8. Литвак О.М. Державний контроль за злочинністю: дис. на здобуття наук. ступеня канд. юрид. наук: спец.12.00.08. Харків, 2001. С. 6–10.

9. Побегайло А.Э. Семейное неблагополучие и несовершеннолетний преступник. Ставрополь, 2006. 154 с.

КУРМАН О. В.,
кандидат юридичних наук,
доцент кафедри криміналістики
(Національний юридичний університет імені Ярослава Мудрого)

УДК 343.98
DOI https://doi.org/10.32842/2078-3736-2019-4-45

ТАКТИЧНІ ТА ОРГАНІЗАЦІЙНІ ОСОБЛИВОСТІ ПОЧАТКУ ДОСУДОВОГО РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

У статті розглядаються проблемні питання тактичних та організаційних особливостей початку досудового розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Процес інформатизації суспільства розвивається дуже стрімко, що в свою чергу створює цілий ряд проблем. Серед них: забезпечення безпеки громадян, збереження конфіденційності персональних даних, захист комерційної та інших видів таємниць, втрата важливої інформації через технічні збої, протиправні посягання на електронні бази та інформаційні ресурси. Останні посідають одне з найважливіших місць у забезпеченні безпеки суспільства та країни.

У той же час практика не завжди може ефективно протидіяти зростаючим загрозам через низку причин, у тому числі через слабке методичне забезпечення процесу розслідування. З урахуванням стрімких змін у кримінальному середовищі та появи нових способів злочинних посягань, ситуація вимагає постійного вдосконалення та доопрацювання засобів вирішення зазначених проблем. Дослідження вказаних процесів із застосуванням криміналістичних підходів, дозволить удосконалити існуючі та розробити нові методики розслідування злочинів у сфері високих інформаційних технологій.

У законодавстві України відсутнє єдине визначення «несанкціонованого втручання в роботу». Виходячи з аналізу понятійного апарату, наведеного у чинному законодавстві, зроблено висновок, що несанкціоноване втручання в роботу – це порушення користувачем умов та правил отримання й обробки інформації.

Саме порушення умов та правил отримання й обробки інформації є однією із обставин, яку необхідно встановити слідчому. У роботі виділяються декілька типових слідчих ситуацій початку кримінального провадження, пропонуються рекомендації щодо тактики та організації проведення допиту заявника й огляду місця події.

Ключові слова: *кіберзлочинність, інформаційні технології, тактика розслідування, допит, огляд місця події.*

The article deals with the problematic issues of tactical and organizational peculiarities of the beginning of pre-trial investigation of unauthorized interference with the work of electronic computers (computers), automated systems, computer networks or telecommunication networks.

The process of informatization of society is developing very rapidly, which in turn creates a number of problems. It is the security of citizens, the preservation of confidentiality of personal data, protection of commercial and other types of secrets, loss of important information due to technical failures, illegal encroachment on electronic databases and information resources. The latter occupy one of the most important places in ensuring the security of society and the country.

At the same time, practice can not always effectively counteract growing threats for a variety of reasons, including due to poor methodological support for the investigation process. Given the rapid changes in the criminal environment, the emergence of new methods of criminal encroachment, the situation requires continuous improvement and refinement of these problems. Investigation of these processes, using forensic approaches, will allow to improve existing and develop new methods of investigation of crimes in the field of high-level information technologies.

Regarding the type of crime under consideration, it is determined that the legislation of Ukraine lacks the unequivocal definition of "unauthorized interference with work". Based on the analysis of the conceptual apparatus referred to in the legislation of Ukraine, it is concluded that unauthorized interference with work is a violation of the user's conditions and rules for receiving and processing information.

The violation of the conditions and rules for receiving and processing information is one of the circumstances that must be established by the investigator. Several typical investigative situations of criminal proceedings are distinguished in the work, and recommendations are given on the tactics and organization of interrogation the applicant and inspection of the place of the an incident.

Key words: *cybercrime, information technology, investigation tactics, interrogation, inspection of the place of the an incident.*

Вступ. Характерною ознакою сучасного світу стало масове й стрімке впровадження цифрових інформаційних технологій у різні сфери суспільної діяльності. Державне управління, медицина, наука, військова сфера, правоохоронна діяльність, товарне виробництво, зв'язок – все перейшло на електронний документообіг, цифрову обробку, збереження та використання інформації.

Сьогодні у світі нараховується 5,11 млрд мобільних користувачів, що на 100 млн більше, ніж у минулому. У 2019 році користувачів мережі Інтернет нараховувалось 4,39 млрд осіб, що на 366 млн більше, ніж у 2018 році. У соціальних мережах зареєстровано 3,48 млрд користувачів. У середньому один мільйон осіб кожного дня відкривають для себе глобальну мережу. В Україні порівняно з 2018 роком кількість осіб, які хоча б один раз скористалися можливостями Інтернету, зросла на 60% та становить 15325054 користувачів [2].

