УДК 343.98
DOI https://doi.org/10.32841/2307-1745.2019.39.27

Заболотна Ю. В.,
кандидат юридичних наук,
викладач кафедри криміналістики та судової експертології
факультету № 1
Харківського національного університету внутрішніх справ

Іванко Є. Б.,
головний судовий експерт
Харківського науково-дослідного експертно-криміналістичного центру

ПРОБЛЕМИ ВЗАЄМОДІЇ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Анотація. У статті авторами здійснено аналіз проблем взаємодії при розслідуванні кіберзлочинів. Розглянуто особливості міжнародного співробітництва при розслідуванні кіберзлочинів. Зосереджено увагу на аналізі 5 груп злочинів: злочини, що спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних, злочини, пов'язані з контентом (змістом), злочини, пов'язані з порушенням авторських прав, злочини, пов'язані із застосуванням комп'ютерних засобів та комп'ютерних систем, акти расизму і ксенофобії, що здійснюються за допомогою комп'ютерних мереж. Виділено ряд проблем, що виникають при боротьбі з кіберзлочинністю та запропоновано шляхи їх подолання. До основних проблем віднесено латентність скоєних злочинів, прозорість кордонів або, так звана, транс національність, висока підготовленість і професійність суб'єктів, відсутність законодавчих актів, що регулюють кримінально-процесуальну діяльність, відсутність технічних засобів і взаємозв'язку з органами, що здійснюють боротьбу з кіберзлочинністю, так як дані злочини носять інтернаціональний характер, недостатня компетентність осіб, які займаються виявленням та розкриттям кіберзлочинів, пошуком доказів вчинення протиправних дій. Автори приходять до висновку, що необхідно створити більш дієвий механізм взаємодії держав у питаннях правової допомоги, на будь-якому рівні для розслідування кіберзлочинів необхідно забезпечити підготовку висококваліфікованих фахівців у даній галузі та вдосконалити законодавство для побудови ефективної правової основи для забезпечення слідчої, оперативно-розшукової діяльності правоохоронних органів і спецслужб у боротьбі з подібними злочинами, а також необхідні оперативні дії, що спираються на координацію зусиль національних центрів із запобігання і розслідування транснаціональних комп'ютерних злочинів з аналогічними міжнародними центрами в інших країнах .

Ключові слова: кіберзлочин, інформатизація суспільства, боротьба з кіберзлочинністю, кіберсфера.

Постановка проблеми. Початок XXI століття ознаменувався переходом людства в цифровий світ. Цифровізація впевнено проникає у всі сфери людської життєдіяльності. Поточні розробки в сфері IT-технологій відкривають широкі можливості не тільки для розвитку і вирішення глобальних завдань, що стоять перед суспільством сьогодні, але і створюють велике поле діяльності для кіберзлочинців.

Більшість досліджень, що проводяться в області комп'ютерних і кіберзлочинів сьогодні в основному зосереджені на фінансових махінаціях, зломах, незаконних спостереженнях, створеннях онлайн-ринків і т. д. Однак злочини, вчинені у цифровому просторі, давно вийшли за рамки перерахованих вище. Нові види злочинів зачіпають проблеми соціального та економічного характеру, дозволяють вершити правосуддя самостійно. Злочинність поступово з реального світу переходить у світ цифрового, що несе ще більшої шкоди плановому розвитку сучасності.

Аналіз останніх досліджень і публікацій.

Питання кіберзлочинності та аналіз окремих елементів злочинів пов'язаних з використанням засобів комп'ютерної техніки розглядалися у працях Ю.М. Батуріна, П.Д. Біленчука, В.Б. Вєхова, В.О. Голубєва, М.Д. Діхтяренко, Б.Х. Толеубекова, А.А. Васильєва, О.Г. Волеводза, О.В. Мещерякова, Т.Л. Тропіної та інших науковців.

Формулювання завдання дослідження. Метою роботи є дослідження проблем взаємодії при розслідуванні кіберзлочинів.

