УДК 343.9.024: (343.533:004)

Г. М. Чернишов
кандидат юридичних наук, доцент кафедри кримінології
та кримінально-виконавчого права
Національного університету «Одеська юридична академія»

КІБЕРЗЛОЧИННІСТЬ ЯК ВИКЛИК ГЛОБАЛІЗАЦІЇ ТА ЗАГРОЗА СВІТОВІЙ БЕЗПЕЦІ: ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Глобалізаційні перетворення зробили інформаційні технології доступними та поширеними по всьому світу. За останні кілька десятиліть використання телекомунікаційних та комп'ютерних систем вийшло на абсолютно новий рівень, що призвело до глобальної інформатизації суспільних відносин та появи суспільства нового типу – інформаційного суспільства.

Цифрові технології стали основою появи електронної економіки, а разом з нею – усіх супутніх засобів ведення економічної діяльності: електронних грошей, системи безготівкових розрахунків та віртуальних ринків.

Але інформатизація стосується не лише економічних відносин. Сьогодні практично усі форми людської діяльності, так чи інакше, пов'язані з роботою комп'ютерів та мережі Інтернет, тобто є комп'ютеризованими. Це робить функціонування всіх без винятку сфер суспільного життя залежними від роботи комп'ютерів та інших електронних пристроїв.

На серверах, жорстких дисках та інших носіях інформації зберігаються особисті, комерційні та інші конфіденційні дані, що можуть стати об'єктами цілеспрямованого викрадення, шпіонажу, та, пов'язаних з цим, інших злочинних посягань. Несанкціоноване втручання у роботу цих систем може мати наслідки не тільки у підриві особистої безпеки фізичних або юридичних осіб, але й національної та навіть міжнародної безпеки.

Крім того, сьогодні мережа Інтернет у цілому виступає самостійною платформою для вчинення абсолютно різних за спрямуванням, небезпечністю та наслідками правопорушень: втручання у роботу систем; порушення авторських та суміжних прав; поширення дитячої порнографії; шахрайство; торгівля наркотиками, зброєю; проституція та інші форми торгівлі людьми; розпалювання національної, расової чи релігійної ворожнечі та ненависті; вербування учасників терористичних організацій та втягнення у вчинення терористичного акту; фінансування тероризму; пропаганда війни тощо. Масове поширення таких проявів протиправної активності призвело до появи якісно нового різновиду злочинної активності – кіберзлочинності.

Використання сучасних електронних технологій надає необмежені можливості для ведення злочинної діяльності по всьому світу. Руйнуючи національні кордони, кіберзлочинність стала транснаціональною проблемою та у сучасних умовах є однією з головних загроз XXI століття.

Проблемам впливу інформаційно-комунікаційних технологій на суспільне життя, інформаційній безпеці, кіберзлочинності та кібербезпеці присвячені роботи багатьох учених у галузі кібернетики, інформатики, економіки та фінансів, цивілістики, кримінального права, кримінології, криміналістики та інших наук. Різні аспекти згадуваної проблематики розглядаються у роботах таких вітчизняних та зарубіжних учених, як Д.С. Азаров, Ю.М. Батурин, П.Д. Біленчук, О.І. Бугера, В.М. Бутузов, С.А. Буяджи, В.В. Гостєв, М.В. Гуцалюк, М.А. Дем'янчук, В.М. Дрьомін, Д.В. Дубов, С.В. Кавун, О.В. Климчук, А.А. Комаров, А.П. Леонов, В.В. Лунєєв, В.В. Марков, В.А. Номоконов, Ю.М. Онищенко, К.С. Пивоварська, Н.А. Розенфельд, Т.Л. Тропіна, Д.М. Цехан, В.Т. Шатун та інших.

Метою статті є визначення поняття кіберзлочинності та її основних проявів.

Бурхливий розвиток телекомунікаційних технологій супроводжується процесами масової віктимізації їх користувачів. На протязі тривалого часу термін «кіберзлочинність» так і не здобув загального універсального визначення на конвенціональному рівні чи в інших міжнародних правових документах. Учені та спеціалісти з різних галузей знань доклали чимало зусиль для розкриття сутності цього явища та інтерпретації основних його проявів.

У науковій літературі для характеристики злочинів, які вчиняються у кіберпросторі, використовуються різні поняття: «кіберзлочинність», «комп'ютерна злочинність», «злочинність у сфері використання електронно-обчислювальних машин», «злочинність у сфері високих технологій», «злочинність у сфері інформаційних технологій», «злочини у сфері ІТ-технологій», «інформаційна злочинність», «hi-tech злочини» тощо.

