ПИТАННЯ КРИМІНАЛЬНОГО ПРАВА, КРИМІНОЛОГІЇ ТА КРИМІНАЛЬНО-ВИКОНАВЧОГО ПРАВА

БУГЕРА О. І.,
кандидат юридичних наук, доцент,
доцент кафедри права
(Київський національний лінгвістичний університет)

УДК 343.97

ЗАГАЛЬНА КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА МЕРЕЖІ ІНТЕРНЕТ ТА ЗАПОБІГАННЯ ЗЛОЧИННОСТІ

Стаття присвячена дослідженню загальної кримінологічної характеристики мережі Інтернет. Встановлено, що загальна кримінологічна характеристика мережі Інтернет стосується насамперед кіберзлочинності. Обґрунтована доцільність розроблення методичних рекомендацій щодо використанням мережі Інтернет для запобігання злочинності.

Ключові слова: *мережа Інтернет, кримінологічна характеристика, злочинність, запобігання, методичні рекомендації.*

Статья посвящена исследованию общей криминологической характеристики сети Интернет. Установлено, что общая криминологическая характеристика сети Интернет касается прежде всего киберпреступности. Обоснована целесообразность разработки методических рекомендаций по использованию сети Интернет для предотвращения преступности.

Ключевые слова: *сеть Интернет, криминологическая характеристика, преступность, предупреждение, методические рекомендации.*

The article is devoted to the study of the general criminological characteristics of the Internet. It has been established that the general criminological characteristics of the Internet concern, first of all, cybercrime. The expediency of developing methodological recommendations on the use of the Internet for crime prevention is substantiated.

Key words: *Internet network, criminological characteristic, crime, prevention, methodical recommendations.*

Вступ. Стрімке впровадження цифрових технологій в усі сфери людського життя наприкінці XX – на початку XXI ст. зумовило появу нових суспільних відносин. Найбільш значущою і поширеною стала технологія Інтернет, яка з'єднала людей по всій земній кулі, зробила комунікації дешевими і безперешкодними, а також відкрила нові горизонти для всього світового співтовариства. Інтернет останнім часом дав людині безмежні можливості у сфері поширення інформації, дозволив виконувати фінансово-банківські операції, незважаючи на відстань і кордони. Однак варто зауважити, що, крім позитивного ефекту, Інтернет також може завдавати шкоди. Деякі особливості даної технології, які допомогли їй поширитися по всьому світу, створюють сприятливі умови для багатьох видів злочинної діяльності. Новизна суспільних відносин, що виникли в результаті появи Інтернету, і відсутність відповідного правового

поля щодо даної технології, призвели до безлічі проблем, що негативно впливають на становлення відносин у світовій комп'ютерній мережі, заснованих на законі. Викликає побоювання те, що величезний технічний потенціал і безмежні можливості Інтернету все частіше використовуються в злочинних цілях. До того ж Інтернет, з одного боку, дозволив більш ефективно і безкарно вчиняти традиційні злочини, а з іншого – створив нові, невідомі світовій спільноті види суспільно небезпечних посягань. Глобальна мережа останніми роками стала використовуватися не тільки для скоєння загальнокримінальних злочинів, але і для вкрай небезпечних діянь міжнародного значення, як-от мережева війна, інтернет-тероризм, інтернет-страйк, що загрожує безпеці цілих держав і всього світового співтовариства [1, с. 145–146].

Питання загальної кримінологічної характеристики мережі Інтернет з погляду кіберзлочинності (комп'ютерної злочинності) досліджували такі автори, як: В. Кутузов, В. Павловський, О. Головко, В. Голубєв, М. Дзігора, В. Марков, Д. Никифорчук, М. Погорецький, В. Семенов та ін.

Постановка завдання. У результаті науково-технічного прогресу суспільство реально відчуває наступ інформаційної революції. Її сутність учені зводять до зміни технічних основ способів передачі, зберігання і оброблення інформації, розвитку проводового і радіозв'язку, появи телебачення, що дозволяє більшій кількості людей бути причетними до світу подій. Україна, будучи органічною частиною світової спільноти, не може бути винятком. Становлення ринкової економіки, поява нових її галузей, лібералізація сфери інформаційних суспільних відносин зумовили справжній розквіт комп'ютерної злочинності [2, с. 227].

Метою статті є здійснення загальної кримінологічної характеристики мережі Інтернет, обґрунтування доцільності розроблення методичних рекомендацій щодо запобігання злочинності з використанням можливостей Мережі.

