DOI: 10.18372/2307-9061.66.17419
УДК 342.951:351.82 +32.019.51(045)

Guoqiang Fu,
Legal Specialist, Singapore
ORCID ID: https://orcid.org/0009-0003-9479-1113

Є. В. Криволап,
здобувач вищої освіти третього (освітньо-наукового) рівня
ORCID ID: https://orcid.org/0000-0003-2599-2520

ОСОБЛИВОСТІ ТЕРМІНОЛОГІЇ В АНГЛОМОВНІЙ ЛІТЕРАТУРІ У СФЕРІ КІБЕРБЕЗПЕКИ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: krivolap.evgeniy@gmail.com

Метою *статті є дослідження англомовних джерел, присвячених термінології у сфері кібербезпеки.* ***Методи дослідження:*** *документальний аналіз, узагальнення правової інформації, інформації із сфери кіберзахисту інформаційно-комунікаційних систем, а також практики кіберзахисту інформації від різноманітних кібератак.* ***Результати:*** *встановлено, що єдиного підходу до формулювання термінології у сфері кібербезпеки на даний момент не існує, однак при формулюванні поняття «кібербезпека», на відміну від прийнятого у п. 5 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», де «кібербезпека» – це стан, в англомовних джерелах переважає розуміння, що «кібербезпека» – це дія. При цьому ця дія спрямовується не тільки на захист від кібератак, але й усунення їх наслідків. Серед англомовних авторів існує певна єдність з приводу класифікації типів кібербезпеки на п'ять основних типів: безпека критичної інфраструктури; безпека комп'ютерних програм; мережева безпека; хмарна безпека; безпека пристроїв системи Інтернет. Порівняно погляди англомовних авторів на визначення об'єктів критичної інфраструктури. В Законі України «Про основні засади забезпечення кібербезпеки України», а також у Стратегії кібербезпеки України від 14.05.2021 р. використовується поняття «вразливість» до кібератак, однак офіційного визначення цьому поняттю не надано. Пропонується відтворити в українському законодавстві відповідне визначення, наведене у міжнародному стандарті ISO 27005. Відтворені українською мовою конкретні рекомендації, які містяться в англомовній літературі, користувачам електронних мереж щодо запобігання кібератакам або зменшенню їх наслідків.* ***Обговорення:*** *результати дослідження дозволили запропонувати окремі удосконалення законодавства України з метою уніфікації із законодавством ЄС.*

Ключові слова: *кібербезпека; кібератака; критична інфраструктура; вразливість; комп'ютерні мережі.*

Постановка проблеми та її актуальність. На початку 2000-х років 21 ст. лідери західних країн були «здивовані» налаштуванням президента росії Путіна на руйнування структур західного світу, у тому числі засобами кібератак. Натомість на практиці Інституції НАТО, Європейський парламент, ОБСЄ тощо зазнали потужних ударів у кібернетичній сфері. Наприклад, протягом 2016 року Франція заблокувала 24 тисячі кібератак, спрямованих проти її збройних сил, а Україна зазнала 24 тисячі кібератак лише за останні два місяці того ж року [1, с. 53]. Разом із тим, у поточному, 2023-му, році така ситуація вже мало кого дивує. Так, за зві-

том Групи аналізу загроз (TAG) Google, підтримувані російським урядом кібезловмисники збільшили кількість спроб зламу українських користувачів минулого року на 250 % порівняно з 2020 роком. У 2023 році Google очікує, що Москва посилить атаки не лише на Україну, але й на партнерів по НАТО [2]. Тому запобігання кіберзагрозам можливе завдяки поєднанню національної та міжнародної стратегій кіберзахисту [3 та ін.]. Отже, дослідження англомовної термінології у сфері кіберзахисту є актуальним.

