DOI: 10.33994/kndise.2024.69.02
УДК 343.98: 351.746.1

Ірина Віталіївна Гора
Докторка юридичних наук, професорка, провідна наукова співробітниця науково-організаційного центру Національної академії Служби безпеки України
ORCID: 0000-0003-2940-5338, e-mail: irvitgora@ukr.net

Валерій Аркадійович Колесник
Доктор юридичних наук, професор, головний науковий співробітник науково-організаційного центру Національної академії Служби безпеки України
ORCID: 0000-0003-3570-8984, e-mail: kovaleriy@u*kr.net*

Актуальні питання криміналістичного забезпечення досудового розслідування злочинів проти інформаційної безпеки держави

Стаття присвячена розгляду проблемних питань криміналістичного забезпечення досудового розслідування злочинів проти інформаційної безпеки держави. Доведено, що поява інформаційних технологій визначила мультиплікативний характер їх інтеграції у криміналістичну діяльність. Це викликає зміни в усіх сферах криміналістичного знання, в загальній теорії, в криміналістичній техніці, тактиці, методиці розслідування окремих видів злочинів.

Ключові слова: *інформаційна безпека; досудове розслідування; криміналістика; криміналістичне забезпечення; експертні дослідження; судові експертизи; слідчі та негласні слідчі дії.*

Постановка проблеми. Особливості сучасних загроз у світі, пов'язаних з відкритою військовою агресією росії проти нашої держави, суттєво впливають на стан національної безпеки як України, так і країн ЄС загалом. Захист національних інтересів потребує не розширення життєвого простору держави, а усунення іноземного впливу на внутрішню й зовнішню політику, забезпечення недоторканності державних кордонів й захищення власної ідеологічної основи та соціального добробуту населення. У результаті світових процесів глобалізації виникла

нова група загроз, серед яких найбільш значущими є встановлення глобального контролю над державними й всесвітніми інформаційними мережами, розповсюдження масової неконтрольованої і нелегальної міграції, поява й розповсюдження міжнародного тероризму та ін. Протягом останніх років в умовах інформаційної та військової агресії рф проти України забезпечення державної безпеки країни багато в чому залежить від системної протидії новітнім загрозам. Нарощування країною-агресором розвідувально-підривної, терористичної та іншої протиправної діяльності щодо України, ведення агресивної війни проти нашої держави, у тому числі й інформаційної, покладає сьогодні на органи й підрозділи СБ України актуальні завдання забезпечення інформаційної безпеки держави. При цьому необхідно враховувати, що з огляду на динаміку розвитку інформаційного суспільства та злочинного інструментарію, який використовується зловмисниками у цій сфері, СБ України постійно стикається з новими викликами, вирішення яких залежить як від компетентності її співробітників, такі і відповідних кроків законодавця у контексті створення реальних механізмів функціонування адекватних засобів протидії існуючим загрозам.

Зростання кількості кримінальних діянь, зумовлених уразливістю інформаційної сфери держави, особливий характер суспільно небезпечних наслідків злочинів цього виду, необхідність виявлення сутності таких злочинів з метою встановлення внутрішніх зв'язків між елементами криміналістичної структури цього виду кримінально караних діянь та їх пізнанням, складність процесу їх виявлення й досудового розслідування в силу недостатності конкретних рекомендацій з проведення слідчих та негласних слідчих (розшукових) дій, використання спеціальних знань тощо визначили актуальність даної статті.

Аналіз останніх досліджень і публікацій. Питання захисту інформації від неправомірного втручання та її протиправного використання, інформаційної безпеки держави, виявлення й досудового розслідування злочинів в інформаційній сфері, що посягають на основи національної безпеки України та завдають шкоди державі, об'єктами посягання або засобами вчинення яких виступають інформаційні, цифрові, комп'ютерні засоби і технології тощо, досліджували відомі фахівці в галузі криміналістики, кримінального права й процесу, криміналістики, теорії судової експертизи, оперативно-розшукової та контррозвідувальної діяльності. Цим питанням приділяли свою увагу багато відомих вітчизняних вчених і практиків, зокрема: О. Балинська, Р. Благута, В. Вєртузаєв, В. Гавловський, Ю. Гаврилін, В. Голубєв, В. Горбулін, І. Гриненко, К. Захаренко, М. Карчевський, Б. Кормич, В. Ліпкан, Ю. Нізовцев, Ю. Орлов, В. Пилипчук, Д. Прокоф'єва-Янчиленко, А. Скрипник, О. Стрільців, О. Тарасенко, Б. Теплицький, А. Усов, В. Хахановський, В. Ходанович, С. Чернявський, А. Черняк, О. Юдін та інші дослідники зазначених проблем. Аналіз висловлених наукових точок зору вказує на те, що сьогодні в Україні започатковано важливі кроки з розв'язання проблем протидії злочинам

у сфері інформаційної безпеки держави. Це дало змогу виокремити питомі напрями розвитку теоретико-правових поглядів на проблему злочинності в інформаційній сфері, зокрема: розроблення поняття та розкриття сутності таких злочинів; удосконалення кримінально-правових засобів боротьби з ними; дослідження криміналістичних аспектів протидії зазначеним кримінальним діянням.

