УДК 32.019.51:323.28:323.2(477)

КАЛАЙДА Ю.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-1408-2145.

АГРЕСІЯ РФ У КІБЕРПРОСТОРІ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Анотація. *Стаття присвячена аналізу агресії рф у кіберпросторі. Висвітлено історію кібервійни України з рф, виділено її ознаки і етапи. Проаналізовано законодавство України у сфері забезпечення кібербезпеки. Внесені пропозиції щодо напрямів реформування сектору безпеки і оборони у цій сфері, а також реалізації законодавчих ініціатив у сфері протидії кібератакам. Наголошено на необхідності якнайшвидшого створення та функціонування кібервійськ у складі Збройних Сил України.*

Ключові слова: *кібервійна, агресія, кібератака, протидія кібератакам, кібервійська.*

Summary*. The article is devoted to the analysis of Russian aggression in cyberspace. The history of Ukraine's cyber war with the Russian Federation is highlighted, its features and stages are defined. The legislation of Ukraine in the sphere of ensuring cyber security has been analyzed. Proposals were made regarding the directions of reforming the security and defense sector in this area, as well as the implementation of legislative initiatives in the field of countering cyber attacks. The need for the creation and functioning of cyber troops as part of the Armed Forces of Ukraine was emphasized.*

Постановка проблеми. Війна рф проти України має багато вимірів, одним з яких є кібернетичний. У кібернетичній площині протистояння України з рф має тривалу історію. Перші атаки хакерів рф на інформаційні системи державних установ України були зафіксовані ще в 2013 році під час масових протестів на Майдані. З 2014 року кібервійна переросла у відкрите збройне протистояння – російсько-українську війну [1], одним з важливих елементів якої стали кібератаки на об'єкти критичної інфраструктури України. Найбільш потужна хакерська атака на Україну з боку рф відбулася в червні 2017 року із використанням вірусу NotPetya. З 24 лютого 2022 року кібервійна набула нових обертів в умовах неприкритої агресії рф проти України. Протягом 2022 року в Україні сталося майже втричі більше кіберінцидентів, геолокація яких пов'язана з РФ, ніж у 2021 році [2]. Хакери рф здійснюють кожного дня у середньому понад десять кібератак на Україну [3].

Це різні типи кібератак, іноді дійсно масові, іноді досить витончені. Цілі у цих атак доволі різні: державні ресурси, об'єкти критичної інфраструктури тощо [4, с. 163]. Кібератаки рф, не визнають жодних правил – під ударом інфраструктура, гуманітарні організації, приватні та державні компанії. Хакери рф не приймають обмежень та не визнають кордонів, атакуючи різні держави, якщо вони допомагають Україні [5].

Результати аналізу наукових публікацій. Проблеми застосування інформаційної зброї в інформаційних війнах висвітлені у працях В. Брижка [6], О. Данильяна, О. Дзьобаня, В. Пилипчука, Г. Почепцова [7].

Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану висвітлені у роботах Я. Мануілова [8] та С. Краснікова [4].

Інформаційно-психологічну складову агресії рф проти України досліджували фахівці Національного інституту стратегічних досліджень України. Загальний огляд вимірів агресії рф здійснили фахівці Держспецзв'язку України [5]. Істотний внесок у дослідження кібервійни в умовах глобалізації та розвитку кіберпростору зробили зарубіжні вчені, серед яких можна виділити роботи Д. Белла, Р. Кларка [9], Е. Тоффлера [10], Б. Хофмана [11] та ін.

Проте серед науковців і практичних фахівців у сфері інформаційних технологій немає єдиних підходів до визначення поняття "кібервійна", її ознак та етапів. Існують також розбіжності поглядів щодо форм і різновидів такої війни. Відсутні системні підходи до інструментів та засобів, які використовуються під час кібервійни. Не достатньо дослідженим залишається питання створення та функціонування кібервійськ у ході такої війни.

Метою статті є з'ясування сутності кібервійни рф проти України, визначення її етапів та масштабу в контексті вироблення ефективних механізмів та шляхів протидії агресії рф в кіберпросторі.

Виклад основного матеріалу. Визначення агресії було сформульоване ще у 1974 році у Резолюції Генеральної Асамблеї Організації Об'єднаних Націй № 3314. Водночас, міжнародне право фактично ігнорує поняття агресії у кіберпросторі, яке часто називають кібервійною.

На жаль, серед науковців немає єдності поглядів щодо поняття "кібервійна". Не існує уніфікованого визначення цього поняття і в законодавстві України. Наслідком відсутності нормативно-правової бази є неможливість формування адекватних сил і засобів реагування на наявні ризики та загрози у сфері кібербезпеки [4, с. 122].

