УДК 32.019.51:323.28:323.2(477)

ГОРУН О.Ю., головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0002-0447-1729

КІБЕРЗАГРОЗИ УКРАЇНИ В УМОВАХ АГРЕСІЇ РФ

DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340520

Анотація. *У статті розглянуто нові кіберзагрози в умовах повномасштабної збройної агресії Російської Федерації проти України. Відзначається зміна стратегії кібератак протягом останніх років. Охарактеризовано сучасні вектори кібератак, засоби інформаційно-психологічного впливу та технічного втручання в ІТ-системи. Класифіковано види кібератак та їх найбільш небезпечні наслідки. Визначено можливий перелік об'єктів кіберпосягань. Розглядаються проблеми протидії кібератакам в кіберпросторі України в умовах війни. Зроблено висновок, що формування нової якості національної системи кібербезпеки зумовлює потребу залучення до діяльності суб'єктів забезпечення кібербезпеки громадських організацій, волонтерських об'єднань, незалежних аналітичних груп, які активно беруть участь у виявленні та нейтралізації кіберзагроз. Звертається увага на необхідність підготовки нової Стратегії кібербезпеки України. Визначено шляхи удосконалення протидії кібератакам та підвищення кіберстійкості в умовах війни.*

Ключові слова: *кіберзагрози, кібератаки, кібербезпека, інформаційна безпека, суб'єкти забезпечення кібербезпеки, кіберпростір, інформаційні операції, міжнародна співпраця.*

Summary*. The article examines new cyber threats in the context of full-scale armed aggression of the Russian Federation against Ukraine. The change in the strategy of cyber attacks in recent years is noted. Modern vectors of cyber attacks, means of informational and psychological influence and technical intervention in IT systems are characterized. Types of cyberattacks and their most dangerous consequences are classified. A possible list of objects of cyberattacks is determined. Problems of countering cyberattacks in the cyberspace of Ukraine in conditions of war are considered. It was concluded that the formation of a new quality of the national cybersecurity system necessitates the involvement of public organizations, volunteer associations, and independent analytical groups in the activities of cybersecurity entities that actively participate in the identification and neutralization of cyber threats. Attention is drawn to the need to prepare a new Cybersecurity Strategy of Ukraine. Ways to improve counteraction to cyberattacks and increase cyber resilience in wartime are identified.*

Keywords: *cyber threats, cyberattacks, cybersecurity, information security, cybersecurity entities, cyberspace, information operations, international cooperation.*

Постановка проблеми.

Стратегія кібербезпеки України проголошує, що забезпечення кібербезпеки є одним із пріоритетів у системі національної і державної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [1].

З початку повномасштабного вторгнення рф в Україну у 2022 році наша держава стала об'єктом чисельних кібератак, спрямованих проти державних органів, установ, приватних організацій та окремих громадян, а кіберпростір остаточно трансформувався

у повноцінний театр воєнних дій. Це спричинило виникнення нових та посилення існуючих кіберзагроз у кіберпросторі.

На тлі традиційних збройних загроз спостерігається стрімке зростання інтенсивності та технологічної складності кібератак та інших кібероперацій, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. У 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2541 кіберінцидентів. Таким чином, у минулому році кількість кібератак на Україну зросла на 70% [2]. Наша держава стала полігоном для реалізації масштабних кібероперацій, що вимагає дослідження як нових векторів кіберзагроз, так і адекватної реакції з боку держави, з урахуванням міжнародного та європейського досвіду та вітчизняних наукових напрацювань.

Результати аналізу наукових публікацій. Різні аспекти забезпечення кібербезпеки України в умовах воєнного стану досліджували у своїх працях такі вчені, як: І. Діордіца [3], Д. Журбинський [4], Є. Колосовський [5], В. Костенко [4], С. Красніков [6], В. Ліпкан [3], О.Романова [7] та ін.

Водночас, з огляду на появу нових інструментів і механізмів кібератак недостатньо дослідженими залишаються природа кіберзагроз, їх види, а також сучасні заходи протидії цим загрозам. Це зумовлює актуальність цієї статті.

Метою статті є визначення природи та видів кіберзагроз України в умовах агресії рф для удосконалення заходів протидії таким загрозам.

