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,

інформаційних війн тощо. Можливості кіберпростору породжують нові та вдосконалюють наявні форми кримінальних правопорушень. Використання кіберпростору для вчинення злочинів різних видів безперечно зумовлює необхідність привернення уваги до нього в криміналістичних дослідженнях.

В сучасній криміналістиці кіберпростору приділялась увага в контексті засобів або обстановки вчинення злочинів, зокрема В. А. Динту, С. П. Кушніренком, В. А. Мещеряковим, Є. С. Шевченком та багатьма іншими криміналістами [1–3]. У закордонних публікаціях з проблем кіберзлочинності автори часто ототожнюють кіберпростір та обстановку вчинення злочину, використовуючи англійський вислів «crime scene cyberspace» [4], що дослівно перекладається як «обстановка кіберпростору» або «кіберпростір як місце злочину». Втім, вітчизняні та закордонні науковці не підходять до природи кіберпростору системно, приділяючи увагу лише окремим особливостям кіберпростору, що зумовлюють особливості розслідування окремих видів злочинів. Метою цієї статті є визначення природи кіберпростору як об'єкта криміналістичного дослідження.

Кіберпростір дуже часто ототожнюють з інформаційним простором, тому досліджуючи природу кіберпростору потрібно ці терміни розмежувати. В цьому сенсі доречно звернутися до кібернетики як теорії управління в живому та неживому світі, що розглядав Н. Вінер. Наприкінці 40-х років XX ст. вибухнула «криза надлишку інформації». Суспільство могло бути «задушене» інформацією, якби не сталося винайдення комп'ютера. «Вінерівська кібернетика» була орієнтована саме на інформаційні проблеми. Дослідник визнавав, що теорія інформації є основою цієї науки [4, с. 18]. Сучасна кібернетика є міжгалузевою наукою про загальні закономірності процесів управління й передавання інформації в машинах, живих організмах і суспільстві [5]. Утім формування інформаційного суспільства є сучасною переважною тенденцією розвитку-впровадження людства в глобальний інформаційний простір на базі інформаційно-комп'ютерних технологій, Інтернету, засобів масової інформації тощо [6]. Тож, зміст терміна «інформаційний простір» є ширшим за «кіберпростір» та містить останній як визначальну складову.

Правники, політологи неодноразово вдавалися до спроб надати визначення поняття «кіберпростір», але одностайності щодо сутності кіберпростору навіть у науках кримінального циклу досягти не вдалося [7 – 10]. Джон Барлоу – автор праці «Декларація незалежності кіберпростору» – зазначав, що електронний інформаційний простір має два рівні: 1) обмін інформацією у формі програмних кодів, який здебільшого й створює кіберпростір; 2) віртуальні життя, створювані внаслідок обміну інформацією між

аватарами [11] (так традиційно називають користувачів мережі). Тож, кіберпростір утворюється в результаті взаємодії між людьми шляхом обміну інформацією в електронній цифровій формі. Тому для розуміння сутності кіберпростору як об'єкта криміналістичного дослідження необхідно дослідити його подвійну природу: технічну та соціальну.

Технічна природа кіберпростору. Розвиток глобального електронного простору розпочався із замовлення Управління перспективних досліджень Міністерства оборони США у 1969 році на побудову мережі, здатної забезпечити обмін інформацією між користувачами за умов ядерної війни. Наприкінці 80-х років XX ст. мережа поєднувала комп'ютери не лише в США, а й по всьому світу, хоча інформація, що надходила каналами зв'язку, на екранах моніторів мала вигляд текстових символів. З 1992 року було задіяно так звану «WWW» (з англ. «word» – «світ», «wide» – «широко», «web» – «павутиння»), або «Всесвітню павутину», створену як інформаційну технологію Тімом Бернесом-Лі – фахівцем Європейського центру ядерних досліджень у м. Женева. Власне, це засіб доступу до інформаційних ресурсів Інтернет, тобто мережі пов'язаних між собою сторінок, що є веб-вузлами всього світу з гіпертекстовими посиланнями [12, с. 75].