Аналіз досліджень і публікацій з проблеми. У публікації [4] Pasindu Wijesinghe зазначає, що у цьому світі кібербезпека є найбільш необхідною для захисту конфіденційності інформації. Заходи кібербезпеки захищають комп'ютерні мережі від загроз їх апаратному забезпеченню, програмному забезпеченню або даним. Разом із тим, В.В. Філінович констатує, що єдиного підходу до визначення сутності кібербезпеки не існує. [5, с. 39]. Аналогічно D. Schatz (із співавторами) зазначає, що є досить мало розуміння поняття «кібербезпека», що потенційно може викликати значні проблеми в контексті організаційної стратегії, бізнес-цілей або міжнародних угод [6]. Натомість як зазначається у статті [7], термінологія займає особливе місце в збереженні та передаванні знань, оскільки саме на неї припадає основне інформаційне навантаження. Matt Rosenthal (США) виділяє п'ять основних, на його думку, типів кібербезпеки: безпека критичної інфраструктури; безпека комп'ютерних програм; мережева безпека; хмарна безпека; безпека пристроїв системи Інтернет [8]. Alison Grace Johansen надає аналогічну класифікацію, наголошуючи на необхідності поєднання безпеки комп'ютерних програм та безпеки даних, що зберігаються в комп'ютерних мережах [9]. У публікаціях [10, 11] розглядаються, зокрема, генеза поняття «кібербезпека» та класифікація вразливостей. Stefan P. Bargan систематизував відомості про пошукові англомовні системи у сфері кібербезпеки [12]. Отже, подальші дослідження у цій сфері з метою узагальнення, уніфікації і врахування в українській і міжнародній практиці кіберзахисту є актуальними.

Виклад основного матеріалу дослідження. Як зазначалося вище, єдиного підходу до визначення сутності кібербезпеки не існує. [5, с. 39]. Abi Tyas Tunggal, Kaushik Sen визначають кібербезпеку як стан або процес захисту та відновлення комп'ютерних систем, мереж, пристроїв і програм від будь-якого типу кібератак [13]. Ці ж автори зазначають, що кібербезпека важлива, оскільки вона захищає всі категорії даних від крадіжки та пошкодження. Сюди входять конфіденційні дані, ідентифікаційна інформація (PII), захищена інформація про здоров'я (PHI), особиста інформація, інтелектуальна власність, дані та державні та галузеві інформаційні системи. Кібератаки становлять дедалі складнішу та дедалі більшу небезпеку для ваших конфіденційних даних, оскільки зловмисники використовують нові методи на основі соціальної інженерії та штучного інтелекту (AI), щоб обійти традиційні засоби контролю безпеки даних.

Kagalwalla N., Churi P.P. розглядають кібербезпеку як спосіб захисту комп'ютерних систем від загроз на кшталт вірусів [14].

Фахівці CISCO, американської ТНК і світового лідера в галузі високих технологій, під кібербезпекою розуміють практику захисту систем, мереж і програм від цифрових атак. При цьому вказується, що кібератаки зазвичай спрямовані на доступ, зміну або знищення конфіденційної інформації; вимагання грошей у користувачів за допомогою програм-вимагачів; або переривання звичайних бізнес-процесів. Наголошується, що впровадження ефективних заходів кібербезпеки сьогодні є особливо складним, оскільки пристроїв більше, ніж людей, а зловмисники стають все більш інноваційними [15].

Згаданий вище Matt Rosenthal [8], який визначає п'ять основних, на його думку, типів кібербезпеки, описує їх наступним чином.

А. *Безпека критичної інфраструктури* – зосереджена на захисті кіберфізичних систем, мереж і активів, на які покладаються сучасні суспільства. Безпека та стійкість критичної інфраструктури життєво важливі для безпеки та добробуту нашого суспільства. Типові приклади критичної інфраструктури: електрична мережа; водопостачання; світлофори; торгові центри; лікарні. Організаціям, яким доручено захистити

критично важливу інфраструктуру, слід виявити вразливі місця, пов'язані з системою цієї інфраструктури, і створити план запобігання майбутнім збиткам. Компанії, які не відповідають за критично важливу інфраструктуру, але все ще залежать від неї для частини своїх операцій, також повинні розробити план на випадок надзвичайних ситуацій, оцінивши, як атака на інфраструктуру, від якої вони залежать, може вплинути на них.

Варто зазначити, що в Україні на законодавчому рівні запроваджена система визначення об'єктів критичної інфраструктури. Згідно із ч. 4 ст. 10 Закону України «Про критичну інфраструктуру», до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема: 1) урядування та надання найважливіших публічних (адміністративних) послуг; 2) енергозабезпечення (у тому числі постачання теплової енергії); 3) водопостачання та водовідведення; 4) продовольче забезпечення; 5) охорона здоров'я; 6) фармацевтична промисловість; 7) виготовлення вакцин, стале функціонування біолабораторій; 8) інформаційні послуги; 9) електронні комунікації; 10) фінансові послуги; 11) транспортне забезпечення; 12) оборона, державна безпека; 13) правопорядок, здійснення правосуддя, тримання під вартою; 14) цивільний захист населення та територій, служби порятунку; 15) космічна діяльність, космічні технології та послуги; 16) хімічна промисловість; 17) дослідницька діяльність.

