УДК 343.2
DOI https://doi.org/10.24144/2307-3322.2024.84.3.43

ПРОБЛЕМИ АКТІВ КІБЕРТЕРОРИЗМУ В УМОВАХ ВОЄННОГО СТАНУ

Драгоненко А.О.,
доцент, кандидат юридичних наук,
доцентр кафедри кримінального права та кримінології
факультету № 1 ДонДУВС
ORCID: 0000-0001-8353-2341
e-mail: dragonenko84@gmail.com

Федорчак І.В.,
викладач кафедри криінального права та кримінології
факультету № 1 ДонДУВС
ORCID: 0000-0001-8353-2341
e-mail: kirov0079@gmail.com

Драгоненко А.О., Федорчак І.В. Проблеми актів кібертероризму в умовах воєнного стану.
Кожна сучасна соціально активна людина в Україні користується мобільними пристроями та мають доступ до Інтернету, державні установи перейшли на електронний документообіг, стабільна робота банківського сектору, залізниці, авіаційного транспорту та великих компаній залежить від стабільності кіберпростору, в якому вони працюють і покладаються на комунікацію за допомогою електронних засобів.

В умовах воєнного стану діяльність органів державної влади та органів місцевого самоврядування зводиться до сприяння органам управління, створеним в окремих регіонах, у безпосередньому виконанні завдань національної оборони. У системі органів державної влади, що діють в умовах воєнного стану, органи внутрішніх справ займають особливе місце, що зумовлено характером завдань, які вони виконують у цих оперативних умовах. Ефективність діяльності органів внутрішніх справ є життєво важливою для безпосереднього забезпечення внутрішньої безпеки.

Саме з цією метою необхідно чітко визначити компетенцію органів внутрішніх справ. Адже лише наявність певних повноважень забезпечує гарантію дотримання законності при виконанні функцій службами та підрозділами органів внутрішніх справ. Безумовно, для успішного виконання завдань, покладених на Міністерство внутрішніх справ в умовах воєнного стану, обов'язки та права Міністерства внутрішніх справ повинні відповідати базовому принципу, що новим обов'язкам відповідають нові права. Дуже важливим є включення до системи примусових заходів розширення повноважень органів внутрішніх справ під час запровадження воєнного стану. Співробітники внутрішньої безпеки не можуть виходити за межі дозволених способів і засобів здійснення охоронних операцій. На нашу думку, обсяг повноважень працівника органів внутрішніх справ у таких випадках має бути розширений. Складність повноважень Міністерства внутрішніх справ відображається на внутрішньому управлінні різними установами.

Законодавство України про кримінальну відповідальність, яке розроблялося для потреб мирного часу, виявилося в ситуації збройної агресії РФ недостатньо ефективним у сфері протидії злочинності. Така ситуація обумовила необхідність термінової адаптації законодавства України до умов воєнного стану.

Ключові слова: кібертероризм, воєнний стан, Україна, кіберзлочин, війна.

Dragonenko A., Fedorchak I. Problems of acts of cyber-terrorism in the conditions of martial law.
Every modern socially active person in Ukraine uses mobile devices and has access to the Internet, state institutions have switched to electronic document management, the stable operation of the banking sector, railways, air transport and large companies depends on the stability of the cyberspace in which they work and rely on communication using electronic means.

In the conditions of martial law, the activities of state authorities and local self-government bodies are reduced to assisting the governing bodies created in individual regions in the direct performance of national defense tasks. In the system of state authorities operating under martial law, internal affairs bodies occupy a special place due to the nature of the tasks they perform under these operational conditions. Effectiveness of internal affairs bodies is vital for the direct provision of internal security.

