УДК 002.6:341.48

СКУЛИШ Є.Д., *доктор юридичних наук, професор,*
Заслужений юрист України

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИЗНАЧЕННЯ ОБ’ЄКТА ТА ПРЕДМЕТА КІБЕРЗЛОЧИНІВ

Анотація. *У статті розглянута проблема, що стосується визначення об’єкта та предмета кіберзлочинів. Вказано на те, що цей вид злочинності має самостійний предмет та об’єкт, що дає змогу не змішувати його із комп’ютерними злочинами.*

Ключові слова: *кіберзлочинність, об’єкт, предмет, суспільні відносини, злочинне посягання.*

Аннотация. *В статье рассмотрена проблема, которая касается определения объекта и предмета киберпреступлений. Указано, что этот вид преступности имеет самостоятельный предмет и объект, что позволяет не смешивать его с компьютерными преступлениями.*

Ключевые слова: *киберпреступность, объект, предмет, общественные отношения, преступное посягательство.*

Summary. *The article considers the problem concerning the determination of crime object and the crime subject. It is indicated on that this type of criminality has independent crime object and the crime subject, that enables not to mix it up with computer-related crimes.*

Keywords*: computer-facilitated criminality, crime object, crime subject, public relations, criminal trespass.*

Постановка проблеми. Комп’ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань, показники поширення яких швидко збільшуються, що зумовлено прискореним розвитком інформаційних технологій та постійним і стрімким розширенням сфери застосування комп’ютерної техніки.

Серед безлічі причин цієї ситуації присутні не тільки процесуальні та криміналістичні труднощі виявлення, розкриття і розслідування більшості видів кіберзлочинів. В умовах постійно мінливого, не повною мірою кодифікованого і не завжди досконалого законодавства, складні схеми, які застосовуються кіберзлочинцями, широкий спектр злочинів, які вчиняються в кіберпросторі, не додають прозорості у розумінні основних ознак більшості складів цих злочинів.

На сьогодні немає єдиного розуміння щодо обсягу протиправних посягань, які можуть розцінюватися як кіберзлочини, а також є проблема із відмежуванням кіберзлочинності як принципово нового виду злочинної діяльності від злочинів, які традиційно вчиняються з використанням комп’ютерних технологій. Особливо проблематичними в цьому плані є такі ознаки, як об’єкт та предмет кіберзлочинів, які, являючи собою характерні риси загального поняття “кіберзлочинність”, безпосередньо окреслюють сферу застосування тієї чи іншої кримінально-правової норми.

Водночас, ця проблема є принципово важливою з точки зору теоретико-методологічних засад визначення об’єкта та предмета кіберзлочинів. Труднощі в цьому плані пов’язані з тим, що вони вчиняються не в середовищі матеріального світу, а в ідеальному “віртуальному середовищі”, коли важко виокремити традиційні елементи складу злочину, дослідити сукупність юридичних об’єктивних і суб’єктивних ознак, що характеризують групу суспільно небезпечних діянь, спрямованих на заподіяння шкоди правам і свободам людини, інтересам суспільства і держави, за вчинення яких передбачено покарання [13, с. 8].

Важливість теми дослідження пояснюється труднощами, пов’язаними з розумінням і застосуванням об’єкта та предмета кіберзлочинів, а також визначенням переліку кіберзлочинів за їх предметом.

Питання, пов’язані з існуванням кіберзлочинності як принципово нового виду злочинної діяльності, досліджували Н.Ф. Ахраменка, Ю.М. Батурин, А.М. Жодзишський, А.Г. Волеводз, В.Ю. Максимов та ін. Ці автори розвинули теоретичні уявлення про кіберзлочинність, зазначили, що ці злочини спрямовані проти встановленого порядку суспільних відносин, який регулює виготовлення, використання, поширення і захист комп’ютерної інформації, і вважають, що об’єктом комп’ютерних злочинів виступають відносини щодо безпечного використання комп’ютерної інформації [5, с. 23].

Проте, продовжує існувати проблема остаточного визначення об’єкта та предмета кіберзлочинності, що є суттєвою прогалиною сучасної науки і потребує додатково уточнення.

Метою статті є уточнення визначення об’єкта та предмета кіберзлочинності.

