УДК 343.96 **DOI:** https://doi.org/10.32631/v.2023.3.37

Дмитро Сергійович Мельник,
кандидат юридичних наук, старший дослідник,
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при Раді національної безпеки
і оборони України, м. Київ (провідний науковий співробітник);
https://orcid.org/0000-0002-1497-950X,
e-mail: d-melnik@ukr.net

КІБЕРТЕРОРИЗМ: ЗМІСТ, ФОРМИ ТА ПЕРСПЕКТИВНІ ЗАХОДИ ПРОТИДІЇ

Проаналізовано сучасні підходи до визначення змісту кібертероризму та його соціальної і правової природи. Описано типові ознаки кібертероризму та запропоновано визначення його поняття. Розкрито основні форми кібертероризму: вчинення терористичних актів організаціями, групами й окремими особами за допомогою комп'ютерів і комп'ютерних мереж або шляхом впливу на інформацію, яка в них обробляється (циркулює), а також використання кіберпростору для інших цілей терористичної діяльності, безпосередньо не пов'язаних зі здійсненням терактів. Запропоновано шляхи вдосконалення системи заходів протидії кібертероризму.

Ключові слова: кібертероризм, комп'ютерні системи і мережі, кіберпростір, заходи протидії.

Оригінальна стаття

Постановка проблеми

Глобальний інформаційний простір упродовж кількох останніх десятиліть став ареною боротьби між світовими державами-лідерами за отримання переваги у вирішенні проблем і конфліктів. Процеси глобалізації та невпинний розвиток інформаційних технологій породили нові загрози національній безпеці, насамперед терористичні та кібернетичні, виникнення кібертероризму, безпосередньо пов'язаного з рівнем науково-технічного прогресу. Поява кібертероризму, що розглядається фахівцями як різновид технологічного тероризму та визнаний одним із найнебезпечніших видів кіберзлочинності, зумовлена переходом до електронного управління технологічними процесами [1, с. 91].

Із приєднанням нашої держави до глобального кіберпростору проблема кібертероризму стала для України надактуальною. Рівень інформатизації української держави і суспільства, що зростає, зумовлює потребу створення сучасної та надійної системи гарантування кібербезпеки.

Стан дослідження проблеми

Наукову розробку проблеми тероризму здійснювали такі науковці, як В. Антипенко, Л. Багрій-Шахматов, А. Бакаєв, Д. Белл, Д. Белявський, Ж. Бодріяр, Е. Гіденс, В. Ємельянов, К. Жаринов, В. Крутов, В. Ліпкан, Б. Леонов, О. Соколовський, Е. Тоффлер, Б. Хофман, А. Шмід, Ф. Фукуяма та ін. Інформаційні кібернетико-технологічні аспекти тероризму досліджувалися вітчизняними та іноземними дослідниками (К. Андерсон, К. Беляков, В. Бутузов, В. Голубєв, Д. Дубов, В. Ібрагімов, А. Келлі, Дж. Левіс, Б. Леонов, В. Тафоя, К. Тітуніна та ін.), які спробували виокремити кібертероризм у спеціальний вид і дослідити його зміст.

Мета і завдання дослідження

Метою статті є уточнення поняття кібернетичного тероризму та його основних форм. *Завданням* дослідження є вироблення пропозицій із формування системи заходів протидії кібертероризму з урахуванням уточненого змісту і форм цього протиправного явища.

Наукова новизна дослідження

З'ясовано правову природу і сутність кібернетичного тероризму та його основні форми, напрацьовано пропозиції з формування системи заходів протидії кібертероризму насамперед в умовах повномасштабної збройної агресії рф проти нашої країни, які досі були малодосліджені науковцями.

Виклад основного матеріалу

Сучасні високотехнологічні терористичні акти здатні викликати системну кризу на місцевому, регіональному та світовому рівнях. Реальна можливість застосування терористами новітніх інформаційних технологій створює передумови до масштабних аварій на виробництві, блокування роботи транспорту, дезорганізації державного управління, фінансової системи, роботи наукових та медичних центрів. В умовах всеохоплюючого проникнення інформаційних технологій у системи управління державою та керування процесами критичної інфраструктури вони стають дедалі більш вразливими для кіберзагроз, зокрема кібертероризму.

