УДК 343.98

П. Д. Біленчук
кандидат юридичних наук, доцент, професор

Київський університет права НАН України

Л. В. Борисова
кандидат юридичних наук, доцент

Національний університет цивільного захисту України

В. П. Колонюк
кандидат юридичних наук, доцент,
учений секретар

Київський науково-дослідний інститут судових експертиз
Міністерства юстиції України

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ТРАНСНАЦІОНАЛЬНИХ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

У статті на основі аналізу нормативних документів встановлено, що сьогодні не існує чітко визначеного поняття «комп'ютерний злочин», зроблено висновок, що сформульовані визначення не враховують таких специфічних дій як посягання на новий різновид суспільних відносин – захисту законної діяльності в сфері інформаційних технологій, запропоновані уточнюючі поняття основних елементів криміналістичної характеристики транснаціональних комп'ютерних злочинів.

Ключові слова: *транснаціональні комп'ютерні злочини, криміналістична характеристика.*

Комп'ютерна злочинність стає одним з найбільш небезпечних видів злочинних посягань: злочинці дуже швидко усвідомили масштаби можливостей Інтернет і телекомунікацій. За даними ООН збитки, що спричиняються комп'ютерними злочинами, зіставлені з прибутками від незаконного обігу наркотиків і зброї. Серед комп'ютерних злочинів, вчинених у світі, все більше стає «міжнародних», таких, які в якості засобів або жертв використовують телекомунікаційні системи різних держав: через відкриті телекомунікаційні мережі можливий доступ до національних, у тому числі й спеціально захищених інформаційних ресурсів.

Різним аспектам комп'ютерної злочинності, способам і механізму їх вчинення, технології та техніці виявлення і закріплення слідів, тактиці проведення слідчих дій приділялася увага в наукових працях

вітчизняних і зарубіжних вчених: В. Г. Афанасьєва, Ю. М. Батуріна, В. П. Бахіна, Н. Вінера, В. Б. Вєхова, А. Б. Венгерова, О. А. Гаврилова, В. О. Голубєва, М. В. Гуцалюка, І. З. Карася, В. В. Крилова, В. Д. Курушина, В. О. Мещерякова, М. С. Полєвого, В. Ю. Рогозіна, М. Г. Шурухнова. Теоретичним підґрунтям дослідження стали роботи вчених Р. С. Бєлкіна, В. І. Галагана, І. Ф. Герасимова, В. Г. Гончаренка, Л. Я. Драпкіна, А. В. Іщенка, Н. І. Клименко, В. В. Клочкова, М. В. Костицького, В. С. Кузьмічова, В. К. Лисиченка, Є. Д. Лук'янчикова, О. Є. Манохи, Г. А. Матусовського, Л. С. Митричева, В. О. Образцова, М. В. Салтевського, М. Я. Сегая, В. В. Тіщенка, В. Ю. Шепітька, М. П. Яблокова та інших.

Разом з тим, є потреба у подальшому поглибленому дослідженні відомостей про транснаціональні комп'ютерні злочини, з метою підсилення ефективності боротьби з протиправними діями в сфері інформаційних технологій.

На початку 60-х років американський юрист Д. Б. Паркер, запровадила термін «комп'ютерна злочинність» для позначення злочинів, у яких ЕОМ є як об'єктом злочину, тобто ЕОМ завдається матеріальна шкода шляхом фізичного пошкодження, так і засобом, коли її використовують для вчинення актів обману, приховування або привласнення з метою отримання власності, грошей, послуг, політичних чи ділових переваг [1, с. 15]. Склади комп'ютерних злочинів як самостійної групи кримінальних правопорушень були вперше сформульовані у 1979 році в м. Далласі на конференції асоціації адвокатів США. Запропонована у той час ними система виглядала наступним чином [2, с. 7]:

– використання або спроба використання комп'ютера, обчислювальної системи або мережі комп'ютерів з метою отримання грошей, власності чи послуг, прикриваючись фальшивими приводами та неправдивими обіцянками або видаючи себе за іншу особу;

– навмисна несанкціонована дія, що має за мету зміну, пошкодження, знищення або крадіжку комп'ютера, обчислювальної системи, мережі комп'ютерів чи систем математичного забезпечення, що містяться в них, а також програм або інформації;

– навмисне несанкціоноване порушення зв'язку між комп'ютерами, обчислювальними системами або мережами комп'ютерів.