Виклад основного матеріалу. Злочини, що здійснюються у віртуальному світі, але мають наслідки в світі реальному, називають кіберзлочинами, а особи, які їх здійснюють – кіберзлочинцями.

Під кіберзлочинністю розуміють протизаконну діяльність, чинену за допомогою електронних пристроїв і мережі інтернет, спрямованих на порушення особистих прав і свобод громадян [4, с .148].

В якості об'єкта кіберзлочинів виступають інформаційна система, інформаційні дані та інформаційно-комунікаційна мережа.

Суб'єктом, у свою чергу, є користувачі.

Кіберзлочинність відносно новий вид злочинної діяльності. Сучасне суспільство не готове протистояти подібним атакам, більшою мірою, через необізнаність в комп'ютерній сфері. Очевидно, що класичні методи розкриття злочинів не завжди застосовні у кіберсфері, тому ведуться розробки, спрямовані на розслідування подібних злочинів [5, с. 68].

Боротьба з кіберзлочинністю ведеться на міжнародному рівні. Виділимо такі нормативно-правові акти, прийняті на сьогоднішній день [7, с. 2].

– Конвенція ООН проти транснаціональної організованої злочинності (2000 р.).

– Програма «Інформація для всіх», (ЮНЕСКО, 2001 р.).

– Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» (Женева, 2003 р.).

– «Туніська програма для інформаційного суспільства», (2005 р.).

В рамках Конвенції Ради Європи слід виділити такі: «Про взаємної правової допомоги по кримінальних справах в тому, що стосується судових доручень про перехоплення телекомунікаційних повідомлень», «Про боротьбу з піратством у сфері авторського права і суміжних прав», «Про порядок використання персональних даних поліцією», «Про захист персональних даних у сфері телекомунікаційних послуг, особливості телефонних послуг», «Про злочини, пов'язані з комп'ютерами», «З проблем кримінально-процесуального права, пов'язаних з інформаційними технологіями» [7, с. 43].

Виділяють 5 груп злочинів, що відносяться до розглянутої області [8, с. 338]:

– злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних;

– злочини, пов'язані з контентом (змістом);

– злочини, пов'язані з порушенням авторських прав;

– злочини, пов'язані із застосуванням комп'ютерних засобів та комп'ютерних систем;

– акти расизму і ксенофобії, що здійснюються за допомогою комп'ютерних мереж.

До першої групи належать комп'ютерні злочини, спрямовані проти конфіденційності та цілісності даних. Наприклад, протизаконний доступ до особистої інформації, перехоплення даних не призначених для загального доступу і т. д.

До другої групи входять злочини, пов'язані зі змістом даних (наприклад, зміною їх на шкоду кому-небудь).

Злочини, що відносяться до третьої групи, пов'язані з порушенням авторських прав. Такими порушеннями вважаються привласнення чужої праці і незаконне використання його в своїх цілях.

Основу четвертої групи складають злочини, що здійснюються за допомогою комп'ютерних технологій (наприклад, витяг і блокування даних, отримання економічної вигоди та ін.).

До п'ятої групи належать злочини, спрямовані на розпалювання міжнаціональних конфліктів, актів расизму і т.д., за допомогою комп'ютерних технологій та мережі інтернет.

Існує ряд проблем, що виникають при боротьбі з кіберзлочинністю. Це такі проблеми як:

– латентність скоєних злочинів;

– прозорість кордонів або, так звана, транснаціональність;

– висока підготовленість і професійність суб'єктів;

– відсутність законодавчих актів, що регулюють кримінально-процесуальну діяльність;

– відсутність технічних засобів і взаємозв'язку з органами, що здійснюють боротьбу з кіберзлочинністю, так як дані злочини носять інтернаціональний характер [1, с. 23].

Основною проблемою при розкритті злочинів в даній області сьогодні є недостатня компетентність осіб, які займаються виявленням та розкриттям кіберзлочинів, збір доказів вчинення протиправних дій.

