УДК 343.32

Ю. І. Когут
здобувач
Навчально-наукового інституту права імені князя Володимира Великого
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»

ПЕРСПЕКТИВНІ НАПРЯМИ УДОСКОНАЛЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ЗАГРОЗ КІБЕРТЕРОРИЗМУ

Постановка проблеми та її актуальність. Аналіз безпеки національних інформаційних інфраструктур показав, що більшість життєво важливих об'єктів держав світу уразливі до можливих кібератак. Так, славнозвісні кібератаки «Stuxnet», «Duqu», «Flame», «Gauss» та інші на державні інформаційні системи засвідчили, наскільки вразливі ІТ-інфраструктури паливно-енергетичних, виробничих, транспортних, інформаційно-телекомунікаційних, комунальних, фінансових та інших систем життєзабезпечення суспільства та наскільки катастрофічними можуть бути наслідки викликаних подібними кібератаками збоїв та відмов у їх роботі [1, с. 41].

Швидка інформатизація України, масштаби потенційних наслідків вчинення злочинів у кіберпросторі вимагають від органів державної влади країни активізації уваги до питання подальшого розвитку національної системи забезпечення кібербезпеки з підвищенням ефективності роботи відповідних інституційних структур та з урахуванням зарубіжного досвіду в цій сфері, зокрема, до питань належної організації кіберзахисту ІТ-інфраструктури критично важливих об'єктів (КВО) держави. Тому слід постійно вивчати досвід зарубіжних країн у сфері забезпечення кібербезпеки і реалізовані в них заходи з протидії кібертероризму.

При цьому головним суб'єктом забезпечення безпеки кіберпростору в інтересах бізнесу та суспільства має бути держава. Підвищення ефективності кібербезпеки повинно розглядатися як стратегічна державна задача.

Аналіз останніх досліджень і публікацій. Значний внесок у розробку дієвих заходів запобігання та боротьби з кіберзлочинністю, зокрема кібертероризмом, зробили багато вчених-правознавців В. А. Ліпкан, В. А. Мазуров, В. М. Бутузов, В. А. Васенин, В. А. Голубєв, І. В. Діордіца, В. В. Топчій, Г. В. Форос, А. В. Форос, Є. А. Макаренко, М. М. Рижиков, М. А. Ожеван, В. К. Грищук, О. В. Кубишкін, В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа, О. Д. Довгань, І. М. Доронін, О. В. Бойченк, С. О. Гнатюк, С. Б. Гавриш, М. В. Гуцалюк, А. І. Марущак тощо.

Однак, незважаючи на наявність значної кількості наукових праць, присвячених питанням протидії кіберзлочинності, які є безперечно вагомим внеском у розроблення заходів боротьби з цим суспільно небезпечним явищем, на жаль, вони торкалися лише окремих аспектів зазначеної проблематики, актуальних на певних етапах розвитку законодавства та правоохоронної практики України. З огляду на значні зміни останніми роками організаційно-правової інфраструктури запобігання кіберзлочинності, зокрема кібертероризму, та постійну трансформацію нормативно-правової бази з її протидії в Україні, а також зважаючи на необхідність теоретичного аналізу впливу нових нормативно-правових актів на реальний стан боротьби з цим суспільно небезпечним явищем ця проблематика потребує подальших досліджень у цьому напрямку з урахуванням згаданих вище змін, адже кіберзлочинність постійно видозмінюється залежно від зміни соціально-економічних відносин. Чимало питань, що стосуються сучасного стану поширення кіберзлочинності, у тому числі кібертероризму, в Україні та проблем, які виникають у процесі її запобігання, продовжують залишатися дискусійними, або окремі питання досі взагалі не висвітлювалися науковцями.

Мета цієї **статті** полягає у надати пропозицій з підвищення ефективності протидії кібертероризму та створення системи захисту інформаційного простору України від загроз кібертероризму шляхом визначення перспективних напрямів удосконалення захисту інформаційного простору України від загроз кібертероризму.

