УДК 343.9
DOI https://doi.org/10.32782/39221335

Кузьменко О. В.,
кандидат юридичних наук, доцент,
доцент кафедри кримінальної юстиції
Державного податкового університету

ОСОБЛИВОСТІ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

FEATURES OF CRIMINALISTIC CHARACTERISTICS OF CYBER CRIMES

Статтю присвячено особливостям криміналістичної характеристики кіберзлочинів, а саме окремих її елементів. Зазначено, що разом з поширенням впровадження сучасних інформаційних технологій в Україні постійно зростає загроза як для державних комп'ютерних систем, так і для приватних організацій та окремих громадян.

Проаналізовано, що сучасний рівень інформатизації суспільства вимагає від України забезпечити належний та ефективний механізм боротьби із кіберзлочинами як однієї із серйозних загроз національній безпеці держави. Така потреба стає ще більш очевидною, враховуючи військову агресію Російської Федерації проти нашої держави.

Зазначено, що Конвенція про кіберзлочинність виділяє таки види правопорушень: 1) проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані чи систему та зловживання пристроями); 2) пов'язані з комп'ютерами (підробка та шахрайство); 3) пов'язані зі змістом (наприклад, з дитячою порнографією); 4) пов'язані з порушенням авторських та суміжних прав.

Крім того, встановлено, що до основних елементів криміналістичної характеристики кіберзлочинів слід віднести: спосіб вчинення кримінального правопорушення, особу злочинця, особу потерпілого та сліди кримінального правопорушення.

З'ясування під час досудового розслідування важливих криміналістичних даних про особу кіберзлочинця є одним з основних факторів у розслідуванні кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). Крім того, кіберзлочинця мають характеризувати у сукупності як загальні (вік, стать, соціальний та психологічний стан тощо), так і спеціальні (професійні звички, особливий «почерк» тощо) ознаки.

Автором зазначено, що до слідів як елементів криміналістичної характеристики кіберзлочинів можна віднести: 1) матеріально фіксовані сліди (документи, відбитки, технічні пристрої тощо); 2) відомості та дані, зафіксовані в цифровій формі на матеріальних носіях; 3) електронна інформація, створена комп'ютером чи людиною; 4) програмне забезпечення; 5) комп'ютерні системи.

Ключові слова: *кіберзлочин, кіберзлочинність, криміналістична характеристика, кіберзлочинець, типові сліди кіберзлочину, способи вчинення кіберзлочину, Конвенція про кіберзлочинність.*

The article is devoted to the peculiarities of the forensic characteristics of cybercrimes, namely, its individual elements. It is noted that along with the spread of the introduction of modern information technologies in Ukraine, the threat to both state computer systems and private organizations and individual citizens is constantly growing.

It has been analyzed that the current level of informatization of society requires Ukraine to provide a proper and effective mechanism for combating cybercrime as one of the serious threats to the national security of the state. This need becomes even more obvious, taking into account the military aggression of the Russian Federation against our state.

It is noted that the Convention on Cybercrime distinguishes the following types of offenses: 1) against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, interference with data or system and misuse of devices); 2) related to computers (forgery and fraud); 3) related to the content (for example, child pornography); 4) related to the violation of copyright and related rights.

In addition, it was established that the main elements of the forensic characteristics of cybercrimes should include: the method of committing a criminal offense, the identity of the criminal, the identity of the victim, and traces of the criminal offense.

Clarification during the pre-trial investigation of important forensic data about the identity of the cybercriminal is one of the main factors in the investigation of criminal offenses committed with the use of information technologies (cybercrimes). In addition, the cybercriminal should be characterized in aggregate by both general (age, gender, social and psychological state, etc.) and special (professional habits, special "handwriting", etc.) characteristics.

The author states that traces as elements of the forensic characteristics of cybercrimes include: 1) materially fixed traces (documents, prints, technical devices, etc.); 2) information and data recorded in digital form on physical media; 3) electronic information created by a computer or a person; 4) software; 5) computer systems.

Key words: *cyber crime, cybercrime, forensic characteristics, cybercriminal, typical traces of cybercrime, methods of committing cybercrime, Cybercrime Convention.*

Постановка проблеми. На сьогодні кримінальні правопорушення, передбачені Розділом XVI Особливої частики Кримінального кодексу (далі – КК) України [1], є, на жаль, надзвичайно розповсюдженими. А після початку повномасштабного вторгнення Російської Федерації на територію України 24.02.2022 року більш гостро стало питання захисту наших ІТ-системи, комп'ютерних мереж і мереж електрозв'язку. Війна внесла свої корективи, і з метою підлаштування кримінального законодавства до реалій сьогодення, 24.03.2022 року був прийнятий Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» [2]. Все це надзвичайно актуалізує необхідність дослідження криміналістичної характеристики кібезлочинів.

