Черняховський Богдан Вікторович
старший слідчий в особливо важливих справах Головного слідчого управління Національної поліції України, ад'юнкт кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРИЗНАЧЕННЯ КОМП'ЮТЕРНИХ ЕКСПЕРТИЗ У РОЗСЛІДУВАННІ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Сучасні передумови розбудови правової держави передбачають інтеграцію інформаційно-технологічних процесів як у діяльність громадян так і функціонування державних інституцій. Так, відомий українському загалу «курс на діджиталізацію держави» формує нові виклики для органів досудового розслідування щодо забезпечення якісного розкриття та доказування кіберзлочинів, як складового елементу надійної держави для міжнародних партнерів та стратегічних союзників.

Форсований перехід державних підприємств, установ, організацій на систему електронного документообігу, започаткування систем електронної реєстрації, розширення можливостей застосування електронного підпису та утворення нових, зручних та швидких у використанні електронних реєстрів, баз/банків даних, вимагає готовності правоохоронців до ідентифікації та належного дослідження ознак можливих несанкціонованих дій, пов'язаних з втручанням в роботу таких інформаційних систем. Жодна інформаційна система світу не має абсолютного імунітету від кібератак та стороннього втручання. Тому забезпечення ефективного та якісного розслідування злочинів у сфері інформаційних технологій, технічна сторона яких не є профільною основою в системі підготовки кадрів для органів досудового розслідування, вимагає вивчення цих питань на поглибленому науковому рівні.

Дослідженню окремих аспектів розслідування злочинів у сфері комп'ютерних технологій приділяла увагу значна кількість учених-криміналістів, зокрема: Т. В. Авер'янова, К. І Бєляков, В. В. Бірюков, В. Б. Вєхов, В. В. Крилов, В. О. Мєщєряков, І. Ю. Михайлов, О. В. Орлов, О. Р. Росинська, М. В. Салтевський, Б. Б. Теплицький, В. Г. Хахановський, С. С. Чернявський та ін. У той же час актуальною є необхідність удосконалення системи знань та навичок слідчих щодо особливостей роботи

з цифровою інформацією під час кримінального провадження, зокрема щодо особливостей її фіксації, вилучення та дослідження під час судових експертиз.

Одним із найбільш розповсюджених злочинів у сфері інформаційних технологій є передбачене статтею 361 Кримінального кодексу (далі – КК) України несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, 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 і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації. [3]

Ключову роль у доказуванні факту несанкціонованого втручання відіграють результати проведення судових експертиз – дослідження на основі 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. [4] Відповідно до положень пунктів 13 та 14 Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 08.10.1998 № 53/5 (у редакції наказу Міністерства юстиції України від 26.12.2012 № 1950/5) (далі – наказ Мін'юсту № 53/5) регламентовано порядок застосування експертизи комп'ютерної техніки і програмних продуктів (у криміналістичній літературі більш вживане поняття «комп'ютерно-технічна експертиза») та експертизи телекомунікаційних систем і засобів.

Основні завдання комп'ютерно-технічної експертизи з науково-практичної точки зору сформульовано директором Державного науково-дослідного експертно-криміналістичного центру МВС України – керівником Експертної служби МВС України Б. Б. Теплицьким, а саме: 1) діагностування апаратних засобів комп'ютерної системи; 2) визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану представленого програмного, системного та прикладного значення; 3) пошук, виявлення, аналіз й оцінювання кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі. [2]

Наближеною за своєю суттю, проте ширшою за змістом, є експертиза телекомунікаційних систем та засобів, що обумовлюється об'єктом її дослідження: телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається, приймається та обробляється.

Наказ Мін'юсту № 53/5 передбачає орієнтовний перелік питань, які ставляться для вирішення при призначенні кожного із зазначених видів експертиз. Однак, в залежності від обставин розслідуваного злочину

слідчому рекомендовано в обов'язковому порядку, коригувати, конкретизувати та доповнювати питання з урахуванням консультативної допомоги спеціаліста чи експерта, який проводитиме експертизу.

