ПрАТ «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

КОГУТ ЮРІЙ ІВАНОВИЧ

УДК(043.3)343.32(477)=161.2

ПРОТИДІЯ КІБЕРТЕРОРИЗМУ ЯК ЗАГРОЗІ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

21.07.01 – забезпечення державної безпеки України

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана у ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом».

Науковий керівник – доктор юридичних наук, професор,
заслужений працівник освіти України
СТРЕЛЬБИЦЬКИЙ Микола Павлович,
Національна Академія СБУ, головний науковий співробітник науково-організаційного центру

Офіційні опоненти: доктор юридичних наук, професор,
заслужений юрист України
СКУЛИШ Євген Деонізійович,
Національна академія правових наук України, керівник науково-дослідного центру правового забезпечення інформаційної і національної безпеки науково-дослідного інституту інформатики і права.

доктор юридичних наук,
ПЕТРОВ Станіслав Геннадійович,
Департамент Служби зовнішньої розвідки України, заступник директора.

Захист відбудеться «30» березня 2021 р. об 11.00 годині на засіданні спеціалізованої вченої ради К 26.142.05 ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» за адресою: 03039, м. Київ, вул. Фрометівська, 2.

З дисертацією можна ознайомитись у Міжнародному бібліотечно-інформаційному центрі ім. Ярослава Мудрого ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» за адресою: 03039, м. Київ, вул. Фрометівська, 2.

Автореферат розіслано «26» лютого 2021 р.

Учений секретар
спеціалізованої вченої ради **Ю. П. Тимошенко**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Одним з головних чинників розвитку соціально-політичної системи будь-якої держави є підготовка і використання інформації. У сучасних умовах вона відіграє ключову роль у функціонуванні громадських і державних інститутів. Інформаційно-комунікаційні системи використовуються в усіх сферах діяльності держави. Це забезпечення національної безпеки, надання державних послуг у галузі охорони здоров'я, освіти, житлово-комунального господарства, управління аеро- і залізничним транспортом, водопостачання, енергетика, державне управління, торговельно-фінансова сфера тощо. Однак стрімкий розвиток інформаційно-комунікаційної сфери та інформаційних технологій зумовив появу суспільно-небезпечних діянь – кіберзлочинів, зокрема кібертероризму. Отримали значне поширення випадки, коли жертвами кібертерористів у кіберпросторі стають не лише окремі користувачі мереж, а й держави.

Кібертероризм – це багатогранний феномен, обумовлений безконтрольним використанням глобальних мереж, а також недостатньою увагою з боку держави, суспільства та спецслужб до можливостей використання кіберпростору. За останні роки час переходу від загрози до реального акту кібертероризму значно скоротився. За оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет є найшвидшими на планеті. У 2015 р. Україна стала абсолютним лідером за внутрішніми та зовнішніми кіберзагрозами в Європі. У період 2014–2020 рр. Україна зазнала безпрецедентної кількості кібератак на об'єкти критичної інфраструктури. При цьому протягом 2018–2020 рр. кібератаки на критичну інфраструктуру України стали більш замаскованими, ніж у попередні роки, а на початку червня 2020 р. було виявлено новий тип DDOS-атаки на низку українських і світових провайдерів.

Кіберзлочинність, зокрема кібертероризм, завдають державам і приватним особам значних збитків, які, зважаючи на глобалізацію інформаційних відносин та значну технологічну базу кіберзлочинців, щорічно будуть лише зростати. Згідно з офіційним звітом про кіберзлочинність, опублікованим провідною світовою компанією Cybersecurity Ventures, світові втрати через кіберзлочинність зростатимуть на 15 % щорічно до 2025 р. і сягатимуть 10,5 трлн дол., тоді як у 2015 р. цей показник становив 3 трлн дол. Станом на початок 2021 р. глобальний збиток від кіберзлочинності оцінюється у 6 трлн дол.[1]. За даними американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS), хакерські атаки протягом 2020 р. коштували світовій економіці понад 1 трлн дол. або 820 млрд євро[2].

Таким чином, кібератаки загрожують безпеці особистості, суспільства і держави на всіх рівнях взаємодії. В умовах розвитку інформаційного

[1] Cybercrime facts and statistics. 2021 Special Report: Cyberwarfare In The C-Suite / Editor-in-Chief Steve Morgan. January. 21, 2021. URL: https://cybersecurityventures.com/our-company

[2] Cybersecurity and Technology. The Center for Strategic and International Studies (CSIS). URL: https://www.csis.org/topics/cybersecurity-and-technology

суспільства кібертероризм вже давно переріс межі регіонального та національного масштабу. Коли підвищений рівень терористичної загрози поєднується зі стрімко зростаючим рівнем залежності суспільства від інформаційних технологій, це питання стає особливо актуальним і вимагає скоординованих всеосяжних заходів на державному рівні. Масштаби поширення та наслідки від кібертерористичних актів диктують необхідність більш поглибленого аналізу загроз кібертероризму, систем інформаційної безпеки провідних держав світу, розробки та здійснення ефективної антикібертерористичної державної стратегії.

Наразі є чимало наукових доробок як зарубіжних дослідників, так і українських науковців, які займаються проблемою кібертероризму. Зокрема, варто виокремити таких дослідників кібербезпеки та кіберзлочинності, які зробили значний внесок у розробку заходів щодо протидії кібертероризму, як: Ю. Р. Акчурін, К. І. Бєляков, О. В. Бойченко, В. Л. Бурячок, В. М. Бутузов, В. А. Васенін, С. Б. Гавриш, О. С. Геращенко, С. О. Гнатюк, В. А. Голубєв, В. К. Грищук, М. В. Гуцалюк, І. В. Діордіц, О. Д. Довгань, І. М. Доронін, О. В. Копан, О. В. Кубишкін, В. А. Ліпкан, В. А. Мазурова, Є. А. Макаренко, А. І. Марущак, В. В. Мохор, М. А. Ожеван, С. Г. Петров, В. Г. Пилипчук, М. М. Рижиков, Л. М. Стрельбицька, М. П. Стрельбицький, Є.Д. Скулиш, А. В. Тарасюк, В. Б. Толубко, С. В. Толюпа, В. В. Топчій, Г. В. Форос, А. В. Форос, В. О. Хорошко, В. С. Цимбалюк, О. Г. Широкова-Мурараш та інші.

Однак, не дивлячись на чималу увагу багатьох правознавців до досліджуваної проблематики, виняткового значення для забезпечення кібербезпеки України набуває наукове обґрунтування ефективних механізмів забезпечення стратегії протидії кіберзлочинності, зокрема кібертероризму: деякі з них потребують удосконалення, інші взагалі ще не сформовані. З огляду на сучасні виклики кіберзагроз, недостатній розвиток сфери забезпечення кібербезпеки України вимагає невідкладної розробки оновленої стратегії з протидії кібертероризму, а також дієвих заходів, пов’язаних з реалізацією цієї стратегії.

Необхідність створення повноцінного єдиного центру координації процесу розбудови національної системи забезпечення кібербезпеки обумовила актуальність теми дисертації.

