УДК 343.32
DOI https://doi.org/10.32849/2663-5313/2020.12.29

Юрій Когут,
здобувач
Навчально-наукового інституту права імені князя Володимира Великого
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»,
генеральний директор
ТОВ «Консалтингова компанія «СІДКОН»

ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ ТА РОЗВИТКУ ДЕРЖАВНОЇ СИСТЕМИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В УКРАЇНІ

У статті проаналізовані законодавчі та інші нормативно-правові акти, які врегульовують протидію кібертероризму в Україні. У межах розгляду правових засад формування та розвитку державної системи протидії кібертероризму в Україні як загрозі інформаційній безпеці автор підтримує і розвиває думку, що сучасне законодавство з кібербезпеки України не має чіткої, ієрархічної побудови, єдності, комплексності, що спричиняє суперечливе тлумачення та застосування його норм на практиці, зокрема, через те, що окремі цілісні проблеми вирішуються в різних нормативних актах фрагментарно і без узгодження між собою. Зокрема, автором визначено, що у Законі України «Про основні засади забезпечення кібербезпеки України» не надані дефініції багатьох ключових термінів, які вживаються у сфері протидії кібертероризму («інформаційний тероризм», «комп'ютерний тероризм», «віртуальний тероризм»), що слід усунути. Поряд із цим також встановлено, що визначення, по суті, головним органом національної системи кібербезпеки Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку) зумовило виникнення низки проблемних питань у правозастосуванні Закону України «Про основні засади забезпечення кібербезпеки України», до яких, зокрема, належать насамперед особливості статусу Держспецзв'язку, який попри те, що не є міністерством, формує та реалізує державну політику у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій тощо. Крім того, у статті доведено, що правовий статус CERT-UA (урядової команди реагування на комп'ютерні надзвичайні події України) та Державного центру кіберзахисту також законодавчо не визначений. Водночас автором обґрунтовано, що робочий орган РНБОУ – Національний координаційний центр кібербезпеки, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, що забезпечують кібербезпеку, повинен мати функції управління, а не лише функції координації, які мають здійснюватися на основі інформації про кібератаки зі всіх ресурсів у режимі real-time чи близькому для нього.

Ключові слова: кібертероризм, кібербезпека, стратегія кібербезпеки, національна система кібербезпеки, кіберзахист, кіберзлочини, кіберінциденти, кіберпростір, кібератаки.

Постановка проблеми. Інформаційні відносини, пов'язані із забезпеченням кібернетичної безпеки та розвитку державної системи протидії кібертероризму в Україні, натепер урегульовані законами України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про державну таємницю», «Про науково-технічну інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України», «Про боротьбу з тероризмом» та Указами Президента України «Про Доктрину інформаційної безпеки України», «Про Стратегію кібербезпеки України», «Про Концепцію боротьби з тероризмом в Україні», «Про Стратегію національної безпеки України», «Воєнна Доктрина України». Водночас у межах даної проблематики діють три стратегічні документи – «Стратегія кібербезпеки України», «Доктрина інформаційної безпеки України» та Закон України «Про основні засади забезпечення кібербезпеки України». Крім того, 07.09.2005 р. Верховною Радою України ратифікована Конвенція Ради Європи про кіберзлочинність (Будапештська Конвенція) [9], яка є першим і найбільш визнаним міжнародно-правовим документом у сфері боротьби з міжнародною і національною кіберзлочинністю, у тому числі кібертероризмом. Однак Україна ратифікувала цю Конвенцію, щоправда, не в повному обсязі – із заявами і застереженнями. Наприклад, в українське законодавство не імплементовані положення цієї Конвенції щодо Процедурного права. Можливо, не в останню чергу це пояснюється низькою якістю офіційного українського перекладу Конвенції, розміщеного на сайті Верховної Ради України [4, с. 7].

Аналіз публікацій, у яких започатковано розв'язання задекларованої проблематики. Аналіз генези наукової думки щодо розуміння поняття «кібертероризм» та напрямів протидії кібертероризму в Україні дозволило виділити низку вчених-правознавців, які вивчали правові засади забезпечення кібербезпеки держави: В. М. Бутузова, В. А. Васенина, В. А. Голубєва, І. В. Діордіца, В. В. Топчія, Г. В. Форос, А. В. Фороса, К. Л. Бугайчука, Г. М. Шорохову, М. А. Ожевана, В. К. Грищука, В. Л. Бурячка, В. Б. Толубка, В. О. Хорошка, С. В. Толюпу, О. Д. Довганя, І. М. Дороніна, О. І. Жайворонка, А. В. Турчак, Т. Ю. Ткачука, О. В. Бойченка, С. О. Гнатюка, В. В. Мохора, С. Б. Гавриша, М. В. Гуцалюка тощо. Однак, незважаючи на чималу увагу цих правознавців до досліджуваної проблематики, виняткового значення для забезпечення кібербезпеки України набуває наукове обґрунтування перспективних напрямів удосконалення захисту інформаційного простору України від загроз кібертероризму на основі удосконалення законодавчих та інших нормативно-правових актів, які врегульовують протидію кібертероризму в Україні.