На це звертають увагу П. Горінов та Р. Драпушко, які констатують, що транскордонний характер кіберпростору, його залежність від складних інформаційних технологій, активне використання сайтів і сервісів кіберпростору всіма верствами населення виявляють нові можливості, але також викликають нові загрози, в тому числі: а) шкоду правам, інтересам і життю окремих осіб, організацій, державних установ; б) кібертероризм; в) використання кіберзброї на війні; г) кібервійни, в тому числі ті, які супроводжують традиційну ворожнечу [12].

О. Мережко визначає кібервійну як використання Інтернету й пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави [13].

Річард А. Кларк в своїй книзі "Кібервійна" (CyberWarfare) пише, що кібервійна – "дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування" [9]. Американський журнал "Економіст" (The Economist) описує кібервійну як "п'яту сферу війни, після землі, моря, повітря і космосу".

Окремі дослідники пропонують шлях дослідження кібервійни в контексті протистояння гібридній агресії роZZійського фашизму проти України в рамках:

- цивілізаційно-порівняльного, ідейно-політичного протистояння демократичних форм організації суспільства (в нашому випадку – української олігархічної республіки) проти тоталітарних форм організації суспільства (у формі роZZійської православно-кримінальної, фашистської недоімперії);
- формування глобального інформаційного суспільства, національних моделей інформаційного суспільства, особливостей становлення і функціонування глобального

інформаційного простору і національних моделей інформаційного простору та історичного часу [14].

За визнанням фахівців, лідерами у веденні кібервійни зараз є Китай та рф. Остання залишається одним з основних джерел загроз національній та міжнародній кібербезпеці України, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [15].

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. 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 [15].

Багатовимірність агресії рф проявила себе ще до повномасштабного вторгнення як елемент гібридної війни. Але саме з 24 лютого 2022 року кореляція між різними видами атак набула системного характеру [5]. Зауважимо, що з 24 лютого 2022 року хакерські атаки відбуваються не лише з боку спецслужб держави-агресора, який використовує віртуальний простір для завдання шкоди національній безпеці України. Непоодинокими є випадки вчинення кіберзлочинів з боку хакерів різного рівня кваліфікації, протидія яким ускладнюється на тлі реформування правоохоронних органів України.

Перший етап кібервійни розпочався з анексії Криму в 2014 році, коли інформаційно-обчислювальні системи України стали об'єктами атак з боку рф. 23 грудня 2015 року сталась перша у світі підтверджена хакерська атака, спрямована на виведення з ладу енергосистеми: зловмисникам рф вдалось успішно атакувати комп'ютерні системи управління в диспетчерській "Прикарпаттяобленерго", зокрема, було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Ця атака відбувалась із використанням троянської програми BlackEnergy [16].

27 червня 2017 року на підприємства різної форми власності була здійснена масштабна хакерська атака із використанням комп'ютерного хробака сімейства Petya. На думку Адміністрації Президента США, така хакерська атака на Україну з боку рф стала найбільшою відомою у світі [1].

В жовтні 2017 року сталася доволі масова атака вірусом-хробаком BadRabbit.

14 січня 2022 року за даними правоохоронних органів було атаковано близько 22 державні органи та 70 українських вебсайтів [1; 5].

15 лютого 2022 року хакери рф розпочали найпотужнішу в історії України DDoS-атаку, яка, серед іншого, була спрямована на фінансовий сектор (DDoS-атака на 15 банківських сайтів, сайтів з доменом gov.ua, також сайтів Міноборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин) [5; 17].

23 лютого 2022 року, за день до вторгнення рф в Україну, відбулися чергові атаки на державні та банківські сайти. Було пошкоджено сайти Верховної Ради, Кабінету Міністрів України та Міністерства закордонних справ, СБУ та інші. Міністерство освіти

і науки з метою запобігання кібератаці закрило доступ до свого вебсайту [18]. Посадовці Держдепартаменту США пов'язують цю атаку з рф. За даними компанії ESET, атака стала можливою через зараження сотень комп'ютерів вірусом HermeticWiper, який був скомпільований ще 28 грудня 2021 року [19].

З початком неприкритої агресії масштаб кібератак проти України збільшився в кілька разів.

2 січня 2023 року Державна служба спеціального зв'язку та захисту інформації України повідомила, що від початку вторгнення рф в Україну урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зареєструвала та дослідила понад 1500 атак. Більшість із них відбулася з боку рф [1; 5].

На нашу думку, умовно можна виділити такі етапи кібервійни рф проти України:

перший етап – з початку анексії Криму в 2014 році під час якої інформаційно-обчислювальні системи України стали об'єктами атак з боку рф;

другий етап – 23.12.2015 – 23.02.2022 рр. – період хакерських атак, інтенсивність і масштаб яких лише збільшувався з часом;

третій етап – 24.02.2022 р. – по теперішній час – триваючий період неприкритої агресії рф, важливим елементом якої стала повномасштабна кібервійна.

