

УДК 343.9(082)

НЗ4

Редакційна колегія:

Вдовічен Віталій Анатолійович, доктор юридичних наук, доцент, декан юридичного факультету Чернівецького національного університету імені Юрія Федьковича;

Жаровська Галина Петрівна, докторка юридичних наук, доцентка, завідувачка кафедри кримінального права Чернівецького національного університету імені Юрія Федьковича;

Stoica Adrian – PhD. Habilitat, Professor, Dean of the Faculty of Law and Administrative Sciences, Ovidius University of Constanta, Romania.

Ботнару Стела – докторка юридичних наук, доцентка, заступниця декана юридичного факультету Молдовського державного університету, Молдова.

Nina Kaiser – Hans Gross Centre for interdisciplinary criminal sciences, Institut of Criminal Law, Criminal Procurement Law and Criminology, University of Graz.

Кунчев Йонко – доктор юридичних наук, професор Варненського вільного університету імені Чорноризця Храбра (Болгарія).

Балук Ігор Григорович – директор Чернівецького науково-дослідного експертно-криміналістичного центру МВС .

НЗ4

III Наукові читання пам'яті Ганса Гросса : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівец. нац. у-нт. ім. Ю.Федьковича, 2023. 260 с.

ISBN 978-966-423-838-7

Матеріали викладено в авторській редакції. Відповідальність за їхню якість, достовірність, а також відсутність у них відомостей, що становлять державну таємницю та інформацію для службового користування, несуть автори.

УДК 343.9(082)

ISBN 978-966-423-838-7

©Чернівецький національний університет
імені Юрія Федьковича, 2023

Навроцька В.В. Вимоги до клопотання про застосування примусових заходів медичного характеру з огляду на практику Європейського суду з прав людини	163
Попович О.В. Умови правомірності спричинення шкоди за згодою людини	166
Продан Т.В. Кібертероризм в умовах сьогодення.....	171
Родіонова Т.В. Кримінальні правопорушення в умовах воєнного стану	175
Смирнов М.І. Проблеми притягнення до відповідальності за злочин агресії проти України	180
Ткаченко К.В. Кримінально-правовий інститут реституції та компенсації в умовах євроінтеграції.....	185
Тома М.Г. Вік суб'єкта кримінального правопорушення та його вплив на кримінальну відповідальності.....	191
Фігурський В.М. Доктринальні підходи розуміння доказів та унормування способів їх використання у кримінальному процесуальному праві європейських держав	196
Юрчишин В.М. Функції процесуального керівника в умовах воєнного стану	202
Юрчишин П.В. Особливості провадження контролю за вчиненням злочину в умовах воєнного стану.....	205
Ющик О.І. Правові аспекти застосування пробаційної програми для кривдників	209
Трибуна Молодого Науковця	215
Доголич І.В. Принцип юридичної визначеності в умовах трансформації кримінального законодавства	215
Єленчук К.В. Актуальні питання кримінальної відповідальності за порушення законів та звичаїв війни	219

Продан Т.В.,
кандидат юридичних наук, доцент,
асистент кафедри кримінального права,
Чернівецький національний університет імені Юрія Федьковича,
м. Чернівці, Україна

КІБЕРТЕРОРИЗМ В УМОВАХ СЬОГОДЕННЯ

Протягом останніх років стрімкий прогрес та широке впровадження інформаційних технологій, що застосовуються практично у всіх сферах людського життя, суттєво полегшили передачу інформації завдяки використанню телекомунікаційних мереж. Однак, цей розвиток породив низку проблем, пов'язаних із забезпеченням безпечних умов використання кіберпростору. Це зробило сферу кіберпростору досить привабливою для злочинців, оскільки такий розвиток відкрив їм нові можливості. Так, відповідно до висновків експертів контррозвідувальних служб, кібертерористи використовують електронну пошту для передачі інструкцій, карт, схем, паролів та іншої значущої інформації у зашифрованій формі [5, с. 575]. Розголошення цієї інформації може зашкодити національній безпеці держави.

Також, варто відзначити, що кібертероризм не має державних кордонів, і відповідно є транскордонним злочином. А це свідчить про те, що кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці світу шляхом використання спеціального програмного забезпечення, призначеного для несанкціонованого втручання в комп'ютерні мережі та здійснення віддалених кібератак на інформаційні ресурси потенційної жертви [1, с. 65]. Звідси випливає, що кібертероризм представляє загрозу не лише для національної, але й для міжнародної безпеки загалом.

Що ми розуміємо під кібертероризмом? Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням [6]. Визначення, яке наведене у законі, на нашу думку, є дуже скупим та зовсім не розкриває його повноцінної суті. Існують різні доктринальні напрацювання у сфері визначення досліджуваного явища, проте єдиного чіткого визначення поняття «кібертероризму» як на національному, так і на міжнародному рівнях немає. Більшість науковців

дійшли висновку, що під кібертероризмом необхідно розуміти: «навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя та здоров'я людей або настання інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту» [8].

