УДК 343

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: ПРИЧИНИ, ОЗНАКИ ТА ЗАХОДИ ПРОТИДІЇ

CYBERCRIME IN UKRAINE: CAUSES, FEATURES AND MEASURES OF COUNTERING

Бондаренко О.С.,
кандидат юридичних наук,
викладач кафедри кримінально-правових дисциплін та судочинства
Навчально-наукового інституту права
Сумського державного університету

Рєпін Д.А.,
студент
Навчально-наукового інституту права
Сумського державного університету

Статтю присвячено засадам появи та розвитку кіберзлочинності, з'ясуванню та вирішенню головних проблем, що заважають ефективно боротися з такими злочинами. Зазначені причини виникнення та характерні ознаки кіберзлочинів. Розглянуто актуальні типи правопорушень у сфері комп'ютерної інформації, із застосуванням електронно-обчислюваних машин на території України.
Ключові слова: кіберзлочинність, кіберзлочини, інтернет-піратство, кібербезпека, мережа Інтернет, камкординг, кардшаринг, кіберзлочинці.

Статья посвящена основам появления и развития киберпреступности, выяснению и решению главных проблем, которые мешают эффективно бороться с подобными преступлениями. Указаны причины возникновения и характерные признаки киберпреступлений. Рассмотрены актуальные типы правонарушений в сфере компьютерной информации, с применением электронно-вычислительных машин на территории Украины.
Ключевые слова: киберпреступность, киберпреступления, интернет-пиратство, кибербезопасность, сеть Интернет, камкординг, кардшаринг, киберпреступники.

The article is devoted to the principles of the emergence and development of cybercrime, the clarification and decision of the main problems that do not allow the effective fight against such crimes. The indicated reasons for the emergence and characteristic signs of cybercrime. The article deals with the actual types of offenses in the field of computer information, the use of electronic computers in the territory of Ukraine.
Key words: cybercrime, cyber-crime, Internet piracy, cyber security, Internet network, camcorders, card sharing, cybercriminals.

Постановка проблеми. Протидія кіберзлочинності неможлива без всебічного розуміння ефективного правового регулювання діяльності інформаційних мереж. Розгляд взаємовідносин між мережами або їх користувачами та спричинені ними правові й соціальні труднощі, з якими стикаються правоохоронні органи та законодавці, – це, можливо, перший крок до створення реально діючих механізмів, що сприятимуть зменшенню кіберзлочинності.

Сьогодні комп'ютери відіграють вкрай важливу роль у різних сферах діяльності суспільства, виконуючи різноманітні функції як у роботі, так і в повсякденному житті. Так, наприклад, будь-яка державна чи то приватна організація неможлива без надійної системи захисту комп'ютерної техніки та засобів комунікацій.

За останні 10 років в Україні зросла кількість користувачів мережі Інтернет, бо це доступно для кожного, і, звичайно, зручно. Сьогодні комп'ютер, мобільний телефон із підключенням до Інтернету сприймається як належне та необхідне. Популярність Інтернету зрозуміла, оскільки він забезпечує безмежний доступ до неймовірної кількості інформації, передачі різноманітних документів, файлів та будь-яких даних, здатність здійснювати банківські операції, грошові транзакції, розвивати торгівлю, біржі тощо. Інтернет – це також можливість спілкування. Для багатьох людей соціальні мережі стали цілим світом, але віртуальним, а це, можливо, і є однією із причин злочинності в цьому світі.

Водночас віртуальний простір став місцем злочину та його інструментом. Тепер для скоєння злочину не потрібно мати із жертвою особистий контакт. Головним інструментом правопорушника є лише комп'ютер та доступ до інформаційних систем, де він, використовуючи відповідне програмне забезпечення, здійснює неправомірні діяння, які можуть загрожувати будь-кому.

