

УДК 343.98

СУДОВА ТЕЛЕКОМУНІКАЦІЙНА ЕКСПЕРТИЗА ЯК ДЖЕРЕЛО ДОКАЗІВ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Вадим КОРШЕНКО,
провідний фахівець факультету № 4
Національного університету внутрішніх справ

SUMMARY

In the article the author considers the problems of obtaining evidence, which occur in the investigation of cybercrime and the possibility of a telecommunication forensic as a new kind of engineering-technical forensic. The article also deals with the concept of traces of the crime, defines the problems that arise during the implementation of telecommunication forensic, provided recommendations on their elimination and discusses the methodologies of telecommunication forensic.

Key words: cybercrime, investigations, traces, telecommunication forensic, methods.

АНОТАЦІЯ

У статті автором розглядаються актуальні проблеми отримання доказів, які виникають під час розслідування кіберзлочинів, та можливості нового роду інженерно-технічних судових експертиз – телекомунікаційної експертизи. Також у статті аналізуються поняття слідів злочину, визначаються проблеми, які виникають під час провадження телекомунікаційних експертиз, надаються відповідні рекомендації щодо їх усунення та розглядається питання розробки методик телекомунікаційних експертиз.

Ключові слова: кіберзлочин, розслідування, сліди, телекомунікаційна експертиза, методики.

Постановка проблеми. Стрімкий розвиток телекомунікаційних систем, який став наступним етапом глобальної комп'ютеризації суспільства і розвитку сучасних інформаційних технологій, призводить до зміни філософії використання таких звичних ресурсів, як місце для зберігання даних, обчислювальні потужності тощо. Дедалі більше різноманітних електронних пристроїв обладнуються різними засобами телекомунікацій. За реаліями сьогодення комп'ютер, не підключений до мережі Інтернет вважається анахронізмом, а комунікаційний модуль Wi-Fi або Bluetooth можна знайти в телевізорі, телефоні, холодильнику, гідромасажному боксі, лампі освітлення тощо. Усе більше особистої, корпоративної та державної інформації зберігається за хмарними технологіями та на віддалених хостингах, обчислювальні операції переносяться з персональних систем в обчислювальні кластери, на віртуальні сервери, в хмарні технології. Науково-технічний прогрес, крім позитивних досягнень, має шкідливі наслідки. Різноманіття телекомунікаційних ресурсів є багатогатним полем для появи нових витончених способів злочинної діяльності. Злочинів у сфері високих телекомунікаційних технологій стає дедалі більше, методи і засоби вчинення кіберзлочинів стають дедалі технологічними. Вказане вимагає використання сучасних способів протидії кіберзлочинам, впровадження інноваційних технологій та методів у роботу правоохоронних органів для своєчасного виявлення та кваліфікованого їх розслідування.

У різні часи в Україні деякі аспекти розслідування злочинів, вчинених із використанням комп'ютерних технологій, висвітлювались у працях українських вчених: П.Д. Біленчука, М.С. Вергузасва, А.Ф. Волобуєва, В.О. Голубєва, М.В. Гуцалоюка, Г.О. Душейка, М.А. Зубань, О.І. Могляха, П.І. Орлова, Л.П. Паламарчук, М.В. Салтєвського, О.П. Снігерьова, В.С. Цимбалюка та ін. Багато закордонних вчених також присвятили свої дослідження цим злочинам: Б.В. Андрєєв, А.А. Васильєв, В.Б. Вєхов, Ю.В. Гаврилін, А.В. Касаткін, В.С. Козлов, В.В. Крилов, В.О. Мєшєряков, П.Н. Паєк, В.Ю. Рогозін, С.А. Смирнова, Н.Г. Шурухнов, О.М. Яковлев та інші. Використання спеціальних знань під час розслідування цих злочинів роз-

глядалися А.А. Васильєвим, Д.В. Пашнєвим, О.Р. Росинською, А.І. Семікаленовою, М.Г. Щєрбаковським, О.І. Усовим та ін. Однак розвиток телекомунікаційних технологій вимагає вдосконалення існуючих та розвиток нових способів виявлення слідів злочинів на основі використання спеціальних знань.

Метою статті є розгляд проблем становлення нового роду інженерно-технічних судових експертиз – телекомунікаційної експертизи.

Виклад основного матеріалу дослідження. Ефективність розслідування кіберзлочинів багато в чому залежить від своєчасного виявлення слідів злочинних дій. Сліди злочинів у сфері використання інформаційних технологій утворюються в результаті зовнішнього або внутрішнього неправомірного впливу на телекомунікаційну систему, окремих електронних пристроїв, програму чи на комп'ютерну інформацію і являють собою будь-які зміни комп'ютерної інформації, які відбулися в результаті вчинення злочину із застосуванням комп'ютерних технологій [1, с. 62]. Вказані сліди у вигляді змін параметрів функціонування системи, її окремих елементів або програм, модифікації, копіювання або знищення інформації свідчать про незаконний доступ до системи, атаки чи спроби злomu. Сама інформація також може зберегти сліди її часткового знищення чи модифікації, наприклад додавання або видалення окремих записів до бази даних, зміна текстів документів, внесення змін (монтаж) фотографій, графічних зображень та відео файлів тощо.