Не маючи на меті визначення та розмежування усіх указаних понять, слід зазначити, що термін «кіберзлочинність» є універсальним та найбільш вдалим для використання у межах даного дослідження. Пояснюється це тим, що, по-перше, саме термін «кіберзлочинність» (cybercrime) отримав

законодавче закріплення на міжнародному та вітчизняному рівнях. Це Конвенція Ради Європи «Про кіберзлочинність» [1], Закон України «Про основні засади забезпечення кібербезпеки України» [2].

Крім того, підтвердженням практичної поширеності як універсального терміну «кібер» є створення у 2015 р. Департаменту кіберполіції Національної поліції України [3]. Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність [4].

У багатьох країнах світу діють спеціалізовані суб'єкти забезпечення кібербезпеки, які також у своїй назві використовують корінь «кібер» (cyber): наприклад, у США, Великій Британії та Німеччині – Національні центри кібербезпеки (National Cybersecurity Center, Nationales Cyber-Abwehrzentrum) і т.д.

По-друге, префікс «кібер» у даному випадку робить акцент не тільки на способи та засоби вчинення злочинів, але й на специфічне середовище реалізації злочинного умислу – кіберпростір. Використання терміну «кіберзлочинність» охоплює більшу за обсягом сферу, аніж, наприклад, «комп'ютерна злочинність», «Інтернет злочинність». Поняття «кіберпростір» у даному випадку є родовим, універсальним, що об'єднує функціонування всіх систем комунікації, зв'язку, комп'ютерів, мережі Інтернет, інших автоматизованих пристроїв та інформаційних технологій.

Схожу точку зору висловлюють В.А. Номоконов та Т.Л. Тропіна. Учені зазначають, що поняття кіберзлочинності як сукупності злочинів поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину [5, с. 88].

В.М. Дрьомін, досліджуючи місце мережі Інтернет у механізмі інституціоналізації злочинності, звертає увагу на глобалізацію кіберзлочинності та її транснаціональний характер. Він зазначає: «комп'ютерні злочини небезпечні не тільки самі по собі, але й тим, що створюють умови для вчинення нових злочинів, розширюють сферу кримінальної дійсності та сприяють відтворенню злочинності, глобалізуючи її. Електронна комунікація може бути використана злочинцями для планування або координації практично усіх незаконних дій у будь-якій точці світу. Інтернет сприяє інституціоналізації неформальних соціальних практик, адже неформальні стандарти спілкування набувають глобальний та фактично неконтрольований характер» [6, с. 370-371, 377].

Згадувана вище Конвенція Ради Європи «Про кіберзлочинність» не містить визначення кіберзлочинності. Відповідна дефініція міститься у нормах національного законодавства, а саме у Законі України «Про основні засади забезпечення кібербезпеки України».

Так, у ст. 1 цього закону кіберзлочинність визначається як сукупність кіберзлочинів. У свою чергу, кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2]. Цей же нормативний документ визначає кіберпростір як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене у результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [2].

Одними з перших з вітчизняних дослідників, хто звернув увагу на загрози кіберзлочинності були П.Д. Біленчук та М.А. Зубань. На самому початку незалежності, 25 років тому, коли комп'ютерами та, тим більше, мережею Інтернет у нашій країні мало хто користувався, вийшов навчальний посібник «Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти» [7]. Під комп'ютерними злочинами запропоновано розуміти суспільно небезпечні дії або бездіяльність, що здійснюються з використанням сучасних технологій і засобів комп'ютерної техніки, з метою заподіяння шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадських організацій і громадян, а також правам особи [7, с. 6].

Слід погодитись із думкою В.А. Номоконова, який вказує, що явище кіберзлочинності складають собою злочини, вчинені у кіберпросторі. Він пише: «кіберзлочинність – це сукупність злочинів, що здійснюються у кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних» [8, с. 48].

Порівнюючи близькі за змістом категорії «кіберзлочинність» та «комп'ютерна злочинність», В.А. Номоконов та Т.Л. Тропіна зазначають, що ці терміни дуже близькі за змістом, але не синонімічні. Поняття «кіберзлочинність» ширше, ніж

«комп'ютерна злочинність», і більш точно відображає природу такого явища, як злочинність в інформаційному просторі [5, с. 87].