Виклад основного матеріалу. Для визначення безпосередньо об’єкта кіберзлочинності методологічно вірним буде звернення до теорії інформаційної безпеки та до тих теоретико-практичних напрацювань, які стосуються цієї проблеми. У свою чергу, визначення об’єкта кіберзлочинності є теоретико-методологічною базою для визначення предмета злочинів, які поєднуються цим терміном в окремий вид злочинної діяльності.

Звертаючись до розгляду цього питання, треба насамперед вказати на те, що основне функціональне призначення загального складу злочину полягає в тому, що він виступає як правова модель злочину або є законодавчою конкретизацією такої ознаки злочину, як протиправність. Склад злочину вказує на ті ознаки, лише при наявності яких суспільно небезпечна поведінка може бути визнана злочином, в даній структурі об’єкт і предмет у сукупності утворюють самостійний елемент складу злочину. У науці традиційно вважається, що об’єктом злочину є суспільні відносини, на які посягають злочини, а предметом злочину слід вважати будь-які речі матеріального світу, з певними властивостями яких кримінальний закон пов’язує наявність у діях особи ознак конкретного складу злочину [6, с. 22-24].

Відповідно до цих визначень виділення в структурі кіберзлочинності її об’єкта не викликає суттєвих складнощів, інша справа, коли йдеться про її предмет, оскільки ним у даному випадку є ідеальна субстанція, а саме – інформація. Здається, що ідеальна сутність інформації не дає змоги визначитися з предметом даного виду злочинності, але якщо вдатися до наукових джерел, то можна виділити інформацію в окремий елемент матеріального світу, яка існує в будь-якому матеріальному об’єкті у вигляді різноманіття його станів і передається від об'єкта до об'єкта в процесі їх взаємодії [4].

Відповідно матеріальність інформації вимагає її правового захисту від злочинних посягань, хоча самі злочини, які здійснюються в цій сфері потребують певної структуризації з метою правильного визначення їх об’єкта та предмета.

Термін “кіберзлочинність” у наш час часто вживається поряд з терміном “комп’ютерна злочинність”, причому нерідко ці поняття використовуються як синоніми. У вітчизняній літературі найбільша перевага віддається поняттю “комп’ютерна злочинність”. Дійсно, ці терміни дуже близькі, але все-таки не синонімічні, поняття “кіберзлочинність” (в англомовному варіанті – cybercrime) ширше, ніж “комп’ютерна злочинність” (computer crime) і більш точно відображає природу такого явища, як злочинність в інформаційному просторі [12].

Аналіз наукової літератури, норм Кримінального кодексу та міжнародного права також дає змогу автору цієї статті дійти висновку, що в структурі нинішньої злочинності,

які пов’язана із використанням комп’ютерної техніки та інформаційних технологій, доцільно відокремлювати дві самостійні групи, які відрізняються власним об’єктом та предметом, – комп’ютерну злочинність та кіберзлочинність.

Ця позиція підтверджується і тим, що на X Конгресі ООН з попередження злочинності і поводження із правопорушниками, пов’язаними з комп’ютерами та комп’ютерними мережами, поняття про кіберзлочини розглядалося з точки зору двох аспектів:

1. Кіберзлочин у вузькому сенсі (комп’ютерний злочин): будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є безпека комп’ютерних систем і оброблюваних ними даних.

2. Кіберзлочин у широкому розумінні (як злочин, пов’язаний з комп’ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов’язане з комп’ютерами, комп’ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп’ютерних систем або мереж [12].

Звернення до напрацювань попередників, зокрема Ю.М. Батурина і А.М. Жодзишського, свідчать, що історично першою формою цього виду злочинності є злочинність комп’ютерна. Науковці вважали, що об’єктом комп’ютерних злочинів є відносини суспільної безпеки з приводу роботи комп’ютерної техніки та комп’ютерних систем [1, с. 89], що знаходять свій вираз у викраденні комп’ютерних даних, їх перекрученні, блокуванні роботи комп’ютерів та комп’ютерних систем, порушенні маршрутизації чи знищенні інформації, яка міститься у комп’ютерах та у комп’ютерній мережі [7, с. 49].

При цьому, Конвенція Ради Європи про кіберзлочинність визначає чотири типи комп’ютерних злочинів “у чистому вигляді”, розглядаючи їх як злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем:

1. Незаконний доступ – протиправний навмисний доступ до комп'ютерної системи або її частини.

2. Незаконне перехоплення – протиправне умисне перехоплення не призначених для громадськості передач комп’ютерних даних на комп'ютерну систему, з неї або в її межах.