Мета дослідження. Метою статті є дослідження можливостей криміналістичної науки у виявленні й досудовому розслідуванні злочинів, що посягають на інформаційну безпеку держави.

Викладення основного матеріалу. Загрози державній безпеці та національним інтересам — це об'єктивні фактори, які не залежать загалом від волі держави, але вона має на них впливати та ураховувати їх у своїй життєдіяльності. Такі загрози можуть мати різні види та ступінь значущості, внаслідок чого вони не становлять єдину й постійну сукупність. Окремого значення набувають злочини в інформаційній сфері, вчинення яких зумовлене використанням зловмисниками віртуального середовища й всесвітньої мережі Інтернет. Два останні роки поспіль СБ України має справу із активізацією розвідувально-підривної діяльності спецслужб іноземних держав, насамперед рф, у кіберпросторі з активним використанням сучасних інформаційних технологій у війні проти нашої держави й фінансуванням терористичних угруповань, з інформаційними кібератаками на вищі державні органи, військові формування та об'єкти критичної інфраструктури тощо. Водночас доводиться констатувати й появу нових загроз у сфері державної безпеки. Це, насамперед, повномасштабне проведення спеціальних інформаційних та інформаційно-психологічних операцій, інших заходів, спрямованих на дискредитацію української влади, заперечення агресивної сутності дій супротивника й втягнення населення тимчасово окупованих територій до колабораційної діяльності, активне залучення з числа місцевих жителів джерел інформації, які використовуються окупантами для отримання відомостей про місця розташування й маршрути пересування наших військових, рятувальних загонів і техніки, гуманітарні коридори та ін.

До підслідності слідчих СБ України віднесено значний перелік тяжких кримінальних правопорушень. Йдеться про злочини, які можуть завдати великої шкоди державній і національній безпеці. Це, зокрема, розслідування шпигунства, державної зради, колабораційної діяльності, посягання на конституційний лад і територіальну цілісність України, воєнних злочинів, розголошення державної таємниці, злочинів терористичного характеру тощо. На слідчих цього правоохоронного відомства покладається водночас велика відповідальність за розслідування багатьох інформаційних злочинів.

Криміналістика як прикладна наука гостро реагує на усі потреби практики, що пов'язані не лише із боротьбою зі злочинністю, а й з іншими викликами сучасності і має сприяти своїми методами й засобами

вирішенню проблем, пов'язаних із забезпеченням державної безпеки, у тому числі й в інформаційній сфері. Сучасна криміналістика має величезний арсенал технічних, тактичних та методичних засобів для виявлення й розслідування кримінальних правопорушень. Водночас, на нашу думку, сьогодні особливо витребуваними стають основи використання методів і засобів криміналістики, функція яких є суто запобіжною. Тому окремим напрямом криміналістичного забезпечення протидії злочинам у сфері інформаційної безпеки держави має стати озброєння контррозвідувальних підрозділів з кібербезпеки відповідними криміналістичними розробками. Адже ефективність пошуково-пізнавальної діяльності цих суб'єктів запобігання інформаційним злочинам багато в чому визначається наявним у них арсеналом криміналістичних засобів. Водночас особливістю досудового розслідування найбільш небезпечних інформаційних злочинів є те, що здебільшого кримінальні провадження за ними розпочинаються за матеріалами контррозвідувальної та оперативно-розшукової діяльності.

Зміст досудового розслідування більшості злочинів проти інформаційної безпеки держави фактично визначається чотирма основними видами діяльності, котрі працівники правоохоронних органів можуть здійснювати як одночасно, так і в різноманітних комбінаціях залежно від обстановки досудового розслідування: пізнання обставин події злочину; пошук джерел інформації про ці обставини; фіксація, аналіз й оцінка отриманої інформації та її джерел; подолання протидії розслідуванню. Необхідно зважати й на те, що існує певна складність у виявленні, припиненні і розслідуванні таких злочинів, що значною мірою пов'язана із електронною формою інформації про них. Одним із питань, що виникають під час досудового розслідування, постає пошук місця створення й зберігання такої інформації, її фізичних носіїв, шляхів передачі користувачам, способів і наслідків використання, знищення, модифікації тощо. Встановлювати такі місця буває доволі непросто, і в цьому слідчому, прокурору мають надати допомогу працівники оперативних підрозділів та спеціалісти. Не завжди така інформація, за допомогою якої вчинено або готується до вчинення злочин, а також інформація, що була піддана злочинному впливу, зберігається на фізичному носієві — комп'ютері і його жорсткому диску, флешкарті чи іншому фізичному носієві-накопичувачі. Сьогодні користувачі комп'ютерних засобів широко використовують хмарні технології зберігання цифрової інформації, порядок доступу до якої визначається власниками інформації і ресурсу для її збереження. Ці особи можуть перебувати не просто в різних віддалених місцях, а й у різних країнах чи навіть на різних континентах, зокрема й з різними юрисдикціями та різним порядком надання доступу і використання інформації. Відповідно, для вітчизняних правоохоронців важливо знати і правильно враховувати законодавство тієї держави, де фізично зберігається інформація про факт або сліди злочину, використовувати можливості міжнародної правової допомоги, в тому числі й з питань підготовки та проведення судово-експертних досліджень.

