УДК 343.98 DOI: 10.37025/1992-4437/2021-36-2-59

Ю. Ю. Нізовцев, *кандидат юридичних наук,*
провідний науковий співробітник
науково-дослідної лабораторії
Центру судових і спеціальних експертиз,
Український науково-дослідний інститут
спеціальної техніки та судових експертиз
Служби безпеки України, м. Київ
ORCID: https://orcid.org/0000-0002-7641-6403
email: nizovtsev.yurii@gmail.com
О. С. Омельян, *аспірант,*
Національна академія
Служби безпеки України, м. Київ
ORCID: https://orcid.org/0000-0003-4495-7835
email: omelan_ssu@ukr.net

ЩОДО ПІДГОТОВКИ ТА ПРИЗНАЧЕННЯ СУДОВИХ ЕКСПЕРТИЗ У МЕЖАХ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ КІБЕРАТАКАМИ

Мета статті – науково обґрунтувати теоретичні засади підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень, пов'язаних із кібератаками, сформувати відповідні науково-прикладні рекомендації. ***Методологія***. Достовірність отриманих результатів і висновків забезпечено сукупністю методів загальнонаукового і конкретно-наукового рівнів. Зокрема, основним є загальний діалектичний метод наукового пізнання явищ, процесів та об'єктів, а також моделювання та прогнозування, формально-логічний, системно-структурний методи. ***Наукова новизна***. Уточнено перелік запитань, які можуть бути поставлені на вирішення судової експертизи в разі втручання у роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні та застосування шкідливих програм. ***Висновки***. Констатовано, що до об'єктів дослідження у межах розслідування кіберзлочинів належать носії інформації або їх клони чи бітові образи; дампи оперативної пам'яті; лог-файли; файли-звіти діагностичних утиліт; налаштування логіювання; налаштування діагностичних утиліт; схеми будови автоматизованих систем і мереж; налаштування обладнання та програмного забезпечення; листування електронною поштою; вихідні коди шкідливих програм та самі шкідливі програми, засоби їх розроблення та адміністрування. Виокремлено особливості вилучення об'єктів дослідження у межах розслідування кіберзлочинів, які полягають у тому, що криміналістично значуща інформація вилучається як з атакованих комп'ютерів, так і з комп'ютерів підозрюваних осіб. При цьому слід зважати на те, що зловмисники, як правило, намагаються приховати сліди кібератаки на атакованому комп'ютері, а на власному комп'ютері застосувати заходи «контркриміналістики». Розроблено науково-прикладні рекомендації щодо підготовки та призначення судових експертиз у межах розслідування кіберзлочинів, виявлено перспективні напрями розширення можливостей судової експертизи за грамотного формулювання запитань, які ставляться для її вирішення.

Ключові слова: судова експертиза; комп'ютерно-технічна експертиза; телекомунікаційна експертиза; інформаційна безпека; кіберзагроза; кіберзлочин; кібератака; кіберінцидент; шкідливі програмні засоби; лог-файл.

Вступ

У реаліях сьогодення забезпечення кібербезпеки постало чи не найважливішим завданням держави. Адже найбільшу небезпеку автоматизованим системам становлять не «звичайні» злочинці, а спецслужби (переважно недемократичних країн), які нерідко вчиняють кібершпигунство (Diorditsa, 2020) і кібертеракти. Крім того, кібератаки можуть бути складовою підривних інформаційно-психологічних операцій, типовий приклад яких так звана «картинка Ярошa» (Zhora, 2017).

Протидія кібератакам передбачає не лише ефективний захист і швидке реагування на кіберзагрози. Важливим елементом протидії є розслідування кіберінцидентів, що в разі вчинення кіберзлочинів здійснюють уповноважені правоохоронні органи та, за наявності підстав, спецслужби.

