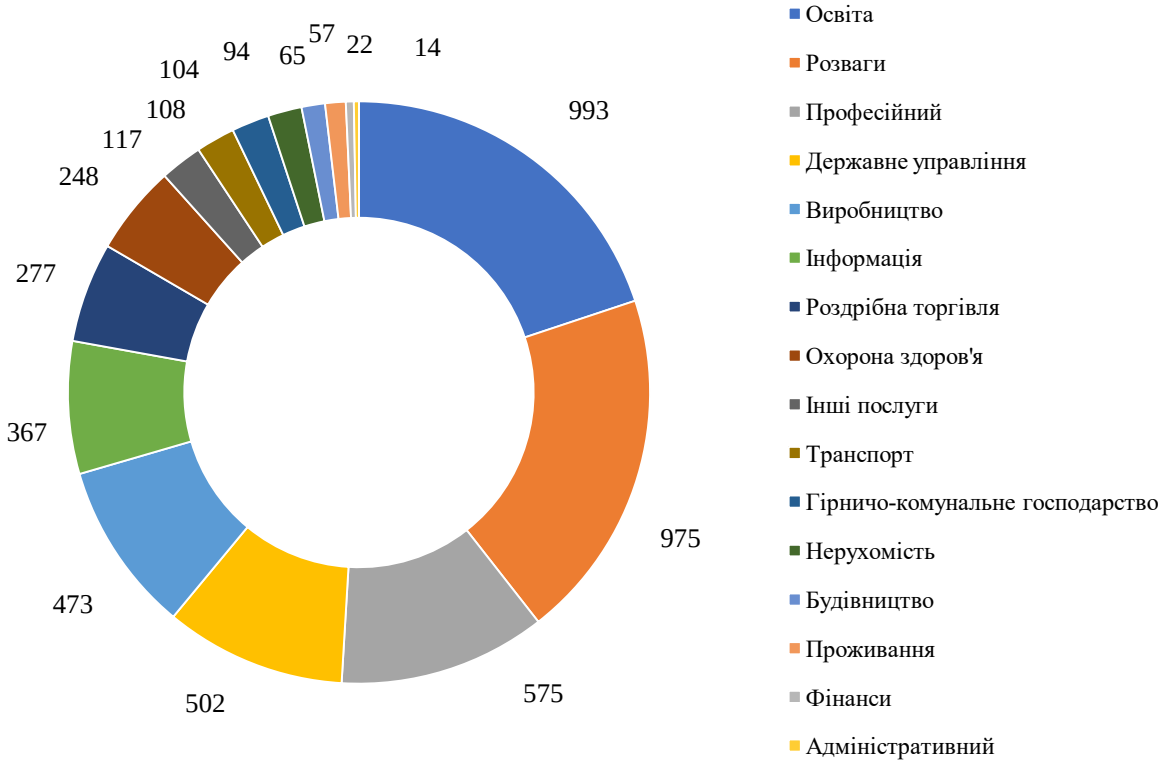
Джерело: сформовано на основі [11]

Рис. 6. Динаміка атак із використанням зловмисного програмного забезпечення у світі, 2015–2023 рр., тис. одиниць

У 2023 р. кількість атак із використанням зловмисного програмного забезпечення у світі зросла на 10 % порівняно з попереднім роком, досягнувши 6,06 млрд випадків. Найбільший сплеск атак було зафіксовано в 2018 р., коли їхня кількість сягнула 10,5 млрд по всьому світу. У 2023 р. найбільше постраждав освітній сектор, який зазнавав у середньому 2046 атак на тиждень, що трохи менше ніж 2314 атак у попередньому році. На другому місці опинились урядові та військові організації, а за ними –

медичні установи. Загалом у 2022 р. освітня галузь зазнала понад п’ять мільйонів атак із використанням зловмисного програмного забезпечення [6–9].

