УДК [351.74:004](477)(08)
П83

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх справ
від 18.01.2023 № 3

Протидія кіберзлочинності та торгівлі людьми :
П83 зб. матеріалів міжнарод. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2023. – 176 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі; проаналізовано питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми; кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу; розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

УДК [351.74:004](477)(08)

Матеріали викладено в авторській редакції з незначними коректорськими правками. За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних назв, географічних назв, а також за розголошення фактів, що не належать відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.

Електронна копія збірника розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари та круглі столи», а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

злочину передбачають, що: 1) виконавець залучив особу у вчинення одного чи кількох актів сексуального характеру; 2) діяння було скоєно у рамках широкомасштабного чи систематичного нападу на цивільне населення; 3) виконавець знав, що діяння є частиною широкомасштабного чи систематичного нападу на цивільне населення, або мав намір зробити його частиною такого нападу. За наявності цих особливих умов діяння має бути кваліфіковане за ст. 438 КК України.

Іншим воєнним злочином, який відповідає ознакам торгівлі людьми, що полягала у переміщенні людини, вчиненому з метою експлуатації, є переміщення прямо або опосередковано державою, що окупує, частини її власного цивільного населення на окуповану нею територію, або депортація чи переміщення населення окупованої території або окремих частин його в межах або за межі цієї території (пп. «viii» п. «а» ч. 2 ст. 8 Римського статуту). Кваліфікація цього діяння як порушення законів і звичаїв війни за ст. 438 КК України можлива за наявності таких спеціальних умов: 1) виконавець: а) перемістив, прямо чи опосередковано, частину свого власного населення на окуповану ним територію; або б) депортував або перемістив населення окупованої території або окремі частини їх у межах або межі цієї території; 2) дія мала місце в контексті міжнародного збройного конфлікту та була пов’язана з ним; 3) виконавець усвідомлював фактичні обставини, що засвідчували про існування збройного конфлікту.

Одержано16.04.2023

УДК 004.771.34.096

ЛОСИНЕЦЬ Аліна Сергіївна,
студентка 3 курсу
Криворізького навчально-наукового інституту
Донецького державного університету внутрішніх справ
https://orcid.org/0009-0000-5849-9615;

ВЕСЕЛОВ Микола Юрійович,
доктор юридичних наук, професор,
професор кафедри державно-правових дисциплін факультету № 2
Криворізького навчально-наукового інституту
Донецького державного університету внутрішніх справ
https://orcid.org/0000-0002-3963-2764

КІБЕРЗЛОЧИННІСТЬ І ЗАХОДИ ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У наші дні використання інформаційних технологій пронизує майже усі сфери життя. «Віртуальний світ» вбирає від реального не лише позитивні, а й негативні його прояви, зокрема з розвитком ІТ-технологій та віртуального середовища відбувається і трансформація злочинних проявів. Кожен знає про такий вид злочинності як кіберзлочинність Цей вид включає в себе різні форми правопорушень, що здійснюються в мережі Інтернету, з огляду на що постає актуальне питання, як саме убезпечити себе чи суспільні (державні) інтереси від цих негативних проявів.

Кіберзлочини – це кримінальні правопорушення, вчинені в кіберпросторі за допомогою спеціальних пристроїв (комп’ютерів, смартфонів, планшетів, терміналів

та інших), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, та пов'язані з протиправним, несанкціонованим створенням, зберіганням, обробкою, підробкою, блокуванням, знищенням об'єктів інформаційної інфраструктури [1]. Поширене використання зазначених гаджетів, інформатизація комунікативних зв'язків на побутовому (приватному) та публічному рівнях, а також діджиталізація багатьох соціально-економічних відносин привертає дедалі більше уваги до цих ресурсів і з боку злочинного контингенту. При цьому спостерігається трансформація і цієї категорії зловмисників: вони стають винахідливішими, технічно розвинутими, умовно кажучи, постійно «тримають руку на пульсі» сучасних технологічних перетворень та соціальних катаклізмів. Слід зазначити, що *кіберзлочинність* стає міжнародним та глибоко інтегрованим у різні соціальні процеси явищем, заснованим на тотальному користуванні людством, бізнесом, владою Інтернет-мережами.

