ПРЕДМЕТ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНОГО СТ. 361-1 КК УКРАЇНИ

ЧОВГАН Ігор Михайлович - аспірант кафедри адміністративного права, інтелектуальної власності та цивільно-правових дисциплін Київського університету інтелектуальної власності та права Національного університету «Одеська юридична академія»

ORCID: https://orcid.org/0009-0006-4797-9318

УДК 343.98

DOI: https://doi.org/10.71404/EP.2025.1.21

Стаття присвячена вивченню питання визначення сутності предмета кримінального правопорушення, передбаченого ст. 361-1 КК України.

У статті детально проаналізовано ст. 361-1 Особливої частини КК України в частині предмета кримінального правопорушення. Розглянуто основні елементи, які є визначенням поняття «предмет кримінального правопорушення».

У статті вказується, що в доктрині кримінально-правової науки, предметом більшості комп'ютерних злочинів виступають комп'ютерна інформація та комп'ютерна система.

Встановлено, що предметом злочину, що передбачений ст. 361-1 КК України, є шкідливі програмні або технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Цієї думки дотримується абсолютна більшість представників кримінально-правової науки.

Акцентовано, що предмет кримінального правопорушення, передбачений ст. 361-1 КК України, необхідно розглядати в широкому та вузькому значеннях. У вузькому значенні предметом кримінального правопорушення будуть виступати шкідливі програмні або технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. У широкому значенні предмет кримінального правопорушення буде включати комп'ютерну інформацію, комп'ютери, інформаційні системи і технології, телекомунікаційні мережі, різні носії комп'ютерної інформації, шкідливі програмні і технічні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, телекомунікаційних мереж, інформаційних систем і технологій.

Ключові слова: кримінальне правопорушення, предмет кримінального правопорушення, шкідливі програмні засоби, шкідливі технічні засоби, комп'ютерна інформація, комп'ютерна система.

Постановка проблеми

Різним аспектам кримінально-правової характеристики, кримінальної відповідальності за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що передбачені статтями 361–363-1 КК України, було присвячено чимало наукових праць.

Актуальність дослідження цих питань обумовлена тим, що особливості формулювання кримінально-правових норм щодо цих злочинів певною мірою ускладнюють, а в деяких випадках практично унеможливлюють їх застосування, зумовлюють неоднозначне їх розуміння працівниками правоохоронних і судових органів, виникнення помилок при кваліфікації злочинів тощо.

Аналіз останніх досліджень та публікацій

Дослідження предмета кримінального правопорушення, передбаченого ст. 361-1 КК України неодноразово знаходило своє відображення у доктрині кримінального права. Зокрема, окремі проблеми, які стосуються предмета кримінального правопорушення, передбаченого ст. 361-1 КК України, розглядали Д.С. Азаров, Ю.В. Баулін В.І. Борисов, О.О. Волков, В.О. Голубєв, Н.С. Козак, О.О. Кирбят'єв, В.М. Куліуш, Л.М. Кривоченко, В.А. Ломако, М.І. Панов, Д.О. Ричка, Н.А. Розенфельд, М.В. Салтевський, В.В. Сташис, В.Я. Тацій, М.І. Хавронюк та ін. Разом із тим, певні концептуальні підходи до розуміння предмета кримінального правопорушення, передбаченого ст. 361-1 КК України, потребують окремих подальших досліджень.

Мета і завдання дослідження

Метою статті є визначення предмета кримінального правопорушення, передбаченого ст. 361-1 КК України. Для досягнення поставленої цілі необхідно вирішити низку наступних наукових завдань: узагальнити наукові підходи щодо визначення поняття предмета кримінального правопорушення, передбаченого ст. 361-1 КК України; проаналізувати судову практику з цієї проблематики.

Наукова новизна дослідження

Наукова новизна статті визначається тим, що в ній отримав подальше опрацювання теоретичний підхід щодо розкриття сутності предмета кримінального правопорушення, передбаченого ст. 361-1 КК України та характеристика його елементів.

