УДК 343.32

Ю. І. Когут
генеральний директор ТОВ «Консалтингова компанія «СІДКОН»,
голова правління ГО «Міжнародна ліга кібербезпеки»,
здобувач Навчально-наукового інституту права імені князя Володимира Великого
Міжрегіональної Академії управління персоналом

ГЕНЕЗА НАУКОВОЇ ДУМКИ ЩОДО НАПРЯМКІВ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В УКРАЇНІ

Постановка проблеми та її актуальність. Глобалізація інформаційних процесів, підвищення рівня залежності критичної інфраструктури держав від новітніх технологій, широкомасштабне використання інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання у світі, відкритість Інтернету спровокували появу такого суспільно небезпечного протиправного явища, як кібертероризм. Кібертероризм поступово приходить на заміну традиційним формам терористичної діяльності. На жаль, провідні держави світу, незважаючи на розвиненість правової та технічної регламентації захисту від несанкціонованого впливу у діяльність інфраструктури інформаційних технологій (IT-інфраструктури), не в змозі забезпечити її стовідсотковий захист від кібертерористичних атак.

На сьогоднішній день вчені приділяють значну увагу розгляду заходів з протидії кіберзлочинності, у тому числі кібертероризму, разом із тим багато питань понятійно-категоріального апарату протидії кібертероризму залишаються недостатньо відпрацьованими з позицій юридичних наук. Серед науковців і практиків немає єдності в термінологічному позначенні кібернетичної терористичної діяльності – кібертероризму [4, с. 61]. На міжнародному рівні також не існує єдиного визначення кібертероризму, суперечливими є і методики до розуміння його сутності та способів протидії йому у різних зарубіжних країнах.

Щодо міжнародного трактування цього поняття, то навіть у Міжнародній конвенції про боротьбу з фінансуванням тероризму та Міжнародній конвенції про боротьбу з актами ядерного тероризму не міститься уніфікованого визначення кібертероризму [4, с. 62].

Аналіз останніх досліджень і публікацій. Теоретичну основу методик протидії кіберзлочинності, у тому числі кібертероризму, становлять фундаментальні методологічні напрацювання таких учених з цих питань, як: В. А. Ліпкана, В. А. Мазурова, В. М. Бутузова, І. В. Діордіца, В. В. Топчія, Г. В. Форос, А. В. Фороса, В. К. Грищука, В. Л. Бурячка, В. Б. Толубка, В. О. Хорошка, С. В. Толюпу, О. Д. Довганя, І. М. Дороніна, С. О. Гнатюка, С. Б. Гавриша, М. В. Гуцалюка, А. І. Марущака, С. Г. Петрова тощо.

Поняття «комп'ютерний тероризм», «кібертероризм», «інформаційний тероризм» достатньо давно використовують у засобах масової інформації та наукових публікаціях. При цьому, незважаючи на це, термін «кібертероризм» вже довгий час має різноманітне трактування щодо своїх кваліфікуючих ознак. Крім того, в українській і зарубіжній науковій літературі, пов'язаній з дослідженням кібертероризму, наявні різні наукові думки щодо напрямків протидії цьому суспільно небезпечному протиправному діянню.

Не заперечуючи вагомого внеску вказаних науковців, слід констатувати, що сьогодні в Україні бракує окремого наукового дослідження, присвяченого узагальненню наукових праць видатних вчених з питань розробки методик протидії кіберзлочинності, у тому числі кібертероризму, з подальшим удосконаленням наявних заходів боротьби з цим суспільно небезпечним діянням.

Мета цієї статті полягає у розкритті низки теоретико-методологічних засад протидії кібертероризму як загрозі інформаційній безпеці, а саме розгляді генезу наукової думки, загальних теоретичних підходів щодо напрямків протидії кібертероризму в Україні.

Виклад основного матеріалу. Серед здобутків перших на початку 2000-х років наукових досліджень, присвячених проблемі протидії кібертероризму, особливо слід виділити розгорнутий розгляд природи та особливостей цього поняття, зроблений низкою вчених, серед яких особо виділяються наукові праці В. М. Бутузова [2; 1]. В осторонь В. М. Бутузова не залишились й питання розробки шляхів протидії кібертероризму, який він асоціює з комп'ютерним тероризмом, хоча, водночас, й наголошує, що тактика і прийоми, що використовуються при вчиненні кібертероризму, відрізняються від тактики і прийомів вчинення класичних комп'ютерних злочинів тим, що комп'ютерний терористичний акт повинен мати небезпечні наслідки та стати широко відомим населенню й одержати великий суспільний резонанс [2, с. 319].

