УДК 32.019.51:323.28:323.2(477)

АЛЕКСЕЄВА О.А., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6629-3606.

КІБЕРЗБРОЯ: ПОНЯТТЯ, ЇЇ ПРОЯВИ ТА ЗАХОДИ ПРОТИДІЇ

DOI...

Анотація. *Стаття присвячена аналізу поняття "кіберзброя", її проявів та заходів протидії. Висвітлено існуючі у юридичній літературі точки зору до визначення кіберзброї, виділено її ознаки та види. Встановлено коло злочинних цілей використання кіберзброї. Зазначається, що кіберзброя стала серйозним засобом інформаційного впливу у кіберпросторі як новому театрі воєнних дій. Проаналізовано зарубіжні та вітчизняні підходи до визначення кіберпростору. Внесені пропозиції щодо удосконалення протидії застосуванню кіберзброї у національному кіберпросторі. Звернута увага на необхідність реалізації законодавчих ініціатив у сфері протидії кібератакам.*

Ключові слова: *кіберзброя, агресія, кібератака, протидія кіберзброї, кібервійська.*

Summary. *The article is devoted to the analysis of the concept of "cyber weapons". Modern approaches to its definition are highlighted, its signs and types are defined. The range of criminal purposes for the use of cyber weapons has been established. It is noted that cyber weapons have become a serious means of informational influence in cyberspace as a new theater of military operations. Foreign and domestic approaches to defining cyberspace are analyzed. Proposals were made to counter the use of cyber weapons in national cyberspace. Attention is drawn to the need to implement legislative initiatives in the field of combating cyberattacks.*

Keywords: *cyberweapons, aggression, cyberattack, countering the use of cyberweapons, cyberwarfare.*

Постановка проблеми. Наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, мають негативний вплив на стан кібербезпеки держави [1]. Одним із сучасних викликів для України у сфері кібербезпеки є мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі. Стратегія кібербезпеки України найбільш небезпечною загрозою кібербезпеці України називає гібридну агресію рф проти нашої держави у кіберпросторі [2]. Зазначається, що "держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки рф спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності" [2].

Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності [2].

У Стратегії забезпечення державної безпеки констатується посилення кіберзагроз для критичної інфраструктури, пов'язаних з тимчасовою окупацією частини території

України, триваючими гібридними впливами з боку суб'єктів розвідувально-підривної діяльності, погіршенням технічного стану такої інфраструктури та намаганнями несанкціонованого втручання в її функціонування, зокрема фізичного і кіберхарактеру [3].

На сьогодні, немає підстав вважати, що інтенсивність кібератак буде зменшуватися. Питання лише в тому, на чому вони будуть фокусуватися [4].

Результати аналізу наукових публікацій. Сучасні загрози застосування кіберзброї висвітлені у роботах А. Білюги [5], П. Біленчука, М. Гуцалюка [6], Д. Дубова [7], Ю. Калайди [8] та ін. Проблеми застосування кіберзброї в інформаційних війнах висвітлені у працях В. Брижка, М. Швеця [9], Г. Почепцова [10].

Різні аспекти цієї тематики у своїх наукових працях розкривали зарубіжні дослідники П. МакБарні (P. McBurney), С. Морган (S. Morgan) [11], С. Меле (S. Mele) [12], Т. Рід (T. Rid) [13].

Однак, не зважаючи на значну кількість наукових праць, присвячених кіберзброї, в інформаційному праві немає єдиних підходів до визначення поняття "кіберзброя", її ознак та видів. Відсутні системні підходи до формування системи протидії застосуванню кіберзброї у національному кіберпросторі.

Метою статті є з'ясування сутності та ознак кіберзброї, визначення її потенційного масштабу і цілей, внесення пропозицій для вжиття заходів протидії застосуванню кіберзброї у національному кіберпросторі.

Виклад основного матеріалу. Для провідних країн світу кіберпростір вже давно став новою ареною протистояння. Одним з можливих театрів воєнних дій він визнаний і в Україні [2].

У Доктрині НАТО щодо ведення операцій у кіберпросторі зазначено, що кіберпростір – це глобальний домен з'єднаних між собою комунікаційних, інформаційних та інших електронних систем, мереж та їхніх даних, у яких обробляється, зберігається та передається інформація [14].

Інший підхід до визначення кіберпростору міститься в керівних документах Збройних Сил США, де кіберпростір визначається як глобальний простір в межах інформаційного середовища, що складається з взаємозалежної мережі об'єктів ІТ-інфраструктури, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори та контролери [15].