Призначення судових експертиз – важливий етап у розслідуванні майже будь-якого кримінального правопорушення. Актуальність проведення експертизи значно підвищується, коли розслідуються «наукоємні», «високоінтелектуальні» та «високотехнологічні» злочини. Для виявлення

слідів таких злочинів, їх фіксації та дослідження, дальшого відтворення всіх етапів вчинення протиправних діянь замало суто юридичних, необхідні й спеціальні знання. Така закономірність цілком стосується розслідування кримінальних правопорушень, пов'язаних із кібератаками, для вчинення яких потрібні досить глибокі знання у сфері сучасних інформаційних технологій. І, відповідно, розслідування таких кримінальних правопорушень важко уявити без призначення комп'ютерно-технічної та/або телекомунікаційної експертизи. Водночас вислів, що правильно сформульоване запитання – це вже половина відповіді, доречний, як ніде, коли призначаються судові експертизи, що відбивається на ефективності процесу доказування. Як засвідчує практика, ініціатор, який призначив експертизу, незрідка ставить запитання некоректно, при цьому, трапляється, не зважаючи на те, що проведення експертизи для з'ясування питань права не допускається (*Kryminalnyi protsesualnyi kodeks Ukrain*, 2012, st. 242, ch. 1), чи копіює до постанови про призначення експертизи всі запитання з довідника, методичних рекомендацій (*Naukovo-metodychni rekomendatsii*, 1998) або відповідної відомчої інструкції (*Instruktsiia pro pryznachennia ta provedennia sudovykh ekspertyz*, 2015). У кращому разі значна кількість запитань уповільнить роботу експерта, у гіршому – питання не вирішуватимуться, оскільки відповідь на них виходить за межі компетенції експерта. Певні проблеми мають місце і з підготовкою матеріалів для експертизи.

Отже, підготовка та призначення судових експертиз під час розслідування кіберзлочинів постають актуальними об'єктами наукового дослідження з метою вироблення науково обґрунтованих рекомендацій щодо їх здійснення.

Проблемні аспекти підготовки та призначення судових експертиз вивчали науковці і практики, серед них В. Г. Гончаренко, А. В. Іщенко, Н. І. Клименко, В. К. Лисиченко, І. В. Пиріг, М. Я. Сегай, Е. Б. Сімакова-Єфремян, М. Г. Щербаковський, призначення експертиз саме під час розслідування кіберзлочинів досліджували, зокрема, С. М. Бобрицький, В. А. Коршенко, Б. Д. Леонов, Д. В. Пашнєв, В. С. Серьогін, та ін. Плідно працюють у цьому напрямі й зарубіжні колеги (Karafili, Cristani, & Viganò, 2018; Karafili, Wang, Kakas, & Lupu, 2018; Karafili, Wang, & Lupu, 2020; Torabi, Bou-Harb, Assi, & Debbabi, 2020; Horsman, 2021; Torabi, Dib, Bou-Harb, Assi, & Debbabi, 2021; Shrivastava, Gupta, & Sharma, 2021).

Вітчизняні науковці останнім часом порушують такі питання: особливості експертного експерименту під час проведення судових комп'ютерно-технічних експертиз (Polishchuk, 2018); основи методики розслідування кримінальних правопорушень, вчинених у кіберпросторі (Samoilenko, 2020); особливості проведення окремих судових експертиз (Symonenko, 2020); організаційно-тактичні основи призначення експертиз (Kholostenko, & Motruk, 2020); використання спеціальних знань і проблеми призначення судових експертиз (Syvodied, 2021); актуальні питання призначення криміналістичних судових експертиз в Україні (Lazebnyi, & Bozhuk, 2021); сутність і цілі використання судових експертиз у досудовому розслідуванні кримінального провадження (Ortynskyi, 2021).

Проте методологічні підходи щодо призначення судових експертиз під час розслідування кіберзлочинів і досі недостатньо розроблені. На цьому, поділяючи думку інших науковців, наголошує А. А. Русецький, вивчаючи місце судової експертизи в системі протидії кіберзагрозам в Україні (Rusetskyi, 2018). Досить докладно сутність і зміст розслідування кіберінцидентів та кібератак працівниками підрозділів Служби безпеки України розглядає М. В. Кулешов, але не висвітлюючи особливостей призначення судових експертиз (Kuleshov, 2019).

Отже, на часі започаткування науково-прикладних рекомендацій щодо особливостей призначення судових експертиз під час розслідування кіберзлочинів, придатних для застосування безпосередньо у практичній діяльності, що й зумовлює актуальність обраної тематики і визначає напрям наших дальших розвідок.

Мета й завдання дослідження

Мета статті – науково обґрунтувати теоретичні засади підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень, пов'язаних із кібератаками, сформувати відповідні науково-прикладні рекомендації.

