УДК 343.98
DOI https://doi.org/10.32850/LB2414-4207.2021.21.19

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ І ТАКТИКИ ПРОВЕДЕННЯ ОБШУКУ КОМП'ЮТЕРНИХ ЗАСОБІВ

Курман Олександр Васильович,
кандидат юридичних наук,
доцент кафедри криміналістики
(Національний юридичний університет
імені Ярослава Мудрого,
м. Харків, Україна)

Статтю присвячено актуальним проблемам розроблення (вдосконалення) методик розслідування кримінальних правопорушень у сфері інформаційних технологій. Нині все більшого поширення набувають технології передачі інформації через телекомунікаційні мережі. Інформаційні технології використовуються у галузях медицини, у правоохоронній і судовій діяльності, в управлінні процесами виробництва продукції та надання послуг, зв'язку, у фінансовій і банківській сферах, електронній комерції, освіті тощо.

Поява нових перспектив і можливостей призвела до виникнення раніше невідомих викликів і загроз у сфері кібербезпеки та інформаційних технологій. З урахуванням зазначеного, питання розроблення нових та оновлення наявних криміналістичних методів розслідування злочинів у сфері інформаційних технологій є актуальними і такими, що потребують постійного дослідження. Одним із обов'язкових елементів структури будь-якої криміналістичної методики розслідування є перелік типових процесуальних дій, серед яких завжди виділяють обшук.

У представленій роботі аналізується процесуальна регламентація проведення таких процесуальних дій, як «обшук» та «зняття інформації з електронних інформаційних систем». Зазначено, що існують певні нормативні протиріччя у ст.ст. 168 та 236 КПК України у частині визначення комп'ютерних засобів та інших електронних пристроїв зв'язку як тимчасово вилученого майна. Здійснено порівняльний аналіз вітчизняного законодавства з аналогічними нормами у США і Німеччині у частині дистанційного обшуку. На підставі аналізу кримінального процесуального законодавства України і міжнародної Конвенції «Про кіберзлочинність» сформульовано висновок щодо наявних протиріч у частині регламентації проведення дистанційного обстеження електронних інформаційних систем або їхніх частин за відсутності дозволу суду.

Ключові слова: обшук, дистанційний обшук, дистанційне обстеження електронних інформаційних систем, кібербезпека, методика розслідування.

PROBLEM ISSUES OF LEGAL REGULATION AND TACTICS OF SEARCH OF COMPUTER TOOLS

Kurman Oleksandr Vasilievich,
Candidate of Legal Sciences,
Associate Professor
of the Criminalistics Department
(Yaroslav Mudryi National Law
University,
Kharkiv, Ukraine)

The article is devoted to topical issues of development (improvement) of methods of investigation of criminal offenses in the field of information technology. Today, technologies for transmitting information through telecommunications networks are becoming more widespread. Information technology is used in medicine, law enforcement and the judiciary, production and service management, communications, finance and banking, e-commerce, education and more.

The emergence of new perspectives and opportunities has led to previously unknown challenges and threats in the field of cybersecurity and information technology. In view of the above, the issues of developing new and updating existing forensic methods of investigating crimes in the field of information technology are relevant and require constant research. One of the obligatory elements of the structure of any forensic methods of investigating crimes is a list of typical procedural actions, among which a search is always.

The presented work analyzes the procedural regulation of such procedural actions as "search" and "obtaining information from electronic information systems." It is noted that there are certain normative contradictions in Art. 168 and 236 of the Criminal Procedure Code of Ukraine. These controversies relate to the definition of computer equipment and other electronic communications devices as temporarily seized property. Comparative analysis carried out of domestic legislation with similar norms of the United States and Germany in terms of remote search. Based on the analysis of the criminal procedure legislation of Ukraine and the International Convention on Cybercrime, a conclusion is formulated on the existing contradictions in the regulation of remote research of electronic information systems or their parts in the absence of court permission.

Key words: search, remote search, remote inspection of electronic information systems, cybersecurity, investigation methods.