Разом із тим, слід зазначити, що, на думку американського фахівця, у цей список повинні окремо входити торгові центри та засоби забезпечення дорожнього руху (світлофори).

B. *Безпека комп'ютерних програм* – захищає програмний код і дані від кіберзагроз і зломів. Він використовує програмні та апаратні методи для боротьби із зовнішніми загрозами, які можуть виникнути на етапі розробки програми, включаючи етапи проектування та розгортання. Оскільки додатки доступніші через мережі, важливо негайно запровадити стандарти безпеки, процедури, системи та інструменти, щоб захистити використовувані додатки на всіх етапах розробки. Типи безпеки комп'ютерних програм: аутентифікація; авторизація; антивірусні програми; антишпигунське програмне забезпечення; програми шифрування; брандмауери; тестування безпеки програми. Ці заходи безпеки допомагають запобігти несанкціонованому доступу до використовуваних програм і захистити активи конфіденційних даних за допомогою спеціальних процесів безпеки програми.

C. *Безпека мережі*. Оскільки кібербезпека стосується зовнішніх загроз, безпека мережі захищає від несанкціонованого вторгнення у використовувані внутрішні мережі через зловмисний намір. Безпека мережі гарантує безпеку внутрішніх мереж шляхом захисту інфраструктури та блокування доступу до неї. Команди безпеки тепер використовують автоматичний контроль в реальному часі, щоб позначати ненормальний трафік і сповіщати про загрози в режимі реального часу, щоб краще керувати моніторингом безпеки мережі. Адміністратори мережі продовжують впроваджувати політики та процедури для запобігання неавторизованому доступу, модифікації та експлуатації мережі. Загальні приклади реалізації безпеки мережі: додаткові логіни; нові паролі; безпека програми; антивірусні програми; антишпигунське програмне забезпечення; шифрування; брандмауери, контрольований доступ до Інтернету.

D. *Хмарна безпека* – це програмний інструмент безпеки, який захищає та контролює дані у ваших хмарних ресурсах. Хмарні постачальники постійно створюють і впроваджують нові інструменти безпеки, щоб допомогти корпоративним користувачам краще захистити свої дані. Навколо хмарних обчислень поширений міф про те, що вони менш безпечні, ніж традиційні підходи. Користувачі схильні вірити, що їх дані більш безпечні, якщо вони зберігаються на фізичних серверах і системах, якими користувач безпосередньо володіє та керує. Однак за допомогою хмарної безпеки було доведено, що контроль не означає, що безпека та доступність важливіші за фізичне розташування ваших даних. Зокрема, користувачі локального середовища зазнають у середньому 61,4 атак, а клієнти середовища постачальника послуг зазнають у середньому 27,8 атак.

Безпека хмарних обчислень подібна до традиційних локальних центрів обробки даних, лише без часу та витрат на підтримку величезних об'єктів обробки даних, а ризик порушення безпеки мінімальний.

Е. *Безпека пристроїв системи Інтернет* – це захист інтернет-пристроїв і мереж, до яких вони підключені, від кіберзагроз і зломів. Цей тип рішення для кібербезпеки захищає, визначає та відстежує ризики, одночасно допомагаючи усунути вразливості пристроїв, які можуть спричинити загрози безпеці для вашого бізнесу. Такі пристрої стосуються широкого спектру критичних і некритичних кіберфізичних систем, таких як прилади, датчики, телевізори, маршрутизатори Wi-Fi, принтери та камери безпеки. Пристрої часто поставляються у вразливому стані та майже не пропонують захисту, що створює унікальні проблеми безпеки для всіх користувачів.

Згаданий вище Alison Grace Johansen [9] вважає, що кібербезпека – це стан або процес захисту та відновлення мереж, пристроїв і програм від будь-якого типу кібератак. Кібербезпека – це практика захисту використовуваних електронних систем, мереж, комп'ютерів, мобільних пристроїв, програм і даних від зловмисних цифрових атак. Кіберзлочинці можуть застосовувати різноманітні атаки проти окремих жертв або компаній. Ці атаки можуть включати доступ, зміну або видалення конфіденційних даних; вимагання платежу; втручання в бізнес-процеси. Кібератаки становлять небезпеку для організацій, співробітників і споживачів. Ці атаки можуть бути спрямовані на доступ або знищення конфіденційних даних або вимагання грошей. Фактично вони можуть зруйнувати бізнес і завдати шкоди фінансовому стану та особистому життю, особливо якщо ви стали жертвою крадіжки особистих даних.

