УДК 32:004.7; 32:519.7
DOI https://doi.org/10.32782/2312-1815/2025-20-23

Микола Ґеник
ORCID: 0000-0002-5716-8299

МЕТОДОЛОГІЧНІ ПРОБЛЕМИ ДЕФІНІЦІЇ ТЕРМІНІВ «КІБЕРБЕЗПЕКА» І «КІБЕРЗАГРОЗА»

Протягом останніх десятиліть кардинально змінилися способи і методи гарантування національної та міжнародної безпеки. Розвиток комп'ютерних технологій спричинив перенесення суперництва в кібернетичну галузь чи домен. Кібербезпека пронизує всі сфери діяльності держав і суспільств, стає одним із найважливіших елементів. Інформаційно розвинені держави формують стратегії протистояння в кіберсфері, яка у близькому майбутньому визначатиме форми і зміст міжнародного суперництва та конфліктів. Незважаючи на часте вживання термінів «кібербезпека» і «кіберзагроза», словники й енциклопедії не оперують універсальними визначеннями згаданих категорій. Завдання статті – проаналізувати основні підходи до дефініції понять у науковій літературі та правових актах.

У Законі України «Про основні засади забезпечення кібербезпеки України» дано визначення кібербезпеки як «захищеності 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 в кіберпросторі».

Після проведення аналізу наявних визначень Д. Крейген, Н. Дякун-Зіболт і Р. Пьорс запропонували вичерпну універсальну інклюзивну дефініцію: «кібербезпека – це організація і збір ресурсів, процесів і структур, що використовуються для захисту кіберпростору та систем, що використовують кіберпростір, від дій, які розмежовують де-юре і де-факто права власності».

Кібербезпека залишається однією з найважливіших і найуразливіших сфер у системі безпеки, що зумовлено відносною новизною та стрімким технологічним розвитком інформаційних мереж. Правове врегулювання діяльності в кіберпросторі є актуальним завданням внутрідержавного та міжнародного права.

Ключові слова: *кібербезпека, кіберпростір, кібератака, кіберзагроза, інформаційні системи.*

Вступ. Протягом останніх десятиліть кардинально змінилися способи і методи гарантування національної та міжнародної безпеки. Розвиток комп'ютерних технологій спричинив перенесення суперництва в кібернетичну галузь чи домен. Кібербезпека пронизує всі сфери діяльності держав і суспільств, стає одним із найважливіших елементів. Інформаційно розвинені держави формують стратегії протистояння в кіберсфері, яка у близькому майбутньому визначатиме форми і зміст міжнародного суперництва та конфліктів.

Матеріал і методи дослідження. Основою аналізу стали дефініції понять «кібербезпека» і «кіберзагрози», які містяться в енциклопедіях, словниках, державно-правових документах, наукових публікаціях. Використано інституціональний, компаративістський, системний методи, контент-аналіз тощо.

Мета дослідження. Незважаючи на часте використання термінів «кібербезпека» і «кіберзагроза», словники й енциклопедії не оперують універсальними визначеннями згаданих категорій. Завдання статті – проаналізувати основні підходи до дефініції понять у науковій літературі та правових актах.

Результати та обговорення. Кібернетична безпека стрімко розвивається і набуває все більшого значення з кінця 1960-х рр., коли з'явилися модеми (пристрої, що дозволяють

комп'ютерам спілкуватися через телефонні лінії). Поширення персональних комп'ютерів у 1980-х рр. ускладнило проблему, оскільки вони дозволили хакерам незаконно отримувати доступ до основних комп'ютерних систем. З бурхливим розвитком інтернету наприкінці 20-го і на початку 21-го ст. комп'ютерна безпека стала широко розповсюдженою проблемою. Розвиток передових технологій безпеки спрямований на зменшення таких загроз, хоча паралельне вдосконалення методів комп'ютерних злочинів створює постійну небезпеку.