It is for this purpose that it is necessary to clearly define the competence of internal affairs bodies. After all, only the presence of certain powers ensures compliance with legality in the performance of functions by services and divisions of internal affairs bodies. Of course, for the successful implementation of the tasks assigned to the Ministry of Internal Affairs under martial law, the duties and rights of the Ministry of Internal Affairs must correspond to the basic principle that new duties correspond to new rights. It is very important to include in the system of coercive measures the expansion of the powers of internal affairs bodies during the introduction of martial law. Internal security officers cannot go beyond the permitted methods and means of carrying out security operations. In our opinion, the scope of powers of the employee of internal affairs bodies in such cases should be expanded. The complexity of the powers of the Ministry of Internal Affairs is reflected in the internal management of various institutions.

The legislation of Ukraine on criminal responsibility, which was developed for the needs of peacetime, turned out to be insufficiently effective in the field of combating crime in the situation of armed aggression of the Russian Federation. Such a situation necessitated the urgent adaptation of the legislation of Ukraine to the conditions of martial law.

Key words: cyberterrorism, martial law, Ukraine, cybercrime, war.

Постановка проблеми. Виявлення проблем та розробка рекомендацій щодо удосконалення кримінально-правової протидії актам кібертероризму в умовах воєнного стану. Підвищення ефективності боротьби з кіберзлочинністю у воєнний час та посилення відповідальності за пов'язані з нею правопорушення. Кіберпростір потребує більшого захисту та змін. Відкрита агресія Росії стимулювала вдосконалення існуючого законодавства та безпеки в сучасному інформаційному середовищі.

Мета дослідження – аналіз актів кібертероризму в умовах воєнного стану.

Стан опрацювання проблематики. З початком війни Україна стала об'єктом численних кібератак, що впливають на державні установи, громадські організації та громадян. Зокрема, компанії, що працюють у секторах критичної інфраструктури, таких як енергетика, телекомунікації, медіа та фінансові компанії, також повинні бути в стані підвищеної готовності, оскільки ці сектори часто визнаються пріоритетними цілями під час війни. Таким чином, об'єктом уваги діяльності органів внутрішніх справ є внутрішні загрози військового стану України, особливо такі, як криміналізація суспільства, розвиток «тіньової економіки», різні прояви тероризму, неналежне виконання законів і низький рівень правопорядку та ін. Отже, основною функцією органів внутрішніх справ та служби безпеки України щодо забезпечення режиму воєнного стану є протидія внутрішнім загрозам, чого досягають вирішенням таких завдань, як боротьба зі злочинністю, особливо з її організованими формами; протидія різним проявам тероризму; забезпечення громадської безпеки тощо.

Виклад основного матеріалу. Виклики, що постали перед Україною на фоні збройної агресії РФ 2014–2022 рр., стали серйозним випробуванням для держави, обумовили екстрену трансформацію державної політики у сфері національної безпеки, у тому числі в аспекті вдосконалення правового регулювання протидії злочинності.

Термін «кібертероризм» поєднує в собі два поняття: «кібер» («кіберпростір») і «тероризм». У літературі все частіше використовуються терміни «віртуальний простір» і «віртуальний світ». На основі поєднання понять «тероризм» і «віртуальний простір» можна дати наступне визначення: кібертероризм – це комплексна закономірність, що виражається в таких діях, як навмисні і політично мотивовані атаки на комп'ютери та інформацію, що обробляється комп'ютерними системами, порушення громадської безпеки, якщо вони вчиняються з метою провокації військового конфлікту, залякування населення, створення небезпеки для життя чи здоров'я людей або настання інших тяжких наслідків.

Розвиток інформаційних технологій та глобалізація обумовили появу нових загроз як міжнародній, так і національній безпеці, зокрема кібертероризму [1], визнається однією з найнебезпечніших формою кіберзлочинності.

Експерти, які займаються дослідженням даної проблеми, визнають, що кібертероризм відносно новий різновид тероризму, у XXI столітті має тенденцію до поширення.

Кібертероризм – це серйозна загроза людству, порівняна з ядерною, бактеріологічною та хімічною зброєю, причому ступінь цієї загрози через свою новизну не до кінця усвідомлений і вивчений [2]. Аналізуючи проблеми світових загроз, директор ЦРУ США Джордж Тенет свого часу наголошував, що кібертероризм у світі стрімко набуває неочікувано великих масштабів і зрештою стає реальною загрозою для національної безпеки будь-якої держави [3].

