УДК 35.078.3 DOI: https://doi.org/10.33099/2304-2745/2023-3-79/31-38

Сніцаренко П. М., доктор технічних наук, старший науковий співробітник (0000-0002-6525-7064)
Саричев Ю. О., кандидат технічних наук, старший науковий співробітник (0000-0003-1380-4959)
Гордійчук В. В., кандидат технічних наук, старший дослідник (0000-0003-1380-4959)
Грицюк В. В., доктор філософії (0000-0003-3665-4201)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Кіберстійкість в умовах воєнної агресії РФ: досягнення України та проблемні питання

Резюме. У статті досліджується явище забезпечення кіберстійкості в Україні в умовах широкомасштабної воєнної агресії РФ. Проведено аналіз стану кіберборотьби напередодні та під час вторгнення РФ на територію України. Окреслено характерні закономірні особливості та проблемні питання в інтересах досягнення належної кіберстійкості в Україні в умовах зовнішньої воєнної агресії.

Ключові слова: кіберпростір; кібербезпека; кіберборотьба; кібератака, кібероборона; кіберстійкість.

Постановка проблеми. У сучасних воєнних конфліктах поряд з традиційними операційними середовищами (суша, море, повітря, космос), розглядають також інформаційне середовище, передусім його невід'ємну складову – кіберпростір, у якому динамічно відбуваються кібердії [1–3].

На сьогодні протиборство у кіберпросторі в умовах широкомасштабної збройної агресії РФ проти України набуло значного масштабу. Воно характеризується застосуванням широкого кола різних стратегій, тактик, технік, методів. Примітно, що агресія в кіберпросторі з боку Росії здійснюється як для виконання самостійних завдань, так і у взаємодії з іншими складовими ведення війни. Найбільше агресивних дій противник спрямовує на об'єкти, операційні середовища яких пов'язані з мережею Інтернет. В цьому протистоянні важливого значення набуває узагальнений розгляд питання кіберстійкості як засадничого елемента національної системи кібербезпеки України, а в умовах зовнішньої воєнної агресії також як чинника кібероборони держави.

Аналіз останніх публікацій. Сутність кіберстійкості для України визначено Стратегією кібербезпеки України [4] у 2021 році як *здатність швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед критичних об'єктів інформаційної інфраструктури.* Незважаючи на те, що питання кібербезпеки, зокрема протистояння в кіберпросторі, неодноразово висвітлювалися в наукових публікаціях [5–10], їх автори зосереджувалися переважно на концептуально-теоретичних підходах розгляду кіберборотьби або загалом кібервійни, а в інших випадках розглядали тактичні чи технічні аспекти кібервпливу на об'єкти інформаційної інфраструктури, не приділяючи при цьому уваги стратегічному питанню кіберстійкості держави.

За таких умов сутність кіберстійкості для сфер діяльності України в практичних деталях на сьогодні залишається нерозкритою, зокрема в умовах широкомасштабної воєнної агресії РФ, а тому це питання потребує наукового аналізу та узагальнення. Виходячи із цього, дослідження проблеми створення та сталого функціонування стійкого вітчизняного кіберпростору, є актуальним для розгляду та подальшого наукового опрацювання.

Отже, для розуміння загальної картини протистояння у вітчизняному кіберпросторі з позиції розгляду складової кіберстійкості держави необхідно проаналізувати процеси такого протистояння, що, в свою чергу, дозволить визначити його загальний характер, системні особливості та систематизувати отримані дані в інтересах удосконалення кібербезпеки України та складової її забезпечення – кібероборони держави.

Метою статті є розкриття закономірних особливостей забезпечення кіберстійкості в Україні в умовах широкомасштабної воєнної агресії РФ.