Зв’язок роботи з науковими програмами, планами, темами. Обраний напрям дослідження ґрунтується на положеннях Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки, схваленої Указом Президента України від 20 травня 2015 р. № 276; Національної стратегії у сфері прав людини на період до 2020 року, затвердженої Указом Президента України від 25 серпня 2015 р. № 501, та Плану заходів щодо її реалізації, схваленого розпорядженням Кабінету Міністрів України від 23 листопада 2015 р. № 1393–р.; узгоджується з Пріоритетними напрямами розвитку науки і техніки на період до 2020 року, затвердженими Законом України від 9 вересня 2010 р. № 2519-VI; Стратегією розвитку наукових досліджень Національної академії правових наук України на 2016–2020 роки,

схваленою Постановою загальних зборів НАПрН України від 3 березня 2016 р., та виконаний відповідно до Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 рр., затвердженого наказом МВС України від 16 березня 2015 р. № 275, пунктами 4.1, 4.4 розділу IV Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. № 96/2016, та Загального плану науково-дослідної роботи ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» на 2014–2018 рр. «Теоретико-методологічні засади становлення української державності і соціальна практика: політичні, юридичні, економічні та психологічні проблеми» (номер державної реєстрації 0113U007698).

Тема дисертації затверджена на засіданні Вченої ради ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» 27 січня 2016 р. (протокол № 1) й уточнена 30 травня 2018 р. (протокол № 5).

Мета і завдання дослідження. *Метою* дослідження є аналіз поняття, змісту кібертероризму, виокремлення його основних закономірностей з огляду на світові тенденції реалізації кіберзагроз і формування на цій основі засад комплексної національної системи протидії кібертероризму як загрозі інформаційній безпеці.

Для реалізації зазначеної мети необхідно виконати такі *завдання:*

– розкрити сутність і соціально-правову природу кібертероризму, окреслити його сутнісні юридично, економічно та організаційно значимі ознаки, на підставі яких удосконалити визначення поняття «кібертероризм»;

– здійснити аналіз світових тенденцій поширення кібертероризму і наслідків кібертерористичних актів;

– з’ясувати та визначити можливості застосування в Україні зарубіжного досвіду щодо розвитку систем протидії загрозам кібертероризму на державному рівні;

– визначити низку важливих теоретичних положень, висновків і рекомендацій, спрямованих на вдосконалення заходів протидії кібертероризму як загрозі інформаційній безпеці України, можливості запровадження кращих світових практик реалізації державних стратегій та імплементації вимог міжнародно-правових документів з протидії кібертероризму;

– розробити комплекс заходів щодо створення загальнонаціональної системи забезпечення безпеки стратегічно важливих об’єктів національної критичної інфраструктури;

– надати пропозиції щодо підвищення ефективності протидії кібертероризму та створення системи захисту інформаційного простору України від загроз кібертероризму шляхом впровадження норм міжнародних стандартів, стандартів ЄС у сфері кібербезпеки та кіберзахисту;

– визначити шляхи модернізації механізмів реалізації стратегії протидії кібертероризму в Україні та напрями удосконалення захисту інформаційного простору України від загроз кібертероризму.

Об’єктом дослідження є суспільно-правові відносини, що виникають у

процесі протидії кібертероризму в інформаційному просторі України.

Предметом дослідження є протидія кібертероризму як загрозі інформаційній безпеці України.

Методи дослідження. Методологічне підґрунтя дослідження становить цілісна та узгоджена система методів наукового пізнання, що надала можливість проаналізувати таке складне соціально-правове криміногенне явище, як кібертероризм: *діалектичний метод* використовувався при формулюванні поняття «кібертероризм», вивченні стану дослідження, організаційно-правового забезпечення протидії кібертероризму у зарубіжних країнах, аналізі правових засад формування та розвитку державної системи протидії кібертероризму в Україні як загрозі інформаційній безпеці (підрозділи 1.1, 1.3, 2.3, 3.1); *компаративний (порівняльно-історичний) метод* – при розгляді різних історичних моделей зарубіжних систем протидії загрозам кібертероризму на державному рівні, зарубіжних практик реалізації державних стратегій та вимог міжнародно-правових документів з протидії кібертероризму, генези наукової думки щодо напрямів протидії кібертероризму в Україні в історичному аспекті, при формулюванні пропозицій щодо вдосконалення нормативно-правового регулювання протидії кібертероризму в Україні (підрозділи 1.2, 1.3, 2.3, 3.1, 3.2); *системний метод* – при розгляді структури національної системи кібербезпеки України, основних загроз кібертероризму в інформаційному просторі України (підрозділи 1.1, 2.1, 2.3); *формально-юридичний метод* – при вивченні понятійно-категоріального апарату протидії кібертероризму, нормативно-правових актів у сфері забезпечення кібербезпеки в Україні та зарубіжних країнах, міжнародно-правових документів з протидії кібертероризму (підрозділи 1.1, 1.3, 2.2, 2.3, 3.1), *порівняльно-правовий метод* – при вивченні міжнародно-правових актів і законодавства зарубіжних країн з протидії кібертероризму (підрозділи 1.3, 3.1); *статистичний метод* – при аналізі наслідків кібертероризму у світі, систематизації хронології цільових кібератак, реалізованих в Україні та зарубіжних країнах (підрозділ 2.1); *методи аналізу та синтезу* – при узагальненні практики боротьби з кібертероризмом в Україні та зарубіжних країнах, розробці пропозицій щодо напрямів удосконалення системи заходів протидії кібертероризму (підрозділи 1.3, 3.2, 3.3).

Теоретичну базу дослідження становлять роботи вітчизняних і закордонних фахівців у галузі забезпечення кібербезпеки, пов’язані з тематикою дисертаційного дослідження.

Нормативно-правовою основою дослідження є Конституція України, законодавство України щодо забезпечення кібербезпеки, протидії кіберзлочинності та тероризму, чинне кримінальне законодавство, міжнародно-правові акти (конвенції, директиви тощо), законодавство з питань захисту інформації.

Емпіричну та інформаційну базу дисертації становлять статистичні дані Служби безпеки України (СБУ), Державної служби спеціального зв’язку та захисту інформації (Держспецзв’язку), матеріали узагальнень правоохоронної практики у сфері протидії кіберзлочинності, показники, опубліковані в різних літературних і спеціальних джерелах, аналітичні та оглядові матеріали.