У колективній монографії «Світова гібридна війна: український фронт», підготовленій експертами Національного інституту стратегічних досліджень, звертається увага на те, що частка кібертероризму в світі зростає, а його вплив на національну та міжнародну безпеку стає все більш відчутним. DDoS-атаки на сайти урядів (США, Канади, Південної Кореї, Ізраїлю, Естонії та ін.), державних і приватних компаній (NASA, Delta Air Lines, Dell, Yahoo, Amazon, E-bay, Sony, CNN) та міжнародних організацій (ООН, МОК) [4] відбуваються все частіше.

Відзначаючи внесок науковців у дослідження різних аспектів тероризму загалом та кібертероризму зокрема, варто зауважити, що питання кримінально-правових заходів протидії цьому явищу досліджено недостатньо. З іншого боку, масштаби кібертерористичних актів та масштаби їх наслідків вимагають більш глибокого правового аналізу кібертерористичної загрози в Україні та розробки і впровадження ефективних кримінально-правових заходів протидії цьому явищу. Підвищення ефективності кримінально-правових заходів протидії потребує комплексних досліджень, ранньої ідентифікації загрози, розвитку правової бази та культури, а також комплексу превентивних заходів, що об'єднують зусилля світових держав, українських державних інституцій та неурядових організацій.

Науковці зазначають, що прояви кібертероризму дуже широкі, починаючи від протиправного впливу на процеси прийняття необґрунтованих рішень, поширення паніки та безладу, проникнення в канали та системи супутникового зв'язку, навігації, енергоменеджменту, транспорту, банківської справи тощо. На відміну від традиційних терористів, які для досягнення своїх цілей використовують вибухівку та стрілецьку зброю, кібертерористи використовують спеціалізоване програмне забезпечення, призначене для незаконного проникнення в сучасні інформаційні технології, комп'ютерні системи, мережі та комп'ютерні комплекси і організації віддалених атак на цільові інформаційні ресурси [6].

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року, зазначено, що Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці та поєднує деструктивні дії в кіберпросторі з інформаційно-психологічними операціями, активно впроваджує концепцію інформаційної війни, що базується на застосуванні інформаційних війн - механізму, який активно використовується в гібридній війні, розв'язаній проти України. Така підривна діяльність створює реальну загрозу кібертероризму та кібердиверсій проти національних інформаційних інфраструктур.

Пріоритетними цілями кібертероризму є ядерні об'єкти, електро- та водопостачання, електронні комунікації, фінансовий та банківський сектори, повітряний та залізничний транспорт, об'єкти зберігання стратегічної сировини, хімічні та біологічні об'єкти (стаття 1, пункти 5 та 8 Стратегії) [7].

Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням (стаття 13 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року). М.О. Єфремова у своєму дисертаційному дослідженні пропонує визначати кібертероризм як незаконний вплив на інформаційно-комунікаційні системи з метою залякування населення та впливу на процеси прийняття рішень органами влади та міжнародними організаціями; Д. Деннінг визначає кібертероризм як «незаконну атаку або загрозу атаки на комп'ютери, мережі або інформацію, що міститься в них, яка здійснюється для того, щоб змусити органи влади підтримати досягнення політичних або соціальних цілей» [8].

Аналізуючи питання боротьби з кібертероризмом, Є.Д. Данильченко зазначає, що військово-політичне керівництво США вперше розглянуло кіберпростір як нове поле бою поряд із сушею, морем і повітрям. У 2001 році Конгрес США ухвалив Антитерористичний закон, відомий як «Акт патріотів США» (USA PATRIOT Act). Цим законом Конгрес ввів нове юридичне поняття «кібертероризм», яке включає в себе різні форми кваліфікованого злому і пошкодження захищених комп'ютерних мереж громадян, юридичних осіб і державних установ, а також комп'ютерів,

що використовуються державними органами для організації національної оборони і забезпечення національної безпеки. Тепер це також включає в себе нанесення шкоди системам.

