

Яременко А. В.,
студент 5 курсу,
12 групи, Інституту прокуратури та кримінальної
юстиції,
Національного юридичного університету імені
Ярослава Мудрого

ПРОБЛЕМА РОЗУМІННЯ КАТЕГОРІЇ ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ ТА ЇЇ ІДЕНТИФІКАЦІЇ В УКРАЇНІ

Ключові слова: організована, кіберзлочинність, кібербезпека, кіберзлочин, кіберпростір.

Keywords: organized, cybercrime, cybersecurity, cyber-domain.

Анотація: розглянуто питання організованої кіберзлочинності в системі злочинності на території України: кількісний та якісний показник вчинюваних кіберзлочинів; проаналізовано необхідність зміни встановленої державою політики визначення та ідентифікації організованої кіберзлочинності.

Abstract: The role of organized cybercrime in the crime system of Ukraine is considered: quantitative and qualitative indicators for cybercrimes; analysis of public policies of Ukraine for determination of cybercrime.

Як відомо, теорія кримінології виділяє декілька ознак, за якими класифікують сучасну

злочинність. Задля досягнення мети дослідження, автор пропонує розглянути лише одну з таких ознак – кількість осіб, задіяних у злочинній діяльності. За цим критерієм можливо виокремити: а) злочинність, яка формується зі злочинів, вчинених одним суб'єктом та б) злочинів, вчинених спільно з іншими особами. Так, відповідно, з останньої категорії можна додатково виокремити злочинність, кількісний показник якої формується а) групами осіб та б) стійкими злочинними спільнотами (організована злочинність).

Організована злочинність, безсумнівно, вважається найбільш небезпечним видом злочинності, існування якої недопустиме у епоху високих технологій, зважаючи на велику кількість способів її виявити та побороти. Разом з тим, організована злочинність як соціальне явище також не зупиняється на місці. Процеси глобалізації та інформатизації суспільства призводять до того, що представникам організованої злочинності вдається не лише обходити подекуди застарілі (недієві) інструменти держав щодо їх ідентифікації, а й пристосовуватися до світових тенденцій, входячи в якісно нову площину кіберзлочинності [4].

Деякі фахівці визначають організовану кіберзлочинність як сукупність кіберзлочинів, які вчиняються у зв'язку зі створенням та діяльністю у кіберпросторі організованих злочинних угруповань [3, с.315]. Під кіберзлочинами пропонується розуміти злочини, пов'язані з протиправним використанням кібернетичних комп'ютерних систем [3, с.315] – будь-якого пристрою або групи взаємопов'язаних або пов'язаних пристроїв, один чи більше з яких, у відповідності до певної програми, виконує автоматичну обробку даних [6].

Законодавство України щодо категорії злочинів, які можна віднести до кіберзлочинів, принципово відрізняється від законодавства європейських країн. Так, до кіберзлочинів віднесено злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електров'язку (ст.ст. 361-363-1 Кримінального кодексу України) [5]. Зазначений підхід законодавця визначається нами як хибний та такий, що ґрунтується на неправильному розумінні процесів функціонування інформаційних систем, оскільки глумачиться недопустимо вузько, що тягне за собою неефективність процесу виявлення та розслідування кіберзлочинів.

Недослідженість явища кіберзлочинності в Україні, почасти на складність виявлення та розслідування класичної організованої злочинності, зокрема, її латентний характер [1], дає досить невтішні результати. Так, відповідно до даних, наданих Генеральною прокуратурою України, за період з 01.01.2016 по 01.05.2017 було зареєстровано 1 723 кіберзлочинів, при загальній кількості – 592 604 облікованих злочинів лише за 2016 рік [5]. Особливої уваги заслуговують статистичні дані щодо злочинів, які складають організовану кіберзлочинність в Україні за період з 01.01.2016 по 01.05.2017 – два злочини.

Автор критично ставить до зазначених статистичних показників та погоджується з думкою О. Шостко про те, що за таких умов організована злочинність [будь-який її вид] не є загрозою для України, і при збереженні сучасної динаміки за декілька десятків років може просто зникнути, звісно, якщо вивчати це явище тільки з позицій облікованих суспільно небезпечних діянь [1].

Особливістю кіберзлочинів є «місце» їх вчинення – кіберпростір. Кіберпростором не є мережа Інтернет, або комп'ютерна мережа, або мережа радіо- / мобільного зв'язку тощо по окремість [4]. Науковці вважають кіберпростором віртуальний простір, який надає можливості для здійснення комунікацій, утворений в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та / або інших глобальних мереж передачі даних [2], тобто, є інтегратором всіх зазначених мереж.

Автором стверджується, що перелік кіберзлочинів, який вважається законодавцем вичерпним [5], таким не є. Розділяючи думку В. Шеломенцева, зауважимо, що кіберзлочинами є не лише протиправні діяння у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електров'язку. Це можуть бути злочинні посягання на суспільні відносини в різних галузях людської діяльності, пов'язані як з використанням інформаційних об'єктів, так й інформаційною взаємодією суб'єктів діяльності в електронній цифровій формі (несанкціоноване втручання у роботу кібернетичних комп'ютерних мереж, телетайпне перехоплення даних, шахрайство, вимагання, шпіонаж, фіктивне підприємництво, терористичний акт, хуліганство, розголошення державної таємниці, пропаганда війни тощо, вчинені у кіберпросторі) [3, с.317].