Виклад основного матеріалу. Росія почала широкомасштабне вторгнення в Україну 24 лютого 2022 року, але

цілеспрямовані російські кібератаки проти України тривають із моменту незаконної анексії Росією Криму у 2014 році, хоча окремі події в кіберпросторі України відбувалися і раніше. Як свідчить Дослідницька служба Європарламенту [11], вже 13 березня 2014 року, за три дні до псевдо референдуму щодо статусу Криму, Росія здійснила DDoS-атаку (атака "відмова в обслуговуванні"), спрямовану на дестабілізацію українських комп'ютерних мереж і комунікацій, щоб відвернути увагу громадськості від присутності російських військ у Криму. Упродовж наступного часу аж до широкомасштабного вторгнення в Україну кібератаки на об'єкти інформаційної інфраструктури України продовжувалися перманентно з тією чи іншою інтенсивністю. А найбільш резонансними і руйнівними за цей період були кібератаки на електромережі України у 2015–2016 роках (коли від DDoS-атаки постраждали кол-центри та мережа енергорозподільчих компаній і близько 20-ти електропідстанцій, а кількасот тисяч споживачів зазнали відключень електроенергії до шести годин), а також у 2017 році, коли здійснено запуск шкідливого програмного забезпечення (вірусу) NotPetya, що вразив численні установи України та ще 65 країн світу зі збитками на суму понад 10 млрд доларів США.

За даними компанії Microsoft [12] існує тісний зв'язок російських суб'єктів здійснення кібератресії з державними структурами РФ, які їх координують за напрямами діяльності у кіберпросторі. Зазначені підрозділи вели підготовку до широкомасштабного вторгнення як мінімум з березня 2021 року.

У 2021 році та на початку 2022 року, з нарощуванням російських військ вздовж українських кордонів, російські кіберпідрозділи почали деструктивні кібератаки на українські організації з дедалі більшою інтенсивністю, що додатково підтверджувало наявність фази ескалації та подальшого загострення дій РФ проти України. У цей період кібератак найбільше зазнали сайти Кабінету Міністрів України, деяких міністерств, зокрема і Міністерства оборони України, а також мережі понад сотні організацій енергетичного, фінансового, бізнесового, IT-, медіа-, авіаційного, інших державних та некомерційних секторів життєдіяльності України [13]. Ці кібероперації були спрямовані, переважно, на зниження спроможності українського уряду, порушення роботи критичних об'єктів інфраструктури держави та обмеження доступу української громадськості до інформації [14].

З початком широкомасштабного вторгнення 24 лютого 2022 року інтенсивність кібератак РФ проти України суттєво зросла, вони стали більш координованими та здійснювалися з метою досягнення цілей так званої "спеціальної військової операції" за двома напрямами:

підтримка та посилення воєнних дій із застосуванням кінетичної зброї;

нанесення найбільш можливих збитків кіберінфраструктурі України з негативними наслідками у різних сферах життєдіяльності держави.

До того ж, одночасність російських кінетичних ударів та кібератак свідчить про системність такої кореляції як один із проявів сучасної воєнної стратегії РФ та суттєвої ознаки гібридності її агресії проти України.

Згідно з даними Держспецзв'язку України [14] за 2022 рік Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зареєструвала 2 194 кіберінциденти. На рис. 1 відображено графік часового розподілу сукупності зафіксованих у 2022 році кіберінцидентів різного рівня загрози, представлений у звіті Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку України) [13]. Тут рівні загроз визначені згідно із загальноприйнятою системою ранжування вразливостей інформаційно-комунікаційних систем [15] відповідно до галузевого стандарту оцінки показника вразливості комп'ютерної системи (Common Vulnerability Scoring System – CVSS). Сутність такої системи ранжування полягає в кількісному оцінюванні ризику безпеці інформації (електронних інформаційних ресурсів) на шкалі 0,1 – 10,0 з відповідними діапазонами оцінок загроз (низька, середня, висока, критична) через негативний вплив на її базові характеристики (достовірність, достатність, доступність, цілісність, конфіденційність).

На графіку видно, що після травня 2022 року, з переломом Україною в кінетичних боях, інтенсивність кібератак знизилась, але систематика атак з прощупуванням усього спектру можливих вразливостей інформаційно-комунікаційних систем залишилась, причому динамічно прив'язаною до подій у політичній сфері та активності кінетичних бойових дій. Статистика свідчить, що головною метою російських атак на український кіберпростір є

блокування або знищення об'єктів інформаційної інфраструктури, шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій сил оборони), а також інформаційно-психологічні акції та операції (з метою підриву довіри до органів державної влади, поширення панічних настроїв серед населення тощо).

