УДК 336.7:340.5:347.7
DOI https://doi.org/10.32782/2524-0374/2022-8/70

КІБЕРБЕЗПЕКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: СПІВВІДНОШЕННЯ ПОНЯТЬ

CYBER SECURITY AND INFORMATION SECURITY: THE RELATIONSHIP OF THE CONCEPTS

Луценко Ю.В., д.ю.н., доцент,
начальник відділу
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

Тарасюк А.В., д.ю.н., доцент,
доцент кафедри кримінального процесу та криміналістики
Львівський державний університет внутрішніх справ

Денисенко М.М., к.ю.н.,
докторант відділу аспірантури і докторантури
Національна академія Служби безпеки України

Стаття присвячена дослідженню актуальних питань, пов'язаних із кібербезпекою та інформаційною безпекою держави. Вагомою складовою успішної протидії широкомасштабній агресії РФ проти України та сталого розвитку інформаційного суспільства в нашій державі останнім часом відбувається не лише за рахунок нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення вичерпних заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави.

У роботі звертається увага на основні напрямки загроз національним кіберпросторам, до яких можна віднести такі: кібершпигунство та воєнні дії, які здійснюються за підтримки або з відома держави; використання Інтернету у терористичних цілях; кіберзлочинність (викрадення персональних даних та відмивання коштів, одержаних незаконним шляхом).

Наголошено, що одним із новітніх викликів в інформаційній сфері є виникнення одноособових і групових хакерських утворень, котрі, керуючись власними принципами та правилами, виступають у соціальних мережах Інтернету і традиційних засобів масової інформації із критикою соціально-політичних негараздів і пов'язаних із цим державних чиновників, олігархів.

Зазначається, що відмінність інформаційної безпеки від кібернетичної, полягає в тому, що перша спрямована на комплексний захист інформаційних ресурсів у будь-якій із можливих форм їх існування, тоді як кібербезпека опікується захистом винятково цифрових форм даних.

У ході дослідження з'ясовано, що важливим чинником, який зумовлює потребу категоріального виокремлення кібербезпеки, є також розроблення деякими державами доктрин ведення спеціальних операцій в інформаційному просторі й втілення цих стратегій проти окремих країн чи інших об'єктів за допомогою спеціалізованих органів і структур.

Ключові слова: безпека, кібернетична безпека, інформаційне право, інформаційні правовідносини, загрози, інформаційна політика, кібербезпека, кіберзагрози, інформаційне законодавство, кіберпростір.

The article is devoted to the study of current issues related to cyber security and information security of the state. An important component of the successful counteraction to the large-scale aggression of the Russian Federation against Ukraine and the sustainable development of the information society in our country is not only due to the increase of technological capabilities for information exchange, but also the deep awareness by all subjects of information relations of the need to implement comprehensive measures to protect information resources and ensure information security of the state.

The work draws attention to the main directions of threats to national cyberspace, which include the following: cyberespionage and military actions carried out with the support or knowledge of the state; use of the Internet for terrorist purposes; cybercrime (theft of personal data and laundering of illegally obtained funds).

It was emphasized that one of the newest challenges in the information field is the emergence of individual and group hacker entities, which, guided by their own principles and rules, appear in social networks of the Internet and traditional mass media with criticism of socio-political troubles and related government officials , oligarchs.

It is noted that the difference between information security and cyber security is that the former is aimed at the comprehensive protection of information resources in any of the possible forms of their existence, while cyber security takes care of the protection of exclusively digital forms of data.

In the course of the study, it was found that an important factor that determines the need for a categorical separation of cyber security is also the development by some states of doctrines of conducting special operations in the information space and the implementation of these strategies against individual countries or other objects with the help of specialized bodies and structures.

Key words: security, cyber security, information law, information legal relations, threats, information policy, cyber security, cyber threats, information law, cyberspace.

Постановка проблеми. Реалії сьогодення постають перед Україною з новими викликами та загрозами. Під час опору різноплановим проявам гібридної війни та бойових дій, розгорнутої РФ, стало очевидним, що наразі наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини та верховенства права, добробуту, миру й безпеки, – а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки і оборони в умовах обмежених ресурсів.