Мета статті полягає у здійсненні аналізу правових засад формування та розвитку державної системи протидії кібертероризму в Україні як загрозі інформаційній безпеці та формулюванні пропозицій щодо їх вдосконалення.

Виклад основного матеріалу. Розвиток вітчизняного законодавства у сфері забезпечення кібербезпеки відбувався поступово, з урахуванням документів міжнародно-правового характеру та стратегій кібербезпеки зарубіжних країн.

Початок формування та розвитку державної системи протидії кібертероризму в Україні був покладений у 2011 р. рішенням РНБОУ «Про виклики та загрози національній безпеці України у 2011 році», яке було введено в дію Указом Президента від 10.12.2010 р. № 1119/2010 (натепер втратило чинність) та яким передбачалось розроблення за участю СБУ пропозицій щодо створення єдиної загальнодержавної системи протидії кіберзлочинності, а також переліку об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак.

Важливим кроком у процесі протидії проявам кібертероризму слід вважати Указ Президента України від 15.03.2016 р. № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [10]. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Саме цією Стратегією з метою розвитку потенціалу сектору безпеки і оборони у сфері боротьби з кібертероризмом передбачається необхідність «підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі» [10].

Однак найбільш вагомим нормативно-правовим актом, який фактично заклав засади формування та розвитку державної системи протидії кібертероризму в Україні, став Закон України «Про основні засади забезпечення кібербезпеки України» [8], який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Цей Закон є комплексним спеціальним законодавчим актом у сфері забезпечення кібербезпеки [2, с. 103].

Закон України «Про основні засади забезпечення кібербезпеки України» [8] є важливим кроком на шляху створення національної системи кібербезпеки – одного з ключових завдань політики національної безпеки. Такий системоутворюючий (базовий) закон у сфері кібербезпеки зафіксував ключові терміни в цій сфері, визначив поняття критично важливих об'єктів інфраструктури, об'єктів критичної інформаційної інфраструктури та механізми захисту таких об'єктів, принцип побудови національної системи кібербезпеки та її складових елементів, повноваження і координацію дій суб'єктів забезпечення кібербезпеки.

Згідно з ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [8] національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Тобто у національну систему кібербезпеки одночасно входять і суб'єкти забезпечення кібербезпеки, і відповідні заходи.

Одним з основних суб'єктів національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку), у складі якої знаходиться Державний центр кіберзахисту – ДЦКЗ, який був створений 1 липня 2015 р. Його було створено на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв'язку [11].

Визначення, по суті, головним органом національної системи кібербезпеки Держспецзв'язку зумовило виникнення низки проблемних питань у правозастосуванні Закону України «Про основні засади забезпечення кібербезпеки України» [8]. До них належать насамперед особливості статусу Держспецзв'язку, що відповідно до ч. 1 ст. 2 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» є державним органом, який формує та реалізує державну політику у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку. Але згідно з вимогами ч. 1 ст. 1 Закону України «Про центральні органи виконавчої влади» формують державну політику тільки міністерства, а згадана Держспецзв'язку не належить до міністерств.

Вказаний вище Державний центр кіберзахисту (разом з урядовою командою CERT) має діяти за умови забезпечення його функціонування з боку Держспецзв'язку, при цьому їхні завдання хоча і визначені у Законі України «Про основні засади забезпечення кібербезпеки України» [8] (ст.ст. 8 і 9), але окремі повноваження цим органам не надані, отже, виконання завдань буде організовано з урахуванням повноважень, законодавчо наданих Держспецзв'язку, правовий статус якої з формування державної політики у певних сферах не повністю відповідає вимогам чинного законодавства [3, с. 64].

Серед завдань ДЦКЗ – забезпечення функціонування команди реагування на комп'ютерні надзвичайні події України CERT-UA, а також проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах органів державної влади. Крім того, ДЦКЗ відповідатиме за функціонування, безпеку та розвиток Національної системи конфіденційного зв'язку, функціонування та розвиток системи антивірусного захисту інформації для органів державної влади, національних інформаційних ресурсів, забезпечення функціонування та модернізації системи захищеного доступу державних органів до мережі Інтернет та Захищеного вузлу Інтернет-доступу Держспецзв'язку [11].