Приклади протиправного застосування наприкінці XX століття кібернетичних засобів проти критичної інфраструктури країн заходу засвідчили її вразливість і непередбачуваність наслідків. Неодноразові спроби проникнення хакерів у бази даних Пентагону, системи управління супутниками у Великобританії тощо та розміри завданих ними збитків засвідчують відсутність системи ефективного захисту від загрози кібертероризму. Тому він розглядається як одна з основних загроз національній безпеці, зокрема європейських країн.

Відомо, що значні сподівання на кібертероризм покладають ісламські екстремісти, щоб підірвати політичну й економічну стабільність країн Заходу. Свого часу Усама бен Ладен з прихильниками розглядав комп'ютерні теракти та диверсії як один із кроків до розгрому США й побудови всесвітнього халіфату [2, с. А3]. Терористична організація «Арабський Електронний Джихад» (AEJT), що обрала своїм гаслом «поставити на коліна мережу "Інтернет"», заявила про своє існування ще у 2003 році. Метою діяльності організації визначено знищення всіх ізраїльських, американських та інших неприйнятних сайтів.

Першим масовим проявом хактивізму в Україні стали події щодо припинення роботи файлообмінного сервісу EX.ua, що наочно продемонстрували неготовність нашої держави до подібних атак. Після спроб правоохоронців заблокувати роботу вказаного сервісу невстановленими особами було вчинено DDoS-атаки на низку інтернет-сайтів державних органів, зокрема Адміністрації Президента та МВС України. Саме відсутність прямих економічних збитків не призвела до надання правової оцінки цим подіям та належних висновків, а Україна виявилась непідготовленою до протистояння з рф у кібернетичній сфері [3, с. 212].

Таким чином, політично вмотивована діяльність у кіберпросторі у формі атак на урядові та приватні вебсайти набуває все більшого поширення. При цьому дедалі частіше об'єктами кібератак стають інформаційні ресурси фінансових установ, підприємств енергетики і транспорту, органів безпеки й оборони держави, захисту від надзвичайних ситуацій. Новітні технології використовують для вчинення нових видів злочинів, типових для держави і суспільства з високим рівнем інформатизації.

Сьогодні на міжнародному рівні поняття кібертероризму не визначене. У багатьох країнах світу досі не існує ані законодавчого, ані визнаного наукового визначення кібертероризму: найчастіше цим підвидом тероризму називають різноманітні прояви кіберзлочинності, кібервійни чи традиційного тероризму [4]. Однак фактично кібертероризм полягає у протиправному використанні новітніх інформаційних (комп'ютерних, електронних комунікаційних та інших технологій) з терористичною метою.

Термін «кібертероризм» *(cyber-terrorism)* був запропонований ще у 80-х роках XX століття співробітником американського Інституту безпеки та розвідки Б. Колліном, який використав його в контексті переходу тероризму з фізичного у віртуальний світ, перетинання та зрощування цих світів [5, p. 55].

Національна конференція законодавчих зборів штатів (NCSL) у США визначила кібертероризм як використання інформаційних

технологій терористами для досягнення своїх цілей, що може включати в себе організацію та здійснення атак на телекомунікаційні мережі, інформаційні системи та комунікаційну інфраструктуру або обмін інформацією, а також погрози з використанням засобів електрозв'язку, зокрема злам інформаційних систем, внесення вірусів до вразливих мереж, дефейс вебсайтів, DDoS-атаки, терористичні погрози, надіслані електронними засобами зв'язку [6, p. 64].

Водночас Національна стратегія США з протидії внутрішньому тероризму від 15 червня 2021 року не містить визначення та не оперує поняттям кібертероризму. Однак вона все ж передбачає певні заходи протидії тероризму в мережі Інтернет: протидія вербуванню терористів в інтернеті та їхній мобілізації для здійснення терактів, формування інноваційних способів розвитку цифрової грамотності та зміцнення стійкості населення щодо дій терористів; видалення з інтернету матеріалів терористичного і екстремістського характеру з дотриманням права на свободу вираження поглядів; протидія поляризації суспільства шляхом підтримки здорового інформаційного середовища [7, с. 3–4].

Однак зарубіжні дослідники зазначають, що, попри реальність і зростання загрози політично мотивованих кіберзлочинів, термін «кібертероризм» вживається занадто часто, а небезпека явища часто перебільшується мас-медіа та виробниками засобів кібербезпеки, які бажають наростити продажі своїх продуктів [8].