М.О. Кравцова у межах власного дисертаційного дослідження під кіберзлочинністю пропонує розуміти соціально-правовий феномен, що проявляється у забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [9, с. 7].

Дещо дискусійні визначення кіберзлочинів та кіберзлочинності формулює С.А. Буяджи: «кіберзлочинами є найбільш небезпечні кіберправопорушення, вчинення яких на різних стадіях безпосередньо пов'язане із використанням комп'ютерної техніки через комп'ютерні системи, або із комп'ютерними системами, та за які чинним законодавством передбачено кримінальну відповідальність» [10, с. 39, 178]. «Кіберзлочинність – сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об'єктів, розташованих на ній за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі і комп'ютерні дані» [10, с. 25; 11, с. 6].

В.М. Бутузов пропонує розглядати комп'ютерну злочинність як підсистеми злочинності у сфері високих інформаційних технологій, яка пов'язана із протиправним використанням комп'ютерних технологій автоматизованої обробки інформації. Зазначається, що злочини у сфері високих інформаційних технологій – вчинені умисно або з необережності суспільно небезпечні діяння (дії або бездіяльність), що посягають на відносини у сфері обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, надання та отримання телекомунікаційних послуг, проведення електронних розрахунків [12, с. 303].

Беручи за основу теоретичний аналіз наукових напрацювань інших учених, а також законодавче трактування кіберзлочинів, можемо надати наступне визначення кіберзлочинності.

Кіберзлочинність – явище, яке виражається у системі злочинів, вчинених у кіберпросторі з використанням та/або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку.

Інакше кажучи, кіберзлочинність – злочини, вчинені з використанням та/або проти кіберпростору. Кіберзлочинність – злочини, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення.

Таким чином, кіберзлочинність має такі основні ознаки:

1) специфічне середовище (сфера) злочинних посягань – кіберпростір;

2) використання кіберпростору як способу вчинення злочинів;

3) злочинні посягання проти кіберпростору (несанкціоноване втручання у роботу комп'ютерів, комп'ютерних мереж або систем, а також інших телекомунікаційних мереж тощо).

Конвенція Ради Європи «Про кіберзлочинність» [1] та додатковий протокол до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [13], передбачають криміналізацію наступних кіберзлочинів:

1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ; нелегальне перехоплення комп'ютерних даних; втручання у дані; втручання у систему; зловживання пристроями.

2. Правопорушення, пов'язані з комп'ютерами: підробка і шахрайство, пов'язані з комп'ютерами.

3. Правопорушення, пов'язані зі змістом (з контентом): правопорушення, пов'язані з дитячою порнографією.

4. Правопорушення, пов'язані з порушенням авторських та суміжних прав.

5. Дії расистського та ксенофобного характеру, вчинені через комп'ютерні системи: поширення расистського та ксенофобного матеріалу через комп'ютерні системи; погроза з расистських та ксенофобних мотивів; образа з расистських та ксенофобних мотивів; заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства.

Кримінальна відповідальність за кіберзлочини передбачена різними розділами та статтями КК України. Це розділ XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електронного зв'язку» (ст. ст. 361, 361-1, 361-2, 362, 363, 363-1); ч. 3 ст. 190 «Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки»; ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення».

Про комп'ютери, комп'ютерні програми та інші спеціальні пристрої як засоби вчинення злочинів указується у ст. 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер», ст. 173 «Порушення авторського права і суміжних прав» КК України.

Кіберзлочинність у сучасних умовах інформаційного суспільства та глобальної комп'ютеризації є однією з найбільших загроз світовій безпеці.

Кіберзлочинність – явище, яке виражається у системі злочинів, вчинених у кіберпросторі з використанням та/або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку.

Кіберзлочинність – злочини, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення.

Кіберзлочинність – не єдина загроза інформаційній безпеці. Є й інші ризики, які безпосередньо пов'язані з роботою сучасних високих технологій. Мова йде не лише про використання телекомунікаційних мереж у злочинній діяльності, але й про тотальне порушення громадянських прав та свобод.

Сьогодні боротьба з тероризмом, екстремізмом, шпіонажем та іншими загрозами національної безпеки нерідко пов'язана з втручанням в особисте життя. Крім того, браузери, електрона пошта, соціальні мережі, мобільні додатки, пошукові та платіжні системи відкрито (про що говориться у політиці конфіденційності цих сервісів) чи негласно збирають інформацію про своїх користувачів.