Постановка проблеми. Нині в Україні все більшого поширення набувають технології передачі інформації через телекомунікаційні мережі. Підприємства, установи, організації, приватні особи користуються електронними пристроями і системами для роботи, навчання, розваг, спілкування. Інформаційні технології використовуються у галузях медицини, у правоохоронній і судовій діяльності, в управлінні процесами виробництва продукції і надання послуг, зв'язку, у фінансовій та банківській сферах, електронній комерції, освіті тощо. У нашій країні запущено онлайн-сервіс державних послуг «Дія» і проєкти електронної державної реєстрації речових прав на нерухоме майно та їхніх обтяжень; для юридичних і фізичних осіб (підприємців і громадських формувань) – е-Бізнес; для актів цивільного стану – е-ДРАЦС; для цифрової трансформації вищої, фахової передвищої і професійної (професійно-технічної) освіти – е-Університет; для системи управління запасами лікарських засобів і медичних виробів – створення/модернізація Державного реєстру лікарських засобів і Державного реєстру медичних виробів, розвиток застосування електронних рецептів.

Поява нових перспектив і можливостей призвела до виникнення раніше невідомих викликів і загроз у сфері кібербезпеки та інформаційних технологій. Йдеться про підвищення кількості кримінальних правопорушень, які вчиняються із використанням інформаційно-телекомунікаційних технологій.

Нині, маючи бажання і певні технічні та фінансові можливості, можна знайти, отримати інформацію (зокрема конфіденційну) майже про кожну людину або підприємство, установу, організацію та використати її для шантажу, погроз, впливу під час прийняття рішення державним посадовцем, суддею, прокурором, слідчим, громадським діячем тощо. Слід пам'ятати і про шахрайства у сфері надання послуг через мережу Інтернет і «кібертероризм», які набувають все більш загрозливих масштабів.

Не викликає сумнівів, що правоохоронна система має адекватно відображати зміст своєї діяльності щодо боротьби з високотехнологічними кримінальними правопорушеннями. Насамперед це стосується збирання слідів злочинної діяльності на електронних носіях інформації, у середовищі транспортних телекомунікаційних мереж та в електронних системах.

Аналіз останніх досліджень і публікацій. Нині проблематика процесуального порядку, криміналістичних способів отримання, фіксації, вилучення та оцінки інформації, яка міститься в електронних джерелах, постає як ніколи актуальною. Зокрема, свої праці у цьому напрямку криміналістичного дослідження присвятили такі науковці, як Л. В. Борисова [1], М. В. Дяченко [2], Г. А. Зацеркляний [3], Н. С. Козак [4], Д. О. Максимус [5], М.М. Менжега [6], О. І. Мотлях [7], М. В. Рудик [8], О. А.Федотов [9], М. Г. Щербаковський [10] та інші. Однак з урахуванням криміногенних тенденцій у сфері електронних інформаційних технологій, постійного розвитку технічних електронних (комп'ютерних) засобів, програмного забезпечення, прогалин і протиріч у законодавстві, що регулює цю сферу суспільних відносин, питання про розроблення нових та оновлення наявних криміналістичних методів розслідування злочинів у сфері інформаційних технологій є актуальними і такими, що потребують постійного дослідження.

Мета статті. Метою роботи є дослідження протиріч у правовому регулюванні процедури проведення обшуку комп'ютерних засобів і проблем тактики проведення зазначеної процесуальної дії, які виникають у цьому зв'язку.

Виклад основного матеріалу. Одним із обов'язкових елементів структури будь-якої криміналістичної методики розслідування є перелік типових процесуальних дій, серед яких завжди виділяють обшук. Процесуальна регламентація процедури проведення обшуку визначена ст.ст. 13, 223, 233–236 КПК України. Серед різних видів обшуків у криміналістичній літературі залежно від характеру об'єктів виділяють обшук комп'ютерних засобів [11, с. 371]. Враховуючи те, що під час вчинення кримінальних правопорушень у сфері інформаційних технологій переважна кількість слідів зосереджується у комп'ютерах, інших електронних технічних пристроях (планшетах, мобільних телефонах тощо), телекомунікаційних мережах, електронних системах, такий вид обшуку є дієвим інструментом виявлення джерел доказової та орієнтувальної інформації.