Виклад основного матеріалу. З метою удосконалення захисту інформаційного простору будь-якої країни від загроз кібертероризму, як правило, виокремлюються такі основні перспективні напрями боротьби з кібертероризмом:

– уніфікація та гармонізація національного законодавства та міжнародних актів у сфері кібербезпеки;

– постійний моніторинг інформаційного середовища на випадок потенційної кібертерористичної загрози;

– ефективний захист об'єктів критичної інфраструктури;

– проведення наукових розробок у сфері створення сучасних технологій виявлення та запобігання терористичним впливам на інформаційні ресурси;

– створення та оновлення програмного забезпечення, яке зможе захистити кіберпростір держави;

– створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та кібертероризмом;

– удосконалення міжнародної організаційно-правової взаємодії з питань протидії кібертероризму;

– удосконалення багаторівневої системи підготовки кадрів у сфері кібербезпеки.

Недостатній розвиток сфери забезпечення кібербезпеки України вимагає невідкладного вирішення таких завдань, як [1, с. 44-45]:

– розробка оновлених основних напрямків державної політики в галузі забезпечення кібербезпеки держави з огляду на сучасні виклики кіберзагроз, а також розробка заходів і механізмів, пов'язаних з реалізацією цієї державної політики;

– вдосконалення системи забезпечення кібербезпеки держави, включаючи вдосконалення форм, методів і засобів виявлення, оцінки та прогнозування загроз кібербезпеці України, а також системи протидії цим кіберзагрозам, у тому числі загрозі кібертероризму;

– розробка загальнодержавних цільових програм забезпечення кібербезпеки і протидії кібертероризму;

– розробка критеріїв і методів оцінки ефективності систем і засобів забезпечення кібербезпеки держави та протидії кібертероризму, а також сертифікація цих систем і засобів;

– вдосконалення нормативно-правової бази забезпечення кібербезпеки і протидії кібертероризму в Україні;

– обов'язкова державна координація діяльності державних органів, органів місцевого самоврядування, підприємств, установ і організацій незалежно від форми власності в сфері забезпечення кібербезпеки держави;

– розвиток науково-практичних основ забезпечення кібербезпеки держави з урахуванням сучасної геополітичної ситуації, умов політичного і соціально-економічного розвитку України та реальності загроз застосування кіберзброї проти держави;

– забезпечення технологічної незалежності України в найважливіших галузях інформатизації, телекомунікації та зв'язку, що визначають її кібербезпеку, і, в першу чергу, в галузі створення кіберзброї, а також спеціалізованої обчислювальної техніки для зразків озброєння і військової техніки;

– розробка сучасних методів і засобів захисту інформації, забезпечення безпеки інформаційних технологій, перш за все, що використовуються в екологічно небезпечних та економічно важливих виробництвах;

– розвиток і вдосконалення державної системи захисту інформації та системи захисту державної таємниці;

– розширення взаємодії з міжнародними та зарубіжними органами і організаціями при вирішенні науково-технічних і правових питань забезпечення безпеки інформації, що передається за допомогою міжнародних телекомунікаційних систем і систем зв'язку;

– забезпечення умов для активного розвитку вітчизняної інформаційної інфраструктури в процесах створення і використання глобальних інформаційних мереж і систем;

– створення єдиної якісної системи підготовки кадрів в сфері кібербезпеки.

З метою створення ефективної національної системи забезпечення кібербезпеки можна виділити такі перспективні напрями удосконалення чинного законодавства у цій сфері на основі визначення основних перешкод та розробки шляхів їх подолання [2, с. 24-25]:

1) Необхідність створення повноцінного єдиного центру координації процесу розбудови національної системи забезпечення кібербезпеки, оскільки на сьогодні спостерігається неефективність та непрозорість діяльності Національного координаційного центру кібербезпеки (НКЦК) у сфері забезпечення кібербезпеки, незрозумілість його правових засад функціонування.