Для досягнення цієї мети необхідно вирішити такі завдання:

визначити об'єкти дослідження у межах розслідування кіберзлочинів;

розкрити особливості їх вилучення;

сформувати науково-прикладні рекомендації щодо підготовки та призначення судових експертиз у межах розслідування кіберзлочинів.

Виклад основного матеріалу

Відповідно до законодавства України про судову експертизу «судова експертиза – це 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» (st. 1). «Судовими експертами можуть бути особи, які

мають необхідні знання для надання висновку з досліджуваних питань» (st. 10, ch. 1) (*Pro sudovu ekspertyzu*, 1994).

Згідно з кримінальним процесуальним законодавством України «експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань» (st. 69, ch. 1). «Експертиза проводиться експертною установою, експертом або експертами, яких залучають сторони кримінального провадження або слідчий суддя за клопотанням сторони захисту у випадках та порядку, передбачених статтею 244 цього Кодексу, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання. Не допускається проведення експертизи для з'ясування питань права» (st. 242, ch. 1) (*Kryminalnyi protsesualnyi kodeks Ukrain*, 2012).

Отже, судового експерта вирізняє наявність спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо, яких, власне, і бракує іншим учасникам кримінального провадження. Що більш «високотехнологічне» кримінальне правопорушення, то, зрозуміло, більшою є потреба в призначенні судових експертиз. Комп'ютерні технології наразі характеризуються особливо інтенсивним розвитком, нові технічні рішення постають чи не щодня. Послуговуються ними і злочинці, вчиняючи протиправні дії. А втім, для слідчого, так само як і прокурора, слідчого судді, судді, фаховими є правові знання, які він здобув як юрист. Тому, розслідуючи кіберзлочини, потрібна допомога експерта, який володіє технічними знаннями в галузі інформаційних технологій.

Залежно від виконуваних завдань та змістового навантаження виокремимо дві групи експертиз, які умовно можна назвати «*спеціальними*» (у межах розслідування конкретних кримінальних правопорушень) і «*загальними*» (звичайні, що призначаються під час розслідування багатьох кримінальних правопорушень).

У межах розслідування кіберзлочинів до «спеціальних» належать такі експертизи, компетенцію яких становлять дослідження механізмів та засобів кібератак і що потребують спеціальних знань у галузі інформаційних технологій, а саме – комп'ютерної техніки й телекомунікацій.

До «загальних» можна віднести всі інші експертизи. Наприклад, дактилоскопічну, об'єктом дослідження якої, зокрема з метою ідентифікації особи за папілярними лініями рук, є сліди пальців, у нашому випадку – з клавіатури комп'ютера, або портретну експертизу, серед основних завдань якої – ідентифікація особи за відеозаписами, скажімо з камер спостереження певного закладу (чи установи), через мережу якого зловмисник вчиняв кібератаку. Слід зазначити, що залежно від предмета дослідження, наприклад історії листування через месенджери смартфона, до «загальних» можна віднести й комп'ютерно-технічну експертизу, оскільки в цьому разі не вивчаються механізми та засоби кібератаки. Потреба в дослідженні листування через месенджери може постати, коли розслідують крадіжки, корупційні або пов'язані з корупцією правопорушення тощо. Водночас, якщо листування містить опис кібератаки, то це вже компетенція експерта, який у межах «спеціальної» експертизи досліджуватиме механізм атаки.

Розглянемо докладніше «спеціальні» експертизи. Для такого дослідження надають об'єкти, що містять:

сліди підготовки до кібератаки;

сліди реалізованої кібератаки (або окремих її етапів), інформацію про наслідки.

Масштабні кібератаки, серед яких APT-атаки (англ. *Advanced Persistent Threat* – постійна загроза підвищеної складності), що становлять різновид складних кібератак із метою отримати несанкціонований доступ до інформаційних систем жертви та забезпечити прихований доступ до неї з метою використання або контролю в майбутньому (Daly, 2009, Nov. 4), зазвичай реалізуються кількома етапами. Кожен із них, зокрема й підготовчий, може бути окремою кібератакою. Сліди таких етапів можна розглядати і як підготовку до кібератаки (у цьому випадку кібератакою вважається фінальний етап), і як окрему кібератаку в низці інших кібератак, що є складовими масштабної кібератаки.