Чинне кримінально-процесуальне законодавство України серед загальних правил проведення такого виду обшуку виділяє певні особливості. Зокрема, ч. 7 ст. 236 КПК України дозволяється оглядати і вилучати документи, тимчасово вилучати речі, які мають значення для кримінального провадження. Вилучені речі і документи, які не входять до переліку, щодо якого прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку, та не відносяться до предметів, вилучених законом із обігу, вважаються тимчасово вилученим майном. Виникає питання: якщо в ухвалі

слідчого судді прямо надано дозвіл на відшукання комп'ютерної техніки, електронних пристроїв, які можуть містити сліди вчення злочинів, то чи відносяться вони до тимчасово вилученого майна? Адже ч. 2 ст. 168 КПК України вказує, що тимчасове вилучення електронних інформаційних систем або їхніх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюється лише у разі, якщо вони зазначені в ухвалі суду. Тобто ст. 236 КПК України визначає, що тимчасово вилученим майном можуть бути частини електронних інформаційних систем (наприклад комп'ютери), якщо вони прямо не зазначені в ухвалі слідчого судді, а ст. 168 КПК України вказує, що такі речі вважаються тимчасово вилученим майном, якщо прямо зазначені в ухвалі.

Законодавець установив перелік умов, за яких дозволяється, як виняток, вилучати інформаційні системи або їхні частини, мобільні термінали систем зв'язку. Зокрема, тимчасове вилучення можливе за наявності однієї із таких умов: 1) потрібно здійснити експертне дослідження електронної інформації, але воно неможливе без вивчення самого технічного пристрою; 2) такі об'єкти отримані внаслідок вчинення кримінального правопорушення; 3) технічні пристрої є засобом або знаряддям учинення кримінального правопорушення; 4) доступ до них обмежується їхнім власником, володарем або утримувачем; 5) доступ до них пов'язаний із подоланням системи логічного захисту. Водночас, установивши умови вилучення, законодавець не розтлумачив зміст деяких із них. Наприклад, що означає положення «доступ до інформаційних систем або їхніх частин, мобільних терміналів зв'язку обмежується власником, володарем або утримувачем»? Якщо власник роутера розташував його у шафі, яка знаходиться в окремій кімнаті квартири і двері до якої постійно зачинені, то чи можна це вважати обмеженням доступу і чи є це підставою для вилучення пристрою?

Нині у деяких країнах світу існує практика проведення дистанційного обшуку. Зокрема, у США може проводитися дистанційний доступ до комп'ютерів, інших технічних пристроїв для пошуку на електронних носіях інформації або її вилучення чи копіювання, яка зберігається в електронному вигляді [12]. Аргументацією необхідності таких обшуків є те, що злочинці все частіше приховують своє місце знаходження, використовуючи анонімайзери та мережу Tor. Отже, проникнення до комп'ютера підозрюваного є єдиною можливістю встановити його особу та зібрати докази [13].

Федеральна поліція Німеччини застосовує спеціальне програмне забезпечення для доступу і контролю за мобільними пристроями та комп'ютерами [14]. Зазначений правоохоронний орган Німеччини використовує троянський вірус для отримання інформації, яка зберігається на планшетах, смартфонах і комп'ютерах. Таке програмне забезпечення дозволяє відстежувати чати і розмови користувачів на їхніх пристроях ще до того, як вони будуть зашифровані такими месенджерами, як Telegram, WhatsApp тощо [15].

Законодавство України містить подібну норму щодо дистанційного обстеження інформаційних систем. У ст. 264 КПК України «Зняття інформації з електронних інформаційних систем» зазначається, що пошук, виявлення і фіксація відомостей, які містяться в електронній інформаційній системі або їхніх частинах, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володаря або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо існують відомості про наявність інформації в електронній інформаційній системі або її частині, яка має значення для певного досудового розслідування. Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володарем або утримувачем або не пов'язаний із подоланням системи

логічного захисту [16]. Якщо на своєму домашньому комп'ютері власник не встановив жодних обмежень у доступі через набрання на клавіатурі логіну і паролю, то чи може це вважатися відсутністю обмеження або необхідністю подолання системи логічного захисту?