Ще у 1986 році в Парижі група експертів Організації економічного співробітництва та розвитку дала визначення комп'ютерного злочину під яким розумілася «будь-яка незаконна, неетична або заборонена поведінка, яка зачіпає автоматизовану обробку і (або) передачу даних» [3, с. 9]. У США визначенням, яке на сьогодні має велике розповсюдження, є ствердження, що комп'ютерний злочин – це будь-

яка незаконна дія, для вчинення якої використовується знання комп'ютерної технології [4].

Першим документом Ради Європи стосовно цього питання є Рекомендація № R89(9) Комітету Міністрів держав-членів Ради Європи про злочини, які пов'язані з комп'ютером, прийнята 13 вересня 1989 року, де була сформульована перша спроба визначити поняття і коло злочинів, пов'язаних з використанням комп'ютера [5].

У Рекомендаціях № R(95)13 з проблем кримінально-процесуального права, що пов'язані з інформаційними технологіями, Рада Європи термін «злочин з використанням комп'ютера» замінила терміном «злочин, пов'язаний з використанням комп'ютерних технологій» [6]. У цьому документі підкреслюється, що злочини, які пов'язані з використанням інформаційних технологій, можуть вчинятися не тільки за допомогою окремого комп'ютера, але й комп'ютерної системи, що може бути як об'єктом, так і середовищем вчинення злочину.

Посилаючись на матеріали Десятого Конгресу ООН з попередження злочинів і поводження з правопорушниками, який відбувся у Відні 10-17 квітня 2000 року, кіберзлочин (у вузькому смислі – «комп'ютерний злочин») – злочин, вчинений в електронному середовищі, тобто деяке незаконне діяння, що веде до кримінальної відповідальності, хоч у різних державах існують різні підходи щодо оцінки «незаконності» тих чи інших дій. Кіберзлочин може бути вчинений засобами комп'ютерних систем і мереж, у комп'ютерній системі або мережі, чи проти комп'ютерної системи або мережі [7, с. 4].

Перша точка зору, яку сформулював Ю. М. Батурін, полягала в тому, що комп'ютерна злочинність з юридичної точки зору не існує, але багато традиційних видів злочинів модернізуються за рахунок використання обчислювальної техніки, тому правильніше сказати про комп'ютерні аспекти злочинів [8, с.129]. І. З. Карась зазначав, що «час вимагає прискорення темпу розвитку правового забезпечення інформатики, бо стихійно сформовані відношення можуть уповільнити та деформувати бажані для суспільства зміни» [9, с. 3]. У зв'язку з можливими матеріальними і моральними втратами в сфері інформаційних технологій, слід було б винайти резерви для створення випереджаючих темпів розвитку нормативної бази системи охорони автоматизованих даних [10, с. 3].

М. С. Полєвий і В. Б. Вєхов відносять до даного виду злочинів такі з них, у яких комп'ютер використовується безпосередньо як предмет або знаряддя посягання [11, с. 243; 12, с. 24]. Зазначимо, що під таке визначення підпадає крадіжка засобів обчислювальної техніки. У випадку, коли комп'ютер не містить інформації, яка охороняється законом, немає необхідності виділяти такий замах з ряду злочинів, спрямованих проти власності. Наприклад, підробка грошей,

документів, штампів з використанням обчислювальної техніки (більшість сучасних поліграфічних комплексів базується на персональних ЕОМ) сьогодні є комп'ютерним злочином. Такі дії як блокування комп'ютерної інформації в телекомунікаційних мережах загального користування за допомогою некомп'ютерних засобів згідно з цим визначенням не є комп'ютерним злочином, а це суперечить відповідним статтям Кримінального кодексу.