Інтернет є основним, але не єдиним засобом створення кіберпростору. З урахуванням комп'ютерної складової електронного обміну інформацією, кіберпростір утворюють усі телекомунікаційні мережі, комп'ютерні системи й пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача.

У сучасній юридичній літературі широкого вжитку набув термін «віртуальний простір», який найчастіше використовують як синонім поняття «кіберпростір» та визначають як модельований за допомогою комп'ютера інформаційний простір, де містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному чи будь-якому іншому вигляді, що перебувають у процесі руху локальними і глобальними комп'ютерними мережами, або ж це відомості, що зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки й передавання [13]. На нашу думку, таке трактування понять може спричинити плутанину під час досліджень у науках кримінально-правового циклу, зокрема щодо криміналістичних методик розслідування окремих видів злочинів, учинених з використанням кіберпростору.

Етимологічно «віртуальний» походить від лат. virtus – римляни вживали його для позначення таких якостей воїна, як мужність,

хоробрість, рішучість [14]. Віртуальність (від лат. virtus – потенційний, можливий) – вигаданий, уявний (можливо, з певною метою) об'єкт, суб'єкт, категорія, ставлення, дія тощо, відсутній на цей момент у реальному світі, а створений лише грою людської уяви або зімітований за допомогою інших об'єктів [15]. Застосуванню терміна «віртуальний» в комп'ютерній галузі сприяло його використання відносно об'єктів, яких не існує у фізичному світі, що не мають чіткої просторової форми.

Однак у науках кримінально-правового циклу в аспекті розроблення та вдосконалення засобів боротьби зі злочинністю кіберпростір не можна розглядати як віртуальний, адже злочинці, котрі використовують його для вчинення злочину, не можуть бути віртуальними. До того ж, інформація в електронній цифровій формі, що має криміналістичне значення, за своєю фізичною природою є доступною безпосередньому сприйняттю через використання програмно-технічних засобів. Унаслідок впливу (знищення, модифікації, копіювання, блокування тощо) комп'ютерної інформації шляхом доступу до неї утворюються певні відомості, які в криміналістиці називають «нетрадиційними», або інформаційними слідами [16, с. 145–146; 17]. Їх можуть зберігати на матеріальному носії постачальники Інтернет-послуг (провайдери), користувачі. Для їх виявлення та вилучення необхідне застосування відповідних технічних засобів [18, с. 74–76].

Сучасний користувач комп'ютерних мереж має можливість здійснювати різноманітні дії в модельованому комп'ютером електронному просторі в реальному часі (наприклад, під час комп'ютерних ігор у мережі, спілкування в соціальних мережах). Ці дії створюють так звану «віртуальну реальність» або «реальну віртуальність». Це система, в якій реальність як така (матеріальне або символічне існування людей) повністю занурена у віртуальні образи, вигаданий світ, у якому зображення не просто перебуває на екрані, через який передається досвід, але й саме стає досвідом [19 с. 22]. У сучасних словниках поняття «віртуальна реальність» подано у вузькому й широкому сенсі [20; 21]. У вузькому розумінні – це ті ігрові або необхідні в технічному плані «штучні реальності», які виникають унаслідок впливу комп'ютера на свідомість, коли, наприклад, на людину одягають «електронні окуляри» й «електронні рукавички». У широкому – це будь-які змінені стани свідомості, як-от: шизофренічні марення, наркотичне чи алкогольне сп'яніння, гіпнотичний стан, ігроманія. Шляхом використання різних комп'ютерних аудіовізуальних технологій людина може реалізовувати свою комунікативну функцію, контактувати не лише з іншими людьми, а й зі штучними персонажами, створеними іншими особами, з метою використання цих образів для подальшого вчинення злочину. Тож, віртуальність – це одна з ознак

кіберпростору, особливість, яка приваблює злочинців для його використання в механізмі вчинення злочину.