Основна мета хакерів рф із початком активної фази війни змінилась. Якщо напередодні вторгнення та в перший місяць війни кібератаки були скеровані на комунікації, які мали обмежити функціональність військових і влади в Україні, то після перших невдач на фронті російський агресор сконцентрувався на завданні максимальної шкоди цивільному населенню [5].

Інтенсивність кібервійни спонукала українську державу до рішучих кроків у напрямку реформування сектору безпеки і оборони у частині удосконалення механізмів протидії агресії рф у кіберпросторі.

5 жовтня 2017 року був прийнятий Закон України "Про основні засади забезпечення кібербезпеки України", положення якого містить визначення кібератаки як спрямованих (навмисних) дій в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (зокрема й інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів 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 режимів функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів і засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [20]. Вважаємо, що наведене визначення істотно покращує діяльність із запобігання кібератак з урахуванням розуміння її ознак та властивостей.

У цьому ж році було створено Національний координаційний центр кібербезпеки, положення про який затверджено Указом Президента України від 7.06.16 р. № 242. Серед основних завдань цього Центру виділяється: здійснення аналізу стану кібербезпеки, а також стану кіберзахисту критично важливих об'єктів інфраструктури; здійснення аналізу стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення превентивних заходів у боротьбі з кіберзлочинністю; упровадження вітчизняних програмних та програмно-апаратних засобів для здійснення уповноваженими суб'єктами заходів із кіберрозвідки,

кібероборони, контррозвідувального захисту кібербезпеки держави, розслідування кіберзлочинів.

У 2017 році СБУ отримала технічне обладнання і програмне забезпечення для роботи Центру в рамках виконання першого етапу Угоди про реалізацію трастового фонду Україна-НАТО з питань кібербезпеки [21].

26 січня 2018 року Служба безпеки України утворила Ситуаційний центр забезпечення кібербезпеки на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ.

29 грудня 2021 року Кабінетом Міністрів України затверджено "Положення про організаційно-технічну модель кіберзахисту" [22], приписи якого передбачають три рівні інтегрованих інфраструктур кіберзахисту:

організаційно-керівна (основні суб'єкти національної системи кібербезпеки);

технологічна (взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо);

базова (захищена інформаційна інфраструктура та суспільство (громада).

Потужним інструментом кіберзахисту вважаємо застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) в рамках яких забороняється Інтернет-провайдерам надавати послуги з доступу користувачам мережі Інтернет до низки російських інформаційних ресурсів та порталів. Вважаємо, що дія таких санкцій з часом має посилюватися.

Важливим кроком стало затвердження Указом Президента України від 26.08.21 р. № 447/2021 Стратегії кібербезпеки України, положення якої визначають загрози та виклики у сфері кібербезпеки, головною з яких є гібридна агресія рф проти України у кіберпросторі, засади розбудови, пріоритети та стратегічні цілі кібербезпеки. Серед основних загроз у цій сфері виділяється Розділ 4 "Національна система кібербезпеки: засади розбудови" Стратегії передбачає, що для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням;

утворення у системі Міністерства оборони України кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору [15].

План заходів у сфері реалізації положень Стратегії кібербезпеки України на 2023 – 2024 роки, затверджений розпорядженням Кабінету Міністрів України від 19 грудня 2023 року, передбачає створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору [23].

Рішенням РНБО України "Про невідкладні заходи з кібероборони держави" від 14.05.21 р. Кабінетові Міністрів України доручено у двомісячний строк розробити та внести на розгляд Верховної Ради України законопроект щодо створення та функціонування у системі Міністерства оборони України кібервійськ [24].

Постановою Кабінету Міністрів України "Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості" від 12.07.22 р. № 787 [25] утворено центральний орган виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Урядом України. Ще в травні 2014 року змінами до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" був закріплений офіційний статус команди реагування на кіберзагрози в Україні CERT-UA [1].

Висновки.

Агресія рф проти України має багатовимірною та масштабною. Віртуальний простір став сферою, де точиться запекла боротьба із супротивником. Сутність кібервійни пов'язана з використанням державою інформаційних та інших технологій з метою заподіяння шкоди економічному військовому, технологічному, економічному, політичному потенціалу іншої держави, населенню, окремим громадянам та довкіллю.

Кібервійну рф проти України умовно можна виділити на такі етапи: перший етап – з початку анексії Криму в 2014 році під час якої інформаційно-обчислювальні системи України стали об'єктами атак з боку рф; другий етап – 23.12.2015 – 23.02.2022 рр. – період хакерських атак проти України, інтенсивність і масштаб яких збільшувалася з часом; третій етап – 24.02.2022 р. – по теперішній час – триваючий період неприкритої агресії рф, важливим елементом якої стала кібервійна; з цього періоду кореляція між різними видами атак набула системного характеру, а потерпілими від них є не тільки держава, а й цивільне населення.