Згідно з дослідженням SonicWall Capture Labs [11], у першій половині 2024 р. кількість атак із використанням зловмисного програмного забезпечення для Інтернету речей (IoT) зросла на 107 %. Пристрої, які зазнали кібератак, перебували під загрозою в середньому 52,8 години. На рисунку 7 представлені сектори промисловості у світі, які найбільше зазнавали атак зловмисного програмного забезпечення в період з листопада 2022 р. по жовтень 2023 р.

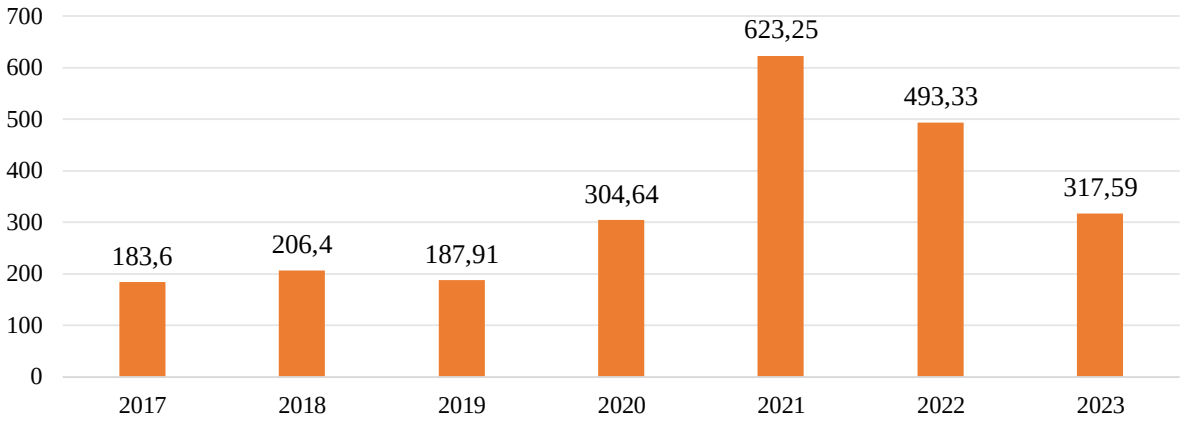


Джерело: сформовано на основі [10]

Рис. 7. Сектори промисловості у світі, які найбільше зазнавали атак зловмисного програмного забезпечення, листопад 2022 р.–жовтень 2023 р., тис. одиниць

У період з листопада 2022 р. по жовтень 2023 р. освітній сектор посів перше місце серед глобальних галузей, які найбільше піддаються атакам зловмисного програмного забезпечення. За досліджуваний період в галузі сталося більше ніж 993 інциденти кібератак. Друге місце посів сектор розваг – понад 975 інцидентів, а професійний сектор займає третє місце з 575 виявленими атаками зловмисного програмного забезпечення.

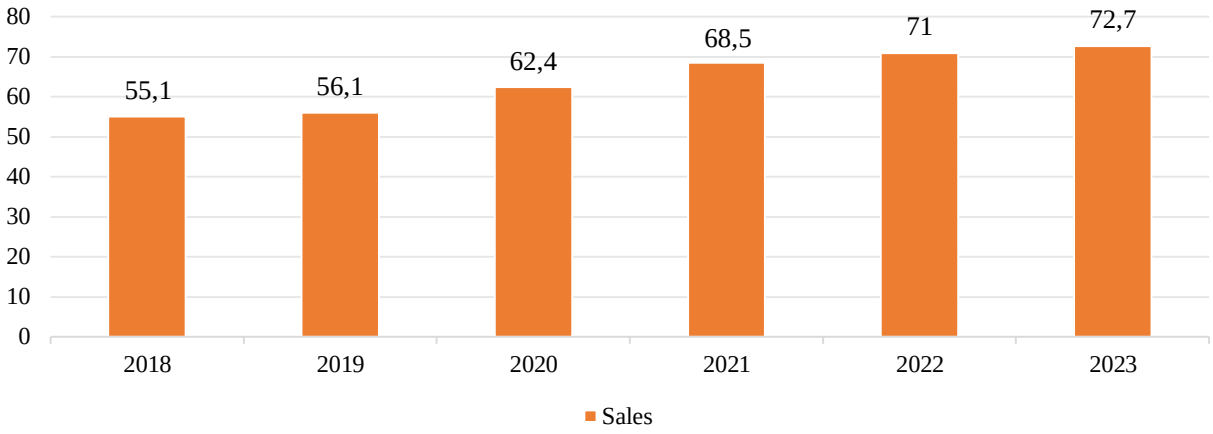
У 2023 р. організації в усьому світі зафіксували понад 317,59 млн спроб атак програм-вимагачів (рис. 8), що на 175,74 млн спроб менше ніж у попередньому році. Атаки програм-вимагачів зазвичай спрямовані на організації, які збирають великі обсяги даних і є критично важливими. У разі атаки ці організації вважають за краще заплатити викуп за відновлення вкрадених даних, ніж негайно повідомити про атаку. Випадки втрати даних також завдають шкоди репутації компаній, що є однією з причин, чому не повідомляється про атаки програм-вимагачів.