Виклад основного матеріалу.

Поновмасштабна агресія рф проти України засвідчила перехід сучасних традиційних війн до нової площини, де кіберпростір став одним із головних театрів воєнних дій. Україна в умовах війни зіштовхується з новими типами кібератак, які охоплюють як деструктивні чинники втручання, так і операції інформаційно-психологічного впливу, спрямовані на дискредитацію державної влади.

З 2014 року Україна перебуває під постійним тиском з боку агресора не лише у військовій площині, але й у кіберпросторі. Повномасштабне вторгнення РФ у 2022 році позначилося безпрецедентним зростанням інтенсивності та складності кібератак, спрямованих на державні інституції, об’єкти критичної інфраструктури, ЗМІ та приватний сектор [4, с. 76; 8]. Найчастіше об’єктами кібератак стають: місцеві органи влади, урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації[1]. Серед суб’єктів таких атак слід виділити, в першу чергу, державні органи держави-агресора, російські хакерські угрупування, автоматизовані системи розвідки.

На початку повномасштабного вторгнення у 2022 році російські хакери зосереджувалися на деструктивних операціях, намагаючись паралізувати критичну інфраструктуру України, викрасти дані та посіяти паніку серед населення. Тоді основними цілями були енергетичний та телекомунікаційний сектори, а також державні установи. серед перших прикладів кібервійни були: атака на системи зв’язку газети “Kyiv Post” та супутникову мережу “KA-SAT” за годину до вторгнення (24 лютого), атака IssacWiper на урядові веб-сайти (25 лютого), кібератака на пункт прикордонного контролю з метою перешкоджання виїзду біженців до Румунії (25 лютого) та атаки на цифрову інфраструктуру України, що призвело до блокування доступу до фінансових послуг та енергетичних ресурсів (28 лютого) [9].

У 2023 році стратегія ворога змінилася. Замість широких, деструктивних атак російські хакери почали зосереджуватися на прихованому зборі розвідувальних даних та закріпленні присутності в ключових системах. Зросла кількість складних атак, а також

з’явилися нові, раніше невідомі хакерські угруповання. Особлива увага приділялася атакам на месенджери, популярні серед військових, з метою збору критичних даних. Також збільшилася кількість фінансово мотивованих кібератак [9].

У 2024 році цей тренд продовжився. Фокус змістився на об’єкти, безпосередньо пов’язані з військовими операціями та постачальниками послуг, які підтримують військові зусилля. Кількість критичних інцидентів зменшилася, натомість значно зросли кібератаки на державні організації та органи місцевого самоврядування (до 60% всіх інцидентів), що може бути пов’язано зі спробами початкового доступу [9].

Під час війни найціннішою для ворога є інформація про плани сил оборони України, дані підприємств оборонно-промислового комплексу, Уряду України та інших організацій, які здійснюють підтримку військових. Для досягнення цих цілей зловмисники зазвичай використовують масові розсилки шкідливого програмного забезпечення та фішингових листів. Такі типи кібератак залишаться наймасовішими” [1].

Сучасні кіберзагрози, з якими стикається Україна, умовно можна розділити на чотири основні категорії:

1. Деструктивні атаки, зміст яких передбачає використання програм-руйнівників (wiper), як-от HermeticWiper, WhisperGate, котрі були зафіксовані в перші дні повномасштабного вторгнення. Метою цих атак є виведення з ладу систем управління, баз даних та пошкодження об’єктів критичної інфраструктури.

2. Фішингові атаки, значна частина яких реалізується через соціальну інженерію — від імені державних органів розповсюджуються фішингові листи, підроблені застосунки (наприклад, фейкові “Дія”) з метою збору персональних даних або проникнення в інформаційні системи. Останнім часом фішингові атаки стали ще більш витонченими, а для приховування свого місцезнаходження хакери використовують складні ланцюжки SSH-тунелів через TOR[9].

3. Кібершпигунство (тривале проникнення у комп’ютерні мережі з метою збору розвідданих, ураження комунікаційних систем або підготовки до фізичних атак) під час якого, зокрема, використовуються RAT-інструменти, модулі screen-capture, кейлогери.