В останні десятиліття воєнні стратегії технологічно розвинених держав стали впроваджувати поняття кіберпростору. Зокрема, Міністерство оборони США, зважаючи на зміни міжнародної ситуації та нові форми конфліктів, оновило воєнну стратегію. Зокрема, документ "Field Manual 3.0" («Польовий посібник 3.0») передбачає ведення американськими збройними силами багатодоменних операцій (Multi-Domain Operations, MDO), коли боротьба точиться одночасно на суходолі, на морі, у повітрі, у космосі та в кіберпросторі. Кіберпростір – це взаємозалежні мережі інформації, вузли, які пронизують кожен домен. Мережі кіберпростору перетинають географічні та політичні кордони, об'єднують людей, організації та системи по всьому світу. Кіберпростір дозволяє взаємодію між особами, групами, організаціями та національними державами. Кіберпростір складний, суперечливий і критично важливий для успішної роботи технологічної інфраструктури та резидентних даних, зокрема й інтернету, телекомунікаційних мереж, комп'ютерних систем, вбудованих процесорів і контролерів. Кіберпростір – це розгалужена та складна глобальна мережа дротового та бездротового з'єднання, вузли, які пронизують кожен домен [4, с. 16].

Кіберпростір – це створена людьми домена, яка стала результатом поєднання комп'ютерів, роутерів, серверів, кабелів, світловодів, безпровідних пристроїв, супутників та інших подібних компонентів, яка уможливлює пересилання інформації з великою швидкістю [6, с. 143–161]. Об'єднаний комітет начальників штабів США оперує дефініцією кіберпростору як глобальної домени всередині інформаційного середовища, що складається із взаємозалежних мереж інформаційних технологій і належних до них даних, зокрема й інтернету, телекомунікаційних мереж, комп'ютерних систем, і вбудованих процесорів та інстальованих переспрямовувачів. Закон України «Про основні засади забезпечення кібербезпеки України» (ст. 1) містить визначення кіберпростору як середовища (віртуального простору), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій із використанням мережі «Інтернет» та/або інших глобальних мереж передачі даних. Кіберпростір – поряд із повітряним, суходільним, морським і космічним, належить до 5 домен, які використовуються людьми для своїх цілей. Однак, на відміну від них, він не існує фізично, створений не природою, а людьми і піддається трансформаціям.

«Кібербезпека» є широко вживаним терміном, визначення якого дуже поліваріантні, часто суб'єктивні та неінформативні. Відсутність стислого, загальноприйнятого визначення яке б відображало багатовимірність кібербезпеки, становить перепони технологічному і науково-технічному прогресу, посилює переважно технічний погляд на кібербезпеку та штучно відокремлює дисципліни, які мають діяти узгоджено для вирішення складних проблем у цій галузі. Кібербезпека є предметом зацікавлення різних сфер науки та людської життєдіяльності: інформатики, інженерії, політології, соціології, комп'ютерних і воєнних наук, права, державного управління, бухгалтерського обліку, психології, менеджменту тощо. Відповідно кожна з наук оперує своїм визначенням цього поняття, здефінійованого через категорії технічних чи гуманітарних дисциплін. Більшість енциклопедій і словників не містять визначення кібербезпеки через відносну новизну терміна та нерозробленість категоріального апарату. Р.А. Кеммерер уважав, що «кібербезпека в основному складається з методів захисту та використовується для виявлення та запобігання потенційним зловмисникам». Дж.А. Льюїс наголошував на тому,

що «кібербезпека передбачає безпеку комп'ютера, мережі й інформації, яка на них міститься, від проникнення, зловмисного пошкодження чи знищення». Е. Аморозо пропонував визначення кібербезпеки через «зменшення ризику зловмисних впливів на програмне забезпечення, комп'ютери та мережі. Сюди входять інструменти, які використовуються для виявлення зламів, протидії вірусам, блокування зловмисного доступу, забезпечення автентифікації, увімкнення зашифрованих комунікацій тощо» [2, с. 13–21].