Ведучи мову про питання криміналістичного забезпечення діяльності СБ України із протидії злочинам проти інформаційної безпеки держави, вважаємо за потрібне зупинити окрему увагу на визначенні їх криміналістичних аспектів. Розкриваючи сутність поняття «інформаційний злочин», вітчизняний фахівець О. Тихомиров слушно звертає увагу на те, що ознака «інформаційне» визначає передусім характер цілої групи протиправних діянь, до якої належать, по-перше, безпосередні порушення інформаційних прав і свобод суб'єктів, а по-друге, інші правопорушення у разі їхньої реалізації через інформаційну сферу. На його переконання, правопорушення може бути інформаційним не тільки за спрямуванням — якщо посягає на інформацію або засоби її обробления, передавання та збереження, а й за способом вчинення — з використанням інформаційних технологій, систем, засобів. За усього різноманіття протиправних діянь, пов'язаних з інформацією, достатньо чітко виділяються певні їх сукупності, спільні за змістом (спрямуванням), які становлять видові групи інформаційних правопорушень: проти інформації, інформаційних ресурсів, що посягають на інформаційні правовідносини щодо забезпечення належних технологічних характеристик інформації (конфіденційності, цілісності, доступності тощо); проти інформаційного простору, які посягають на інформаційні правовідносини, пов'язані із якістю і цінністю інформації, зокрема належним наданням відповідної інформації, недопущенням поширення небезпечної інформації, використанням технологій деструктивного інформаційно-психологічного впливу; проти інформаційної інфраструктури, що посягають на інформаційні правовідносини, які виникають у сфері використання об'єктів інформаційної інфраструктури (інформаційно-телекомунікаційних систем, комп'ютерів, серверів, їхнього програмного забезпечення тощо); інші інформаційні правопорушення, для яких властиве використання інформації, інформаційного простору, інформаційної інфраструктури при здійсненні протиправних діянь, що посягають на інші правовідносини (щодо приватної власності, суспільної та державної безпеки, господарської діяльності тощо) [1].

У зв'язку з багатоваріантністю проявів функціональних властивостей комп'ютерних засобів і телекомунікаційних мереж, інформаційна сутність яких є беззаперечною, вважаємо, що криміналістичне поняття має ґрунтуватися на характеристиці в першу чергу функціональної сторони злочину, підкреслювати механізм його вчинення та формування слідів, що власне кажучи й становить інтерес для криміналістики. З криміналістичної точки зору злочинами проти інформаційної безпеки держави слід вважати ті, в предметі яких і в елементах способу котрих реалізуються функціональні властивості процесів, методів і засобів створення й перетворення цифрової інформації, а також знання й практичні вміння з їх здійснення. Криміналістична структура злочинів проти інформаційної безпеки держави розглядається нами як складова інформаційної основи досудового розслідування таких злочинів, в якій необхідно проводити аналіз її елементів, зокрема: об'єктів-носіїв

слідів злочинної діяльності; обстановки реалізації злочинного задуму з використанням інформаційних технологій; способів вчинення протиправних діянь вказаного виду; особи злочинця у сфері інформаційної безпеки та ін. Особливістю такої структури є наявність жорсткого детермінованого зв'язку між елементами системи. Правильна криміналістична оцінка об'єктів-носіїв слідів протиправної діяльності дає можливість створити інформаційну основу для з'ясування механізму події злочину. До того ж особлива увага має бути приділена вивченню саме цифрових слідів як доказів протиправного діяння.