Кібербезпека є підмножиною IT-безпеки. IT-безпека – це безпека інформаційних технологій (IT), також відома як безпека електронної інформації або InfoSec, – це захист даних – як там, де вони зберігаються, так і під час переміщення через мережу. У той час як кібербезпека захищає лише цифрові дані, IT-безпека захищає як цифрові, так і фізичні дані (по суті дані в будь-якій формі) від несанкціонованого доступу, використання, зміни, розголошення, видалення або інших форм зловмисного наміру з боку зловмисників. IT-безпека захищає як фізичні, так і цифрові дані, а кібербезпека захищає цифрові дані у ваших мережах, комп'ютерах і пристроях від несанкціонованого доступу, атак і знищення.

Безпека мережі, або безпека комп'ютера, є підмножиною кібербезпеки. Цей тип безпеки використовує апаратне та програмне забезпечення для захисту будь-яких даних, які надсилаються через ваш комп'ютер та інші пристрої в мережу. Безпека мережі слугує для захисту IT-інфраструктури та захисту від перехоплення, зміни чи викрадення інформації кіберзлочинцями.

Alison Grace Johansen [9] в цілому визначає ті ж п'ять основних типів кібербезпеки, що і Matt Rosenthal [8]. Натомість Alison Grace Johansen [9] класифікує 3 категорії кіберзагроз: атаки на конфіденційність, атаки на цілісність і атаки на доступність.

А. *Атаки на конфіденційність*. Ці атаки можуть бути спрямовані на викрадення ідентифікаційної інформації (PII), як-от номер соціального страхування особи, а також банківський рахунок або дані кредитної картки. Після цих атак ця персональна інформація може бути продана або обміняна в нелегальній мережі для купівлі та використання іншими.

Різновидом атаки на конфіденційність є так звана соціальна інженерія. Це процес психологічного маніпулювання людьми, які змушують їх виконувати дії або передавати інформацію. Фішингові атаки є найпоширенішою формою соціальної інженерії. Фішингові атаки зазвичай здійснюються у вигляді оманливого електронного листа з метою змусити одержувача надати особисту інформацію.

В. *Атаки на цілісність*. Ці атаки складаються з особистого або корпоративного саботажу і часто називаються витоками. Кіберзлочинець отримає доступ до конфіденційної інформації та оприлюднить її з метою оприлюднення даних і впливу на суспільство, щоб воно втратило довіру до особи чи організації.

Типом атаки на цілісність є так звані розширені постійні загрози (advanced persistent threats**,** APTs), коли неавторизований користувач про-

никає в мережу непоміченим і залишається в мережі протягом тривалого часу. Метою APT є викрадення даних, а не шкода мережі. APT часто трапляються в секторах з високою цінністю інформації, таких як національна оборона, виробництво та фінансова галузь.

С. *Атаки на доступність*. Метою цього типу кібератак є блокування користувачам доступу до їхніх власних даних, доки вони не сплатять комісію або викуп. Як правило, кіберзлочинець проникає в мережу та позбавляє попередньо авторизованих сторін доступу до важливих даних, вимагаючи викупу. Компанії іноді платять викуп, а потім виправляють кібервразливість, щоб уникнути припинення комерційної діяльності.

Тип атаки на доступність – використання шкідливого програмного забезпечення. Це стосується програмного забезпечення, призначеного для отримання доступу до комп'ютера або його пошкодження без відома власника. Зловмисне програмне забезпечення може зробити все: від викрадення конфіденційної реєстраційної інформації та використання комп'ютера до розсилки спаму та збою комп'ютерної системи. Деякі з поширених типів шкідливих програм відомі як шпигунські програми, клавіатурні шпигуни, справжні віруси та хробаки.

Програми-вимагачі – інша форма зловмисного програмного забезпечення – також є типом атаки на доступність. Мета програм-вимагачів – заблокувати та зашифрувати дані вашого комп'ютера чи пристрою, фактично тримаючи ваші файли в заручниках, а потім вимагати викуп за відновлення доступу. Як правило, жертва повинна сплатити викуп протягом встановленого періоду часу, інакше ризикує назавжди втратити доступ до інформації. До поширених типів програм-вимагачів належать зловмисне програмне забезпечення для криптовалют, блокувальники та програми-страхи.