3. Втручання в дані – протиправне пошкодження, видалення, порушення, зміна або припинення комп’ютерних даних.

4. Втручання в систему – серйозне протиправне перешкоджання функціонуванню комп’ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміни або припинення комп’ютерних даних [2, с. 67].

Згідно з розділом XVI чинного Кримінального кодексу України до комп’ютерних злочинів віднесені злочини щодо використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Предметом цих злочинів є комп’ютери та комп’ютерні мережі, тобто сукупність інформаційних ресурсів, програмних і технічних засобів, на які здійснюється злочинне посягання. Об’єктивна сторона злочинів, як правило, проявляється у формі незаконного втручання у роботу комп’ютерних мереж та комп’ютерів, що тягне за собою негативні наслідки для власника, призводить до знищення, перекручення комп’ютерної інформації.

Подальший розвиток інформаційного суспільства, комп’ютерної техніки, мережевих технологій, призвели до виникнення принципово нового виду злочинності – кіберзлочинності, яка має власний об’єкт та предмет, яким, на думку автора даної статті, слід вважати інформаційну безпеку.

Звертаючись до нормативних джерел, зокрема до Доктрини інформаційної безпеки України, можна визначити, що ця проблема є вкрай актуальною, оскільки за сучасних умов

інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки [8]. Саму ж інформаційну безпеку науковці включають до складу національної безпеки, виходять з того, що інформаційна безпека являє собою напрям державної політики, що спрямований на безперешкодну реалізацію суспільством і окремими його членами своїх конституційних прав, пов’язаних з можливістю вільного одержання, створення й розповсюдження інформації [3].

У свою чергу Законом України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” визначено, що інформаційна безпека являє собою стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [9].

Це широке трактування інформаційної безпеки знаходить підтримку у науковців, які досліджують проблематику кіберзлочинності. Так, наприклад, А.О. Стрельцов визначає інформаційну безпеку як сукупність суспільних відносин, що складаються в процесі захисту інформаційних ресурсів та охорони прав суб’єктів інформатизації, а також забезпечення безпеки користувачів і користування комп’ютерними системами і мережами [11, с. 76].

М.О. Сивицька вважає, що родовим об’єктом цієї групи злочинів виступає інформаційна безпека, під якою розуміється специфічна група суспільних відносин, зміст якої складають права та інтереси різних суб’єктів у сфері забезпечення безпеки використання інформації та інформаційних ресурсів, необхідних для нормальної життєдіяльності соціуму [10, с. 87].

Якщо ж звернутися безпосередньо до переліку злочинів, які входять до структури кіберзлочинності, то слід зазначити, що на X Конгресі ООН було запропоновано кілька категорій кіберзлочинів. Одна з класифікацій передбачає поділ на: насильницькі або інші потенційно небезпечні (загроза фізичної розправи, кіберпереслідування, дитяча порнографія, кібертероризм) і ненасильницькі злочини (протиправне порушення володіння у кіберпросторі, кіберкрадіжка, кібершахрайство, реклама послуг проституції в мережі Інтернет, незаконний обіг наркотиків з використанням мережі Інтернет, азартні ігри в мережі Інтернет, відмивання грошей за допомогою електронного переміщення, деструктивні кіберзлочини, інші кіберзлочини) [12].

Характеризуючи ці злочини, Д.Л. Шиндер вказує, що кібертероризм – це тероризм, спланований, вчинений або скоординований у кіберпросторі – тобто за допомогою комп’ютерних мереж [14].

Ця категорія злочинів включає також використання електронної пошти для зв'язку між учасниками злочинної змови, передачі інформації, що використовується для здійснення насильницьких дій, вербування нових учасників терористичних груп через веб-сайти мережі Інтернет.

Кіберпереслідування – форма електронного переслідування, яка найчастіше пов'язана з явно вираженими або уявними фізичними погрозами, що створюють відчуття небезпеки у жертви. Іноді це переростає у переслідування в реальному житті і агресивну поведінку. Загроза фізичної розправи може бути передана через електронну пошту. Цей злочин полягає у заподіянні особі постійного страху за власне життя чи за життя дорогих їй людей (це правопорушення іноді називають терористичною загрозою). До цього виду злочинів можна також віднести передані електронною поштою фірмам або владним структурам загрози, наприклад, вибуху бомби.