Кіберзлочинність не обмежується рамками однієї держави або ж республіки, тому робота правоохоронних органів у цьому напрямку буде ефективною лише в разі якісного міжнародного співробітництва. Розслідування подібних злочинів ускладнюється з наступних причин:

– брак працівників зі специфічною освітою та досвідом;

– недостатній рівень технічного забезпечення правоохоронних структур;

– місце розташування в рамках всього світу;

– можливість вибору злочинцем найбільш лояльної правової системи.

Для подолання комп'ютерних злочинів необхідно погоджений міжнародний підхід. На будь-якому рівні для розслідування кіберзлочинів необхідні добре підготовлені кадри і вдосконалене законодавство для створення ефективної правової основи для забезпечення слідчої, оперативно-розшукової діяльності правоохоронних органів і спецслужб у боротьбі з подібними злочинами, а також необхідні оперативні дії, що спираються на координацію зусиль національних центрів із запобігання і розслідування транснаціональних комп'ютерних злочинів з аналогічними міжнародними центрами в інших країнах [3, с .61].

Важливим кроком спрямованим на вирішення цієї проблеми, є прийняття Радою Європи 23 листопада 2001 р. Конвенції про кіберзлочинність. Конвенція про кіберзлочинність - перший міжнародний договір у галузі протидії злочинам, що вчиняються через комп'ютерні мережі. Основна мета - проведення загальної політики у сфері кримінального права, спрямованої на захист суспільства від комп'ютерних злочинів. Форми міжнародної співпраці включають видачу, надання допомоги в галузі права, визнання судових рішень, неофіційна співпраця правоохоронних органів різних країн. Зважаючи на теперішню ситуацію в галузі міжнародної співпраці виникає ризик утворення міждержавних угрупувань, найбільше це стосується співпраці при розслідувані [4].

Хоча й було здійснено велику кількість спроб щодо більш тісного міжнародного співробітництва, проте на наш погляд варто систематизувати всі версії, які були наданні , як науковцями , так і законодавчими органами різних країн та створити більш зручні підходи для тісного контакту між державами у сфері боротьби із кіберзлочинністю. Міжнародне співробітництво регулюється такими принципами:

1) найширші обсяги співпраці шляхом застосування відповідних міжнародних документів, укладених угод на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства;

2) здійснення співробітництва з метою розслідування або судового переслідування щодо злочинів, пов'язаних з комп'ютерними системами і комп'ютерними даними.

Також не менш важливим є усунення прогалин у міжнародних відносинах, щодо таких питань як:

1) доступ до даних без отримання згоди користувача чи власника, але з наступним обов'язковим повідомленням особи чи компетентних органів держави, де знаходиться комп'ютерна система чи дані;

2) відсутність регулювання механізму відмови у транскордонному доступі особі, яка володіє законним правом на управління комп'ютерною системою і даними;

3) порядок оскарження рішення про збирання комп'ютерних даних при транскордонному доступі;

4) захист конфіденційності інформації, отриманої вказаним вище способом;

5) судовий та відомчий контроль національних судів і компетентних органів за законністю дій іноземних органів;

6) не передбачається можливість проведення транскордонного обшуку у комп'ютерних мережах компетентними органами держави, в якій розслідується комп'ютерний злочин [5].

Підсумовуючи вищезазначене, ми вважаємо, що необхідно створити більш дієвий механізм взаємодії держав у питаннях правової допомоги. Варто також звернути увагу на створення нових та доповнення існуючих нормативно-правових актів для врегулювання всіх прогалин, які існують, проте їх варто не тільки розробити, а й імплентувати в їх національне законодавство, що дозволило б ефективно розслідувати кіберзлочини. А також створити компетентні органи, які будуть виконувати свої функціональні обов'язки на більш високому рівні та матимуть доступ до всієї інформації, необхідної для більш кращого виконання роботи. Не менш важливим є систематизація даних, створення загальних умов на національному рівні для всіх банків, а саме однаковий порядок організації роботи та видачі інформації стосовно певної особи та її рахунку і надання доступу патрульним до даних необхідних для якіснішого виконання ними своїх повноважень.