Питання криміналістичного забезпечення розслідування злочинів проти інформаційної безпеки держави необхідно розглядати за такими напрямами, як техніко-, тактико- та методико-криміналістичне. За напрямом техніко-криміналістичного забезпечення здійснюються науково-дослідні роботи щодо розробки: технічних засобів і методів виявлення, фіксації, збирання, дослідження слідів злочину, іншої криміналістично значущої інформації; засобів і методів фіксації ходу і результатів слідчих та негласних слідчих (розшукових) дій; методик проведення комп'ютерно-технічних, телекомунікаційних, лінгвістичних та інших видів судових експертиз та їх впровадження в практику; методичних рекомендацій з підготовки об'єктів дослідження та ін. За напрямом тактико-криміналістичного забезпечення науково-методичні розробки стосуються питань: організації і тактики проведення окремих слідчих та негласних слідчих (розшукових) дій; використання в розслідуванні результатів контррозвідувальної та оперативно-розшукової діяльності; особливостей проведення окремих тактичних операцій та комбінацій з подолання протидії розслідуванню таких злочинів та ін. Методико-криміналістичне забезпечення спрямовано на розроблення типових і окремих методик розслідування злочинів, в основі яких лежить інформаційно-комунікаційна складова. І якщо стосовно перших двох напрямів наукові розробки ведуться сьогодні більш-менш активно, то питання методико-криміналістичного забезпечення значно відстають від потреб практики. Сучасний стан боротьби зі злочинами в інформаційній сфері визначив для криміналістики низку невирішених завдань. Найбільш суттєві з них — у галузі криміналістичної методики, оскільки саме тут відзначається основне відставання рівня науково-методичних рекомендацій від потреб практики. Як справедливо підкреслює Б. Теплицький, йдеться не лише про відсутність методик розслідування «нових» кримінальних правопорушень, а й про застарілість підходів до розслідування тих діянь, що, зберігаючи стару кримінально-правову форму, значно змінилися змістовно. Нині у криміналістиці розробка окремих методик ведеться за шаблоном, у якому практичний аспект нерідко взагалі відсутній, тоді як їх основою повинні бути саме методи, адаптовані до рівня сприйняття конкретним користувачем [2, с. 41]. Це повною мірою стосується злочинів проти інформаційної безпеки держави, при вчиненні яких використано сучасні інформаційно-комунікаційні технології.

Терміносполучення «злочини проти інформаційної безпеки держави» певною мірою є абстрактним. До цієї групи можна віднести абсолютно різнопланові кримінальні правопорушення, зокрема такі, як: злочини проти національної безпеки держави; проти громадської безпеки; проти миру, безпеки людства та міжнародного правопорядку та ін. Тому в аспекті дослідження проблем досудового розслідування інформаційних злочинів нами виокремлено дві великі групи таких кримінально караних діянь: 1 — в яких інформаційні технології мають прояв у функціональних місцях як предмет злочину; 2 — в яких використовується операційна функція інформаційних технологій, у тому числі як знаряддя та засіб вчинення злочину. Успішність розслідування будь-якого злочину проти інформаційної безпеки держави зазвичай залежить саме від уміння слідчого проникнути не тільки в кримінально-правову, а й у криміналістичну його сутність. Для цього він повинен знати типові криміналістично значущі риси злочинної діяльності для конкретного інформаційного злочину, а також уміти цілеспрямовано виявляти й вивчати необхідну для цього криміналістичну інформацію в кожному конкретному злочині, зіставляючи її з криміналістичною характеристикою злочину відповідного виду.

Розглядаючи проблеми розслідування злочинів проти інформаційної безпеки держави, передусім вважаємо за потрібне зупинити увагу на питаннях розроблення основ загальної методики їх розслідування. Деякі науковці вважають, що сутність криміналістичної методики втілюється в рекомендаціях щодо встановлення часу, місця, осіб, які брали участь у розслідуваній події, її обставин, способу вчинення злочину й обставин, що сприяли його вчиненню. У найзагальнішому значенні — це рекомендації щодо виявлення слідів кримінального правопорушення, їх аналізу та правової оцінки. Оскільки під час вчинення різних видів злочинів використовують специфічний набір засобів і способів досягнення злочинної мети, кожному з них будуть притаманні специфічні сліди й обумовлені цим засоби та методи їх виявлення, вилучення, дослідження та використання.

Ми підтримуємо позицію відомого вітчизняного криміналіста В. Журавля, який зазначає, що виходячи з концептуальних підходів до формування конфігурації системи криміналістичних методик розслідування злочинів, її основними елементами виступають: базова методика як універсальна, уніфікована модель, за якою мають створюватися інші окремі криміналістичні методики; видові криміналістичні методики (за видами злочинів, визначених у відповідних розділах Особливої частини КК України); підвидові криміналістичні методики; родові криміналістичні методики (за групами злочинів, об'єднаних за ознакою родового об'єкта й на підставі криміналістично значущих ознак, притаманних декільком видам; міжродові криміналістичні методики (за групами злочинів, диференційованих відповідно до групування їх у різних розділах Особливої частини КК України й на підставі криміналістично значущих

ознак, притаманних декільком видам); комплексні криміналістичні методики, у яких відображені рекомендації з розслідування комплексів взаємопов'язаних злочинних дій, об'єднаних на підставі одночасного врахування кримінально-правових й криміналістичних критеріїв класифікації злочинів [3, с. 196-197]. Підтримуємо також думку цього науковця і щодо необхідності формування комплексних групових криміналістичних методик розслідування укрупнених категорій злочинів, які є синтезованою моделлю відповідної категорії злочинів й основою для виокремлення особливостей розслідування таких, що входять до неї злочинів [4, с. 164]. В нашому випадку мова може йти про окремі види злочинів, наслідки яких завдають шкоду інформаційній безпеці держави. Криміналістична класифікація таких кримінальних правопорушень дає можливість віднести конкретний інформаційний злочин до певної або іншої класифікаційної групи і вже на початку досудового розслідування на основі знань криміналістичних ознак побудувати алгоритм дій, спрямованих на пошук і фіксацію доказів за конкретним кримінальним провадженням.