Вивчення слідчої і експертної практики та аналіз наукових джерел засвідчили, що на вирішення комп'ютерно-технічних експертиз ставляться, та успішно вирішуються експертами питання, які передбачені наказом Мін'юсту № 53/5, наприклад: чи міститься (містилася) на наданому на дослідження носії інформація, яка 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 здійснювався вихід у мережу Інтернет, за якими адресами, в який період часу?; чи наявні на досліджуваному комп'ютері програмні продукти, призначені для злому пароля та несанкціонованого доступу до комп'ютерних систем?; чи можливе вирішення певного завдання за допомогою програмного продукту (зазначається 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 і засоби програмування, що застосовувалися при створенні досліджуваного програмного продукту, прийомам і засобам, якими користується певна особа? [1]

Під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, об'єктом посягання є інформація, що зберігається в самому комп'ютері, на певному носії, та/або програмне забезпечення. При цьому жорсткі диски комп'ютерів нерідко є місцем зберігання чи навіть приховування інформації, що становить інтерес для досудового розслідування. Відповідно, комп'ютер або комп'ютерна мережа досліджуються як середовище, в якому здійснено несанкціонований виток, втрату, підробку, блокування інформації, спотворений процес її обробки або порушено встановлений порядок її маршрутизації.

У таких випадках органам досудового розслідування слід дотримуватись вимог чинних нормативних-правових та розпорядчих (відомчих) актів України, забезпечивши залучення експертної установи, експерта або експертів для проведення комплексної судової експертизи комп'ютерної техніки і програмних продуктів та експертизи телекомунікаційних систем та засобів. Такий висновок експерта відповідатиме положенням кримінального процесуального законодавства України, а також пунктам 13 та 14 наказу Мін'юсту № 53/5.

Доцільність призначення у кримінальному провадженні за ст. 361 КК України саме комплексної судової експертизи комп'ютерної техніки, програмного забезпечення, телекомунікаційних систем та їх засобів у відповідних випадках обґрунтовується й наявністю у Реєстрі методик

проведення судових експертиз Міністерства юстиції України відповідної методики даного виду експертного дослідження. У той же час цей реєстр не містить окремо визначеної методики проведення дослідження телекомунікаційних систем (обладнання) та засобів, на відміну від методики дослідження комп'ютерної техніки та програмних продуктів. [5]

Досудове розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, з огляду на специфіку злочину та способів його вчинення, вимагає спеціальної підготовки слідчого, наявності у нього відповідних криміналістичних знань, а також умінь та навичок. Тому вивчення можливостей таких експертиз як експертиза комп'ютерної техніки і програмних продуктів та експертиза телекомунікаційних систем і засобів є одним із ключових елементів набуття навичок формування доказової бази від час розслідування кіберзлочинів в Україні.

Список використаних джерел

1. Експертизи в судочинстві України: науково-практичний посібник/ [С. Б. Бойченко, В. І. Бояров, Т. В. Будко та ін.]. Київ: Юрінком Інтер., 2015. 504 с.;

2. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи: Юридичний часопис Національної академії внутрішніх справ/[Б.Б. Теплицький, 2019 № 1 (18). с.24-32;

3. Кримінальний кодекс України від 05 квіт. 2001 р. № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14 [Дата звернення 20.10.2019];

4. Про судову експертизу: Закон України від 25 лют. 1994 р. № 4038-XII URL: https://zakon.rada.gov.ua/laws/show/4038-12 [Дата звернення 20.10.2019];

5. Реєстр методик проведення судових експертиз. URL: http://rmpse.minjust.gov.ua [Дата звернення 20.10.2019].

Чорний Микола Васильович,
доцент кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат медичних наук, доцент

РЕТРОСПЕКТИВНИЙ АНАЛІЗ ПЕРЕДСМЕРТНИХ ЗАПИСОК СУЇЦИДЕНТІВ

Протягом століть релігійне виховання прищеплювало думку про гріховність самогубства, що не могло не знайти свого відображення в специфіці слов'янської ментальності: з одного боку, покійного прийнято