Ще до підготовки до призначення експертизи, як правило, проводять слідчі дії, під час яких вилучають речові докази, що в майбутньому можуть бути надані для дослідження експерту. Так, під час огляду атакованої системи як об'єкти дослідження можуть бути вилучені:

носії інформації або їх клони чи бітові образи;

дампи оперативної пам'яті;

лог-файли служб і додатків;

налаштування логіювання;

файли-звіти діагностичних утиліт;

налаштування роботи діагностичних утиліт;

схеми будови автоматизованих систем, їх об'єднання у кластери, мережі;

схеми внутрішніх мереж (LAN, Local Area Network) і під'єднання до глобальної мережі (WAN, Wide Area Network);

налаштування мережевого обладнання;

налаштування програмного забезпечення (системного, серверного, користувацького) автоматизованої системи, зокрема налаштування віддаленого доступу;

листування електронною поштою – насамперед листи з вкладеними файлами (потенційно шкідливими програмними засобами) або зовнішні посилання (потенційні джерела завантаження шкідливих програмних засобів).

Кожна кібератака має свої особливості. Найбільш типові такі.

Носії інформації атакованої системи (їх клони чи бітові образи) можуть бути основними носіями слідів кібератаки. Їх інформаційний вміст становлять, зокрема:

шкідливі програмні засоби, їх залишки та/або сліди функціонування;

нові файли, які з'явилися на носії під час кібератаки (поміщені на носій зловмисником);

сліди чи залишки знищених під час кібератаки файлів;

зашифровані під час кібератаки файли;

лог-файли, налаштування тощо.

Зазвичай найбільших результатів досягають, коли вилучають бітові образи носіїв інформації. Якщо ці носії відносно невеликого обсягу, на один носій криміналістичної інформації може бути поміщено кілька бітових образів. Переваги методу – оригінальні носії інформації не вилучаються, а автоматизована система, відновившись після кібератаки, може функціонувати далі. Недоліки – створення образів потребує багато часу.

Клонування передбачає побітове копіювання носія інформації на новий або очищений від попередньої інформації інший носій. Інакше під час дослідження може бути виявлена інформація, яка не стосується розслідуваного кримінального правопорушення, а залишилась на носії-реципієнті після його попереднього використання. Переваги методу – дещо більша швидкість порівняно зі створенням образу. Недоліки – необхідність використовувати по одному носію-реципієнту на кожен вихідний носій. Крім того, носій-реципієнт, коли він значно більшого обсягу за вихідний носій, застосовується неоптимально. Приміром, якщо з носія обсягом 100 ГБ зробити клон на носій обсягом 1000 ГБ, буде зайнято тільки 100 ГБ, а решта 900 ГБ залишаться невикористаними. Натомість, якщо в такому самому випадку робити бітові образи, на носії-реципієнті може розміститись дев'ять вихідних носіїв інформації (не десять, оскільки частина інформаційного наповнення диска-реципієнта зайнята службовою інформацію, насамперед файловою системою).

Значно швидшим є вилучення самих вихідних носіїв інформації. Це актуально, якщо час обмежений, а для функціонування ураженої автоматизованої системи таке вилучення некритичне (скажімо, є запасні носії).

Водночас трапляються серверні рішення, у яких застосовуються дуже специфічні носії інформації та/або контролери носіїв інформації (наприклад, апаратні RAID-контролери), які відсутні в експерта і емуляція яких програмними засобами також неможлива. У такому разі, імовірно, доведеться вилучати всю автоматизовану систему.

Дампи оперативної пам'яті атакованої системи можуть містити шкідливі програмні засоби, які не записуються на носій інформації, а існують лише в оперативній пам'яті – так звані резидентні шкідливі програмні засоби (є й нерезидентні шкідливі програми, які крім оперативної пам'яті також записуються на носій інформації комп'ютера). Для створення дампів оперативної пам'яті можна застосувати спеціалізовані утиліти або можливості самої операційної системи, використовуючи скрипти командного рядка. При цьому варто обирати утиліту якнайменшого розміру, оскільки вона, сама завантажуючись до оперативної пам'яті, може витісняти певні важливі дані. Використання скриптів залежить від конкретної операційної системи.