У ст. 1 Угоди про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами в сфері інформаційних технологій від 31.05.01 року комп'ютерний злочин визначається як кримінально каране діяння, предметом якого є комп'ютерна інформація [13].

До комп'ютерного злочину пропонуємо відносити всяке протиправне діяння, що здійснюється за допомогою будь-яких програмних або технічних засобів і має за мету впливати на засоби комп'ютерної безпеки та дані, які обробляються або зберігаються в комп'ютерній системі, структури розміщення даних у пам'яті ЕОМ, програми управління базами даних у випадку, а також другорядні або побічні загрози, такі як підготовка до більш серйозних атак: передача комп'ютерних паролів, ключів кодування, кодів доступу та інше.

Аналіз нормативних документів дозволяє стверджувати, що сьогодні не існує чіткого визначення поняття «транснаціональний комп'ютерний злочин». Акцентуємо, що ці формулювання не враховують відповідних специфічних дій як посяганням на новий різновид суспільних відносин – захисту законної діяльності в сфері інформаційних технологій.

На підставі аналізу вітчизняних і зарубіжних нормативних актів та наукових праць пропонується дефініція «транснаціональний комп'ютерний злочин» як посягання на новий вид суспільних відносин – захисту законної діяльності у сфері інформаційних технологій, тобто передбачені кримінальним законом суспільно-небезпечні дії, в яких машинна інформація є засобом або об'єктом злочинних замахів, які призвели до знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, систем ЕОМ і їхніх мереж, створення та розповсюдження шкідливих програм, а також незаконне володіння інформацією та її розповсюдження в телекомунікаційних мережах.

Криміналістична характеристика злочинів, «повинна являти собою відносно стабільну сукупність інформації про ознаки конкретного виду злочинів» [14, с. 423]. Вперше про криміналістичну характеристику як елемент методики згадує Л.О. Сергєєв, зробивши спробу дати розгорнуте поняття перерахуванням елементів як сукупності ознак злочину і відзначивши взаємозв'язки між цими елементами [15, с. 4–5], С. П. Митричев надав важливого значення вивченню «типових ознак, які характеризують особливості даного виду злочинів» [16, с. 28]. Точка зору М. П. Яблокова базується на основі аналізу криміналістичних

особливостей різних видів злочинної діяльності в період її підготовки, вчинення та приховування з урахуванням структури відповідного виду злочинної діяльності. Сукупність матеріальних, інтелектуальних та інших слідів – наслідків злочинної діяльності, що дає уявлення про її характерні особливості, утворює фактичну (інформаційну) основу криміналістичної характеристики [17, с. 36].

М. В. Салтевський, вважає найбільш досконалим інформаційний підхід при конструюванні визначення криміналістичної характеристики, як інформаційної моделі, що являє собою якісно-кількісну систему опису типових ознак конкретного виду (групи) злочинів [14, с.418–419] і, аналізуючи структури криміналістичних характеристик, прийшов до висновку, що більшість авторів виділяють такі чотири основні елементи [213 18, с.130–133]:

- предмет безпосереднього посягання;
- спосіб вчинення злочину в його широкому розумінні;
- типову обстановку – «слідову картину» в її широкій інтерпретації;
- особу злочинця.

Р. С. Бєлкін у якості основних елементів криміналістичної характеристики окремого виду (типу) злочинів, розглядає криміналістично значущі відомості про вихідну інформацію стосовно злочину, що має надати повну уяву про предмет доказування, а характер і склад вихідних даних на початок розслідування є важливими для визначення його напряму [19, с. 302]. До характеристики вихідної інформації належить віднести:

- поняття даного типу злочинів;
- дані про безпосередньо об'єкт та предмет посягання;
- дані про обставини вчинення злочину (місце, час, інші обставини).