У свою чергу дитяча порнографія має безліч проявів: створення порнографічних матеріалів за участю неповнолітніх, поширення цих матеріалів, одержання доступу до них. Коли будь-яка з цих дій пов’язана з використанням комп’ютерів або комп'ютерних мереж, дитяча порнографія стає кіберзлочином. Дитяча порнографія зазвичай вважається тяжким злочином, навіть якщо особи, залучені до її виробництва, не мали ніякого фізичного контакту з дітьми. Причиною цього є те, що для виробництва подібних порнографічних матеріалів потрібна сексуальна експлуатація дітей. Крім того, споживачі цих матеріалів часто не обмежуються інтересом до картинок і сексуальних фантазій, а й практикують або прагнуть практикувати педофілію в реальному житті.

Водночас більшість кіберзлочинів здійснюються без застосування насильства, це наслідок того, що одна з основних характеристик віртуального світу – здатність взаємодії без фізичного контакту. Удавана анонімність і “нереальність” віртуальної взаємодії – елементи, що роблять кіберпростір привабливим місцем для вчинення злочинів.

Ненасильницькі кіберзлочини можуть бути поділені на такі категорії: протиправне порушення володіння у кіберпросторі; киберкрадіжки; кібершахрайство; руйнування та інші кіберзлочини.

Під час порушення володіння у кіберпросторі, при злочинному доступі до ресурсів комп’ютера правопорушники не пошкоджують дані і не мають наміру їх використання. Звичайний приклад – це хакер-підліток, який “порушує кордони” тільки для того, щоб продемонструвати або вдосконалити свої навички, довести будь-що одноліткам або самому собі.

Існує багато різних типів кіберкрадіжок або засобів використання комп’ютерів і мереж для розкрадання інформації, грошей та інших цінностей. Оскільки прибуток є універсальним мотивом, а також з тієї причини, що здатність вкрасти “на відстані” зменшує для злодія ризик бути виявленим або спійманим, розкрадання – один з найпопулярніших видів кіберзлочинів. До цих злочинів включені такі соціально небезпечні вчинки:

1. Розтрата і привласнення. Ці злочини включають незаконне привласнення грошей або власності, доручених особі. Наприклад, службовець, який використовує свій законний доступ до платіжної відомості у комп’ютерній системі, змінює дані так, щоб в результаті йому заплатили додаткові кошти. Або за допомогою комп’ютера переміщує фонди з рахунків у банку на свій особистий рахунок.

2. Незаконне асигнування, яке відрізняється від розтрати тим, що цінності не були доручені злочинцеві, але він, маючи доступ до системи, змінює документи, в результаті чого набуває право на майно, яке не мало йому належати.

3. Корпоративне (промислове) шпигунство, коли працівники підприємства або інші особи використовують комп’ютери та мережі для розкрадання комерційної таємниці (наприклад, рецепт напою, виготовленого конкурентом). Предметом розкрадання можуть також виступати фінансові дані, конфіденційні списки клієнта, маркетингові стратегії або інша інформація, яка може використовуватися для підриву бізнесу або одержання конкурентоспроможної переваги.

4. Піратство, тобто неправомірне копіювання захищеного авторським правом програмного забезпечення, а також музики, кіно, книг, інших творів мистецтва, що завдає збитків законному власнику авторських прав.

5. Розкрадання персональних даних, коли Інтернет використовується для отримання особистих даних жертви, наприклад, номерів водійських прав, кредитних карт і банківських рахунків для наступних шахрайських дій, у тому числі отримання за допомогою особистих даних грошей чи іншого майна.

6. Неправомірна зміна даних DNS (сервера доменних імен). Це форма неправомірного перехоплення, за якої зловмисники управляють змістом DNS для переадресації даних, переданих мережею, на свій сервер.

Висновки.

Відповідно до зазначеного вище переліку об’єктом кіберзлочинності слід вважати комплекс суспільних відносин, які виникають у сфері використання мережевих технологій при здійсненні взаємодії громадян з інформаційним середовищем, що забезпечують стан захищеності інтересів людини та суспільства в цьому середовищі.

Предметом цього злочину слід вважати віртуальний інформаційний простір, доступ до якого здійснюється за допомогою комп’ютера, в якому міститься інформація про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному чи будь-якому іншому вигляді, яка знаходяться в процесі руху по локальних і глобальних комп’ютерних мережах, або відомості, що зберігаються у пам’яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки та передачі [1].