Поширення комп'ютерних вірусів, шахрайство, крадіжки коштів із банківських рахунків або електронних гаманців, викрадення персональної та комерційної інформації, порушення правил роботи комп'ютерних систем – це далеко не повний перелік кіберзлочинів, оскільки з кожним днем їхні кількість і розмаїття тільки збільшується через такі причини: анонімність, що ускладнює виявлення злочину, злочинця; простота швидкого збагачення, доступність комп'ютерної техніки, за допомогою якої можна скоїти злочин майже з будь-якого куточка світу, а також доступність інтернет-інформації, яка тільки дозволяє вчиняти неправомірні діяння в мережі Інтернет.

Стан опрацювання. Питання кіберзлочинності й інших суспільно небезпечних діянь у сфері комп'ютерних інформаційних технологій досліджували такі вчені, як: В. Голіна, Б. Головкін, А. Голуб та інші.

Метою статті є визначення основ розвитку кіберзлочинності та з'ясування головних проблем, що заважають ефективно та остаточно усунути або мінімізувати зазначені види злочинів.

Виклад основного матеріалу. Термін «кіберзлочинність» у нормативних документах не визначений. Водночас сама концепція була сформована завдяки діяльності правоохоронних органів розвинутих країн Європи та світу і стосується злочинів у сфері комп'ютерної інформації та телекомунікацій, незаконного обігу радіоелектронних і спеціальних технічних засобів, поширення неліцензованого програмного забезпечення для комп'ютерів, а також деяких інших видів злочинів [1, с. 332].

Сьогодні кіберзлочинність для нашої держави є більш небезпечною, ніж навіть 5 років тому. Незважаючи на всі заходи правоохоронних органів, спрямовані на боротьбу з кіберзлочинністю, їх перелік не зменшується, а, навпаки, постійно зростає.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння правових питань регулювання інформаційних мереж. Аналіз взаємозв'язку між технічними характеристиками мережі, юридичними та соціальними компо-

нентами, з якими стикаються ці правоохоронні органи та законодавці, є першим кроком до можливого розвитку механізмів адекватного реагування на розвиток та зростання кількості кіберзлочинів.

Причини розвитку кіберзлочинності:

І. Головною причиною розвитку кіберзлочинності є велика прибутковість. Злочинці внаслідок окремих кіберзлочинів отримують величезні гроші, а якщо вести мову про невеличкі афери, з невеликими сумами грошей, то вони відбуваються майже кожної миті. Дослідження іноземних учених показують, що кіберзлочинність посідає третє місце після торгівлі зброєю та наркотиками за рівнем збагачення. Так, наприклад, за оцінками Рахункової палати Сполучених Штатів Америки, річний дохід злочинців лише від крадіжок і шахрайств, скоєних із використанням комп'ютерних технологій через Інтернет, сягає 5 мільярдів доларів.

ІІ. Технологічні причини – це ті, які проявляються в технічній простоті вчинення кіберзлочинів. Навіть із загальними знаннями в області системного адміністрування або програмування ви можете отримати доступ до слабо захищенних комп'ютерних мереж. Високопрофесійні хакери можуть обходити будь-який захист і замаскувати всі сліди вторгнення. Негативною тенденцією є також поширення вірусного ринку програмного забезпечення в Інтернеті, що дає можливість вчинити злочини тим особам, які навіть не мають комп'ютерних знань

ІІІ. Соціальні чинники є підґрунтям функціонування та розвитку кіберзлочинності. Передусім це зміни в суспільному житті, спричинені науково-технічним прогресом, пов'язані зі всебічною комп'ютеризацією суспільства, а також із формуванням інформаційного простору, заснованого на використанні комп'ютерів. У зв'язку із цим багато сфер соціальної активності переходять у віртуальний простір, що, у свою чергу, породжує нові проблеми – різні злочини з використанням електронно-обчислювальної техніки. І виникає необхідність у регулюванні цих проблем відповідним законодавством.