Найбільше значення криміналістична класифікація і відповідна криміналістична методика мають на початковому етапі розслідування. Визначення за їх допомогою класифікаційної групи злочину проти інформаційної безпеки держави дає можливість визначити обставини та зібрати відповідні докази, запобігти їх ймовірному знищенню або фальсифікації з боку злочинців. Цінним в криміналістичній класифікації злочинів проти інформаційної безпеки держави є те, що визначаючи цілком конкретні класифікаційні групи злочинів, вона дає можливість зосередитися на найбільш ймовірних кореляційних зв'язках між різноманітними криміналістично значущими ознаками певного виду або певної групи злочинів. Це дає можливість на основі знання однієї з ознак із високим ступенем ймовірності вести мову про існування, а отже, й потребу пошуку іншої. Тому на основі цього знання можна планувати й організовувати відповідну слідчу діяльність.

Як окремий напрям криміналістичного забезпечення діяльності з виявлення, розкриття й розслідування інформаційних злочинів можна розглядати програмно-цільовий метод організації діяльності оперативних та слідчих підрозділів і їх співробітників за допомогою заздалегідь розроблених типових криміналістичних програм, котрі являють собою систему рекомендацій, що мають на меті надання працівникам правоохоронних органів допомоги в організації досудового розслідування і отримання у кримінальному провадженні нових знань, правильного і своєчасного розв'язання завдань слідства. Такі програми акумулюють результати вивчення оперативної й слідчої практики та криміналістичних досліджень і є джерелами інформації про типові завдання розслідування, методи, засоби, прийоми їх розв'язання, допомагають правильно оцінити наявну і таку, що надходить, інформацію, знайти оптимальне і правильне рішення. Розроблення та використання типових

криміналістичних програм для виявлення, розкриття й розслідування окремих видів злочинів дає змогу створити й застосувати систему послідовних логічно-упорядкованих типових завдань, розв'язання яких надасть можливість найбільш ефективного отримання й вивчення потрібної для розслідування інформації за виявленим комплексом слідів злочину, об'єктів та встановлених обставин [5, с. 108—109].

Досліджуючи будь-який злочин проти інформаційної безпеки держави, вивчають сукупність дій осіб, що його підготували, вчинили, приховали сліди та ін. Тобто аналізу в таких випадках піддається вся діяльність злочинців. При системному дослідженні злочин розглядається як певна множинність елементів, взаємозв'язок котрих зумовлює цілісні властивості цієї множинності. Для криміналістів особливого значення набувають криміналістичні аспекти цього аналізу та можливість використання отриманих результатів у досудовому розслідуванні. З огляду на специфіку злочинів проти інформаційної безпеки держави, зумовлену особливостями пошуку, збирання й дослідження цифрових доказів, необхідно звернути увагу на специфічність такого криміналістичного аналізу. До основних його елементів необхідно віднести такі.

По-перше, це відомості про предмет злочинного посягання, а саме: вид і цільове призначення інформації, проти якої спрямований злочин; матеріальні носії, що використовувалися для зберігання й обробки та передачі цієї інформації. По-друге, це відомості про середовище вчинення злочину, зокрема: вид і особливості апаратного, програмного й інформаційного забезпечення автоматизованої інформаційної системи, у якій вчинено, наприклад, колаборaційну або екстремістську діяльність; встановлений порядок його функціонування і технологічна схема обробки та захисту інформації відповідно до цільового призначення автоматизованої інформаційної системи. По-третє, це відомості про особу та особистісні якості злочинця. По-четверте, це типова мотивація і цілеспрямованість злочинного поводження при вчиненні злочинів проти інформаційної безпеки держави. По-п'яте, це типові способи підготовки та вчинення злочину, способи його приховування, у т.ч. типові знаряддя (засоби). По-шосте, це відомості про типові обставини вчинення певного злочину — колаборaційної діяльності, державної зради у формі шпигунства або закликів чи розповсюдження матеріалів із закликами до вчинення дій, пов'язаних із посяганнями на територіальну цілісність і недоторканність України, зокрема: обстановку, час, місце, виконувану інформаційно-технологічну операцію. По-сьоме, відомості про сліди вчиненого злочину і його типові наслідки. Щодо останнього елемента, то до переліку таких слідів мають входити як традиційні для інших видів злочину сліди — дактилоскопічні, трасологічні, сліди підроблення документів тощо, так і специфічні для даного виду злочинів цифрові сліди [6, с. 354—355]. Криміналістичний аналіз — це не лише теоретична розробка можливостей пізнання злочину проти інформаційної безпеки

держави, а й практична діяльність слідчого, прокурора з організації та здійснення досудового розслідування.