4. Інформаційно-психологічні операції: дезінформація, поширення фейкових повідомлень, deepfake-відео, маніпуляція громадською думкою через Telegram-канали, Інтернет та соціальні мережі. Ці операції спрямовані, у першу чергу, на посилення напруги у суспільстві, дискредитацію державної влади України. Кіберзлочинці використовують новітні методи для поширення дезінформації і створення хаосу.

Вищезазначені кіберзагрози мають різні наслідки – від пошкодження об’єктів критичної інфраструктури до крадіжки даних та поширення дезінформації, у тому числі за допомогою технології “діпфейк”. До інших видів зловмисної кібердіяльності належать: розподілені атаки “відмова в обслуговуванні”, використання шкідливого програмного забезпечення для знищення даних тощо

Найбільшу небезпеку становлять цілеспрямовані атаки на енергетичні об’єкти, водопостачання, системи зв’язку та логістики України. Кібератаки Російської Федерації 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].

Отже, основною кіберзагрозою залишається агресія росії проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального

призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки [2].

Новою кіберзагрозою стало використання штучного інтелекту (далі AI) та автоматизації у кібератаках. Сьогодні зростає кількість автоматичних атак, що застосовують AI для пошуку вразливостей, створення фішингових листів та глибоких фейків для дезінформації. Це ускладнює захист систем і вимагає вдосконалення механізмів реагування на такі атаки.

Протидія кібератакам в кіберпросторі України в умовах війни продемонструвала низку проблем, розв'язання яких передбачає:

опрацювання питання адаптивного управління ризиками, що передбачає прогнозування сценаріїв та можливих варіантів кібератаки;

вироблення єдиного підходу до формування протоколу реагування на кібератаки з подальшим нормативним закріпленням обов'язкових компонентів протоколів з кібербезпеки для об'єктів критичної інфраструктури, у т.ч. з урахуванням можливих сценаріїв повної втрати контролю (blackout model);

розвиток державної системи кіберосвіти, яка передбачає обов'язкове вивчення кібергігієни для державних службовців, службовців сектору безпеки та оборони, розширення магістерських програм у сфері забезпечення кібербезпеки. У подальшому роль освітнього компонента буде тільки зростати;

підвищення кваліфікації суб'єктів забезпечення кібербезпеки, зокрема створення програм підготовки офіцерів кібероборони;

криміналізацію кібератак на об'єкти критичної інфраструктури шляхом внесення змін до КК України та доповнення Закону України "Про основні засади забезпечення кібербезпеки України";

визначення шляхів вирішення обмеженого ресурсного забезпечення суб'єктів забезпечення кібербезпеки, оскільки сьогодні частина суб'єктів забезпечення кібербезпеки недостатньо оснащені сучасними засобами захисту або не мають чітких протоколів реагування, що в умовах війни ускладнює швидке реагування і недопущення поширення кібератак;

розв'язання проблеми міжвідомчої координації суб'єктів забезпечення кібербезпеки України;

створення вітчизняних кібервійськ для захисту як критичної інформаційної інфраструктури від кібератак, так і для реалізації превентивних наступальних кібероперацій (до прикладу, DDoS-атаки на корпоративні, новинні та державні сайти противника, виведення з ладу критично важливих об'єктів інфраструктури росії, компрометація баз даних телекомунікаційних, роздрібних та урядових організацій тощо);

створення окремого державного органу — Агентства кіберстійкості, яке координуватиме впровадження міжнародних стандартів інформаційної безпеки, моніторинг кіберінцидентів та сертифікацію критичних IT-рішень;

залучення наукової спільноти та громадських організацій до розробки нормативно-правових актів з питань забезпечення кібербезпеки;

посилення міжнародної співпраці з НАТО та ЄС з питань кібербезпеки, у т.ч. з Агентством ЄС з питань кібербезпеки (ENISA);

удосконалення взаємодії суб'єктів забезпечення кібербезпеки з правоохоронними органами іноземних держав, особливо з Агентством з кібербезпеки та безпеки інфраструктури США (CISA).