Міжнародний телекомунікаційний союз оперує визначенням, згідно з яким «кібербезпека – це сукупність інструментів, політик, концепцій безпеки, керівних принципів, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можуть бути використані для захисту кіберсередовища, організацій і активів користувачів» [2, с. 13–21].

Комітет із систем національної безпеки США під кібербезпекою розуміє «здатність захищати або обстоювати використання кіберпростору від кібератак». Словник Національної ініціативи з кар'єри та навчання у сфері кібербезпеки Міністерства внутрішньої безпеки США пропонує визначенням, згідно з яким кібербезпека – це «діяльність або процес, здатність або можливість, або стан, за допомогою яких інформаційні та комунікаційні системи й інформація, що міститься в них, захищені від пошкодження, несанкціонованого використання, модифікації або експлуатації» [2, с. 13–21].

«Огляд політики Білого дому щодо кіберпростору» давав визначення кібербезпеки як «стратегії, політики і стандартів, що стосуються безпеки й операцій у кіберпросторі й охоплюють увесь спектр політик і заходів щодо зменшення загроз, зменшення вразливості, стримування, міжнародної взаємодії, реагування на інциденти, забезпечення стійкості та відновлення, зокрема й операцій із комп'ютерними мережами, захисту інформації, правоохоронних, дипломатичних, військових і розвідувальних місій, оскільки вони стосуються безпеки та стабільності глобальної інформаційно-комунікаційної інфраструктури» [5].

Відділ громадської безпеки при уряді Канади у своїх документах користується визначенням кібербезпеки як «сукупності технологій, процесів, практик і заходів реагування та пом'якшення наслідків, призначених для захисту мереж, комп'ютерів, програм і даних від кібератак, пошкодження або несанкціонованого доступу, з метою забезпечення конфіденційності, цілісності та доступності». К. Канонгія і Р. Мандаріно (C. Canongia, R. Mandarino) запропонували визначення кібербезпеки як «мистецтва забезпечення існування та безперервності інформаційного суспільства нації, гарантування та захисту в кіберпросторі її інформації, активів і критичної інфраструктури».

«Оксфордський словник» визначає кібернетичну безпеку як «стан захищеності від злочинного або несанкціонованого використання електронних даних, або заходи, ужиті для досягнення цієї мети». Електронна версія «Британіки» містить визначення комп'ютерної безпеки як захисту комп'ютерних систем та інформації від шкоди, крадіжки та несанкціонованого використання [1].

Закон України «Про основні засади забезпечення кібербезпеки України» (ст. 1) дає визначення кібербезпеки як «захищеності 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 в кіберпросторі» [7].

Після проведення аналізу наявних визначень Д. Крейген, Н. Дякун-Зіболт і Р. Пьорс запропонували вичерпну універсальну інклюзивну дефініцію: «кібербезпека – це організація і збір ресурсів, процесів і структур, що використовуються для захисту кіберпростору та систем, що використовують кіберпростір, від дій, які розмежовують де-юре і де-факто права власності» [2, с. 13–21].

Заходи безпеки, пов'язані з комп'ютерною інформацією та доступом до неї, спрямовані на боротьбу із чотирма основними загрозами, як-от:

1) крадіжка даних, наприклад воєнної таємниці, з урядових комп'ютерів;

2) вандалізм, зокрема і знищення даних комп'ютерним вірусом;

3) шахрайство, наприклад переведення співробітниками банку коштів на власні рахунки;

4) утручання у приватне життя, як-от незаконний доступ до захищених особистих фінансових або медичних відомостей із бази даних.

Найпростішим засобом захисту комп'ютерної системи від крадіжок, вандалізму, вторгнення в особисте життя й інших безвідповідальних дій є електронне відстеження та реєстрація доступу до комп'ютерної системи та дій різних користувачів. Зазвичай це робиться шляхом присвоєння індивідуального пароля кожній особі, яка має доступ до системи. Тоді сама комп'ютерна система може автоматично відстежувати використання цих паролів, записувати такі дані, як і те, до яких файлів було отримано доступ під яким паролем тощо. Ще одним заходом безпеки є зберігання даних системи на окремому пристрої або носії, який зазвичай недоступний через комп'ютерну систему. Нарешті, дані часто шифрують так, щоб їх могли розшифрувати лише власники єдиного ключа шифрування [3].