Результати дослідження. У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, зокрема злочинність, в її нових формах і проявах. Кіберзлочинність складається з різних видів злочинів, що вчиняються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі й інша особиста інформація як фізичних осіб, так і бізнесу та державного сектора. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні. Найпоширенішими видами кіберзлочинів у сучасному світі є: кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу, «трояни», «боти»); фішинг – клієнтам платіжних систем надсилаються повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи із проханням вказати свої рахунки та паролі; вішинг – у повідомленнях міститься прохання зателефонувати на певний міський номер, а під час розмови запитуються конфіденційні дані власника картки; онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку; піратство – незаконне поширення інтелектуальної власності в Інтернеті; кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення; соціальна інженерія – технологія управління людьми в інтернет-просторі; мальваре – створення та поширення вірусів і шкідливого програмного забезпечення; протиправний контент – контент, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства; рефайлінг – незаконна підміна телефонного трафіка [3].

Під час розгляду поняття злочинності, що пов'язана з використанням мережі Інтернет, необхідно зазначити, що в Конвенції про кіберзлочинність [4] зазначено, що до правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем належать: незаконний доступ; нелегальне перехоплення; втручання в дані; втручання в систему; зловживання пристроями. До правопорушень, пов'язаних із комп'ютерами, належать: підроблення, пов'язане з комп'ютерами; шахрайство, пов'язане з комп'ютерами. Правопорушення, пов'язані зі змістом, – це злочини, пов'язані з дитячою порнографією. У Конвенції також вказується на правопорушення, пов'язані з порушенням авторських та суміжних прав.

У ст. 2 Додаткового протоколу до Конвенції про кіберзлочинність [5], який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, який ратифіковано відповідно до Закону України «Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи», зазначено, що «расистський та ксенофобний матеріал» означає будь-який письмовий матеріал, будь-яке зображення чи будь-яке інше представлення ідей або теорій, які захищають, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої із цих дій.

У ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» [6] зазначено, що кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. Кіберзлочинність – сукупність кіберзлочинів.

Відповідно до Кримінального кодексу України [7], до злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку належать: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення з метою використання, поширення або збуту шкідливих програмних чи технічних засобів, а також їх поширення або збут; несанкціоновані збут або поширення інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового поширення повідомлень електрозв'язку.

Варто зазначити, що кіберзлочинність набуває глобального масштабу, оскільки необмежений доступ до мережі Інтернет, використання інформаційних технологій у повсякденному житті, легкість швидкого збагачення зваблюють все більше людей долучатися до такої злочинної діяльності [8, с. 74].

Говорячи про загальну кримінологічну характеристику мережі Інтернет, варто зазначити, що власне кримінологічна характеристика – це опис властивостей, закономірностей, тенденцій, чинників злочинності або окремих її видів, а також особи злочинців [9, с. 401].

Злочинність із використанням мережі Інтернет ототожнюється насамперед із кіберзлочинністю. Виділяють такі ознаки кіберзлочинності: ці злочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до них. Кіберзлочини вчиняються проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Отже, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину. Сьогодні найбільш поширена класифікація кіберзлочинів на 1) агресивні та 2) неагресивні. До першою групи належать: кібертероризм, погроза фізичної розправи (наприклад, передана електронною поштою), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, поширення цих матеріалів, отримання доступу до них). Друга група містить: кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство, поширення спаму та вірусних програм. Водночас цей різновид злочинів має високий рівень латентності. За експертними оцінками, рівень

латентності кіберзлочинів становить 90–95%. Кримінологічна характеристика особи кіберзлочинця вказує на те, що типовому кіберзлочинцю притаманні такі індивідуально-психологічні риси: виражені порушення емоційно-вольової сфери; відхилення в психосексуальному розвитку; виражені аутичні прояви в сполученні із соціальним аутсайдерством; користолюбство; мстивість; антигуманна спрямованість; озлобленість; відчуття нерівності чи другорядності; боязкість і лякливість у соціальних та міжособистих стосунках; заглибленість у свої думки, мрії, фантазії; філософське сприйняття світу; відсутність буттєвих ціннісних орієнтацій; викривлена (збочена) система життєвих цінностей; тотальна недовірливість та виражений цинізм; прагнення уникнути перешкод у подоланні життєвих труднощів. У механізмі детермінації кіберзлочинності можна умовно виділити такі групи чинників: соціальні, політичні, економічні, технологічні, психологічні, а також чинники, пов'язані з діяльністю правоохоронних органів та віктимною поведінкою потерпілих [10, с. 294–297].

Необхідно зазначити, що метою Стратегії кібербезпеки України [11] є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Боротьба з кіберзлочинністю передбачає здійснення установленим порядком, серед іншого, таких заходів: створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства в кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їхніх регіональних підрозділів; удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень; запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду; унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік; врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису; упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю; підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів; запровадження особливого порядку зняття інформації з каналів телекомунікацій у разі розслідування кіберзлочинів; підвищення кваліфікації співробітників правоохоронних органів.