Бурхливий розвиток новітніх технологій разом із комфортом створює суспільству проблеми, пов'язані з виникненням нових видів злочинності. Одним із них є так звані кіберзлочини. Так, за даними Департаменту кіберполіції України у 2018 році було зареєстровано 6 000 злочинів у сфері високих інформаційних технологій: з них 680 у сфері протиправного контенту, 2 398 у сфері платіжних систем, 1 598 у сфері електронної комерції, 1 325 у сфері кібербезпеки [9].

Процес криміналізації сфери використання комп'ютерів, систем та комп'ютерних мереж носить системний характер. До чинників, які впливають на розповсюдження та зростання рівня злочинів, відносяться:

1. Суттєве збільшення обсягів інформації, що накопичується та зберігається в автоматизованих системах комп'ютерної обробки даних. Все більше видів інформації різного рівня конфіденційності та різної приналежності у сучасному суспільстві зберігається в електронному вигляді. Інформація про результати чужих прикладних і фундаментальних досліджень дає змогу заощадити власні сили й кошти та зосередити увагу на виробництві й маркетингу. Подальший розвиток науково-технічного прогресу і жорстка конкуренція роблять викрадення чужих таємниць особливо прибутковою, а тому дуже перспективною справою.

2. Подальше розширення масштабів та ускладнення технологій обробки інформації в комп'ютерах та електронних мережах.

3. Розширення кола осіб, які мають доступ до комп'ютерної техніки та зростає їх кваліфікація.

4. Недостатнє фінансування науки, відсутність держзамовлень для молодих фахівців призводить до витоку спеціалістів із державного сектору та від'їзду їх за кордон.

Також розповсюдженню злочинам сприяють наступні специфічні умови:

1. висока латентність злочинів, пов'язана зі складністю встановлення місця та часу вчинення злочину, а також особи, винної у його вчиненні;

2. наявність специфічної доказової бази, а саме електронних доказів, єдиний підхід до оцінки їх належності, допустимості, достовірності й достатності так і не вироблений чинним кримінально-процесуальним законодавством;

3. недостатній рівень підготовки правоохоронних органів щодо запобігання вчиненню, виявленню, розкриттю та розслідуванню зазначених видів злочинів [5].

Питанням протидії злочинам у сфері високих інформаційних технологій у вітчизняній криміналістичній літературі приділялася певна увага з акцентуванням на деякі проблеми у тактиці та методиці розслідування цих злочинних деліктів. Зокрема, зазначеній проблематиці у різні часи присвятили свої роботи такі вчені: В.О. Голубєв, М.А. Погорецький, О.І. Мотлях, Л.П. Паламарчук, Д.В. Пашнєв, І.Р. Шинкаренко, В.Ю. Шепітько, Н.В. Карчевський та інші. Однак з урахуванням стрімких змін у кримінальному середовищі й появи нових способів злочинних посягань, ситуація вимагає постійного вдосконалення та доопрацювання засобів вирішення зазначених проблем.

Постановка завдання. Метою статті є дослідження тактичних та організаційних особливостей проведення початкових слідчих (розшукових) дій при розслідуванні злочинних посягань на інформаційну безпеку країни за ст. 361 КК України.

Результати дослідження. У Кримінальному кодексі України (ст. 361) передбачено відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Обов'язковим елементом злочинного механізму цього виду злочинів є «несанкціоноване втручання в роботу». На жаль, законодавство України не дає однозначного визначення цієї категорії. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» наводиться дефініція поняття «несанкціоновані дії щодо інформації в системі», до яких відносяться такі, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Згідно зі ст. 1 зазначеного Закону доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі. Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила її обробки. Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних й програмних засобів. Виходячи з аналізу наведених категорій, можна зробити висновок, що несанкціоноване втручання в роботу – це порушення користувачем умов та правил отримання й обробки інформації [6, с. 129]. Відтак однією з обставин, яку

необхідно встановити слідчому на початковому етапі розслідування, є встановлення факту порушення умов та правил отримання й обробки інформації.

Як правило, первинну інформацію про можливу злочинну подію слідчий отримує із заяви власника інформації, уповноваженої ним особи чи законного користувача. Така сукупність фактичних та інших даних, що впливають на хід та стан розслідування, отримала назву слідчої ситуації.