Отже, кібербезпека зводиться до сукупності заходів і дій, спрямованих на запобігання, протидію кібератакам чи мінімізацію завданої ними шкоди. У цьому комплексі є 3 основні компоненти:

1) класичні засоби забезпечення інформаційних систем (антивірусні програми, шифрування даних, спеціальна підготовка користувачів);

2) активна оборона (цілеспрямовані та заплановані тести зламання системи, щоб виявити її слабкі сторони);

3) дії в інших сферах (дипломатичних, юридичних, економічних, воєнних) – з метою відлякування від проведення атак.

Захист систем передбачає:

1) спеціальну програму керування ризиками;

2) обмежене довір'я, тобто інші системи трактуються як потенційні джерела загроз;

3) спеціальне програмне забезпечення (далі – ПЗ), яке стежить за обміном інформації з іншими системами;

4) багаторівневий ступінь захисту (тобто зламання одного рівня не дає доступу до даних);

5) систематичні тести безпеки;

6) обмеження доступу користувачів тільки до окремих даних, які їм необхідні;

7) мінімізація функціональності (тільки ті ПЗ та функції, які необхідні).

У цьому контексті варт згадати також відокремлення дуже важливих мереж від інтернету – наприклад, американська система *SIPRNet3* для керування військами. Дозволяється використання обладнання та програмного забезпечення, виробленого у своїй країні чи в союзників (шпигунське ПЗ може бути інстальоване при виробництві – так звані маньчжурські чіпи). Особливо варто звертати увагу на захист критичної інфраструктури, яка включає всі об'єкти, прилади, структури, системи і мережі (фізичні чи віртуальні), які настільки важливі для держави, що їх пошкодження, паралізування чи знищення ослабить безпеку держави і громадян [6, с. 143–161].

Інформаційні технології можуть бути використані в інформаційній боротьбі 2 способами:

1. Допоміжним способом, тобто посилюючи ефект операцій і заходів іншого, ніж інформаційний вид (поширення пропаганди, залучення фінансових засобів для діяльності, рекрутація нових членів, добровольців, симпатиків, внутрішньогрупова комунікація).

2. Безпосереднім способом, як зброя і засіб знищення деяких об'єктів (наступальні операції в кіберпросторі, які можуть спричинити негативні (матеріальні чи нематеріальні) наслідки для об'єктів, які зазнали нападу).

Операції в кіберпросторі поділяються на 2 групи:

1. Наступальні (кібератаки – заходи, що використовують комп'ютерні мережі та спрямовані на маніпуляцію, пошкодження, створення перешкод, знищення інформаційної системи й інформаційної мережі).

2. Оборонні (пасивні чи активні операції, що мають на меті збереження здатності до використання та захист даних).

Кібернетична загроза – небезпека чи можливість спроби пошкодження, переривання роботи чи знищення інформаційної мережі чи системи. Виділяють 5 видів кіберзагроз (кібервійна, кібершпигунство, кібертероризм, кіберзлочинність і хактивізм):

Кібервійна – сукупність дій, орієнтованих на отримання переваги в кіберпросторі під час воєнних дій, напередодні них чи як альтернатива до класичних воєнних дій. У доктрині ЗС США мережеві операції (англ. *CNO – Computer Network Operations*) поділені на 3 види, як-от:

1) експлуатація комп'ютерних мереж;
2) атаки на комп'ютерні мережі;
3) захист комп'ютерних мереж.

Кібервійна стосується атак і захисту комп'ютерних мереж, а експлуатацією займається кібершпигунство.

Атаки на комп'ютерні мережі здійснюються на 4 об'єкти:

1. Логістичні системи (спеціальні програми, що забезпечують постачання військ).

2. Інформаційні системи контролю за промисловими і технологічними процесами (SCADA – *Supervisory Control And Data Acquisition*).