Наукова новизна одержаних результатів полягає в комплексному дослідженні сучасних проблем протидії такому соціально-правовому криміногенному явищу, як кібертероризм. Розглянуто питання імплементації відповідних міжнародно-правових актів у національне законодавство в процесі створення національної системи кібербезпеки України. У результаті проведеного дослідження сформульовано низку науково-практичних висновків, положень і пропозицій, які викладені у сфері забезпечення кібербезпеки, зокрема:

вперше:

– розроблено комплекс заходів щодо створення загальнонаціональної системи забезпечення безпеки стратегічно важливих об'єктів національної критичної, зокрема інформаційної, інфраструктури з обґрунтуванням необхідності прийняття Стратегії кіберзахисту критичної інфраструктури України, розроблення національної програми, яка забезпечує кібербезпеку критично важливих інфраструктур держави, та Закону України «Про національну критичну інфраструктуру України та її кіберзахист», а також імплементації у вітчизняне законодавство Директиви Ради ЄС від 8 грудня 2008 р. № 2008/114/EU щодо захисту критичної інфраструктури;

– обґрунтовано необхідність внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України» щодо визначення низки ключових термінів, які вживаються у сфері протидії кібертероризму, зокрема «інформаційний тероризм», «комп'ютерний тероризм», «віртуальний тероризм», «кібертерористичний акт»;

– у процесі планування та реалізації організаційно-технічних заходів щодо захисту критично важливих об'єктів (КВО) у державі доведено доцільність впровадження системи управління інформаційною безпекою (СУІБ) КВО відповідно до серії міжнародних стандартів інформаційної безпеки ISO/IEC 27000 та стандарту ISO/IEC 27032:2012, що дозволяє оптимізувати процес захисту інформаційних ресурсів та управління ризиками для цих ресурсів;

– сформульовано принципи забезпечення захисту КВО від кіберзагроз щодо системності (комплексності) забезпечення кібербезпеки та кіберзахисту КВО; безперервності удосконалення і розвитку кібербезпеки та кіберзахисту КВО; своєчасності й адекватності заходів захисту від реальних і потенційних загроз кібербезпеці КВО; достатності ресурсів для сталого розвитку систем кібербезпеки КВО; єдиної системи кібербезпеки для всіх бізнес-процесів КВО, яка повинна забезпечити безпечність і надійність функціонування бізнес-процесів КВО;

удосконалено:

– визначення поняття «кібертероризм», в якому відображено предметно-сутнісні, юридично, економічно та організаційно значимі ознаки цього суспільно небезпечного протиправного явища;

– визначення проявів, особливостей, закономірностей, тенденцій кібертероризму, а також підходів до розуміння його сутності в Україні та окремих зарубіжних країнах;

– підходи до необхідності розробки єдиного, консолідуючого законодавчого акта з питань протидії кібертероризму – Закону України «Про забезпечення протидії кіберзлочинності»;

– виокремлення основних тенденцій кібертероризму у світі;

– положення про доповнення Угоди про асоціацію між Україною та ЄС європейською Директивою NIS щодо мережевої та інформаційної безпеки та Регламентом GDPR щодо захисту персональних даних з подальшою імплементацію в українське законодавство;

– обґрунтування доцільності врегулювання питання використання електронних доказів у кримінальному судочинстві та визначення чіткого процесуального порядку їх отримання відповідно до Кримінального процесуального кодексу України (КПК);

– положення щодо створення законодавчо-нормативної бази з функціонування системи сповіщення про кіберінциденти, впровадження системи кібераудиту і заходів мережевої та інформаційної безпеки;

дістали подальшого розвитку:

– наукові положення щодо особливостей співвідношення понять «кібертероризм», «інформаційні війни», «кібервійни» та «мережево-центричні війни»;

– позиція про доцільність створення в Україні системи (мережі) центрів реагування на кіберінциденти CERT, яка буде включати як загальнодержавні, так і локальні та галузеві центри, адже сьогодні Україна має на своїй території тільки один такий центр;

– наукові положення про необхідність криміналізації дій, пов’язаних з вчиненням кібертерористичних атак, а також розробки єдиного процесуального законодавства з питань боротьби з кіберзлочинністю, кібертероризмом та запобігання загрозі кібервійни;

– обґрунтування перегляду доцільності подальшої підтримки та фінансування деяких національних проєктів у сфері кібербезпеки, зокрема: Національної системи конфіденційного зв’язку (НСКЗ), Комплексної системи захисту інформації (КСЗІ), захищеного вузлу Інтернет-доступу для державних структур (ЗВІД-2) тощо, які вже морально та фізично застаріли та не відповідають на виклики сьогодення з протидії сучасним кіберзагрозам;

– питання врегулювання державно-приватного партнерства у сфері протидії кібертероризму шляхом створення механізмів зацікавленості власників (розпорядників) критично важливих об’єктів щодо забезпечення кібербезпеки на основі такої взаємодії;

– положення щодо доцільності обмеження повноважень Держспецзв’язку та СБУ у сфері забезпечення кібербезпеки з метою зменшення ризиків шпигунства та корупційних ризиків шляхом проведення кібераудиту незалежними аудиторами, що зменшить ризик корупціювання великого та середнього бізнесу владними структурами.

Практичне значення одержаних результатів полягає в тому, що сформульовані висновки і пропозиції можуть бути використані у:

– *правотворчій діяльності* – при внесенні змін і доповнень до чинного законодавства України щодо забезпечення кібернетичної безпеки та розвитку державної системи протидії кібертероризму в Україні, а також до відповідних кримінально-правових норм (акт впровадження РНБО України від 10 вересня 2020 р.);

– *науково-дослідній діяльності* – як основа для подальшого теоретичного пошуку вирішення проблем, пов'язаних із застосуванням заходів протидії кібертероризму в Україні (Акт впровадження Національної академії внутрішніх справ від 15 вересня 2020 р.);

– *освітньому процесі* – під час викладання дисципліни «Сучасні проблеми боротьби з тероризмом», у ННіП Міжрегіональної Академії управління персоналом (Акт впровадження ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» від 16 жовтня 2020 р.).

Апробація результатів дисертації. Основні положення, висновки та пропозиції, сформульовані в дисертації, оприлюднено на міжнародних науково-практичних конференціях: «Правові засоби забезпечення та захисту прав людини: вітчизняний та зарубіжний досвід» (м. Харків, 20–21 листопада 2020 р.); «Правові системи суспільства: сучасні проблеми та перспективи розвитку» (м. Львів, 20–21 листопада 2020 р.); «Реалізація державної антикорупційної політики в міжнародному вимірі» (м. Київ, 9–10 грудня 2020 р.) та Круглому столі, присвяченому 72-й річниці прийняття Загальної декларації прав людини (м. Київ, 10 грудня 2020 р.).

Публікації. Основні положення та висновки, що сформульовані в дисертації, відображено в 10 наукових публікаціях, з яких п'ять статей – у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, одна – у закордонному юридичному виданні, чотири – у збірниках тез наукових доповідей, оприлюднених на міжнародних науково-практичних конференціях і круглому столі.

Структура та обсяг дисертації. Робота складається з анотації, переліку умовних позначень, вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел (167 найменувань на 19 сторінках) та 3 додатків (на 11 сторінках). Повний обсяг дисертації становить 259 сторінок, з них основного тексту – 214 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, визначено ступінь наукової розробленості проблеми, зв'язок роботи з науковими програмами, планами, темами, сформульовано мету та завдання, об'єкт і предмет дослідження, вказано використані з урахуванням специфіки завдань дослідження наукові методи, емпіричну базу дослідження, визначено наукову новизну узагальнень і висновків автора, теоретичне та практичне значення одержаних результатів, наведено відомості щодо апробації та публікації результатів дослідження.

Розділ 1 «Теоретичні засади протидії кібертероризму як загрозі

інформаційній безпеці України» складається з трьох підрозділів, які присвячено розгляду понятійно-категоріального апарату протидії кібертероризму в інформаційному просторі України, визначенню загального поняття «кібертероризм», його сутності, напрямків протидії кібертероризму в Україні, вивченню зарубіжного досвіду протидії загрозам кібертероризму на державному рівні.

