УДК 343.533

ЮРИДИЧНА ПРИРОДА КІБЕРЗЛОЧИНІВ

LEGAL NATURE OF CYBERCRIMES

Римарчук Г.С.,
кандидат юридичних наук,
асистент кафедри кримінального права та процесу
Інституту права та психології
Національного університету «Львівська політехніка»
Мельник В.І.,
оперуповноважений
Державної служби боротьби
з економічною злочинністю
ГУ МВС України у Львівській області

Стаття присвячена огляду питання вчинення злочинів у мережі Інтернет. Мова йде про кіберзлочинність – новоутворений термін, не закріплений в законодавстві України, його соціальну та юридичну природу, визначення характерних ознак та складових елементів, за якими комп'ютерні злочини виділені серед інших видів злочинів, передбачених Кримінальним кодексом України, а також які засоби інтернет-впливу можуть використовувати в своєму арсеналі суб'єкти злочину.

Ключові слова: кіберзлочини, злочини в мережі Інтернет, комп'ютерні злочини, онлайн-банкінг.

Статья посвящена рассмотрению вопроса о совершении преступлений в сети Интернет. Речь идет о киберпреступности – новообразованном термине, не закрепленном в законодательстве Украины, его социальной и юридической природе, определении характерных признаков и элементов, согласно которым компьютерные преступления выделены среди других видов преступлений, предусмотренных Уголовным кодексом Украины, а также какие средства интернет-воздействия могут использовать в своем арсенале субъекты преступления.

Ключевые слова: киберпреступления, преступления в сети Интернет, компьютерные преступления, онлайн-банкинг.

The presented article is devoted to the issue of cybercrimes. First of all, it is admitted that the notion «cybercrime» is newly developed, not outlined in the legislation of Ukraine. Besides, the article covers social and legal nature of cybercrimes, intrinsic elements and characteristic features on the basis of which cybercrimes are distinguished among other types of crimes provided by Criminal Code of Ukraine. And finally, means of internet-impact, applied by the subjects of criminal offences, are highlighted.

Key words: cybercrimes, Internet crimes, computer crimes, online-banking.

Постановка проблеми. З метою ефективної правової регламентації відносин, що місять в собі нові елементи злочину (об'єкт, суб'єкт, просторові рамки та ін.), та результативності юридичного закріплення даного виду злочинного діяння необхідним є розуміння природи вчинюваного кримінального правопорушення. Так, комп'ютеризацію як суспільне явище можна вважати не лише прогресивним кроком людства, але й негативним стимулом, що призвів до появи нового виду злочинів – злочинів у мережі Інтернет (кіберзлочинів).

Мета публікації. Варто з'ясувати дефініцію поняття кіберзлочинів, які характеристики притаманні даному кримінальному правопорушенню, в чому полягає новизна об'єкту та суб'єкту кіберзлочину для кримінального законодавства, а також шляхи доступу суб'єктів кіберзлочинів до інформаційних даних користувачів.

Аналіз досліджень проблематики статті. Проблему кіберзлочинності на теренах України та у зарубіжній науці досліджували такі автори, як В. Дзюндзюк, Б. Дзюндзюк, М. МакГуайр, С. Даулинг, С. Фафінські та ін.

Виклад основного матеріалу. Можливість дистанційного керування справами як на освітньому ринку, так і на ринку товарів і послуг, доступ до великого різноманіття інформаційних ресурсів та баз даних, зручність управління валютно-фінансовими операціями, безумовно, сприяють позитивній динаміці розвитку та вдосконалення відносин громадського та приватного сектору, вносять свої корективи у виробництво, товарообіг і реалізацію, надають додаткові можливості споживачам у доступі до інформації, каталогу товарів/послуг та шляхів їх одержання.

Зробивши ставку на останні досягнення в сфері новітніх технологій, ми стаємо заручниками не лише вдосконалених умов життя, а й власної безпеки. Якщо машина створена з використанням людського потенціалу, то чому той же вихідний ресурс не може взяти її під свій контроль. Ми маємо на увазі контроль за даними, що перебувають у законній власності третіх осіб, отримання та обробку інформації в закритому доступі, неправомірне заволодіння та передачу будь-яких джерел під грифом приватності.

Явище кіберзлочинності має такі характеристики: незаконна дія, крадіжка та шкода. Метою злому комп'ютера є контроль над власністю та інформацією жертви, таким чином, незаконно отримуючи доступ до її персональних даних.

Під кіберзлочинами (також їх називають комп'ютерними злочинами) розуміють використання комп'ютера як інструмента для вчинення по-

дальших незаконних дій, таких як шахрайство, дитяча порнографія, порушення права інтелектуальної власності та персональних даних [1].