Стан дослідження теми. Питанню кібербезпеки та інформаційної безпеку приділяли увагу такі науковці, як: О. А. Баранов [1], Б. М. Головкін [2], О. Д. Довгань [3], Є. В. Кубанов [4], Т. Ю. Ткачук [5], В. М. Фурашев [6] та інші. Не дивлячись, що більшість наукових праць були виконані у різні часи державотворення, праці цих науковців залишаються фундаментальними та актуальними й дотепер. Наявна збройна агресія РФ проти України, а також протидія інформаційним загрозам світовій безпековій політиці потребують нових фундаментальних підходів у розумінні сучасної кібербезпеки та інформаційної безпеки.

Мета статті. Метою статті є дослідження співвідношення понять кібербезпека та інформаційна безпека в контексті сучасних викликів та загроз.

Викладення основного матеріалу. Запорукою успішної протидії широкомасштабній зовнішній агресії та сталого розвитку інформаційного суспільства в Україні є сьогодні не лише нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення вичерпних заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави [7, с. 45–46], що неможливо без чіткого усвідомлення сутності останньої. Цікавим є і той факт, що самі російські дослідники відзначають, що інформаційна безпека від другої половини XX сторіччя стає одним із найважливіших елементів національної безпеки.

Стаття 17 Конституції України визначає, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [8], що свідчить про набуття категорією «інформаційна безпека» в нормативно-правовому аспекті конституційного статусу [9, с. 30].

Зауважимо, що система інформаційної безпеки, особливо на рівні її вихідних компонентів, може бути структурована за різними критеріями. Щодо кібернетичної безпеки, то Законом України «Про основні засади забезпечення кібербезпеки України» [10] вона визначена 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». Виокремлення кібербезпеки зумовлене специфікою середовища, у якому функціонують інформаційні системи, здійснюється обіг інформації, реалізуються законні інтереси суб'єктів інформаційних процесів. Тож «кібернетичний вимір» властивий усім складовим інформаційної безпеки.

Саме прийняття Закону України «Про основні засади забезпечення кібербезпеки України» означає для України закріплення на законодавчому рівні понятійного апарату з приставкою «кібер» і початок регулювання цифрової економіки в цілому.

Закон розширив і доповнив положення Стратегії кібербезпеки України, затвердженої указом Президента України у 2021 році. Метою стратегії є пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. При цьому основний масив положень стратегії стосується сфери національної оборони і не зачіпає бізнес. Стратегія стала підтвердженням прийнятого Україною курсу на євроінтеграцію, початком якого було підписання та ратифікація Україною Конвенції про кібербезпеку. Країни – члени Ради Європи та деякі інші, які підписали конвенцію, взяли на себе зобов'язання вжити загальних та індивідуально-країнових заходів для запобігання кримінальним правопорушенням у цифровій сфері.

Основним досягненням Закону України «Про основні засади забезпечення кібербезпеки України» є імплементація в правове поле визначень, що стосуються кібербезпеки, кібератак і кіберзахисту.

Не вдаючись до детального аналізу даного закону, можна визначити низку принципово важливих, на нашу думку дискусійних аспектів, які в перспективі слід буде доопрацьовувати та вдосконалювати:

– чи поширюється дія закону на приватні мережі суб'єктів господарювання, адже такі мережі, усе ж таки, підключені до мережі Інтернет;

– неузгодженість та відсутність конкретизації повноважень суб'єктів національної системи кібербезпеки;

– декларативний зміст деяких положень, що потребує прийняття цілої низки конкретизуючих підзаконних нормативно-правових актів.

У поняття «кібербезпека» входить широкий спектр практичних прийомів, інструментів і концепцій, тісно пов'язаних із технологіями інформаційної та операційної безпеки. Відмітна риса кібербезпеки полягає в тому, що вона включає в себе використання інформаційних технологій у наступальних цілях для атак противника. По суті, кібербезпека повинна включати не лише заходи оборони та контрзахисту, а й наступу. Що стосується сучасного стану кібербезпеки України – пріоритетним її напрямом мають стати заходи активної оборони.

Термін «cybersecurity» слід використовувати для позначення практичних методів забезпечення безпеки, що поєднують у собі заходи наступального й оборонного характеру, які включають в себе сукупність або системи інформаційних та (або) операційних технологій або які ґрунтуються на них. Це всього лише одне визначення й одна рекомендація, але, зрозуміло, вони не єдині, на які спираються фахівці. Спостерігається, що деякі спеціалісти починають використовувати цей термін, або не надаючи технології для атак противника, або надаючи технології, які непридатні для таких атак.

У більшості підходів до тлумачення категорії «кібербезпека» немає такого елемента, як «наступальний характер». Проте такий підхід може мати винятково формальний характер, пов'язаний із необхідністю не розголошувати секретну інформацію.