3. Системи керування збройними силами.

4. Системи озброєння (програмне забезпечення літаків, вертольотів, протиповітряних батарей, кораблів, дронів).

У сучасному світі 4 держави лідирують у теоретичних аспектах кібервійни: США, КНР, РФ, Ізраїль. У західній воєнній думці використовується термін «кібервійна», у РФ та КНР – «інформаційна війна». КНР розробляє теорію електронної війни в інтегрованих системах – поєднане, скоординоване та синхронізоване застосування знарядь радіоелектронної боротьби (засобів, що створюють перешкоди в роботі радіолокаторів чи зброї, генеруючої електромагнітний імпульс) зі звичайними кібератаками. У воєнній доктрині РФ кібервійна – елемент інформаційної війни, де використовуються військові, економічні та культурні засоби (доктрина Герасимова). У США переважає вузьке сприйняття кіберпростору як структури комп'ютерних мереж і систем. У рамках повітряних сил (U.S. Air Forces) створено Кібернетичне командування (Cyber Command, CYBERCOM), яке відає кібернетичними операціями ЗС США. Тобто західне сприйняття інформаційної загрози вужче, обмежене технічно-інформаційними кібернетичними аспектами інформаційної боротьби, а східне (російсько-китайське) – ширше, з акцентом на пропаганду [6, с. 143–161].

Кібершпигунство – викрадення даних шляхом зламування інформаційних мереж і комп'ютерних систем.

Кібертероризм – використання кіберпростору для терористичної діяльності (пропаганда, рекрутація нових членів, збір фінансових засобів, комунікація, збір інформації стосовно цілей замаху й іншої розвідувальної інформації).

Кіберзлочинність – використання кіберпростору з метою, що суперечить праву, за допомогою швидкості, віддаленості, шифрування, тобто операція і її виконавець залишаються невикритими. У вужчому розумінні кіберзлочинність – нелегальні дії в кіберпросторі, для яких цей кіберпростір необхідний і дуже помічний (розсилка спаму, крадіж цифрової ідентифікації, підробка електронного підпису тощо). Кіберзлочини поділяються на 2 типи:

1. Такі, де комп'ютери є знаряддям чи засобом, за допомогою якого здійснюється злочин (переслідування, цькування, торгівля забороненими матеріалами, шахрайство, саботаж, крадіж ідентифікації, даних).

2. Такі, де комп'ютерні й інформаційні системи є об'єктами злочину (хакерство, розсилання шкідливого програмного забезпечення, атаки на кшталт DDoS).

Хактивізм (хакер + активізм) – це використання технік і методів хакерства з метою спричинення суспільних змін, тобто містить неегоїстичні політичні, суспільні й економічні цілі. Прикладом можуть бути зламування систем із науковими публікаціями та викладення їх у загальний доступ, ніби це сприятиме науково-технічному прогресові [6, с. 143–161].

Кібератака – навмисна та зловмисна спроба отримати несанкціонований доступ до цифрової системи [3]. Кібератаки можуть впливати на комп'ютери, смартфони або інші пристрої, підключені до інтернету. Основною метою кіберзлочинців часто є крадіжка грошей, персональних даних, облікових даних, інтелектуальної власності або іншої цінної інформації. Зловмисники також можуть мати на меті вивести з ладу або пошкодити систему, на яку спрямована атака. Кібератаки часто передують більш серйозним кіберзлочинам, як-от крадіжка особистих даних, утручання у приватне життя та шахрайство. Найсучасніші кібератаки виводять із ладу промислове обладнання, транспорт, інтернет-зв'язок у цілих регіонах.