Джерело: сформовано на основі [12]

Рис. 8. Динаміка спроб атаки програм-вимагачів у світі, 2017–2023 рр., тис. одиниць

На рисунку 9 зображено частку організацій, які постраждали від атак програм-вимагачів у всьому світі протягом 2018–2023 рр.

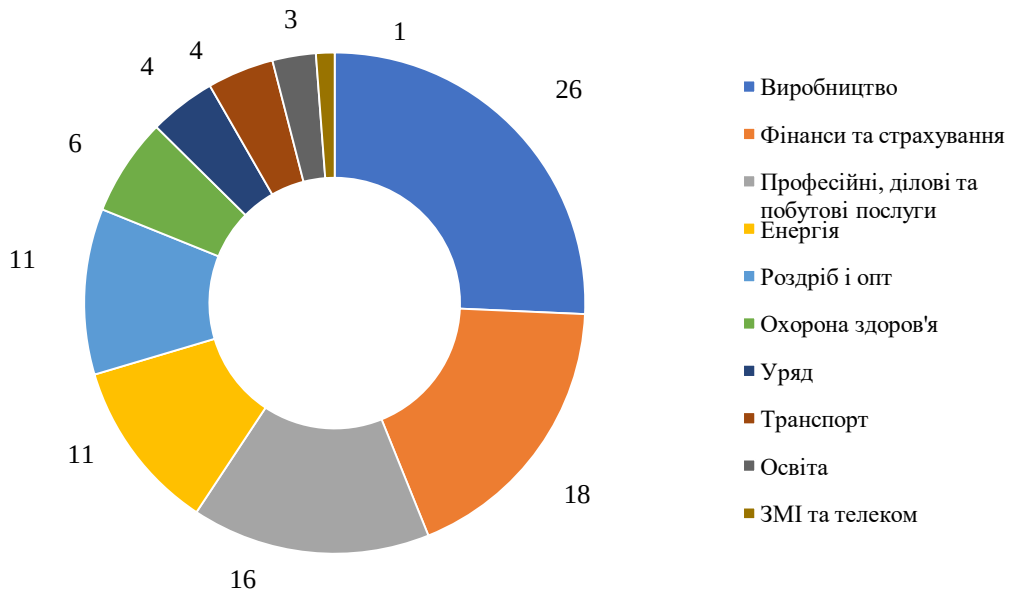


Джерело: сформовано на основі [12]

Рис. 9. Частка організацій, які постраждали від атак програм-вимагачів у всьому світі, 2018–2023 рр., %

Станом на 2023 р. понад 72,7 % компаній у всьому світі постраждали від атак програм-вимагачів. Цей показник демонструє зростання порівняно з попередніми п'ятьма роками досліджень і є, безумовно, найвищим зафіксованим значенням. Загалом, починаючи з 2018 р., більше половини респондентів щороку заявляли, що їхні організації стали жертвами програм-вимагачів.