Лог-файли служб і додатків атакованої системи відбивають особливості функціонування цих служб і додатків у різні моменти часу. Якщо логіювання налаштовано правильно, лог-файли відображатимуть усі або більшість змін у нормальній роботі програми, які сталися внаслідок кібератаки. Водночас служби логіювання не завжди налаштовані оптимально, а іноді логіювання взагалі відключене (докладніше про особливості криміналістичного дослідження лог-файлів, зокрема про те, що інформація з лог-файлів використовується адміністраторами для аналізу подій, виявлення помилок, збоїв, зведення статистичних даних, звітування, відстеження дій підозрілих користувачів, вузлів тощо і що саме за допомогою аналізу логів можна встановити, що відбувається, чи відбулося на комп'ютері або в мережі, див.: Nizovtsev, 2013; 2016, s. 8–16).

Якщо автоматизована система функціонує не в штатному режимі (різко знижується продуктивність роботи, спостерігається певна нестабільність тощо) або є збої у роботі мережі, можуть застосовуватися спеціалізовані ***діагностичні утиліти***. Послуговуються ними й коли є підозра щодо збоїв на певному рівні мережевої моделі, що не фіксуються у лог-файлах відповідно до налаштувань системи. Результати роботи цих утиліт можуть бути виведені як на екран, так і в спеціальний файл-звіт. Аналіз файлів-звітів може допомогти локалізувати та діагностувати проблему (Nizovtsev, 2016, s. 8–9).

Лог-файли, якщо вони містять інформацію за значний проміжок часу (тижні, місяці, роки) і про роботу кількох сервісів одночасно, через їх немалий обсяг доцільно копіювати не цілком, а виокремивши фрагмент чи здійснивши вибірку. При цьому в протоколі обов'язково зазначають, якою програмою та за якими параметрами виконувалися ці дії.

З огляду на те, що результати логіювання та роботи діагностичних утиліт значною мірою залежать від їх ***налаштувань***, актуально також зафіксувати ці налаштування, щоб на них зважати у майбутньому під час судової експертизи.

Схеми будови автоматизованих систем, схеми внутрішніх мереж і під'єднання до глобальної мережі, налаштування мережевого обладнання, налаштування програмного забезпечення автоматизованої системи, зокрема налаштування віддаленого доступу, відображають штатне функціонування автоматизованої системи: взаємодію структурних елементів, мережеву маршрутизацію та фільтрацію, методи автентифікації, механізми захисту тощо. Усі ці дані зазвичай необхідні для подальшого відтворення кібератаки, наприклад під час судової експертизи.

Електронна пошта є одним із типових шляхів проникнення шкідливих програм до комп'ютерних систем. Лист може містити шкідливий програмний засіб або посилання на його завантаження. Саме тому листування електронною поштою також слід вилучити та дослідити, насамперед зосередившись на листах, які містять вкладені файли або посилання на зовнішні ресурси.

Під час обшуку помешкання зловмисників насамперед варто звернути увагу на їх комп'ютерні засоби. Так, на носіях інформації можуть бути виявлені вихідні коди шкідливих програм і засоби їх розроблення, самі шкідливі програми та/або їх складові, засоби керування шкідливими програмними засобами, листування зі співучасниками щодо планування кібератаки, інформація з атакованих комп'ютерів тощо. Водночас слід зважати на те, що зловмисники, маючи поглиблені знання в інформаційних технологіях, можуть використовувати технології так званої «контркриміналістики» або «антикриміналістики», щоб протидіяти криміналістичному дослідженню об'єктів, що здійснюють правоохоронні органи. Наприклад, зловмисники можуть вдатися до шифрування носіїв інформації або зберігати всі критично важливі дані у хмарному сховищі.

Коли призначають судові експертизи, дуже важливо правильно сформулювати запитання експерту (перелік запитань у разі втручання в роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні та застосування шкідливих програм див.: Nizovtsev, 2016; 2021). Проте, убачається, згаданий перелік потребує, зокрема, доповнення такими орієнтовними запитаннями, які можуть бути поставлені на вирішення судової експертизи:

Чи є ознаки втручання в роботу телекомунікаційної системи? (*Naukovo-metodychni rekomendatsii*, 1998, rozd. II, hl. 14, p. 14.3), водночас це запитання можна сформулювати й так:

Чи містять надані на дослідження лог-файли (зазначити, які саме) та/чи файли-звіти діагностичних утиліт (зазначити, які саме) ознаки кібератаки? – фактично це базове запитання, оскільки від наявності ознак кібератаки залежить напрям подальшого розслідування. Інакше кажучи: *чи став кіберінцидент наслідком кібератаки або його причиною слугував технічний збій?* Зрозуміло, що в разі виявлення ознак кібератаки розслідування спрямовуватиметься на встановлення кіберзлочинців. Але й за технічного збою може вбачатися склад кримінального правопорушення, адже він міг статися, якщо системний адміністратор неналежно виконує свої обов'язки, а то й свідомо порушує інструкції чи правила налаштування автоматизованої системи. При цьому слід уточнити, чому в описаному запитанні йдеться саме про ознаки кібератаки, а не про встановлення факту. Як уже згадувалось, причиною кіберінциденту може бути технічний збій. Не завжди є можливість достеменно встановити, що мав місце саме технічний збій, особливо якщо такий збій відбувся не на ураженій системі, а зовні. Наприклад, за певної несправності сторонній комп'ютер може масово надсилати повідомлення на мережевий інтерфейс ураженої системи, скажімо, якщо користувач комп'ютера відвідав інтернет-сторінку на ураженій системі, але потім через «залипання» клавіші F5 браузер комп'ютера почав нескінченно оновлювати інтернет-сторінку, здійснюючи фактично віддалену атаку на відмову в обслуговуванні. Звичайно, це може бути також і наслідком свідомих дій користувача – достатньо затиснути клавішу F5 якимось предметом. Технічно в обох випадках відбувається те саме. Але в першому це – технічний збій, без будь-якого умислу користувача. А в другому – умисні протиправні дії користувача. При цьому в лог-файлах ураженої автоматизованої системи не відображається причина натискання клавіші F5 на комп'ютері користувача, фіксується лише інформація про численні запити певної інтернет-сторінки з певного комп'ютера. Саме тому йдеться лише про ознаки кібератаки. Для встановлення факту кібератаки вихідних даних може бути замало. Водночас у певних випадках є можливість встановити саме факт певних подій;

Чи мав місце факт доступу до телекомунікаційної системи та в який спосіб? (*Naukovo-metodychni rekomendatsii*, 1998, rozd. II, hl. 14, p. 14.3) – у цьому разі йдеться про віддалене керування ураженою автоматизованою системою. Таке керування можливе за допомогою штатних засобів операційної системи, як-от: RDP для операційних систем MS Windows (англ. *Remote Desktop Protocol* – протокол віддаленого робочого стола) або SSH для Unix/Linux-подібних операційних систем (англ. *Secure Shell* – «безпечна оболонка»). Крім того, нерідко для віддаленого адміністрування використовують додатки сторонніх розробників: TeamViewer, Radmin, Ammyy Admin тощо. Зловмисники можуть отримати облікові дані для віддаленого доступу за допомогою зазначених вище програмних засобів (наприклад, підбираючи пароль). У такому разі система логіювання (за умови її активації та коректного налаштування) зафіксує вхід під певним обліковим записом у той час, коли справжній користувач до системи не входив. Разом із тим для проникнення до автоматизованих систем зловмисники часто використовують спеціально розроблені шкідливі програмні засоби – так звані бекдори (від англ. *back door* – чорний хід). Коли їх застосовують кіберзлочинці, встановити факт доступу до системи, зокрема час доступу та виконаних дій, не завжди можливо;

Чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб? (*Naukovo-metodychni rekomendatsii*, 1998, rozd. II, hl. 14, p. 14.3) – нерідко кіберзлочинці завантажують на уражену систему додаткові файли (зазвичай для додаткової функціональності, наприклад для віддаленої атаки на відмову в обслуговуванні на іншу систему) або вивантажують певні файли з цієї системи. Інформація про такі дії може залишитись у лог-файлах, наприклад файлі історії командного рядка Unix/Linux-подібних операційних систем.

Наукова новизна

Уточнено перелік запитань, які можуть бути поставлені на вирішення судової експертизи в разі втручання у роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні та застосування шкідливих програм.

Висновки

1. До об'єктів дослідження у межах розслідування кіберзлочинів належать носії інформації або їх клони чи бітові образи; дампи оперативної пам'яті; лог-файли; файли-звіти діагностичних утиліт; налаштування логіювання; налаштування діагностичних утиліт; схеми будови автоматизованих систем і мереж; налаштування обладнання та програмного забезпечення; листування електронною поштою; вихідні коди шкідливих програм та самі шкідливі програми, засоби їх розроблення та адміністрування.