Т. Ю. Ткачук відмічає, що *«кібернетичний*, або *спеціальний програмно-математичний вплив* реалізується з використанням засобів знищення, перекручення або розкрадання інформаційних масивів. Після подолання систем захисту противника з його інформаційних масивів отримується інформація, володіння якою вважається необхідним; доступ до них для законних користувачів при цьому обмежується чи взагалі унеможливлюється. У рамках кібервпливу вдаються також до дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем тощо» [5, с. 132–133].

У Європейській Конвенції з кібернетичних злочинів наведено таке визначення цього поняття: «*кіберзлочини – це правопорушення, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і даних, а також їх неправомірне використання»* [11]. Віртуальний характер кіберзлочинів, а також засоби, за допомогою яких вони здійснюються, дають змогу зловмисникам швидко знищити сліди. Це значно ускладнює з'ясування обставин і пошук винуватців, тож постає нагальна потреба в розробленні нових методів розслідування кіберзлочинів і відповідних законодавчих норм, що регламентують сферу інформаційної безпеки.

«Інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття, – зазначається в Окінавській Хартії глобального інформаційного суспільства. Їх революційний вплив стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду та громадянського суспільства. Інформаційні технології швидко стають життєво важливим стимулом розвитку світової економіки» [12]. Відповідно міжнародне законодавство останнім часом почало приділяти значну увагу кіберзагрозам та протидії їм.

Серед основних загроз національним кіберпросторам стратегії більшості країн визначають:

– *«кібершпигунство та воєнні дії, які здійснюються за підтримки або з відома держави*. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигунства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією» [13]. Так, однією

з найрезонансніших кібератак за останній час стали дії КНДР проти компанії «Sony Pictures Entertainment», внаслідок яких зловмисники заволоділи конфіденційними даними, зокрема й інформацією про комерційні операції компанії [14];

– *«використання Інтернету у терористичних цілях»*. Терористичні угрупування використовують Інтернет із метою пропаганди, збирання коштів і вербування прихильників, та інші протиправні дії [13];

– *«кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом»*. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе програмне забезпечення.

Відповідно, національні законодавства країн, як правило, регулюють питання:

– захисту персональних даних (Естонія, Іспанія, Канада, Швеція, Нідерланди, Фінляндія);

– захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (Естонія, Італія, Канада, Польща, США);

– захисту дітей (США);

– захисту важливих об'єктів інфраструктури та інформаційних систем (Франція) [15, с. 244].

По-різному й трактують поняття «кібербезпека» в зарубіжних країнах:

– сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору (*Політика захисту кіберпростору Республіки Польщі*);

– бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму (*Стратегія кібербезпеки Німеччини*);

– заходи з попередження шкоди від збоїв у роботі інформаційно-комп'ютерних технологій та її усунення (*Національна стратегія кібербезпеки Королівства Нідерландів*);

– бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою (*Стратегія безпеки та оборони інформаційних систем Франції*) [16, с. 143].

Усе це зайвий раз доводить нагальну потребу розробки та прийняття Закону України «Про інформаційну безпеку України» як базового нормативно-правового акту, що регулюватиме відповідні питання [17, с. 89]. Такий закон як фундамент для побудови ефективної стратегії інформаційної безпеки має містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи її забезпечення, механізм її функціонування, повноваження і схему взаємодії суб'єктів забезпечення інформаційної безпеки тощо [18, с. 21].

Це зумовлюється і досить динамічним розвитком інформаційного суспільства. У цьому ракурсі ми поділяємо думку В. М. Брижка, що в наш час життєдіяльність світової цивілізації все більше спрямовується інформаційною сферою, яка завдяки інформаційно-технологічним змінам, що почалися наприкінці XX століття, об'єктивно зумовила появу нового типу суспільства – інформаційного суспільства [19, с. 20]. Досить цікавою в ракурсі цього дослідження є думка В. Фурашева про те, що інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на задоволення інформаційних потреб усіх живих істот на Землі [20, с. 45].

Підсумовуючи, зазначимо, що проведена диференціація інформаційної та кібернетичної безпеки не є чисто умоглядною. Її необхідність, на концептуальному рівні, зумовлена переходом людства на стадію інформаційного суспільства – нової соціально-економічної формації. І якщо донедавна питаннями забезпечення кібербезпеки переймалися й опікувалися здебільшого військові в межах інформаційного та радіоелектронного протиборства, то нині подібні проблеми стосуються і держави загалом, і суспільства, і кожної окремої особи.