Варто зазначити, що українське законодавство також знає поняття «кіберзагроза». Так, згідно пункту 6 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Тобто, на відміну від англомовних авторів, Законом України кіберзагроза розглядається як загроза в широкому сенсі – національним інтересам Держави, і не розглядається як загроза інтересам конкретних осіб.

Цікаво зазначити, що автором публікації [9] надаються практичні рекомендації щодо захисту від можливих дій кіберзловмисників.

А. Надаючи особисту інформацію, використовуйте лише перевірені сайти. Хорошим практичним правилом є перевірка URL-адреси. Якщо сайт містить «https://», то це безпечний сайт. Якщо URL-адреса містить «http://» – зверніть увагу на пропущену «s» – уникайте введення конфіденційної інформації, наприклад даних вашої кредитної картки або номера соціального страхування.

Б. Не відкривайте вкладення електронної пошти та не натискайте посилання в електронних листах із невідомих джерел. Один із найпоширеніших способів потрапляння зловмисного програмного забезпечення та вірусів у мережі та користувачів – це електронні листи, які маскуються як ті, кому ви довіряєте. Важливим емпіричним правилом є відвідування самого вебсайту, а не натискання посилання електронної пошти на веб-сайт.

В. Завжди оновлюйте свої пристрої. Оновлення програмного забезпечення містять важливі виправлення для усунення вразливостей системи безпеки. Кіберзловмисники також можуть націлитися на застарілі пристрої, на яких може не працювати найновіше програмне забезпечення безпеки.

С. Регулярно створюйте резервні копії файлів для додаткового захисту в разі кібератак. Це допоможе зберегти ваші файли в безпечному окремому місці, якщо вам буде потрібно очистити пристрій через кібератаку або отримати доступ до ваших даних у разі атаки програм-вимагачів.

У публікації [10] наведені наступні дефініції: комп'ютерна безпека, кібербезпека або безпека інформаційних технологій (IT-безпека) – це захист комп'ютерних систем і мереж від атак зловмисників, які можуть призвести до несанкціо-

нованого розкриття інформації, крадіжки або пошкодження обладнання, програмного забезпечення або даних, а також від порушення або неправильного спрямування послуг, які вони надають [16].

Зазначимо, що на відміну від автора [9], у даному визначенні поняття «кібербезпека» та «ІТ-безпека» ототожнюються.

Наголошується, що галузь «кібербезпеки» стала важливою завдяки розширенню залежності від комп'ютерних систем, Інтернету та стандартів бездротових мереж, таких як Bluetooth і Wi-Fi, а також завдяки зростанню розумних пристроїв, включаючи смартфони, телевізори та різні пристроїв, які інтегровані у мережу Інтернет. Кібербезпека є одним із найбільш важливих викликів сучасного світу як через складність інформаційних систем, так і через суспільство, яке вони підтримують. Безпека особливо важлива для об'єктів, які керують великомасштабними системами з далекосяжними фізичними ефектами, такими як розподіл влади, вибори та фінанси [17, 18].

В публікаціях [10, 11] розглядаються підходи до визначення вразливості комп'ютерних систем до кібератак. Вразливості – це недоліки в комп'ютерній системі, які послаблюють загальну безпеку пристрою/системи. Вразливості можуть бути слабкими місцями в самому апаратному забезпеченні або програмному забезпеченні, яке працює на апаратному забезпеченні. Уразливості можуть бути використані суб'єктом загрози, наприклад зловмисником, для перетину меж привілеїв (тобто для виконання неавторизованих дій) у комп'ютерній системі. Щоб використати вразливість, зловмисник повинен мати принаймні один відповідний інструмент або техніку, яка може підключитися до слабкої сторони системи. У цьому розумінні вразливі місця також називають поверхнею атаки.

Управління вразливістю – це циклічна практика, яка містить загальні процеси, що включають: виявлення всіх активів, визначення пріоритетів активів, оцінку або виконання повного сканування вразливостей, звіт про результати, усунення вразливостей, перевірку виправлення – повторення. Ця практика зазвичай стосується вразливостей програмного забезпечення в обчислювальних системах. Гнучке управління вразливістю означає запобігання атакам шляхом якнайшвидшого виявлення всіх вразливостей [19].

