УДК 343.102/.148:343.982.9 doi: https://doi.org/10.33270/04202002.81

Черняховський Б. В. – ад'юнкт кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ, м. Київ
ORCID: https://orcid.org/0000-0002-7289-3034

Сучасні можливості судових експертиз у розслідуванні несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Метою *дослідження є висвітлення можливостей використання судових експертиз у кримінальних провадженнях щодо несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.* ***Методологія.*** *У статті застосовано емпіричні й теоретичні методи дослідження. Серед емпіричних методів використано опитування працівників оперативних підрозділів кіберполіції та судових експертів системи Міністерства внутрішніх справ, аналіз даних відкритої частини Єдиного державного реєстру судових рішень. З-поміж теоретичних методів застосовано аналіз і синтез, аналогію, порівняння, узагальнення.* ***Наукова новизна.*** *Запропоновано методологію дослідження слідової картини злочину, передбаченого ст. 361 Кримінального кодексу України, з використанням можливостей судово-експертних досліджень різних видів для фіксації та дослідження фізичних слідів злочину, а також призначення саме комплексної судової експертизи комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем та їх засобів. Обґрунтовано необхідність удосконалення нормативних актів відповідно до методики дослідження комп'ютерної техніки та програмних продуктів.* ***Висновки.*** *1. Результати судово-експертних досліджень є ключовим елементом доказової бази сторони обвинувачення в кримінальних провадженнях щодо несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. 2. Застосування спеціальних знань у досудовому розслідуванні кіберзлочинів є невід'ємною складовою для досягнення завдань кримінального провадження. 3. Нормативно-правове забезпечення судово-експертної діяльності для забезпечення потреб досудового розслідування потребує вдосконалення на підставі сучасних провідних методик проведення експертних досліджень.*

Ключові слова: комп'ютер; автоматизована система; комп'ютерна мережа; мережа електрозв'язку; несанкціоноване втручання в роботу комп'ютерів; кіберзлочини; судова експертиза.

Вступ

Активізація процесів інтеграції інформаційних технологій у суспільні відносини є одним із найвагоміших показників розширення можливостей самореалізації громадянина в правовому полі держави. Свідченням цього є стрімка інформатизація як приватного, так і публічного сектору громадського життя, оскільки більшість функцій підприємств, установ чи організацій здійснюють за допомогою комп'ютерів, комп'ютерних систем чи комп'ютерних мереж.

Розвиток інформаційних технологій розширює коло можливостей кіберзлочинності, забезпечує безпосередню можливість ефективного захисту від них. Нині функціонування інформаційних, комп'ютерних систем стає дедалі важливішим для належного функціонування держави. Тому несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж провокує та поглиблює суспільні кризові явища, послаблює імідж держави на світовій арені, негативно позначається на економічних процесах, перешкоджає налагодженню конструктивного діалогу між представниками державної влади та громадськістю, руйнує засади розбудови демократичної правової держави.

Жодна з інформаційних систем світу не мала й не має абсолютного імунітету від кібератак і стороннього втручання. Змінюються лише способи їх учинення та ставлення до таких інцидентів держави й суспільства.

У зв'язку із цим забезпечення ефективного та якісного розслідування злочинів у сфері інформаційних технологій, технічний аспект яких нині ще не є профільною основою в системі підготовки кадрів для органів досудового розслідування, потребує вивчення цих питань на поглибленому науковому рівні.

Досліджували деякі питання розслідування злочинів у сфері комп'ютерних технологій такі вчені-криміналісти: Т. В. Авер'янова, К. І. Бєляков, В. В. Бірюков, В. Б. Вєхов, В. В. Крилов, В. О. Мещєряков, І. Ю. Михайлов, О. І. Мотлях, О. В. Орлов, Ю. Ю. Орлов, О. Р. Россинська, М. В. Салтевський, В. Г. Хахановський, С. С. Чернявський та ін. Однак, з огляду на потреби слідчої практики та постійний гіперактивний розвиток комп'ютерних технологій, залишається актуальною потреба регулярного вдосконалення системи знань та навичок слідчих щодо особливостей роботи із цифровою інформацією під час кримінального провадження, зокрема щодо її

фіксації, вилучення та подальшого дослідження під час судових експертиз.

Мета і завдання дослідження

Метою статті є висвітлення можливостей використання судових експертиз у кримінальних провадженнях щодо несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Для досягнення мети дослідження необхідно виконати такі завдання:

– здійснити криміналістичну характеристику збирання доказів, зокрема в цифровій (електронній) формі, їх вилучення та дослідження в межах судово-експертних досліджень у розслідуванні несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– визначити сутність й особливості судово-експертного дослідження матеріальної та нематеріальної (цифрової) складових доказової бази, висвітлення методів комплексного пошуку та фіксації матеріальних (традиційних) та цифрових (електронних) доказів;

– на підставі аналізу наявної практики сформувати практичні рекомендації щодо оптимізації та підвищення якості дослідження слідової картини злочину, передбаченого ст. 361 КК України.