Відповідно до ч. 5 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [8] ДЦКЗ здійснює впровадження організаційно-технічної моделі кібербезпеки як складової частини національної системи кібербезпеки.

Водночас правовий статус ДЦКЗ не розкривається ні у Законі України «Про основні засади забезпечення кібербезпеки України» [11], ні у Законі України «Про державну службу спеціального зв'язку та захисту інформації України», ні у будь-якому іншому чинному нормативно-правовому акті, проте Державний центр кіберзахисту дійсно функціонує, як вже наголошувалось, з 2015 р. як структурний підрозділ Держспецзв'язку.

Нині Міністерство цифрової трансформації разом з Адміністрацією Держспецзв'язку готують Кабінету Міністрів пропозиції з реорганізації ДЦКЗ Держспецзв'язку. Передбачається, що Держспецзв'язку оптимізує свою організаційну структуру, позбудеться невластивих їй функцій та посилить кіберзахист об'єктів критичної інфраструктури. Додатково Держспецзв'язку координуватиме забезпечення кібербезпеки.

У свою чергу, CERT-UA – урядова команда реагування на комп'ютерні надзвичайні події України – спеціалізований структурний підрозділ Державного центру кіберзахисту, що функціонує в рамках Державної служби спеціального зв'язку та захисту інформації України. Проте це відомство може займатися тільки технічним припиненням кібератак. При цьому правовий статус CERT-UA, як й ДЦКЗ, також законодавчо не визначений.

Структурний підрозділ Держспецзв'язку – CERT-UA – створений, по суті, щоб запобігати кіберзлочинам, виявляти їх, збирати інформацію та інформувати про них [6, с. 160].

Відповідно до розділу 6 «Доктрини інформаційної безпеки України» та п. 1 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» [8] координація діяльності органів виконавчої влади у сфері кібербезпеки, зокрема, щодо забезпечення національної безпеки в інформаційній сфері здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України (РНБОУ). Як відомо, ці положення закону корелюються з вимогами ст. 3 Закону України «Про Раду національної безпеки і оборони України», де визначається, що до її функцій належить, окрім іншого, координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони.

Закон України «Про основні засади забезпечення кібербезпеки України» [8] визначає у ч. 2 ст. 5 робочим органом РНБОУ Національний координаційний центр кібербезпеки (НКЦК), який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, що забезпечують кібербезпеку, та який вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

НКЦК утворений у 2016 р. відповідно до рішення РНБОУ від 27.01.2016 р. «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15.03.2016 р. № 96 [10]. 7 червня 2016 р. Указом Президента України № 242/2016 було затверджено «Положення про Національний координаційний центр кібербезпеки» [7].

НКЦК відіграє вагому координуючу роль у національній системі кібербезпеки України. Зокрема, діяльність НКЦК дозволяє забезпечити координацію та контроль за діяльністю суб'єктів національної системи кібербезпеки під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у процесі формування та реалізації державної політики у сфері кібербезпеки. НКЦК вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Фактично фахівці НКЦК займаються аналітикою, аналізом кіберінцидентів, подій, про які звітують основні суб'єкти забезпечення кібербезпеки. Зараз НКЦК займається тим, щоб залучити до звітування кіберінцидентів й приватний сектор.

Отже, створення в Україні НКЦК було зумовлено саме необхідністю вирішення питання ефективної координації всіх суб'єктів, які діють у сфері кіберзахисту України.

Водночас НКЦК повинен мати функції управління, а не лише функції координації [5], які мають здійснюватися на основі інформації про кібератаки зі всіх ресурсів у режимі real-time чи близькому для нього.

Однак, незважаючи на формулювання концептуальних засад щодо особливостей функціонування національної системи кібербезпеки, досі не розроблені і не впроваджені суб'єктами забезпечення кібербезпеки в Україні дієві механізми обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків. Підрозділи кібербезпеки Збройних Сил України, інші утворені відповідно до законів України військові формування, правоохоронні органи спеціального призначення повинні узгоджувати та координувати розгортання заходів протидії кібертероризму.

Суб'єкти системи забезпечення кібербезпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції. У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють струнку організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією із забезпечення кібербезпеки [12].

Висновки

Отже, сучасне законодавство з кібербезпеки України не має чіткої, ієрархічної побудови, єдності, комплексності, це спричиняє суперечливе тлумачення та застосування його норм на практиці, зокрема, через те, що окремі цілісні проблеми вирішуються в різних нормативних актах фрагментарно і без узгодження між собою [1].