Пошук носіїв інформації про подію злочину й складових його елементів є ключовим моментом в пошуковій і розшуковій діяльності слідчого. Лише після виявлення носіїв інформації, визначення їх як джерел відомостей, що відносяться до події злочину проти інформаційної безпеки держави і мають значення для даного кримінального провадження, можливим є вирішення інших задач розслідування — фіксації, вилучення, передачі, обробки, а також процесуального оформлення джерел і відомостей про фактичні дані для їх використання як доказів. Правильна криміналістична оцінка об'єктів-носіїв протиправної діяльності дає можливість вже на початковому етапі розслідування за вихідними даними створити інформаційну основу для з'ясування механізму злочинної події й здійснення досудового розслідування. Жодне кримінальне провадження, що відкрите за фактом вчинення кримінального діяння у даній сфері, не може бути успішно розслідуване без ретельного вивчення саме інформаційних слідів. До того ж основними взаємодіючими об'єктами, які залишають сліди при вчиненні державної зради, шпигунства, колабораційної діяльності або дій з незаконного поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів та інших злочинів, які завдають шкоду інформаційній безпеці, є з одного боку, матеріальні об'єкти у виглядів засобів комп'ютерної техніки, мобільного зв'язку тощо, а з іншого — інформаційні об'єкти у вигляді цифрових алгоритмів команд, окремих файлів.

Необхідно зазначити, що у процесі досудового розслідування злочинів проти інформаційної безпеки держави часто залишається без уваги з боку слідчого навіть та інформація, котра цілком доступна для її виявлення, вилучення й фіксації та подальшого дослідження. Це є особливо характерним для вчинення злочинів проти основ національної безпеки, тероризму та ін., які вчинені новими способами, що відрізняються високим ступенем завуальованості й протидії з боку зацікавлених осіб, активним використанням при вчиненні шпигунства, державної зради, колабораційної діяльності сучасних засобів комунікації, мережі Інтернету тощо. Врахування цих даних у типовому аналізі злочину значною мірою може полегшити пошукову діяльність слідчого, надати орієнтири такого пошуку в типових слідчих ситуаціях, допомогти в прийнятті відповідних рішень у разі виходу за їх межі.

На окрему увагу заслуговує визначення й дослідження такого елемента криміналістичного аналізу злочинів проти інформаційної безпеки держави, як обстановка їх вчинення. Важливими її факторами є ті, які характеризують інформаційні процеси, що відбуваються під час підготовки, вчинення злочину та здійснення певних дій відразу після вчинення для приховування або фальсифікації його слідів. Така обстановка і її характер можуть впливати на прийняття злочинцями рішення про час

і місце вчинення злочину, спосіб та знаряддя, що потрібні для реалізації злочинного умислу тощо. Наприклад, доступ до таємної інформації, що зберігається на персональному комп'ютері легітимного користувача, здійснюється в той час, коли законний користувач відволікся або з інших причин втратив контроль над засобами комп'ютерної техніки, залишив у відкритому доступі коди доступу до такої інформації тощо. Для доступу до таємних відомостей злочинець обирає час проведення в установі регламентних робіт на комп'ютерному обладнанні або в телекомунікаційній мережі. Все це характеризує обстановку вчинення шпигунства, яка водночас впливає на спосіб збирання зловмисником для передачі іноземним спецслужбам таємної інформації. Криміналістичному аналізу піддаються й зв'язки системи «злочин» з іншими системами, а також сліди-відображення, що утворюються на усіх стадіях вчинення того або іншого інформаційного злочину. Об'єктами пошуку, виявлення, фіксації, вилучення й дослідження за кримінальними провадженнями виступають сліди й слідоутворюючі об'єкти матеріального світу як джерела криміналістично значущої й доказової інформації, що зібрана й використовується в межах кримінального судочинства.

Заслуговує на увагу та обставина, що доволі часто слідчі не мають, окрім юридичної, додатково освіти, пов'язаної із комп'ютерними технологіями. Це призводить до того, що вони часто не можуть оперативно й повною мірою усвідомити усі фактори, які впливають на механізм утворення відомостей про той або інший вид інформаційного злочину, а отже, й усвідомити всі фактори, що необхідні для формування повного й всебічного уявлення про сам злочин, сліди, які вказують на спосіб його вчинення та причетних осіб. Тому на успішність досудового розслідування злочинів проти інформаційної безпеки держави значною мірою впливає залучення слідчим, а на етапі оперативної роботи — оперативними працівниками фахівців, що володіють спеціальними знаннями в галузі інформаційних технологій, телекомунікацій, програмування та захисту інформації. Допомога таких фахівців є необхідною буквально на кожному етапі — від виявлення ознак таких злочинів співробітниками контррозвідувальних чи оперативно-розшукових підрозділів при проведенні відповідних заходів — до участі спеціалістів у проведенні окремих слідчих та негласних слідчих (розшукових) дій і виконанні судово-експертних досліджень.