Вітчизняні дослідники у своїх підходах до визначення поняття кібертероризму варіюють від усвідомлення використання з терористичною метою новітніх електронних комунікаційних систем, мереж і технологій як засобу вчинення злочину, інформації, що в них обробляється, як предмета протиправного посягання до використання кіберпростору як технологічного середовища для вчинення злочину.

Так, О. Климчук та Р. Кравченко вважають кібертероризм формою терористичного прояву, в якій комп'ютери, комп'ютерні системи та мережі використовують як засіб учинення злочину [9, с. 28]. В. Бутузов визначає кібертероризм як суспільно небезпечну діяльність, що полягає в цілеспрямованому та свідомому застосуванні насильства шляхом залякування органів влади і населення з використанням комп'ютерів, комп'ютерних систем і мереж або вчинення інших посягань на життя чи здоров'я людей, або погрози вчинення таких дій для досягнення злочинних цілей [10, с. 135–136].

Схожу позицію мають С. Мельник, О. Тихомиров та О. Лєнков, які розглядають кібертероризм як суспільно небезпечну діяльність, що полягає в цілеспрямованому й свідомому залякуванні органів влади та населення для досягнення злочинних цілей і здійснюється з використанням інформаційно-комунікаційних систем [11, с. 164].

В. Пилипчук та О. Дзьобань розглядають акт кібертероризму як політично вмотивовану навмисну атаку на комп'ютерну систему, мережу та/або інформацію, яка в них обробляється, що викликає небезпеку для життя й здоров'я людей чи настання інших тяжких наслідків, коли така дія була здійснена з метою посягання на державну або суспільну безпеку, залякування населення, провокації військового конфлікту чи загрозу вчинення цих дій [12, с. 15]. О. Довгань і В. Хлань уважають, що кібертероризм – це суспільно небезпечна діяльність, яка проводиться із терористичною метою в кіберпросторі чи з використанням технологічних можливостей останнього і полягає в цілеспрямованому залякуванні органів влади та населення, здійсненні інших посягань на життя й здоров'я людей [13, с. 51].

Основні складові цих підходів були переважно враховані українським законодавцем. Так, у п. 13 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII надано визначення *кібертероризму* як терористичної діяльності, що відбувається в кіберпросторі або здійснюється з його використанням та фактично визнається різновидом *технологічного тероризму*.

Відповідно до абз. 4 ч. 1 ст. 1 Закону України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV технологічний тероризм охоплює кримінальні правопорушення, які вчиняються з терористичною метою із застосуванням комп'ютерних систем та комунікаційних мереж включно із захопленням, виведенням з ладу і руйнуванням потенційно небезпечних об'єктів, які створили або загрожують появою загрози надзвичайної ситуації внаслідок цих дій та викликають небезпеку для персоналу, інших людей й довкілля; створюють передумови для аварій і техногенних катастроф.

Водночас Концепція боротьби з тероризмом в Україні, затверджена Указом Президента України від 5 березня 2019 року № 53/2019, не використовує термін «кібертероризм» і не передбачає заходів протидії йому. Такий підхід, безумовно, впливає на протидію терористичним правопорушенням в інтернеті.

Таким чином, законодавче визначення кібертероризму з точки зору потреб практики правозастосування видається надто загальним, а тому потребує уточнення з адекватним відображенням його змісту як у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», так і у ст. 1 Закону України «Про боротьбу з тероризмом».

У контексті викладеного заслуговує на увагу наукова позиція, відповідно до якої кібертероризм – це навмисна, політично мотивована кібератака на комп'ютерну систему та (або) мережу, інформацію, що в них обробляється, якщо така атака викликає розлади в роботі

елементів критичної інфраструктури держави та небезпеку для життя й здоров'я людей або спричиняє інші тяжкі наслідки, якщо такі дії були вчинені з метою посягання на суспільну безпеку, залякування населення, провокації військового чи міжнародного конфлікту, впливу на прийняття рішень чи вчинення дій органами державної влади/місцевого самоврядування, їх посадовцями, громадськими об'єднаннями, юридичними особами, звернення уваги громадськості до певних політичних, релігійних чи інших поглядів [14, с. 49].

На відміну від уже традиційних різновидів тероризму, для кібертероризму властивим є застосування новітніх досягнень науки й техніки у сфері комунікацій, комп'ютерних та інформаційних технологій тощо.