Виклад основного матеріалу

Протидія злочинам у сфері використання комп'ютерних технологій потребує активного впровадження та застосування комплексу новітніх способів, методів і засобів для результативного досудового розслідування. Одним із найпоширеніших злочинів у сфері інформаційних технологій є передбачене ст. 361 КК України несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Відповідно до статистичних даних Національної поліції України, за 2017 рік унаслідок масових кібератак комп'ютерного вірусу «PetyaA» на об'єкти української інфраструктури кількість зареєстрованих кримінальних правопорушень із зазначеною вище кваліфікацією становила 2186 проти 592 2016 року. Водночас показники зареєстрованих кримінальних правопорушень за ст. 361 КК України протягом останніх двох років залишаються на доволі високому рівні, з огляду на статистичні дані. Так, протягом одинадцяти місяців 2020 року було зареєстровано 1174 кримінальні правопорушення, що є співмірним 1289 кримінальним правопорушенням, зареєстрованим протягом 2019 року ("Opryliudnennia publichnoi informatsii", 2020).

За своїм змістом ст. 361 КК України передбачає несанкціоноване втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для несанкціонованого проникнення в ці машини, системи чи комп'ютерні мережі й здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації ("Kryminalnyi kodeks", 2001).

Фахівці у сфері інформатизації та зв'язку стверджують, що кібератаки зокрема, які підпадають під санкцію ст. 361 КК України, реалізують зловмисники для порушення конфіденційності, цілісності або доступності державних інформаційних ресурсів (чи приватних), що зберігають, обробляють і циркулюють у комп'ютерній/інформаційно-телекомунікаційній системі. Із цією метою використовують переважно вразливості таких систем, тобто їх нездатність протистояти реалізації певної загрози або сукупності загроз (Salnyk, Storchak, & Kramskyi, 2019, p. 122).

Для окреслення кола експертних досліджень, які дають змогу розкрити та довести факт злочину, передбаченого ст. 361 КК України, необхідно використовувати типові слідчі ситуації початкового етапу розслідування, а саме:

1) учинення злочину шляхом прямого (фізичного) доступу зловмисника до апаратної частини комп'ютера, підключення до комп'ютерної мережі через під'єднання на комутуючих шафах або дротових лініях, що здійснюють, зокрема, шляхом таємного проникнення до приміщення;

2) учинення злочину шляхом віддаленого доступу до комп'ютера, комп'ютерної чи автоматизованої системи через інші комп'ютери за допомогою телекомунікаційних чи бездротових мереж.

Висновки судових експертів у переважній кількості кримінальних проваджень та інших видах судочинства відіграють роль найважливіших доказів, без яких вирішити певну справу по суті майже неможливо (Kliuiev, 2019, p. 110).

Результативність розслідування, відповідно до зазначених слідчих ситуацій, передбачає призначення та проведення судових експертиз – досліджень на підставі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду ("Zakon Ukrainy", 1994), Залежно від конкретних обставин початкового етапу розслідування призначають і проводять трасологічні,

біологічні та головні в процесі доказування – комп'ютерно-технічні види судових експертиз.

Відповідно до зазначених слідчих ситуацій, для дослідження слідів незаконного доступу до апаратної частини комп'ютера, комп'ютерної мережі необхідно вивчити сліди злочинних дій, які залишилися на предметах, їхніх поверхнях, проаналізувати обстановку місця події: оглянути місця можливого підключення до дротових ліній, які ведуть до приміщення, стан підключень у комутуючих шафах, цілісність дверних замків, наявність слідів рук, взуття (ніг), інших частин тіла, волосся, запахових слідів у можливих місцях фізичного контакту злочинця з елементами обстановки тощо. Слід зосередити увагу на наявності таких слідів злочину, як: сліди рук (папілярні візерунки), сліди взуття (ніг), які залишив зловмисник під час здійснення доступу до комп'ютерного обладнання, або ж сліди злому замків, дверей, пломб на комутуючих шафах тощо.

Поділяючи думку О. М. Дуфенюка, зазначимо, що для методологічного забезпечення судово-експертної діяльності в кримінальному провадженні пріоритетним є, зокрема, алгоритмізація дій експерта, що дасть змогу з меншими затратами ресурсів і часу отримати більш точні й достовірні результати (Dufeniuk, 2019, p. 168).

Передусім встановлюють потребу проводити *трасологічну експертизу* виявлених слідів, що спрямована ідентифікувати або визначити родову (групову) належність індивідуально визначених об'єктів за матеріально фіксованими слідами, зокрема за відображеннями їхніх слідоутворювальних поверхонь; діагностувати властивості, стан об'єкта; установити механізм слідоутворення (ситуалогічні завдання) тощо.

Розглянемо завдання та можливості судових експертиз у кримінальних провадженнях про несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Предметом дослідження трасологічної експертизи під час розслідування злочину, передбаченого ст. 361 КК України, є дві основні групи слідів: 1) сліди людини (сліди рельєфу шкіряних покривів людини, слідів взуття, слідів одягу (рукавичок тощо); 2) сліди знарядь й інструментів (сліди злому, сліди на механічних замках, запірних і контрольних пристроях тощо).

Зазначений перелік не є вичерпним, це основа для криміналістичного пізнання ситуації слідчим, тому для виявлення інших слідів рекомендовано здійснювати огляд місця події із залученням спеціаліста-криміналіста, експерта.