Як відзначають науковці, основною формою кібертероризму є атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних та інші складові інформаційної інфраструктури. Ці атаки здійснюються злочинними групами або окремими фізичними особами. Результатом таких атак є проникнення в інформаційно-телекомунікаційні мережі або комунікаційну інфраструктуру, захоплення управління, пригнічення засобів мережевого інформаційного обміну та інші деструктивні дії. Ефективність же форм та методів кібертероризму залежить від особливостей інформаційної інфраструктури та рівня її захищеності [4].

Протягом останніх років Україна все більше відчуває масштаби кібернетичних атак та їх негативні наслідки. Так, Україна зазнає кібератак різної потужності, починаючи ще з 2014 року. Однією з найбільш масштабних та наслідкових була атака, що призвела до поширення вірусу NotPetya, який 27 червня 2017 року атакував численні комп'ютерні системи українських державних та комерційних установ. За оцінками експертів від Microsoft та ESET, ця кібератака зачепила принаймні 65 країн. З'ясовано, що основною метою цієї кібератаки була саме Україна [3]. Ще до повномасштабного вторгнення російської федерації в лютому 2022 року експерти з кібербезпеки прогнозували збільшення проявів кібертероризму в Україні. Починаючи з моменту повномасштабного вторгнення російською федерацією Україна стала об'єктом чисельних кібератак, які зачепили державні установи, приватні організації та громадян. У 2022 році російська федерація втричі збільшила кількість таких атак на Україну [9]. Як бачимо, що наша держава не зможе оперативно реагувати на кібертерористичні акти та є зовсім беззахисною перед скерованими кібератаками.

Для своєчасного виявлення та відповідного реагування на відповідні кіберзагрози в Україні діє ефективний орган «CERT-UA» – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації, який співпрацює з Службою зовнішньої розвідки. Відповідно до

своєї діяльності фахівці даного структурного підрозділу підготували аналітичний звіт за перше півріччя 2023 року «Російські кібероперації: зміна тактик, цілей і спроможностей хакерських груп уряду рф та контрольованих ним угруповань». У своєму звіті вони відзначили, що у першому півріччі 2023 року постійну діяльність здійснюють щонайменше 23 російських кібертерористичних хакерських угруповань. Усі вони переслідують різні цілі, зокрема й воєнні, та атакують як державний, так і приватний сектори. Серед найбільш активних, небезпечних та дієздатних груп – Gamaredon (контрольована ФСБ росії) та Sandworm (діяльність асоціюють із Головним управлінням Генерального штабу Збройних сил російської федерації, раніше відомого як ГРУ) [2].

Очевидно, що актуальність цієї загрози буде продовжувати зростати в майбутньому, відповідно до розвитку та поширення інформаційно-телекомунікаційних технологій. Рівень кібертерористичних загроз проти України, як бачимо, збільшується в умовах повномасштабного вторгнення. Особливо помітно значущий ріст кількості кібератак на державні інформаційні ресурси та об'єкти критичної інфраструктури України з боку російських хакерів.

Таким чином, незважаючи на всі позитивні зрушення на законорачому рівні у даній сфері, загроза кібертероризму в даний час залишається дуже серйозною проблемою. Наше законодавство потребує ще більшого вдосконалення та подальшого забезпечення механізмів протидії кібертероризму. Зокрема, необхідно відзначити, що проєкт нового Кримінального кодексу України передбачає встановлення кримінальної відповідальності за вчинення терористичного акту з використанням кібертероризму. А саме у статті 7.2.4. проєкту КК України зазначається, що у терористичному акті визнається винною особа, яка: «...незаконно втрутилася в роботу інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної комунікаційної мережі» [7].

Отже, як ми вже зазначили, кібертероризм має транснаціональний характер, а тому доцільним є налагодження міжнародного співробітництва як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства. Міжнародні організації такі як: ООН, ОБСЕ, Інтерпол, ЄС та ряд інших установ та організацій відіграють важливу роль у координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі з цим негативним явищем.

Література:

1. Білан І.А. Кібертероризм: інформаційно-правовий аспект. *Інформація і право*. 2023 № 4 (47). С. 64-71.
2. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/proti-ukrayini-pracyuyut-shonaimenshe-23-rosiiski-kiberterroristichni-khakerski-grupi> (дата звернення: 02.12.2023).
3. Інформаційна безпека та кібербезпека держави: аналітична доповідь до Щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». Київ: Національний інститут стратегічних досліджень, 2017. С. 47-56.
4. Конрі-Мюррей Е. Політика безпеки в часи терору. URL: <http://www.osp.ru/lan/2002/02/083.htm> (дата звернення: 03.12.2023).
5. Лисько Т.Д. Інформаційний тероризм як загроза національній безпеці та спосіб інформаційної війни. *Юридичний науковий електронний журнал*. 2022. № 10. С. 574-576.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 02.12.2023).
7. Проект Кримінального кодексу України станом на 14.10.2023 року. URL: <https://newcriminalcode.org.ua/upload/media/2023/10/15/kontrolnyj-tekst-proyektu-kk-14-10-2023.pdf> (дата звернення: 03.12.2023).
8. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf (дата звернення: 02.12.2023).
9. Victor Zhora. State Service of Special Communications and Information Protection of Ukraine. *Russia's Cyber Tactics: Lessons Learned*. 2022. URL: <https://cip.gov.ua/en/news/russia-scyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwaragainst-ukraine> (дата звернення: 02.12.2023).