Масштабна збройна агресія Російської Федерації проти України супроводжувалася актами кібертероризму в кіберпросторі, здебільшого спрямованими на об'єкти критичної інфраструктури та цивільне населення. У 2022 році кібервійна опинилася в центрі відкритої атаки, що призвела до перехоплення секретної інформації та оборонних рішень. Кібератаки на штаби загрожують військовій стратегії, а перехоплення інформації про поведінку бойових підрозділів ставить під загрозу оборонні позиції. За даними Microsoft, загарбники здійснили кібератаки на українські державні установи та урядові організації, зливаючи та компрометуючи конфіденційну інформацію [9].

Український правознавець Р. Мовчан зазначає, що «перш ніж оголосити «спецоперації» і відкрито застосувати танки, артилерію, авіацію та одурманених пропагандою солдатів, Росія за кілька тижнів до 24 лютого 2022 року широко проводила іншу форму агресії. Це була масштабна кібератака на нашу країну, спрямована не лише на порушення функціонування об'єктів критичної інфраструктури, а й на поширення паніки серед українського населення».

Кібератаки продовжилися і після ескалації бойових дій та введення воєнного стану, хоча цілі були дещо іншими. Академік зазначив, що, по-перше, всі російські кібератаки, на які посилаються у доданому документі автори закону від 24 березня 2022 року, здійснювалися і продовжують здійснюватися з єдиною метою - послабити нашу державу. По-друге, потенційні наслідки, про які йдеться у вищезгаданій забороні у вигляді «серйозних техногенних аварій чи екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків», насправді є наслідками реалізації тієї ж диверсії, тобто суто «масового винищення людей», ушкодження людського організму чи іншої шкоди здоров'ю, знищення або пошкодження об'єктів, що мають важливе народногосподарське чи оборонне значення, радіоактивного забруднення, масових отруєнь, поширення інфекційних хвороб, епідемій та пандемій»; Р. Мовчан стверджує, що відповідними кібератаками в РФ є ті, що зазначені в ч. 4 ст. 361 КК і фактично є лише формою диверсії та підпадають під ч. 1 ст. 113 КК за звичайних обставин, а також під ч. 2 ст. 113 КК, якщо вони вчинені в умовах воєнного стану або в період збройного конфлікту [10]. Є підстави вважати, що кібератаки з боку Росії здійснювалися і продовжують здійснюватися насамперед з терористичною метою (залякування населення, вплив на процеси прийняття рішень, вчинення або невчинення дій органами державної влади, міжнародними організаціями тощо) у розумінні статті 258 КК «Терористичне діяння».

За оцінками експертів, метою спонсорованих Російською Федерацією національних та військових кібероперацій є підтримка стратегічних політичних цілей Росії. Ці цілі включають підрив політичної системи США, підрив суверенітету України та зображення України як лиходія у світі, як це було під час кібератаки NotPetya у 2017 році [11].

У Регламенті від 17 травня 2019 року (статті 1(1) та 1(4)) ЄС визначає серйозну кібератаку як загрозу державі-члену ЄС, її критичній інфраструктурі, послугам або підтримці соціального функціонування, здоров'ю, безпеці та добробуту її громадян, зокрема у сферах енергетики, транспорту, банківської справи, охорони здоров'я, питної води та цифрової інфраструктури. Вона визначається як зовнішня загроза основним державним інституціям та процесам [12].

За даними СБУ, хакерське угруповання «Армагеддон» є спеціальним проектом ФСБ Росії, спрямованим проти України: з початку російської окупації у 2014 році цей підрозділ ФСБ здійснив понад 5 000 кібератак і намагався «заразити» понад 1 500 державних комп'ютерних систем. Основними цілями зловмисників були:

– контроль над об'єктами критичної інфраструктури (електростанції, системи теплопостачання, водопостачання);

– викрадення інформації та збір інформації, в тому числі з обмеженим доступом (сектор безпеки та оборони, державні установи);

– використання розвідки та психологічного впливу;

– блокування інформаційних систем [13].

