КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.98.06

Самойленко О.А.
Національний університет «Одеська юридична академія»

ІНФОРМАЦІЙНИЙ ПРОДУКТ ЯК ПРЕДМЕТ ПОСЯГАННЯ ПІД ЧАС ВЧИНЕННЯ ЗЛОЧИНІВ ІЗ ВИКОРИСТАННЯМ ОБСТАНОВКИ КІБЕРПРОСТОРУ

У статті визначено зміст інформаційного продукту та його природу як предмета посягання під час вчинення злочинів із використанням обстановки кіберпростору. Деталізовано зміст інформації з обмеженим доступом та об'єктів авторського права або суміжних прав із позиції різновидів інформаційного продукту як предмету посягання. Автор приходить до висновку, що цінність інформаційного продукту, пов'язана з характером зафіксованих у ньому відомостей, зумовлює обрання злочинцем конкретного різновиду останнього для здійснення на нього впливу. Останній є скерованим загальним мотивом злочинної діяльності.

Ключові слова: *інформація, інформаційний продукт, злочин, кіберпростір, механізм злочину, предмет посягання.*

Постановка проблеми. Еволюційні процеси технологій кіберпростору призвели до того, що сьогодні інформація отримала значення цінного ресурсу суспільства, який дає можливість задовольнити конкретній людині широкий спектр потреб у фінансово-економічній, соціальній, державно-політичній або духовній сферах її життя. Утім, під час транспортування інформації в кіберпросторі остання все частіше піддається злочинному впливу, виступаючи для злочинця-користувача інформаційним продуктом, результатом задоволення його інформаційних потреб. Оскільки зі всіх елементів механізму злочинної діяльності саме предмет посягання першим потрапляє в поле зору слідчого, то окремого значення набуває питання природи інформаційного продукту як предмета посягання під час вчинення традиційних злочинів із використанням обстановки кіберпростору .

Аналіз останніх досліджень і публікацій. У криміналістиці до природи інформаційного продукту як предмета посягання підходили багато науковців (П.Д. Біленчук, А.С. Білоусов, В.Б. Вехов, В.О. Голубєв, О.І. Мотлях, Н.А. Розенфельд, В.С. Цимбалюк, В.П. Шеломенцев). Однак вони стояли на позиціях розроблення окремих методик розслідування комп'ютерних злочинів, що суттєво звужує зміст інформаційного продукту як предмета посягання під час вчинення злочинів із використанням обстановки кіберпростору.

Постановка завдання. Оскільки полімотивованість злочинної діяльності в кіберпросторі зумовлює існування певної системи предметів таких посягань, то ми ставимо перед собою мету визначити зміст інформаційного продукту та його природу як предмета посягання під час вчинення злочинів із використанням обстановки кіберпростору.

Виклад основного матеріалу дослідження. Дискусії про те, що розуміти під інформаційним продуктом, ведуться з позицій багатьох наук, зокрема інформатики, економіки, маркетингу, бібліотечної справи. При цьому кожна з галузей знань визначає інформаційний продукт, вихо-

дячи зі своєї предметної сфери. Так, в економіці інформаційний продукт розглядається як один із складових моментів інформаційного ринку, що з позиції виробника інформаційних послуг є сукупністю даних, яка сформована для поширення в речовинній або нематеріальній формі [1, с. 74]. В інформаційно-аналітичній діяльності, науковій інформатиці та бібліотечній справі інформаційний продукт ототожнюється з інформаційною продукцією, що являє собою документи, інформаційні масиви, бази даних і інформаційні послуги, які є результатом функціонування інформаційних систем [2, с. 130–140].

Згідно зі ст. 1 Закону України «Про національну програму інформатизації» інформаційний продукт (або продукція) являє собою документовану інформацію, яка підготовлена і призначена для задоволення потреб користувачів [3]. Відзначимо, що слово «продукт» у тлумачних словниках традиційно позначається як наслідок, витвір, результат будь-чого; речовий або інтелектуальний результат людської праці [4, с. 1159]. Слово «інформаційний» виступає прикметником, що використовується для вказівки на зв'язок основного слова з інформацією. Згідно з однією з позицій у тлумачному словнику «термін «інформаційний» стосується інформації як сукупності відомостей або сигналів, що містяться де-небудь або що передаються від одного об'єкта іншому» [4, с. 512]. У цьому сенсі інформаційний продукт – це інформація/відомості, що зафіксовані в електронній формі як результат задоволення потреб користувача/ів кіберпростору.