Завдання *дактилоскопічної експертизи* полягає у встановленні тотожності особи за сукупністю загальних й окремих ознак, що відобразилися в сліді рук. Інструкція про призначення та проведення судових експертиз та експертних досліджень, затверджена наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5 (у редакції наказу Міністерства юстиції України від 26 грудня 2012 року № 1950/5) (далі – наказ Мін'юсту № 53/5), визначає типовий перелік питань, які ставлять для вирішення експерта: чи є на об'єкті сліди рук; чи придатні ці сліди для ідентифікації особи; чи залишені сліди рук конкретною (однією) особою; чи залишені однією особою сліди рук, вилучені в різних місцях; чи є на цьому предметі сліди рук, якщо так, то чи придатні вони для ідентифікації; які особливості мають руки людини, що залишила сліди (відсутність пальців, наявність шрамів тощо); унаслідок якої дії залишено слід (захоплення, торкання тощо); чи були сліди до вилучення на поверхні конкретного об'єкта; чи є ознаки перенесення вилучених слідів з однієї поверхні на іншу тощо ("Nakaz Ministerstva yustytsii", 1998).

У проаналізованій категорії кримінальних проваджень нерідко призначають *трасологічні експертизи для дослідження слідів взуття.* На вирішення цього експертного дослідження можуть ставити такі питання: чи є на цій поверхні (цьому предметі) сліди взуття та чи придатні ці сліди для ідентифікації взуття; чи залишені сліди взуттям, вилученим у певної особи; чи залишені одним і тим самим взуттям сліди, вилучені з різних місць; взуттям якого виду залишені ці сліди, які його характеристики, відмітні ознаки (розмір, ступінь зношеності тощо); який орієнтовно зріст людини, що залишила сліди тощо ("Nakaz Ministerstva yustytsii", 1998).

Діагностичне завдання такого дослідження надає також можливість встановити особливості пересування особи, розмір її взуття, орієнтовний зріст тощо. Для забезпечення об'єктивності дослідження слідчому обов'язково необхідно повідомляти експерта про факти носіння чи ремонту наданого на дослідження взуття після події злочину та до моменту призначення експертизи.

Експертне дослідження слідів злому дає змогу встановити конкретний екземпляр або вид (особливості) знаряддя злому, інструмента, агрегату за слідами його прямої дії. Цей вид трасологічної експертизи вирішує питання, пов'язані зі встановленням механізму (способу) злому, напрямку, у якому здійснювали злом перешкоди (із внутрішнього чи зовнішнього боку), типу (виду) виробу, що залишив слід, можливого способу його виготовлення тощо.

Для виконання цих завдань перед експертом ставлять такі питання: чи цим знаряддям (інструментом) було вчинено злом або іншу дію; знаряддям якого виду вчинено злом; яким способом розділено предмет (шляхом розрізування, розрубування, розпилювання,

свердління тощо); знаряддям якого виду розділено предмет; чи не залишено сліди злому, вилучені з різних місць подій, одним і тим самим знаряддям ("Nakaz Ministerstva yustytsii", 1998).

Для проведення цієї експертизи експерту переважно надають предмет зі слідами злому. Подеколи рекомендують надавати зліпки з об'ємних об'єктів.

Реалії практичної слідчої діяльності засвідчують, що в разі, якщо немає впевненості в тому, що вилучені знаряддя відповідають виявленим слідам злому, необхідно повідомити експерта й поставити питання щодо способу та можливих допоміжних елементів для вчиненого злому.

Окрема слідча ситуація, пов'язана з таємним проникненням до приміщення з комп'ютерним обладнанням, полягає в знеструмленні систем сигналізації, камер спостереження внаслідок блокування їх сигналу шляхом пошкодження кабелів.

У такому випадку *трасологічна експертиза кабелів та інструментів* надає можливість з'ясувати такі питання: яким способом розділено кабель (шляхом розрізування, розрубування, розпилювання, перекушення тощо); чи цим знаряддям (інструментом) було розділено кабель (досліджуваний торець кабелю зі слідом розділення); одним чи декількома інструментами було розділено кабель (досліджуваний торець кабелю зі слідом розділення); чи становили єдине ціле фрагменти кабелю, вилучені під час (окремих) оглядів місця події (дати процесуальних дій) ("Nakaz Ministerstva yustytsii", 1998).

Об'єктами експертизи замикальних і запобіжних (контрольних) пристроїв (засобів) є замки й інші замикальні пристрої, пломби, контрольні пристрої (засоби). Завдання цього дослідження полягає у встановленні факту та способу відмикання (злому) пристрою, виду предмета, застосованого для цього, його ідентифікації. У разі дослідження пломб можливою є ідентифікація пломбувальних лещат, факту переклеювання паперових контрольних засобів тощо. Під час дослідження замків експерту, за можливості, направляють відмички й інші предмети, які могли використовувати для відмикання або злому замка, а також усі ключі від цих замків.

Трасологічне дослідження замків надає відповіді на такі питання: чи в справному стані знаходиться наданий замок; яка причина несправності наданого замка; чи є на поверхнях наданого замка сліди сторонніх предметів; якщо так, то якими саме предметами (знаряддям) їх залишено; чи відмикали замок відмичкою, підібраним або підробленим ключем; чи можливо відімкнути замок наданим ключем (відмичкою); яким способом (здійснено злом наданого замка) відімкнено наданий замок; чи наданим знаряддям зламано замок тощо ("Nakaz Ministerstva yustytsii", 1998).