2. Особливості вилучення об'єктів дослідження у межах розслідування кіберзлочинів полягають у тому, що криміналістично значуща інформація вилучається як з атакованих комп'ютерів, так і з комп'ютерів підозрюваних осіб. При цьому слід зважати на те, що зловмисники, як правило, намагаються приховати сліди кібератаки на атакованому комп'ютері, а на власному комп'ютері застосувати заходи «контркриміналістики».

3. Розроблено науково-прикладні рекомендації щодо підготовки та призначення судових експертиз у межах розслідування кіберзлочинів, виявлено перспективні напрями розширення можливостей судової експертизи за грамотного формулювання запитань, які ставляться для її вирішення.

References

Daly, M. K. (2009, Nov. 4). *The Advanced Persistent Threat (or Informationized Force Operations).* USENIX. Uziato z https://static.usenix.org/event/lisa09/tech/slides/daly.pdf.

Diorditsa, I. V. (2020). Poniattia ta zmist kibershpyhunstva. *Naukovi pratsi Natsionalnoho universytetu «Odeska yurydychna akademiia»*, 26, 49–55 [in Ukrainian].
DOI: https://doi.org/10.32837/npnuola.v26i0.660.

Horsman, G. (2021). Contemporaneous notes for digital forensic examinations. *Forensic Science International: Digital Investigation,* 37, 301173.
DOI: https://doi.org/10.1016/j.fsidi.2021.301173.

Instruktsiia pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen v systemi Sluzhby bezpeky Ukrainy: zatv. nakazom Tsentralnoho upravlinnia Sluzhby bezpeky Ukrainy № 371. (2015). Uziato z https://zakon.rada.gov.ua/laws/show/z0738-15#Text [in Ukrainian].

Karafili, E., Cristani, M., & Viganò, L. (2018). A Formal Approach to Analyzing Cyber-Forensics Evidence. In: Lopez, J., Zhou, J., & Soriano, M. (Eds.), *Computer Security.* ESORICS 2018. Lecture Notes in Computer Science, vol. 11098. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-99073-6_14.

Karafili, E., Wang, L., Kakas, A. C., & Lupu, E. (2018). Helping Forensic Analysts to Attribute Cyber-Attacks: An Argumentation-Based Reasoner. In: Miller T., Oren N., Sakurai Y., Noda I., Savarimuthu B., Cao Son T. (Eds.), *PRIMA 2018:*

Principles and Practice of Multi-Agent Systems. PRIMA 2018. Lecture Notes in Computer Science, vol. 11224. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-030-03098-8_36.

Karafili, E., Wang, L., & Lupu, E. C. (2020). An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks. *Forensic Science International: Digital Investigation*, 32, 300925.
DOI: https://doi.org/10.1016/j.fsidi.2020.300925.

Kholostenko, A. V., & Motruk, V. A. (2020). Orhanizatsiino-taktychni osnovy pryznachennia ekspertyz pid chas rozsliduvannia ekonomichnykh zlochyniv. *South Ukrainian Law Journal*, 4, 285–289 [in Ukrainian].
DOI: https://doi.org/10.32850/sulj.2020.4.48.

Kryminalnyi protsesualnyi kodeks Ukrain: Zakon Ukrainy № 4651-VI. (2012). Uziato z https://zakon.rada.gov.ua/laws/show/4651-17#n1191 [in Ukrainian].

Kuleshov, M. V. (2019). Sutnist ta zmist rozsliduvannia kiberintsydentiv ta kiberatak pidrozdilamy SB Ukrainy. *Informatsiia i pravo*, 2 (29), 115–122. Uziato z http://nbuv.gov.ua/UJRN/Infpr_2019_2_15 [in Ukrainian].

Lazebnyi, A. M., & Bozhuk, I. I. (2021). Aktualni pytannia pryznachennia kryminalistychnykh sudovykh ekspertyz v Ukraini. *Aktualni problemy prava: teoriia i praktyka*, 1 (41), 68–76 [in Ukrainian].
DOI: https://doi.org/10.33216/2218-5461-2021-41-1-68-76.

Naukovo-metodychni rekomendatsii z pytan pidhotovky ta pryznachennia sudovykh ekspertyz ta ekspertnykh doslidzhen: zatv. nakazom Ministerstva yustytsii Ukrainy № 53/5. (1998). Uziato z https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

Nizovtsev, Yu. Yu. (2013). Kryminalistychne doslidzhennia avtomatyzovanykh system, shcho piddavalysia viddalenii atatsi na vidmovu v obsluhovuvanni: loh-faily servisiv ta faily-zvity diahnostychnykh utylit yak bezposeredni obiekty doslidzhennia. *Krymynalystyka y sudebnaia ekspertyza*, 58, ch. 2, 452–455 [in Ukrainian].