До шляхів подолання кібертероризму В. М. Бутузов відносить превентивні заходи для недопущення його становлення, що зумовлює, на думку автора, необхідність невідкладного вирішення цієї проблеми, а основою забезпечення боротьби

з кібертероризмом вважає створення ефективної системи заходів із запобігання, виявлення та припинення такого виду діяльності [2, с. 321].

Цікаві доробки щодо шляхів протидії кібертероризму (комп'ютерному тероризму) на початку 2000-х рр. представив науковій спільноті С. Б. Гавриш [3]. Автор прогнозує у подальшому бурхливий розвиток комп'ютерного тероризму в Україні та надає деякі пропозиції щодо ефективної протидії цьому явищу. Зокрема, С. Б. Гавриш обґрунтовує, що протидія проявам комп'ютерного тероризму вимагає комплексного підходу, що поєднує силові, політико-дипломатичні, економічні й гуманітарні форми та методи дій, а також ефективного поєднання антитерористичних заходів, що вживаються як на національному, так і на міжнародному рівнях [3].

Водночас, С. Б. Гавриш безпідставно вважає, що «загроза кібертероризму, про яку говорять багато урядових органів і спецслужби, сьогодні переоцінюється» [3]. Зокрема, він непереконливо стверджує, що інфраструктури в індустріальних країнах стійкі до проявів кібертероризму [3]. Цей автор навіть доходить помилкового, з врахуванням багаточисельних прикладів вчинення кібертерористичних актів сьогодення, висновку, що «в контексті макроекономіки збої в системах електропостачання, збої у функціонуванні транспортного руху та інші «сценарії» кібертерору – стандартні події, які не стосуються національної безпеки» [3]. Він підкреслює, що «для національної економіки, де десятки або навіть сотні систем забезпечують найважливіші інфраструктури, збій у системах унаслідок кібератаки може залишитись непоміченим у повсякденному житті або бути віднесеним до стандартних затримок та виходу з ладу обладнання» [3]. При цьому С. Б. Гавриш не заперечує руйнівний характер інформаційного аспекту кібертероризму.

Послідовники наукових ідей С. Б. Гавриша – Т. В. Смачило, А. Р. Кривцун [7, с. 126], у свою чергу, виокремлюють наступні завдання, які в комплексному застосуванні допоможуть створити суттєвий кіберзахист для держави від проявів кібертероризму: постійний моніторинг кіберпростору на випадок потенційної кібертерористичної загрози; захист елементів вітчизняної критичної інфраструктури; створення та оновлення програмного забезпечення, яке зможе захистити кіберпростір держави; усунення прогалин у законодавстві держави; боротьба з неліцензованим програмним забезпеченням; створення системи, яка забезпечить загальнодержавний захист інформації. При цьому головним методом боротьби з кібертероризмом ці автори називають підтримку новітніх інформаційних технологій та стимули для науково-технічного прогресу всередині держави, що допоможе запобігти кібертероризму.

Наукові погляди С. Б. Гавриша розділяють низка інших вчених. Так, як зазначають сучасні дослідники поняття кібертероризму О. Д. Довгань, І. М. Доронін, які узагальнили різні наукові методики до вирішення проблеми протидії кібертероризму, боротьба з цим явищем має проваджуватися комплексно та мати такі складові [5, с. 37]:

- правову – пов'язана з розробленням нормативно-правових актів, які регламентують відносини в інформаційній сфері, і нормативно-методичних документів із питань забезпечення інформаційної безпеки;
- організаційну – полягає в удосконаленні організаційної структури державних і комерційних підприємств, сертифікації і стандартизації засобів захисту інформації та ліцензуванні діяльності у сфері захисту інформації;
- психологічну – передбачає формування морально-етичних норм у співробітників, які працюють з інформаційними системами, що забезпечують критичну інфраструктуру держави;
- технічну – ґрунтується на створенні і постійному вдосконаленні системи забезпечення інформаційної безпеки на об'єктах інформатизації та попередження нападу.

Боротьба з кібертероризмом повинна проводитися шляхом застосування узгоджених заходів, а не окремо [4, с. 66]. Кібертероризм може завдавати шкоди не лише інформації, а й безпеці держави загалом.

