

Проаналізувавши все вище сказане, можемо дійти до таких висновків. Проблема кібербулінгу є досить актуальною на сьогоднішній час і потребує подальшого вивчення та напрацювання нового теоретичного матеріалу, що дасть можливість втілити його на практиці під час профілактичних заходів щодо віртуального насильства. Необхідно також звернути увагу на те, що діяння у чинному законодавстві України не криміналізоване. В майбутньому, доречним є розгляд питання щодо криміналізації досліджуваного феномену.

Список бібліографічних посилань

1. Найдюнова Л. А. Медіапсихологія: основи рефлексивного підходу: підручник / Нац. акад. пед. наук України, Ін-т соц. та політ. психології. Вид. 2-ге, стер. Кіровоград : Імекс-ЛТД, 2015. 244 с.
2. Бочавер А. А., Хломов К. Д. Кибербуллинг: травля в пространстве современных технологий. *Психология. Журнал Высшей школы экономики*. 2014. Т. 11(3). С. 177-191.
3. Aiken M. UK London: Hachette; 2016. The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behaviour Changes Online, Aug 18; pp. 119–138.

Одержано 31.10.2018

УДК 343.231

Михайло Васильович ГУЦАЛЮК,

кандидат юридичних наук, доцент,

провідний науковий співробітник

Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України;

Тетяна Сергіївна ПЕРЕДЕРІЙ,

слухач магістратури факультету № 6

Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПРОБЛЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Сьогодні в Україні суттєво збільшується рівень злочинності у сфері використання комунікаційних систем із застосуванням мережі Інтернет, що негативно впливає на забезпечення національної безпеки держави. Злочини з використанням інформаційно-комунікаційних технологій не лише гальмують впровадження позитивних тенденцій розвитку, а й формують нові інструменти у вчиненні злочинів.

За даними Департаменту кіберполіції Національної поліції України, за перше півріччя 2018 року було виявлено понад 2, 3 тисячі кримінальних правопорушень у сфері протидії кіберзлочинності [2].

Кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється і йде в ногу з

технологіями, що у свою чергу ускладнює виявлення та протидію зазначеним протиправним діям [3].

У Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, визначено поняття «кіберзлочин» та «кіберзлочинність», однак конкретний перелік таких злочинів відсутній. Відповідно до п. 2 ст. 4 цього ж закону об'єктами кіберзахисту є: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [4].

Основними елементами криміналістичної характеристики кіберзлочинів є: відсутність державних кордонів у кіберпросторі, складність виявлення місця вчинення злочину (їх може бути кілька), відсутність безпосереднього контакту з постраждалою фізичною чи юридичною особою, а також необхідність збору, зберігання та аналізу електронних (цифрових) доказів.

Слід зазначити, що для ефективного проведення розслідування кіберзлочинів вкрай важливим є вміння та практичні навички працівників правоохоронних органів у роботі з електронними доказами, правильність їх збору та зберігання, а також проведення їхнього аналізу. Тому процесуальні дії з електронними доказами мають регулюватися Кримінально-процесуальним кодексом України і супроводжуватися посиленням кримінальної відповідальності за вчинення кіберзлочинів.

Як показує практика, не всі організаційно-технічні процедури можливо описати в законі, однак ефективні способи протидії кіберзлочинності мають включати: постійне вдосконалення методів та прийомів розслідування, розробку нових способів виявлення та дослідження обставин вчинення таких злочинів, забезпечення технічної оснащеності органів досудового розслідування.

На нашу думку, процедура отримання оперативної інформації має регулюватися в рамках чинного законодавства та відповідно укладеного Меморандуму про співпрацю між постачальниками послуг і правоохоронними органами.

Згідно зі статистикою Національної поліції України, у 2017 році ст. 361-363-1 КК України пред'явлено обвинувачення 154 особам. За даними судової статистики, у цьому ж році за вищезазначеними статтями було засуджено всього 42 особи: з яких позбавлено волі 5 осіб на строк до 3 років та тільки 2 особи на строк від 3 до 5 років.

Крім того, характер кіберзлочинів вимагає створення міждержавної взаємодії у протидії цим злочинам, що неможливо без міжнародного співробітництва. Одним з основних документів, що регулює порядок проведення розслідувань кіберзлочинів є європейська Конвенція про кіберзлочинність. Важливим положенням «Конвенції» є можливість приймати законодавчі та інші заходи, які уповноважують її компетентні власті конфіскувати або подібним чином забезпечити від знищення дані, які є у провайдера і необхідні для розслідування. Це дає можливість правоохоронним органам проводити розслідування таких злочинів або вживати дії для збереження даних, які можуть бути знищені після закінчення певного моменту часу [5]. Участь у проведенні спільних міжнародних операціях таких, наприклад, як «Avalanche» у 2016 р., у якій були задіяні правоохоронці з понад 40 країн, проведені одночасні обшуки у 37 локаціях, та заарештовані як організатори так і співучасники великої міжнародної організованої злочинної організації.

Висновок. Ефективний контроль негативних явищ у кіберпросторі, таких як кіберзлочинність, вимагає набагато більших зусиль: постійне вдосконалення методів та прийомів розслідування, розробку нових способів виявлення та дослідження обставин вчинення таких злочинів, забезпечення технічної оснащеності органів досудового розслідування. Крім того, має бути внесено зміни у чинне законодавство, зокрема щодо посилення кримінальної відповідальності за кіберзлочини, а також дії з електронними доказами мають регулюватися Кримінально-процесуальним кодексом України.

Список бібліографічних посилань

1. Від початку року в Україні виявили 2,3 тисячі кіберзлочинів // ЦЕНЗОР.НЕТ. 14.07.2018 18:05. URL: https://ua.censor.net.ua/photo_news/3076614/vid_pochatku_roku_v_ukrayini_vyavyly_23_tysyachi_kiberzlochyniv_np_u_infografika (дата звернення: 30.10.2018).
2. Кіберполіція відмічає збільшення кількості правопорушень у сфері платіжних систем та кібербезпеки // Офіційний сайт кіберполіції України. 14 липня 2018 р. 13:36. URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-vidmichaye-zbilshennya-kilkosti-pravoporushen-u-sferi-platizhnyx-system-ta-kiberbezpeky-1519/> (дата звернення: 30.10.2018).
3. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 30.10.2018).
4. Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2011. № 4. С. 27-30. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/FP_index.htm_2011_4_6.pdf (дата звернення: 30.10.2018).

Одержано 31.10.2018