ІV. Політичні причини, які проявляються в недостатній обізнаності уряду країни щодо можливих суспільних наслідків кіберзлочинності. Через це скорочується бюджетне фінансування робіт зі створення правового, організаційного та технічного підґрунтя державної інформаційної безпеки, а також для захисту прав і свобод громадян, їхніх інтересів в інтернет-просторі. Також досить мало уваги приділяється правовому регулюванню комп'ютерної сфери, яка на тлі жорстокого та непідконтрольного розвитку призводить до деградації правових норм щодо потреб суспільства в інтеренет-просторі.

Ще одним важливим чинником у розвитку кіберзлочинності є психологічний, зумовлений особливостями механізму віртуального простору. У звичному повсякденному житті наявні якісь інструменти стримування, а у віртуальному світі – злочинці не бачать своїх жертв, яких вони обрали для нападу. І тому набагато простіше красти в тих, кого не бачиш, до кого не потрібно торкатися або застосовувати неправомірні дії у вигляді завдання фізичної шкоди, кровопролиття або інших небезпечних діянь. Злочини в мережі – це злочини на відстані. Щодо цього винні особи мають певну впевненість в анонімності та відсутності безпосередньої небезпеки виявлення і переслідування.

Ми переконані, що зараз є безліч злочинів, які мають латентний характер і не знайшли свого місця в законодавстві, тому потрібно удосконалювати кібербезпеку будь-якої комп'ютерної техніки, залучати спеціалістів у цій сфері, а також не потрібно забувати і про міжнародне співробітництво, що сприятиме значному посиленню безпеки, зменшенню кількості кіберзлочинів (особливо на початковому рівні їх скоєння).

Для досліджуваних злочинів характерні такі особливості:

– анонімність злочинця – це реальна можливість залишитися на відстані багатьох тисяч кілометрів від свої жертви. Також це зумовлює складність виявлення та розслідування кіберзлочину, оскільки особа скоює злочин за допомогою комп'ютера, будь-які візуальні ознаки правопорушника відсутні, окрім IP-адреси, яка навряд буде справжньою, оскільки зараз є безліч програм у відкритому доступі, що можуть допомогти в зміні адреси персонального комп'ютера, мінімальна можливість наявності свідків;

– складність виявлення та розслідування кіберзлочинів, адже злочин вчинений за допомогою електронно-обчислюваної машини (далі – ЕОМ), а в кожної з них є своя адреса в мережі Інтернет, і відповідні кваліфіковані органи чи особи мають шукати ту адресу серед усіх користувачів Інтернету, або тих, що приєднані до відповідної мережі, а таких осіб не десятки чи сотні, а як мінімум десятки чи сотні тисяч;

– значні збитки навіть від одного злочину. Ця особливість полягає в тому, що, наприклад, комп'ютерним вірусом можна «вбити» ЕОМ, і всю цінну інформацію, що була на ній, втратити назавжди. Наприклад, якщо йдеться про камкординг, то в цьому разі збитки від одного злочину можуть становити сотні тисяч, а то й мільйони доларів;

– складність доведення в суді згаданих злочинів полягає в такому: правопорушник може скоїти злочин не зі свого комп'ютера або будь-якого іншого технічного засобу, або просто може прибрати ці докази шляхом руйнування знаряддя злочину.

Ще однією особливістю кіберзлочинів є те, що розслідування та розкриття їх неможливе без використання комп'ютерних технологій. Ця необхідність пов'язана з пошуком, вилученням і збиранням доказів в електронній формі, оскільки злочини, що скоєні в Інтернеті або з його допомогою, наприклад, поширення кінофільмів, що були здобуті шляхом камкордингу, неможливо виявити або розслідувати поза Інтернетом. Також широко використовуються комп'ютерні технології для здійснення оперативно-розшукових дій. Але є чинники, які пов'язані з діяльністю правоохоронних органів і відіграють велику роль у функціонуванні та розвитку кіберзлочинності:

– недостатнє забезпечення правоохоронних органів спеціальними технічними засобами, що допоможуть виявити та розслідувати кіберзлочини (відсутність належних комп'ютерних систем та програмного забезпечення для виявлення злочинця – *О. Б., Д. Р.*);