Офіційне визначення поняття «вразливість» надано у міжнародному стандарті ISO 27005, який визначає вразливість як слабкість активу або групи активів, які можуть бути використані однією або декількома загрозами, де активом є все, що має цінність для організації, її бізнес-операцій та їх безперервності, включаючи інформаційні ресурси, які підтримують місію організації [11].

Варто зазначити, що поняття «вразливість» використовується і в Законі України «Про основні засади забезпечення кібербезпеки України», а також у Стратегії кібербезпеки України від 14.05.2021 р., затвердженій Указом Президента України від 26.08.2021 р. № 447/2021. Наприклад, 28.11.2022 року Держспецзв'язку повідомило, що він постійно посилює захищеність інформаційних ресурсів країни. Одним із напрямів такої роботи є виявлення вразливостей українських інформаційних ресурсів, попередження відповідальних та контроль про необхідність нейтралізувати знайдені «дірки» у кібербезпеці[1]. Однак визначення цього поняття ані в Законі, ані в Стратегії не надано. Очевидно, є сенс запровадити у відповідні нормативні документи України поняття «вразливість» відповідно до міжнародного стандарту ISO 27005.

Варто також зазначити, що поняття «кібербезпека» також звичайно використовується в Законі України «Про основні засади забезпечення кібербезпеки України» і визначене як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (п. 5 ст. 1 Закону).

Тобто, ідеологія цього визначення дещо відрізняється від тій, що поширена в англомовних

[1] https://www.cip.gov.ua/ua/news/derzhspeczv-yazku-pidsilyuye-i-kontrolyuye-zakhishenist-derzhavnikh-informaciinikh-resursiv

публікаціях. Так, якщо у визначенні Закону України «Про основні засади забезпечення кібербезпеки України» «кібербезпека» – це стан, то у більшості англомовних визначень «кібербезпека» – це дія, спрямована на забезпечення захищеності, зокрема, це «процес захисту та відновлення комп'ютерних систем…» [9, 13]; «спосіб захисту комп'ютерних систем від загроз…» [14]; «захист комп'ютерних систем і мереж…» [10]. Крім того, відповідно до визначень [9, 13], «кібербезпека» – це не тільки захист від кібератак, але й усунення їх наслідків.

Висновки. Проведене дослідження англомовних джерел, присвячених термінології у сфері кібербезпеки. Встановлено, що, дійсно, єдиного підходу до формулювання цих визначень на даний момент не існує, однак при формулюванні поняття «кібербезпека», на відміну від прийнятого у п. 5 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», де «кібербезпека» – це стан, в англомовних джерелах переважає розуміння, що «кібербезпека» – це дія. При цьому ця дія спрямовується не тільки на захист від кібератак, але й усунення їх наслідків.

Серед англомовних авторів існує певна єдність з приводу класифікації типів кібербезпеки на п'ять основних типів: безпека критичної інфраструктури; безпека комп'ютерних програм; мережева безпека; хмарна безпека; безпека пристроїв системи Інтернет. Порівняно погляди англомовних авторів на визначення об'єктів критичної інфраструктури. Показано, що, з урахуванням цих поглядів, перелік об'єктів критичної інфраструктури, передбачених ч. 4 ст. 10 Закону України «Про критичну інфраструктуру», слід доповнити такими об'єктами, як торгові центри та засоби забезпечення дорожнього руху (світлофори).

В Законі України «Про основні засади забезпечення кібербезпеки України», а також у Стратегії кібербезпеки України від 14.05.2021 р., затвердженій Указом Президента України від 26.08.2021 р. № 447/2021, використовується поняття «вразливість» до кібератак, однак офіційного визначення цьому поняттю не надано. Пропонується відтворити у українському законодавстві відповідне визначення, наведене у міжнародному стандарті ISO 27005.

Відтворене українською мовою конкретні рекомендації, які містяться в англомовній літературі, користувачам електронних мереж щодо запобігання кібератакам або зменшенню їх наслідків.

Література

1. Кузьо Тарас. Війна Путіна проти України. Революція, націоналізм і криміналітет / пер. з англ. Андрія Павлишина. Київ, 2018. 560 с.