У Законі України «Про основні засади забезпечення кібербезпеки України» [8] нарешті надане визначення терміна «кібертероризм», адже багато років чинне законодавство оперувало зазначеним терміном без його офіційного визначення, тому вчені розуміли цю дефініцію кожний по-своєму. Водночас у цьому законі не надані визначення інших ключових термінів, які вживаються у сфері кібербезпеки. Зокрема, не зрозуміло, як співвідносяться між собою такі терміни, як «кібертероризм», «інформаційний тероризм», «комп'ютерний тероризм», «віртуальний тероризм».

Незважаючи на регулювання вищевказаними нормативно-правовими документами процесу забезпечення державної кібербезпеки, в Україні тільки формується правова база з боротьби з кібертероризмом. Потребує досконалого правового обґрунтування питання організації ефективного протистояння кібертероризму в умовах активізації глобальних викликів та впливів, нових інформаційних технологій [2, с. 105].

Список використаних джерел:

1. Бугайчук К. Л., Шорохова Г. М. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти. *Протидія терористичній діяльності: міжнародний досвід і його актуальність для України* : матеріали II Міжнар. наук.-практ. конф. (15 груд. 2017 р.). Київ, 2018. С. 135–138.
2. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ: Видавничий дім «АртЕк». 2017. 107 с.
3. Доронін І. М. Правові проблеми визначення компетенції суб'єктів забезпечення кібербезпеки України. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. С. 62–64. URL: http://academy.ssu.gov.ua/upload/file/aktualn_problemi_upravl_nnya_nformac_ycnoyu_bezpekoyu_derzhavi.pdf. (дата звернення: 02.11.2020).
4. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Policy Paper). USAID. 2017. 28 с.
5. Національний координаційний центр кібербезпеки посилює співпрацю із міжнародними виробниками кібер-технологій. URL: https://www.rnbo.gov.ua/ua/Diialnist/4658.html. (дата звернення: 02.11.2020).
6. Потерейко О. О. Віртуалізація держави: теоретико-методологічний аналіз : дис. ... канд. політич. наук: 23.00.01. Львів, 2019. 201 с.
7. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 р., № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text. (дата звернення: 02.11.2020).
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/main/2163-19#Text. (дата звернення: 02.11.2020).
9. Про ратифікацію Конвенції Ради Європи про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text. (дата звернення: 02.11.2020).
10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11. (дата звернення: 02.11.2020).
11. У Держспецзв'язку створено Державний центр кіберзахисту та протидії кіберзагрозам. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473. (дата звернення: 02.11.2020).
12. Шпачук В. В. Суб'єкти державного управління кібербезпекою країни: зарубіжний досвід. *Державне управління: удосконалення та розвиток.* 2019. № 2. URL: http://www.dy.nayka.com.ua/pdf/2_2019/7.pdf. (дата звернення: 02.11.2020).

Yurii Kohut. Legal fundamentals of the formation and development of the state system of cyber-security in Ukraine

The article analyzes the legislative and other regulations that regulate the fight against cyberterrorism in Ukraine. As part of the legal framework for the formation and development of the state system of combating cyberterrorism in Ukraine as a threat to information security, the author joins, supports and develops the view that modern cybersecurity legislation in Ukraine does not have a clear, hierarchical structure, unity, complexity, which causes conflicting interpretation and application. norms in practice, in particular due to the fact that individual holistic problems are solved in different regulations in fragments and without coordination with each other. In particular, the author states that the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" does not provide a definition of many key terms used in the field of combating cyberterrorism ("information terrorism", "computer terrorism", "virtual terrorism"), which should be eliminated. In addition, it was also established that the determination, in fact, the main body of the national cybersecurity system of the State Service for Special Communications and Information Protection (State Special Communications) led to a number of problematic issues in law enforcement of the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine". which, in particular, include, first of all, the peculiarities of the status of the State Special Communications, which, not being a ministry, but forms and implements state policy in the areas of cryptographic and technical protection of information, cyber security, telecommunications and more. In addition, the article proves that the legal status of CERT-UA (the government team for responding to computer emergencies in Ukraine) and the State Center for Cyber Security is also not legally defined. At the same time, the author substantiates that the working body of the National Security and Defense Council – the National Cyber Security Coordination Center, which coordinates and monitors the activities of security and defense sector entities that provide cybersecurity, should have management functions, not only information-based coordination functions. about cyberattacks from all resources in real-time mode or close to it.

Key words: cyberterrorism, cybersecurity, cybersecurity strategy, national cybersecurity system, cyber defense, cybercrime, cyber incidents, cyberspace, cyber attacks.