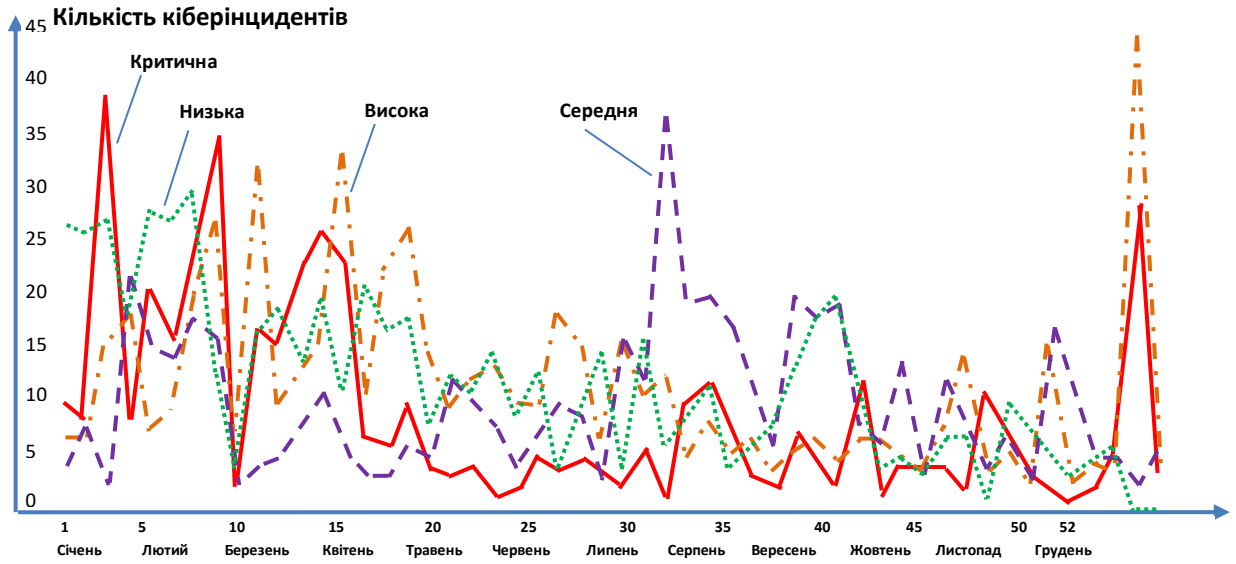

Рис. 1. Часовий розподіл сукупності зафіксованих кіберінцидентів різного рівня загрози в 2022 році

Зауважимо, що після того як "бліцкриг" захлинувся, відмічено спад кіберактивності противника. Це пояснюється тим, що відомі агресору вразливості кіберпростору України були вже використані, тому виникла потреба пошуку нових вразливостей, і, відповідно перерозподілу на це необхідного кіберпотенціалу.

Крім того, у кібероборонців України з'явилась можливість послідовного реагування на наступні кіберінциденти, а також до кіберборотьби підключились західні партнери та кіберволонтери. Це змусило агресора змінити парадигму стратегії ведення кібервійни та діяти відповідно до змін характеру збройного протистояння, гаряча фаза якого перейшла у більш прогнозований процес з ознаками тривалого воєнного конфлікту. Якщо на початку широкомасштабного вторгнення чітко прослідковувалося, що кібератаки здійснювались в підтримку кінетичних бойових дій (деструктивний вплив на програмне забезпечення та інформацію, активне супроводження пропагандистської кампанії противника, дезінформація та залякування населення – з метою викликання паніки, посадових осіб – з метою подавлення рішучості та волі до прийняття рішень), то в подальшому російські кібератаки спрямувались на добування інформації – кібершпигунство, а також пошук кібервразливостей України для їх подальшого використання. У цей період було здійснено численні кібератаки на системи бойового кіберпростору Збройних Сил України [16, 17], зокрема на системи тактичної ланки "Кропива" та ситуаційної обізнаності "Дельта", що пов'язані із Інтернет-сервісами, з метою їх злому та блокування. Але, завдяки застосованим захисним заходам, кібератаки не мали успіху.

Також зауважимо, що ефективність ворожих дій у кіберпросторі додатково підвищувалася шляхом фізичного руйнування елементів інформаційної інфраструктури України в ході бойових дій та після них, вже на окупованій території, чи переключенням комунікаційних мереж на операторів ворожої сторони. Такі дії слід вважати частиною загальної кіберкампанії противника щодо зменшення можливості використання національного кіберпростору України, нівелюючи цим управлінські функції держави в умовах агресії.