У загальній проблемі слідчої ситуації розрізняють ситуації, що характеризують розслідування в цілому, і такі, що виникають при провадженні окремих слідчих (розшукових) дій [8, с. 20]. Стосовно виду злочинів, що розглядаються, може бути виокремлено декілька типових слідчих ситуацій початку кримінального провадження: 1) заявник самостійно виявив факт або ознаки злочину, особа злочинця невідома; 2) заявник самостійно виявив факт або ознаки злочину та надав певні відомості про можливого злочинця. Для перевірки інформації, що міститься у заяві, необхідно провести наступні початкові слідчі дії: 1) допит заявника та осіб, що вказані у заяві (по можливості в залежності від ситуації); 2) проведення огляду місця події. Подальший перелік слідчих (розшукових) дій залежатиме від результатів допиту та огляду.

Допит – одна із найбільш важливих слідчих дій. Визначаючи значення допиту в кримінальному судочинстві, треба виходити із наступних положень: допит – це найбільш розповсюджена слідча дія; допит – це дуже важливий спосіб отримання доказів у кримінальному провадженні; допит – це спосіб перевірки інших зібраних доказів [1, с. 239].

Особливістю допиту заявника є те, що у слідчого, як правило, немає достатнього часу для його підготовки, як рекомендують у підручниках із криміналістики. Однак у тактичному плані такий допит є дуже важливим, оскільки завдяки його проведенню слідчий отримує первинну інформацію, яка в подальшому впливає на планування розслідування, визначення первинних дій, обрання їх тактики.

Під час допиту заявника необхідно з'ясувати: 1) коли, як, за яких обставин було виявлено злочин; 2) які докази вчинення саме протиправних дій у нього наявні; 3) у чому полягає виток, втрата, підробка, блокування інформації або спотворення процесу її обробки; 4) на який саме вид інформації було вчинено посягання; 5) у чому важливість цієї інформації; 6) хто працював з цією інформацією на законних підставах; 7) який порядок доступу встановлено до такої інформації та чим він закріплений; 8) які системи захисту від несанкціонованого втручання встановлено так який алгоритм їх роботи; 9) чи були раніше позаштатні ситуації при роботі комп'ютерів чи електронних систем; 10) кому вигідно втручання в роботу комп'ютерів та кого могла цікавити інформація; 11) в яких протиправних цілях злочинці можуть використовувати інформацію або проблеми з її обробкою; 12) хто може вчинити цей злочин, хто може його замовити; 13) які є докази на підтвердження цих припущень; 14) які дії було здійснено власником інформації (уповноваженою ним особою), законними користувачами після виявлення кримінального правопорушення; 15) хто може бути свідками та яку корисну інформацію для слідства можуть повідомити ці особи.

Після допиту заявника та з'ясування первинної інформації доцільно проводити огляд місця події. Враховуючи специфіку розслідування злочинів у сфері високих інформаційних технологій, проведення огляду черговою слідчо-оперативної групою буде малоефективним через відсутність у керівника такої групи, як правило, необхідного досвіду та відповідних штатних спеціалістів. Професійних знань інспектора-криміналіста, який входить до складу такої групи, також може бути не достатньо. Враховуючи викладене, огляд доречно проводити слідчим, який спеціалізується на розслідуванні таких злочинів, із залученням співробітника кіберполіції та відповідних спеціалістів.

Основними цілями проведення огляду місця події є: 1) встановлення обставин події (способу, місця, часу вчинення злочину, особи злочинця, тощо) шляхом дослідження ознак злочину; 2) виявлення, фіксація, вилучення та оцінка слідів злочину (як традиційних криміналістичних, так і нетрадиційних – інформаційних електронних слідів); різних речових доказів; 3) отримання інформації, необхідної для побудов та перевірки слідчих версій і проведення розшукової роботи [10, с. 200].

Стадії огляду місця події доцільно розділити на два етапи: 1) огляд приміщення, де встановлено комп'ютер; 2) безпосередній огляд робочого місця та комп'ютера. Під час огляду необхідно враховувати, що злочинець може вдаватися до інсценування некримінальної події або вчинення іншого злочину.

Серед інсценувань при вчиненні злочинів у сфері комп'ютерної інформації найбільш розповсюджені наступні: 1) створення уявлення того, що файли було пошкоджено в результаті невмілого поводження з ними осіб, котрі мають доступ до них на законних підставах; 2) зараження комп'ютерним вірусом користувачем з необережності; 3) пошкодження носія інформації через причини, не пов'язані з роботою користувача (скачки електричної напруги в мережі тощо); 4) інсценування іншого злочину [7, с. 184-185].

Основними об'єктами, що підлягають огляду, є: 1) приміщення, де розташована комп'ютерна техніка; 2) окремі комп'ютери, які не підключені до мережі; 3) сервери; 4) периферійні телекомунікаційні пристрої; 5) магнітні та оптичні носії інформації; 6) роздруківки та записи; 7) технічна та інша документація [4, с. 43].