Отже, головною зброєю у боротьбі з кібертероризмом є законодавство. До інших необхідних заходів з протидії кібертероризму, як вважає С. О. Гнатюк, можна віднести: проведення кібернавчань, створення загонів кібервійськ тощо [12, с. 126].

Ми згодні з С. О. Гнатюком [12, с. 126-127], що доцільно створити систему (мережу) центрів реагування на кіберінциденти CERT, яка буде включати як загальнодержавні, так і локальні та галузеві центри, адже на сьогодні Україна має на своїй території тільки один такий центр, а для найбільшої за територією європейської країни це критично мало.

Одним із дієвих шляхів протидії кібертероризму, виходячи з низки наукових праць, є підвищення кваліфікаційного рівня осіб, які обслуговують об'єкти критичної інфраструктури, щодо здатності протидіяти кібератакам. Багато випадків ураження об'єктів критичної інфраструктури відбулися через відсутність належним чином підготовлених до масштабних кібератак професійних кадрів.

Однак переважно усі вчені, які займаються питаннями протидії кібертероризму, переконані у важливості здійснення комплексного підходу на загальнодержавному рівні до організації протидії актуальним кіберзагрозам, що, в першу чергу, має передбачати підвищення кібербезпекових

спроможностей держави та розбудову ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки України [8].

При цьому, як вважає І. В. Діордіца [4, с. 65], В. В. Топчій [9], основою забезпечення боротьби з кібертероризмом є створення ефективної системи заходів із запобігання, виявлення та припинення такого виду злочинності. На думку В. В. Топчія [9], найбільш дієвим напрямом у вирішенні комплексної проблеми протидії кіберзлочинності, у тому числі кібертероризму, в наш час є міжнародне співробітництво правоохоронних органів у сфері інформаційної безпеки на основі узгодження національного та міжнародного законодавства.

Висновки. Узагальнюючи доробки наукових праць видатних вчених у сфері протидії кібертероризму, слід наголосити на таких висновках щодо основних напрямків подолання та нейтралізації цього суспільно небезпечного протиправного явища:

• протидія проявам кібертероризму вимагає подальшого удосконалення законодавства у цій галузі; створення ефективної системи заходів із запобігання, виявлення та припинення такого виду діяльності, а також запровадження комплексного підходу, що поєднує силові, політико-дипломатичні, економічні й гуманітарні форми та методи дій, а також ефективного поєднання антитерористичних заходів, що вживаються як на національному, так і на міжнародному рівнях;

• слід здійснювати систематизацію та гармонізацію національного законодавства та міжнародних актів щодо запобігання кібертероризму; проводити наукові розробки в галузі створення сучасних технологій виявлення та запобігання терористичним впливам на інформаційні ресурси; удосконалювати міжнародну організаційно-правову взаємодію з питань протидії кібертероризму; удосконалювати багаторівневу систему підготовки кадрів у сфері кібербезпеки зі створенням так званих кіберполігонів; налагоджувати ефективну систему координації взаємодії спеціалізованих підрозділів у сфері боротьби з кібертероризмом;

• масштабне завдання із протидії кібертероризму вимагає багато часу та істотних фінансових витрат.

Як результат вивчення здобутків вчених у сфері забезпечення кібербезпеки та протидії кібертероризму нами виокремлені наступні завдання, які в комплексному застосуванні допоможуть створити суттєвий кіберзахист для держави від проявів кібертероризму:

• постійний моніторинг кіберпростору на випадок потенційної кібертерористичної загрози;

• надійний захист елементів вітчизняної критичної інфраструктури;

• розробка проекту Закону України «Про забезпечення безпеки об'єктів критичної інфраструктури»;

• створення та оновлення програмного забезпечення, яке зможе захистити кіберпростір держави, підтримка новітніх інформаційних технологій, стимулювання і підтримка фундаментальних та прикладних наукових досліджень у галузі, створення сучасних технологій виявлення та запобігання несанкціонованим кібератакам;

• створення спеціалізованих підрозділів щодо боротьби з кібертероризмом із ефективною системою координації їх взаємодії, забезпечення їх найсучаснішою матеріально-технічною базою;

• чіткий та прозорий розподіл обов'язків спеціальних державних інституцій щодо захисту кіберпростору держави;