Розглянемо елементи криміналістичної характеристики злочинів, пов'язаних з використанням комп'ютерної інформації (рис.1.1).

Вихідною інформацією про транснаціональні комп'ютерні злочини стають відомості про предмет замаху – характеристики комп'ютерної інформації та її носіїв. Вважаємо, носії комп'ютерної інформації не є об'єктом криміналістичних досліджень, доки не несуть в собі сліди вчиненого злочину або такого, що вчиняється. Така інформація може бути сприйнята не тільки суб'єктом, але й технічними пристроями, а також бути віддалена від відображення об'єкта пізнання.

Місце вчинення злочину – як елемент криміналістичної характеристики, дозволяє відповісти на запитання – де вчинено злочин? При розслідуванні багатьох злочинів необхідно враховувати: місце, де відбуваються підготовчі дії до злочину; місце безпосереднього вчинення злочину; місце, де залишені сліди (у широкому розумінні) злочинного посягання; місце приховування слідів злочину, знарядь і засобів його вчинення, предмета злочинного посягання [20, с. 193].

Рис. 1.1 Елементи криміналістичної характеристики комп'ютерних злочинів.

З урахуванням міжнародних масштабів телекомунікаційних мереж стає все менш ймовірним, що всі елементи комп'ютерних злочинів обмежуються територією окремої держави: несанкціоноване підключення до інформаційних ресурсів комп'ютерних систем або їхніх мереж може здійснюватися шляхом програмного чи технічного, контактного або безконтактного втручання в фізичні чи віртуальні мережі, тобто присутність правопорушника на місці, де знаходяться інформаційні ресурси, які представляють для нього інтерес, не є необхідною. Можливими є декілька місць вчинення злочину, а саме:

- місця підключення мережевих пристроїв і аксесуарів для використання комп'ютерної системи у складі мережі (локальної, регіональної, глобальної);
- місце високої інтенсивності роботи в мережі (локальної, регіональної, глобальної);
- місце безпосереднього впливу спеціальних технічних і програмних засобів для несанкціонованого доступу до комп'ютерної інформації;
- місце обробки і постійного зберігання комп'ютерної інформації;
- місце використання результатів несанкціонованого доступу до комп'ютерної інформації (держава, в якій такі діяння не передбачають кримінальної відповідальності, що дає можливість комп'ютерним злочинцям знаходитися під захистом закону цієї країни).

Дані про спосіб вчинення злочину в криміналістичному розумінні складають один із найважливіших елементів структурної системи криміналістичної характеристики. О. М. Васильєв, пропонує криміналістичне визначення «способу вчинення злочину як комплексу дій, які вибрав злочинець (злочинці) для досягнення злочинної мети у відповідності з його (їхніх) особистісними властивостями та об'єктивними обставинами й умовами, що утворюють механізм вчинення злочину і відображеного в матеріальних слідах злочину, що дозволяє зробити висновок про психічні та фізичні риси злочинця, його місце серед людей та речей в події злочину і його ціле покладання» [36 21, с. 66]. Спосіб вчинення злочину свідчить про те, як, яким чином особа вчинює суспільно небезпечну дію, які прийоми, методи і засоби вона застосовує для цього. У цьому випадку важливою цінністю є сліди, що вказують, якими діями злочинець учинив наступне: потрапив на місце злочину, пішов з нього, подолав перешкоди, використав своє службове положення, виконав злочинний намір, характер зв'язку злочинця з предметом злочину, які навики, знання і зусилля застосував, намагався чи ні приховати сліди злочину [20, с. 191].

Пропонуємо способи злочинної діяльності в сфері інформаційних технологій поділити на дві групи.