Створення НКЦК як робочого органу Ради національної безпеки і оборони України (РНБОУ), без сумніву, значно підвищило можливості щодо більш узгодженого співробітництва суб'єктів системи забезпечення кібербезпеки. Однак правовий статус цього державного органу до кінця не є зрозумілим, що призводить до того, що НКЦК фактично виступає інформаційно-експертним органом без належних повноважень щодо інших суб'єктів системи забезпечення кібербезпеки.

Розширення Угоди про асоціацію між Україною та ЄС та створення в Урядовому офісі з питань європейської та євроатлантичної інтеграції спеціального підрозділу з питань кібербезпеки дозволило б систематизувати висновки українських та міжнародних експертів щодо різних проєктів в галузі кібербезпеки, налагодити прямий контакт з експертами НАТО, ЄС, Ради Європи, ОБСЄ, інших організацій, зробити процес законотворчості у цій сфері більш прозорим, підзвітним та зрозумілим.

Як відомо, Кабінет Міністрів України 04.10.2017 р. ухвалив Постанову № 759 «Про Урядовий офіс координації європейської та євроатлантичної інтеграції» [3]. Цей документ регламентує діяльність Урядового офісу координації європейської та євроатлантичної інтеграції, який здійснює координацію діяльності органів виконавчої влади для системного планування та

виконання заходів державної політики згідно із зобов'язаннями України у сферах європейської та євроатлантичної інтеграції. Однією з функцій Офісу також є оцінка результатів такої діяльності.

Так, зазначений Урядовий офіс здійснює координацію діяльності органів виконавчої влади з розроблення та здійснення заходів, спрямованих на виконання Угоди про асоціацію між Україною та Європейським Союзом, а також спрямування та контроль політичного та політико-військового діалогу і практичного співробітництва з НАТО та державами-членами Північноатлантичного Альянсу.

Зокрема, ключовими завданнями Урядового офісу координації європейської та євроатлантичної інтеграції є [4]:

– координація процесу адаптації законодавства України до права Європейського Союзу (acquis ЄС) та стандартів і рекомендацій НАТО;

– аналіз залучення і використання міжнародної допомоги, спрямованої на підтримку виконання завдань у сферах європейської та євроатлантичної інтеграції;

– розроблення та реалізація стратегій, програм та інших документів з інформування громадськості та комунікації у сферах європейської та євроатлантичної інтеграції;

– забезпечення здійснення перекладу acquis ЄС українською мовою, оновлення глосарію термінів acquis ЄС;

– проведення спільних засідань органів асоціації Україна – ЄС та секретаріатство української частини таких органів;

– оцінка результативності виконання завдань у сферах європейської та євроатлантичної інтеграції.

У межах Урядового офісу координації європейської та євроатлантичної інтеграції є фахівці, які займаються експертизою законодавства України на відповідність праву ЄС.

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 та неможливості їх своєчасного усунення.

До цього слід додати, що відсутність єдиного центру збору інформації щодо кіберінцидентів ускладнює правильну обробку цієї інформації, яка переважно є конфіденційною.

Тому варто в найближчий час провести прозорий кібераудит об'єктів критичної інфраструктури України незалежними міжнародними аудиторськими компаніями.

3) Необхідність подолання недовіри та розвитку співробітництва між суб'єктами забезпечення кібербезпеки та суб'єктами національної системи кібербезпеки згідно із Законом України «Про основні засади забезпечення кібербезпеки України» [5].

Забезпечення достатнього рівня кібербезпеки держави неможливе без плідного співробітництва між суб'єктами забезпечення кібербезпеки та суб'єктами національної системи кібербезпеки, зокрема між суб'єктами національної системи кібербезпеки, постачальниками інформаційно-телекомунікаційних послуг, власниками (розпорядниками) об'єктів критичної інфраструктури та користувачами.

На жаль, у діяльності більшості силових органів, які входять у склад національної системи кібербезпеки, спостерігаються значні корупційні ризики. В цих умовах сподіватись на ефективність механізмів саморегуляції (хоча б на рівні «гарячих ліній» для скарг на кіберінциденти) і подальшої співпраці між постачальниками інформаційно-телекомунікаційних послуг, власниками (розпорядниками) об'єктів критичної інфраструктури та суб'єктами національної системи кібербезпеки не доводиться.