У *підрозділі 1.1 «Історіографія та дослідження сучасних поглядів щодо протидії кібертероризму в інформаційному просторі України»* здійснено аналіз і систематизовано основні методики до визначення поняття «кібертероризм». Аналіз наукових праць, присвячених проблематиці протидії кібертероризму, показав, що єдиного тлумачення цього поняття наразі немає. Тому з метою відображення предметно-сутнісних, юридично, економічно та організаційно значимих ознак кібертероризму надано таке його визначення: кібертероризм – це проведення кібератак на інформаційно-комунікаційні та телекомунікаційні системи у кіберпросторі, з можливим настанням тяжких наслідків для держави, пов'язаних з аваріями і катастрофами техногенного характеру, що має на меті порушення державної безпеки, залякування державних органів влади та управління, виведення з ладу і руйнування критично важливих об'єктів інфраструктури держави.

Узагальнення наукових праць видатних учених у сфері протидії кібертероризму дозволило дійти таких висновків щодо природи та особливостей кібертероризму: – кібертероризм – це різновид тероризму; – кібертероризм нерозривно пов'язаний з іншим важливим у цій сфері поняттям – кібератаками; – термін «кібертероризм» є синтезом понять «кіберпростір» і «тероризм»; – кібертероризм є видовим, а інформаційний тероризм – родовим поняттям одного негативного явища – тероризму; – кібертероризм є різновидом інформаційного тероризму; – поняття кібертероризму більше співвідноситься з інформаційно-технічним тероризмом, аніж з будь-яким іншим різновидом інформаційного тероризму; – кібертероризм – це технологічний вид тероризму. Кібертерористи використовують високі інформаційні технології як кіберзброю; – кібертероризм не є різновидом комп'ютерної злочинності, оскільки специфічність сфери здійснення дій кібертерористами – кіберпростір – відмежовує кібертероризм від комп'ютерної злочинності; – кібертероризм не потрібно ототожнювати з інформаційними війнами.

У *підрозділі 1.2 «Ґенеза наукової думки щодо напрямів протидії кібертероризму в Україні»* здійснено узагальнення доробку наукових праць вітчизняних і зарубіжних учених у сфері протидії кібертероризму щодо основних напрямів подолання та нейтралізації цього суспільно небезпечного протиправного явища. З огляду на це виокремлено такі завдання, які в комплексному застосуванні допоможуть створити суттєвий кіберзахист для держави від проявів кібертероризму. Узагальнено напрями протидії кібертероризму в Україні, зокрема це: – постійний моніторинг кіберпростору на випадок потенційної кібертерористичної загрози; – надійний захист елементів вітчизняної критичної інфраструктури; – створення та оновлення програмного забезпечення, яке зможе захистити кіберпростір держави, підтримка новітніх

інформаційних технологій; – створення спеціалізованих підрозділів по боротьбі з кібертероризмом та ефективної системи координації їхньої 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; – 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 і запобігання загрозі кібервійни.

У *підрозділі 1.3 «Зарубіжний досвід щодо розвитку систем протидії загрозам кібертероризму на державному рівні»* досліджено зарубіжний досвід щодо здійснення організаційних заходів, спрямованих на розбудову систем забезпечення кібербезпеки держави.

На основі вивчення та аналізу зарубіжного досвіду з протидії кібертероризму встановлено, що в основі національних систем кібербезпеки знаходиться окремий центральний державний орган, який формує політику забезпечення кібербезпеки, здійснює законотворчу та нормативну діяльність у цій сфері, координує діяльність щодо кіберзахисту інших державних органів, забезпечує партнерство з приватним сектором, займається питаннями міжнародного співробітництва щодо протидії кібертероризму та іншим кіберзлочинам.

Доведено, що міжнародне співтовариство поки що перебуває у пошуку не лише механізмів протидії кібертероризму, але і в процесі вироблення відповідної єдиної політики. Обґрунтовано, що ці недоліки державних систем забезпечення кібербезпеки зарубіжних країн викликані тим, що як у європейських правових нормах, так і в міжнародно-правових актах немає єдиного визначення поняття «кібертероризм», що, своєю чергою, призводить до вироблення державами різних підходів до складання стратегій кібербезпеки, що унеможливлює чітку координацію зусиль державних органів усіх країн та ускладнює процес міжнародного співробітництва у сфері протидії кібертероризму.

Розділ 2 «Методологія, методика та напрями дослідження протидії кібертероризму в Україні» складається з трьох підрозділів, в яких досліджено основні загрози кібертероризму в інформаційному просторі України, розкрито концептуальні засади державної стратегії з протидії кібертероризму та викладено правові засади формування і розвитку державної системи протидії кібертероризму в Україні.

У *підрозділі 2.1 «Методика виявлення основних кіберзагроз в інформаційному просторі України на шкоду національним інтересам, пов'язаних з проявами кібертероризму»* проаналізовано основні прояви, особливості, закономірності й тенденції кібертероризму в Україні та зарубіжних країнах.

На основі узагальнення проявів реалізації загроз кібертероризму в Україні зроблено висновок, що наразі актуальним завданням у сфері забезпечення кібербезпеки України є чітке розуміння суб'єктами національної системи кібербезпеки типів кібератак, які можуть пошкодити мережу або призвести до витоку інформації з об'єктів критичної інфраструктури держави, володіння потрібними знаннями та інструментами для запобігання цим протиправним діям і розмежовування доступу до важливих елементів критичної інформаційної інфраструктури.

Акцентовано на таких важливих особливостях сучасного кібертероризму, як його добре структурований та організований характер, наявність підрозділів кіберрозвідки і кіберконтррозвідки, комплексність та складний характер кіберзагроз, спеціалізація хакерів.

Доведено, що сьогодні основним об'єктом кібертерористичних атак є об'єкти критичної інфраструктури. Наголошено, що у зв'язку з інтенсивним впровадженням зарубіжних інформаційних технологій у сфери діяльності нашої держави, а також з широким застосуванням відкритих інформаційно-телекомунікаційних систем, інтеграцією вітчизняних і міжнародних інформаційних систем зросли загрози застосування кіберзброї проти інформаційної інфраструктури держави. Роботи з адекватної комплексної протидії цим загрозам ведуться при недостатній координації державних органів – суб'єктів національної системи кібербезпеки – і слабкому бюджетному фінансуванні.

У *підрозділі 2.2 «Концептуальні засади державної стратегії з протидії кібертероризму»* розкрито концептуальні (методологічні) засади для розробки оновленої Стратегії кібербезпеки України з визначенням пріоритетів національних інтересів України у сфері кібербезпеки, а також основних напрямів формування питань кіберзахисту.