У відповідь на сучасні виклики до законів деяких штатів (США, Джорджія) були внесені поправки, що включають такі злочини, як кібертероризм. На особливу увагу в цих законах заслуговує положення статті 324[1] Розділу 11 «Злочини проти держави» КК Грузії, що має назву «Кібертероризм»: «Карається кібертероризм, тобто правопорушення, вчинені з метою залякування

громадськості або (та) впливу на владу, тобто незаконне отримання, використання або загроза використання комп'ютерної інформації, що охороняється законом, з ризиком настання в результаті цього серйозних наслідків». Назва статті КК «Кібертероризм» видається невдалою, оскільки в ній йдеться про конкретні акти кібертероризму як прояв цього явища.

На нашу думку, акти кібертероризму, що вчиняються в нашій країні, повинні регулюватися статтею 258 ККУ «Терористичне діяння». У світлі вищевикладеного, заслуговує на увагу підхід М.А. Єфремової, яка пропонує визначити положення статті 258 КК під назвою «Терористичне діяння» наступним чином: «Вибухи, підпали, незаконний вплив на інформаційно-телекомунікаційні системи або інші дії з метою впливу на прийняття рішень органами влади чи міжнародними організаціями для залякування населення, заподіяння загибелі людей, створення небезпеки заподіяння тяжких наслідків у вигляді загибелі людей, заподіяння майнової шкоди чи настання інших тяжких наслідків, а також погроза вчинення зазначених дій із зазначеною вище метою».

Такий підхід міститься в положеннях статті 237 «Акти тероризму».

Відповідно до статті 237 «Акти тероризму» розділу 3 «Кримінальні правопорушення проти державної влади» Кримінального кодексу Естонії, згідно з якою «...втручання в комп'ютерні дані або функціонування комп'ютерних систем, а також погроза вчинення таких дій, якщо вони вчинені з метою спричинити або запобігти вчиненню державою або міжнародною організацією дій ... . . караються позбавленням волі на строк від п'яти до двадцяти років або довічним позбавленням волі» [14]. Таким чином, окремі дії, перелічені у вищезгаданих актах, є актами кібертероризму.

Стаття 5.2.4 нового проекту Основного Закону України (від 18 травня 2022 року) «Терористичне діяння» звучить наступним чином: «той, хто з метою залякування населення, дестабілізації діяльності органів державної влади чи міжнародних організацій або примусу чи перешкоджання вчиненню ними будь-яких дій:

1) затримує осіб;

2) застосовує зброю чи інші предмети, здатні створити небезпеку для життя чи серйозну загрозу здоров'ю;

3) захоплює, утримує, знищує або пошкоджує об'єкти критичної інфраструктури чи обладнання, необхідне для функціонування таких об'єктів, або приводить таке обладнання у непридатність;

4) використовує літаки, кораблі, інші пасажирські або вантажні транспортні засоби;

5) виробляє, набуває, перевозить, доставляє або використовує вогнепальну зброю, вибухові пристрої, ядерну, біологічну або хімічну зброю або володіє такою зброєю;

6) викидає токсичні речовини в навколишнє середовище або спричиняє пожежу, повінь або вибух, небезпечні для життя людей;

7) порушує постачання води, а також природних ресурсів, необхідних для інших, є злочином п'ятого ступеня [15].