Не менш важливим є створення відповідних умов для розвитку індустрії кібербезпеки – як на фінансовому (пільги, проведення прозорих публічних закупівель (конкурсних торгів) на бюджетне фінансування тощо) та організаційному (затвердження прозорих та зрозумілих «правил гри» в індустрії кібербезпеки) рівнях.

Корисним кроком у цьому напрямку може стати укладання відповідних меморандумів між учасниками індустрії кібербезпеки (наприклад, кібераудиторами, саморегулівними організаціями у сфері забезпечення кібербезпеки) та відповідними суб'єктами національної системи кібербезпеки.

4) Доцільність активізації просвітницької діяльності, підвищення обізнаності населення у сфері забезпечення кібербезпеки, нарощування технологічного потенціалу з метою ефективного кіберзахисту.

Підвищення обізнаності у сфері забезпечення кібербезпеки, освіта та навчання у відповідності до чітко визначених пріоритетів, принципів, політики, процесів, програм кібербезпеки є надзвичайно важливим компонентом забезпечення достатнього рівня кіберзахисту у державі. Цим питанням повинно приділятися багато уваги на усіх рівнях – політичному, законодавчому, регуляторному, бізнесовому, волонтерському.

Потенційним напрямком досліджень у сфері забезпечення кібербезпеки та протидії кібертероризму повинні стати проєкти зі створення автоматизованих систем моніторингу кібербезпеки, що дозволяють виявляти кіберзагрози критично важливим об'єктам інформаційних інфраструктур, оцінити їх кореляцію і реагувати на них у режимі реального часу.

Висновки. Отже, на сьогоднішній день в Україні фактично відсутній єдиний центр координації роботи щодо законодавчого та нормативно-правового забезпечення ефективної системи кібербезпеки, яка б базувалась на комплексному аналізі наявного стану в цій сфері, викликів, існуючих та потенційних кіберзагроз, враховувала інтереси усіх суб'єктів системи кібербезпеки, інтегрувалась в європейську та глобальну міжнародну систему кібербезпеки, мала б достатнє фінансове, організаційне, технічне, кадрове забезпечення [2, с. 5]. НКЦК як робочий орган РНБОУ, на жаль, на основі обсягу виконуваних функцій таким єдиним центром координації роботи у сфері кібербезпеки так й не став.

Крім того, на державному рівні важливо здійснювати діяльність з профілактики кіберзлочинів у інформаційному просторі України. На наш погляд, попередження кіберзлочинності, зокрема кібертероризму, має здійснюватися одночасно в декількох напрямках [1, с. 45]:

1) стратегічний напрямок, який включає в себе довгострокове прогнозування кібертерористичної активності з визначенням можливих суб'єктів, які здійснюють кібератаки, і об'єктів атак останніх; випередження; блокування кібертероризму на «початковій» стадії, недопущення його становлення та розвитку;

2) виявлення об'єктів і суб'єктів кібертероризму, його причин, а також способів вчинення; запобігання кібертерористичним атакам, які могли б бути вчинені найближчим часом або в недалекому майбутньому;

3) запобігання, виявлення і припинення подібних до кібертероризму злочинів, як кібердіверсії, кіберекстремізм;

4) передача всього керування антикібертерористичною діяльністю низці спецслужб при невтручанні в їхню роботу будь-яких інших державних органів влади та управління.

Враховуючи досвід розвинених країн світу Україна має можливість запозичити дієві способи та методи щодо запобігання кіберзлочинам, у тому числі кібертероризму. Аналіз емпіричних даних щодо протидії кіберзлочинності у багатьох країнах-членах ЄС та США дозволяє дійти висновку про те, що вітчизняна система забезпечення кібербезпеки потребує вдосконалення, зокрема приведення у відповідність до міжнародних стандартів. З цією метою варто [6, с. 57]:

1) сформувати державну політику так, щоб можна було б забезпечити досконалу боротьбу з кіберзлочинністю, у тому числі кібертероризмом, та залучити до цієї проблеми одночасно громадські та урядові організації;

2) забезпечити технічний розвиток інновацій, що буде гарантувати кібербезпеку. Зокрема, Україна повинна створити високотехнічну систему для забезпечення надійності і безпеки зв'язку в кіберпросторі, інструменти «активного кіберзахисту», а враховуючи існуючий стан України в цих питаннях, це не є простим завданням;

3) удосконалити діяльність та переглянути повноваження спеціальних силових органів, які здійснюють боротьбу з кіберзлочинами.