При цьому прояви кібертероризму фахівці розподіляють на такі групи: 1) реалізація терористичних актів у кіберпросторі, компоненти якого фактично стають інструментом учинення протиправних дій; 2) використання компонентів кіберпростору як предмета злочинних посягань; 3) використання кіберпростору для досягнення суміжних або проміжних цілей терористичної діяльності [15, с. 122].

Водночас більш оптимальним видається групування, яке дозволяє виокремити *дві основні форми* кібертероризму [16, с. 78–80], які потребують належної протидії:

1) вчинення терактів організаціями, групами й окремими особами за допомогою комп'ютерів чи комп'ютерних мереж або шляхом впливу на інформацію, яка в них обробляється (циркулює), виведення з ладу інформаційно-комунікаційних систем (далі – ІКС) управління державою, об'єктів критичної інфраструктури (далі – ОКІ), спричинення інших надзвичайних подій шляхом втручання в роботу програмного забезпечення ІКС зазначених об'єктів, зокрема з використанням комп'ютерних вірусів. Ця форма кібертероризму полягає у використанні комп'ютерних мережевих інструментів для несанкціонованого впливу на припинення роботи національних критичних інфраструктур (енергетика, логістичні перевезення, фінансові платежі, урядові операції тощо) та/або примушування чи залякування урядів або цивільного населення;

2) використання можливостей кіберпростору терористичними організаціями, групами й окремими терористами для інших цілей, не пов'язаних з учиненням терактів, однак спрямованих на забезпечення терористичної діяльності (координація та планування протиправної діяльності; збір необхідної інформації; використання як засобу зв'язку зі своїми членами й однодумцями; пропаганда тероризму; збирання коштів для фінансування терористичних рухів; вербування нових членів тощо). Резолюція Генеральної Асамблеї ООН від 26 червня 2018 року A/RES/72/284 звернула увагу на факти

широкого використання в умовах глобалізованого суспільства терористами та їх посібниками новітніх інформаційно-комунікаційних технологій (мережа Інтернет, соціальні мережі тощо) для вчинення, вербування виконавців, планування та/або фінансування терактів чи підбурювання до них, пошуку однодумців і підтримки від тих, хто їм співчуває.

Таким чином, основною формою кібертероризму є кібератака на комп'ютерну інформацію, електронні обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури. Наслідком такої атаки є проникнення в інформаційно-комунікаційну мережу або інфраструктуру, блокування засобів мережевого інформаційного обміну, перехоплення управління та вчинення інших дестабілізуючих дій [17, с. 163].

Передумовою для існування й подальшого розвитку явища кібертероризму є залежність національної критичної інфраструктури від автоматизованих систем (далі – АС) управління ОКІ, що зростає. Новітні інформаційно-комунікаційні технології широко застосовуються терористами для порушення штатних режимів роботи АС управління технологічними процесами на ОКІ поряд із традиційними способами вчинення терористичних актів.

Тому вчинення терористичних атак через інтернет в умовах зацентралізованості вітчизняних органів державного управління та недостатньої кваліфікації персоналу ІКС, що суттєво посилюють вразливість національної інфраструктури, може спричинити її руйнування [18, с. 57–58].

Вказаний стан справ знижує ефективність виконання уповноваженими суб'єктами безпекових завдань, перешкоджає забезпеченню ефективного захисту ОКІ, що суттєво підвищує небезпечність відповідних загроз національній безпеці України. Однак варто враховувати, що кібератаки активно використовують у сучасному кіберпросторі з протиправною метою вже не лише приватні особи, а й спецслужби іноземних держав та підконтрольні їм групи й організації.

На думку авторів Науково-практичного коментаря Закону України «Про основні засади забезпечення кібербезпеки України», вмотивовані державою кібератаки, які спрямовані на викрадення інформації з обмеженим доступом, знищення, дестабілізацію роботи інформаційних ресурсів, важливих для інших держав, або блокування доступу до них для отримання політичних, економічних, військових переваг у зовнішніх стосунках, є однією із сучасних форм розвідувально-підривної діяльності в мирний час, а в умовах війни такі кібератаки перетворюються на форму бойових дій [19, с. 105].