На рисунку 10 наведено показники розподілу кібератак серед світових галузей у 2023 р.

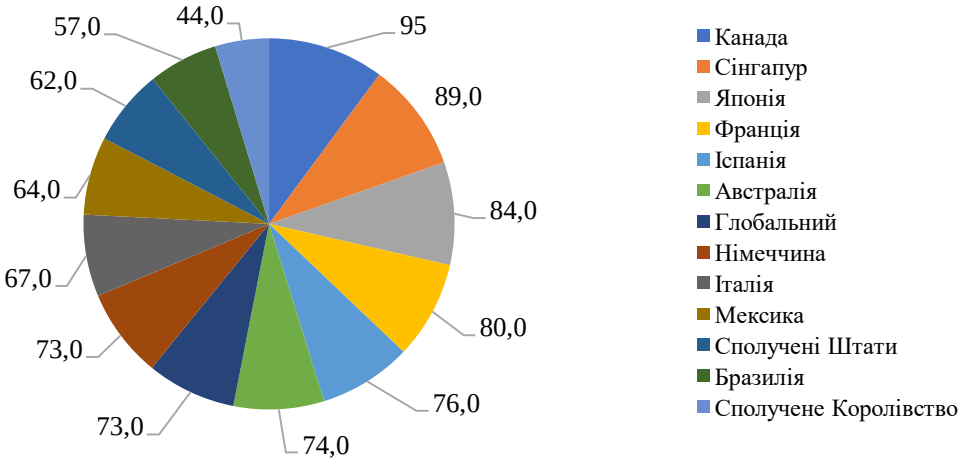


Джерело: сформовано на основі [13–15]

Рис. 10. Розподіл кібератак у світових галузях в 2023 р., %

Найбільша частка зафіксованих кібератак серед світових галузей у 2023 р. стосувалася сфери виробництва. Протягом досліджуваного року компанії-виробники зіткнулися з майже чвертю від загальної кількості кібератак. На другому місці опинилися фінансові та страхові організації, що зазнали близько 18 % кібератак. Професійні, ділові та споживчі послуги посідають третє місце з 15,4 % зареєстрованих кібератак.

На рисунку 11 зображено частку організацій у різних країнах світу, яким загрожує кібератака, станом на червень 2023 р.

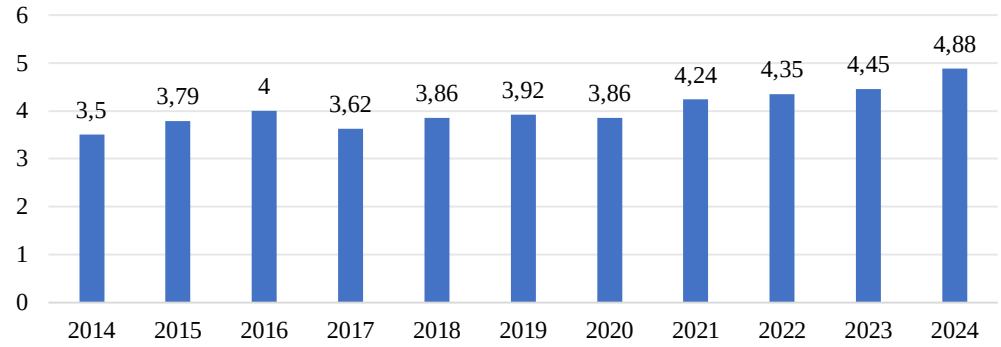


Джерело: сформовано на основі [15]

Рис. 11. Частка організацій у різних країнах світу, яким загрожує кібератака, станом на червень 2023 р., %

Серед досліджених країн світу, яким загрожують кібератаки різного виду, найбільш вразливою є Канада, понад 95 % її організацій перебували під серйозною загрозою кібератак. У Сінгапурі більшість опитаних членів правління (понад 89 %) вважали, що їхні компанії зіткнуться з таким ризиком протягом наступного року. Японські компанії опинилися на третьому місці за рівнем занепокоєння щодо можливості загрози нових кіберзлочинів – близько 84 % респондентів.