Особливістю врахування природи цифрових слідів є те, що оскільки сліди злочинів проти інформаційної безпеки є здебільшого нематеріальними, їх вивчення не може здійснити криміналіст, який не володіє спеціальними знаннями у сфері *IT*-технологій. Цим мають займатися *IT*-криміналісти, а також експерти в галузі комп'ютерно-технічної експертизи, участь яких в розслідуванні дасть змогу провести низку слідчих дій професійно, не знищивши і не пошкодивши сліди злочину. Невмілі чи неправильні дії органів досудового розслідування і працівників експертних установ можуть призвести до отримання результатів

експертизи, котрі будуть суперечити основним вимогам, що висуваються до доказів, а саме: достовірності, оскільки може мати місце вихід за межі компетенції експерта; належності, оскільки експерт, який не володіє знаннями в галузі інформаційно-телекомунікаційних технологій, не може вірогідно визначити й диференціювати часові характеристики створення, редагування та фіксації даних; допустимості, оскільки орган, який надав об'єкт, що несе в собі ознаки цифрового сліду, проте не розглядає його як такий, надає його з порушеннями правил, застосовуваних до порядку виявлення, фіксації, вилучення доказів в електронно-цифровій формі, вносячи до нього невиправні зміни [7, с. 300].

Окремої уваги потребують й питання судово-експертного забезпечення виявлення й досудового розслідування злочинів проти інформаційної безпеки держави. Завдання забезпечення розслідування необхідним інформаційно-технологічним інструментарієм мають виразний комплексний характер, а їх вирішення потребує широкого спектра спеціальних знань відповідних фахівців у галузі комп'ютерно-технічної, телекомунікаційної, лінгвістичної та інших видів судових експертиз. Особливістю значної кількості сучасних експертних досліджень є те, що їхніми об'єктами виступають продукти мовленнєвої діяльності, які знаходять своє втілення в усному або писемному мовленні та зберігаються на матеріальних носіях у графічній або цифровій формі. Експертному дослідженню підлягають як самі матеріальні носії, так і мовленнєвий продукт, що зберігається на них. Лінгвістичні дослідження мовленнєвої діяльності у комплексі із дослідженнями фахівців у галузі комп'ютерно-технічної та телекомунікаційної експертиз є вкрай необхідними для отримання й перевірки доказів за значним колом злочинів проти інформаційної безпеки держави. В окремих випадках експертні висновки стають чи не основним доказом події злочину, дають можливість встановити злочинну мотивацію й винуватість суб'єкта злочину, а також інші обставини, що входять до предмета доказування.

Висновки. На сучасному етапі розвитку суспільства інформатизація створює інноваційні різновиди злочинних дій, які надають можливість розширення зони охоплення різних напрямів протиправної діяльності, зокрема шпигунської, колабораційної, терористичної, екстремістської та іншої, що посягає на інформаційну безпеку держави чи пов'язана із вчиненням інших інформаційних злочинів. Недостатня обізнаність слідчих про різновиди типових слідчих ситуацій, слідчих версій, що можуть бути висунуті і взяті на перевірку, призводить до погіршення результативності дій слідчого на початковому та й наступних етапах досудового розслідування у зв'язку з неправильним визначенням його перспективних напрямів, вибору комплексу слідчих та негласних слідчих (розшукових) дій. На сьогодні перед СБ України під час розслідування злочинів проти інформаційної безпеки держави виникають певні проблеми, що характеризують водночас і специфіку цього процесу, а саме:

складність у встановленні факту вчинення такого злочину і вирішення питання про початок кримінального провадження; труднощі у визначенні правильної кваліфікації злочинних діянь кожного з винних осіб; труднощі у підготовці й проведенні окремих слідчих та негласних слідчих (розшукових) дій; відсутність необхідних спеціалістів, що потрібні для залучення для участі в проведенні СРД та НСРД; відсутність у значної кількості слідчих і оперативних працівників елементарних знань у галузі інформаційно-комунікаційних технологій та ін. Якісне криміналістичне забезпечення діяльності оперативних та слідчих підрозділів, що здійснюють протидію злочинам в інформаційній сфері, здатне підвищити результативність як виявлення, так і розслідування таких злочинів.

Перелік посилань

1. Тихомиров О. О. Інформаційні правопорушення: теоретико-правова концепція. *Інформаційна безпека людини, суспільства, держави.* 2015. № 1 (17). С. 38—47.
2. Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. 268 с.
3. Журавель В. А. Окремі методики в системі криміналістичних знань. URL: http://www.journals-lute.lviv.ua/index.php/visnyk-law/article/view/135/126.
4. Журавель В. А. Криміналістична класифікація злочинів: засади формування та механізм застосування. *Вісник Академії правових наук України.* № 3 (30). 2002. С. 160—163.
5. Колесник В. А. Криміналістична тактика в забезпеченні діяльності оперативних та слідчих підрозділів СБ України з виявлення й розкриття злочинів : монографія. Київ: НВВ НА СБ України, 2011. Ч.1. 270 с.

