КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ВІЙНИ

Петро Петрович ГАЛУШКО,

аспірант Харківського національного університету внутрішніх справ

Повномасштабна збройна агресія російської федерації проти України поставила на порядок денний гостру проблему формування багатошарової системи захисту національної безпеки від неординарного комплексу комбінованих загроз, що поєднують у собі як фактори, дії фізичного плану, бойового характеру, так і інтелектоємні практики, спрямовані на порушення стійкості інформаційних систем, використання кіберпростору для підриву політичної стабільності в країні, послаблення руху опору, зриву програм по зміцненню обороноздатності країни. Відтак ординарний кримінологічний феномен кіберзлочинності постає у сегменті політичної злочинності, як елемент метакомплексу злочину агресії проти України.

В цьому сенсі не зайвим буде наголосити на тому, що Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. 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 [1].

Російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, 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 [1].

Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед російської федерації, міжнародних хакерських угруповань для реалізації кібервпливу [1].

Звертає на себе увагу той факт, що команда реагування на надзвичайні ситуації пов'язані з комп'ютерами в Україні (CERT-UA) зафіксувала майже 4 000 кіберінцидентів у період з січня 2022 року по вересень 2023 року. Це втричі більше, ніж у довоєнний період. Держспецзв'язку повідомляло, що тільки впродовж січня-червня 2023 року кількість кібератак проти України зросла до 762. Це більш ніж удвічі більше за показники другої половини 2022 року. Водночас кількість критичних кібернападів за цей період, зменшилася на 81% — до 27, що свідчить про покращення захисту. Росія координувала кібератаки, спрямовані проти України, проникнення в мережу та шпигунство в країнах, які сприймаються як союзники України, а також операції кібервпливу на людей у всьому світі [2].

При цьому кіберактивність у контексті російсько-української війни не обмежується урядовими акторами. Фіксуються недержавні кіберактори, що націлюються на широкий спектр організацій, у тому числі в секторі фінансових послуг, за допомогою відносно нескладних інцидентів, відомих як розподілені атаки на відмову в обслуговуванні (DDOS). Наприклад, у червні 2023 року проросійська хакерська група NoName057 погрожувала атакувати фінансовий сектор України. Протягом наступних чотирьох днів численні українські банки зазнали DDoS-атак [2].

Окремо слід наголосити на тому, що у кіберпросторі росія використовує таку саму тактику, як і на полі бою – вона

намагається атакувати цивільну інфраструктуру України. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка займається в ручному режимі запобіганням, виявленням і реагуванням на кібератаки, кіберінциденти, відслідковує діяльність понад 80 груп, більшість із яких – це хакерські угруповання з РФ, і 90 % членів таких хакерських угруповань – це російські військові. Від початку 2023 року командою CERT-UA було відбито й опрацьовано 700 кіберінцидентів, третина із них – це атаки на органи влади. Так, у квітні опрацьовано 151 атаку і кіберінцидент, 54 із яких – на органи влади, а це в у 2,5 рази більше, ніж атак на сектор сил безпеки й оборони [3].

Дійсно, кібератаки щільно вмонтовані у комбіновані способи впливу як на бойову обстановку (себто безпосередньо на полі бою), так і на тилові системи управління й забезпечення. Цілком зрозуміло, що оборона країни – справа комплексна, а нормальне функціонування, скажімо, фінансового сектору є необхідним для виконання оборонного замовлення зі всіма його компонентами, включаючи продовольче забезпечення війська. Саме тому не слід недооцінювати кіберзлочинність в умовах війни, визначати її тільки у контурах ординарної злочинності. Більш того, на сьогоднішній день є всі підстави для того, аби поставити питання про можливість визнання окремих кіберзлочинів як воєнних злочинів, як одних з проявів порушень законів і звичаїв війни. Зокрема, це стосується тих випадків, коли кібератак зазнають об'єкти критичної інфраструктури, що забезпечують життєдіяльність цивільного населення (системи електромережі, системи управління водопостачанням тощо).

Отже, вчасне реагування, запобігання, припинення кібератак в контексті збройного конфлікту є однією з базових умов забезпечення національної безпеки та зміцнення обороноздатності України.

Список використаних джерел:

1. 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. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Свиридюк Ю. В Україні зафіксували майже 4 000 кібератак з боку РФ. *Суспільне. Новини.* 2023. 18 листопада. URL: https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/

3. Держспецзв'язку: в кіберпросторі Росія використовує таку саму тактику, як і на полі бою. *Радіо Свобода*. 2023. 02 травня. URL: https://www.radiosvoboda.org/a/news-khaker-kiberataka-viyna-rosiya/32390482.html