Вирішення проблеми інформаційної безпеки можливо лише за створення та ратифікування документів, які стосуються сфери інформаційної безпеки держав та створення необхідних умов для розслідування цих злочинів.

Висновки. Таким чином, виявити кіберзлочинців досить складно, так як існує безпосередня залежність від інформаційно-комунікаційних технологій; можливість несвоєчасного виявлення скоєного злочину; кількість користувачів, що здійснюються протиправні дії; знищення слідів активності; незалежність від місця розташування; брак механізмів контролю та ін.

З розвитком новітніх технологій стає необхідною криміналізація злочинів, скоєних в кіберпросторі. Даний вид злочинів, повною мірою, відповідає класичним характеристикам правопорушень, але в той же час вносить свої корективи. Дії, що здійснюються злочинцями, порушують конституційні права громадян на захист доброго імені, захист від посягань на честь і гідність, втручання в приватне життя і т. д. Безкарність породжує злочинність, тому необхідно направити можливі сили на припинення та придушення подібних дій.

Література:

1. Актуальні питання розслідування кіберзлочинів: матеріали Міжнар. наук.-практ. конф. (Харків, 10 груд. 2013 р.). Харків: ХНУВС, 2013. С. 272.
2. Бутусова Л.И. К вопросу о киберпреступности в международном праве. Вестник экономической безопасности. 2016. № 2. С. 48–52.
3. Карчевський М. В. Комп'ютерна інформація, як предмет злочину в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку. *Боротьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення* : матеріали міжвуз. наук.-практ. конф. (Донецьк, 14 груд. 2012 р.). Донецьк, 2012. С. 61–64.
4. Номоконов В.А., Тропина Т.Л. Киберпреступность: проблемы борьбы и прогнозы. *Библиотека криминалиста.* Москва, 2013. С. 148–159.
5. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. Москва: ИНФРА, 2018. 352 с.
6. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5–6. С. 71.
7. Користін О.Є., Бутузов В.М., Василевич В.В. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посібник. Київ: Вид. дім «Скіф», 2012. 736 с.
8. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки: зб. наук. праць. Київ: Вид.-поліграф. центр «Київський університет», 2009. № 19. С. 338–342.

Zabolotna Y., Ivanko E. Problems of interaction in the investigation of cybercrime

Summary. In this article, the authors analyze the problems of interaction in the investigation of cybercrime. The features of international cooperation in the investigation of cybercrime are considered. The focus is on the analysis of such 5 crime groups as crimes against the confidentiality, integrity and availability of computer data, crimes related to content (content), crimes related to copyright infringement, crimes against related to the use of computer facilities and computer systems, acts of racism and xenophobia carried out through computer networks. A number of problems that arise in the fight against cybercrime are identified and ways to overcome them are suggested. The main problems include the latency of the crimes committed, transparency of borders or the so-called transnationality, high preparedness and professionalism of the subjects, lack of legislative acts regulating criminal procedure activity, lack of technical means and interconnection with bodies engaged in the fight with cybercrime, as these crimes are international in nature, lack of competence of persons involved in the detection and disclosure of cybercrime, the search for evidence of wrongdoing. The authors conclude that there is a need for a more effective mechanism of state cooperation in matters of legal aid, at any level for the investigation of cybercrime, it is necessary to provide training for highly qualified specialists in this field and to improve the legislation to build an effective legal framework for the provision of investigative, operational and search activities law enforcement agencies and special services in the fight against such crimes, as well as the necessary operational actions based on coordination of efforts of national prices to prevent and investigate transnational computer crimes with similar international centers in other countries.

Key words: cybercrime, Informatization of society, fight against cybercrime, cyber sphere.