Тому слід погодитися з позицією дослідників про те, що кібертероризмом можуть бути визнані лише дії окремих індивідів, незалежних

груп чи організацій, учинені з терористичною метою. Відповідно будь-які кібератаки, вчинені державними організаціями, фактично є проявом *кібервійни* [16, с. 78]. Водночас сучасні особливості протидії гібридній війні рф проти України, що переросла в повномасштабну військову агресію, засвідчують можливість опосередкованого використання іноземними спецслужбами можливостей підконтрольних хакерів, хакерських груп та організацій для вчинення терактів і диверсій у кіберпросторі.

Водночас, якщо при визначенні поняття «кібертероризм» застосувати підхід, аналогічний до законодавчого визначення тероризму (ст. 1 Закону України «Про боротьбу з тероризмом»), то до актів кібертероризму можна віднести лише такі атаки на комп'ютерні системи через мережу Інтернет, які загрожують майну чи життю і здоров'ю людей, здатні призвести до серйозного порушення функціонування ОКІ та здійснюються недержавними агентами. Відповідно всі інші акти необхідно розцінювати як прояви кіберзлочинності чи кібервійни.

Для вчинення акту кібертероризму можуть бути використані різні способи протиправної діяльності в кіберпросторі:

– отримання несанкціонованого доступу до відомостей, що становлять державну, військову або банківську таємницю, персональних даних тощо;

– завдання збитків окремим елементам інформаційної інфраструктури ОКІ: руйнування мереж зв'язку та енергоживлення, блокування їх роботи, використання шкідливих програм для руйнування програмно-апаратних засобів тощо;

– викрадення або знищення інформації, програмного забезпечення та ресурсів шляхом подолання захисту, впровадження шкідливих програм;

– шкідливий вплив на роботу програмного забезпечення та інформацію, що обробляється (циркулює);

– розкриття та погроза опублікувати інформацію з обмеженим доступом;

– захоплення медіа-каналів з метою поширення дезінформації та чуток, демонстрації потужності терористичної організації і оголошення вимог;

– знищення або активне придушення систем і мереж зв'язку, перевантаження комунікаційних вузлів, невірна адресація;

– здійснення інформаційно-психологічних акцій і операцій тощо.

Сучасні терористи переважно завдають асиметричні удари, коли стратегічні цілі досягаються звичайними засобами, без використання високотехнологічної зброї. Однак їхні технічні можливості постійно підвищуються: вони використовують все більш доступні для

широкого загалу супутниковий зв'язок, сучасні засоби підробки документів, новітні інформаційні технології, нарощують свою присутність та активність у кіберпросторі для поширення пропаганди, вербування нових членів, підтримання комунікації з осередками, зокрема через Darknet та з використанням новітніх методів шифрування, надання послідовникам інструкцій щодо підготовки та вчинення терористичних атак, протиправної діяльності в кіберпросторі (здійснення кібератак, викрадення даних тощо).

При цьому у вільному доступі в мережі Інтернет можна отримати рецепти виготовлення вибухових пристроїв, супутникові знімки майбутнього об'єкта терористичної атаки та прилеглої місцевості, а системи онлайн-платежів і використання криптовалют суттєво спрощують і прискорюють проведення фінансових операцій, пов'язаних із забезпеченням терористичної діяльності. За різними оцінками, в мережі Інтернет існує не менше 5 000 такого типу сайтів, створених терористами [20, с. 6].

В умовах глобалізації та урбанізації міста є вузлами комп'ютерних мереж і технологій. Тому дослідники констатують пропорційну залежність між кількістю проявів кібертероризму та рівнем інформатизації й комп'ютеризації країни, яка обрана як ціль терористичної атаки [21, с. 134].

Бажаючи звернути увагу керівників нашої держави на зростання загрози кібертероризму, фахівці зауважують, що терористів можуть зацікавити державні установи та ОКІ, де використовують інформаційно-комунікаційні технології: АС управління та DATA-центри урядових установ, військових та медичних центрів управління, АС управління реакторами АЕС, сховищ радіоактивних матеріалів, нафтой газопроводів, систем водопостачання та розподілу електроенергії, космічних супутників, транспортних вузлів, оборонних та хімічних заводів і бактеріологічних лабораторій [22, с. 319–320]. У разі реалізації вказаних проявів загрози терористи можуть завдати національній безпеці України значної шкоди.

З іншого боку, використання новітніх інформаційних технологій у системах державного управління та життєдіяльності сучасного суспільства, так званої критичної інфраструктури (енергетика, транспорт, банківська сфера тощо), робить їх особливо вразливими для терактів.