References

1. Tikhomirov O. O. Information crimes: theoretical and legal concept. *Informational security person, society, state.* 2015. No. 1 (17). P. 38—47 [in Ukrainian].
2. Teplytsky B. B. Technical and forensic support for the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage: the dissertation on competition of a scientific degree of The Candidate of Legal Sciences on a specialty 12.00.09, Kyiv, 2021. 268 p. [in Ukrainian].
3. Zhuravel, V. A. Separate methods in the system of forensic knowledge. URL: http://www.journals-lute.lviv.ua/index.php/visnyk-law/article/view/135/126 [in Ukrainian].
4. Zhuravel, V. A. (2002). Forensic classification of crimes: principles of formation and mechanism of application. *Bulletin of the Academy of Legal Sciences of Ukraine.* No. 3 (30). Pp. 160—163 [in Ukrainian].
5. Kolesnyk, V. A. (2011). Forensic tactics in ensuring the activity of operational and investigative units of the Security Service of Ukraine for the detection and disclosure of crimes: a monograph. Kyiv: NVV NA SB of Ukraine. Part 1. 270 p. [in Ukrainian].

6. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування : монографія / І. В. Гора, В. А. Колесник, В. В. Малюк, В. О. Ходанович, А. М. Черняк, Л. І. Щербина; за заг. ред. В. А. Колесника. Київ: 7БЦ, 2023. 512 с.

Crimes against information security of the state: concepts, detection, pre-trial investigation (2023) : monograph / I. V. Hora, V. A. Kolesnyk, V. V. Malyuk, V. O. Khodanovich, A. M. Chernyak, L. I. Shcherbyna; according to general ed. V.A. Kolesnyka. Kyiv: 7BC. 512 p. [in Ukrainian].

7. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні : монографія / І. В. Гора, В. А. Колесник, В. В. Малюк, В. О. Ходанович, А. М. Черняк, Л. І. Щербина; за заг. ред. В. А. Колесника. Київ : 7БЦ, 2024. 484 с.

Electronic evidence in criminal proceedings: concept, collection, use in evidence (2024) : monograph / I. V. Hora, V. A. Kolesnyk, V. V. Malyuk, V. O. Khodanovych, A. M. Chernyak, L. I. Shcherbina; in general ed. V.A. Kolesnyka. Kyiv: 7BC. 484 p. [in Ukrainian].

Current issues of forensic support of investigation of crimes against information security of the state

I. Hora, V. Kolesnyk

The problems of forensic support for the investigation of crimes against the information security of Ukraine are considered. The main problems arising in the practice of their pre-trial investigation are identified. It is emphasized that the aggressor country's build-up of reconnaissance, subversive, terrorist and other illegal activities against Ukraine, the waging of an aggressive war, including information warfare, imposes on the bodies and divisions of the Security Service the task of protecting its information sphere. Attention is drawn to the fact that modern criminology acutely responds to all the needs of practice related not only to the fight against crime, but also to other illegal challenges of our time, and its methods and means become an important arsenal and effective tools in the work of operational and investigative units. There is difficulty in identifying and investigating such crimes, which is largely due to the electronic form of the subject of the attack, the instruments of the crime, as well as the traces and other evidence they leave. An important issue is the search for places of creation and storage of evidentiary information, its physical media, ways of transmission to users, methods and consequences of use, destruction, modification. The article discusses the forensic essence of the concept of crimes against the information security of the state. It is substantiated that they should be considered those in the subject and in the elements of the method of implementation of which the properties of the processes, methods and means of creating, converting digital information, as well as knowledge

and practical skills for their implementation are realized. A correct forensic assessment of digital objects that carry traces of illegal activity makes it possible to create an information basis for clarifying the mechanism of a crime event. Issues of forensic support for the detection and investigation of crimes against the information security of the state are considered in such areas as technical, tactical and methodological forensics. It is proposed to pay special attention to the issues of methodological and forensic support aimed at developing standard and private methods for investigating crimes, which are based on the information and communication component. Attention is drawn to the possibility of using special knowledge in the field of computer technology, telecommunications and linguistic expertise.

Keywords: information security; pre-trial investigation; forensics; forensic support; expert research; forensic examinations; investigative and covert investigative actions.

⇒ Гора, І. В., Колесник, В. А. (2024). Актуальні питання криміналістичного забезпечення досудового розслідування злочинів проти інформаційної безпеки держави . *Криміналістика і судова експертиза.* Вип. 69. С. 20—34. DOI: 10.33994/kndise.2024.69.02.