Виклад основного матеріалу

Слід зазначити, що зовсім недавно класична теорія кримінального права використовувала матеріалістичний підхід до визначення предмета кримінального правопорушення. М.І. Панов, вказуючи, що предмети злочину – речі матеріального світу, впливаючи на які, особа зазіхає на цінності (благо), що належать суб'єктам суспільних відносин, а також наполягаючи на тому, що засоби скоєння злочину – це предмети матеріального світу, які застосовуються злочинцем під час вчинення суспільно небезпечного діяння [1, с.292-297]. Проте з урахуванням сучасних тенденцій розвитку суспільних відносин та інформаційного суспільства, цілком доцільно до предмета цих злочинів додати й комп'ютерну інформацію та інші об'єктивні матеріальні утворення, наприклад, комп'ютерні віруси, програмні та технічні засоби та ін. [2, с.266; 3, с.76]. Відповідно, модернізація характеру суспільних відносин, яка пов'язана з використанням високих технологій та інформаційного розвитку суспільства, перенесла деякі суспільні відносини у віртуальну площину, що дозволило науковцям виділити новий різновид предмета кримінального правопорушення – віртуальний предмет – (інформацію) [4, с.81]. Під віртуальним предметом кримінального правопорушення слід розуміти такий предмет об'єктивного світу, який створений за допомогою спеціальних методів та (або) способів, не має зовнішнього уявлення, проте може його придбати за допомогою спеціальних методів та способів впливу [5, с.11-12].

Аналізуючи інформацію як предмет злочину, О.Е. Радутний зазначає, що сьогоденні реалії вимагають визнавати в подальшому під предметом злочину речі або інші явища об'єктивного світу (інформація, енергія тощо), з певними властивостями яких кримінальний закон пов'язує наявність у діянні особи складу конкретного злочину [6, с.10].

Законодавець під інформацією розуміє будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [7].

Поняття інформації тісно пов'язане з поняттями повідомлення, сигналу, складності, структури і різноманітності. Розрізняють чимало видів інформації. За змістом інформація поділяється на такі види: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; кри-

тична технологічна інформація [7]. За режимом доступу: відкрита (загальнодоступна); обмеженого доступу (конфіденційна, таємна, службова інформація [8].

У зв'язку з чим, у доктрині кримінально-правової науки, предметом більшості комп'ютерних злочинів виступають: 1) комп'ютерна інформація [9, с.579-581; 10, с.57]; 2) комп'ютерна система [11, с.35; 12, с.90].

У свою чергу, як зазначає Д.О. Ричка, під комп'ютерною системою слід розуміти будь-яку з наступних систем [13, с.81-83]:

1) електронно-обчислювальна машина (ЕОМ) – комп'ютер – комплекс електронних технічних засобів, які побудовані на основі мікропроцесорів і призначені для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань. Як правило, ЕОМ складається із трьох частин: системного блока, який включає в себе мікропроцесор та інші пристрої, необхідні для її роботи, клавіатури, за допомогою якої вводяться в ЕОМ символи, та монітора, на якому відображається текстова і графічна інформація [14, с.458; 15, с.556]. Враховуючи сучасні здобутки науки і техніки, до ЕОМ доцільно додати такі пристрої, як: ноутбук, нетбук, планшет, телефон та ін.;

2) автоматизовані системи (АС) – системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення [3, с.76-82]. У склад АС входить принаймні одна ЕОМ та периферійні пристрої, що працюють на основі такої ЕОМ: принтер, сканер, модем, мережевий адаптер та ін. АС включають у себе комп'ютерні мережі і мережі електрозв'язку. Можна погодитися із думкою Д.О. Рички з приводу того, що до складу автоматизованих систем можна включити банкомати та термінали [13, с.81-82]. Адже відповідно до Закону України «Про платіжні системи та переказ коштів в Україні», банківський автомат самообслуговування (банківський автомат) – програмно-технічний комплекс, який надає можливість держателю електронного платіжного засобу здійснити самообслуговування за операціями одержання коштів у готівковій формі, внесення їх для зарахування на відповідні рахунки, одержання інформації щодо стану рахунків, а також виконати інші операції згідно з функціональними можливостями цього комплексу [16]. Вчиняється багато злочинів, пов'язаних з роботою саме банкоматів та терміналів, тому вважаємо за потрібне включити їх до предметів злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж та мереж електрозв'язку.