Класифікувати цей вид кримінальних правопорушень можна за наступним типом: 1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема: незаконний доступ, наприклад, шляхом злому, обману та іншими засобами; нелегальне перехоплення комп'ютерних даних; втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру; зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів; 2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів; 3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія; 4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг [2].

Питання кібербезпеки перебувають на особливому контролі з боку міжнародної спільноти, про що свідчить прийнята 23.11.2001 р. Конвенція про кіберзлочинність. Ратифікація цієї Конвенції в Україні (07.09.2005 р.) спонукало до вжиття низки організаційно-правових заходів, зокрема утворення спеціальних підрозділів у складі правоохоронних органів держави.

Викликає стурбованість висока латентність даного виду правопорушень – 95%, тобто шанси у злодія бути виявленим дуже низькі. На нашу думку, такий стан речей обумовлений низкою суб'єктивно-об'єктивних причин: відсутність достатньої кількості фахівців за даним напрямком у складі правоохоронних органів, необхідних технічних ресурсів (при тому, що Україна має достатньо багато кваліфікованих «ІТ-ишників»); небажання самих людей звертатися до правоохоронних органів та повідомляти про скоєний щодо них злочин (це обумовлено низьким рівнем довіри до ефективності правового захисту з правоохоронців); використання злочинцями сучасних новітніх інформаційних технологій та засобів шифрування інформації (криптографія, стеганографія тощо), які потребують спеціальної освіти та високого інтелектуального рівня.

Задля протидії різним проявам кіберзлочинності НАТО у 2011 році розпочала формулювати концепцію Групи швидкого реагування. Створення цієї групи стало результатом перегляду політики кіберзахисту НАТО, яка була переглянута міністрами оборони в червні 2011 року. Зазначені фахівці з кіберзахисту відповідальні за надання допомоги країнам-членам, які звертаються по допомогу в разі нападу національного значення [3. с 182]. Заслуговує на увагу досвід німецьких правоохоронців у даркнеті (до речі, придбати там можна будь-що, від підроблених товарів відомих брендів до зброї та наркотиків). В Мюнхені в 2015 році чоловік придбав зброю саме з даркнету та вбив 9 людей. Близько 140 співробітників федерального відомства кримінальної поліції відповідають саме за кіберзлочинність і саме даркнет є одним з напрямків їх роботи. На міжнародному рівні у співпраці з німецькою кримінальною поліцією було закрито понад 30 торговельних майданчиків та відкрито справи проти їх адміністраторів, а також найважливіших торговців та клієнтів [4].

Тож, основними заходами боротьби з кіберзлочинністю та покращення кібербезпеки в Україні має бути: зміцнення кваліфікованого кадрового та технічно-ресурсного потенціалу спеціальних підрозділів правоохоронних органів; продовження освітньо-профілактичних заходів серед населення країни щодо інформаційної обізнаності; додаткові технічні, організаційні та правові (включаючи посилення юридичної відповідальності) заходи захисту конфіденційної інформації тощо.

Список використаних джерел

1. Кривенко К. Кіберзлочинність: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika (дата звернення: 07.04.2023).

2. Пфо О. М. Основні поняття і класифікація кіберзлочинності. Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукраїнської науково-практичної конференції (м. Кропивницький, 23–25 листоп. 2016 року). Кропивницький, 2016. С. 33–34. URL: https://core.ac.uk/download/pdf/84825482.pdf (дата звернення: 07.04.2023).

3. Войціховський А. В. Діяльність НАТО у боротьбі з кіберзлочинністю. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали Міжнародної науково-практичної конференції (м. Харків, 12 листоп. 2014 р.). Харків, 2014. С. 181–184. URL: https://univd.edu.ua/general/publishing/konf/76.pdf (дата звернення: 07.04.2023).

4. Фон Гайн М., Мехед Н. Як німецькі слідчі борються зі злочинністю у «даркнеті» (29.07.2016). URL: https://www.dw.com/uk/боротьба-з-кіберзлочинністю-німецькі-слідчі-беруть-даркнет-у-поле-зору/a-19432742 (дата звернення: 07.04.2023).

Одержано 18.04.2023