З метою створення ефективної системи забезпечення кібербезпеки в Україні та з огляду на кращу світову практику в цій сфері, задля розробки оновленої Стратегії кібербезпеки України запропоновано реалізувати такі заходи з організації протидії кібертероризму: – доповнити Угоду про асоціацію Угоди про асоціацію між Україною та ЄС європейською Директивою NIS щодо мережевої та інформаційної безпеки та Регламентом GDPR щодо захисту персональних даних з подальшою імплементацію в українське законодавство; – для належної імплементації Конвенції Ради Європи про кіберзлочинність та усунення однієї з найбільших невідповідностей українського законодавства до європейського в сфері кібербезпеки – внести зміни до чинного КПК України щодо врегулювання питання використання електронних доказів у кримінальному судочинстві та визначення чіткого процесуального порядку їх отримання згідно з цим Кодексом; – після розробки та затвердження оновленої Стратегії кібербезпеки України – розробити Комплексну програму забезпечення кібербезпеки держави, де конкретизувати заходи щодо протидії загрозам

кібербезпеці, зокрема загрозам кібертероризму, а також визначити терміни виконання цих заходів і відповідальні за їх реалізацію державні органи; – при оновленні Стратегії кібербезпеки орієнтуватися на вимоги до національних стратегій кібербезпеки, які визначені в ст. 7 європейської Директиви NIS; – переглянути доцільність подальшої підтримки та фінансування деяких національних проєктів у сфері кібербезпеки, зокрема: Національної системи конфіденційного зв'язку (НСКЗ), Комплексної системи захисту інформації (КСЗІ), захищеного вузла Інтернет-доступу для державних структур (ЗВІД-2) тощо, які вже морально та фізично застаріли і не відповідають на виклики сьогодення з протидії сучасним кіберзагрозам; – налагодити якісну взаємодію у рамках державно-приватного партнерства, адже переважна більшість кібератак спрямована саме на приватний сектор, а захист з боку держави наразі є недостатнім; – урегулювати питання щодо створення механізмів зацікавленості власників (розпорядників) КВО в аспекті забезпечення кібербезпеки на основі державно-приватного партнерства; – розробити комплекс заходів щодо створення загальнонаціональної системи забезпечення безпеки стратегічно важливих об'єктів національної критичної, зокрема інформаційної, інфраструктури на основі єдиного методологічного підходу до ідентифікації критично важливих об'єктів та вибору методів і засобів підвищення їх захищеності; – розробити національну програму, що забезпечуватиме кібербезпеку критично важливих інформаційних інфраструктур держави.

У *підрозділі 2.3 «Правові засади формування та розвитку державної системи протидії кібертероризму в Україні як загрозі інформаційній безпеці»* вивчено законодавчі та інші нормативно-правові акти, що регулюють питання протидії кібертероризму в Україні.

У межах розгляду правових засад формування та розвитку державної системи протидії кібертероризму в Україні як загрозі інформаційній безпеці підтримано і розвинуто думку відносно того, що сучасне законодавство з кібербезпеки України не має чіткої ієрархічної побудови, єдності, комплексності, що викликає 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. Встановлено, що у Законі України «Про основні засади забезпечення кібербезпеки України» не надано дефініції багатьом ключовим термінам, які вживаються у сфері протидії кібертероризму («інформаційний тероризм», «комп'ютерний тероризм», «віртуальний тероризм», «кібертерористичний акт»), що потрібно усунути.

Доведено, що неможливість забезпечення кібербезпеки в Україні одним державним органом в силу специфіки об'єкта регулювання зумовила «розпорошення» повноважень між низкою державних органів, що може призвести взагалі до втрати контролю над ефективним управлінням кіберпростором у нашій державі.

Встановлено, що наявність значної кількості суб'єктів національної системи кібербезпеки може призвести до зловживань, вчинюваних цими суб'єктами у процесі здійснення ними повноважень щодо забезпечення

кібербезпеки у державі. І це при тому, що у чинному законодавстві містяться положення щодо необхідності подання щорічних звітів про результати проведення незалежного аудиту діяльності основних суб'єктів національної системи кібербезпеки. З огляду на правовий статус суб'єктів національної системи кібербезпеки виникає запитання, до компетенції якого державного органу буде входити обов'язок проведення незалежного аудиту діяльності цих суб'єктів.

Розділ 3 «Створення системи захисту інформаційного простору України від загроз кібертероризму та шляхи і напрями підвищення ефективності протидії кібертероризму» складається з трьох підрозділів, в яких вивчено досвід зарубіжних країн з розробки державних стратегій, окреслено вимоги міжнародно-правових документів з протидії кібертероризму, запропоновано шляхи модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні, а також визначено перспективні напрями удосконалення захисту інформаційного простору України від загроз кібертероризму.

У *підрозділі 3.1 «Запровадження в Україні кращих практик реалізації державних стратегій та імплементація вимог міжнародно-правових документів з протидії кібертероризму як загрозі інформаційній безпеці»* розкрито зміст міжнародно-правових актів і державних стратегій зарубіжних країн з протидії кібертероризму для визначення оптимальних та ефективних напрямів запровадження відповідного міжнародного і зарубіжного досвіду в Україні.

З метою покращення практики протидії кібертероризму в Україні на основі застосування відповідного зарубіжного досвіду запропоновано: – розробити проєкт Закону України «Про національну критичну інфраструктуру та її кіберзахист»; – імплементувати у вітчизняне законодавство в повному обсязі Конвенцію про кіберзлочинність, Директиву Ради ЄС від 8 грудня 2008 р. № 2008/114/EU щодо захисту критичної інфраструктури, Директиву ЄС від 12 серпня 2013 р. № 2013/40/EU щодо кібератак на інформаційні системи; – продовжити роботу у напрямі подальшого удосконалення нормативно-правової бази шляхом впровадження норм міжнародних стандартів, стандартів ЄС і НАТО у сфері кібербезпеки та кіберзахисту.

В процесі планування та реалізації організаційно-технічних заходів щодо захисту КВО у державі доведено доцільність впровадження такого міжнародного стандарту інформаційної безпеки, як ISO/IEC 27032:2012 «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». Встановлено, що обов'язковим для застосування разом зі стандартом ISO/IEC 27032:2012 є стандарт з питань інформаційної безпеки ISO/IEC 27000:2018 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник».

Обґрунтовано, що впровадження СУІБ КВО відповідно до серії стандартів ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів.

Зроблено висновок, що застосування норм зазначених міжнародних стандартів ISO, загальноприйнятих у міжнародній практиці принципів

забезпечення інформаційної безпеки і кіберзахисту, сприятиме підвищенню захисту КВО від загроз кібертероризму завдяки впровадженню на цих об’єктах СУІБ.

Сформульовано принципи забезпечення захисту КВО від кіберзагроз, зокрема загроз кібертероризму: 1) системності методів до забезпечення кібербезпеки та кіберзахисту КВО; 2) безперервності процесу удосконалення та розвитку кібербезпеки та кіберзахисту КВО, який має здійснюватися шляхом обґрунтування та реалізації раціональних засобів, методів, заходів на основі вимог чинного законодавства, відповідних національних і міжнародних стандартів з питань забезпечення кібербезпеки та із застосуванням найкращого міжнародного досвіду; 3) своєчасності та адекватності заходів захисту від реальних і потенційних загроз кібербезпеці КВО; 4) достатності ресурсів, зокрема фінансових, для забезпечення сталого розвитку систем кібербезпеки КВО; 5) єдності системи кібербезпеки для всіх бізнес-процесів КВО, яка має забезпечити безпечність і надійність функціонування бізнес-процесів КВО.

У *підрозділі 3.2 «Шляхи модернізації механізмів реалізації стратегії протидії кібертероризму в Україні»* досліджено механізми державного реагування на кіберзагрози, зокрема загрози кібертероризму, в Україні.