3) комп'ютерні мережі (мережа ЕОМ) – це об'єднання кількох комп'ютерів (ЕОМ) і комп'ютерних систем, взаємопов'язаних і розподілених за фіксованою територією орієнтованих на колективне використання загальномережевих ресурсів. Вони передбачають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, що входять до комп'ютерних систем; можуть включати дві чи більше автоматизовані комп'ютерні системи (АКС), як сукупність взаємопов'язаного ЕОМ, периферійного устаткування та програмного забезпечення, призначених для автоматизації прийому, збереження, обробки, пошуку та видачі інформації споживачам. Комп'ютерні мережі можуть бути регіонального і галузевого характеру [3, с.76-82; 14, с.458-459];

4) мережі електрозв'язку – це сукупність технічних засобів та споруд зв'язку, об'єднаних у єдиний технологічний процес забезпечення інформаційного обміну – маршрутизації, комунікації, передачі, випромінювання або прийому знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах (телефонний, телеграфний, телетайпний та факсимільний зв'язок). Предмети мережі електрозв'язку включають: телефони, факси, телетайпи, телеграфи, інші апарати, пристрої і обладнання мереж електрозв'язку, призначені для передачі й обміну інформацією [13, с.82];

5) комп'ютерна інформація може бути в різних формах фіксації: текстовою, цифровою, графічною чи іншого виду (дані, відомості) про осіб, предмети, події, явища, що існують в електронному вигляді і знаходять-

ся в ЕОМ, АС чи в комп'ютерній мережі, а також зберігається на відповідних електронних носіях, до яких належать гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти та ін., така інформація носіїв може використовуватися, оброблятися чи змінюватися за допомогою ЕОМ (комп'ютерів) [13, с.82-83];

6) враховуючи, що одним із різновидів мереж електрозв'язку виступають комп'ютерні мережі, то інформація, що передається мережами електрозв'язку (телекомунікаційними мережами) – будь-які відомості, подані у вигляді сигналів, знаків, звуків, зображень чи в інший спосіб (телефонні повідомлення, радіо- та телепередачі тощо), у тому числі і за допомогою комп'ютера, якщо вона передається через мережі електрозв'язку [14, с.459]. Така інформація, що передається мережами електрозв'язку, може бути предметом цих злочинів лише тоді, коли цими мережами передається комп'ютерна інформація від однієї комп'ютерної системи до іншої [2, с.103, 104; 17, с.58]. Саме злочинний вплив на ці предмети або їх злочинне використання дає підстави визначити наявність об'єкта цих злочинів, тому що вони є невід'ємною частиною охоронюваних розглядуваними нормами суспільних відносин [11, с.35].

У такому випадку варто в кримінальному законодавстві уніфікувати понятійно-категоріальний апарат шляхом внесення змін та доповнень до чинного законодавства України. Можна погодитися із думкою Н.С. Козак з приводу того, що з урахуванням диспозицій норм КК України, розвитку комп'ютерних наук, до предметів злочинного посягання комп'ютерних злочинів слід віднести комп'ютерну інформацію, комп'ютери, інформаційні системи і технології, телекомунікаційні мережі, різні носії комп'ютерної інформації, шкідливі програмні і технічні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, телекомунікаційних мереж, інформаційних систем і технологій [18, с.57]. Якщо розглядати предмет комп'ютерних злочинів взагалі, то одним з них виступає саме інформація, під якою розуміються відомості про осіб, предмети, факти, події, явища і процеси, зафіксовані на машинному носії, в ЕОМ, системі ЕОМ або їх мережах. Конкретизуючи предмет злочину, відповідальність за який передбачена ст.361-1 КК України, слід зазначити, що в цьому випадку предмет буде дещо відрізнятися, виходячи із філософського розуміння сутності явищ від загального до конкретного. Мається на увазі, що предмет кримінального правопорушення, передбаченого ст. 361-1 КК України охоплюється поняттям «комп'ютерна інформація» та є більш конкретизованим.