– технічна складність відстеження інформаційних загроз (відсутність відповідного програмного забезпечення та кваліфікованих працівників у цій сфері – *О. Б., Д. Р.*);

– відсутність належної взаємодії правоохоронних органів та приватного бізнесу з питань захисту комп'ютерних мереж, надання необхідної інформації щодо порушень у віртуальному просторі (така взаємодія значно вдосконалить протидію кіберзлочинності, а також допоможе ефективніше та швидше усувати всі можливі загрози – *О. Б., Д. Р.*);

– недосконаліть чинного кримінального та кримінально-процесуального законодавства (у вітчизняному законодавстві немає поняття кіберзлочинності, а це ускладнює встановлення наявності та складу злочину – *О. Б., Д. Р.*);

– дуже слабка скоординованість у боротьбі з кіберзлочинністю, а також відсутність ефективного міжнародного співробітництва в цій сфері, що є необхідним складником у розкритті таких злочинів або хоча б зменшенні збитків від них (світовий досвід повинен залучатися і в Україні, оскільки треба рівнятися на розвинуті країни для того, щоб якомога ефективніше працювати в кіберсфері, сприяти залученню іноземних працівників, отриманню досвіду з новітніх технологій, необхідно модернізувати українське законодавство, зважаючи на успіхи інших країн – *О. Б., Д. Р.*).

Найпоширенішими сьогодні є такі типи злочинів:
– камкординг;
– кардшаринг;
– фальшиві інтернет-аукціони;
– розсилка листів (спам);
– азартні онлайн-ігри (зі вкладом грошей);
– створення вірусів;
– крадіжка персональних даних та особистої інформації.

Звичайно, що вищезазначений перелік кіберзлочинів не можна вважати вичерпним, але, на наш погляд, піратство сьогодні є найактуальнішим в Україні. Порушення авторських прав (інтернет-піратство) – це дії, спрямовані на незаконне використання об'єктів інтелектуальної власності, що належать іншим особам, свідомо вчинені особою, яка розуміє протиправний характер цих дій, для отримання прибутку.

Нині кіберзлочинність є одним із найпоширеніших видів суспільно небезпечних діянь. Темпи зростання інтернет-піратствата збільшуються, їхня соціальна небезпека також.

Ми хочемо виділити саме камкординг та кардшаринг через їхню актуальність на території України. Що стосується цих видів інтернет-піратства, то зауважимо, що населення пострадянських країн через свою ментальність не готове платити кошти за фільм чи за перегляд телевізійних каналів, що є звичайним явищем для мешканців країнах Європи або Північною Америки. Також згадаємо заборону кінострічок і ТВ-каналів, що характерно саме для нашої країни, оскільки через військові дії на сході України в такий спосіб держава прагне унеможливити вплив країни-агресора в усіх сферах.

Правове регулювання цієї сфери в Україні досить сильно відстає від розвитку новітніх технологій, що, своєю чергою, ускладнює проблему з кіберзлочинністю. Будь-які фізичні особи вчиняють такі злочини за допомогою піратського програмного забезпечення, завдяки якому злочинці можуть отримати доступ до персональних даних фізичної або юридичної особи. За даними дослідження Асоціації виробників програмного забезпечення (BSA), на 2011 р. рівень піратства в Україні становив майже 85%. А за даними Міжнародного союзу інтелектуальної власності (ІІРА), Україна була визнана «піратом № 1» у світі [2].

Ст. 1 Закону України «Про авторське право і суміжні права» визначено поняття камкордингу. Якщо коротко, то це копія аудіовізуального твору, яка була зроблена в кінотеатрі або іншому подібному закладі під час демонстрації цього ж самого твору, для будь-яких цілей, без надання дозволу суб'єкта авторського права або суміжних прав [3].

