Список використаних джерел

1. 67 % дітей в Україні зазнали цькувань у попередні 2–3 місяці. URL: https://humanrights.org.ua/material/67_ditej_v_ukrajini_zaznali_ckuvan_u_poperedni_23_misjiaci.
2. Український інститут дослідження екстремізму. Дослідження «Стоп шкільний терор. Профілактика та протидія булінгу». URL: http://uire.org.ua/wpcontent/uploads/2017/11/Doslidzhennya-buling.pdf.
3. Найдьонова Л. А. Кібер-булінг або агресія в інтернеті: способи розпізнання і захист дитини : метод. рек. Вип. 4. Київ, 2011. 34 с.
4. Насилля в школі. URL: https://familytimes.com.ua/harakter/kiberbuling.https://glavcom.ua/specprojects/stopbullying/kiberbuling-novitni-nebezpeki-v-internet-prostori-460488.html.
5. Звернення про боулінг. URL: https://www.5.ua/suspilstvo/torik-v-ukraini-narakhuvaly-maizhe-110-tys-zvernen-pro-bulinh-175437.html.
6. Булінг як різновид катувань серед неповнолітніх. URL: http://www.nusta.edu.ua/wp-content/uploads/Жеброва Анастасія Олександрівна/pdf.
7. Депутати пропонують штрафувати за цькування дітей у школі. URL: https://expres.online/archive/news/2018/07/11/301122-deputaty-proponuyut-shtrafuvaty-ckuvannya-ditey-shkoli.

Леонов Б. Д.,
провідний науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ, доктор юридичних наук, старший науковий співробітник;
Серьогін В. С.,
науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ

ПОНЯТТЯ КІБЕРЗЛОЧИННОСТІ: ДИСКУСІЯ ТРИВАЄ

Сьогодні стрімкий розвиток інформаційних технологій, масштаб застосування глобальних телекомунікаційних мереж, розробка новітніх телекомунікаційних пристроїв створює умови для зростання злочинності у сфері комп'ютерної інформації як в Україні, так і за її межами. Масштаб та рівень суспільно небезпечних наслідків кіберзлочинності обумовлюють необхідність впровадження адекватних підходів щодо удосконалення кримінально-правового забезпечення протидії кіберзлочинності.

Останнім часом у теорії кримінального права загострилася дискусія щодо проблеми визначення поняття кіберзлочинності. З'ясування цього питання має велике значення для визначення напрямків кримінально-правової боротьби з кіберзлочинністю в цілому та кіберзлочинами зокрема.

Законом України «Про основні засади забезпечення кібербезпеки України» «кіберзлочин» (комп'ютерний злочин) визначається як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

На думку фахівців ГНЕУ Апарату Голови Верховної Ради України, цей термін має бути узгоджений із Кримінальним кодексом України (далі – КК України), який містить окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», де використовується термін «комп'ютерний злочин» [2].

Схожої точки зору додержуються фахівці Головного юридичного управління Апарату Голови Верховної Ради України, які дійшли висновку, що наведене в проекті Закону України «Про основні засади забезпечення кібербезпеки України» (реєстраційний №2126а) визначення кіберзлочинності як сукупності кіберзлочинів є яскравим прикладом порушення базових правил формальної логіки, що мають застосовуватися при формулюванні визначень, оскільки дефініція кіберзлочинності містить у собі так зване «коло» – визначаюче поняття, фактично, буквально повторює визначуване поняття. Запропонована редакція поняття «кіберзлочин» насправді складається з дефініцій, відповідно, злочину, яке вже використовується в чинних нормативно-правових актах, з додаванням словосполучення «в кіберпросторі» [3].

На помилковість застосування категорії «кіберпростір» у визначенні кіберзлочину звертає увагу М. В. Карчевський, на думку якого зміст інформаційного середовища не може розглядатися як вид певного простору чи території у класичному розумінні [4, с. 12].

Т. Тропіна пропонує визначати кіберзлочинність як винне вчинене суспільно небезпечне кримінальне каране втручання у роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, вчинені за допомогою комп'ютерів, комп'ютерних програм, комп'ютерних мереж, а також за допомогою інших засобів доступу [5, с. 38]. До речі, залишається невирішеною проблема співвідношення «кіберзлочину» з такими поняттями, як «комп'ютерний злочин», «злочин у сфері використання комп'ютерів», «злочин у сфері використання комп'ютерних технологій».

Найбільш поширеним у вітчизняній юридичній літературі є підхід, згідно з яким до кола комп'ютерних злочинів слід відносити всі суспільно небезпечні посягання, при вчиненні яких комп'ютери використовуються як технічні засоби [6; 7]. Тобто, в основу такої класифікації злочинів покладено ознаки, що характеризують засоби, які використовуються при їх вчиненні. Але самі по собі засоби не змінюють сутності злочину. Отже, такий підхід не позбавлений недоліків з огляду на його невідповідність головному принципу структурування національного законодавства про кримінальну відповідальність – систематизації кримінального закону на підставі класифікації злочинних посягань за об'єктом. Визначення нової групи злочинів має проводитися з урахуванням ознак, що характеризують об'єкт злочинного посягання. Саме тому у межах національного кримінально-правового дискурсу необґрунтованим вбачається виділяти певні групи злочинів на основі ознак, що характеризують спосіб, знаряддя чи засоби злочину [6, с. 11; 8, с. 22].