В умовах повномасштабної війни Україна намагається посилити свою кібероборону шляхом зовнішньої допомоги. Уряд України залучив волонтерів з усього світу для того, щоб формувати ІТ-армію. У відповідь на російські атаки ІТ-команда, створена Мінцифри України, здійснила кілька DDoS-атак та атак wiper [7, с. 58; 9]. Перші порушують роботу серверів, штучно створюючи великий обсяг трафіку, а інші – призводять до видалення даних. Серед цілей атак – уряд росії, медіа-системи, фінансові установи, оборонні об'єкти, електромережі. У рамках протидії кібератакам незалежні хакери з усього світу викрали та оприлюднили російські урядові та фінансові дані, зокрема, електронні листи, інформацію про банківську діяльність, виробництво енергії та пропагандистські кампанії, а також дані про військовослужбовців та агентів ФСБ[9].

Така волонтерська активність позитивно впливає на забезпечення кібербезпеки України та допомагає діяльності законодавчо визначених суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Відповідно до ст. 5 Закону України "Про основні засади забезпечення кібербезпеки України" до кола таких суб'єктів віднесено: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури [10].

Безпосередня протидія кіберзагрозам здійснюється в Україні на рівні Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, CERT-UA, Міністерства оборони України, а також залучених партнерських структур НАТО та ЄС.

Формування нової якості національної системи кібербезпеки зумовлює потребу залучення до діяльності суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, громадських організацій, волонтерських об'єднань, незалежних аналітичних груп, які активно беруть участь у виявленні та нейтралізації кіберзагроз.

Формування такої системи потребує чіткого та зрозумілого визначення актуальних поточних завдань із забезпечення кібербезпеки України.

Серед таких завдань доцільно виділити:

створення кіберрезерву та відпрацювання механізму його мобілізації;

щоденний моніторинг кіберзахисту об'єктів критичної інфраструктури (зокрема енергетики);

координація діяльності суб'єктів забезпечення кібербезпеки з міжнародними групами (CSIRT, ENISA);

формування нової Стратегії кібербезпеки України, оскільки чинна Стратегія кібербезпеки України була затверджена Указом Президента України від 26 серпня 2021 року і розрахована на період до 2025 року.

Нова Стратегія кібербезпеки України має враховати нові кіберзагрози в умовах повномасштабної війни, а її зміст потребує максимальної конкретизації.

7 березня 2025 року Кабінет Міністрів України затвердив план заходів на 2025 рік з реалізації Стратегії кібербезпеки [11]. Цей План визначає низку завдань, які мають бути виконані протягом цього року для посилення кіберстійкості. Зокрема, це заходи за такими напрямами: нормативно-правове забезпечення діяльності у сфері кібербезпеки; розвиток організаційно-технологічної складової національної системи кібербезпеки;

налагодження більш тісного співробітництва з міжнародними партнерами України; впровадження ризик-орієнтованого підходу в частині заходів із забезпечення кібербезпеки об’єктів критичної інфраструктури та державних органів; подальший розвиток системи підготовки кадрів у сфері кібербезпеки[12].

Водночас, низка заходів цього Плану залишається не достатньо реалізованими або частково виконаними. Серед таких заходів виділяються заходи щодо: створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору (п. 1 Плану); запровадження ефективних механізмів взаємодії основних суб’єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (п. 2 Плану); удосконалення системи розвідувального забезпечення кібербезпеки держави в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці в кіберпросторі (п. 10); розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі (п. 14 Плану); впровадження ризик-орієнтованого підходу в частині заходів із забезпечення кібербезпеки об’єктів критичної інфраструктури та державних органів (п. 16 Плану); забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти (п. 19); розроблення національних стандартів у сфері кібербезпеки, організаційних і технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, із урахуванням європейських і міжнародних стандартів (п. 24) [11]. Очевидно, що частина цих заходів, які залишилися не реалізованими, мають бути визначені у новій Стратегії кібербезпеки України.

Формування нової якості національної системи кібербезпеки щодо обміну інформацією про інциденти кібербезпеки, кібератаки та кіберзагрози, удосконалення координації суб’єктів національної системи під час реагування на кібератаки передбачено у проєкті 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 29.09.2022) [13]. Метою цього акта є створення належної правової основи для здійснення заходів з попередження, виявлення і припинення актів агресії у кіберпросторі в умовах війни російської федерації проти України, а також на загальне удосконалення нормативно-правової бази у сфері кібербезпеки та захисту інформації задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам. Вважаємо, що прийняття цього Закону матиме позитивний вплив на стан захищеності від кібератак державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури.