На рисунку 12 наведено середню вартість збитків від витоку даних у світі.

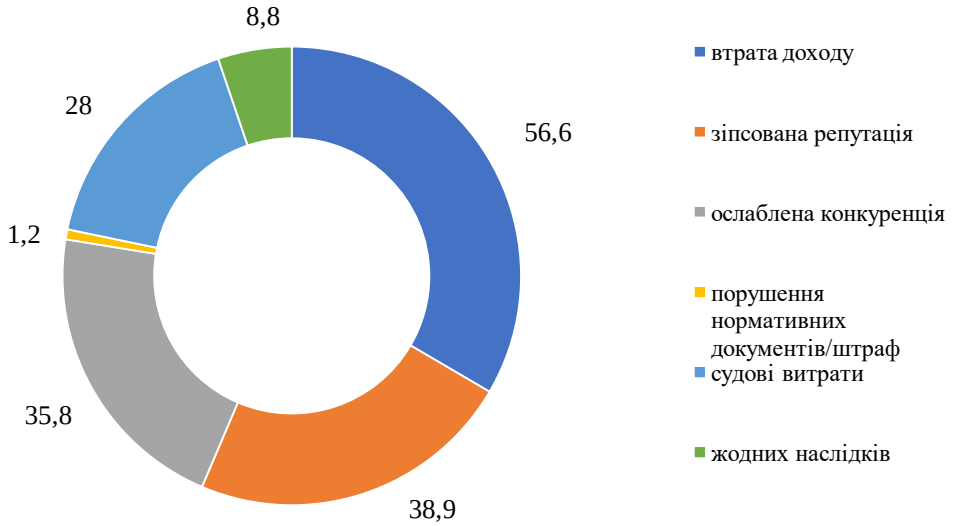


Джерело: сформовано на основі [15]

Рис. 12. Середня вартість збитків від витоку даних у світі, з 2018 р. по лютий 2024 рр., млр дол. США

Щорічно показник середньої вартості збитків від витоку даних збільшується. Так у 2023 р. розмір завданих збитків становив близько 4,45 млрд дол. США, а вже на кінець лютого 2024 р. – оцінювався в 4,88 млрд дол. США. Витік даних має жахливі фінансові наслідки, адже вони впливають як на окремих осіб, так і на організації, компанії та державні установи в цілому.

На рисунку 13 відображено наслідки втрати конфіденційної інформації для організацій у світі у 2023 р.