Іншою особливістю функціонування кіберпростору є те, що Інтернет провайдери як головні суб'єкти глобальної мережі, що забезпечують доступ до інформації та надають відповідні послуги, не здатні контролювати весь обсяг розміщеної в Інтернеті інформації, оскільки фактично її може бути розміщено на комп'ютері – www-сервері, розташованому в будь-якій частині світу [22]. Зобов'язання щодо здійснення такого контролю має для суспільства як позитивні, так і негативні наслідки.

Так, з одного боку, визнання на державному рівні (у Російській Федерації, Китаї, Ірані та деяких інших країнах) суверенного права держави регулювати комунікаційні можливості в Інтернеті призводить до технічних помилок електронного зв'язку через надмірну обережність провайдерів. Також це зумовлює негативний ефект відносно загального права на свободу слова, спричиняючи певні обмеження.

З іншого боку, незабезпечення державою належної правової охорони відносин у кіберпросторі, наявність неузгодженості щодо чинності законів конкретної держави в межах Інтернету є обставинами, що приваблюють особу, котра має намір віддалено від себе (дистанційно) отримати реальний злочинний результат. Адже правоохоронні органи стикаються зі значними труднощами, коли під час розслідування встановлюють факт перебування під юрисдикцією іншої держави телекомунікаційної мережі, використаної для вчинення злочину, або власника інформаційного ресурсу, якого необхідно захищати від протиправного посягання.

Зрештою, однією з особливостей кіберпростору як складної технічної системи є можливість користувачів здійснювати обмін інформацією в електронній цифровій формі. Такому обміну притаманна оперативність створення, поширення, модифікації або знищення інформації Саме тому в процесі вчинення окремих видів злочинів використання кіберпростору значно прискорює досягнення злочинної мети, а також сприяє якісному приховуванню фактів їх учинення. Тому для ефективної боротьби зі злочинами, вчиненими з використанням кіберпростору, необхідно враховувати як особливості вчинення злочину певної кримінально-правової кваліфікації, так і можливості, які створює кіберпростір для їх учинення, вплив останніх на методику розслідування окремих видів злочинів. У механізмі такої злочинної діяльності кіберпростір як обстановка злочину є передумовою більш ефективного та швидкого досягнення злочинного результату, порівняно з традиційною речовинною обстановкою вчинення злочину.

Соціальна природа кіберпростору. Згідно з першим законом технологій М. Крацберга, виведеним дослідником під час вивчення

розвитку технологій та їх взаємодії з соціокультурними змінами, «сама по собі технологія є ні гарною, ні поганою, але й нейтральною її не назвеш» [23]. Дійсно, результати використання нових технологій залежать від мети суб'єкта їх застосування. Однак саме технології стають визначальним чинником у формуванні стилю життя, цінностей, інститутів та інших елементів сучасного суспільства. Тому, виникнувши як суто технічний спосіб передавання інформації, кіберпростір перетворився на важливе соціальне явище, пов'язане з комунікаційною складовою Інтернет-технологій.

Комунікаційні технології кіберпростору (електронна пошта, скайп, чати, форуми, вебінари, відеоконференції, соціальні мережі) слугують для формування взаємозв'язків зі значними масами населення, впливу на них або взаємодії з ними, інформаційного захоплення чи тиражування інформаційного продукту [24, с. 48]. Користувачі можуть здійснювати один з двох типів доступу до інформаційного простору: а) on line доступ, що дозволяє використовувати мережу в режимі реального часу; б) off line доступ – коли підготовка завдання для мережі відбувається заздалегідь, а з'єднання необхідне лише для передавання чи прийому підготовлених даних.

Учасники комунікації в кіберпросторі взаємодіють між собою з певною мотивацією: діловою (отримання або надання послуг, ведення бізнесу); комунікаційною (спілкування з однодумцями, участь у визначеній загальними інтересами спільноті); пізнавальною (отримання освіти); розважальною (інтерактивні ігри, перегляд телебачення) тощо. Тож, кіберпростір слугує альтернативою реальному матеріальному світові. Своєю чергою, користувачі мережі є учасниками суспільних відносин, що набули поширення в сучасному інформаційному суспільстві, утворили визначені за певним критерієм соціальні групи.