Цифрова інформація, яка в автоматичному комп'ютеризованому режимі збирається, аналізується та зберігається відповідними організаціями та службами, несе у собі відомості щодо об'єктів спостереження, якими, як правило, виступають звичайні громадяни. Якщо додати до цього автоматизовані персональні дані за місцем навчання, роботи, медичного обслуговування, дані з різного роду електронних реєстрів (наприклад, у нашій країні – це єдині реєстри військовозобов'язаних, внутрішньо переміщених осіб, електронних декларацій та ін.), які не рідко передаються, викрадаються або використовуються не за призначенням, то фактично відкрито доступ до усіх особистих даних кожної особи.

Все це руйнує кордони особистого та недоторканого. Враховуючи кількість активних користувачів Інтернету по всьому світу, можна вести мову про тотальне стеження, яке вже неодноразово ставало темою різних авторитетних міжнародних форумів. Це дозволяє стверджувати, що права людини порушуються не тільки злочинністю, але й діяльністю щодо протидії їй.

Література

1. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р.: ратифікована Законом України від 07.09.2005 р. Відомості Верховної Ради. 2006. № 5-6. Ст. 71.

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

3. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13 жовтня 2015 р. URL: http://zakon.rada.gov.ua/laws/show/831-2015-п

4. Про підрозділ / Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/contacts/

5. Номоконов В.А., Тропина Т.Л. Киберпреступность: угрозы, прогнозы, проблемы борьбы. Information Technology and Security. 2013. № 1. С. 86-94.

6. Дрьомін В.М. Злочинність як соціальна практика: інституціональна теорія криміналізації суспільства: монографія. О.: Юридична література, 2009. 616 с.

7. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навч. посіб. К.: Українська академія внутрішніх справ, 1994. 72 с.

8. Номоконов В. А., Тропина Т.Л. Киберпреступность как новая криминальная угроза. Криминология: вчера, сегодня, завтра. 2012. № 1. С. 45-55.

9. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. … канд. юрид. наук: 12.00.08 / Харк. нац. ун-т внутр. справ. Харків, 2016. 16 с.

10. Буяджи С.А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект: дис. … канд. юрид. наук: 12.00.01 – Теорія та історія держави і права; історія політичних і правових учень / Класичний приватний університет, Ун-т Короля Данила. Київ, 2018. 203 с.

11. Буяджи С.А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект: автореф. дис. … канд. юрид. наук: 12.00.01 – Теорія та історія держави і права; історія політичних і правових учень. Івано-Франківськ, 2018. 16 с.

12. Бутузов В.М. Співвідношення понять «комп'ютерна злочинність» і «злочинність у сфері високих інформаційних технологій». Боротьба з організованою злочинністю і корупцією (теорія і практика). 2010. Вип. 23. С. 302-307.

13. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р.: Ратифіковано із застереженням Законом України від 21.07.2006 р. Відомості Верховної Ради. 2006. № 39. Ст. 328.

Анотація

Чернишов Г. М. **Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження.** – Стаття.

Стаття присвячена дослідженню кіберзлочинності як транснаціональної проблеми та загрози світовій безпеці. На підставі детального теоретичного аналізу розкривається сутність та надається кримінологічне визначення поняття «кіберзлочинність». Аналізуються основні прояви кіберзлочинності, передбачені міжнародними документами та актами вітчизняного законодавства.

Ключові слова: глобалізація, кіберзлочинність, кіберзлочини, комп'ютерна злочинність, інформаційна безпека.

Аннотация

Чернышев Г. М. **Киберпреступность как вызов глобализации и угроза мировой безопасности: теоретические основы исследования.** – Статья.

Статья посвящена исследованию киберпреступности как транснациональной проблемы и угрозы мировой безопасности. На основании детального теоретического анализа раскрывается сущность и предоставляется криминологическое определение понятия «киберпреступность». Анализируются основные проявления киберпреступности, предусмотренные международными документами и актами отечественного законодательства.

Ключевые слова: глобализация, киберпреступность, киберпреступления, компьютерная преступность, информационная безопасность.

Summary

Chernyshov H. M. **Cybercrime as a challenge to globalization and as a threat to world security: theoretical foundations of the study.** – Article.

The article deals with issues related to the study of cybercrime as a transnational problem and as a threat to global security. Based on a detailed theoretical analysis, the essence is revealed and a criminological definition of the concept of «cybercrime» is given. The main manifestations of cybercrime, provided by international documents and acts of domestic legislation, are analyzed.

Key words: globalization, cybercriminality, cybercrime, computer crime, information security.