Кібератаки становлять значну загрозу для комп'ютерних систем не лише через шкоду, якої вони можуть завдати, але й через низьку вартість проникнення. Одна людина, яка володіє належним програмним забезпеченням, може здійснити атаку проти цілої країни. Навіть більше, зловмисники можуть легко приховати свою особу, місцезнаходження та мотиви. Заходи кіберзахисту повинні постійно стримувати атаки, які можуть різнитися за масштабами та методами, тоді як кібератака має бути успішною лише один раз; незахищений сервер може зазнавати сотні атак на день. Проте межа між кіберзахистом і кібератакою іноді розмивається. Наприклад, шпигунське програмне забезпечення *Pegasus* було розроблене ізраїльською фірмою *NSO Group* для боротьби з тероризмом, стало використовуватися для відстеження та моніторингу впливових осіб без їхнього відома. Програма дозволяє прослуховувати розмови, отримати доступ до електронної пошти, фото чи відео, що містяться в інфікованому смартфоні.

Кібератаки можуть здійснювати як окремі особи, так і організації, але такі атаки відрізняються від кібервійни, яка зазвичай ведеться між країнами. Кібервійна може включати фізичні атаки на цифрову інфраструктуру (наприклад, знищення систем зв'язку або обладнання) на додаток до кібератак [3].

Семантичні кібератаки намагаються обманом змусити жертву надати цінну інформацію або доступ до цінних систем, за допомогою стратегії, відомої як соціальна інженерія. Поширеним прикладом соціальної інженерії є фішинг – практика надсилання шахрайських електронних листів, які видають себе за надійні контакти, із проханням надати особисту інформацію.

Кібератаки можна поділити на дві категорії: нецільові та цільові. Нецільові атаки мають на меті вплинути на якомога більшу кількість пристроїв або сервісів. Наприклад, зловмисники іноді використовують «водяні діри», коли створюється або компрометується вебсторінка, а потім відвідувачі піддаються атаці під час доступу до неї. Іншим прикладом є сканування, коли зловмисники систематично намагаються знайти вразливості в системі, часто шукають точки входу. Цілеспрямовані кібератаки спрямовані на конкретну особу або організацію [3].

Кібератаки можуть здійснюватися з різними цілями:

1. Атаки з метою викрадення даних.

2. Атаки з метою видалення даних (програми англ. *wiper malware*).

3. Атаки DDoS (англ. *Distributed Denial of Service* – розпорошена відмова обслуговування) – блокування функціонування інтернет-сторінки шляхом висилання з різних інфікованих

комп'ютерів великих пакетів даних (атака у 2008 р. на грузинські установи та ЗМІ, щоб збільшити хаос і не дати можливості висвітлити грузинське бачення конфлікту з РФ).

4. Атаки для фізичного пошкодження чи знищення технічної інфраструктури (вірус *Stuxnet* проти іранських атомних об'єктів у 2009–2010 рр.).

5. Атаки з метою дезінформації та маніпуляції [6, с. 143–161].

«Шкідливе програмне забезпечення» – це загальний термін для позначення програм, що використовуються в кібератаках, які зазвичай установлюються на пристрої жертв, коли вони взаємодіють із небезпечним посиланням або електронним листом. Програми-вимагачі, які також називають криптовалютними вимагачами, блокують доступ до цифрового активу або пристрою доти, доки власник не сплатить викуп.

Фішинг – це поширена тактика соціальної інженерії, коли кібератаки видають себе за надійні джерела, зазвичай через електронну пошту, щоб викрасти цінні дані або встановити шкідливе програмне забезпечення.

Атаки типу «людина посередині», які іноді називають атаками підслуховування, відбуваються тоді, коли зловмисники перехоплюють комунікацію між людьми або між людиною та сервером.

Міжсайтовий скриптинг (XSS) – зловмисник заражає вебсайт, часто за допомогою коду JavaScript, що зазвичай передбачає переспрямування на інший сайт або викрадення цільових даних [3].

Першочерговим завданням кібербезпеки має бути запобігання кібератакам. Ефективною стратегією запобігання кібератакам може бути просте оновлення програмного забезпечення й уникнення невідомих посилань. Стратегії управління ідентифікацією та доступом, як-от багатофакторна авторизація, надійні паролі та віртуальні приватні мережі (VPN), забезпечують додатковий рівень безпеки. Організації можуть працювати над запобіганням кібератакам, навчати співробітників принципів кібербезпеки, залучати сторонніх експертів із безпеки або інвестувати у внутрішню команду з кібербезпеки.