Огляд місця події має ряд особливостей. Специфіка слідчої дії вимагає залучення спеціалістів у сфері мережевих технологій, системам електрозв'язку, програмістів тощо. Застосування спеціальних знань при роботі з комп'ютерною технікою необхідне для: 1) визначення статусу об'єкта як машинних носіїв інформації, його стану, призначення і особливостей; 2) дослідження комп'ютерної інформації, включаючи її пошук та вилучення; 3) виявлення ознак і слідів впливу на машинні носії інформації та на саму інформацію; 4) здійснення допоміжних дій з виявлення, закріплення і вилучення доказів.

Спеціаліст у галузі комп'ютерних технологій може надати консультацію з приводу побудови комп'ютерної програми, її роботи, місцезнаходження інформації, яка цікавить слідчого, способах її вилучення із пам'яті електронного пристрою, проведення певних операцій за допомогою комп'ютера. Невміле поводження з комп'ютером може призвести до того, що необхідну інформацію не буде виявлено або взагалі буде знищено.

У той же час при залученні спеціаліста до участі в огляді місця події слідчому важливо переконатися у його компетентності. На практиці має місце велика кількість помилок через залучення некомпетентного спеціаліста, що викликало труднощі у проведенні слідчої дії (наприклад, в якості спеціаліста використовують побутового користувача ПК, який не володіє навичками роботи на великих обчислюваних комплексах) [3, с. 11].

Під час огляду місця події понятих слід залучати із осіб, не пов'язаних трудовими відносинами з власником комп'ютерної інформації або уповноваженою ним особою. Це пояснюється необхідністю збереження таємниці слідства, оскільки в іншому випадку поняті можуть виявитися причетними до витоку, втрати, підробки, блокування інформації та використати отримані відомості для протидії розслідуванню й свого захисту.

Висновки. Стрімкий процес інформатизації суспільства створює цілий ряд проблем, серед яких: забезпечення безпеки громадян, збереження конфіденційності персональних даних, захист комерційної та інших видів таємниць, втрата важливої інформації через технічні збої, протиправні посягання на електронні бази та інформаційні ресурси.

Останні займають одне з найважливіших місць у забезпеченні безпеки суспільства та країни. У той же час практика не завжди може ефективно протидіяти зростаючим загрозам через цілу низку причин, у тому числі через слабке методичне забезпечення процесу розслідування.

Застосування криміналістичних підходів дослідження зазначених процесів дозволить удосконалити існуючі та розробити нові методики розслідування злочинів у сфері високих інформаційних технологій.

Список використаних джерел:

1. Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы : моногр. М. : Юрлитинформ, 2015. 328 с.

2. Вся статистика интернета на 2019 год в мире. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (дата звернення: 10.07.2019).
3. Гаврилов М., Иванов А. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации. Законность. 2001. № 9. С. 11–16
4. Гаврилов М.В., Иванов А.Н. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации : учеб. пособ. Саратов : Изд-во Сарат. гос. акад. права, 2004. 136 с.
5. Карачевська Г.Р. Кіберзлочинність – правовий аспект. URL: http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_karachevska_cybercrime/ (дата звернення: 09.07.2019).
6. Курман О.В. Криміналістична характеристика несанкціонованого втручання у роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'зку. Наук. вісн. Херсон. держ. ун-ту. Серія «Юрид. науки». Вип. 4. Т. 2. 2017. С. 127–130.
7. Косынкин А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации : моногр. / под ред. Н.А. Подольного. М. : Юрлитинформ, 2013. 216 с.
8. Криміналістика: підруч. Т. 2 / за ред. В.Ю. Шепітка. Харків : Право, 2019. 328 с.
9. Підсумки 2018 року у цифрах. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення: 05.07.2019).
10. Расследование неправомерного доступа к компьютерной информации: учеб. пособ. / под ред. Н.Г. Шурухнова. М. : Моск. ун-т МВД России, 2004. 352 с.

ОРЖИНСЬКА Е. І.,
кандидат юридичних наук,
доцент кафедри професійних
та спеціальних дисциплін
*(Херсонський факультет
Одеського державного університету
внутрішніх справ)*

ЛИТВІН О. Я.,
слухач
*(Національний юридичний університет
імені Ярослава Мудрого)*

УДК 343.98.067.343
DOI https://doi.org/10.32842/2078-3736-2019-4-46

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ МЕТОДІВ У ПРОТИДІЇ КОНТРАБАНДІ НАРКОТИКІВ

Статтю присвячено дослідженню деяких спеціальних методів розкриття і розслідування контрабанди наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів.

Розкриття і розслідування контрабанди наркотиків, психотропних речовин, їх аналогів і прекурсорів супроводжується значними труднощами, які пов'язані