Загалом російські кібератаки на Україну через мережу Інтернет під час російсько-української війни направлені на спектр базових властивостей інформації (конфіденційність, цілісність, доступність), що підлягають захисту на усіх рівнях мережевої моделі OSI (Open Systems Interconnection) та електронних середовищах обміну і обробки інформації. До того ж, найбільш пріоритетними цілями таких кібератак були інформаційні об'єкти сектору безпеки і оборони, а основними завданнями:

кібершпигунство – порушення конфіденційності – добування інформації;

кібердиверсія – порушення цілісності та доступності інформації;

підтримка інших акцій – інформаційно-психологічний вплив для деморалізації населення України, дезінформаційні, пропагандистські, маніпулятивні дії, а також встановлення віддаленого доступу, викрадення коштів тощо [14].

Така стратегія ведення кібервійни РФ з Україною залишається незмінною і під час сучасного розвитку воєнних дій.

Між тим, уже на початок широкомасштабного російського вторгнення державні інституції України та їх відповідні структурні підрозділи вже мали певні механізми протидії кіберагресії. Як зазначає низка зарубіжних кіберфахівців, що також підтвердив заступник голови Держспецзв'язку України [18], кіберагресія РФ не досягла поставлених цілей. До основних чинників, що позитивно вплинули на кіберстійкість в Україні як критичну характеристику її кібербезпеки, у тому числі кібероборони держави, в умовах воєнної агресії, слід віднести такі об'єктивні явища:

1. Цифрова інфраструктура України в цілому була структурно стійкою. Децентралізована топологія комп'ютерних мереж критичних об'єктів інфраструктури держави, пов'язаних з Інтернет, дала змогу зберегти працездатність після порушення роботи окремих вузлів чи підмереж. Частина сервісів була розміщена в хмарних середовищах ще до початку широкомасштабної агресії.

Окремо зауважимо, що важливим позитивним фактором у кіберборотьбі з РФ виявилося те, що в секторі безпеки і оборони України процеси управління лише частково зав'язані на мережу Інтернет. Враховуючи той факт, що на озброєнні ЗС України перебуває значна частина радянських зразків озброєння та військової техніки, багато процесів управління військовими силами та засобами досі здійснюються автономно (автоматизовано в локальному кіберпросторі або вручну). Тому, навіть у разі потужнішого кібервпливу, ніж був, РФ не змогла б повністю подавити управління, координацію та бойове застосування українських сил оборони через неможливість вторгнення у їх автономні мережі шкідливих програмних продуктів.

2. Потужним чинником посилення кіберстійкості в Україні після 2014 року, зокрема, стало міжнародне співробітництво у сфері кібербезпеки [19, 20] та інтеграція в міжнародний безпековий кіберпростір. Дієвими напрямами такого співробітництва стали:

обмін актуальною інформацією;

обмін стандартними операційними процедурами, а також тактиками, техніками та методиками з країнами-партнерами;

участь у спільних проєктах і програмах (зведені кіберпідрозділи, кібернавчання, хакатони, конкурси тощо);

підготовка українських кіберфахівців силами партнерів та ін.

Найважливіші країни-партнери – США, Велика Британія, країни Балтії.

3. З початком широкомасштабної війни з переважаючим противником протистояти кіберагресії в України не було достатньо сил та засобів навіть з набутим досвідом. Але у цій критичній ситуації державні органи, у першу чергу, Міністерство цифрової трансформації України, швидко адаптувались до умов, що склались, та прийняли ряд нетривіальних рішень для мобілізації кіберресурсів, започаткували низку спільних з волонтерами та хактивістами ІТ-проєктів для протистояння агресії [21–23].

Показовим прикладом є створена наприкінці лютого 2022 року на заклик Уряду України з метою боротьби з кібервторгненням в український інформаційний простір волонтерська (хактивістська) кіберорганізація "ІТ-армія України" [21]. Ця організація має мету та завдання, але не має чіткої ієрархії, структури підпорядкування та визначеної чисельності, яка варіюється в межах сотень тисяч "кібербійців". Після початку російського вторгнення в Україну організація проводить, переважно, наступальні кібероперації на відкриті сайти держави-агресора та своєю діяльністю вже паралізувала тисячі російських онлайн-ресурсів, зокрема в держустановах, банківській, освітянській та медіа-сферах, наносячи цим фінансову, репутаційну та моральну шкоду росіянам.