Зважаючи на важливість запобігання кіберзлочинності та досягнення кібербезпеки, Указом Президента України від 7 червня 2016 р. № 242/2016 затверджено Положення про Національний координаційний центр кібербезпеки [12]. Основними завданнями Центру є: 1) здійснення аналізу: стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів гарантування кібербезпеки до виконання завдань із питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю; 2) участь у розробленні галузевих індикаторів стану кібербезпеки; 3) прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України; 4) розроблення концептуальних засад та пропозицій щодо гарантування кібербезпеки держави, спрямованих на підвищення ефективності заходів щодо виявлення й усунення чинників, які формують потенційні та реальні загрози у сфері кібербезпеки, підготовка проектів відповідних програм та планів щодо їх попередження та нейтралізації; 5) узагальнення міжнародного досвіду у сфері гарантування кібербезпеки.

Висновки. У підсумку необхідно зазначити, що загальна кримінологічна характеристика мережі Інтернет стосується насамперед кіберзлочинності. Основними ознаками кіберзлочинності є те, що кіберзлочини вчиняються здебільшого з використанням мережі Інтернет та за допомогою комп'ютерних систем.

Проблема профілактики кіберзлочинності та боротьби з нею в Україні є комплексною. Сьогодні закони повинні відповідати вимогам, висунутим сучасним рівнем розвитку

комп'ютерних технологій. Пріоритетним напрямом є також організація взаємодії та координація зусиль правоохоронних органів, спецслужб, судової системи як на національному, так і на міжнародному рівні [13, с. 117].

На нашу думку, одним з ефективних шляхів запобігання злочинності (зокрема, кіберзлочинності) є використання можливостей мережі Інтернет. Для цього необхідне розроблення відповідних методичних рекомендацій, які можуть мати таку структуру: загальні положення; визначення понять; мета та завдання використання мережі Інтернет для запобігання злочинності; особливості використання інтернет-технологій для збирання, зберігання й аналізу кримінологічно значущої інформації, здійснення оперативно-розшукових дій, підвищення рівня правової культури громадян та ін.

Список використаних джерел:

1. Солдатова В. Окремі заходи попередження і боротьби з кіберзлочинністю. Вісник Кримінологічної асоціації України. 2013. № 3. С. 145–155. URL: https: //files.visnikkau.org/200001289-0b2090c1e7/Visnyk3_17.pdf (дата звернення: 20.09.2018).

2. Ступник Я., Когут М. Протидія наркозлочинності в мережі Інтернет: виклики сьогодення. Науковий вісник Ужгородського національного університету. Серія «Право». Випуск 26. 2014. С. 226–230. URL: https://dspace.uzhnu.edu.ua//ПРОТИДІЯ%20НАРКОЗЛОЧИННОСТІ%20В%20М (дата звернення: 20.09.2018).

3. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // Ресурсний центр ГУРТ: сайт. URL: https://www.gurt.org.ua /articles/34602/ (дата звернення: 20.09.2018).

4. Конвенція про кіберзлочинність від 23 листопада 2001 р. Конвенцію ратифіковано із застереженнями і заявами Законом № 2824–IV від 7 вересня 2005 р. Відомості Верховної Ради України. 2006. № № 5–6. Ст.71.

5. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28 січня 2003 р. Протокол ратифіковано із застереженням Законом № 23–V від 21 липня 2006 р. Відомості Верховної Ради України. 2006. № 39. Ст. 328.

6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163–VIII. Відомості Верховної Ради. 2017. № 45. Ст. 403.

7. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341–III. Відомості Верховної Ради України. 2001. № № 25–26. Ст. 131.

8. Русецький А., Куцолабський Д., Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». Право і безпека. 2017. № 1 (64). С. 74–78. URL: //https: oaji.net/pdf.html?n=2017/2258-1494833207.pdf (дата звернення: 20.09.2018).

9. Кримінологія: підручник для студентів вищих навч. закладів / О. Джужа, Я. Кондратьєв, О. Кулик, П. Михайленко та ін.; за заг. ред. О. Джужи. К.: Юрінком-Інтер, 2002. 416 с.

10. Голіна В., Головкін Б. Кримінологія: Загальна та Особлива частини: навчальний посібник. Х.: Право, 2014. 513 с.

11. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 20.09.2018).

12. Положення про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 р. № 242/2016. URL: http://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 20.09.2018).

13. Семенов В., Дзігора М. До питання боротьби з кіберзлочинністю в Україні. Прикарпатський юридичний вісник. Випуск 6 (15). 2016. С. 174–178. URL: http:// pjv.nuoua.od.ua/v6_2016/41.pdf (дата звернення: 20.09.2018).