У Конвенції Ради Європи про кіберзлочинність (зокрема, Додатковому протоколі до неї) визначено перелік протиправних посягань, за які на національному рівні повинна встановлюватися кримінальна відповідальність: а) проти конфіденційності, цілісності та доступності даних, вчинені з використанням технічних засобів і комп'ютерних даних; б) пов'язані з комп'ютерами (комп'ютерна підробка, комп'ютерне шахрайство); в) пов'язані з виробленням, володінням або пропонуванням

громадськості чи наданням доступу через кібернетичні комп'ютерні системи, розповсюдженням, передаванням або набуттям за допомогою кібернетичних комп'ютерних систем, інформації, яка за своїм змістом є: дитячою порнографією; матеріалами расистського та ксенофобного характеру; погрозами (у розумінні національного кримінального права); образами з расистських та ксенофобних мотивів; запереченням, значною мінімізацією, схваленням або виправданням геноциду чи злочинів проти людства; пособництвом та підбурюванням до вчинення будь-якого з зазначених правопорушень); г) пов'язані з порушенням за допомогою кібернетичних комп'ютерних систем прав інтелектуальної власності [6].

Отже, правоохоронними органами при виявленні та розслідуванні злочинів, що складають організовану кіберзлочинність, не враховується факт складності злочинних процесів у кіберпросторі, що зумовлює неможливість їх вчинення одиничним суб'єктом. Так, зокрема, злочинні дії, передбачені в пункті «а», щодо кібернетичного нападу на інформаційні бази даних з метою порушити режим їх конфіденційності та обійти їх мережевий захист, коли це стосується державних органів або інших масштабних об'єктів з недержавним статусом, часто супроводжується множинністю суб'єкта посягання, на що не звертається належна увага. Притягнення до відповідальності відбувається за принципом «першого підозрюваного», щодо якого вдалося зібрати мінімальну доказову базу.

Зважаючи на наведені автором теоретичні аспекти та незадовільні фактичні дані щодо розуміння та правової ідентифікації кіберзлочинів, в тому числі, явища організованої кіберзлочинності, в Україні, існує явна необхідність у продовженні дослідження та лобюванні відповідних законодавчих ініціатив, за результатами такого дослідження.

Список використаних джерел:

1. Шустко О. Ю. Сучасний стан організованої злочинності в Україні [Електронний ресурс] / Олена Юрївна ШОСТКО // Проблеми законності. – 2016. – Вип. 135. – С. 136-146. Режим доступу до ресурсу: <https://www.ceeol.com/search/article-detail?id=474678>.
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія [Електронний ресурс] / Д. В. Дубов // К. : НІСД – 2014. – Режим доступу до ресурсу: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf.
3. Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття / Володимир Петрович Шеломенцев. // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – №21. – С. 314–322.
4. Гриненко І. Структура кримінальних відносин у кіберпросторі [Електронний ресурс] / І. Гриненко, Д. Прокоф'єва-Янчиленко, М. Прокоф'єв // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – Режим доступу до ресурсу: http://pnzzi.kpi.ua/25/25_p27.pdf.
5. Відповідь Генеральної прокуратури України на інформаційний запит щодо про зареєстровані кримінальні правопорушення, пов'язані з кіберзлочинністю [Електронний ресурс]: Офіційний лист-відповідь з додатками на 3 сторінках № 19/4-681вих-17 від 11.05.2017. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v
6. Про кіберзлочинність: Конвенція Ради Європи // Офіц. вісник України. – 2007. – № 65.– Ст. 2535. – С. 107. – 10 верес. – Код акту 40846 /2007.

Міністерство освіти і науки України
Національний юридичний університет
імені Ярослава Мудрого

ЗЛОЧИННІСТЬ У ГЛОБАЛІЗОВАНОМУ СВІТІ

Матеріали XVI Всеукраїнської кримінологічної
конференції для студентів, аспірантів та молодих вчених

(м. Харків, 12 грудня 2017 р.)

За загальною редакцією
професора *А. П. Гетьмана* і професора *Б. М. Головкина*

Харків
«Право»
2017

УДК 343.9.01:005.44
ББК 67.61я431
3-68

Редакційна колегія:
проф. А. П. Гетьман,
проф. Б. М. Головкін,
канд. юрид. наук, доц. О. В. Ткачова,
канд. юрид. наук, ас. О. В. Таволжанський,
канд. юрид. наук, ас. Н. В. Сметаніна,
канд. юрид. наук, ас. К. Д. Кулик,
канд. юрид. наук, ас. О. О. Шуміло,
ст. лаб. К. С. Остапко

**Злочинність у глобалізованому світі : матеріали XVI Всеукр.
3-68 кримінол. конф. для студентів, аспірантів та молодих вчених (м. Хар-
ків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. –
Харків : Право, 2017. – 420 с.**

ISBN 978-966-937-307-6

ISBN 978-966-937-307-6

© Національний юридичний університет
імені Ярослава Мудрого, 2017
© Оформлення. Видавництво «Право», 2017