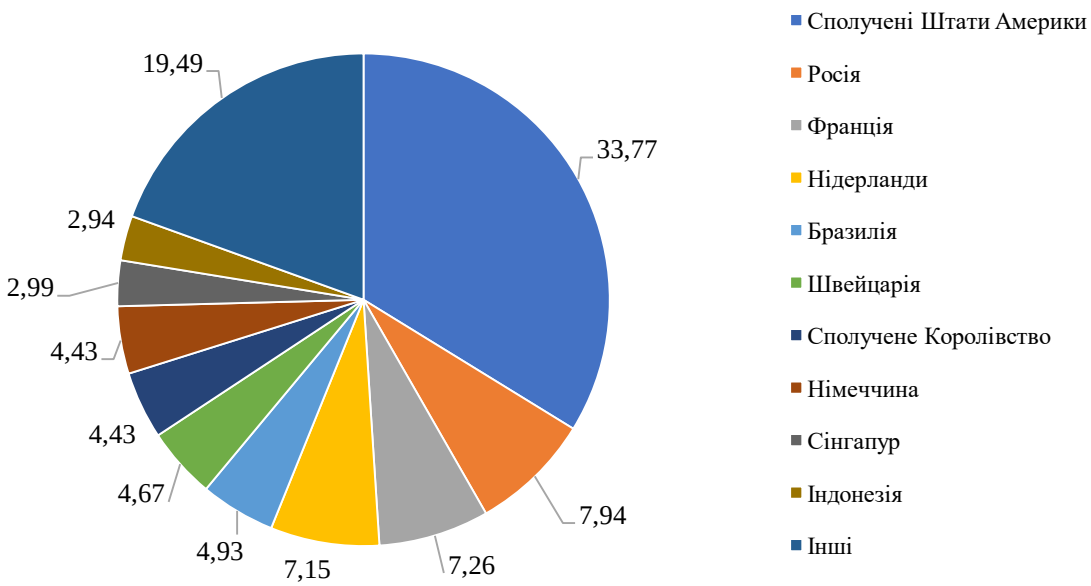


Джерело: сформовано на основі [15]

Рис. 13. Наслідки втрати конфіденційної інформації для організацій у світі у 2023 р., %

Серед найпоширеніших наслідків втрати конфіденційної інформації для організацій у світі в 2023 р. найбільшу частку становила втрата доходу – понад 56,6 % від загальної структури. На другому місці опинилися зіпсована репутація компаній (38,9 %) та послаблення конкуренції (35,8 %).

Сполучені Штати Америки станом на жовтень 2023 р. стали лідерами за кількістю джерел фінансування кібератак (рис. 14), забезпечуючи понад 33,7 % від загальної частки атак у світі. Причиною цього явища є розміщення великої кількості серверів для інтернет-користувачів у США. На другому місці знаходиться росія, її частка становить 7,94 %, а третє місце ділять Франція – 7,26 % та Нідерланди – 7,15 %.



Джерело: сформовано на основі [15]

Рис. 14. Розподіл джерел кібератак у світі з листопада 2022 р. по жовтень 2023 р. за країнами

Висновки. Отже, на основі проведеного аналізу глобального стану кіберзлочинності можна зробити такі висновки: кількість здійсненних кібератак щорічно зростає, а їх характер дедалі стає складнішим. Фішингові атаки є лідерами серед кіберзлочинів у світі, які демонструють тенденцію до подальшого збільшення. У 2023 р. кількість атак із використанням зловмисного програмного забезпечення становила 6,06 млрд випадків, що свідчить про масштабність проблеми. Глобальні фінансові втрати від кіберзлочинності у 2023 р. склали понад 7,1 трлн дол. США, а до 2029 р. можуть зрости до 15,63 трлн дол. США. Основними наслідками для організацій від втрати конфіденційної інформації є: втрата доходу (56,6 %), погіршення репутації (38,9 %) та послаблення конкурентних позицій (35,8 %). Найбільш вразливими залишаються освітній сектор, урядові структури, сектор розваг та фінансові установи. У цих галузях є значна кількість інцидентів із використанням зловмисного програмного забезпечення. США, росія, Франція та Нідерланди є основними країнами-джерелами кібератак, тоді як Канада та Сінгапур демонструють найвищий рівень непокоєння щодо можливих загроз.

Доведено, що боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Зокрема, діяльність таких міжнародних інституцій, як Інтерпол та Європол, є одним із найефективніших засобів протидії кіберзлочинності на міжнародному рівні. Встановлено, що захист від кіберзагроз залежить від усвідомлення всіх учасників цифрового простору того, що забезпечення безпеки є спільною відповідальністю. Відсутність обміну інформацією про кібератаки між державними організаціями, приватними підприємствами, бізнесом та фізичними особами, а також нестача глибоких досліджень, ефективних інструментів протидії та організованих консультацій значно підвищують ризик виникнення кіберзагроз. Для протистояння хакерським діям необхідна тісна співпраця між компаніями, організаціями та урядовими структурами, зокрема у сфері обміну інформацією про загрози та новітні методи захисту. Крім того, впровадження освітніх програм з кібербезпеки для широкої аудиторії сприятиме підвищенню рівня свідомості користувачів і зниженню ризиків, пов’язаних із людським фактором.