• мінімізація відсотку застосування програмних та апаратних засобів іноземного виробництва, стимулювання створення власних операційних систем, антивірусних комплексів, телекомунікаційного обладнання (особливо це стосується об'єктів критичної інформаційної інфраструктури держави);

• встановлення кримінальної відповідальності за кібертероризм;

• прийняття єдиного, консолідуючого законодавчого акта з питань протидії кіберзлочинності – Закону України «Про забезпечення протидії кіберзлочинності»;

• детальна розробка механізму реалізації національної системи кібербезпеки, в якому в контексті реалізації державної кібербезпекової стратегії мають бути визначені мета, час, місце, завдання, функції та відповідальні за її виконання;

• налагодження взаємоузгодженої роботи та міжвідомчої взаємодії складових єдиної сучасної системи ситуаційних центрів державних органів з метою створення ефективного механізму протидії кібертероризму;

• створення єдиного процесуального законодавства з питань боротьби з кіберзлочинністю, кібертероризмом та запобігання загрозі кібервійни.

Література

1. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. К.: КИТ, 2010. 145 с.

2. Бутузов В. М., Тітуніна К. В. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2007. Вип. 17. С. 316–324.

3. Гавриш С. Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2009. №20.

4. Діордіца І. В. Поняття і зміст кібертероризму. *Прикарпатський юридичний вісник.* 2016. Вип. 3 (12). С. 61–68.

5. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / НАПрН України, НДІІП. К. : Видавничий дім «АртЕк». 2017. 107 с.

6. Смачило Т. В., Кривцун А. Р. Феномен інформаційного тероризму як загрози міжнародній безпеці. *Молодий вчений.* 2017. №11 (51). С. 124–127.

7. Ткачук Н. А. Актуальні кіберзагрози сучасного безпекового середовища. *Міжнародний науковий журнал «Інтернаука». Серія: Юридичні науки.* 2018. № 7. URL: https://www.inter-nauka.com/uploads/public/15381330973208.pdf.

8. Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки.* 2015. Вип. 6(3). С. 65–68.

9. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security.* 2013. № 19/2. С. 118–129.

Анотація

Когут Ю. І. **Генеза наукової думки щодо напрямків протидії кібертероризму в Україні.** – Стаття.

У статті здійснено узагальнення доробок наукових праць вчених у сфері протидії кібертероризму щодо основних напрямків подолання та нейтралізації цього суспільно небезпечного протиправного явища. В результаті з'ясовано, що переважно усі вчені, які займаються питаннями протидії кібертероризму, переконані у важливості здійснення комплексного підходу на загальнодержавному рівні до організації протидії актуальним кіберзагрозам, що, в першу чергу, має передбачати підвищення кібербезпекових спроможностей держави та розбудову ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки України. Поряд з цим, переважна більшість вчених наголошує на необхідності подальшого удосконалення законодавства з метою протидії проявам кібертероризму; здійснення систематизації та гармонізації національного законодавства та міжнародних актів щодо запобігання кібертероризму; проведення наукових розробок в галузі створення сучасних технологій виявлення та запобігання терористичним впливам на інформаційні ресурси; удосконалення міжнародної організаційно-правової взаємодії з питань протидії кібертероризму; удосконалення багаторівневої системи підготовки кадрів у сфері кібербезпеки зі створенням так званих кіберполігонів. Як результат вивчення цих праць виокремлені такі завдання, які в комплексному застосуванні допоможуть створити суттєвий кіберзахист для держави від проявів кібертероризму: постійний моніторинг кіберпростору на випадок потенційної кібертерористичної загрози; надійний захист елементів вітчизняної критичної інфраструктури; розробка проекту Закону України «Про забезпечення безпеки об'єктів критичної інфраструктури»; чіткий та прозорий розподіл обов'язків спеціальних державних інституцій щодо захисту кіберпростору держави; встановлення кримінальної відповідальності за кібертероризм; прийняття єдиного, консолідуючого законодавчого акту з питань протидії кібертероризму – Закону України «Про забезпечення протидії кібертероризму»; створення єдиного процесуального законодавства з питань боротьби з кіберзлочинністю, кібертероризмом та запобігання загрозі кібервійни.

Ключові слова: кібертероризм, кібербезпека, кіберзагроза, кібервійна, кібератаки, кіберпростір, кіберзахист, критична інфраструктура, національна система кібербезпеки, кіберзлочинність, кібервійська, кіберінцидент.