Визначення кіберпростору передбачено і в чинному законодавстві України.

В Законі України "Про основи забезпечення кібербезпеки України" кіберпростір визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [16].

У Стратегії кібербезпеки проголошено, що Україна:

прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави;

розвиватиме національний кіберпростір як глобальний, відкритий, вільний, стабільний та безпечний задля захисту суверенітету держави, соціального і економічного розвитку суспільства [2].

Отже, розвиток кіберпростору, поява нових ІТ-технологій, активне використання мережі Інтернет зі злочинною метою зумовили виникнення абсолютно нового феномену, який отримав назву "кіберзброя".

На міжнародному рівні не існує загальновизнаного визначення кіберзброї. Не визначеним це поняття залишається і в Україні. Численними є визначення різних видів зброї у військових словниках та довідниках. Однак, сьогодні бракує визначень поняття "кіберзброя", а також досліджень щодо її природи, ознак та видів. Існують різні точки зору на це поняття серед вітчизняних і зарубіжних вчених.

На думку Білюги А.Д., кіберзброя – технічно-технологічний комплекс, що складається зі спеціального комп'ютерного обладнання, технологій та програм, призначених для цілеспрямованого порушення роботи інформаційно-технічних систем, викривлення, пошкодження, заволодіння або знищення критично важливої інформації, що може призвести до катастрофічних наслідків техногенного характеру [5, с. 45].

Горбенко В.І. вважає, що термін "кіберзброя" відноситься до інструментів, технологій або методів, які використовуються в кіберпросторі для здійснення кібератак, кібервійських операцій або впливу на інформаційні системи та мережі [17].

Американські вчені Т. Рід та П. МакБарні розглядають кіберзброю як один з видів зброї: комп'ютерний код, який використовується з метою погрози чи заподіяння фізичної, функціональної та психологічної шкоди структурам, системам чи фізичним особам [13].

Італійський дослідник С. Меле робить висновок, що кіберзброєю може бути пристрій чи будь-який набір інструкцій для комп'ютера, що використовується в конфліктах між державними та недержавними суб'єктами з метою заподіяння (прямо чи опосередковано) фізичних збитків людям чи предметам, а також пошкодження та/або виведення з ладу інформаційних систем [12, с. 7].

До кіберзасобів можна віднести будь-який пристрій, прилад чи механізм, обладнання чи програмне забезпечення, що використовується для ведення кібератак [18, с. 141-142].

Окрім стислих технічних характеристик, наведені визначення кіберзброї свідчать про геополітичний масштаб її застосування, тяжкість наслідків та множинність проявів такої зброї.

Різноманітними є види кіберзброї. Серед основних груп кіберзброї за принципом дії виділяють: мережеву кіберзброю, попередньо встановлену кіберзброю, проникаючу кіберзброю, електромагнітну зброю, комунікаційну кіберзброю [19].

Прикладами кіберзброї визнаються: 1) віруси та програми-шпигуни – збирання конфіденційної інформації або виконання певних дій на комп'ютері без дозволу користувача; 2) віруси-троянці – приховується під виглядом корисної програми або файлу і виконує шкідливі дії при певній активації; 3) комп'ютерні черви – здатні самостійно розповсюджуватися через комп'ютерні мережі, використовують вразливості у програмному забезпеченні; 4) DDoS-атаки (Distributed Denial of Service) – спрямовані на перевантаження веб-серверів або мережевих інфраструктур шляхом надмірного надходження запитів або трафіку; 5) фішинг – один із видів соціально-інженерної атаки, маскування зловмисника як легальні особи або організації для отримання конфіденційної інформації. Технічний фішинг – маскування комп'ютерної системи під виглядом легальної; 6) використання штучного інтелекту – для виявлення вразливостей, розвідки, аналізу Великих Даних та розробки нових методів атак [17].

Найбільш відомим прикладом застосування кіберзброї став комп'ютерний вірус "Stuxnet", який у 2010 р. був скерований проти енергосистем Ірану [20]. Метою вірусу були комп'ютерні системи, які контролювали атомні електростанції. Фактично "Stuxnet" вважається різновидом кіберзброї, створеним за підтримки певної держави (держав). Створення комп'ютерного вірусу "Stuxnet" стало можливим завдяки масштабній

розвідувальній операції на об’єкті критичної інфраструктури, де були порушені основні принципи побудови системи безпеки комп’ютерних систем [5, с. 44].