Для того, щоб зазначені сліди могли перетворитись на докази, необхідно їх знайти, процесуальним шляхом виявити та зафіксувати. Основним процесуальним способом перетворення невидимої інформації та слідів кіберзлочинів на докази є проведення судової експертизи. Отже, потенційна інформація, що знаходиться в слідах злочину, виявлених у електронних пристроях, телекомунікаційних системах і програмах, актуалізується і перетворюється в доказову інформацію саме шляхом використання спеціальних знань у формі судової експертизи. Адже експертиза є самостійною процесуальною формою одержання нових доказів і уточнення (перевірки) тих, що вже отримані.

Ефективність розслідування кіберзлочинів, скоєних із використанням комп'ютерних технологій та телекомунікаційних засобів, безпосередньо залежить від сучасних можливостей та якості проведення судових експертиз. До 2006 року в Україні для вирішення всіх питань, пов'язаних із комп'ютерно-технічними засобами, телекомунікаційними системами, електронними пристроями, програмами тощо, призначали судову комп'ютерно-технічну експертизу. Але перелік питань, які виносились на розгляд експерта, постійно зростає, галузь необхідних для вирішення питань знань розширялась, і логічним наслідком цих процесів було виділення судової телекомунікаційної експертизи в окремий рід інженерно-технічних експертиз [2].

Виникнення телекомунікаційної експертизи зумовлено не тільки значним поширенням телекомунікаційних технологій у виробничій та приватній діяльності, а й тим, що цей вид досліджень потребує окремих знань, пов'язаних із розумінням інформаційних процесів у комп'ютерних мережах, мережах зв'язку, спеціалізованих телекомунікаційних пристроях [3, с. 446]. Поява нового роду судових експертиз вимагає розробку нових судово-експертних методик дослідження. Особливостями існуючих методик експертного дослідження комп'ютерної техніки, програмних продуктів і телекомунікаційних мереж є те, що вони вимагають постійного оновлення та удосконалення у зв'язку з постійною зміною форматів представлення даних, операційних та файлових систем, протоколів передачі даних, технічних засобів передачі інформації. Цілком зрозуміло, що розробка й удосконалення таких методик можливо лише з використанням сучасного обладнання, програмного забезпечення та спеціальних знань фахівців у галузі телекомунікаційних систем і IT-технологій.

Відомо, що розвиток судово-експертної галузі знання пов'язаний із чітким визначенням властивих їй завдань, кола досліджуваних об'єктів, розробкою відповідних методик дослідження. Аналіз спеціальної літератури показує, що на теперішній час існує обмежена кількість публікацій щодо об'єктів і завдань телекомунікаційної експертизи. Підтвердженням недостатньої розробки методичних проблем телекомунікаційної експертизи є відсутність затверджених міністерством юстиції відповідних методик дослідження [4]. Дії експерта в процесі експертного дослідження ґрунтуються в основному на його загальних спеціальних знаннях, отриманих у процесі навчання у вищій навчальній установі, інтуїції і досвіді проведення попередніх експертиз. Погіршує положення факт відсутності достатньої кількості робіт із теоретичних та методичних основ телекомунікаційної експертизи.

Виходячи з вищесказаного, на нашу думку, існують кілька проблем, що виникають під час провадження телекомунікаційних експертиз. Перша з них полягає в тому, що під час дослідження об'єктів телекомунікаційних експертиз експерту необхідний великий обсяг різноманітної довідкової інформації з різних галузей комп'ютерних знань, оскільки на сьогоднішній момент не існує упорядкованої сукупності зведень виключно для телекомунікаційних експертиз. Джерелами довідкової інформації для експерта з телекомунікаційних експертиз виступають інструкції, довідкова література та інформація, розміщена на численних сайтах глобальної мережі «Інтернет». Надійність, або здатність інформаційного джерела достовірно надати необхідні відомості прямо впливає на правильність умовиводів, винесених експертом у висновок. Відповідно, використання експертом у ході проведення телекомунікаційних експертиз неточної чи помилкової довідкової інформації може привести до експертної помилки або призначенню повторної експер-

тизи. Виникає природне питання про надійність зведень, розмішених у вказаних джерелах. На сьогодні це питання для експертів телекомунікаційних експертиз ніякими нормативно-правовими актами не урегульоване. Рішенням цієї проблеми може бути створення певного державного (міждержавного) органу (або використання існуючого), який здійснював би оцінку ступеня надійності довідкових офіційних видань і електронних джерел інформації, використовуваних у телекомунікаційних експертизах, а також вироблення правил доступу до цих джерел.

Другою істотною проблемою є той факт, що в процесі проведення телекомунікаційних експертиз використовуються не сертифіковані технічні засоби і програмне забезпечення, механізм дії яких найчастіше до кінця не вивчений і походження яких невідомо. Зазначені недоліки можуть породити сумніви в обґрунтованості експертних висновків і, як наслідок, у правильності висновку експерта. У зв'язку з вищевикладеним вважаємо за необхідне розробку окремих і типових, а потім на їх основі – загальних експертних методик дослідження, що істотно підвищить методичний рівень висновків телекомунікаційних експертиз і послужить допоміжним фактором у формуванні наукових засад телекомунікаційних експертиз як окремої галузі судової експертології.