2. У Google прогнозують збільшення кібератак РФ на Україну і членів НАТО цього річ. *Економічна правда.* 16.02.2023. URL: https://www.epravda.com.ua/news/2023/02/16/697133/ DOI: https://doi.org/10.1055/a-1946-7604

3. Maskun S.H. Cyber Security: Rule of Use Internet Safely. *Journal of Law, Policy and Globalization.* 2013. Vol. 15. P. 22. DOI: https://doi.org/10.1016/ j.sbspro.2013.10.333

4. Pasindu Wijesinghe. Quantum Computing Impact on Cyber Security. 23.08.2021. URL: https://pasindu-wijesinghe.medium.com/quantum-computing-impact-on-cyber-security-26541a02407c

5. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* Київ: НАУ, 2021. № 3 (60). С. 38-43. DOI: https://doi.org/10.18372/2307-9061.60.15950

6. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 2017. № 2. P. 54-74. DOI: https://doi.org/10.15394/jdfsl.2017.1476

7. Іленков А. Термінологія та її роль у представленні знань. Вісник Нац. ун-ту «Львівська політехніка». Серія «Проблеми української термінології». 2009. № 648. С. 24–29.

8. Matt Rosenthal. 5 Types of Cyber Security. MINDCORE Services. 05.09.2018. URL: https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

9. Alison Grace Johansen. What is cyber security? What you need to know? NORTON.LifeLock. 28.04.2022. URL: https://us.norton.com/ blog/ malware/what-is-cybersecurity-what-you-need-to-know#

10. Computer security. The Free Encyclopedia. URL: https://en.wikipedia.org/ wiki/Computer_ security

11. Vulnerability (computing). The Free Encyclopedia. URL: https://en.wikipedia.org/wiki/ Vulnerability_ (computing)

12. Stefan P. Bargan. 25 Cybersecurity Search Engines. 08.10.2022. URL: https://system weakness. com/25-cybersecurity-search-engines-68bfcc2418ff

13. Abi Tyas Tunggal, Kaushik Sen. Why is Cybersecurity Important? UpGuard. 20.10.2022. URL: https://www.upguard.com/blog/cyber security-important

14. Kagalwalla N., Churi P.P. Cybersecurity in aviation: an intrinsic review. 2019. 5th International conference on computing, communication, control and automation (ICCUBEA). Pp. 1-6. DOI: https://doi.org/10.1109/ICCUBEA47591.2019

15. What Is Cybersecurity? CISCO. URL: https://www.cisco.com/c/en/us/ products/security/what-is-cybersecurity.html

16. Daniel Schatz, Rabih Bashroush, Julie Wall. Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law. 2017, 12 (2). DOI: https://doi.org/ 10.15394/jdfsl.2017.1476

17. Mazaher Kianpour, Stewart J. Kowalski, *Harald Øverby. (2021).* Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability.* 2021, 13 (24): 13677. DOI*:* https://doi.org/ 10.3390/su132413677

18. Tim Stevens Global Cybersecurity: New Directions in Theory and Methods. Politics and Governance. 11 June 2018, 6 (2). 1-4. Archived (PDF) from the original on 4 September 2019. DOI: https://doi.org/10.17645/pag.v6i2.1569

19. Aaron Yi Ding, Gianluca Limon De Jesus; Marijn Janssen (2019). Ethical hacking for boosting IoT vulnerability management: a first look into bug bounty programs and responsible disclosure. Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing – ICTRS ‘19. Ictrs ‘19. 2019. Rhodes, Greece: ACM Press: 49-55.

References

1. Kuzo Taras. Viina Putina proty Ukrainy. Revoliutsiia, natsionalizm i kryminalitet / per. z anhl. Andriia Pavlyshyna. Kyiv, 2018. 560 s.

2. U Google prohnozuiut zbilshennia kiberatak RF na Ukrainu i chleniv NATO tsoho rich. *Ekonomichna pravda.* 16.02.2023. URL: https://www.epravda.com.ua/ news/ 2023/02/16/ 697133/

3. Maskun S.H. Cyber Security: Rule of Use Internet Safely. *Journal of Law, Policy and Globalization.* 2013. Vol. 15. P. 22.

4. Pasindu Wijesinghe. Quantum Computing Impact on Cyber Security. 23.08.2021. URL: https://pasindu-wijesinghe.medium.com/quantum-computing-impact-on-cyber-security-26541a02407c

5. Filinovych V.V. Kiberbezpeka ta zahrozy aviatsiinii sferi: pravovyi aspekt. Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Iurydychnyi visnyk. «Povitriane i kosmichne pravo». 2021. № 3(60). S. 38-43. DOI: 10.18372/ 2307-9061.60.15950

6. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 2017. № 2. P. 54-74.