У межах *трасологічного дослідження пломб,* з огляду на слідчу ситуацію розслідування злочину, передбаченого ст. 361 КК України, необхідно визначити такі питання: чи була обтиснена пломба цими пломбувальними лещатами; чи одними пломбувальними лещатами були обтиснені пломби; чи розкривали й обтискували повторно пломбу після її обтиснення пломбувальними лещатами; у який спосіб і за допомогою якого знаряддя було розкрито й повторно обтиснено пломбу; чи можливо із цієї пломби витягти матеріал, що використовували для опломбування (дріт, шпагат, шнур), без порушення її цілісності; чи не розкривали пломбу наданим знаряддям ("Nakaz Ministerstva yustytsii", 1998).

Для встановлення факту розкриття пломби експертові необхідно, крім пломби, надати пломбувальні лещата, якими її повинні були пломбувати, або експериментальні пломби, обтиснені цими лещатами.

Слід ураховувати, що під час експертизи в процесі проведення експертних експериментів експерт може використовувати понад 10 необтиснених пломб, аналогічних досліджуваним, і таку саму кількість зразків матеріалів (дріт, шпагат, шнур), які використовували під час опломбовування.

Аналіз слідчої практики засвідчує, що в кримінальних провадженнях за ст. 361 КК України трапляються випадки, за яких пособники головних виконавців злочину здійснюють проникнення до приміщення (ст. 162 КК України) із комп'ютерною технікою або мережею в доволі примітивний спосіб – шляхом розбиття скла віконної рами, пластикових перегородок тощо. У таких випадках суб'єктам розслідування окремо слід зважати на можливості *трасологічної експертизи із встановлення цілого за частинами.*

Цей вид досліджень надає можливість встановити, чи мають частини предмета (знайдені уламки, шматки, осколки тощо) спільну лінію (поверхню) розділення, тобто чи становили вони раніше одне ціле. На вирішення експерту можуть ставити такі питання: чи становили знайдені частини єдине ціле; яким способом відокремлено від предмета його частину; до якого виду належить предмет, частину якого вилучено з місця події ("Nakaz Ministerstva yustytsii", 1998).

На експертизу надають усі знайдені частини, які раніше можливо становили один предмет.

Перелік вирішуваних судовими експертизами питань, визначених наказом Мін'юсту № 53/5, є орієнтовним і під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи

мереж електрозв'язку може потребувати уточнення чи коригування за рекомендаціями спеціаліста або експерта залежно від конкретних обставин справи.

Посилену увагу під час фіксації злочинних дій за ст. 361 КК України слід зосередити на можливостях експертизи біологічних слідів людини, які фіксують під час проведення слідчого огляду.

У зв'язку із цим під час розслідування злочину, передбаченого ст. 361 КК України, типовою є *судово-медична експертиза речових доказів*. Залежно від виду речових доказів біологічного походження судово-медичну експертизу здійснює окремий спеціалізований відділ бюро судово-медичних експертиз, відповідно до Правил проведення окремих видів експертиз, затверджених наказом МОЗ України від 17 січня 1995 року № 6 (далі – наказ МОЗ № 6) ("Nakaz Ministerstva", 1995).

З огляду на типові слідчі ситуації початкового етапу розслідування злочину, передбаченого ст. 361 КК України, до речових доказів біологічного походження належать: сліди крові, волосся, шкірний епітелій, слина, слізна рідина тощо.

Алгоритм дослідження зазначених речових доказів охоплює, зокрема, виявлення, опис, фотографування, вилучення і пакування слідів біологічного походження; встановлення наявності у вилучених експертних матеріалах крові, волосся, інших біологічних рідин і тканин (слини, слізної рідини тощо); встановлення видової, статевої, групової приналежності слідів (зокрема за ізосерологічними й імунними системами); виключення або встановлення приналежності слідів біологічного походження конкретній особі (значення молекулярно-генетичних методів) (Mishalov et al., 2018).

Дослідження слідів біологічного походження здійснюють відповідно до методології, затвердженої наказом МОЗ № 6. Переліку орієнтовних запитань, які ставлять на вирішення судово-медичної експертизи, на нормативному рівні не закріплено.

Однак результати співпраці слідчих і судово-медичних експертів під час розслідування злочинів дали змогу сформувати типові запитання, які ставлять на вирішення судово-медичної експертизи речових доказів.

Так, *судово-медична (імунологічна) експертиза слідів крові* під час розслідування злочину, передбаченого ст. 361 КК України, має дати відповіді на такі питання: чи є кров на об'єкті; яка група крові; людині якої статі вона належить; дорослій людині чи дитині вона належить; яке регіональне походження крові; яка давність плям крові; чи можливе походження крові від конкретної людини (Arseniuk et al., 2005, p. 480).

Аналізуючи слідчу практику, ми встановили, що непоодинокими є випадки вилучення та дослідження волосся, виявленого в місцях фізичного доступу до апаратної частини комп'ютерів чи серверів. Такі об'єкти надсилають для проведення *судово-медичної (цитологічної) експертизи.*

У відділеннях судово-медичної цитології проводять дослідження з метою встановлення в слідах і речових доказах наявності клітин тканин людини, визначаючи їх видову, групову, статеву й органо-тканинну приналежність.