Аналіз останніх досліджень і публікацій. Питання, пов'язані з характеристикою, розслідуванням та протидією кіберзлочинності, у своїх працях досліджувало багато вітчизняних та зарубіжних вчених, серед яких Н. М. Ахтирська, Л. Ю. Долженко, А. І. Марущак, Я. В. Неділько, О. С. Омельян, В. О. Точілов, В. Г. Хахановський та інші. Однак, вдосконалення та поява нових методів вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку потребує постійного дослідження.

Виклад основного матеріалу. Відповідно до п. 8 ч. 1. ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» 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 [3].

На думку деяких науковців, «термін «кіберзлочин» утворений сполученням двох слів: кіберпростір і злочин. Термін «кіберпростір» (у вітчизняній літературі частіше зустрічаються терміни «віртуальний простір» або «віртуальний світ») позначає інформаційний простір, що моделюється за допомогою комп'ютера, в якому існують визначені об'єкти або символьне уявлення інформації – місце, де діють комп'ютерні програми і переміщуються дані. Використання цього терміну поширене у світовій науковій літературі та вживається не як юридична категорія, а як визначення соціального та технічного феномену» [4, с. 277].

Конвенція про кіберзлочинність виділяє таки види правопорушень: 1) проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані чи систему та зловживання пристроями); 2) пов'язані з комп'ютерами (підробка та шахрайство); 3) пов'язані зі змістом (наприклад, з дитячою порнографією); 4) пов'язані з порушенням авторських та суміжних прав [5].

Як зазначає П. В. Берназ «одним із найважливіших елементів криміналістичної методики є криміналістична характеристика злочину. Вона є взаємопов'язаною сукупністю індивідуальних особливостей певної категорії злочинів, що характеризують обстановку, спосіб і механізм вчинення та приховування злочину, осіб злочинця і потерпілого та має значення для виявлення, розкриття та розслідування злочину. Криміналістична характеристика злочину в слідчій діяльності використовується як інструмент для висунення слідчих версій та формування обставин, які підлягають встановленню» [6, с. 35].

На нашу думку, до основних елементів криміналістичної характеристики кіберзлочинів слід віднести: спосіб вчинення кримінального правопорушення, особу злочинця, особу потерпілого та сліди кримінального правопорушення.

Як цілком слушно зазначає В. Г. Хахановський, «найважливішим елементом криміналістичної характеристики злочину є спосіб

його вчинення, який складається з комплексу специфічних дій правопорушника з підготовки, вчинення злочину та його маскування. Ці дії являють собою певну систему, вони у зовнішній обстановці утворюють відповідні відображення, які в інформаційному плані є своєрідною моделлю злочину» [7, с. 89].

Деякі науковці вважають, що можна виділити таки групи неправомірного доступу до комп'ютерної інформації:

– способи безпосереднього доступу (наприклад, проникнення до приміщення, де розташовується комп'ютер);

– способи віддаленого доступу (наприклад, підключення до телекомунікаційного обладнання, комп'ютерної системи чи мережі або ж безпосереднє та електромагнітне перехоплення інформації);

– комплексні способи (наприклад, модифікація комп'ютерної програми або доступ до баз даних і файлів шляхом знаходження слабких місць у системах захисту) [7, с. 90–91].

На нашу думку, відповідно до Розділу XVI КК України до способів вчинення кіберзлочинів можна віднести:

1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України);

2) створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361^1 КК України);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (ст. 361^2 КК України);

4) несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ч. 1 ст. 362 КК України);

5) несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації (ч. 2 ст. 362 КК України);

6) 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 (ст. 363 КК України);

7) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363^1 КК України).

Слід погодитись з Я. В. Неділько, що «у криміналістичному аспекті особа сучасного кіберзлочинця має певну індивідуальну специфіку, що обумовлюється наявністю у таких осіб спеціальних знань та навичок з використання інформаційних технологій для досягнення злочинного наміру» [8, с. 203].

В наукових дослідженнях науковців існує багато різних класифікацій комп'ютерних злочинців. Наприклад:

1. За психологією мети та сферою злочинної діяльності: хакери, крекери, фріки, колекціонери [9, с. 188].

2. Залежно від характеру посягання на комп'ютерну інформацію: 1) особи, які вчинюють так звані операційні злочини (оператори, які забезпечують роботу комп'ютерів, периферійних пристроїв тощо); 2) особи, які при вчиненні комп'ютерного злочину використовують програмне забезпечення (системні комп'ютерні програмісти; прикладні комп'ютерні програмісти; фахівці із захисту інформації; розробники відповідних систем); 3) особи, які обслуговують апаратну частину

(інженери-системники, інженери-електронники. інженери-зв'язківці); 4) особи, які займаються організаційною роботою щодо інформаційних систем (безпосередньо керівники підприємств, в яких є комп'ютери, їх мережі; адміністратори комп'ютерних мереж; працівники обчислювальних центрів, служб інформаційного забезпечення установ; адміністратори баз даних).