Визначення кіберзлочинності містить в собі два компоненти, а саме: використання комп'ютерних мереж для вчинення злочину, а також будь-який злочин, скоєний з метою злому комп'ютерної мережі або за допомогою останньої [2].

Наведені визначення дещо звужують бачення природи незаконної поведінки, що входить як складовий елемент до досліджуваного терміну. Проблема кіберзлочинності ускладнюється і тим, що її можна назвати більш соціальним терміном, а не юридичним, оскільки в кримінальному законодавстві відсутнє закріплення кіберзлочину як виду злочину.

Кіберзлочини можна трактувати як злочинну діяльність, спрямовану на захоплення даних, їх змісту, а також порушення копірайту (авторських прав). Оскільки ми розглядаємо мережу Інтернет як глобальний носій інформації, проблема порушення авторського права є надзвичайно розповсюдженою саме в цьому контексті. Нерідко люди знаходять свої наукові чи публіцистичні праці, розміщені у мережі третіми особами за фінансову винагороду, чи використання фотографій відомих людей, зірок шоу-бізнесу, без їх згоди, в недобросовісній рекламі.

Кіберзлочини займають місце злочинів проти інформації, оскільки відбувається «полювання» за інформацією, у чому б вона не була втілена: малюнки, документи, бази даних, рахунки та ін. Саме тому, визначивши об'єкт злочину, можна визначити об'єкт зацікавленості злочинця: чи то інформація про банківський рахунок, чи персональні дані.

Так, можемо констатувати, що кіберзлочинність має вагомий, з огляду на склад злочину, елемент, який полягає у відсутності тактильних характеристик об'єкту злочину. Це обумовлено площиною вчинення злочинної дії, що становить найбільшу складність у роботі правоохоронних органів даної специфіки, полягає у вчасній фіксації незаконної дії з наступним відстеженням джерела презюмованого порушення.

Європейська комісія в 2007 році запропонувала таку інтерпретацію поняття кіберзлочинність: «традиційна форма злочину, вчиненого за допомогою електронних комунікаційних мереж та інформаційних систем, а також публікація інформації, що порушує права третіх осіб, через електронні медіа джерела, злочини, що властиві лише електронним мережам». [3, с. 4-5]

Кіберзлочини можна поділити на три категорії:

- виключно мережеві злочини, де цифрові системи є основною ціллю, що одночасно виступають і засобами посягання. Ця категорія включає в себе посягання на комп'ютерні системи для знищення інфраструктури інтернет-технологій та незаконне заволодіння даними;

- існуючі злочини, що були переведені в площину кіберзлочинів через використання Інтернету;

- використання Інтернету з метою торгівлі наркотиками та як допоміжний інструмент для інших видів злочинів.

Однак необхідно розрізняти злочини, вчинені безпосередньо в мережі, та такі ж, але здійснені оффлайн. Наприклад, переписка про можливий план злочину не буде вважатися кіберзлочином, оскільки в ньому відсутній склад злочину, можна лише припустити хід подій, а вже його безпосередня реалізація поза межами Інтернету не може вважатися кіберзлочином.

Професор Пітер Соммер пояснював: «коли термін «комп'ютерний злочин» став атрибутом активного вжитку в 1970-их, число користувачів комп'ютерів було незначним і, відповідно, не йшлося про такий вид злочинної діяльності, як кіберзлочини. Сучасні підходи до тлумачення кіберзлочинів відображають великий відсоток злочинів з «комп'ютерним» елементом через те, що понад 77% населення мають комп'ютери» [4, с. 118-120].

Кіберзлочинність можна вважати об'єднуючим поняттям, що характеризує пов'язані кримінальні дії: кіберзалежні та кіберутворюючі злочини. Кіберзалежні – це злочини, які вчиняються з використанням комп'ютерів, комп'ютерних мереж чи інших комунікаційних форм. Такі, наприклад, як поширення вірусів та інших шкідливих програм, хакерство, зламування серверів для захоплення мережевої інфраструктури або веб-сторінок. Кіберзалежні злочини спрямовані на пошкодження комп'ютерів та джерел мережі, мають наслідки у вигляді, наприклад, шахрайства. Кіберутворюючі злочини – це традиційні види злочинів, які стали кіберзлочинами через використання комп'ютерів, комп'ютерних мереж та інших видів комунікації. На відміну від кіберзалежних, вони можуть вчинятися і без застосування «комп'ютерного елементу» [5, с. 5].