Між тим, визначення комп'ютерних злочинів (кіберзлочинів) як групи посягань, які характеризуються загальними ознаками способу, засобу чи знаряддя, може бути цілком затребуване з позиції криміналістики [4, с. 13]. В межах останньої йдеться про встановлення особливостей методики виявлення, розслідування злочинців цієї категорії, фіксації їх слідів тощо. До речі, у вітчизняній юридичній літературі термін «комп'ютерний злочин» спочатку застосовувався в криміналістичному аспекті. Під цими злочинами пропонувалося розуміти передбачені кримінальним законом суспільно небезпечні діяння, в яких машинна інформація є засобом або об'єктом злочинного посягання [8, с. 167].

З нашої точки зору, термін «машинна інформація» є застарілим й таким, що не узгоджується з вимогами національного та міжнародного законодавства, адже Конвенція про кіберзлочинність 2001 року і додаткові протоколи до неї оперують поняттями «комп'ютерна система», «комп'ютерні дані». Тому предметом злочинних посягань, відповідальність за які передбачена розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України, є саме комп'ютерна інформація.

Конвенція про кіберзлочинність 2001 року передбачає встановлення відповідальності за: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи» тощо [9].

Ми приєднуємося до позиції вчених, на думку яких кримінально-правовий обсяг поняття «кіберзлочинність» складають як правопорушення

проти конфіденційності, цілісності та доступності комп'ютерних даних, навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних, так і кримінальне каране втручання у роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, навмисне серйозне перешкоджання їх функціонуванню.

Як зазначалося раніше, поряд з поняттям «кіберзлочини» в кримінально-правовому аспекті вживається поняття «злочини у сфері використання інформаційних технологій». Забезпечення кримінально-правового стимулювання позитивних та мінімізації негативних соціальних наслідків інформатизації передбачає визначення як самостійного об'єкта кримінально-правової охорони системи суспільних відносин, які забезпечують реалізацію інформаційної потреби. Для позначення цієї системи використовують термін «інформаційна безпека», а її структуру складають відносини у сфері формування інформаційного ресурсу, забезпечення доступу до інформації, а також відносини у сфері використання інформаційних технологій [4, с. 11; 10]. Суспільна небезпечність злочинів в сфері використання інформаційних технологій головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це і визначає суспільну небезпечність конкретного посягання в сфері використання інформаційних технологій [11].

З урахуванням викладеного, вважаємо більш перспективним закладений у законопроекті про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки (реєстр. № 9575 від 09.12.2011) підхід, згідно з яким родовим об'єктом злочинів, що розглядаються, є суспільні відносини у сфері інформаційної безпеки, що, на думку його розробників, зумовлює зміну назву розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК на «Злочини у сфері інформаційної безпеки» [12].

Водночас слід зазначити, що норми про злочини, які містяться у розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК охоплюють не весь спектр злочинів у сфері інформаційної безпеки. Тому більш прийнятною важаться зміна назви розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини цього Кодексу на «Злочини у сфері використання інформаційних технологій».

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19. (дата звернення 21.05.2019).
2. Офіційний сайт Верховної Ради України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657. (дата звернення 21.05.2019).
3. Офіційний сайт Верховної Ради України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657. (дата звернення 21.05.2019).
4. Карчевский Н. В. «Киберпреступление» или преступление в сфере использования информационных технологий? *Кібербезпека в Україні: правові та організаційні питання :* матеріали всеукр. наук.-практ. конф. (Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 10–14.
5. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. ... канд. юрид. наук : спец. 12.00.08. Владивосток, 2005. 235 с.
6. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М. : Юридическая литература, 1991. 157 с.
7. Біленчук П. Д., Бут В. В., Гавловський В. Д., Гуцалюк М. В., Колпак Р. Л. Комп'ютерна злочинність : навч. посіб. Київ : Атіка, 2002. 240 с.
8. Геллер А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета : дис. ... канд. юрид. наук : спец. 12.00.08. М., 2006. 219 с.
9. Конвенція про кіберзлочинність від 23.11.2001 : ратиф. із застереженнями і заявами Законом України від 07.09.2005 № 2824-IV. *Офіційний Вісник України*. 2007, № 65 від 10.09.2007. Ст. 2535.
10. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 512 с.
11. Карчевський М. В. Дослідження практики використання національними судами норм про кримінальну відповідальність за злочини в сфері використання комп'ютерної техніки та мереж електрозв'язку. Злочини в сфері використання ІТ. URL: http//www.it-crime.at.ua. (дата звернення 21.05.2019).
12. Офіційний сайт Верховної Ради України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=42065.