Згідно із зчинним законодавством, порушення авторського права і суміжних прав (до яких належить камкординг) чітко визначено як кримінальний злочин, передбачений ст. 176 Кримінального кодексу (далі – КК) України, згідно з якою максимальний штраф становить від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або такий злочин карається виправними роботами на строк до двох років, або позбавленням волі на той самий строк [5]. На нашу думку, штраф у такому розмірі є непомірно малим, оскільки ми впевнені, що більшість згаданих злочинів завдає набагато більших збитків, ніж штраф максимум у 17 000 грн. Так, наприклад, відповідно до новин Української антипіратської асоціації за 12 червня 2017 р. сумчанин, який заробляв камкордингом, внаслідок своєї діяльності завдав збитків у розмірі майже 2,4 млн. грн., а водночас зазнав покарання у вигляді умовного терміну на рік та сплатив штраф у розмірі 2,4 тис. грн. Тож, можна дійти висновку, що він зазнав збитків у тисячу разів менше, ніж завдав. І таких випадків безліч, тому було б доречним більш ретельно розглянути питання камкордингу в Україні, більш чітко та справедливо [6].

Окрім камкордингу, поширений також ще один із видів інтернет-піратства, що сьогодні також є значною загрозою для захисту інтелектуальної власності окремих осіб і не тільки. Поняття кардшарингу також визначено в ст. 1 Закону України «Про авторське право і суміжні права». Кардшаринг – це спільне використання карток супутникового телебачення шляхом роздавання ключів через глобальну або локальну мережу [3].

Кардшаринг останнім часом став дуже популярним через політичну ситуацію з Росією, наслідком якої стала заборона майже всіх російських каналів на території України, хоча до цього багато українців дивилися російські телепередачі, а отже, з'явився попит на те, щоб у різний спосіб обійти блокування. Але є окремі недоліки цього інтернет-піратства, а саме, має бути постійна наявність стабільного та швидкого доступу до мережі Інтернет, ці самі сервери кардшарингу дуже нестабільні та недовговічні, що часто затрудняє швидке користування забороненими каналами, або тими, що не транслюються на території України [4].

Найголовнішим мінусом є те, що це злочин, і за нього передбачені відповідні міри покарання, визначені ст. 176 КК України [5].

Очевидним є те, що, як і з будь-яким злочином, з кардшарингом потрібно боротися. Але як? На нашу думку, треба покращувати системи захисту супутникових операторів, залучати для цього справжніх спеціалістів, підтримувати в будь-який спосіб цю систему безпеки, а також залучатися підтримкою представників іншого оператора для того, щоб спільними зусиллями побороти або мінімізувати такий вид інтернет-піратства.

Висновки. Зважаючи на вищезазначене, можна дійти висновку, що кіберзлочинність стала проблемою саме у XXI ст. у зв'язку зі жвавою модернізацією технологій та суспільства, і з кожним роком кількість кіберзлочинів, які поглинають все більше коштів, зростає. Звичайно, вживаються заходи щодо протидії такому виду злочинності, але їх не достатньо, тому потрібно розробляти нові методи боротьби, що дадуть набагато більше позитивних результатів, а також покращити або розробити системи захисту, які допоможуть уникнути або мінімізувати такі види злочинів. Сьогодні кібербезпека в Україні на дуже низькому рівні, не варто нехтувати таким важливим чинником, як безпека в інтернет-просторі, оскільки в передових країнах світу цей напрям є пріоритетним у внутрішній і зовнішній політиці країни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Голіна В., Головкін Б. Кримінологія: Загальна та Особлива частини: навчальний посібник. Х.: Право, 2014. 513 с. URL: http://lib-net.com/book/105_Kriminologiya_Zagalna_ta_Osobliva_chastini.html.
2. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби URL: https://www.gurt.org.ua/articles/34602/.
3. Про авторське право і суміжні права: Закон України. URL: http://zakon3.rada.gov.ua/laws/show/3792-12/page.
4. Зачем нужен кардшейринг URL: http://skatinfo.ru/society/zachem-nuzhen-kardsheyring-19-05-2015.html.
5. Кримінальний кодекс України від 7 березня 2018 р. URL: http://zakon3.rada.gov.ua/laws/show/2341-14/page6.
6. Українська антипіратська асоціація. URL: http://apo.kiev.ua/index.php.