З метою модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні та з огляду на критично низький стан кібербезпекової складової вітчизняного сегменту кіберпростору, численні системні проблеми в організації кібербезпеки центральних органів виконавчої влади та об’єктів критичної інфраструктури запропоновано: – провести об’єктивний незалежний аудит кібербезпеки державних електронних інформаційних ресурсів за міжнародними стандартами під егідою Національного координаційного центру кібербезпеки (НКЦК) при Раді національної безпеки і оборони України (РНБО України) та однієї з авторитетних міжнародних кібербезпекових організацій; – визначити державну структуру (або державні структури), які будуть відповідальними за впровадження в Україні стандартів безпеки мережевих та інформаційних систем, визначити єдиний контактний центр з питань безпеки мережевих та інформаційних систем, взаємовідносини і розподіл повноважень між такою державною установою (установами), контактним центром та CERT (Комп’ютерною групою (Командою) реагування на надзвичайні ситуації в кіберпросторі) Держспецзв’язку; – з метою здійснення адекватного та ефективного кіберзахисту КВО – визначити так звані критерії «значної руйнівної дії» (з точки зору наявності та значимості кіберінцидентів на підставі реалізації кіберзагроз) з урахуванням особливостей надання інформаційно-телекомунікаційних послуг в певних секторах економіки, кількості користувачів сервісу конкретного оператора інформаційно-телекомунікаційних послуг чи провайдера цифрових послуг, залежності інших важливих секторів економіки від сервісу конкретного оператора чи провайдера тощо; – впровадити стандартизацію у сфері кібербезпеки за міжнародними стандартами ISO, зокрема галузеві стандарти кібербезпеки у зв’язку зі специфікою багатьох галузей економіки (охорона здоров’я, енергетика, телекомунікації тощо); – визначити єдиний державний орган, який би здійснював оперативне управління усіма

суб'єктами, чиїм завданням є забезпечення кібербезпеки у мирний час, адже функції інших державних органів, які входять до складу національної системи кібербезпеки, чітко не розмежовані, що призводить до дублювання деяких повноважень; – обмежити повноваження Держспецзв'язку та СБУ у сфері забезпечення кібербезпеки з метою зменшення ризиків шпигунства та корупційних ризиків. Це стане можливим, зокрема, якщо кібераудит буде проводитись незалежними аудиторами, що зменшить ризик корупціювання великого та середнього бізнесу владними структурами; – обмежити об'єкти критичної інфраструктури, перераховані в Законі України «Про основні засади забезпечення кібербезпеки України», залишивши у ньому винятково ті КВО, які знаходяться у власності держави; – скоротити перелік суб'єктів, до повноважень яких віднесено забезпечення кібербезпеки України; – чітко визначити компетенцію кожного з державних органів – суб'єктів національної системи кібербезпеки для усунення дублювання їхніх функцій.

У *підрозділі 3.3 «Напрями удосконалення захисту інформаційного простору України від загроз кібертероризму»* визначено основні напрями боротьби з кібертероризмом, завдання забезпечення кібербезпеки, перспективні напрями удосконалення чинного законодавства у цій сфері, а також ключові напрями у сфері державно-приватного партнерства в процесі забезпечення кібербезпеки.

З метою створення ефективної національної системи забезпечення кібербезпеки виокремлено перспективні напрями удосконалення чинного законодавства у цій сфері на основі визначення основних перешкод і розробки шляхів їх подолання: 1) необхідність створення повноцінного єдиного центру координації процесу розбудови національної системи забезпечення кібербезпеки, оскільки сьогодні спостерігається неефективність і непрозорість діяльності НКЦК у сфері забезпечення кібербезпеки, незрозумілість його правових засад функціонування. Наголошено, що НКЦК фактично виступає інформаційно-експертним органом без належних повноважень щодо інших суб'єктів системи забезпечення кібербезпеки. З'ясовано, що жоден з державних органів наразі не виконує функції координатора з питань державно-приватного партнерства у сфері кібербезпеки. Розширення Угоди про асоціацію між Україною та ЄС і створення в Урядовому офісі з питань європейської та євроатлантичної інтеграції спеціального підрозділу з питань кібербезпеки дозволило б систематизувати висновки українських і міжнародних експертів щодо різних проєктів у сфері кібербезпеки, налагодити прямий контакт з експертами НАТО, ЄС, РЄ, ОБСЄ, інших організацій, зробити процес законотворчості у цій сфері більш прозорим, підзвітним та зрозумілим; 2) доцільність проведення прозорого кібераудиту об'єктів критичної інфраструктури, оскільки відсутність загального розуміння наявного стану національної системи забезпечення кібербезпеки, достовірних оцінок, статистичних даних щодо цих питань призводить до неправильної ідентифікації кіберзагроз КВО, кіберінцидентів і неможливості їх своєчасного усунення; 3) необхідність подолання недовіри та розвитку співробітництва між так званими суб'єктами забезпечення кібербезпеки та суб'єктами національної системи кібербезпеки згідно із Законом України «Про основні засади

забезпечення кібербезпеки України».

З метою ефективного забезпечення кібербезпеки та організації контролю надійності і достатності методів та заходів її забезпечення на КВО інформаційно-телекомунікаційної інфраструктури держави доведено доцільність створення загальнодержавної та регіональних систем управління кібербезпекою та протидії кібертероризму на КВО інформаційно-телекомунікаційної сфери (іншими словами, систем виявлення, попередження та ліквідації наслідків кібератак на КВО інформаційної інфраструктури).

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та надано нове вирішення наукового завдання, яке виявилося у комплексному дослідженні такого суспільно небезпечного явища, як кібертероризм, з акцентуванням уваги на вивченні теоретичних засад протидії кібертероризму як загрозі інформаційній безпеці України, зокрема концептуальних засад державної стратегії з протидії кібертероризму, а також визначенні шляхів і напрямів створення системи захисту інформаційного простору України від загроз кібертероризму та підвищення ефективності протидії кібертероризму. Узагальнення та аналіз емпіричного матеріалу дозволили одержати наукові та практичні результати, спрямовані на протидію кібертероризму в Україні, зокрема:

1. На підставі аналізу сутності та соціально-правової природи такого суспільно небезпечного явища, як кібертероризм, шляхом визначення його сутнісних юридично, економічно та організаційно значимих ознак надано таке авторське визначення цьому поняттю: кібертероризм – це проведення кібератак на інформаційно-комунікаційні та телекомунікаційні системи у кіберпросторі, з можливим настанням тяжких наслідків для держави, пов’язаних з аваріями і катастрофами техногенного характеру, що має на меті порушення державної безпеки, залякування державних органів влади та управління, виведення з ладу і руйнування критично важливих об'єктів інфраструктури держави.

2. До основних тенденцій кібертероризму у світі віднесено: політичний хактивізм; вчинення кібератак державними структурами за допомогою створених кібервійськ і застосованої кіберзброї; функціонування віртуальних мережевих спільнот екстремістського спрямування; тісний зв’язок кібершпигунства з кібертероризмом; поширення шкідливого програмного забезпечення для шифрування вмісту баз даних вебсайтів компаній, які мають об’єкти критичної інфраструктури; розповсюдження кібератак, здійснених ботнетами з інфікованих вірусами «розумних» речей; поширення сервісів Crime-as-a-Service («злочин як послуга») – залучення фахівців, оренда шкідливого програмного забезпечення для організації кібератак тощо.