Зауважимо, що кіберзброя може бути використана для різних злочинних цілей, включаючи розвідку, руйнування об’єктів критичної інфраструктури, шпигунство, міжнародний тероризм, вплив на суспільну думку або завдання шкоди ворогові за допомогою кіберзасобів [17] тощо. Фактично будь-яке суспільно небезпечне діяння у кіберпросторі може бути вчинене за допомогою кіберзасобів, що є ознакою кіберзлочину.

А.Д. Білуга робить обґрунтований висновок, що “кіберзброя є важливим, ефективним і відносно економним компонентом проведення нелегальних операцій у кіберпросторі, що породжує такий негативний феномен, як кіберзлочинність. Кіберзлочини як складова організованої злочинності мають тенденцію до зростання і набули транснаціонального характеру” [5, с. 45].

Дійсно, сучасна модель глобалізації уможливила поширення міжнародного тероризму та міжнародної злочинності, зокрема в кіберпросторі [21].

Сьогодні однією з найбільш небезпечних загроз є організовані та спонсоровані урядами інших держав кібератаки, що пов’язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію [2].

У зв’язку з цим Стратегія кібербезпеки України відзначає:

поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов’язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров’ю людей тощо;

використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності;

інтенсивність проявів кіберзлочинності, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат [2].

На основі аналізу кіберінцидентів та актів національного законодавства у сфері кібербезпеки можна дійти висновку, що національний кіберпростір є повноцінним театром воєнних дій, де фіксуються масштабні прояви його використання терористичними та іншими злочинними організаціями, спецслужбами зарубіжних держав, окремим злочинцями для вчинення низки кримінальних кіберзлочинів. Непоодинокими є прояви застосування вірусних програм, унаслідок чого на урядових порталах мали місце “викрадення” чи пошкодження службової інформації, світові економічні компанії та об’єкти атомної енергетики зазнавали величезних збитків [5, с. 45].

З аналізу суспільно небезпечних проявів кіберзброї видно, що ця зброя застосовується, як правило, під час кібератак.

В ст. 1 Закону України “Про основні засади забезпечення кібербезпеки України” під кібератакою розуміються спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або

сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [16].

Потенційними цілями кібератак можуть бути об'єкти атомної енергетики, продовольчої промисловості, транспорту, електро- та водопостачання, національної критичної інфраструктури, хімічні й біологічні об'єкти тощо.

Країна-агресор для реалізації власних стратегічних цілей в Україні, у тому числі компрометації її державності, системно застосовує кібератаки, продовжуючи гібридну агресію у кіберпросторі України [3].

Ще у березні 2014 року російська кіберзброя під назвою "Змія" або "Уроборос" спричинила хаос в українських державних системах [22].

Наприкінці червня 2017 року масштабна кібератака з використанням вірусу "Petya" заблокувала комп'ютерні системи вітчизняних компаній. Принципова новизна цього вірусу – він містить безліч інструментів, за допомогою яких "ламає" файли в комплексі – від розшифровки паролів до видалення історії свого "втручання". Ці інструменти відомі вже давно, але до цього моменту не було жодного прикладу, коли хакери їх використовували в комплексі [23]. Таким чином, Україна стала першою ціллю нової кіберзброї [23].

Від початку повномасштабного вторгнення росії в Україні зареєстрували та дослідили понад 1500 кібератак. Більшість із них здійснено з боку країни-агресора [24].

У травні 2024 року Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Державній службі спеціального зв'язку та захисту інформації України (Держспецзв'язку), зафіксувала значне зростання кількості кібератак проти України з боку рф. Зокрема, 20 травня 2024 року фахівці CERT-UA зафіксували дві масштабні компанії з розповсюдження шкідливого програмного забезпечення SMOKELOADER [25].

Кібервійни рф включають DoS-атаки, хакерські атаки, розповсюдження дезінформації та пропаганди, участь спонсорованих державою команд у політичних блогах, спостереження в Інтернеті за допомогою технології СОРМ, переслідування кібердисидентів та інші активні заходи [26].

Відповідно до оприлюднених Держспецзв'язку даних, Україна зазнала понад 3000 DDoS-атак з боку країни-агресора: постійно розповсюджується шкідливе програмне забезпечення, здійснюються фішингові розсилки та інші прояви війни у кіберпросторі [27].