У ст. 1 КПК України зазначено, що порядок кримінального провадження на території України визначається лише кримінальним процесуальним законодавством України. Кримінальне процесуальне законодавство України містить відповідні положення Конституції України, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, а також цього Кодексу та інших законів України. Ст. 9 КПК України визначає, що у разі, якщо норми цього Кодексу суперечать міжнародному договору, згода на обов'язковість якого надана Верховною Радою України, застосовуються положення відповідного міжнародного договору України. Парламент України у 2005 році прийняв Закон України «Про ратифікацію Конвенції про кіберзлочинність» [17]. У п. 1 ст. 19 Конвенції визначається, що кожна сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам для обшуку або подібного доступу до: a) комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній; b) комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані на її території. Зазначені норми суперечать положенням ст. 264 КПК України, де встановлено обов'язковість визначення в ухвалі слідчого судді ідентифікаційних ознак електронної інформаційної системи, до якої здійснюється доступ, адже згідно із п. 2 ст. 19 Конвенції, якщо під час доступу до конкретної комп'ютерної системи отримано інформацію, що дані, які розшукуються, зберігаються в іншій комп'ютерній системі чи її частині і до таких даних можна здійснити законний доступ із першої системи, або вони є доступними у першій системі, такі компетентні органи мають право терміново поширити обшук або подібний доступ на іншу систему.

Висновки. Отже, враховуючи те, що законодавство України є одним із видів джерел методик розслідування кримінальних правопорушень, врегулювання зазначених протиріч через внесення однозначних формулювань у відповідні статті КПК України або надання роз'яснень щодо тлумачення вказаних норм, практики їх застосування Верховним Судом допоможе розробити більш дієві та ефективні криміналістичні методики розслідування кримінальних правопорушень.

Список використаних джерел:

1. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : автореф. дис. ... канд. юрид. наук: 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2007. 19 с
2. Дяченко Н. М., Корнійко С. М., Княждвірський В. О. Особливості проведення огляду місця події при вчиненні комп'ютерних злочинів. Київ : Держ. наук.-дослід. експертно-криміналістич. центр МВС України. 2007. 42 с.
3. Зацеркляний Г. А. Виявлення слідів комп'ютерних інцидентів: навч. посіб. Харків : Панов А. М. 2017. 361 с.
4. Козак Н. С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : автореф. дис. ... канд. юрид. наук: 12.00.09 / Нац. ун-т держ. податк. служби України. Ірпінь, 2011. 20 с.
5. Максимус Д. О., Юхно О. О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій. Харків : НікаНова, 2013. 101 с.

6. Менжега М. М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: автореф. дис. ... канд. юрид. наук: 12.00.09 / Саратов: Б. и., 2005. 22 с.

7. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук: 12.00.09 / Київ : Б. в., 2005. 20 с.

8. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : автореф. дис. ... канд. юрид. наук: 12.00.08 / Одес. нац. юрид. акад. Одеса, 2007. 19 с.

9. Федотов О. А. Викриття злочинів у сфері комп'ютерних технологій як різновид боротьби з тероризмом : монографія. Львів : Львівська політехніка, 2014. 219 с.

10. Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків : ХНУВС, 2010. 109 с.

11. Криміналістика : підручник: у 2 т. Т. 1 / В. Ю. Шепітько та ін. Харків : Право, 2019. 456 с.

12. Federal Rules of Criminal Procedure 2021 Edition. Rule 41. Search and Seizure URL: https://www.federalrulesofcriminalprocedure.org/title-viii/rule-41-search-and-seizure/ (дата звернення: 15.09.2021).

13. Верховный суд США разрешил обыск компьютеров в любой юрисдикции. *Хабр*: URL: https://habr.com/ru/news/t/357064/ (дата звернення: 15.09.2021).

14. German federal police use Trojan virus to evade phone encryption. *DW*: 27.01.2018. URL: https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466 (дата звернення: 14.09.2021).

15. German government to use Trojan spyware to monitor citizens. *DW*: 22.02.2016. URL: https://www.dw.com/en/german-government-to-use-trojan-spyware-to-monitor-citizens/a-19066629 (дата звернення: 14.09.2021).

16. Кримінальний процесуальний кодекс України : Закон України від 13.04. 2012 р. № 4651-VI. *Законодавство України*: база даних / Верхов. Рада України. Дата оновлення: 08.08.2021. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n1654 (дата звернення: 14.09.2021).

17. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. N 2824-IV. *Законодавство України*: база даних / Верхов. Рада України. Дата оновлення: 21.09.2010. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n1654 (дата звернення: 14.09.2021).