М.В. Карчевський справедливо робить акцент на цінності інформації [5, с. 60], яка буває різною: може бути цінною по суті, оскільки є результатом тривалої роботи великої кількості осіб, або цінною за призначенням, оскільки її наявність є необхідною умовою для вирішення певного завдання, наприклад, отримання доступу до банківських рахунків, персональні або особисті дані. Утім, у своїх роботах автор цінність інформації все ж таки дорівнює категорії «ціна». У результаті виділення фізичної, економічної та юридичні ознаки комп'ютерної інформації визнає останню предметом злочину та розуміє під нею відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну [6, с. 61]. Економічну ознаку інформації виражає через цілісність, доступність, конфіденційність та ціну останньої. Юридичну ознаку – через специфічність інституту права власності на інформацію. Тож інформаційний продукт як предмет посягання повинен бути чужим для злочинця та мати законного користувача/ів, що закономірно пов'язано з характером зафіксованих у ньому відомостей (наприклад, твір як об'єкт авторського права, персональні дані, банківська таємниця тощо).

Наведене дає можливість стверджувати, що цінність інформаційного продукту, пов'язана з характером зафіксованих у ньому відомостей, зумовлює обрання злочинцем останнього для здійснення на нього впливу, що скерований загальним мотивом злочинної діяльності з використанням обстановки кіберпростору. Доступ сторонніх осіб до таких продуктів обмежений на підставі закону. Зокрема, ними виступає «інформація з обмеженим доступом» та результат чужої інтелектуальної праці. Деталізуємо їх зміст із позиції різновидів інформаційного продукту як предмету посягання.

Інформація з обмеженим доступом. Відповідно до ч. 1 ст. 20 ЗУ «Про інформацію» інформація за порядком доступу до неї поділяється на відкриту інформацію та інформацію з обмеженим доступом. На законодавчому рівні визначені три групи такої інформації, зокрема: службова, таємна та конфіденційна (в тому числі інформація про особу). У Законі України «Про доступ до публічної інформації» конкретизовані загальні вимоги під час обмеження доступу до інформації та правовий статус кожного з видів інформації [7]. Утім, із практичних міркувань доцільно розглядати інформацію з обмеженим доступом у контексті змісту та суб'єкта, що нею володіє. Тому традиційно в теорії інформаційного права вона поділяється на: 1) державну таємницю (секретну інформацію); 2) конфіденційну інформацію, що охоплює інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [8]. Конфіденційна інформація поділяється на: інформацію про особу (персональні дані); інформацію, що є власністю держави (службова таємниця або інформація для службового користування); комерційну таємницю; професійну таємницю (серед якої розрізняю лікарську, адвокатську, нотаріальну, страхову, банківську та деякі інші види таємниці); банківську таємницю [9; 10]. Аналіз матеріалів судово-слідчої практики дозволяє визнати, що злочинець, що використовує обстановку кіберпростору для вчинення злочину, типово посягає на персональні дані (25% проваджень), банківську (25%), державну (40%) та комерційну (10%) таємницю.

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 1 Закону України «Про захист персональних даних») [11]. Не дивлячись на те, що ст. 11 Закону України «Про інформацію» чітко визначає їх перелік, зокрема дані про національність особи, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження, Конституційний Суд України вважає, що перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним [12]. У цьому є сенс, адже, як свідчать наукові розробки та аналіз судово-слідчої практики, до персональних даних відносять дані про інтимні сторони життя людини, неблаговидні вчинки, злочинну діяльність, дані, що скомпрометують або принизять честь і гідність особи чи близьких йому осіб [13; 14, с. 90]. Вивчення матеріалів кримінальних проваджень дозволяє стверджувати, що персональні дані типово стають первинним предметом посягання в механізмі вчинення злочинів, пов'язаних із анархістськими діями в кіберпросторі, що поєднані зі злочинами, вчиненими з корисливих та соціально-економічних мотивів.

Банківська таємниця – це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин із ним чи третіми особами під час надання послуг банку [15]. У ст. 60 Закону України «Про банки і банківську діяльність» чітко визначено перелік відомостей, що становлять банківську таємницю. Окремі відомості, що становлять банківську таємницю, викликають у злочинців особливу зацікавленість, зокрема: 1) відомості про банківські рахунки клієнтів, кореспондентські рахунки банків у НБУ; 2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3) системи охорони банку та клієнтів; 5) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7) коди, що використовуються банками для захисту інформації; 8) інформація про фізичну особу; 9) документи для службового користування з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю. Така інформація вдало використовується в механізмах вчинення злочинів із корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі.