Метою застосування країною-агресором кіберзброї під час кібератак є: 1) втрата функціональності об'єкта – кібератаки можуть спричинити втрату функціональності об'єкта, зупинити роботу його систем або призвести до неправильної роботи; 2) знищення чи пошкодження даних – кібератаки можуть вплинути на цілісність даних об'єкта, що може призвести до їхнього втрати, пошкодження або зміни; 3) порушення конфіденційності інформації – кібератаки можуть призвести до несанкціонованого доступу до конфіденційної інформації об'єкта, що може викликати серйозні проблеми щодо захисту даних та конфіденційності; 4) зміна або викривлення інформації – кібератаки можуть використовуватися для зміни чи викривлення інформації, що може викликати помилкові рішення чи спричинити довіру до об'єкта; 5) підрив робочих

процесів – кібератаки можуть порушити нормальну діяльність об’єкта, зменшити продуктивність або спричинити зброї в роботі систем та процесів; 6) психологічний тиск та деморалізація – кібератаки можуть викликати психологічний тиск на персонал об'єкта, призвести до деморалізації та зниження ефективності роботи [17].

Масштаб та підвищений рівень суспільної небезпечності застосування кіберзброї зумовлюють потребу посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди [2].

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей. Поряд з проголошеними у Стратегії кібербезпеки цілями “Дієва кібероборона” (С. 1), “Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму” (С. 2), Україна має забезпечити безперервне здійснення заходів з виявлення, запобігання та припинення актів застосування кіберзброї у національному кіберпросторі зі злочинною метою. Крім цього, набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об’єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об’єктами [2].

Створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей визнано главою держави невідкладним заходом у сфері кібербезпеки [28].

До речі, належна правова основа для стримування збройної агресії рф у кіберпросторі та надання відсічі агресору передбачена у проекті Закону України “Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури” (реєстр. № 8087 від 29.09.22 р.), де, серед іншого, заплановано створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем [29]. Реалізація цього акта сприятиме якісному удосконаленню законодавства України у сфері кібербезпеки та захисту від кібератак державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури.

Висновки.

Під кіберзброєю слід розуміти спеціальні програмні, технічні та інші технологічні засоби і обладнання, призначені для досягнення злочинних цілей у кіберпросторі. Такими цілями можуть бути розвідка, кібердиверсія, кібертероризм, інші прояви кіберзлочинності, знищення або пошкодження об’єктів критичної інфраструктури, вплив на суспільну думку або завдання шкоди людині, суспільству чи державі.

Для посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі вважається за доцільне:

визначити дієву протидію застосуванню кіберзброї у кіберпросторі як стратегічну ціль Стратегії кібербезпеки України;

розробити методику протидії застосування кіберзброї, яка сприятиме запобіганню масштабним кібератакам і кіберінцидентам у кіберпросторі;

створення кібервійськ, до завдань яких належатиме забезпечення захисту критичної інформаційної інфраструктури від кібератак, проведення превентивних

наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [2];

оптимізувати координацію суб'єктів забезпечення кібербезпеки з метою ефективної протидії застосуванню кіберзброї у сучасному безпековому середовищі.

Як вважаємо, реалізації висловлених пропозицій сприятиме впровадження дієвих механізмів залучення міжнародних партнерів та фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