Досить цікавою є позиція Б.М. Головкіна, О.І. Деньковича, В.В. Луцика, Д.М. Цехан з приводу того, що первинними предметами посягання у кіберпросторі є інформаційний продукт та інформаційний ресурс. Вторинними предметами посягання виступають майно (грошові готівкові або безготівкові кошти, товари), комп'ютери, комп'ютерні мережі, мережі електрозв'язку та документи. Акцентуємо свою увагу на першій групі [19, с.94]. Однак, на наш погляд, поняття «інформаційний продукт» та «інформаційний ресурс» охоплюються за змістом та обсягом поняттям «інформація», що є логічним.

Для характеристики вищезазначених предметів необхідно усвідомлювати, що засоби комп'ютерної техніки за своїм функціональним призначенням можливо розділити на дві основні групи: 1) технічні або апаратні засоби (HardWare); 2) програмні засоби (SoftWare) [20, с.63]. Можна прослідкувати, що в диспозиції ст. 361-1, на відміну від ст. 361, поняття комп'ютерних вірусів розширено до шкідливих програмних засобів. І це правильно тому, що багато програм не є вірусами, але попре це вони здатні порушувати роботу ЕОМ. У зв'язку з вище викладеним, ми вважаємо, що предметом злочину слід визнати шкідливі програмні та технічні засоби.

Отже, предметом кримінального правопорушення, що передбачений ст. 361-1 КК України, є шкідливі програмні або технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Цієї думки дотримується абсолютна більшість представників кримі-

нально-правової науки [13, с.84; 14, с.464; 21, с.6-7; 22, с.43]. Крім того, дослідження компанії «Майкрософт Україна» показали, що понад 56% продуктів, які розповсюджуються на дисках із нібито ліцензійними програмами, а також викладені для безкоштовного скачування на торентах і сайтах-файлообмінниках, мають вбудовані віруси або програми, за допомогою яких можна дистанційно отримувати доступ до комп'ютера користувача та його персональної інформації [23].

Такої самої практики дотримуються й суди при розгляді кримінальних проваджень. Так, Білогірський районний суд Хмельницької області виправдав підсудних О. і С., яких звинувачували в учинені злочину, передбаченого ст. 361-1 КК України, за відсутності предмета злочину, і, відповідно, за відсутності в їхніх діях складу злочину. Згідно з висновком експерта від 27 серпня 2014 року № 56 кт програма «Keylogger Net» (у використанні якої їх звинувачено), що міститься на USB флеш-накопичувачі «Silicon Power» й надана для дослідження, буде мати ознаки шкідливого програмного забезпечення за умови, якщо її встановлення відбувається без відома власника (адміністратора безпеки) автоматизованої системи або без відома власника конкретного персонального комп'ютера. Цих умов дійсно не було дотримано, і це означає, що предмета злочину не було [22, с.43].

Висновки

Таким чином, на нашу думку, предмет кримінального правопорушення передбачений ст. 361-1 КК України, необхідно розглядати в широкому та вузькому значеннях. У вузькому значенні предметом злочину будуть виступати шкідливі програмні або технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. У широкому значенні предмет кримінального правопорушення буде включати комп'ютерну інформацію, комп'ютери, інформаційні системи і технології, телекомунікаційні мережі, різні носії комп'ютерної інформації, шкідливі програмні і технічні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, телекомунікаційних мереж, інформаційних систем і технологій.

Література

1. Панов М.І. Вибрані наукові праці з правознавства. К.: Ін Юре, 2010. 812 с.

2. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. 304 с.

3. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.

4. Мазуренко О., Розенфельд Н. Комп'ютерна інформація як предмет злочинів, передбачених Розділом XVI КК України. *Право України.* 2004. № 6., С. 81-83.

5. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дис. … канд. юрид. наук: 12.00.08. К., 2003. 200 с.

6. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю: автореф. дис. … канд. юрид. наук: 12.00.08. Х., 2002. 21 с.

7. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

8. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: http://zakon5.rada.gov.ua/laws/show/2939-17.

9. Замахін А.Л. Об'єкт та предмет кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Аналітично-порівняльне правознавство.* 2023. № 6. С.576-581.

10. Музика А.А., Азаров Д.С. Законодавство України про відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. К.: Вид. Паливода А.В., 2005. 120 с.

11. Васильєв А.А., Пашнєв Д.В. Особливості кваліфікації злочинів у сфері ви-

SUMMARY

The article deals with the issue of determining the essence of the subject matter of a criminal offense under Article 361-1 of the Criminal Code of Ukraine.

The article analyzes in detail Art. 361-1 of the Special Part of the Criminal Code of Ukraine in terms of the subject matter of a criminal offense. The author examines the main elements which constitute the definition of the concept of "object of a criminal offense".

The article indicates that according to the doctrine of criminal law science, the subject matter of most computer crimes is computer information and computer system.

The author establishes that the subject matter of the crime under Art. 361-1 of the Criminal Code of Ukraine is malicious software or hardware intended for unauthorized interference with the operation of electronic computers, automated systems, computer networks or telecommunication networks. This opinion is shared by the vast majority of representatives of criminal law.

It is emphasized that the subject matter of a criminal offense under Article 361-1 of the Criminal Code of Ukraine should be considered in a broad and narrow sense. In the narrow sense, the subject matter of a criminal offense will be malicious software or hardware intended for unauthorized interference with the operation of electronic computers, automated systems, computer networks or telecommunication networks. In a broad sense, the subject matter of a criminal offense will include computer information, computers, information systems and technologies, telecommunication networks, various computer information carriers, malicious software and hardware designed for unauthorized interference with the operation of computers, telecommunication networks, information systems and technologies.

Keywords: criminal offense, object of criminal offense, malicious software, malicious hardware, computer information, computer system.

користання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України*. 2013. Вип. 5. С. 34-42.

12. Куліуш В.М. Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору: дис. … д-ра філософії: 081 – Право. К., 2024. 240 с.

13. Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: дис. … канд. юрид. наук: 12.00.08. Ірпінь, 2019. 212 с.

14. Кримінальне право України: загальна частина: підручник / Ю.В. Баулін, В.І. Борисов, Л.М. Кривоченко та ін.; за ред. В.В. Сташиса, В.Я. Тація. 4-те вид., переробл. і допов. Х.: Право, 2010. 608 с.

15. Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. К.: Кондор, 2005. 588 с.

16. Про платіжні системи та переказ коштів в Україні: Закон України від 05.04.2001 № 2346-III. URL: http://zakon3.rada.gov.ua/laws/show/2346-14.

17. Карчевський М.В. Злочини у сфері використання комп'ютерної техніки: навчальний посібник. К.: Атіка, 2010. 168 с.

18. Козак Н.С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів: автореф. дис. … канд. юрид. наук: 12.00.09. Ірпінь, 2011. 229 с.

19. Кіберзлочинність та електронні докази = Cybercrime and digital evidence: навчальний посібник / Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан; за ред. О. Денькович, Г. Шмельцер. Львів: ЛНУ ім. Івана Франка, 2022. 298 с.

20. Кирбят'єв О.О. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів: дис. … канд. юрид. наук: 12.00.08. Запоріжжя, 2015. 200 с.

21. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: методичні рекомендації / О.Ф. Вакуленко, О.М. Стрільців, О.С. Тарасенко та ін. К., 2016. 55 с.

22. Волков О.О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів: дис. … канд. юрид. наук: 12.00.09. Дніпро, 2023. 198 с.

23. Шимків Д. Кіберзлочинність – це довершена структура з мільйонним обігом. URL: https://ukurier.gov.ua/uk/articles/dmitro-shimkiv-kiberzlochinnist-ce-dovershena-stru/.