Перша група злочинних дій здійснюється без використання комп'ютерних пристроїв у якості інструменту для проникнення зовні в комп'ютерні системи або впливу на них. Ці дії можуть бути такими:

– перехоплення інформації (безпосереднє, електромагнітне, аудіоперехоплення, відеоперехоплення;

– фотографування інформації в процесі її обробки;

– виготовлення паперових дублікатів вхідних і вихідних документів, копіювання роздруківок;

– крадіжка машинних носіїв інформації;

– огляд і вивчення не повністю знищених роздруківок діяльності обчислювальних центрів.

Друга група злочинних дій здійснюється з використанням комп'ютерних та комунікаційних пристроїв і аксесуарів у якості інструмента для проникнення в інформаційні системи або впливу на них. Характерні особливості даного виду злочинної діяльності включають в себе:

– несанкціонований доступ до комп'ютерної інформації, тобто отримання можливості ознайомитися і здійснювати операції з чужою інформацією, яка знаходиться на машинних носіях – дії, що спрямовані на порушення конфіденційності та цілісності інформації (наприклад, використання пошукової адреси компанії з метою доступу до всієї системи);

– виготовлення і розповсюдження шкідливих програм – «створена або існуюча програма зі спеціально внесеними змінами, що призводять до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ і їхніх мереж» [13], яка спрямована на порушення конфіденційності й цілісності інформації;

– дії, що спрямовані на порушення порядку використання, створення перебоїв у функціонуванні та довільному відключені ЕОМ, її пристроїв.

Час вчинення злочину має важливе значення і впливає на етапи виникнення, існування й використання доказової інформації. Врахування впливу часового фактора в процесі розслідування транснаціональних комп'ютерних злочинів дозволяє визначити час події злочину, встановити часові зв'язки між фактами, з'ясувати черговість подій, дій або факторів, обчислити тривалість різних подій та ін.

За допомогою програм загальносистемного призначення встановлюється час, що дозволяє в будь-який момент за відповідною командою вивести на екран монітора інформацію про день та час виконання певної операції. При вході в систему ЕОМ чи їхню мережу (в тому разі й несанкціонованому), час роботи на комп'ютері будь-якого користувача і час конкретної операції автоматично фіксується в оперативній пам'яті ЕОМ, та відображається у вихідних даних (на

моніторі, роздруківках чи дискеті). Таким чином, точний час несанкціонованого доступу можна встановити слідчим оглядом комп'ютера, роздруківок чи дискет, допитом свідків із числа персоналу, який обслуговує комп'ютерну систему, з'ясовуючи час, коли кожний з них працював на комп'ютері, якщо це не зафіксовано автоматично.

Прийнявши за основу точку зору В. М. Бикова про те, що не для всіх злочинів може бути використана одна структура криміналістичної характеристики [22, с. 6], пропонуємо в криміналістичну характеристику транснаціональних комп'ютерних злочинів замість поняття «спосіб вчинення злочину» ввести *«спосіб впливу на комп'ютерну інформацію впродовж часу вчинення злочину»*, який може бути основою для формування слідчих ситуацій, визначення напряму розслідування, типових наслідків вчинення комп'ютерного злочину (системи слідоутворення) і розкриття злочинів.

Отже, розглядаючи, криміналістичну характеристику транснаціональних комп'ютерних злочинів як ймовірну модель орієнтуючої інформації, яка слугує конкретизації цілей розслідування та його напрямів, зроблено висновки:

– інформаційний підхід до змісту її криміналістичної характеристики зумовлює об'єктивні труднощі, які необхідно долати працівникам правоохоронних органів при розслідуванні транснаціональних комп'ютерних злочинів;

– у сфері інформаційних технологій вчинення транснаціонального злочину характеризується незбіжністю місця здійснення протиправних дій з місцем настання суспільно-небезпечних наслідків.

Перелік посилань

1. *Рассследование* компьютерных преступлений // Проблемы преступности в капиталистических странах. 1984. № 6. С. 14–19.