Таким чином, під *кібернетичним тероризмом* слід розуміти суспільно небезпечну діяльність, яка полягає у вчиненні за допомогою комп'ютерних та електронних комунікаційних засобів навмисних, політично мотивованих атак на комп'ютерні системи/мережі, на інформацію, що обробляється (циркулює) у них, якщо вони викликають порушення роботи критичної інфраструктури держави та

створюють (можуть створювати) при цьому небезпеку для життя й здоров'я людей, завдають (можуть завдати) значної шкоди матеріальним об'єктам або спричиняють інші тяжкі наслідки й були вчинені з метою привернення максимально можливої уваги до політичних вимог терористів, або використання кіберпростору для інших цілей терористичної діяльності, безпосередньо не пов'язаних зі здійсненням терактів. Водночас запропоноване визначення не претендує на всеосяжність та науково-теоретичну досконалість, однак цілком може бути використане для дослідження цього питання.

Враховуючи викладене, закономірним буде висновок про те, що явище кібертероризму в сучасних умовах є реальною загрозою національній безпеці багатьох держав світу. Зокрема, кібертероризм загрожує непередбачуваними наслідками з точки зору руйнування ОКІ – систем управління й життєзабезпечення сучасних держав і суспільства.

Так, Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020, та Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16 лютого 2022 року № 56/2022, серед загроз національній і державній безпеці України виокремлюють: сучасну модель глобалізації, що уможливила поширення міжнародного тероризму та нові схеми його фінансування, зокрема в кіберпросторі; продовження рф гібридної війни проти України у формі систематичних кібератак, застосування інформаційно-психологічних засобів; укорінення в суспільстві радикальних настроїв і середовищ, які є підґрунтям політичного насильства та поширення тероризму; посилення кіберзагроз для ОКІ, пов'язаних із несанкціонованим втручанням у їх роботу, тощо.

Вищевказаний перелік загроз національній і державній безпеці уточнюється у Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021: гібридна агресія рф проти України в кіберпросторі; кібератаки рф, спрямовані на ІКС державних органів та інших ОКІ з метою їх руйнування, отримання прихованого доступу й контролю; використання кіберпростору для здійснення актів кібертероризму, надання матеріальної підтримки терористичній діяльності.

Зазначені загрози та ризики актів кіберагресії та кібертероризму в умовах гібридної війни рф проти України суттєво зросли після початку повномасштабної російської військової агресії та потребують вжиття системних заходів реагування на державному і міжнародному рівнях.

Оцінюючи рівень загрози кібертероризму для України, також слід враховувати: високий потенціал і професійний рівень вітчизняних програмістів, яких цінують провідні компанії світу; здатність молодих

фахівців швидко опановувати новітні технології; зростання економіки, що сприяє посиленню комп'ютеризації країни, тощо [21, с. 134].

З огляду на викладене можна зробити висновок про двоїстий характер проблеми кібертероризму для нашої держави. Так, з одного боку, Україна ще не досить заможна, щоб оперативно переобладнати сучасними системами управління свої ОКІ, що зробить їх невразливими для кібератак терористів. З другого боку, все більше зростає значення інформаційної інфраструктури як стратегічного ресурсу держави, що теж вимагає постійної уваги й охорони.

Комплексний характер загроз національній безпеці, пов'язаних з явищем кібертероризму, потребує визначення інноваційних підходів до формування системи кібербезпеки та кіберзахисту ОКІ й подальшого розвитку кіберпростору в умовах глобалізації й вільного обігу інформації.

Тому для покращення протидії загрозі кібертероризму вважають за доцільне вжити на державному рівні таких заходів [23, с. 114]:

1) *законодавчі*:

– визначити поняття кібертероризму у ст. 1 Закону України «Про боротьбу з тероризмом», а також привести у відповідність до нього визначення кібертероризму у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»;

– передбачити необхідні заходи протидії кібертероризму при підготовці нової редакції Концепції боротьби з тероризмом в Україні;

– внести зміни до розділу XVI Кримінального кодексу України в частині доповнення нормою про кримінальну відповідальність за кібернетичний терористичний акт, яка б дозволила розмежувати поняття кібертероризму та кіберзлочинності;

– вдосконалити нормативно-правове регулювання порядку залучення правоохоронних органів до діяльності з попередження, виявлення та припинення актів кібертероризму;