Існує безліч визначень поняття «соціальна група», проте всі соціологи впевнені в тому, що такою групою можна назвати визначену кількість людей, яка відрізняється від інших за характерними соціальними ознаками [25]. У межах кіберпростору діє аналог соціальної групи, так звана «соціальна мережа» – Інтернет-співтовариство користувачів, об'єднаних за будь-якою ознакою на базі одного сайту [26]. Головним чинником об'єднання користувачів у соціальну мережу також є певна актуальна на окремий момент спільна ознака – фінансове становище, стать, приналежність до тієї чи іншої раси, національності, мовної групи, віросповідання, професії або ж інтереси (спорт, ігри, інші зацікавленості) тощо. Група в соціальній мережі кіберпростору відрізняється від звичайної соціальної групи неважливістю такого критерію, як просторова близькість її учасників, та здатністю постійно перебувати в комунікаційному процесі (що забезпечують технології *on line* доступу).

Нині соціальні мережі створили безмежні можливості для об'єднання віддалених одна від одної (часто безпосередньо не знайомих) осіб з метою спільної злочинної діяльності – у кримінологічному сенсі, для ефективної діяльності утворених організованих злочинних угруповань – у кримінальному. Адже скоєння терористичних актів, незаконний обіг наркотичних засобів, поширення порнографії; піратства та інших транснаціональних злочинів потребує технічного, матеріального й організаційного супроводження, що повною мірою забезпечують можливості кіберпростору. Тому організована злочинність активно використовує обстановку кіберпростіру для досягнення злочинної мети.

Зрештою, такі соціальні мережі стали величезним структурованим масивом відомостей про реальне життя конкретної людини, її вподобання, пересування, коло спілкування, робочі функції тощо. За необхідності цю базу може бути вміло використано для вчинення злочину проти неї.

З огляду на зазначене, ***кіберпростір*** слід розуміти як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача. Проведений нами вище аналіз використання кіберпростору зі злочинною метою, узагальнення матеріалів судово-слідчої практики дозволяють визначити певні *особливості кіберпростору,* які злочинець використовує з метою досягнення злочинного результату:

1) віддаленість (дистанційність) доступу до предмета посягання з використанням кіберпростору, що забезпечує транскордонну складову такої злочинної діяльності, яка викликає необхідність вирішення слідчим питань територіальної юрисдикції;

2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі, що є предметом злочинного посягання або слідом злочину – це сприяє значному прискоренню та якісному прихованню злочинної діяльності;

3) віртуальність, що забезпечує відносну конфіденційність інформації про особу злочинця та можливість упливати на свідомість певної категорії осіб;

4) комунікативність, яка уможливлює створення злочинних груп та ефективну діяльність уже наявної організованої злочинності;

5) недосконалість забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що надає злочинцю можливість уникати кримінальної відповідальності за вчинений злочин.

З урахуванням технічної та соціальної складової такого змісту кіберпростору, останній накладає суттєвий відбиток на механізм цього правопорушення. В цьому аспекті кіберпростір в криміналістичних дослідженнях може розглядатися як:

а) середовище (обстановка), в якому окремі його елементи (телекомунікаційна мережа, комп'ютерна система тощо) могли бути використані як знаряддя досягнення протиправної мети – порушення нормального функціонування цього середовища або заволодіння об'єктами інтелектуальної власності, платіжними засобами, матеріальними цінностями;

б) специфічна обстановка, в яку були внесені зміни в результаті правопорушення (його сліди), які можуть виступати джерелами доказів у кримінальному провадженні.