3. З огляду на зарубіжний досвід зроблено висновок щодо доцільності створення в Україні системи (мережі) центрів реагування на кіберінциденти CERT, яка включала б як загальнодержавні, так і локальні та галузеві центри, адже сьогодні Україна має на своїй території тільки один такий центр – діючу в складі Держспецзв’язку Команду реагування на комп’ютерні надзвичайні події

(Computer Emergency Response Team of Ukraine – CERT-UA).

4. З метою створення ефективної системи забезпечення кібербезпеки в Україні та задля розробки оновленої Стратегії кібербезпеки України запропоновано реалізувати такі заходи з організації протидії кібертероризму: – доповнити Угоду про асоціацію Угоди про асоціацію між Україною та ЄС європейською Директивою NIS щодо мережевої та інформаційної безпеки та Регламентом GDPR щодо захисту персональних даних з подальшою імплементацію в українське законодавство; – для належної імплементації Конвенції Ради Європи про кіберзлочинність внести зміни до чинного КПК України щодо врегулювання питання використання електронних доказів у кримінальному судочинстві та визначення чіткого процесуального порядку їх отримання згідно з цим Кодексом; – після розробки та затвердження оновленої Стратегії кібербезпеки України – розробити Комплексну програму забезпечення кібербезпеки держави, де конкретизувати заходи щодо протидії загрозам кібербезпеці, зокрема загрозам кібертероризму, а також визначити терміни виконання цих заходів і відповідальні за їх реалізацію державні органи; – переглянути доцільність подальшої підтримки та фінансування деяких національних проєктів у сфері кібербезпеки, зокрема: Національної системи конфіденційного зв'язку (НСКЗ), Комплексної системи захисту інформації (КСЗІ), захищеного вузла Інтернет-доступу для державних структур (ЗВІД-2) тощо, які вже морально та фізично застаріли і не відповідають на виклики сьогодення з протидії сучасним кіберзагрозам. Наразі в Україні як єдиний (крім банківського сектору) державний стандарт технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». На відміну від найпоширенішої у світі серії стандартів інформаційної безпеки ISO/IEC 27000 – КСЗІ, впроваджена НД ТЗІ 2.5–004–99 має недостатню гнучкість, громіздкість, застарілу концепцію захисту, впродовж багатьох років довела свою неефективність. Отже, доведено, що Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» і низка нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі.

5. Для підвищення ефективності кіберзахисту КВО запропоновано розробити комплекс заходів щодо створення загальнонаціональної системи забезпечення безпеки стратегічно важливих об'єктів національної критичної, зокрема інформаційної, інфраструктури на основі єдиного методологічного підходу до ідентифікації критично важливих об'єктів та вибору методів і засобів підвищення їх захищеності з обґрунтуванням необхідності прийняття Стратегії кіберзахисту критичної інфраструктури України, розроблення національної програми, яка забезпечує кібербезпеку критично важливих інфраструктур держави, та Закону України «Про національну критичну інфраструктуру України та її кіберзахист», а також імплементації у вітчизняне законодавство Директиви Ради ЄС від 8 грудня 2008 р. № 2008/114/EU щодо захисту критичної інфраструктури тощо.

6. З метою покращення практики протидії кібертероризму в Україні на основі застосування відповідного зарубіжного досвіду запропоновано: – імплементувати у

вітчизняне законодавство в повному обсязі Конвенцію про кіберзлочинність, Директиву ЄС від 12 серпня 2013 р. № 2013/40/EU щодо кібератак на інформаційні системи; – продовжувати роботу у напрямі подальшого удосконалення нормативно-правової бази шляхом впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері кібербезпеки та кіберзахисту.

Доведено доцільність впровадження таких міжнародних стандартів інформаційної безпеки, як ISO/IEC 27032:2012 «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки» та ISO/IEC 27000:2018 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник». Обґрунтовано, що впровадження СУІБ КВО відповідно до серії стандартів ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів.

7. Для модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні та з огляду на критично низький стан кібербезпекової складової вітчизняного сегменту кіберпростору запропоновано: – провести об'єктивний незалежний аудит кібербезпеки державних електронних інформаційних ресурсів за міжнародними стандартами під егідою Національного координаційного центру кібербезпеки при РНБО України та однієї з авторитетних міжнародних кібербезпекових організацій; – визначити державну структуру (або державні структури), які будуть відповідальними за впровадження в Україні стандартів безпеки мережевих та інформаційних систем, визначити єдиний контактний центр з питань безпеки мережевих та інформаційних систем, взаємовідносини та розподіл повноважень між такою державною установою (установами), контактним центром та CERT (Комп'ютерною групою (Командою) реагування на надзвичайні ситуації в кіберпросторі) Держспецзв'язку; – впровадити стандартизацію у сфері кібербезпеки за міжнародними стандартами ISO, зокрема галузеві стандарти кібербезпеки у зв'язку зі специфікою багатьох галузей економіки (охорона здоров'я, енергетика, телекомунікації тощо); – визначити єдиний державний орган, який би здійснював оперативне управління усіма суб'єктами, чиїм завданням є забезпечення кібербезпеки у мирний час, адже функції інших державних органів, які входять до складу національної системи кібербезпеки, чітко не розмежовані, що призводить до дублювання деяких повноважень; – обмежити повноваження Держспецзв'язку та СБ України у сфері забезпечення кібербезпеки з метою зменшення ризиків шпигунства та корупційних ризиків. Це стане можливим, зокрема, якщо кібераудит буде проводитись незалежними аудиторами, що зменшить ризик корупціювання великого та середнього бізнесу владними структурами; – обмежити об'єкти критичної інфраструктури, перераховані в Законі України «Про основні засади забезпечення кібербезпеки України», залишивши у ньому винятково ті КВО, які знаходяться у власності держави; – скоротити перелік суб'єктів, до повноважень яких віднесено забезпечення кібербезпеки України; – чітко визначити компетенцію кожного з державних органів – суб'єктів національної системи кібербезпеки для усунення дублювання їхніх функцій.

Подальші дослідження даної проблематики вбачаються у комплексному підході до вирішення завдань протидії кібертероризму в Україні на основі оновленої Стратегії кібербезпеки України та міжнародного досвіду.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Когут Ю. І. Перспективні напрями удосконалення захисту інформаційного простору України від загроз кібертероризму. *Прикарпатський юридичний вісник*. 2017. Вип. 1. Т. 5. С. 190–196.

2. Когут Ю. І. Генеза наукової думки щодо напрямків протидії кібертероризму в Україні. *Прикарпатський юридичний вісник*. 2018. Вип. 2. Т. 5. С. 207–213.

3. Когут Ю. І. Зарубіжний досвід щодо розвитку систем протидії загрозам кібертероризму на державному рівні. *Юридична наука*. 2019. № 12. С. 178–184.

4. Когут Ю. І. Шляхи модернізації механізмів реалізації стратегії протидії кібертероризму в Україні на основі використання міжнародного досвіду. *Юридичний науковий електронний журнал*. 2020. № 8. С. 291–294.