2) *організаційні*, спрямовані на вдосконалення національної системи кібербезпеки:

– гарантувати кіберстійкість і кібербезпеку національної інформаційної інфраструктури в умовах цифрової трансформації як основне завдання подальшого розвитку системи кібербезпеки України;

– створити національну систему управління кіберінцидентами, для реагування на які упровадити необхідні операційні процедури з метою оцінки критичності подій та пріоритетності такого реагування;

– упровадити ризик-орієнтований підхід щодо забезпечення кібербезпеки ОКІ, розробити методику ідентифікації та оцінки кіберризиків для критичної інфраструктури держави;

– упровадити на ОКІ обов'язковий аудит інформаційної безпеки, сформувати методики та основні алгоритми його проведення;

– впровадити універсальну систему індикаторів кіберзагроз, засновану на міжнародних стандартах з питань кібербезпеки та кіберзахисту;

– поглибити державно-приватну взаємодію в запобіганні кібератакам і кіберінцидентам на ОКІ, реагуванні на них, усуненні їх наслідків в умовах кризових ситуацій, надзвичайного й воєнного стану;

3) *режимні, контррозвідувальні та оперативно-розшукові*, спрямовані на зниження кіберзагроз терористичного характеру:

– запровадити загальнодержавну систему виявлення й нейтралізації кібератак, протидії проявам кібертероризму на ОКІ;

– удосконалити наявну систему контррозвідувального забезпечення кібербезпеки держави, призначену для протидії кіберзагрозам;

– посилити моніторинг контенту в мережі Інтернет (соціальні мережі, блоги, форуми та сервіси) та запроваджувати у практику новітні технологічні рішення, що надають доступ до інформації, яка циркулює в мережі;

– забезпечувати постійне виявлення, запобігання та припинення актів кібертероризму, усунення їх причин і умов;

– нарощувати спроможності уповноважених органів у проведенні негласних перевірок стану готовності ОКІ до кібератак/кіберінцидентів;

– покращувати взаємодію уповноважених державних органів (Служби безпеки України, Національної поліції України, Державної служби спеціального зв'язку та захисту інформації України) між собою та з відповідними компетентними органами іноземних держав, співпрацю з міжнародними організаціями, що протидіють тероризму в усіх його проявах (насамперед з Інтерполом та Європолом).

Висновки

Зважаючи на відсутність чіткого юридичного визначення кібертероризму, важливим є належне унормування його поняття. Цей вид тероризму слід розглядати як суспільно небезпечну політично мотивовану діяльність у формі вчинення кібератак на комп'ютерні системи/мережі та/або на інформацію, що обробляється (циркулює) у них, спрямовану на порушення роботи критичної інформаційної інфраструктури держави та створення при цьому небезпеки для здоров'я й життя людей чи спричинення інших тяжких наслідків, якщо такі дії були вчинені з терористичною метою, або використання кіберпростору для інших цілей, безпосередньо не пов'язаних зі здійсненням терактів. За наявності в українському законодавстві норм про кримінальну відповідальність за терористичний акт та кіберзлочини наразі відсутня окрема норма про відповідальність за кібертеракт.

Доповнення Кримінального кодексу України нормою про кримінальну відповідальність за вчинення акту кібертероризму сприятиме покращенню протидії цьому різновиду тероризму в Україні.

Поширення кіберзагроз на всі сфери життєдіяльності держави й суспільства, пов'язані з функціонуванням критичної інформаційної інфраструктури, та постійне вдосконалення інструментів їх реалізації зумовлюють необхідність зміни підходів у протидії кібертероризму під час повномасштабної військової агресії рф проти України. Потребують перегляду загальні засади забезпечення безпеки критичної інформаційної інфраструктури України від актів кібертероризму.