Дослідження волосся здійснюють під час судово-медичної (цитологічної) експертизи, на вирішення якої ставлять такі питання: чи є наданий об'єкт волоссям; якщо так, то людині чи тварині воно належить; якщо так, то з якої частини тіла воно походить; якщо так, то чи є на ньому механічні пошкодження; якщо так, то який спосіб видалення волосся (випало, вирване, розірване); якщо так, то чи має волосся ознаки хімічної або термічної дії; чи наявні захворювання волосся; яка його статева й індивідуальна приналежність тощо.

Порівняльне цитологічне дослідження на підставі сумарних характеристик встановлює схожість чи несхожість волосся, а не його тотожність, оскільки волосини з голови однієї людини можуть різнитися, натомість волосся різних людей може мати однакові ознаки (Marchuk, 1997). З огляду на таку особливість, здійснюють комплекс досліджень, до якого належить один з варіантів *аналізу ДНК-поліморфізму*, що встановлює джерело походження волосся. Це дослідження має такі назви: *ДНК-експертиза, молекулярно-генетична* або *генотипоскопічна експертиза.* Результати молекулярно-генетичної експертизи змішаних біологічних слідів розмежовують їх та за індивідуальними ознаками визначають конкретних осіб, які їх залишили на наданому для дослідження предметі (Mishalov et al., 2018).

Вагоме значення для розслідування в кримінальному провадженні за ст. 361 КК України мають можливості застосування *експертизи комп'ютерної техніки і програмних продуктів* (у криміналістичній літературі поширенішою є назва «комп'ютерно-технічна експертиза») й *експертизи телекомунікаційних систем і засобів*. Проведення цих досліджень передбачене п. 13 та 14 наказу Мін'юсту № 53/5.

Під час аналізу наукових джерел встановлено підвиди експертизи комп'ютерної техніки та програмних продуктів: 1) апаратне дослідження (вивчення технічних засобів комп'ютера); 2) програмне дослідження (вивчення алгоритмів, які задіяні в пристрої та забезпечують його працездатність); 3) інформаційне дослідження (встановлення, аналіз файлів, якими оперує користувач, оцінювання функціональності даних, їх призначення, ідентифікація приналежності до роду операційної інформації). Завдання експертизи

комп'ютерної техніки та програмних продуктів полягають у: встановленні робочого стану комп'ютерно-технічних засобів; встановленні обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявленні інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установленні відповідності програмних продуктів певним версіям чи вимогам щодо його розроблення.

Експертиза телекомунікаційних систем і засобів сформувалася в процесі удосконалення та поглиблення методик комп'ютерно-технічних експертиз. Це відбулося внаслідок стрімкого розвитку видів і форм передання даних між окремими комп'ютерами. Масове підключення суспільства до глобальної мережі Інтернет, комунікаційні модулі Wi-Fi та Bluetooth визначили загальноприйнятну норму функціоналу комп'ютера. Потреба дослідження маршрутів і способів передання інформації сформували завдання для експертизи телекомунікаційних систем і засобів: визначення характеристик та параметрів телекомунікаційних систем і засобів; встановлення фактів та способів передання (отримання) інформації в телекомунікаційних системах; встановлення фактів і способів доступу до систем, ресурсів та інформації у сфері телекомунікацій; визначення якості надання телекомунікаційних послуг на рівні їх споживання; встановлення конфігурації та робочого стану телекомунікаційних систем і засобів; встановлення типу, марки, моделі й інших класифікаційних категорій телекомунікаційних систем та засобів; дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій ("Nakaz Ministerstva yustytsii", 1998).

Наказ Мін'юсту № 53/5 передбачає орієнтовний перелік питань, які ставлять для вирішення експертизою комп'ютерної техніки та програмних засобів: чи міститься на цьому носії інформація, яка цікавить слідчого, у якому вигляді; чи містить носій досліджуваного комп'ютера інформацію про певні дії користувача; чи проходив досліджуваний накопичувач певні процедури з метою знищення інформації; чи могла бути створена зазначена інформація на цьому комп'ютері, чи її перенесено з іншого носія; як інформацію перенесено на досліджуваний комп'ютер (носій); яка технологія та хронологія створення певного електронного документа; які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію, яка цікавить слідчого; чи містить накопичувач інформації досліджуваного комп'ютера певне програмне забезпечення; які функціональні несправності має це комп'ютерне обладнання або його окремі складові та пристрої, як ці несправності впливають на роботу обладнання загалом; чи можливо виконати певні дії за допомогою цього програмного продукту; чи можливо виконати певне завдання за допомогою цього програмного продукту; чи реалізовано в цьому програмному продукті (програмному коді) функції, передбачені технічним завданням на його розроблення ("Nakaz Ministerstva yustytsii", 1998).

Під час проведення експертизи телекомунікаційних систем і засобів об'єктом дослідження є телекомунікаційні системи, засоби, мережі та їх складові, інформація, яку ними передають, приймають та опрацьовують. Експертиза вирішує такі питання: які тип, марка, модель телекомунікаційного засобу (системи); чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт); які характеристики підключень до мережі має телекомунікаційний засіб; чи змінював користувач телекомунікаційної мережі налаштування окремих пристроїв, у який час, які їх значення; який загальний характер підключень до телекомунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб); за допомогою яких програмних засобів здійснювали підключення до телекомунікаційної мережі; яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему; чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації; які технічні характеристики (параметри) має телекомунікаційний засіб (система); чи наявний факт доступу до телекомунікаційної системи та в який спосіб; чи виявлено використання ресурсів та інформації в телекомунікаційній системі, у який спосіб; чи наявний факт передання (отримання) інформації в телекомунікаційній системі та в який спосіб; чи є ознаки втручання в роботу телекомунікаційної системи; чи могли апаратні засоби об'єднуватися в телекомунікаційну мережу та за якими ознаками; які шляхи маршрутизації даних у телекомунікаційній системі тощо ("Nakaz Ministerstva yustytsii", 1998).