Використана для досягнення злочинного результату обстановка кіберпростору, маючи притаманні лише їй подвійні чинники технічної та соціальної природи, зумовлює необхідність застосування оновлених методів, засобів і прийомів вирішення практичних завдань розслідування такої злочинної діяльності.

Перелік посилань

1. *Шевченко Е. С., Михайлюченко Н. Н.* Киберпространство как элемент обстановки совершения преступлений // Академический юридический журнал. 2015. № 1. С. 52–59

2. *Динту В. А.* Місце кіберпростору в системі обстановки злочину // Науковий вісник Херсонського державного університету. 2016. Вип. 2. Т. 3. С. 72–75

3. *Мещеряков В. А.* Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002. 407 с.

4. *Crime scene* cyberspace. *Globe.* 2012. № 3. Sept. URL: https://www1.ethz.ch/zisc/events/ETHglobe_ZISC_SEP2012.pdf.

5. *Толковый словарь* русского языка С. И. Ожегова [Электронный ресурс]. Режим доступа: URL: http://slovariki.org/tolkovyj-clovar-ozegova/11579.

6. *Дюжев Д. В.* Інформаційне суспільство: соціально-правова парадигма суспільного розвитку: автореф. дис. … канд. філософ. наук: 09.00.03. Донецьк, 2004. 18 с.

7. *Белєнький В. П.* Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльно-правове дослідження): автореф. дис. … юрид. наук: 12.00.08. Київ, 2016. 20 с.

8. *Дубов Д. В.* Кіберпростір як новий вимір геополітичного суперництва: моногр. Київ, 2014. 328 с.

9. *April Mara*, Norm Origin and Development in Cyberspace: Models Of Cybernorm Evolution // Washington University Law Quarterly. 2000. № 78. P. 59–80.

10. *Гавловський В.* Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ, 2000. С. 50–53.

11. *Barlow J. P.* A Declaration of the Independence of Cyberspace. URL: https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

12. *Антонов В. М.* Інтернет: енциклопедичне видання: навч.-метод. посіб. Київ, 2008. 128 с.

13. *Кіпа О.* Правопорушення в мережі Інтернет. Часопис Київського університету права. 2010. № 4. С. 346–349.

14. *Волинець В. О.* Віртуальна реальність: поняття та сутність. Питання культурології. 2014. Вип. 30. С. 35–41.

15. *Глазычев В.* Игры цивилизаций // Век XX и мир. 1994. № 11–12. С. 102–118.

16. *Голубєв В. О.* Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя, 2003. 250 с.

17. *Самойленко О. А.* Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій: моногр. Київ, 2009. 328 с.

18. *Мещеряков В. А.* Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002. 407 с.

19. *Кормич Б. А.* Інформаційне право: підруч. Харків, 2011. 334 с.

20. *Heim M., Helsel Ed. S. K., Roth J. P.* The Metaphysics of Virtual Reality. Virtual Reality: Theory, Practiceand Promise. London, 1991. P. 27–33

21. *Носов Н. А.* Словарь виртуальных терминов. Труды лаборатории виртуалистики // Труды Центра профориентации. М., 2000. Вып. 7. 69 с.

22. *Городенко Л.* Правові взаємини електронних видань та держави // Наукові записки Інституту журналістики. 2005. Т. 20. С. 11–17.

23. *James R.* Hansen Technology and the History of Aeronautics: An Essay. URL: http://www.centennialofflight.net/essay/Evolution_of_Technology/Tech-OV1.htm.

24. *Остапенко Г.* Комунікація та комунікативна активність суспільства в добу Інтернет-технологій: соціальний аспект // Вісник Книжкової палати. 2013. № 9. С.47–49.

25. *Герасимчук А. А., Палеха Ю. І., Шиян О. М.* Соціологія: навч. посіб. 4-те вид., випр. і доп. Київ, 2004. 246 с.