Аннотация

Когут Ю. И. **Генезис научной мысли относительно направлений противодействия кибертерроризма в Украине.** – Статья.

В статье осуществлено обобщенный доработок научных трудов ученых в сфере противодействия кибертерроризма по основным направлениям преодоления и нейтрализации этого общественно опасного противоправного явления. В результате установлено, что в основном все ученые, занимающиеся вопросами противодействия кибертерроризма, убеждены в важности осуществления комплексного подхода на общегосударственном уровне в организации противодействия актуальным киберугрозам, что, в первую очередь, должен предусматривать повышение кибербезпековых возможностей государства и развитие эффективных механизмов взаимодействия основных субъектов национальной системы кибербезопасности Украины. Наряду с этим, подавляющее большинство ученых подчеркивает необходимость дальнейшего совершенствования законодательства в целях противодействия проявлениям кибертерроризма; осуществления систематизации и гармонизации национального законодательства и международных актов по предотвращению кибертерроризма; проведение научных разработок в области создания современных технологий обнаружения и предотвращения террористических воздействиям на информационные ресурсы; совершенствование международной организационно-правового взаимодействия по вопросам противодействия кибертерроризма; совершенствование многоуровневой системы подготовки кадров в сфере кибербезопасности с созданием так называемых киберполигонов. В результате изучения этих работ выделены такие задачи, которые в комплексном применении помогут создать существенную киберзащиту для государства от проявлений кибертерроризма: постоянный мониторинг киберпространства в случае потенциальной кибертеррористической угрозы; надежную защиту элементов отечественной критической инфраструктуры; разработка проекта Закона Украины «Об обеспечении безопасности объектов критической инфраструктуры»; четкое и прозрачное распределение обязанностей специальных государственных институтов по защите киберпространства государства; установление уголовной ответственности за кибертерроризм; принятие единого, консолидирующего законодательного акта по вопросам противодействия кибертерроризма – Закона Украины «Об обеспечении противодействия кибертерроризма»; создание единого процессуального законодательства по борьбе с киберпреступностью, кибертерроризмом и угрозы кибервойны.

Ключевые слова: кибертерроризм, кибербезопасность, киберугрозы, кибервойна, кибератаки, киберпространство, киберзащита, критическая инфраструктура, национальная система кибербезопасности, киберпреступности, кибервойска, киберинцидент.

Summary

Kohut Yu. I. **Genesis of scientific thought in areas countering cyberterrorism in Ukraine.** – Article.

The article summarizes the achievements of scientific works of scientists in the field of combating cyberterrorism on the main directions of overcoming and neutralizing this socially dangerous illegal phenomenon. As a result, it was found that mostly all scientists involved in combating cyberterrorism are convinced of the importance of a comprehensive approach at the national level to countering current cyber threats, which should primarily

increase the state's cybersecurity capabilities and develop effective mechanisms for cooperation subjects of the national cybersecurity system of Ukraine. At the same time, the vast majority of scholars emphasize the need to further improve legislation to combat cyberterrorism; systematization and harmonization of national legislation and international acts on the prevention of cyberterrorism; carrying out scientific developments in the field of creation of modern technologies of detection and prevention of terrorist influences on information resources; improving international organizational and legal cooperation on combating cyberterrorism; improvement of the multilevel system of training in the field of cybersecurity with the creation of so-called cyberfields. As a result of studying these works, the following tasks have been singled out, which in complex application will help to create significant cyber defense for the state from the manifestations of cyberterrorism: constant monitoring of cyberspace in case of a potential cyberterrorist threat; reliable protection of elements of domestic critical infrastructure; development of the draft Law of Ukraine "On ensuring the safety of critical infrastructure facilities"; clear and transparent division of responsibilities of special state institutions for the protection of state cyberspace; establishing criminal liability for cyberterrorism; adoption of a single, consolidating legislative act on combating cyberterrorism - the Law of Ukraine "On Countering Cyberterrorism"; creation of unified procedural legislation on combating cybercrime, cyberterrorism and preventing the threat of cyberwar.

Key words: cyberterrorism, cybersecurity, cyber threat, cyberwar, cyber attacks, cyberspace, cyber defense, critical infrastructure, national cybersecurity system, cybercrime, cyber warfare, cyber incident.