На засіданні Генеральної Асамблеї ООН обговорювалося питання кіберзлочинності, одним із пунктів обговорення було визначення даного поняття. Так, його трактування головним чином залежить від того, в якому контексті буде використовуватися цей термін. Основу кіберзлочинності складає досить обмежене коло діянь, спрямованих на порушення конфіденційності, цілісності та доступності комп'ютерних даних або систем [6, с. 2].

Але достатньо складно знайти загальне юридичне визначення кіберзлочинності по відношенню до дій, вчинених з використанням комп'ютерів з метою отримання особистої вигоди чи фінансового прибутку або нанесення особистої чи фінансової шкоди, включаючи такі форми злочинів, пов'язаних з використанням персональних даних та інформацією, що зберігаються в комп'ютері.

Можна встановити категорії комп'ютерних злочинів в залежності від мети, з якою використовувалось основне знаряддя – комп'ютер:

- комп'ютер як ціль – спрямована дія на комп'ютер як об'єкт посягання (наприклад, поширення вірусів);

- комп'ютер як зброя – використання комп'ютера для вчинення «традиційних» злочинів, таких як шахрайство чи нелегальні азартні ігри;

- комп'ютер як допоміжний засіб – використання комп'ютера як накопичувача та зберігача незаконно отриманої інформації.

Так, наше бачення дефініції кіберзлочинності полягає у наступному: це діяння, скоєні поза межами зако-

ну, в яких відсутній тактильний об'єкт посягання, площиною яких є виключно мережевий простір. В даному твердженні ми робимо акцент на двох суттєвих рисах кіберзлочинів: об'єкт злочину та просторові рамки.

Об'єктом злочину ми визначаємо різновиди інформації, що приймають специфічні форми та містяться на різних носіях, в комп'ютері (файли), на веб-сторінці (персональні дані) чи на банківському рахунку (реквізити рахунків, банківських карток) тощо. Посягання на комп'ютер як на повноцінний об'єкт злочину в цьому контексті ми не можемо розглядати, оскільки, якщо комп'ютер підлягає, наприклад, вірусним атакам, то метою злочинця є не матеріальний носій, а розміщена на цьому носії інформація.

До основних властивостей кіберзлочинності В.Б. Дзюндзюк відносить такі:

- інтелектуальний характер кіберзлочинності;
- відсутність вікового цензу та соціального статусу;
- анонімність і неперсоніфікованість;
- дистанційність кіберзлочинів;
- транснаціональність кіберзлочинів [7, с. 7-9].

Одним із основних елементів кіберзлочинів є неправильне використання програмного забезпечення та засобів інтернет-користування. Злочинці у своєму арсеналі мають безліч способів втручання в особистий простір індивіда, такі як електронна пошта, персональні веб-сторінки тощо. В даному випадку злочинці використовують паролі доступу та засоби дистанційного доступу. Засоби дистанційного доступу були створені з метою виправлення неполадок системи, однак їх можна використовувати і як засіб незаконного посягання на інформацію. Кіберзлочинці можуть використовувати мікрофони та камери на комп'ютері користувача для спостереження за діями останнього.

Ще однією ознакою кіберзлочинів є персоналізація, видача себе за іншу особу, що дозволяє злочинцям проникнути та заволодіти інформацією. Вони ховаються за рекламними акціями, подарунковими сертифікатами, безкоштовними пропозиціями. Вони також знають як видати себе за відому організацію чи установу, пропозиції чи запитання від якої виглядали б абсолютно законно та не викликали підозри. Так, наприклад, одним із способів доступу до персональних даних є прохання підтвердити свій пароль в онлайн банкінгу чи номер рахунку під виглядом виникнення проблеми з онлайн рахунком клієнта.

Американські дослідження показали, що в 2008 році США втратили близько 1,7 млрд доларів через кіберзлочинність. У Великобританії втрати як наслідок онлайн-банкінгового шахрайства становили 39 млн фунтів стерлінгів у першій половині 2009 року, вони збільшились на 55% у порівнянні з 2008 роком [8, с. 7].

Ще одним характерним елементом виступає незахищеність. Без надійного антивірусного забезпечення та паролів доступу комп'ютер користувача є доступним для кіберзлочинця. Інформація буде під загрозою, якщо користувач вимикає антивірусну систему, відкриває інтернет-посилання від незнайомих людей чи створює надто прості паролі до особистих сторінок. Досить популярним видом послуг є послуги інтернет-шопінгу, однак вони є і досить небезпечними, так як дані кредитної картки користувача можуть потрапити до злочинця.