26. *SEO Словник*: [соц. мережа]. URL: //igroup.com.ua/seo-articles/sotsialna-merezha/

ПРИРОДА КИБЕРПРОСТРАНСТВА КАК ОБЪЕКТА КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Е. С. Самойленко

В статье на основании анализа двойственной природы киберпространства, в частности технической и социальной его сути, определена природа киберпространства как объекта криминалистического исследования. Проведен анализ использования киберпространства с преступной целью. Это позволило определить особенности киберпространства, которые преступник использует с целью достижения преступного результата, в частности:

1) отдаленность (дистанционность) доступа к предмету посягательства с использованием киберпространства, что обеспечивает трансграничную составляющую такой преступной деятельности, которая вызывает необходимость решения следователям вопросов территориальной юрисдикции;

2) оперативность создания, распространение, модификации или уничтожение информации в киберпространстве, что является предметом преступного посягательства или следом преступления – это способствует значительному ускорению и качественному сокрытию преступной деятельности;

3) виртуальность, которая обеспечивает относительную конфиденциальность информации о личности преступника и возможности влиять на сознание определенной категории лиц;

4) коммуникативность, которая делает возможным создание преступных групп и повышает эффективность деятельности уже имеющейся организованной преступности;

5) несовершенство обеспечения информационной безопасности и правовой охраны отношений в киберпространстве, что предоставляет преступнику возможность избежать уголовной ответственности за совершенное преступление.

С учетом технической и социальной составляющей такого содержания киберпространства, оно накладывает существенный отпечаток на механизм уголовного правонарушения. В этом аспекте киберпространство в криминалистических исследованиях может рассматриваться как:

а) среда (обстановка), в которой отдельные его элементы (телекоммуникационная сеть, компьютерная система и тому подобное) могли быть использованы как орудие достижения противоправной цели – нарушение нормального функционирования этой среды или завладение объектами интеллектуальной собственности, платежными средствами, материальными ценностями;

б) специфическая обстановка, в которую были внесены изменения в результате правонарушения (его следы); последние выступают источниками доказательств в уголовном производстве.

Использованная для достижения преступного результата обстановка киберпространства, имея присущие лишь ей двойные факторы технической и социальной природы, обуславливает необходимость применения

обновленных методов, средств и приемов решения практических заданий расследования такой преступной деятельности.

NATURE OF CYBERSPACE AS AN OBJECT OF CRIMINALISTICS RESEARCH

O. Samoilenko

In the article on the basis of analysis of ambivalent nature of cyberspace, in particular his essence technical and social, nature of cyberspace as an object of criminalistics research is defined. The analysis of the use of cyberspace with a criminal purpose is conducted. It allowed to define the features of cyberspace, which a criminal uses with the purpose of achievement of criminal result, in particular:

1) remoteness (remotability) of access to the subject of infrigement with the use of cyberspace, that provides a transboundary component of such criminal activity which causes the necessity of decision to the investigators of questions of territorial jurisdiction;

2) the efficiency of the creation, distribution, modification or destruction of information in cyberspace, which is the subject of a criminal offense or the consequence of a crime – it contributes to a significant acceleration and qualitative concealment of criminal activity;

3) virtuality, which provides the relative confidentiality of information about the offender's personality and the ability to influence the consciousness of a certain category of persons;

4) communicative, which makes possible the creation of criminal groups and increases the efficiency of existing organized crime;

5) imperfect provision of information security and legal protection of relations in cyberspace, which gives the offender the opportunity to avoid criminal responsibility for the crime.

Taking into account the technical and social component of such cyberspace content, it imposes a significant imprint on the mechanism of a criminal offense. In this aspect, cyberspace in criminalistics research can be considered as:

a) environment (situation), in which its separate elements (telecommunication network, computer system, etc.) could be used as an instrument for achieving an illegal purpose – violation of the normal functioning of this environment or seizure of intellectual property objects, payment facilities, material values;

b) the specific circumstances in which changes were made as a result of the offense (its traces);

The used cyberspace environment stipulates necessitates the use of updated methods, means and techniques for solving practical tasks for the investigation of such criminal activities to achieve a criminal result, having only dual technical and social factors.