Іншим прикладом оригінальних захисних дій України у кіберпросторі є створення в Інтернет-застосунків типу ботів "Народний месник" чи "е-ППО", або Телеграм-опції для тієї ж "Дельти" – в інтересах отримання додаткових розвідданих в реальному часі про дії противника як в межах підконтрольної території України, так, за можливості, і на її окупованій частині та далі.

4. Низка кіберактивістських груп самоорганізувались та об'єднались для

протидії кіберагресії РФ. Прикладом може бути спільнота українських кіберактивістів з різних міст України і куточків світу "Український кіберальянс" [22], яка утворена ще у 2016 році шляхом об'єднання кількох груп кіберактивістів для боротьби з російською агресією проти України у кіберпросторі.

5. Ефективною у кібероборотьбі з РФ стала допомога іноземних ІТ-організацій та активістів [24–26]. Міжнародні ІТ-партнери на волонтерських засадах активно підтримали Україну, зокрема такі світові лідери з розробки програмного забезпечення, надання сервісів та виготовлення обладнання як: GOOGLE, Eset, Veeam, Cisco, Hewlett Packard Enterprise, TeamViewer, IMPREVA, Maxon, GFI Software, Fudo Security, Canon, Smiddle, Intel, Amazon Web Services (AWS) та ін.

Діють різні програми допомоги, започатковані міжнародними партнерами, зокрема Агентством США з міжнародного розвитку в Україні (USAID) за напрямом "кібербезпека" [25], реалізуються проєкти "Кібербезпека критично важливої інфраструктури в Україні", "Відповідальне та підзвітне врядування в Україні", "Регіональна програма зі зміцнення кібербезпеки в енергетиці" тощо.

6. З початком широкомасштабної агресії РФ на бік України стали ряд іноземних хактивістських організацій, таких як "Anonymous", "AgainstTheWest", "DDoSecrets", "NB65", "KelvinSec" та ін. [26]. Зокрема, міжнародна мережа хактивістів "Anonymous" вже 26 лютого 2022 року провела понад 50 DDoS-атак ємністю понад 1 терабайт на інформаційні структури РФ. У подальшому під атаки "Anonymous" потрапляли різні урядові веб-сайти .РФ, включаючи апарат Президента, Державну думу та Міністерство оборони РФ, значні безпрецедентні перебої були зафіксовані на порталі державних послуг РФ, зламувались телеканали, супутникові приймачі системи супутникової навігації GNSS тощо.

7. Принциповим елементом забезпечення кіберстійкості в Україні в умовах агресії РФ стало надання, за сприяння Мінцифри України, можливості використання вже з кінця лютого 2022 року супутникової радіомережі зв'язку Starlink від компанії Ілона Маска, що стало реальною альтернативою наземним стільниковим мережам зв'язку та забезпечило безперебійне функціонування систем управління, в тому числі в автоматизованому режимі (тобто, через кіберпростір), у різних сферах життєдіяльності держави, зокрема у сфері оборони.

8. Також підкреслимо, що рівень кібербезпеки України було суттєво посилено шляхом надання партнерами актуальної інформації, зокрема в електронному виді та в реальному часі, від тих засобів розвідки, які поки-що недоступні для сил оборони України, що дозволило суттєво підвищити ситуаційну обізнаність (в тому числі в автоматизованому режимі, тобто в електронному середовищі, отже у власному кіберпросторі) і забезпечити своєчасне та адекватне реагування на загрози нападу з боку противника (наприклад, заходи ППО чи оповіщення населення).

Наведений перелік суттєвих чинників позитивного впливу на кіберстійкість в Україні на практиці свідчить про конституційне положення, що забезпечення кібербезпеки держави, зокрема її кібероборони, є справою усього Українського народу.

Однак слід зауважити, що навіть за такої інтеграції національних і міжнародних зусиль України противнику у низці випадків щастило проникати зі шкідливими намірами в її кіберпростір як шляхом кібератак безпосередньо в комп'ютеризованих мережах, так і шляхом їх зовнішнього радіопридушення або фізичного знищення.