References :

1. Baranov, O.A. (2014), «Pro tlumachennia ta vyznachenni poniattia «kiberbezpeka»», *Pravova informatyka*, No. 2 (42), pp. 54–62.
2. Belskii, Yu. (2014), «Shchodo vyznachennia poniattia kiberzlochynu», *Yurydychnyyi visnyk*, Vol. 2014/6, pp. 414–418.
3. «Vsesvitnii ohliad ekonomichnykh zlochyniv», [Online], available at: https://www.pwc.com/ua/uk/Україна
4. Analytics CyberHubs, [Online], available at: https://data.cyberhubs.eu/
5. *Statista*, «Cyber incidents targeting governments global by attack vector 2023», [Online], available at: https://www.statista.com/statistics/1428581/government-worldwide-targeted-cyber-incidents-by-attack-vector/
6. *eSentire*, «Cybercrime to Cost the World $9.5 Trillion USD Annually In 2024», [Online], available at: https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in 2024?utm_medium=email& utm_source=pardot&utm_campaign=autoresponder

7. *Council of the EU*, «Cybersecurity package: Council adopts new laws to strengthen cybersecurity capacities in the EU», [Online], available at: https://www.consilium.europa.eu/en/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/
8. *European Commission*, «Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres», [Online], available at: https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-border-security
9. *ITU DataHub*, «The worldâs richest source of ICT statistics and regulatory information», [Online], available at: https://datahub.itu.int/dashboards/idi/?y=2024&e=UKR
10. *ITU Publication*, «Global Cybersecurity Index 2024», [Online], available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
11. *European Commission*, «LAB – FAB – APP», [Online], available at: https://data.europa.eu/doi/10.2777/477357
12. *StatPlanet*, «EC-OECD STIP Compass», [Online], available at: https://stip.oecd.org/stats/SB-StatTrends.html?i=TOP10_X&v= 3&t=2006,2020&s=UKR
13. *European Commission*, «The Digital Markets Act», [Online], available at: https://digital-markets-act.ec.europa.eu/index_en
14. *European Commission*, «The Digital Services Act», [Online], available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
15. *European Commission*, «The EU Cyber Solidarity Act», [Online], available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

---

Dykyi A., SavitskyiV., Savchuk S., Sokha A.

Global trends in cybercrime and threats to the information security of states

Abstract. This article identifies current global trends in cybercrime and threats to the information security of states, which affect not only the internal development of individual countries, but also constitute a defining global threat of our time, taking into account the transformation of cyberattacks and the mass nature of their implementation. An analysis of the current state of cybercrime will allow us to better understand its dynamics, contribute to the exchange of experience between countries and the formation of international cooperation mechanisms.

The authors conducted a global study of the current state of cybercrime according to certain criteria. In particular, they determined the share of Internet users in individual countries who had ever encountered any cybercrimes in 2022, this analysis showed that cybercrime remains a global threat that affects users regardless of their geographical location. An analysis of the most popular cybercrimes on the Internet in the world for 2017-2022 showed that phishing attacks and tax evasion are most common in the digital environment, the authors presented the dynamics of the number of fraud cases related to payments in 2023 is characterized by an increase in the number of payment fraud, in addition, the dynamics of malware attacks in the world during 2015-2023 is growing. It was found that the leaders of the industry sectors in the world that are most attacked by malware during November 2022 - October 2023 include the educational, entertainment and professional sectors. The share of organizations affected by ransomware attacks worldwide during 2018-2023 was determined, which is 72.7%, which is the highest figure in recent years of the study. Thus, the analysis of these and other indicators has proven that the volume and frequency of cyberattacks is constantly growing and poses a key threat to national and international security, and therefore the fight against cybercrime is a global challenge and requires coordinated interaction between different countries and international organizations. In order to minimize the occurrence of cyberthreats, it is necessary to establish communication between all possible objects of cyberthreats, increase the level of research, the effectiveness of existing tools for countering cyberthreats.

Keywords: cybercrime; information security; cyberattack; cybercrime; information technologies; phishing; fraud.

Стаття надійшла до редакції 24.01.2025.