Висновки. Кібербезпека залишається однією з найважливіших і найуразливіших сфер у системі безпеки, що зумовлено відносною новизною та стрімким технологічним розвитком інформаційних мереж. Правове врегулювання діяльності в кіберпросторі є актуальним завданням внутрідержавного та міжнародного права.

Література:

1. Computer security. URL: https://www.britannica.com/technology/computer-security (дата звернення: 15.01.2025).

2. Craigen D., Diakun-Thibault N., Purse R. Defining Cybersecurity. *Technology Innovation Management Review.* October 2014. P. 13–21.

3. Cyberattack. URL: https://www.britannica.com/topic/cyberattack (дата звернення: 15.01.2025).

4. FM 3.0 Operations. Headquarters, Department of the Army. October 2022. 280 p. P. 16. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf (дата звернення: 15.01.2025).

5. National Initiative for Cybersecurity Careers and Studies. *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases.* URL: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c (дата звернення: 15.01.2025).

6. Furgacz P. Informacyjny wymiar bezpieczeństwa. *Zagrożenia i instytucje bezpieczeństwa międzynarodowego. Redakcja naukowa E.Cziomer.* Kraków : Oficyna wydawnicza AFM, 2016. S. 143–161.

7. Про основні засади забезпечення кібербезпеки України : Закон України. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.01.2025).

References:

1. Computer security. Retrieved from https://www.britannica.com/technology/computer-security.
2. Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review,* October P. 13–21.
3. Cyberattack. Retrieved from https://www.britannica.com/topic/cyberattack.
4. FM 3.0 Operations. Headquarters, Department of the Army, October 2022, 280 p. P. 16. Retrieved from https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.
5. National Initiative for Cybersecurity Careers and Studies. Explore Terms: A Glossary of Common Cybersecurity Words and Phrases. Retrieved from https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c.
6. Furgacz, P. (2016). Informacyjny wymiar bezpieczeństwa. *Zagrożenia i instytucje bezpieczeństwa międzynarodowego. Redakcja naukowa E.Cziomer.* Kraków: Oficyna wydawnicza AFM, S. 143–161.
7. Zakon Ukrayiny "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" (2017) [Law of Ukraine „On the Basic Principles of Ensuring Cybersecurity of Ukraine"]. (Vidomosti Verkhovnoyi Rady (VVR), № 45, st. 403). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennya: 15.01.2025).

Mykola Genyk. Methodological challenges of defining the terms "cybersecurity" and "cyber threat"

In recent decades, the ways and methods of ensuring national and international security have changed dramatically. The development of computer technology has led to the rivalry in the cyber domain. Cybersecurity permeates all spheres of state and society and has become one of the most important elements of national security. Information-driven countries are developing strategies for confrontation in the cyberspace. It is this sphere that will shape the forms and content of international rivalry and conflicts in the near future. Despite the frequent use of the terms "cybersecurity" and "cyber threat", dictionaries and encyclopaedias do not provide universal definitions of these categories. The purpose of this article is to analyse the main approaches to the definition of these concepts in the scientific literature and legal acts.

The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" defines cybersecurity as "the security of vital interests of a person and citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely identification, prevention and neutralisation of real and potential threats to the national security of Ukraine in cyberspace".

Having analysed the existing definitions, D. Craigen, N. Dyakun-Zybolt and R. Pearce proposed a comprehensive universal inclusive definition, i.e. "cybersecurity" is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.

Cybersecurity remains both one of the most significant and most vulnerable areas in the security system, due to its relative novelty and rapid technological development of information networks. Legal regulation of activities in cyberspace is an urgent task of domestic and international law.

Key words: *cybersecurity, cyberspace, cyberattack, cyberthreat, information systems.*

Відомості про автора:

Ґеник Микола – кандидат історичних наук, доцент кафедри політичних наук,
Прикарпатський національний університет імені Василя Стефаника.