Державну таємницю складають відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою [16]. Як пише М.О. Шилін, динаміка сучасної оперативної обстановки по лінії контррозвідувального забезпечення державної безпеки України свідчить про подальшу активізацію діяльності спецслужб іноземних держав, зокрема, з проведення ними легальної розвідки, а також залучення громадян України до збору інформації, що становить державну таємницю в політичній, економічній, військовій, науково-технічній і оборонній сферах [17, с. 22]. Сьогодні державна таємниця типово виступає предметом посягання під час вчинення злочинів в обстановці кіберпростору з антидержавно-політичних мотивів, зокрема всіх класифікаційних підгруп злочинів, що пов'язані з антидержавницькими діями.

Результат чужої інтелектуальної праці. Цей різновид інформаційного продукту в кримінально-правовій сфері має форму об'єктів авторського права або суміжних прав. Останні виступають предметом посягання в механізмі вчинення інтелектуального піратства як різновиду злочинів, вчинених із соціально-економічних мотивів.

Кримінальна відповідальність за такий злочин передбачена в статті 176 КК України «Порушення авторського права і суміжних прав». У ній міститься перелік предметів такого злочину, зокрема: твори науки, літератури, мистецтва, комп'ютерні програми і баз даних, фонограми, програми мовлення та інші об'єкти суміжних прав (виконання літературних, драматичних, музичних, музично-драматичних, хореографічних, фольклорних та інших творів; фонограми, відеограми; передачі (програми) організацій мовлення [18]). У результаті аналізу судово-слідчої практики розслідування вказаної категорії злочинів можна визначити, що серед об'єктів авторського права та суміжних прав предметами незаконного відтворення, розповсюдження та тиражування (щодо об'єктів суміжних прав) у кіберпросторі найчастіше виступають комп'ютерні програми (20% проваджень), аудіовізуальні твори (60% – традиційно фільми, що вийшли в прокатний показ), бази даних (компіляції даних) (10%), фонограми та передачі організацій мовлення (10%).

У контексті предмета посягання в кіберпросторі потрібно окремо зупинитись на такому достатньо новому правовому режимі об'єктів авторського права, як «веб-сайт». Так, 23 березня 2017 року було прийнято Закон України «Про державну підтримку кінематографії в Україні», яким вносились доповнення в Закон України «Про авторське право та суміжні права» щодо порядку захисту права інтелектуальної власності в мережі Інтернет [19]. Якщо раніше в наукових колах тривали дискусії з приводу того, чим є веб-сайт [20]: базою даних (компіляцією даних) [21, с. 45], складеним твором типу мультимедійного твору, засобом масової інформації, або взагалі він не є об'єктом права інтелектуальної власності – то сьогодні законодавець визначився з його природою. Через закріплення прав та обов'язків власників веб-сайту та веб-сторінки сам веб-сайт визнається технічною умовою існування об'єктів авторського права і суміжних прав у кіберпросторі. Мінімальний набір елементів веб-сайту передбачає наявність п'яти їх видів, таких як: 1) дизайн; 2) структурне рішення; 3) програмне забезпечення; 4) контент (змістовне наповнення: будь-які твори (часто аудіовізуальні твори, бази даних, фонограми, програми)); 5) доменне ім'я як ідентифікатор Інтернет-ресурсу, зареєстрований адміністратором мережі [20, с. 74]. Якщо перші чотири закономірно відносити до об'єктів інтелектуальної власності, то щодо останнього тривають наукові дебати. Виваженим вважаємо підхід, в якому доменні імена визначають засобом ідентифікації певного інформаційного ресурсу в мережі Інтернет, який за певних умов є похідним засобом індивідуалізації фізичних та юридичних осіб в мереж Інтернет [22, с. 200]. Отже, доменне ім'я буде предметом посягання в значенні персональної інформації про особу або нематеріального активу юридичної особи, що дорівнюється комерційній тайні.

Висновки. Отже, інформаційний продукт у значенні інформації/відомостей, що зафіксовані в електронній формі як результат задоволення потреб користувача/ів кіберпростору, виступає первинним предметом посягання під час вчинення злочину з використанням обстановки кіберпростору. Цінність інформаційного продукту, пов'язана з характером зафіксованих у ньому відомостей, зумовлює обрання злочинцем конкретного різновиду останнього для здійснення на нього впливу, що скерований загальним мотивом злочинної діяльності. До вищенаведеної категорії предметів посягання можна віднести «інформацію з обмеженим доступом» та результат чужої інтелектуальної праці.