7. Ilenkov A. Terminolohiia ta yii rol u predstavlenni znan. *Visnyk Nats. un-tu «Lvivska politekhnika». Seriia «Problemy ukrainskoi terminolohii».* 2009. № 648. S. 24–29.

8. Matt Rosenthal. 5 Types of Cyber Security. MINDCORE Services. 05.09.2018. URL: https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

9. Alison Grace Johansen. What is cyber security? What you need to know? NORTON.LifeLock. 28.04.2022. URL: https://us.norton.com/blog/ malware/what-is-cybersecurity-what-you-need-to-know#

10. Computer security. The Free Encyclopedia. URL: https://en.wikipedia.org/ wiki/Computer _security

11. Vulnerability (computing). The Free Encyclopedia. URL: https://en.wikipedia.org/wiki/ Vulnerability_(computing)

12. Stefan P. Bargan. 25 Cybersecurity Search Engines. 08.10.2022. URL: https://system weakness. com/25-cybersecurity-search-engines-68bfcc2418ff

13. Abi Tyas Tunggal, Kaushik Sen. Why is Cybersecurity Important? UpGuard. 20.10.2022. URL: https://www.upguard.com/blog/ cybersecurity-important

14. Kagalwalla N., Churi P.P. Cybersecurity in aviation: an intrinsic review. 2019. 5th International conference on computing, communication, control and automation (ICCUBEA). Pp. 1-6. DOI: 10.1109/ICCUBEA47591.2019. 9128483

15. What Is Cybersecurity? CISCO. URL: https://www.cisco.com/c/en/us/ products/ security/ what-is-cybersecurity.html

16. Daniel Schatz, Rabih Bashroush, Julie Wall. Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 2017, 12 (2).

17. Mazaher Kianpour, Stewart J. Kowalski, *Harald Øverby. (2021).* Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability.* 2021, 13 (24): 13677. DOI*:* 10.3390/ su132413677.

18. Tim Stevens Global Cybersecurity: New Directions in Theory and Methods. Politics and Governance. 11 June 2018, 6 (2). 1-4. DOI: 10.17645/ pag.v6i2.1569. Archived (PDF) from the original on 4 September 2019.

19. Aaron Yi Ding, Gianluca Limon De Jesus; Marijn Janssen (2019). Ethical hacking for boosting IoT vulnerability management: a first look into bug bounty programs and responsible disclosure. Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing – ICTRS ‘19. Ictrs ‘19. 2019. Rhodes, Greece: ACM Press: 49-55.

Guoqiang Fu, Evgeniy Krivolap

FEATURES OF TERMINOLOGY IN ENGLISH LITERATURE IN THE FIELD OF CYBER SECURITY

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: krivolap.evgeniy@gmail.com

The aim *of the article is research of English-language sources devoted to terminology in the field of cyber security.* ***Research methods:*** *documentary analysis, summarization of legal information, information from the field of cyber protection of information and communication systems, as well as practices of cyber protection of information from various cyber attacks.* ***Results:*** *it has been established that there is currently no unified approach to the formulation of terminology in the field of cyber security, however, when formulating the concept of «cyber security», unlike the one adopted in clause 5 of Art. 1 of the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine», where «cybersecurity» is a state, in English-language sources the prevailing understanding is that «cybersecurity» is an action. At the same time, this action is aimed not only at protecting against cyber attacks, but also at eliminating their consequences. Among English-speaking authors, there is a certain unity regarding the classification of the types of cyber security into five main types: critical infrastructure security; security of computer programs; network security; cloud security; security of Internet system devices. The views of English-speaking authors on the definition of critical infrastructure objects are compared. The Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» as well as the Cybersecurity Strategy of Ukraine dated May 14, 2021 use the concept of «vulnerability» to cyberattacks, but no official definition of this concept has been provided. It is proposed to reproduce in Ukrainian legislation the relevant definition given in the international standard ISO 27005. Reproduced in Ukrainian are specific recommendations contained in English-language literature to users of electronic networks regarding the prevention of cyber attacks or the reduction of their consequences.* ***Discussion:*** *the results of the study made it possible to propose individual improvements to the legislation of Ukraine with the aim of unification with EU legislation.*

Key words: *cyber security; cyber attack; critical infrastructure; vulnerability; computer networks.*

Стаття надійшла до редакції 07.03.2023