3. Залежно від віку: 1) від 14 до 20 років; 2) від 21 до 45 років [10, с. 161].

На нашу ж думку, кіберзлочинця мають характеризувати у сукупності як загальні (вік, стать, соціальний та психологічний стан тощо), так і спеціальні (професійні звички, особливий «почерк» тощо) ознаки.

Тому, до осіб, які вчиняють кіберзлочин, можна віднести:

1) порушників правил користування комп'ютерами, які займаються поширенням вірусів, несанкціонованим використанням комп'ютерів, відповідних систем та мереж тощо;

2) спеціально підготовлених осіб, які займаються комп'ютерним шпіонажем з метою отримання важливих стратегічних даних в економічній, політичній, технічній та інших сферах;

3) осіб, які страждають на відповідний вид психічних захворювань – інформаційні хвороби (комп'ютерні фобії);

4) професійних комп'ютерних злочинців, які вчиняють певні дії з корисливою метою.

Крім того, у нормах певних статей КК України міститься вказівка на спеціальний суб'єкт вчинення кіберзлочинів, а саме:

1) особа, що має право доступу до інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362);

2) особа, що відповідає за експлуатацію електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363) [1].

На думку В. Г. Хахановського, «потерпілими від кіберзлочинів найчастіше є юридичні особи. Це зумовлено тим, що процес комп'ютеризації широко охоплює, насамперед, юридичних осіб (організації, установи), а значно меншою мірою – фізичних осіб. Саме тому виокремлюють три головні групи потерпілих від таких злочинів: власники комп'ютерної системи; клієнти, які користуються їх послугами та інші особи» [7, с. 92].

Слід також зазначити, що українське законодавство чітко встановлює:

1. Об'єкти кібербезпеки, до яких належать:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

2. Об'єкти кіберзахисту до яких належать:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [3].

Що ж стосується слідів кримінального правопорушення, то варто зазначити, що кіберзлочини характеризуються специфічною їх картиною, оскільки на місці події поруч з матеріально фіксованими слідами утворюються й віртуальні або цифрові сліди.

На думку Я. Найдьон, «віртуальні сліди – це цифровий образ, електронні сигнали, що залишаються в пам'яті електронних і подібних до них пристроїв, що передаються за допомогою заданого алгоритму і мають кримінально-релевантне значення» [11, с. 306].

При цьому, О. С. Омельян зазначає, що «цифрові сліди, що утворюються під час вчинення кіберзлочинів – це інформація, яка зафіксована у цифровому форматі, міститься в різ-

ного роду цифрових пристроях зі створення, обробки, збереження та передачі цієї інформації, причинно пов'язана з подією кіберзлочину та дозволяє встановити як обставини вчиненого правопорушення, так і особу кіберзлочинця» [12, с. 461].

Отже, до слідів як елементів криміналістичної характеристики кіберзлочинів можна віднести:

1) матеріально фіксовані сліди (документи, відбитки, технічні пристрої тощо);

2) відомості та дані, зафіксовані в цифровій формі на матеріальних носіях;

3) електронна інформація, створена комп'ютером чи людиною;

4) програмне забезпечення;

5) комп'ютерні системи.

Висновок. Отже, з огляду на все вищезазначене можна зробити висновок, що кіберзлочинність є вкрай небезпечним соціальним явищем, яке становить загрозу світового масштабу. До основних елементів криміналістичної характеристики кіберзлочинів слід віднести: спосіб вчинення кримінального правопорушення, особу злочинця, особу потерпілого та сліди кримінального правопорушення. Крім того, варто вказати на те, що кіберзлочинця мають характеризувати у сукупності як загальні (вік, стать, соціальний та психологічний стан тощо), так і спеціальні (професійні звички, особливий «почерк» тощо) ознаки.

ЛІТЕРАТУРА:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n3500 (дата звернення: 25.10.2022).

2. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 25.10.2022).

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.10.2022).

4. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2. С. 276-282.

5. Конвенція про кіберзлочинність 23.11.2001 року // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 25.10.2022).

6. Берназ П. В. Поняття «криміналістична характеристика злочину». *Південноукраїнський правничий часопис*. 2017. № 2. С. 34-38.

7. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів. *Юридичний часопис Національної академії внутрішніх справ*. 2011. № 1(1). С. 89-93.

8. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право. Юридичні і політичні науки*. 2020. Вип. 88. С. 202-211.

9. Козак Н. С. Криміналістична характеристика осіб, які вчиняють комп'ютерні злочини. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2013. № 2. С. 186-191.

10. Титаренко А. В. Особа кіберзлочинця як елемент криміналістичної характеристики. *Журнал східноєвропейського права*. 2019. № 62. С. 159-168.

11. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304-307.

12. Омельян О. С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 457-466.