Список літератури:

1. Великородна Д.В. Зміст і структура ринку інформаційних продуктів і послуг. Вісник економіки транспорту і промисловості. 2010. № 29. С. 72–76.
2. Захарова І.В., Філіпова Л.Я. Основи інформаційно-аналітичної діяльності: навч. посіб. К.: Центр учбової літератури, 2013. 335 с.
3. Про національну програму інформатизації: Закон України від 4 лютого 1998 року за № 74/98-ВР. URL: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.
4. Великий тлумачний словник сучасної української мови / За ред. В.Т. Бусел. Київ, Ірпінь: Перун, 2005. 1728 с.
5. Карчевський М.В. Злочини у сфері використання комп'ютерної техніки: навчальний посібник. К.: Атака, 2010. 168 с.
6. Карчевський М.В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж: аналіз складу злочину: дис... канд. юрид. наук: 12.00.08. Луганськ, 2003. 175 с.
7. Про доступ до публічної інформації: Закон України від 13 січня 2011 року за № 2939-VI ВР. URL: http://zakon0.rada.gov.ua/laws/show/2939-17.
8. Про інформацію: Закон України 2 жовтня 1992 року за № 2657-XII-ВР. URL: http://zakon0.rada.gov.ua/laws/show/2657-12.
9. Кормич Б.А. Інформаційне право: підручник. Харків, 2011. 334 с.
10. Марущак А.І. Інформаційне право: доступ до інформації: навч. посіб. Київ, 2007. 531 с.
11. Про захист персональних даних: Закон України від 1 червня 2010 року за № 2297-VI-ВР. URL: http://zakon2.rada.gov.ua/laws/show/2297-17.
12. Справа № 1-9/2012 // Рішення Конституційного суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 смічня 2012 року за № 2-рп/2012. URL: http://zakon2.rada.gov.ua/laws/show/v002p710-12.
13. Чуприна О. Співвідношення понять «персональні дані», «інформація про особу», «конфіденційна інформація про особу». Підприємство, господарство і право. 2013. № 1. С. 104–108.

14. Марущак А.І. Правові основи захисту інформації з обмеженим доступом. К., 2007. 208 с.
15. Про банки і банківську діяльність: Закон України від 7 грудня 2000 року за № 2121-III-ВР. URL: http://zakon0.rada.gov.ua/laws/show/2121-14/page.
16. Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII-ВР. URL: http://zakon5.rada.gov.ua/laws/show/3855-12/page.
17. Шилін М. Національна безпека: проблеми правового забезпечення діяльності суб'єктів сектору безпеки та можливі шляхи вирішення. Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку: збірник наукових праць за матеріалами Міжнародної науково-практичної конференції (1 грудня 2017 р., м. Острог) / за заг. ред. д.ю.н. Романова М.С. Острог, 2017. 180 с. С. 21–24.
18. Про авторські та суміжні права: Закон України від 23 грудня 1993 року за № 3792-XII-ВР. URL: http://zakon3.rada.gov.ua/laws/show/3792-12/page.
19. Про державну підтримку кінематографії в Україні: Закон України від 23 березня 2017 року № 1977-VIII-ВР. URL: http://zakon0.rada.gov.ua/laws/show/1977-19/page.
20. Майданик Н. Web-сайт в мережі Інтернет як особливий об'єкт авторського права. Юридична Україна. 2008. № 12. С. 73–80.
21. Пастухов О.М. Авторське право в Інтернеті. К.: Школа, 2004. 144 с.
22. Кулініч О.О. Доменне ім'я як похідний засіб індивідуалізації інформаційних ресурсів фізичних та юридичних осіб у мережі Інтернет. Актуальні проблеми держави та права. 2009. № 51. С. 195–200.

ИНФОРМАЦИОННЫЙ ПРОДУКТ КАК ПРЕДМЕТ ПОСЯГАТЕЛЬСТВА ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ОБСТАНОВКИ КИБЕРПРОСТРАНСТВА

В статье определены содержание информационного продукта и его природа как предмета посягательства при совершении преступлений с использованием обстановки киберпространства. Детализировано содержание информации с ограниченным доступом и объектов авторского права или смежных прав с позиции разновидностей информационного продукта как предмета посягательства. Автор приходит к выводу, что ценность информационного продукта, связанная с характером зафиксированных в нем сведений, обусловливает избрание преступником конкретной разновидности последнего для осуществления на него влияния, скорректированного общим мотивом преступной деятельности.

Ключевые слова: *информация, информационный продукт, преступление, киберпространство, механизм преступления, предмет посягательства.*

INFORMATIVE PRODUCT AS THE SUBJECT OF CRIMES WITH THE USING OF THE CYBERSPACE ENVIRONMENT

The article defines the content of the information product and its nature as the subject of the crimes using of the cyberspace the environment. The content of information with limited access and objects of copyright or related rights is detailed from the standpoint of varieties of the information product as subject of the crimes. The author comes to the conclusion that the value of an information product, connected with the nature of the information recorded in it, determines the choice of a particular type of criminal by the perpetrator for effecting on him the influence, corrected by the general motive of criminal activity.

Key words: *information, informative product, crime, cyberspace environment, mechanism of crime, subject of the crimes.*