Запропонований перелік є орієнтовним, тому залежно від обставин розслідуваного злочину питання необхідно коригувати, конкретизувати й доповнювати, ураховуючи консультативну допомогу спеціаліста чи експерта, який проводитиме експертизу. На думку О. В. Яковлева, недопустимим з процесуальної позиції є формулювання для експерта надто загальних питань, наприклад: «Чи придатний для дослідження наданий об'єкт?», оскільки навіть у межах одного виду експертизи дослідження можуть бути ідентифікаційні, класифікаційні, діагностичні, ситуаційні. Процесуальні крайнощі спричиняє питання: «чи містить наданий на дослідження накопичувач на жорсткому магнітному диску інформацію, що стосується кримінального провадження?», оскільки експерт не може знати, яка інформація стосується досудового розслідування (Yakovliev, 2019, p. 354).

Наявність конкуренції між недержавними експертними установами, що проводять такі види досліджень, позитивно позначається на розвитку та професійному вдосконаленні фахівців з експертних досліджень комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем та їх засобів. Це сприяє розширенню можливостей комп'ютерно-технічних експертиз, зокрема переліку питань, які вона вирішує.

Вивчення слідчої та експертної практики, аналіз наукових джерел засвідчили, що на вирішення комп'ютерно-технічних експертиз ставлять й інші, не передбачені наказом Мін'юсту № 53/5, питання, які успішно вирішують експерти, наприклад: чи міститься (містилася) на наданому на дослідження носії інформація, що має ключові слова «...»; чи містилися на наданому на дослідження носії файли, що були згодом знищені; якщо так, то які саме файли та який їх зміст; з якого з наданих на дослідження комп'ютерів здійснювали вихід у мережу Інтернет, за якими адресами, у який період часу; чи наявні на досліджуваному комп'ютері програмні продукти, призначені для злому пароля та несанкціонованого доступу до комп'ютерних систем; чи можливе виконання певного завдання за допомогою програмного продукту (зазначають якого); яким є рівень професійної підготовки в галузі програмування і роботи з комп'ютерною технікою особи, яка виконала певні дії з комп'ютером і програмним забезпеченням; чи відповідає стиль програмування досліджуваного програмного продукту стилю програмування певної особи; чи відповідають прийоми та засоби програмування, що застосовували під час створення досліджуваного програмного продукту, прийомам і засобам, якими користується певна особа (Boichenko et al., 2015).

Поряд з основними завданнями комплексної судової експертизи комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем та їх засобів можливо вирішити питання допоміжного характеру щодо рівня професійної підготовки окремих осіб у галузі програмування та роботи із засобами комп'ютерної техніки. Наприклад, ідентифікація користувача за допомогою клавіатурного почерку (за швидкістю набору символів, звичкою використовувати основну чи допоміжну частини клавіатури, особливостями «подвійних», «потрійних» натискань на клавіші, улюбленими прийомами управління комп'ютером. Ідентифікація клавіатурного почерку полягає у виборі відповідного еталону зі списку збережених у пам'яті комп'ютера еталонів, на підставі оцінювання схожості до цього еталона параметрів почерку одного з користувачів, які мають право на роботу з цим комп'ютером (Borysova, Bilenchuk, & Malii, 2020, p. 235).

Доцільність призначення в кримінальному провадженні за ст. 361 КК України саме комплексної судової експертизи комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем та їх засобів у відповідних випадках обґрунтована й наявністю у Реєстрі методик проведення судових експертиз Мін'юсту відповідної методики цього виду експертного дослідження. Водночас цей реєстр не містить окремо визначеної методики проведення дослідження телекомунікаційних систем (обладнання) і засобів, на відміну від методики дослідження комп'ютерної техніки та програмних продуктів ("Reiestr metodyk", 2020).

Наукова новизна

Наукова новизна дослідження сформована результатами аналізу проблематики й особливостей фіксації слідової картини злочину в розслідуванні несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, об'єктом посягання є інформація, яку зберігають у комп'ютері, на певному носії, та/або програмне забезпечення. Розглянуто комплекс заходів фіксації та роботи з матеріальними слідами злочину на апаратній складовій комп'ютерної техніки, а також з інформацією, яку зберігають на їх носіях і яка становить інтерес для досудового розслідування. Виокремлено особливості використання можливостей судово-експертних досліджень під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, об'єктом посягання є інформація, яку зберігають у комп'ютері, на певному носії, та/або програмне забезпечення. Аргументовано доцільність урахування положень методики дослідження комп'ютерної техніки та програмних продуктів, поєднаних із положеннями реєстру методик, визначених Мін'юстом. У таких випадках органам досудового розслідування слід дотримуватися вимог чинних нормативно-правових і розпорядчих (відомчих) актів України, звертатися до слідчого судді з клопотанням про призначення комплексної судової експертизи комп'ютерної техніки та програмних продуктів, експертизи телекомунікаційних систем і засобів. Такий висновок експерта відповідатиме положенням кримінального процесуального законодавства України, а також п. 13 та 14 наказу Мін'юсту № 53/5. Задля ілюстрування такої позиції розглянуто приклади зберігання чи навіть приховування інформації, яка становить інтерес для досудового розслідування, на жорстких дисках комп'ютерів, що зумовлює

дослідження комп'ютера або комп'ютерної мережі як середовища, у якому здійснено несанкціонований виток, втрату, підроблення, блокування інформації, спотворено процес її обробки або порушено встановлений порядок її маршрутизації.