Література

1. Кибертерроризм и информационная безопасность государства. СІДКОН. К., 2013. 50 с.

2. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Policy Paper). USAID. 2017. 28 с.

3. Про Урядовий офіс координації європейської та євроатлантичної інтеграції: Постанова Кабінета Міністрів України від 04.10.2017 р., № 759. URL: https://zakon.rada.gov.ua/laws/show/759-2017-п#Text.

4. Урядовий офіс координації європейської та євроатлантичної інтеграції. URL: https://eu-ua.org/uryadovyy-ofis-koordynaciyi-yevropeyskoyi-ta-yevroatlantychnoyi-integraciyi.

5. 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.

6. Шесть стран создали кибернетические войска Евросоюза. URL: http://eurasian-defence.ru/?q=novosti/shest-stran-sozdali.

Анотація

Когут Ю. І. **Перспективні напрями удосконалення захисту інформаційного простору України від загроз кібертероризму.** – Стаття.

У статті визначені основні напрями боротьби з кібертероризмом, завдання забезпечення кібербезпеки, перспективні напрями удосконалення чинного законодавства у цій сфері. З метою створення ефективної національної системи забезпечення кібербезпеки запропоновано створити повноцінний єдиний центр координації процесу розбудови національної системи забезпечення кібербезпеки, оскільки на сьогодні спостерігається неефективність та непрозорість діяльності Національного координаційного центру кібербезпеки (НКЦК) у сфері забезпечення кібербезпеки, незрозумілість його правових засад функціонування. Автором з'ясовано, що НКЦК фактично виступає інформаційно-експертним органом без належних повноважень щодо інших суб'єктів системи забезпечення кібербезпеки. Доведено, що розширення Угоди про асоціацію між Україною та ЄС та створення в Урядовому офісі з питань європейської та євроатлантичної інтеграції спеціального підрозділу з питань кібербезпеки дозволило б систематизувати висновки українських та міжнародних експертів щодо різних проєктів в галузі кібербезпеки, налагодити прямий контакт з експертами НАТО, ЄС, Ради Європи, ОБСЄ, інших організацій, зробити процес законотворчості у цій сфері більш прозорим, підзвітним та зрозумілим. Поряд з цим, у статті наголошено на доцільності 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 критично важливим об'єктам, кібе-

рінцидентів та неможливості їх своєчасного усунення. Автором також обґрунтована необхідність подолання недовіри та розвитку співробітництва між суб'єктами забезпечення кібербезпеки та суб'єктами національної системи кібербезпеки згідно із Законом України «Про основні засади забезпечення кібербезпеки України». Наостанок, аналіз емпіричних даних щодо протидії кіберзлочинності у багатьох країнах-членах ЄС та США дозволив автору дійти висновку про те, що вітчизняна система забезпечення кібербезпеки потребує вдосконалення, зокрема приведення у відповідність до міжнародних стандартів.

Ключові слова: кібертероризм, кібербезпека, критично важливі об'єкти, кібератаки, кіберпростір, кіберзахист, критична інфраструктура, кіберзагроза, кіберзброя, національна система кібербезпеки, кіберінцидент, кібераудит.

Аннотация

Когут Ю. И. **Перспективные направления совершенствования защиты информационного пространства Украины от угроз кибертерроризма.** – Статья.