В 2011-2012 рр. більше третини (37%) повнолітніх користувачів Інтернет стали жертвами інтернет-шахрайства. Як свідчить дослідження стану злочинності в Англії та Уельсі, число повнолітніх інтернет-користувачів, що стали жертвами кіберзлочинів з 39% зменшилося до 37% у 2011-2012 рр. За 2011-2012 рр. кількість інтернет-користувачів, які стали жертвами комп'ютерних вірусів, становила 31%, 7% – неавторизований доступ чи використання персональних даних, фінансове шахрайство – 3% [9, с. 6].

До поширених форм інтернет-злочинів відносять: шахрайства під виглядом розпродажів, з використанням небезпечного вірусного посилання на інтернет-ресурс; підставні веб-сайти благодійних організацій, наприклад, збір коштів для жертв урагану Катріна тощо; відкритки з поздоровленнями; вірусні реклами, промоакції; результати пошукових запитів, наприклад, певне словосполучення, введене в пошук Google, може видати сайти з вірусами; популярні веб-сайти з великою кількістю відвідувачів, що можуть містити посилання на недоброякісні сторінки; незаконне заволодіння персональними даними через опитування та анкетування з метою отримання подарунків (інших винагород); фальшиві повідомлення про доставку товару, які приходять під видом товарних накладних відомих поштових служб; фальшиві рахунки з інтернет-магазинів.

У переліку країн-жертв злочинів онлайн банкінгу [10, с. 4] найбільший відсоток та, відповідно, найвищі позиції займають країни передових технологій, осередки комп'ютерної еволюції, що призводить до негативних наслідків для користувачів та становить потенційну загрозу для подальшого розвитку кіберзлочинності.

Топ країн-жертв злочинів онлайн банкінгу

США	23%
Бразилія	16%
Японія	12%
Індія	6%
Австралія	3%
Франція	3%
Німеччина	2%
В'єтнам	2%
Тайвань	2%
Мексика	2%
Інші країни	29%

Висновки. Новітні технології певним чином сприяють розвитку криміногенної ситуації, призводячи до утворення нових видів злочинів. Одним з них є кіберзлочини. Відмінність від звичайних злочинів, передбачених кримінальним законодавством, кіберзлочинів полягає у застосуванні Інтернету як головної зброї, націленої на такі кримінальні правопорушення, як шахрайство, дитяча порнографія, порушення права інтелектуальної власності та неправомірне заволодіння і використання персональних даних.

У правовому розрізі поняття кіберзлочинів інкорпорує в собі такі елементи: незаконне винне діяння, яке вчиняється безпосередньо через мережеві

комунікації; об'єктом посягання виступає інформація в різних формах її вираження, суб'єкт злочину є персоніфікованим, він втілюється у найбільш відомі та знайомі користувачеві інтернет-ресурси або такі, що не викликали б у користувача підозри з питання легальності їх розміщення (брендові магазини, банківські установи, служби доставки тощо).

Для мінімізації ризиків становлення жертвою онлайн-махінаторів, збереження приватної інформації варто пам'ятати про необхідність встановлення антивірусних програм, застосування складних кодів доступу до персональних сторінок, уважність при переході на веб-посилання від сумнівних адресатів чи інтернет-джерел.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Encyclopedia Britannica [Електронний ресурс]. – Режим доступу : http://www.britannica.com/EBchecked/topic/130595/cybercrime.

2. Council of Europe Convention on Cybercrime (ETS № 185) 8 November 2001 [Електронний ресурс] – Режим доступу : http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

3. Home Affairs Committee E-crime Fifth Report of Session 2013–14 // Ordered by the House of Commons // [Text] – 17 July 2013. – P. 115.

4. Oxford Internet Institute Forum Mapping and Measuring Cybercrime // Oxford Internet Institute // [Text]. – University of Oxford, 22 January 2010. – P. 129.

5. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications // Home Office Research Report 75 // [Text]. – University of Surrey, October, 2013. – P. 29.

6. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // [Text] – Вена, 25-28 февраля 2013. – С. 21.

7. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності // Державне будівництво// [Текст] – № 1, 2013. – С. 7–9

8. European Union Committee 5th Report of Session 2009/10 Protecting Europe against large-scale cyber-attacks. Report with Evidence // [Text] – March, 2010. – P. 166.

9. Cybercrime: A review of the evidence. Summaries // [Text] – October, 2013. – P. 6 – [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence.

10. The invisible web unmasked // Trend Micro / Trend Labs 3Q 2013 Security Roundup // [Text] – 2013. – P. 22.

11. UK Cybercrime report by Stefan Fafinski // [Text] – 1871 LTD. – 2006. – P. 26.