2. *Компьютерные* преступления: учеб. пособ. Москва, 1995. 104 с.

3. *OECD*, Computer-Related Crime: Analysis of Legal Policy. Paris, 1986. P. 9.

4. *McEwen J. T.* Dedicated Computer crime units, National Institute of Justice.1989, June.

5. *Recommendation № R 89 (9)* of the Committee of Ministers of the Concil of Europa to member States for the Computer-Related Crime and Final Report of the European Committee on Crime Problems. Strasbourg, 1990.

6. *Recommendation № R 89 (9)* of the Committee of Ministers of the Concil of Europa to member States for the concerning problems of criminal procedural law connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies). Strasbourg, 1995.

7. *Преступления*, связанные с использованием компьютерной сети. Справочный документ для семинара-практикума по использованию компьютерной сети. / Десятый Конгресс Организации Объединенных

Наций по предупреждению преступности и обращению с правонарушителями // Документ ООН A/CONF/187/10.

8. *Батурин Ю. М.* Проблемы компьютерного права. Москва, 1991. 268 с.

9. *Карась И. З.* Вопросы правового обеспечения информатики // Микропроцессорные средства и системы. 1986. № 1. С. 3–9.

10. *Литвинов А. В.* Правовые вопросы охраны компьютерной информации // Советское государство и право, 1987. № 8. С. 84–88.

11. *Полевой Н. С.* Правовая информатика и кибернетика. Москва, 1993. 527 с.

12. *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия. Москва, 1996. 182 с.

13. *Угода* про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами в сфері комп'ютерної інформації. (Додаток).

14. *Салтевський М. В.* Криміналістика (у сучасному виклад): підруч. Київ, 2005. 588 с.

15. *Сергеев Л. А.* Расследование и предупреждение хищений, совершаемых при производстве.

16. *Митричев С. П.* Общие положения методики расследования отдельных видов преступлений // Криминалистика и судебная экспертиза. Київ, 1973. Вып.10. С. 27–32.

17. *Криминалистика*: учеб. / отв. ред. М. П. Яблоков. – 2 изд., перераб. и доп. Москва, 2000. 718 с.

18. *Салтевський М.В.* Криміналістика: навч.-довід. посіб. Київ, 1996. 159 с.

19. *Белкин Р. С.* Курс криминалистики: в 3-х т. Москва, 1997. Т. 3: Криминалистические средства, приемы и рекомендации. 480 с.

20. *Настільна* книга слідчого: наук.-практ. видання для слідчих і дізнавачів / *М. І. Панов, В. Ю. Шепітько, В. О. Коновалова* та ін. Київ, 2003. 715 с.

21. *Васильев А. Н.* Следственная тактика. Москва, 1976. 200 с.

22. *Быков В. М.* Особенности расследования групповых преступлений. Ташкент, 1980. 60 с.

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ТРАНСНАЦИОНАЛЬНЫХ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

П. Д. Биленчук
Л. В. Борисова
В. П. Колонюк

В статье на основе анализа нормативных документов установлено, что сегодня нет единого четкого определения понятия «компьютерное преступление», сделан вывод, что сформулированные определения не учитывают такие специфические деяния как посягательства на новый вид общественных отношений – защита законной деятельности в сфере информационных технологий.

Среди компьютерных преступлений, совершенных в мире, все больше становится «международных», которые в качестве средств или жертв используют телекоммуникационные системы разных стран: через открытые

телекоммуникационные сети возможен доступ к национальным, в том числе и специально защищенным ресурсам.

Термин «компьютерное преступление» был разработан для определения абсолютно новых видов преступности, которая ориентируется как на компьютеры, телекоммуникационные сети и их пользователей, так и более традиционных преступлений, для совершения которых сегодня используется компьютерное оборудование.