В статье определены основные направления борьбы с кибертерроризмом, задача обеспечения кибербезопасности, перспективные направления совершенствования действующего законодательства в этой сфере. С целью создания эффективной национальной системы обеспечения кибербезопасности предложено создать полноценный единый центр координации процесса развития национальной системы обеспечения кибербезопасности, поскольку сегодня наблюдается неэффективность и непрозрачность деятельности Национального координационного центра кибербезопасности (НКЦК) в сфере обеспечения кибербезопасности, непонятность его правовых основ функционирования. Автором установлено, что НКЦК фактически выступает информационно-экспертным органом без надлежащих полномочий относительно других субъектов системы обеспечения кибербезопасности. Доказано, что расширение Соглашения об ассоциации между Украиной и ЕС и создание в Правительственном офисе по вопросам европейской и евроатлантической интеграции специального подразделения по вопросам кибербезопасности позволило бы систематизировать выводы украинских и международных экспертов по различным проектов в области кибербезопасности, наладить прямой контакт с экспертами НАТО, ЕС , Совета Европы, ОБСЕ, других организаций, сделать процесс законотворчества в этой сфере более прозрачным, подотчетным и понятным. Наряду с этим, в статье отмечено целесообразность проведения прозрачного кибераудиту объектов критической инфраструктуры, поскольку отсутствие общего понимания существующего положения национальной системы обеспечения кибербезопасности, достоверных оценок, статистических данных по этим вопросам приводит к неправильной идентификации киберугроз критически важным объектам, киберинцидентив и невозможности их своевременного устранения. Автором также обоснована необходимость преодоления недоверия и развития сотрудничества между субъектами обеспечения кибербезопасности и субъектами национальной системы кибербезопасности согласно Закону Украины «Об основных принципах обеспечения кибербезопасности Украины». Напоследок, анализ эмпирических данных по противодействию киберпреступности во многих странах-членах ЕС и США позволил автору сделать вывод о том, что отечественная система обеспечения кибербезопасности нуждается в совершенствовании, в частности приведение в соответствие с международными стандартами.

Ключевые слова: кибертерроризм, кибербезопасность, критически важные объекты, кибератаки, киберпространство, киберзащита, критическая инфраструктура, киберугрозы, кибероружие, национальная системакибербезопасности,киберинцидент,кибераудит.

Summary

Kohut Yu. I. **Promising areas for improving protection information space of Ukraine from the threats of cyberterrorism.** – Article.

The article identifies the main areas of the fight against cyberterrorism, the task of ensuring cybersecurity, promising areas for improving existing legislation in this area. In order to create an effective national cybersecurity system, it is proposed to create a full-fledged single coordination center for the process of building a national cybersecurity system, as currently there is inefficiency and non-transparency of the National Cyber Security Coordination Center (NCCC) in the field of cybersecurity. The author found that the NCCC actually acts as an information and expert body without proper authority over other actors in the cybersecurity system. It is proved that the expansion of the Association Agreement between Ukraine and the EU and the creation of a special unit on cybersecurity in the Government Office for European and Euro-Atlantic Integration would allow systematizing the conclusions of Ukrainian and international experts on various cybersecurity projects, establishing direct contact with NATO experts. , The Council of Europe, the OSCE and other organizations, to make the law-making process in this area more transparent, accountable and understandable. In addition, the article emphasizes the need for transparent cyber audits of critical infrastructure, as the lack of a common understanding of the current state of the national cybersecurity system, reliable assessments, statistics on these issues leads to incorrect identification of cyber threats to critical facilities, cyber incidents and impossibility of their timely elimination. The author also substantiated the need to overcome mistrust and develop cooperation between the subjects of cybersecurity and the subjects of the national cybersecurity system in accordance with the Law of Ukraine «On Basic Principles of Cybersecurity of Ukraine». Finally, the analysis of empirical data on combating cybercrime in many EU member states and the United States allowed the author to conclude that the domestic cybersecurity system needs to be improved, in particular in line with international standards.

Key words: cyberterrorism, cybersecurity, critical objects, cyber attacks, cyberspace, cyber defense, critical infrastructure, cyber threat, cyber weapons, national cyber security system, cyber incident, cyber audit.