Висновки. Вважаємо, що в частині першій статті 258 «Терористичне діяння» чинного Кримінального кодексу України після слів «терористичні акти, тобто застосування зброї, вибухи та підпали» доцільно доповнити текст словами «незаконний вплив на інформаційно-комунікаційні системи». Ми вважаємо, що в новому проекті Кримінального кодексу України (від 18 травня 2022 року) було б доречно додати положення про кібертерористичні акти до статті 5.2.4 «Терористичне діяння». Тому статтю 5.2.4 проєкту КК, який зараз обговорюється, слід доповнити статтею 9, яка передбачає наступне формулювання: «З метою залякування населення, дестабілізації діяльності органів державної влади чи міжнародних організацій або примусу чи стримування їх від вчинення будь-яких дій використовуються такі висловлювання: .... ті, які вчиняють злочини у кіберпросторі з використанням інформаційно-комунікаційних технологій». Вважаємо, що реалізація цих пропозицій сприятиме більш ефективному реагуванню на акти кібертероризму, має певний превентивний потенціал та свідчить про правильне розуміння законодавцем рівня суспільної небезпеки аналізованих діянь.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бойченко О.В., Ончурова О.О. Кібертероризм у складі сучасних проблем національної безпеки. *Форум права*. 2010. №2. С. 57.
2. Голубєв В.А. Кібертероризм як нова форма тероризму. URL: https://www.crime-research.org/library/Gol_tem3.htm.

3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. К.: ДУТ, 2015. С. 58.
4. Світова гібридна війна: український фронт / За заг. ред. В.П. Горбуліна. Національний інститут стратегічних досліджень. К.: НІСД, 2017. С. 89.
5. Gabriel Weimann. Cyberterrorism How Real Is the Threat? Special report. December 2004. P. 11. URL: https://www.usip.org/sites/ default/files/sr119.pdf.
6. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «АртЕк», 2017. С. 35-36.
7. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/ documents/4472021–40013.
8. Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. URL: https://nautilus.org/global-problemsolving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-forinfluencing-foreign-policy-2/?view=pdf.
9. Ахтирська Н., Гуцалюк М. Правові засоби боротьби з кіберзагрозами під час воєнного стану в світлі використання механізмів Другого додаткового протоколу до Конвенції про кіберзлочинність. Актуальні питання розвитку юридичної науки та практики: матеріали Міжнародної науково-практичної конференції (12 травня 2022 року) / За заг. ред. д.ю.н., акад. НАПрН України О.П. Орлюк, к.ю.н., доц. Г.З. Остапенко, к.ю.н. А.В. Айдинян. К., 2022. С. 283-284.
10. Мовчан Р.О. Зміни, направлені на підвищення ефективності кримінально-правової протидії кіберзлочинності в умовах дії воєнного стану URL: https:// www.facebook.com/permalink.php?story_fbid=3243781402611850& id=100009400659772.
11. Наскільки надійна в Україні система захисту кіберпростору, які цілі російських хакерів, хто їх фінансує та в чому їх сильні та слабкі сторони? URL: https://www.epravda.com.ua/publications/2021/11/3/679341/.
12. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. ST/7302/2019/INIT. URL: https://eur-lex.europa.eu/legalcontent/GA/TXT/?uri= CELEX%3A32019R0796.
13. СБУ встановила хакерів ФСБ, які здійснили понад 5 тис. кібератак на державні органи України. URL: https://ssu.gov.ua/novyny/sbu-vstanovyla-khakerivfsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy.
14. Penal Code of the Republic of Estonia (2001, amended 2021). URL: https:// www.legislationline.org/download/id/9098/file/EST_CC_as%20of% 20May%202021.pdf.
15. Кримінальний кодекс України (проєкт). Контрольний текст (станом на 18.05.2002). URL: https://newcriminalcode.org.ua/upload/media/2022/05/19/ kontrolnyj-proekt-kk-18-05-2022.pdf.
16. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
17. Питання кібербезпеки в умовах воєнного часу. URL: https://kpmg.com/ua/uk/ blogs/home/posts/2022/4/pytannya-kiberbezpeky-v-umovakh-voyennoho-chasu.html.
18. 5 порад з кібербезпеки під час війни. URL: https://yur-gazeta.com/dumka-eksperta/5-porad-z-kiberbezpeki-pid-chas-viyni.html.