5. Когут Ю. І. Правові засади формування та розвитку державної системи протидії кібертероризму в Україні. *Підприємництво, господарство і право*. 2020. № 12. С. 170–174.

6. Kohut Y. Measures for protection of the information systems of Ukraine's critical infrastructures against cyberattacks. *Kultura Bezpieczeństwa*. 2020. № 38. P. 57–65.

7. Когут Ю. І. Пріоритети захисту прав і свобод людини і громадянина у кіберпросторі за законодавством України та країн ЄС. *Правові засоби забезпечення та захисту прав людини: вітчизняний та зарубіжний досвід*: матеріали Міжнар. наук.-практ. конф. (Харків, 20–21 листоп. 2020 р.). Харків: ГО «Асоціація аспірантів-юристів», 2020. С. 16–19.

8. Когут Ю. І. Особливості системи кібербезпеки ЄС. *Правові системи суспільства: сучасні проблеми та перспективи розвитку*: матеріали Міжнар. наук.- практ. конф. (Львів, 20–21 листоп. 2020 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2020. Ч. 2. С. 116–120.

9. Когут Ю. І. Реалізація державної антикорупційної політики в процесі управління національною системою кібербезпеки. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали V Міжнар. наук.-практ. конф. (Київ, 9–10 груд. 2020 р.): у 2 ч. / Редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ: Нац. акад. внутр. справ, 2020. Ч. 2. С. 132–135.

10. Когут Ю. І. Захист персональних даних в умовах ескалації кіберзагроз національним інтересам України. *Збірник тез круглого столу, присвяченого 72-й річниці прийняття Загальної декларації прав людини* (Київ, 10 груд. 2020 р.). Київ: ДНДІ МВС України, 2021. С. 106–108.

АНОТАЦІЯ

Когут Ю. І. Протидія кібертероризму як загрозі інформаційній безпеці України. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 21.07.01 – забезпечення державної безпеки України. – ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», Київ, 2021.

Дисертаційне дослідження присвячено проблемі протидії такому негативному суспільно небезпечному соціально-правовому явищу, як кібертероризм, у кіберпросторі України. Порівняльним чином розглянуто відповідні практики у провідних зарубіжних країнах і вимоги міжнародно-правових документів з протидії кібертероризму як загрозі інформаційній безпеці. Проаналізовано основні прояви, особливості, закономірності та тенденції кібертероризму в Україні й зарубіжних країнах. На цій емпіричній та теоретичній основі розглянуто концептуальні засади державної стратегії з протидії кібертероризму, запропоновано напрями підвищення ефективності протидії кібертероризму та створення основ національної системи захисту кіберпростору України від загроз кібертероризму, а також шляхи модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні.

Ключові слова: кібертероризм, кібербезпека, критична інфраструктура, кіберзахист, кібератаки, кіберпростір, національна система кібербезпеки, кібераудит, стратегія кібербезпеки, державно-приватне партнерство.

АННОТАЦИЯ

Когут Ю. И. Противодействие кибертерроризму как угрозе информационной безопасности Украины. – *Квалификационный научный труд на правах рукописи.*

Диссертация на соискание ученой степени кандидата юридических наук по специальности 21.07.01 – обеспечение государственной безопасности Украины. – ЧАО «Высшее учебное заведение «Межрегиональная Академия управления персоналом», Киев, 2021.

Диссертационное исследование посвящено проблеме противодействия такому негативному общественно опасному социально-правовому явлению, как кибертерроризм, в киберпространстве Украины. Сравнительным образом рассмотрены соответствующие практики в ведущих зарубежных странах и требования международно-правовых документов по противодействию кибертерроризму как угрозе информационной безопасности. Проанализированы основные проявления, особенности, закономерности и тенденции кибертерроризма в Украине и зарубежных странах. На этой эмпирической и теоретической основе рассмотрены концептуальные основы государственной стратегии по противодействию кибертерроризму, предложены направления повышения эффективности противодействия кибертерроризму и создания основ национальной системы защиты киберпространства Украины от угроз кибертерроризма, а также пути модернизации механизмов реализации государственной стратегии противодействия кибертерроризму в Украине.

На основе обобщения проявлений реализации угроз и тенденций кибертерроризма в Украине доказано, что сегодня актуальной задачей в сфере

обеспечения кибербезопасности Украины есть четкое понимание субъектами национальной системы кибербезопасности типов кибератак, которые могут повредить сеть или привести к утечке информации с объектов критической инфраструктуры, владение нужными знаниями и инструментами для предотвращения этих противоправных действий и разграничения доступа к важным элементам критической информационной инфраструктуры.

Для дальнейшего совершенствования киберзащиты национальной критической инфраструктуры предложено: окончательно урегулировать процесс создания системы киберзащиты национальной критической инфраструктуры путем принятия Стратегии киберзащиты критической инфраструктуры Украины, разработки национальной программы, которая обеспечивает кибербезопасность критически важных инфраструктур государства, и Закона Украины «О национальной критической инфраструктуре Украины и ее киберзащите»; имплементировать в отечественное законодательство Директиву Совета ЕС от 8 декабря 2008 г. № 2008/114 EU по защите критической инфраструктуры; создать эффективную общегосударственную систему киберзащиты критической инфраструктуры Украины, координации и управления силами и средствами обеспечения ее кибербезопасности.

Ключевые слова: кибертерроризм, кибербезопасность, критическая инфраструктура, киберзащита, кибератаки, киберпространство, национальная система кибербезопасности, кибераудит, стратегия кибербезопасности, государственно-частное партнерство.

ANNOTATION

Kohut Yu. I. Combating cyber terrorism as a threat to information security of Ukraine. – *Qualifying scientific work on the rights of the manuscript.*

Thesis for a Candidate of Law Degree in Specialty 21.07.01 “Ensuring the state security of Ukraine” – PJSC “Higher Educational Institution «Interregional Academy of Personnel Management»”, Kyiv, 2021.

The thesis is devoted to the problem of combating this negative social and legal dangerous social phenomenon as cyberterrorism in Ukraine cyberspace. Comparative been considered appropriate practices in leading foreign countries and the requirements of international law to combat cyber terrorism as a threat to information security. The main manifestations, features, regularities and tendencies of cyberterrorism in Ukraine and foreign countries are analyzed. This empirical and theoretical basis of the conceptual foundations of a state strategy to combat cyber proposed areas of combating cyber efficiency and provide a basis for a national system of protection of cyberspace Ukraine cyber threats and ways to modernize the mechanisms of implementation of the state strategy for combating cyber Ukraine.

Keywords: cyberterrorism, cybersecurity, critical infrastructure, cyber defense, cyber attacks, cyberspace, national cybersecurity system, cyberaudit, cybersecurity strategy, public-private partnership.

Наклад 100. Папір офсетний. Ум.-др. арк. 0,9.
Підписано до друку 22.02.2021. Замовлення 241.

Надруковано в «МП Леся».
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи серія ДК № 892 від 08.04.2002.

«МП Леся»
03148, Київ, а/с 115.
Тел./факс: (066) 60-50-199, (098) 455-41-17
E-mail: lesya3000@ukr.net