На основе обобщение результатов научных исследований и практических материалов дано определение транснациональных компьютерных преступлений, выделены и проанализированы основные элементы их криминалистической характеристики: предмета непосредственного посягательства – характеристики компьютерной информации и ее носителей, которые становятся объектами криминалистических исследований, когда несут в себе следы совершенного преступления или такого, которое совершается и такая информация может быть воспринята не только объектом, но и техническими устройствами; способа совершения преступления в его широком понимании, типичной обстановки – следовой картины; психофизиологические аспекты характеристики личности преступника. Выделены и систематизированы криминалистически значимые сведения о времени, месте совершения преступления, рассмотрены способы несанкционированного доступа к компьютерной информации при совершении транснациональных компьютерных преступлений.

Рассматривая криминалистическую характеристику транснациональных компьютерных преступлений, как вероятную модель ориентирующей информации, которая служит для конкретизации целей расследования и его направлений, сделано вывод, что в сфере информационных технологий совершение транснациональных компьютерных преступлений характеризуется несовпадением наступление места совершения противоправных действий с местом наступлений общественно-опасных последствий.

CRIMINALISTICS CHARACTERISTICS OF TRANSNATIONAL COMPUTER CRIMES

P. Bilenchuk
L. Borysova
V. Koloniuk

In the article, on the basis of analysis of regulatory documents, it is established that today there is no single clear definition of the concept of «computer crime»; it is concluded that the formulated definitions do not take into account such specific acts as an infrigement on a new type of social relations – the protection of lawful activities in the field of information technologies.

Among the computer crimes committed in the world, «international» has become more spread, which as means or victims use telecommunications systems of different countries: through open telecommunication networks access to national, including specially protected resources is possible.

The term «computer crime» was developed to identify completely new types of crime, which is oriented towards computers, telecommunication networks and their users, as well as more traditional crimes for which today computer equipment is being used.

On the basis of the synthesis of the results of scientific research and practical materials, the definition of transnational computer crimes, the main elements of their criminalistics characteristics are identified and analyzed: the subject of direct infringement is the characteristics of computer information and its carriers which become the objects of forensic research when carried traces own traces of a committed crime or something that is happening and such information can be perceived not only by the object and the technical devices; a method of committing a crime in its broad sense, a typical situation – a trace pattern; psychophysiological aspects of the personality characteristics of the offender.

It is singled out criminologically significant information about the time and place of the crime, methods of unauthorized access to computer information in the case of transnational computer crimes.

Considering the forensic character of transnational computer crimes as a probable model of oriented information that serves to specify the objectives of the investigation and its directions, it is concluded that in the field of information technology, the transnational computer crimes are characterized by a divergence of the place of committing unlawful actions with the place of occurrence of socially dangerous consequences.

УДК:343.98.06

О. А. Самойленко
кандидат юридичних наук, доцент

Національний університет «Одеська юридична академія»

ПРИРОДА КІБЕРПРОСТОРУ ЯК ОБ'ЄКТА КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ

У статті на підставі аналізу подвійної природи кіберпростору, зокрема технічної та соціальної його суті, визначено природу кіберпростору як об'єкта криміналістичного дослідження. Відзначено особливості кіберпростору, які злочинець використовує з метою досягнення злочинного результату. Констатується, що кіберпростір накладає суттєвий відбиток на механізм кримінального правопорушення. В цьому аспекті кіберпростір в криміналістичних дослідженнях може розглядатися як середовище (обстановка) вчинення злочину або специфічна обстановка, в яку внесені зміни в результаті правопорушення (його сліди).

Ключові слова: *злочин, злочинна діяльність, кіберпростір, механізм злочину, ознака, технологія.*

Сьогодні усі дії, пов'язані з використаням кіберпростору, мають цілком реальні наслідки. Цей факт відповідним чином детермінував сучасну злочинність, яка пристосувалася до нової обстановки традиційних сфер життєдіяльності суспільства: дистанційного спілкування та освіти, електронних торгівлі, благодійності, комерції,