Необхідність захисту від агресії рф у кіберпросторі створює запит на:

законодавче визначення поняття "кібервійна";

здійснення системних заходів, спрямованих на посилення спроможностей суб'єктів сектору безпеки та оборони у боротьбі із кіберзагрозами воєнного характеру;

вироблення багатовимірної стратегії протидії кібератакам;

створення підрозділів кібервійськ у Збройних Силах України, їх належне організаційне та матеріально-технічне оснащення;

нарощування кібероборонних можливостей держави;

вироблення механізмів притягнення до юридичної відповідальності держави-агресора за кібератаки.

Реалізації цих пропозицій сприятиме прийняття Закону України про створення та функціонування у системі Міністерства оборони України кібервійськ.

Використана література

1. Російсько-українська кібервійна. URL: https://uk.wikipedia.org/wiki
2. 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
3. Російські хакери здійснюють кожного дня у середньому понад десять кібератак на Україну. URL: https://www.ukrinform.ua/rubric-ato/3676108-rosia-zdijsnue-na-ukrainu-ponad-10-kiberatak-za-dobu-sbu.html
4. Красніков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право*. № 3(46)/2023. С. 118-128.
5. Кібератаки, артилерія, пропаганда. загальний огляд вимірів російської агресії. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agres iyi
6. Брижко В. та ін. е-боротьба в інформаційних війнах та інформаційне право / за ред. М. Швеця. Київ: ТОВ "ПанТот", 2007. 218 с.
7. Почепцов Г.Г. Інформаційні війни. (Серія: Освітня бібліотека); москва: Рефл-бук, 2001. 576 с.
8. Мануілов Я.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. № 1(44)/2023. С. 154-167.
9. Clarke, Richard A. Cyber War, Harper Collins. 2010.
10. Тоффлер Є., Тоффлер Х. Війна та антивійна: Що таке війна і як з нею боротися. Як вижити на світанку XXI століття; москва: АСТ: Транзиткнига, 2005. 412 с.

11. Хоффман Б. Тероризм – погляд зсередини ; пер. з анг. Е. Сажина; москва: Ультра. Культура, 2003. 252 с.

12. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2023. № 1. С. 267-270.

13. Мережко А. Конвенція про заборону використання кибервойны в глобальній інформаційній мережі інформаційних і обчислювальних ресурсів (Інтернеті). URL: https://web.archive.org/web/20111007185753; URL:http://www.politik.org.ua/vid/publcontent.php3?y=7&p=5714

14. Бебик В., Куйбіда В., Мякушко Н. Сталий розвиток і соціальна глобалістика: навч. посіб. Київ: Талком. 2022. 256 с.

15. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

16. Кім Зеттер, Wired. Хакерська атака росії на українську енергосистему: як це було. URL: https://texty.org.ua/articles/66125/Hakerska_ataka_rosiji_na_ukrajinsku_jenergosystemu_jak-66125

17. 15 лютого 2022 року відбулася подібна DDoS-атака українських сайтів за якою, як вважають українські посадовці, стоїть росія. URL: https://ain.ua/2022/02/16/shho-vidomo-pro-ddos-ataku-15-lut

18. Сайти банків та органів влади зазнали масової DDoS-атаки. URL: https://www.ukrinform.ua. 25 лютого 2022. URL: https://www.ukrinform.ua/rubric-technology/3410542-sajti-bankiv-ta-oraniv-vladi-zaznali-masovoi-ddosataki.html

19. HermeticWiper: New data-wiping malware hits Ukraine. WeLive Security. 25 лютого 2022. URL: https://web.archive.org/web/20220225000916; URL: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine

20. 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

21. СБУ открыла в Киеве Ситуационный центр обеспечения кибербезопасности с системой реагирования на киберинциденты и лабораторией компьютерной криминалистики. URL: https://itc.ua/news/sbu-otkryila-v-kieve-situatsionnyiy-tsentr-obespecheniya-kiberbezopasnosti-s-sistemoy-reagirovaniya-na-kiberintsidentyi-i-laboratoriey-kompyuternoy-kriminalistiki

22. Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.21 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

23. Про затвердження плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 19.12.23 р. № 1163-р. URL: https://zakon. rada.gov.ua/laws/show/1163-2023-%D1%80#Text

24. Про невідкладні заходи з кібероборони держави: Рішення РНБО України від 14.05.21 р.: введене в дію Указом Президента України від 26.08.21 р. № 446/2021. URL: https://zakon.rada.gov.ua/laws/show/n0053525-21#Text3

25. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості: Постанова Кабінету Міністрів України від 12.07.22 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text

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