Висновки

Досудове розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, з огляду на специфіку злочину та способи його вчинення, потребує спеціальної підготовки слідчого, наявності в нього відповідних криміналістичних знань, а також умінь і навичок. Тому вивчення можливостей таких експертиз, як трасологічної, дактилоскопічної, судово-медичної експертизи речових доказів, молекулярно-генетичної, експертизи комп'ютерної техніки та програмних продуктів, експертизи телекомунікаційних систем і засобів, є важливим під час розслідування різних виявів кіберзлочинності в Україні.

REFERENCES

Arseniuk, T.M., Beliak, Yu.M., & Boiarov, V.I. (et al.). (2005). *Ekspertyzy u sudovii praktytsi [Examinations in judicial practice].* V.H. Honcharenko (Eds.). Kyiv: Yurinkom Inter [in Ukrainian].

Boichenko, S.B., Boiarov, V.I., & Budko, T.V. (et al.). (2015). *Ekspertyzy v sudochynstvi Ukrainy [Expertise in the judicial process of Ukraine].* Kyiv: Yurinkom Inter [in Ukrainian].

Borysova, L.V., Bilenchuk, P.D., & Malii, M.I. (2020). Ekspertyza yak zasib ustanovlennia faktiv i obstavyn vchynennia transnatsionalnykh kompiuternykh zlochyniv [Examination as a means of establishing the facts and circumstances of committing transnational computer crimes]. *Kryminalistyka i sudova ekspertyza, Forensics and forensics, 65,* 230-239. doi: https://doi.org/10.33994/kndise.2020.65.23 [in Ukrainian].

Dufeniuk, O.M. (2019). Zabezpechennia sudovo-ekspertnoi diialnosti u kryminalnomu provadzhenni: systemna paradyhma [Ensuring forensic activity in criminal proceedings: a systemic paradigm]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu, Bulletin of Lviv University of Trade and Economics, 8,* 163-173. doi: https://doi.org/10.36477/2616-7611-2019-08-1 [in Ukrainian].

Kliuiev, O.M. (2019). Udoskonalennia ekspertnoho zabezpechennia pravosuddia: teoretychni, pravovi ta orhanizatsiini aspekty [Improving the expert support of justice: theoretical, legal and organizational aspects]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky, Theory and practice of forensic science and criminology, 19,* 102-117. https://doi.org/10.32353/khrife. 1.2019.08 [in Ukrainian].

Kryminalnyi kodeks Ukrainy : vid 5 kvit. 2001 r. No. 2341-III [Criminal Code of Ukraine from April 5, 2001, No 2341-III]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].

Marchuk, A.I. (1997). *Sudova medytsyna [Forensic Medicine].* Kyiv: Heneza. Retrieved from http://textbooks.net.ua/content/view/4812/38 [in Ukrainian].

Mishalov, V.D., Khokholieva, T.V., & Bachynskyi, V.T. (et al.). (2018). *Sudova medytsyna [Forensic Medicine].* Chernivtsi: Misto [in Ukrainian].

Nakaz Ministerstva okhorony zdorovia Ukrainy "Instruktsiia pro provedennia sudovo-medychnoi ekspertyzy": vid 17 sich. 1995 r. No. 6 [Order of the Ministry of Health of Ukraine "Instructions for forensic examination" from January 17, 1995, No. 6]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/z0254-95 [in Ukrainian].

Nakaz Ministerstva yustytsii Ukrainy "Instruktsiia pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen": vid 8 zhovt. 1998 r. No. 53/5 [Order of the Ministry of Justice of Ukraine "Instructions on the appointment and conduct of forensic examinations and expert studies" from October 8, 1998, No. 53/5]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/z0001-13#Text [in Ukrainian].

Opryliudnennia publichnoi informatsii [Disclosure of public information]. *Sait Natsionalna politsiia", Site "National Police".* Retrieved from https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html [in Ukrainian].

Reiestr metodyk provedennia sudovykh ekspertyz [Register of methods of forensic examinations]. *Sait "Ministerstvo yustytsii Ukrainy", Site "Ministry of Justice of Ukraine".* Retrieved from http://rmpse.minjust.gov.ua [in Ukrainian].

Salnyk, S.V., Storchak, A.S., & Kramskyi, A.Ye. (2019). Analiz vrazlyvostei ta atak na derzhavni informatsiini resursy, shcho obrobliaiutsia v informatsiino-telekomunikatsiinykh systemakh [Analysis of vulnerabilities and attacks on state information resources processed in information and telecommunication systems]. *Systemy obrobky informatsii, Information processing systems, 2(157),* 121-128. doi: https://doi.org/10.30748/soi.2019.157.17 [in Ukrainian].