Список бібліографічних посилань: 1. Беляков К. І., Цимбалюк В. С. Інформаційні технології як чинник терористичного акту. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2003. № 8. С. 90–97. **2.** Минин Т. До халифата – семь шагов. *«2000».* 20.10.2005. С. А3. **3.** Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с. **4.** Baranetsky V. What is cyberterrorism? Even experts can't agree // Harvard Law Record : сайт. 05.11.2009. URL: https://web.archive.org/web/20091112093639/http://www.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186 (дата звернення: 22.08.2023). **5.** Collin B. The Future of Cyberterrorism. *Crime & Justice International Journal.* 1997. Vol. 13. Pp. 51–71. **6.** Gable K. A. Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law.* 2021. Vol. 43, No. 1. Pp. 57–118. **7.** Паливода В. О. Національна стратегія протидії внутрішньому тероризму Сполучених Штатів Америки. Київ, 2021. 5 с. URL: https://niss.gov.ua/sites/default/files/2021-07/usa-national-strategy.pdf (дата звернення: 22.08.2023). **8.** Anderson K. Virtual Hostage: Cyberterrorism and politically motivated computer crime // The Prague Post : сайт. 13.10.2010. URL: http://www.praguepost.com/opinion/5996-virtual-hostage.html (дата звернення: 22.08.2023). **9.** Климчук О. О., Кравченко Р. М. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів. *Інформаційна безпека людини, суспільства, держави.* 2010. № 1 (3). С. 26–30. **10.** Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КИТ, 2010. 408 с. **11.** Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка.* 2011. Вип. 30. С. 159–165. **12.** Пилипчук В. Г., Дзьобань О. П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічна пріоритети.* 2011. № 4 (21). С. 12–17. **13.** Довгань О. Д., Хлань В. Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави.* 2011. № 3 (7). С. 49–53. **14.** Голубев В. Электронный терроризм –

новое лицо терроризма. *Компьютерная преступность и кибертерроризм.* 2004. Вып. 1. С. 49–56. **15.** Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації.* 2013. № 2 (19). С. 118–129. **16.** Тропина Т. Л. Киберпреступность и кибертерроризм. *Компьютерная преступность и кибертерроризм.* 2004. Вып. 1. С. 76–81. **17.** Брижко В. М., Швець М. Я. Е-боротьба в інформаційних війнах та інформаційне право : монографія / за ред. М. Я. Швеця. Київ : НДЦПІ Акад. прав. наук України, 2007. 236 с. **18.** Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001 г.: оценка угроз и предложения по их нейтрализации. Компьютерная преступность и кибертерроризм. 2004. Вып. 1. С. 56–75. **19.** Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». Станом на 1 січня 2019 року / за ред. М. В. Гребенюка. Київ : Нац. акад. прокуратури України, 2019. 220 с. **20.** Резнікова О. О., Місюра А. О., Войтовський К. Є. Міжнародний тероризм: загрози для України. Аналітична записка. Київ, 2020. 32 с. **21.** Голубев В. А. Кибертерроризм – угроза национальной безопасности и интересам Украины. *Юридичний журнал.* 2004. № 1. С. 132–134. **22.** Бутузов В. М., Тітуніна К. В. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2007. № 17. С. 316–324. **23.** Мельник Д. С. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України // Актуальні проблеми управління інформаційною безпекою держави : матеріали IX Всеукр. наук.-практ. конф. (м. Київ, 30 берез. 2018 р.) / МОН України, Ін-т модерн. змісту освіти, М-во інформ. політики України, Нац. акад. СБУ, НДІ інформатики і права НАПрН України. Київ : Нац. акад. СБУ, 2018. С. 114–116.

Надійшла до редколегії 24.08.2023

Прийнята до опублікування 21.09.2023

Melnyk D. S. Cyberterrorism: content, forms and promising countermeasures

The purpose of the study is to clarify the concept of cyber terrorism, its typical features and main forms, and to develop proposals for improving the system of countermeasures. The article highlights modern approaches to defining the content of cyber terrorism and its social and legal nature. This type of terrorism should be regarded as a socially dangerous politically motivated activity aimed at disrupting the critical information infrastructure of the State and thus creating a danger to human life and health or causing other serious consequences, provided that such actions were committed for terrorist purposes, or using cyberspace for other purposes of terrorist activities not directly related to terrorist acts.

Typical features of cyber terrorism are described and a definition of its concept is proposed. The main forms of cyber terrorism are revealed: the commission of terrorist acts by organisations, groups and individuals using computers and computer networks or by influencing the

information processed (circulated) in them, as well as the use of cyberspace for other purposes of terrorist activities not directly related to the commission of terrorist acts.

The counteraction system may be based on the following: proper regulation of the concept of cyber terrorism in national legislation, criminalisation of acts of cyber terrorism and its components; enhancing the security and protection of critical information infrastructure; improving existing and applying new counteraction methods; improving cooperation in the field of combating cyber terrorism.

Key words: cyber terrorism, computer systems and networks, cyberspace, countermeasures.