Використана література

1. Стратегія морської безпеки України: Указ Президента України від 17.07.24 р. № 468/2024. URL: https://www.president.gov.ua/documents/4682024-51461 (дата звернення: 20.08.2024).
2. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 20.08.2024).
3. Стратегія забезпечення державної безпеки: Указ Президента України від 16.02.22 р. № 56. URL: https://www.president.gov.ua/documents/562022-41377 (дата звернення: 20.08.2024).
4. Кібератаки, артилерія, пропаганда: загальний огляд вимірів російської агресії. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi (дата звернення: 20.08.2024).
5. Білюга А.Д. Кіберзброя: сучасні загрози національній безпеці та шляхи протидії. *Наука і оборона* 2021. № 2. С. 42-49. URL: file:///C:/Users/user/Desktop/%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96/239047-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-665063-1-10-20230928.pdf (дата звернення: 20.08.2024).
6. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти / П.Д. Біленчук, М.В. Гуцалюк, О.В. Кравчук, М.В. Козир ; за заг. ред. П.Д. Біленчука. Київ: Наука і життя, 2008. 291 с.
7. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.
8. Калайда Ю.П. Агресія РФ у кіберпросторі як загроза національній безпеці України. *Інформація і право*. № 1(48)/2024. С. 188-194.
9. Брижко В., Швець М. е-боротьба в інформаційних війнах та інформаційне право / за ред. М. Швеця. Київ: ТОВ "ПанТот", 2007. 218 с.
10. Почепцов Г.Г. Информационные войны. (Серия: Образовательная библиотека); москва: Рефл-бук, 2001. 576 с.
11. Morgan S. Report: Cyberwarfare in the C-Suite: Cybercrime facts and statistics / 2021: Jan 21, 2021. Cybersecurity Ventures. Cybercrime Magazine. URL: https://cybersecurityven tures.com /wp-content/uploads/2021/01/ Cyberwarfare-2021- Report.pdf (дата звернення: 20.08.2024).
12. Mele S. Legal Considerations on Cyber-Weapons and Their Definitions. *Journal of Law & Cyber Warfare*. 2014. Vol. 3. № 1. P. 52-69. URL: https://www.jstor.org/stable/26432559 (дата звернення: 20.08.2024).
13. Rid T., McBurney P. Cyber-Weapons *The RUSI Journal*. 2012. Vol. 157, Issue 1. P. 6-13. URL: https://doi.org/10.1080/ 03071847.2012.664354. (дата звернення: 20.08.2024).
14. Allied Joint Doctrine for Cyberspace Operations: NATO Standard AJP-3.20: Edition A Version 1: January 2020. NATO Standardization Office. URL: https://nso.nato.int/nso/zPublic/ap/ PROM/AJP-3.20%20E DA%20V1%20E.pdf. (дата звернення: 20.08.2024).
15. Dictionary.com. URL:http://dictionary.reference.com/browse/cyber (дата звернення: 20.08.2024).
16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.08.2024).

17. Горбенко В.І. Кібервійни та кібербезпека в сучасному світі: лекція. URL: https:file:///C:/Users/user/Desktop/%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96/%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D1%8F%206%20(1).pdf (дата звернення: 20.08.2024).

18. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. URL: https://doi.org/10.1017/CBO978113 9169288 (дата звернення: 20.08.2024).

19. Бабенко В.Г. Основні групи кіберзброї та особливості її застосування: матеріали всеукр. наук-практ. конф. *Актуальні задачі і досягнення у сфері кібербезпеки*, м. Кропивницький, 23-25 лист. 2016. Черкаський державний технологічний університет. 2016. С. 23-24.

20. Stuxnet – перша цифрова зброя-вірус? *BBC News Україна*. URL: https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh (дата звернення: 20.08.2024).

21. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392/202. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.08.2024).

22. Russia's cyber weapons hit Ukraine: How to declare war without declaring war. Christian Science Monitor. URL: smonitor.com/Commentary/Global-Viewpoint/2014/0312/Russia-s-cyber-weapons-hit-Ukraine-How-to-declare-war-without-declaring-war (дата звернення: 20.08.2024).

23. Україна стала першою ціллю принципово нового виду кіберзброї. URL: https://www.ukrinform.ua/rubric-technology/2259655-ukraina-stala-persou-cillu-principovo-novogo-vidu-kiberzbroi.html (дата звернення: 20.08.2024).

24. Стало відомо, скільки ворожих кібератак зареєстрували в Україні. – (02.01.2023 р.). URL: https://ua.news/ua/ukraine/stalo-izvestno-skolko-vrazheskih-kiberatak-zaregistrirovali-v-ukraine (дата звернення: 20.08.2024).

25. Держспецзв'язку попереджає про збільшення кількості кібератак проти бухгалтерів URL: https://lb.ua/society/2024/05/22/614642_derzhspetszvyazku_poperedzhaie_pro.html (дата звернення: 20.08.2024).

26. Кібервійни рф. URL: https://uk.wikipedia.org/wiki/%D0%A0 %D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D1%96_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B2%D1%96%D0%B9%D0%BD%D0%B8 (дата звернення: 19.08.2024).

27. У 2022 році кількість кібератак на Україну зросла майже втричі. 90 % хакерських груп з рф контролюють силовики. URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата звернення: 19.08.2024).

28. Про невідкладні заходи з кібероборони держави: рішення РНБО України від 14.05.21 р.: Указ Президента України від 26.08.21 р. № 446. URL: https://zakon.rada.gov.ua/laws/show/n0053525-21#Textє (дата звернення: 19.08.2024).

29. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проект закону України (реєстр. № 8087 від 29.09.22 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881 (дата звернення: 19.08.2024).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~