Розглядаючи питання кіберстійкості в Україні, важливо також звернути увагу на низку системних особливостей, які проявилися з настанням активної фази російсько-української війни (після 24 лютого 2022 року) та є такими, що створюють проблеми забезпечення кібербезпеки держави, зокрема її кібероборони, які потребують розв'язання.

1. Основним феноменом міцної кіберстійкості в Україні в умовах воєнної агресії (зокрема, як критичної характеристики її кібероборони) слід вважати унікальне та швидке зосередження зусиль спротиву. Причому не стільки із-за чіткості державної організації цього процесу, як завдяки самоорганізації усієї кіберспільноти України (включно із державними установами) та міжнародній кіберсолідарності.

Між тим, такий унікальний синергетичний ефект засвідчив, що, незважаючи на попередні зусилля, кібероборона України у фазі відсічі потужної збройної агресії належним чином ще не була організована, а державний механізм реалізації моделі кібероборони України залишається

недосконалим, насамперед, на рівні відповідної нормативно-правової бази. Із-за цього страждає внутрішньодержавна інтеграція, коли співпраця між інституціями і відомствами України є, але єдиного бачення гармонійної моделі кібероборони з охопленням усіх суб'єктів, чітким розмежуванням їх функцій та завдань, запровадженням вертикалі керівництва і координації кіберсилами та повноважень відповідних органів управління, зокрема під час воєнного стану, ще немає.

2. Об'єкти інформаційної діяльності з реалізацією функцій в середовищі мережі Інтернет виявилися найбільш вразливими до кібератак. Як приклад підтвердження – ефективні кібердії міжнародної хакерської групи ANONYMOUS проти Інтернет-ресурсів РФ, зокрема її силових структур.

3. В умовах війни наземні стільникові мережі зв'язку, як основа мобільних комунікацій, можуть бути порушені у ході бойових дій. Так, зокрема, знищення противником стаціонарних антенних веж суттєво знизило можливості обміну інформацією в Інтернет-середовищі України.

4. В умовах війни альтернативою наземним стільниковим мережам зв'язку можуть бути супутникові (космічні) радіомережі зв'язку (типу Starlink від компанії SpaseX Ілона Маска). Водночас, така мережа, якщо вона приватна, може бути відключена на розсуд її власника. Крім цього, така система зв'язку чутлива до умисних радіозавад в місцях приймання радіосигналу як на Землі, так і на супутнику. Зазначені чинники не надають абсолютної гарантії Інтернет-обміну інформацією.

5. Інформаційні платформи, що діють на основі Інтернет, можуть бути локально відключені (блоковані) на вимогу політичних рішень. Підтвердження цього, зокрема, – технічне відключення для РФ ряду робочих Інтернет-платформ з ініціативи (за пропозицією) керівних державних органів України з причини воєнної агресії проти неї (сервіси SWIFT, PayPal, Visa, MasterCard), або в цих же умовах війни вимушене блокування Роскомнадзором частини власного (внутрішнього) Інтернет-простору в інтересах недопущення в межах території РФ зовнішньої соціально значимої інформації (онлайн-сервіси Facebook, YouTube, Instagram, Google News, Telegram). У сукупності це завдало втрат та клопоту як державі-агресору, так і безпосередньо її значних верств населення.

6. Відкриті Інтернет-сервіси, що діють на території держави, можуть бути цінним джерелом інформації для противника. Про це, зокрема, свідчать випадки розміщення в соціальних мережах матеріалів про результати бойових дій з відеофіксацією та коментарями громадян.

Наведені особливості, що мають негативну змістовність для забезпечення кібербезпеки держави, свідчать про те, що за існуючого стану належний рівень кіберстійкості в Україні, отже кібербезпеки держави та її кібероборони, в умовах воєнного протистояння із переважаючим противником не слід вважати гарантованим, особливо без підтримки міжнародного співтовариства.