Причин такого стану справ чимало. Основними з них убачаються такі:

– вторгнення інформаційних технологій в усі сфери життєдіяльності, розбудова на їхній базі державних, військових та інших управлінських систем;

– розвиток державних програм, спрямованих на формування інформаційного суспільства (електронне урядування тощо);

– недосконаліть міжнародної та національної правових засад відповідальності за правопорушення в інформаційній сфері;

– брак міжнародно-правової заборони застосування інформаційної зброї, проведення інформаційних операцій та війн;

– недостатня участь міжнародних інститутів у сфері забезпечення інформаційної безпеки світової спільноти;

– стрімкий розвиток інформаційних технологій воєнного призначення, зокрема засобів ураження не лише військових, а й цивільних управлінських систем;

– створення та застосування спеціальних сил і засобів ураження критично важливої інформаційної інфраструктури, зокрема й шкідливого програмного забезпечення, яке уражає автоматизовані системи управління промисловими, енергетичними, транспортними й іншими об'єктами критично важливої інфраструктури країни;

– створення деякими державами доктрин ведення агресивних і підривних дій в інформаційному просторі й утілення цих стратегій проти окремих країн чи інших об'єктів;

– виникнення таких форм протесту громадян проти державної політики чи дій (бездіяльності) владних органів, які супроводжуються посяганнями на інформаційну інфраструктуру тощо.

Вважаємо за доцільне детальніше розглянути деякі із наведених чинників з урахуванням потреби виокремити із сукупності безпекових різновидів безпеку кібернетичну. Так, одним із новітніх викликів в інформаційній сфері є виникнення одноособових і групових хакерських утворень, котрі, керуючись власними принципами та правилами, виступають у соціальних мережах Інтернету і традиційних ЗМІ із критикою соціально-політичних негараздів і пов'язаних із цим державних чиновників, олігархів, закликають до протестів тощо. На відміну від хакерів «звичайних», «хактивісти» [21] оголошують себе борцями за справедливість, не приховуючи своєї діяльності. Це свідчить про те, що певна частина хакерської спільноти, виявивши небайдужість до соціально-економічних процесів у країні, прагне вплинути на них за допомогою своїх специфічних засобів, намагаючись провести кібератаки на інформаційні ресурси урядових, військових, бізнесових та інших структур, зорганізувати масові протестні акції. Діяльність таких утворень, їхня часто нігілістична ідеологія, безапеляційно негативне ставлення до всіх державних органів і службовців убачається серйозною загрозою для державного управління, зокрема й для керування збройними силами та їхньої інфраструктури. Останніми роками чимало фахівців з інформаційної безпеки вважають хактивізм чи не провідною негативною тенденцією. Повною мірою це стосується й України з огляду на транскордонний характер цього явища.

Оскільки хактевісти створюють і вдосконалюють шкідливе програмне забезпечення, котре розробляється задля ураження автоматизованих систем управління, потрібні нові підходи до забезпечення безпеки об'єктів критичної інфраструктури, зокрема й військово-промислового комплексу, приділяючи серйозну увагу безпеці систем управ-

ління, запобіганню реалізації можливих загроз, виявленню й усуненню «слабких» щодо можливих атак місць.

Ключовим поняттям у термінологічному словосполученні «інформаційна безпека даних» є «інформаційна безпека». Це – стан захищеності особи й інших суб'єктів (установ, організацій, спільнот, держави й ін.) та їхніх законних інтересів від будь-яких негативних загроз і впливів в інформаційному просторі. Складові інформаційної безпеки відповідають головним властивостям інформації – конфіденційність (доступ до інформації відповідно до визначених на це прав), цілісність (гарантування від несанкціонованих змін), доступність (відкритість для будь-яких суб'єктів відповідно з наданим доступом).

Відмінність інформаційної безпеки від кібернетичної, таким чином, полягає в тому, що перша спрямована на комплексний захист інформаційних ресурсів у будь-якій із можливих форм їх існування, тоді як кібербезпека опікується захистом винятково цифрових форм даних.