Yakovliev, O.V. (2019). Rol prokurora - protsesualnoho kerivnyka dosudovym rozsliduvanniam u pryznachenni sudovoi ekspertyzy ta otsintsi yii rezultativ [The role of the prosecutor - procedural manager of the pre-trial investigation in the appointment of forensic examination and evaluation of its results]. *Kryminalistyka i sudova ekspertyza, Forensics and forensics, 64,* 350-360. doi: https://doi.org/10.33994/kndise.2019.64.30 [in Ukrainian].

Zakon Ukrainy "Pro sudovu ekspertyzu": vid 25 liut. 1994 r. No. 4038-XII [Law of Ukraine "About forensic examination" from February 25, 1994, No. 4038-XII]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/4038-12 [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Експертизи у судовій практиці : бюлетень / [Т. М. Арсенюк, Ю. М. Беляк, В. І. Бояров та ін.] ; за заг. ред. В. Г. Гончаренка. Київ : Юрінком Інтер, 2005. 480 с.

Експертизи в судочинстві України : наук.-практ. посіб. / [С. Б. Бойченко, В. І. Бояров, Т. В. Будко та ін.]. Київ : Юрінком Інтер, 2015. 504 с.

Борисова Л. В., Біленчук П. Д., Малій М. І. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. *Криміналістика і судова експертиза.* 2020. № 65. С. 230–239. doi: https://doi.org/10.33994/kndise.2020.65.23.

Дуфенюк О. М. Забезпечення судово-експертної діяльності у кримінальному провадженні: системна парадигма. *Вісник Львівського торговельно-економічного університету.* 2019. №8. С. 163–173. (Серія «Юридичні науки»). doi: https://doi.org/10.36477/2616-7611-2019-08-1.

Клюєв О. М. Удосконалення експертного забезпечення правосуддя: теоретичні, правові та організаційні аспекти. *Теорія та практика судової експертизи і криміналістики.* 2019. № 19. С. 102–117. doi: https://doi.org/10.32353/khrife. 1.2019.08.

Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

Марчук А. І. Судова медицина : курс лекцій. Київ : Генеза, 1997. 143 с. URL: http://textbooks.net.ua/content/view/4812/38.

Судова медицина : підручник / [В. Д. Мішалов, Т. В. Хохолєва, В. Т. Бачинський та ін.]. Чернівці : Місто, 2018. 575 с.

Інструкція про проведення судово-медичної експертизи : наказ Міністерства охорони здоров'я України від 17 січ. 1995 р. № 6. URL: https://zakon.rada.gov.ua/laws/show/z0254-95.

Інструкція про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0001-13#Text.

Оприлюднення публічної інформації. *Національна поліція :* [сайт]. URL: https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html.

Реєстр методик проведення судових експертиз. *Міністерство юстиції України :* [сайт]. URL: http://rmpse.minjust.gov.ua.

Сальник С. В., Сторчак А. С., Крамський А. Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційно-телекомунікаційних системах. *Системи обробки інформації.* 2019. № 2 (157). С. 121–128. doi: https://doi.org/10.30748/soi.2019.157.17.

Яковлєв О. В. Роль прокурора – процесуального керівника досудовим розслідуванням у призначенні судової експертизи та оцінці її результатів. *Криміналістика і судова експертиза.* 2019. № 64. С. 350–360. doi: https://doi.org/10.33994/kndise.2019.64.30.

Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12.

Стаття надійшла до редколегії 03.07.2020

Cherniakhovskyi B. – Postgraduate Student of the Department of Forensic Support and Forensic Science of the Educational and Research Institute No. 2 of the National Academy of Internal Affairs, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-7289-3034

Modern Possibilities of Forensic Examinations in the Investigation of Unauthorized Interference in the Work of Computers, Automated Systems, Computer Networks or Telecommunication Networks

*The **purpose** of the study is to highlight the possibilities of using forensic science in criminal proceedings for unauthorized interference in the work of computers, automated systems, computer networks or telecommunications networks. **Methodology.** The article uses empirical and theoretical research methods. Among the empirical methods used surveys of employees of operational units of cyberpolice and forensic experts of the Ministry of Internal Affairs, analysis of data from the open part of the Unified State Register of Judgments. Theoretical methods were analysis and synthesis, analogy, comparison, generalization. **Scientific novelty.** The methodology of research of a trace picture of a crime provided by Art. 361 of the Criminal Code of Ukraine using the possibilities of forensic research of various kinds to record and study the physical traces of the crime, as well as the appointment of a comprehensive forensic examination of computers, software, telecommunications systems and their tools. The necessity of improvement of normative acts taking into account the methods of research of computer equipment and software products is substantiated. **Conclusions.** 1. The results of forensic research are a key element of the evidence base of the prosecution in criminal proceedings for unauthorized interference with computers, automated systems, computer networks or telecommunications networks. 2. The use of specialized knowledge in the pre-trial investigation of cybercrime is an integral part of achieving the objectives of criminal proceedings. 3. Regulatory and legal support of forensic activities to meet the needs of pre-trial investigation needs to be improved taking into account modern leading methods of expert research.*

Keywords: computer; automated system; computer network; telecommunication network4 unauthorized interference with computers; cybercrime; forensic examination.