Висновки

1. Розкрито низку закономірних особливостей забезпечення кіберстійкості в Україні в умовах широкомасштабної воєнної агресії РФ, серед яких, зокрема, таке:

з початком широкомасштабного вторгнення РФ в Україну інтенсивність ворожих кібератак, переважно через Інтернет, суттєво зросла, вони стали більш координованими та здійснювалися з метою досягнення цілей так званої "спеціальної військової операції". Системність кореляції російських кінетичних ударів та кібератак свідчить про характерну ознаку гібридності сучасної воєнної стратегії РФ;

незважаючи на потужну агресивність, кіберкампанія РФ не має значного успіху із-за активного кіберспротиву України. Злочинна кіберспільнота РФ наразі основну увагу приділяє виявленню вразливостей кіберпростору України;

в умовах інтенсивної кіберагресії РФ головним фактором відносно високої кіберстійкості в усіх галузях діяльності України став унікальний феномен самоорганізації як національного кіберкластеру України, так і солідарної міжнародної кіберспільноти. У сукупності з цільовою міжнародною допомогою, а також децентралізованим розосередженням значної частини електронних інформаційних ресурсів України, такий підхід зумовив позитивний синергетичний ефект кіберспротиву на рівні усієї держави;

участь багатьох національних складових кібербезпеки у здійсненні кіберспротиву агресії з боку РФ зокрема засвідчила, що кібероборона держави є справою усього Українського народу.

2. Окреслено окремі проблемні питання, що мають негативну змістовність для забезпечення кіберстійкості в Україні, які спричинені подіями російсько-української війни та потребують розв'язання. Найбільш важливими є такі:

унікальний ефект оперативної самоорганізації кіберспільноти засвідчив, що, незважаючи на попередні зусилля, кібероборона України у фазі відсічі потужної збройної агресії належним чином ще не була організована, а державний механізм реалізації моделі кібероборони України залишається недосконалим. Такий стан потребує зусиль щодо подальшого розвитку відповідної системи, включно із чіткою організацією міжнародної взаємодії;

об'єкти інформаційної діяльності з реалізацією функцій в середовищі мережі Інтернет в умовах інтенсивного протиборства виявилися найбільш вразливими до кібератак. Це означає, що, поряд із необхідністю удосконалення захисних властивостей Інтернет-платформ, існує потреба розвивати альтернативні інформаційні мережі, відокремлені від Інтернету, а кіберпростір розглядати як сукупність таких мереж.

Перспектива подальших досліджень полягає у пошуку шляхів підвищення рівня кіберстійкості в Україні на підставі глибокого аналізу організації національної системи кібербезпеки України, зокрема моделі кібероборони держави, урахування досвіду кіберборотьби в умовах воєнного конфлікту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с.
2. Основи стратегії національної безпеки та оборони держави : підручник 2-ге вид., доп. і випр. / О. П. Дузь-Крятченко, Т. М. Дзюба, А. О. Рось та ін. Київ : НУОУ, 2010. 591 с.
3. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021 // Президент України. Офіційне інтернет-представництво. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 14.04.2023).
5. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.
6. Баранов О. Про тлумачення та визначення поняття "кібербезпека" // Інформація і право. 2014. № 2 (42). С. 54–62.
7. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа ; за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
8. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Вид. дім "Києво-Могилянська академія", 2015. 497 с.
9. Забезпечення інформаційної безпеки держави : підручник / В. М. Петрик , М. М. Присяжнюк , Д. С. Мельник та ін. ; за заг. ред. О. А. Семченка та В. М. Петрика. Київ : НДУ Книжкова палата України, 2015. 672 с.
10. Основи забезпечення інформаційної безпеки держави у воєнній сфері : навч. посіб. / за ред. С. А. Микуся. Київ : НУОУ, 2022. 399 с.
11. Пшетачник Я., Тарпова С. (Дослідницька служба Європейського парламенту). Війна Росії проти України: хронологія кібератак // European Parliament. URL: https:// www.europarl.europa.eu/ RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf (дата звернення: 18.09.2023).
12. An overview of Russia's cyberattack activity in Ukraine. Special Report Ukraine: Microsoft Publishing, 2022. 20 p. URL: https:// query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vww (дата звернення: 18.09.2023).
13. Russia's Cyber Tactics: Lessons Learned 2022 – аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни Росії проти України // Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against - ukraine (дата звернення:18.09.2023).
14. Готовність України до нових викликів. Кібербезпека і зв'язок // Державна служба спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbezpeka-i-zv-yazok (дата звернення: 29.09.2023).
15. Severity Levels for Security Issues. web-site. URL: https://www. atlassian.com/trust/ security/ security-severity-levels (дата звернення: 05.10.2023).
16. #Xaknet – #Kremlin Proxy Given Specific Instructions to Hack #Kropyva & #DDoS Telegram // Cybershafarat. URL: https://cybershafarat.com/ 2022/10/31/xaknet-kremlin-proxy-given-specific-instructions-to-hack-kropyva-ddos-telegram/ (дата звернення: 31.10.2023).
17. Ворожа пропаганда атакує ІТ-систему ситуаційної обізнаності ЗСУ. Міністерство оборони України: офіційна сторінка Facebook. веб-сайт. URL: https://www.facebook. com/ MinistryofDefence.UA/posts/pfbid02fjiCupvsbT1N3Vvwu8ZwwPupCEv57WPK v8fVpt9P9qtoVsC7L442 PTvCpejaLnrYl (дата звернення: 25.09.2023).