Матеріальна (фізична) ознака означає, що предметом кіберзлочину можуть бути інформація, її окремі елементи, які об'єктивно існують і можуть мати матеріалізоване вираження у вигляді інформаційних носіїв різних типів. Юридична ознака означає, що об’єкти інформаційного простору можуть стати предметом злочинних посягань, відповідно вони повинні перебувати під правовою охороною. Об’єктивна сторона злочинів, як правило, проявляється у формі розповсюдження матеріалів, які впливають на стан суспільної моралі, громадського миру і спокою, у нав’язуванні інформації, яка сприяє реалізації шахрайських схем, в отриманні доступу до персональних даних осіб, організацій та установ, які в разі їх оприлюднень можуть завдання шкоди репутації, а також дають змогу незаконно заволодівати фінансовими ресурсами даних осіб, використовувати отримані данні для шантажу, отримання конкурентних переваг і т. ін.

Таким чином, предмет і об’єкт кіберзлочинності не збігаються за предметом та об’єктом традиційної комп’ютерної злочинності, вони є більш широкими, що в свою чергу обумовлено самою специфікою даної кримінальної діяльності, яка включає в себе широкий спектр правопорушень, спрямована на порушення прав людини і громадянина, несе в собі підвищену соціальну небезпеку. Унікальність предмета та об’єкта кіберзлочинності полягає в тому, що окремі склади злочинів, що входять до її загальної структури, межують з іншими злочинами, які в принципі можна скоювати, не застосовуючи комп’ютерної техніки та інформаційних технологій (шахрайство, крадіжка, розповсюдження порнографії, шантаж), але в даному випадку саме комп’ютер як знаряддя та засіб вчинення злочину впливає на предмет та об’єкт кіберзлочинності, обумовлює її технологічну спрямованість.

Використана література

1. Батурин Ю.М., А.М. Жодзишский Компьютерные правонарушения: криминализация, квалификация, раскрытие // Советское государство и право. – 1990. – № 12. – С. 86-94.

2. Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершенные с использованием компьютерных технологий : дис. на соискание науч. степени канд. юрид. наук / С.Ю. Бытко. – Саратов, 2002. – 204 с.

3. Галамба М. Інформаційна безпека України : поняття, сутність та загрози. – Режим доступу : //www.justinian.com.ua/ article.php?id=2509

4. Корогодин В.И., В.Л. Корогодина. Информация как основа жизни. – Режим доступу : //www.plam.ru/biophiz/informacija_kak_osnova_ zhizni /p6.php

5. Максимов В.Ю. Компьютерные преступления (вирусный аспект) / В.Ю. Максимов. – Ставрополь : Книжное издательство, 1999. – 97 с.

6. Мирошниченко Н.А. Состав преступления : текст лекций / Н.А. Мирошниченко. – Одесса : “Юридична література”, 2003. – 85 с.

7. Мотлях О.І. Безпека комп’ютерних інформаційних даних : реалії сьогодення та перспективи // Юридичний вісник України. – 2008. – № 4. – С. 47-52.

8. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. – Режим доступу : //www.zakon1.rada.gov.ua/laws/show/514/2009

9. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102. – Режим доступу : //www.zakon1.rada.gov.ua/laws/show/537-16

10. Сивицкая Н.А. Уголовная ответственность за компьютерные преступления в странах СНГ и Балтии (сравнительный анализ законодательства) // Проблемы правовой информатизации. – Мн. : НЦПИ, 2004. – Вып. 1. – С. 86-88.

11. Стрельцов А.А. Обеспечение информационной безопасности России : теоретические и методологические основы ; под ред. В.А. Садовничего и В.П. Шерстюка. – М. : МЦНМО, 2002. – 86 с.

12. Тропина Т.Л. Киберпреступность : понятие, состояние, уголовно-правовые меры борьбы. – Режим доступу : //www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb =1&pb=1

13. Тюменев А.В. Виды криминального насилия (уголовно-правовой и криминологический аспекты) : автореф. дис. на соискание науч. степени канд. юридич. наук : 12.00.08 / А.В. Тюменев. – Рязань, 2002. – 24 с.

14. Шиндер Д.Л. Киберпреступность / Д.Л. Шиндер – (Владивостокский центр по изучению организованной преступности, 2002). – Режим доступу : //www.law.edu.ru/script/cntsource.asp?cnt ID=100087735

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~