Важливим чинником, який зумовлює потребу категоріального виокремлення кібербезпеки, є також розроблення деякими державами доктрин ведення спеціальних операцій в інформаційному просторі й втілення цих стратегій проти окремих країн чи інших об'єктів за допомогою спеціалізованих органів і структур. Сьогодні так звані центри кібернетичного захисту (чи з іншою назвою, але подібними функціями) функціонують у Австралії, Великій Британії, США, ФРН, Китаї, Ізраїлі, Ірані та інших країнах. Основні завдання цих структур (захист, спільно зі спецслужбами та правоохоронними органами, органів державного управління й об'єктів критичної інфраструктури), їхня підпорядкованість здебільшого військовим відомствам, та й навіть самі їхні назви свідчать, що головна їх мета в усіх країнах – забезпечення безпеки державного, зокрема військового, управління.

Слід зазначити, що останніми роками суттєво змінилося ставлення до місця та ролі інформаційного протиборства, яке нині вважається цілком самостійним і вельми ефективним інструментом боротьби з противником, а не допоміжним, супутнім бойовим діям засобом. І в цій своїй новій іпостасі інформаційне протиборство набуває значно ширшого змісту, далеко виходячи за межі традиційних воєнних дій. Воно здатне швидко вивести з ладу головні сили й засоби ворожої країни, не завдаючи при цьому невідновної фізичної шкоди її господарству, критичній інфраструктурі й території, за допомогою не заборонених міжнародно-правовими нормами потужних засобів, котрі, крім того, украй важко виявити й нелегко знешкодити.

Висновки. Отже, подальший розвиток системи забезпечення безпеки інформаційної сфери України, вбачається надзвичайно важливим, особливо в умовах безпрецедентної інформаційної війни та бойових дій, що їх розгорнула проти нашої країни Російська Федерація. Задля виконання цього життєво важливого завдання потрібні узгоджені спільні зусилля всіх без винятку державних інституцій, збройних сил, спеціальних служб, правоохоронних органів, наукових установ, громадських організацій, приватних структур, засобів масової інформації й окремих громадян.

Слід також акцентувати увагу на проблемі істотних розбіжностей між сучасними інформаційними відносинами та їхнім нормативно-правовим регулюванням, яке неналежним, на наш погляд, чином враховує рівень небезпечності нових негативних чинників у сфері інформаційної безпеки. Причому це стосується як вітчизняного законодавства, так і міжнародного права.

ЛІТЕРАТУРА

1. Баранов О. А. Інтернет речей (IoT) і блокчейн. *Інформація і право*. № 1(24)/2018. С. 59−71.
2. Holovkin B. M., Tavolzhanskyi O. V., Lysodyed O. V. Corruption as a cybersecurity threat in conditions of the new world's order. *Linguistics and Culture Review*. 2021. Vol. 5, № (S3). P. 499–512. URL: https://doi.org/10.21744/lingcure.v5nS3.1538.
3. Довгань О. Д. Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1. С. 86−100.
4. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Аспекти публічного правління*. Том 6, № 8. 2018. С. 49−55.
5. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ «*Видавничий дім «АртЕк*», 2018. 422 с.
6. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162−169.
7. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 42−46.
8. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення 20.07.2022).
9. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. *Науково-технічний збірник*. Київ, 2004. С. 30−33.
10. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року: URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення 20.08.2022).
11. Европейская Конвенция по киберпреступлениям. URL : http://inter.criminology.onua.edu.ua/?p=2263 (дата звернення 29.08.2022).
12. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. URL: http://zakon4.rada.gov.ua/laws/show/998_163 (дата звернення 30.08.2022).
13. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (дата звернення 30.08.2022).
14. National Cyber Security Action Plan (2019-2024). Public Safety Canada 2019. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx (дата звернення 30.08.2022).
15. The Department Of Defense Cyber Strategy URL: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата звернення 30.08.2022).
16. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. Актуальні проблеми управління інформ. безпекою держави: мат. наук.-практ. конф. (Київ, НА СБ України. 24.05.17). 2017. С. 142–144.
17. Довгань О. Д., Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1. С. 86−100.
18. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія; НАПрН України, НДІІП. Київ: Видавничий дім «АртЕк». 2017. 107 с.
19. Брижко В. М. *Філософія права*: герменевтика в сфері інформаційного права. *Правова інформатика*. 2014. № 1(41). С. 18−22.
20. Ланде Д. В., Фурашев В. М. Основи інформаційного і соціально-правового моделювання: монографія. Київ: ТОВ «ПанТот», 2012. 144 с.
21. Hacktivist («хакер» +«активіст») – активний член хакерської групи: Звіт про тенденції та ризики інформаційної безпеки за підсумками першого півріччя 2011 року IBMX-Force URL: http://www.ibm.com/news/ru/ru/2011/09/29/q138278b96341x82.html (дата звернення 30.08.2022).