18. У межах місяця кібербезпеки в ЄС Держспецзв'язку поділиться досвідом кіберстійкості з європейськими партнерами // Державна служба спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/events/u-mezhakh-misyacya-kiberbezpeki-v-yes-derzhspeczv-yazku-podilitsya-ukrayinskim-dosvidom-kiberstiikosti-z-yevropeiskimi-partnerami (дата звернення: 05.10.2023).
19. Nick Beecroft. Evaluating the International Support to Ukrainian Cyber Defense. Carnegie Endowment. 2022. URL: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (дата звернення: 16.10.2023).
20. The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/ (дата звернення: 16.10.2023).
21. It Army Of Ukraine: website. URL: https://itarmy.com.ua/ (дата звернення: 16.10.2023).
22. Український кіберальянс: сторінка Facebook. URL: https://www.facebook.com/UkrainianCyberAlliance (дата звернення: 12.10.2023).
23. Глобальний центр взаємодії в кіберпросторі (GC3). URL: https://gc3.digital/ (дата звернення: 16.10.2023).
24. Як IT-партнери підтримують Україну (добірка, що оновлюється). URL: https://wiseit.com.ua/it-partnery-pidtrymuyut-ukrayinu/ (дата звернення: 16.10.2023).
25. Кібербезпека. USAID. URL: https://www.usaid.gov/uk/ ukraine/fact-sheets/aug-05-2022-cybersecurity (дата звернення: 16.10.2023).
26. #Russian state TV channels have been hacked by #Anonymous to broadcast the truth about what happens in #Ukraine. Anonymous TV. URL: https://twitter.com/YourAnonTV (дата звернення: 16.10.2023).

Стаття надійшла до редакційної колегії 11.11.2023

Cyber resilience in the conditions of military aggression of the Russian Federation: Ukraine's achievements and problematic issues

Annotation

In modern military conflicts, along with the traditional operational environments (land, sea, air, space), the information environment is also considered, especially its integral component - cyberspace, where cyber actions are dynamically taking place. In this confrontation, a generalised consideration of the issue of cyber resilience as a fundamental element of Ukraine's national cybersecurity system, and in the context of external military aggression, also as a factor in the cyber defence of the state, is of great importance.

The purpose of the article is to reveal the natural features of ensuring cyber resilience in Ukraine in the context of Russia's large-scale military aggression.

The main factors that have had a positive impact on cyber resilience in Ukraine in the context of military aggression include the following objective phenomena:

Ukraine's digital infrastructure was generally structurally stable;

international cooperation in the field of cybersecurity and integration into the international security cyberspace became a powerful factor in strengthening cyber resilience;

government agencies, first and foremost, quickly adapted to the current conditions and made a number of non-trivial decisions;

a number of cyber-activist groups have self-organised and united to counter Russian cyber aggression;

international IT partners actively supported Ukraine on a volunteer basis;

a number of foreign hacktivist organisations sided with Ukraine;

the possibility of using Elon Musk's Starlink satellite radio network from the end of February 2022;

partners' provision of up-to-date information from intelligence agencies, which significantly increased situational awareness.

Prospect for further research is to find ways to increase the level of cyber resilience in Ukraine based on an analysis of the organization of the national cyber security system.

Keywords: cyberspace; cyber security; cyber warfare; cyber-attack, cyber defence; cyber resilience.