Відомо, що в залежності від об'єктів, обсягу і характеру розв'язуваних завдань розрізняють загальну, типову, окрему експертні методики, а для проведення конкретної експертизи розробляється конкретний методика експертного дослідження [5, с. 69]. Методика являє собою систему категоричних або альтернативних науково обґрунтованих приписів щодо вибору і застосування в певній послідовності і в певних існуючих умовах методів, прийомів і засобів (пристосувань, приладів і апаратури) для вирішення експертного завдання. Істотним моментом під час розробки методик і проведення дослідження телекомунікаційних експертиз є, по-перше, використання надійних апаратних засобів і програмних продуктів, дія яких відома і випробувана; по-друге, використання надійних довідкових відомостей про властивості, характеристики, параметри й інші особливості досліджуваних об'єктів.

Виходячи із цього, методика дослідження повинна містити в собі:

- алгоритм дії експерта під час проведення дослідження з розв'язання типових завдань;
- рекомендації з вибору джерел інформації (технічної літератури, довідкових видань, електронні форуми за даними питанням і т.д.);
- рекомендації з вибору програмного забезпечення для проведення експертизи;
- рекомендації з технічного забезпечення експерта.

Слід зазначити, що під час проведення експертних досліджень використовуються методи, які, як правило, розробляються не самим експертом. Складність сучасних технічних засобів і методів аналізу речових доказів приводить до необхідності формування (розробки) комплексу типових (стандартних) методик. У судово-експертних умовах розроблені визначені процедури перевірки методів (методик) і їхньої апробації. У Міністерстві юстиції України функціонує Науково-консультативна та методична рада з проблем судової експертизи, в обов'язок членів якої входить перевірка методик і надання рекомендацій з їх впровадження. Таким чином, існує визначена процедура, яка гарантує якість і ефективність пропонуваних до використання в експертній практиці методик. Однак розробка методичного забезпечення для проведення телекомунікаційних експертиз йде вкрай повільно, що зумовлено, з одного боку, стрімким розвитком в останні

роки комп'ютерних та телекомунікаційних технологій, відносно новизною цього виду експертиз, а з іншого, – недостатньою кількістю експертів – фахівців у галузі телекомунікаційних експертиз.

Одним із варіантів рішення даної проблеми може бути використання можливостей навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору, створеного в Харківському національному університеті внутрішніх справ, де в реальних умовах можливі розробка й апробація конкретних методик проведення досліджень в області телекомунікаційних експертиз.

Зокрема, на базі центру можуть розроблятися методики рішення таких завдань:

1) оцінка ефективності програмних і апаратних засобів (у тому числі і засобів мережевого захисту);

2) дослідження мережевих взаємодій додатків із метою розробки рекомендацій для проведення телекомунікаційних експертиз при розслідуванні злочинів вчинених у сфері високих технологій;

3) моделювання і реалізація несанкціонованого доступу на корпоративну комп'ютерну мережу організації;

4) вироблення рекомендацій із захисту від зовнішнього проникнення в операційні системи, браузері, додатки та окремі програмні продукти та ін.;

5) розробка і надання технічних рекомендацій оперативним підрозділам правоохоронних органів зі здійснення негласних заходів у рамках боротьби зі злочинністю у сфері високих технологій.

Приведений перелік не вичерпний і може бути розширений у відповідності з виникаючими завданнями.

Висновки. Розслідування злочинів, вчинених із використанням сучасних інформаційних та телекомунікаційних технологій, потребує відповідного експертного забезпечення. Ефективним способом виявлення слідів кіберзлочинів та формування на їх основі доказів є судова телекомунікаційна експертиза, яка вимагає розвитку наукових (висвітлення переліку об'єктів, завдань), методичних (розробка методів, методик дослідження) та організаційних (інформаційного забезпечення) основ.

Список використаної літератури:

1. Пашнев Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. ... канд. юрид. наук: 12.00.09 / Д.В. Пашнев ; Харк. нац. ун-т внутр. справ. – Х., 2007. – 228 с.

2. Про внесення змін до Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки матеріалів та призначення судових експертиз : наказ Міністерства юстиції України від 29.12. 2006 року № 126/5 [Електронний ресурс]. – Режим доступу : http://search.ligazakon.ua/l_doc2.nsf/link1/RE13267.html.

3. Бобрицький С.М. Методичні аспекти дослідження телекомунікаційних систем (обладнання) та засобів / С.М. Бобрицький // Теорія та практика судової експертизи і криміналістики. – Харків : Право, 2008. – Вип. 8. – С. 445–449.

4. Реєстр методик проведення судових експертиз [Електронний ресурс]. – Режим доступу : <http://tmpse.minjust.gov.ua>.

5. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е.Р. Россинская. – М. : Норма, 2005. – 656 с.