Висновки.

Український досвід протидії кіберзагрозам у період повномасштабної війни свідчить про те, що кібербезпека є невід’ємною складовою національної і державної безпеки, а кіберпростір є повноцінним театром воєнних дій. Кіберзахист об’єктів критичної інформаційної інфраструктури залишається пріоритетним напрямком державної політики в сфері забезпечення кібербезпеки.

Удосконалення стратегічного планування, розвиток інституційної кіберспроможності, створення кіберрезерву, залучення громадськості до забезпечення кібербезпеки є запорукою ефективної протидії кіберзлочинності в умовах війни.

Для України кіберзагрози в умовах війни відзначаються підвищеною суспільною небезпечністю. В цих умовах найбільш поширеними серед сучасних кіберзагроз є:

1) деструктивні атаки, спрямовані на виведення з ладу інформаційних систем управління, баз даних та об'єктів критичної інфраструктури; 2) фішингові атаки; 3) кібершпигунство з метою збору розвідданих, ураження комунікаційних систем або підготовки до фізичних атак; 4) інформаційно-психологічні операції.

З метою удосконалення механізму протидії кіберзагрозам в умовах воєнного стану вбачається за доцільне:

посилення технічної та інформаційної безпеки державних органів;

впровадження сучасних технологій моніторингу та автоматичної реакції на кіберінциденти;

проведення навчань та тренінгів з підвищення кваліфікації співробітників суб'єктів забезпечення кібербезпеки;

інтеграція сил і ресурсів суб'єктів забезпечення кібербезпеки для швидкого реагування на кібератаки;

активізація міжнародної співпраці у сфері кібербезпеки, налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі із міжнародними партнерами, насамперед державами-членами НАТО;

залучення до діяльності із забезпечення кібербезпеки громадських організацій, волонтерських об'єднань, незалежних аналітичних груп, які активно беруть участь у виявленні та нейтралізації кіберзагроз;

розробка національної стратегії боротьби з дезінформацією та фейками у кіберпросторі;

підготовка нової редакції Стратегії кібербезпеки України.

Використана література

1. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 року № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. У 2024 році кількість кібератак на Україну зросла на 70%. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931.

3. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і* право. 2017. № 5. С. 174-180.

4. Журбинський Д. А., Костенко В.О. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті європейської інтеграції. *Публічне управління та адміністрування в Україні.* 2023. Випуск 34. С. 74-77.

5. Колосовський Є.Ю., Круць Е.М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. №12. С. 403-405. URL:http://lsej.org.ua/12_2023/100.pdf

6. Красніков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право.* 2023. № 3(46) (2023). С.118-128. http://il.ippi.org.ua/issue/view/17050

7. Романова О.М. Кібербезпека під час повномасштабного вторгнення РФ. *Часопис Київського університету права.* 2024. №2. С.56-59. URL:https://chasprava.com.ua/index.php/journal/article/view/1075/997.

8. Війна Росії проти України: хронологія кібератак URL:https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

9. Російські хакери змінюють тактику: від деструктивних атак до розвідки. Звіт Держспецзв'язку. URL:https://cip.gov.ua/ua/news/rosiiski-khakeri-zminyuyut-taktiku-vid-destruktivnikh-atak-do-rozvidki-zvit-derzhspeczv-yazku.

10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

11. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: розпорядження Кабінету Міністрів України від 07 березня 2025 р. № 204-р. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-2025-rik-z-realizatsii-stratehii-kiberbezpeky-t70325

12. Працюємо над посиленням кіберстійкості держави та захистом від кіберзагроз: затверджено план заходів на 2025 рік з реалізації Стратегії кібербезпеки. URL: https://cip.gov.ua/ua/news/pracyuyemo-nad-posilennyam-kiberstiikosti-derzhavi-ta-zakhistom-vid-kiberzagroz-zatverdzheno-plan-zakhodiv-na-2025-rik-z-realizaciyi-strategiyi-kiberbezpeki

13. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проєкт Закону України (реєстр. № 8087 від 29.09.2022). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881.

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