Nizovtsev, Yu. Yu. (2016). *Sudovo-ekspertne doslidzhennia oznak vtruchannia v robotu informatsiino-telekomunikatsiinykh system shliakhom viddalenykh atak na vidmovu v obsluhovuvanni*: metod. rek. Kyiv: ArtEk. 118 s. [in Ukrainian].

Nizovtsev, Yu. Yu. (2021). *Poshuk ta doslidzhennia shkidlyvykh prohramnykh zasobiv*: metod. rek. Kyiv: ISTE SBU. 192 s. [in Ukrainian].

Ortynskyi, V. (2021). Sutnist ta tsili vykorystannia sudovykh ekspertyz u dosudovomu rozsliduvanni kryminalnoho provadzhennia [The essence and purposes of the use of forensic examinations in the pre-trial investigation of criminal proceedings]. *Visnik Nacionalnogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*, 8 (29), 1–9 [in Ukrainian].
DOI: https://doi.org/10.23939/law2021.29.001.

Polishchuk, V. A. (2018). Osoblyvosti ekspertnoho eksperymentu pid chas provedennia sudovykh kompiuterno-tekhnichnykh ekspertyz. *Kryminalistychnyi visnyk*, 2 (30), 116–121 [in Ukrainian].
DOI: https://doi.org/10.37025/1992-4437/2018-30-2-116.

Pro sudovu ekspertyzu: Zakon Ukrainy № 4038-XII. (1994). Uziato z https://zakon.rada.gov.ua/laws/show/4038-12#Text [in Ukrainian].

Rusetskyi, A. A. (2018). Mistse sudovykh ekspertyz u systemi protydii kiberzahrozam u sferi informatsiinoi bezpeky Ukrainy. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky*, 18, 263–271 [in Ukrainian].
DOI: https://doi.org/10.32353/khrife.2018.29.

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori*: monohrafiia (za zah. red. A. F. Volobuieva). Odesa: TES. 372 s. [in Ukrainian].
DOI: https://doi.org/10.32837/11300.13264.

Shrivastava, G., Gupta, D., & Sharma, K. (2021). *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*. Berlin, Boston: De Gruyter.
DOI: https://doi.org/10.1515/9783110677478.

Symonenko, N. (2020). Osoblyvosti provedennia okremykh sudovykh ekspertyz pid chas rozsliduvannia zlochyniv mynulykh rokiv. *Visnyk Penitentsiarnoi asotsiatsii Ukrainy*, 1, 107–115 [in Ukrainian].
DOI: https://doi.org/10.34015/2523-4552.2020.1.11.

Syvodied, I. S. (2021). Vykorystannia spetsialnykh znan i problemy pryznachennia sudovykh ekspertyz pid chas rozsliduvannia umysnykh ubyvstv viiskovosluzhbovtsiv pid chas provedennia boiovykh dii. *Znannia yevropeiskoho prava*, 4, 176–180 [in Ukrainian].
DOI: https://doi.org/10.32837/chern.v0i4.152.

Torabi, S., Bou-Harb, E., Assi, C., & Debbabi, M. (2020). A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities. *Forensic Science International: Digital Investigation,* 32, Supplement, 300922.
DOI: https://doi.org/10.1016/j.fsidi.2020.300922.

Torabi, S., Dib, M., Bou-Harb, E., Assi, C., & Debbabi, M. (2021). A Strings-Based Similarity Analysis Approach for Characterizing IoT Malware and Inferring Their Underlying Relationships. *IEEE Networking Letters*, 3 (3), 161–165.
DOI: 10.1109/LNET.2021.3076600.

Zhora, V. (2017). Ukrainska hrupa informatsiinoi bezpeky: Kibernastup ne ye nashoiu metoiu, khocha tekhnichno my na noho zdatni. *Interviu z Ukrainy*. Uziato z https://rozmova.wordpress.com/2017/06/28/viktor-zhora/#more-20914 [in Ukrainian].

Список використаних джерел

Daly, M. K. (2009, Nov. 4). *The Advanced Persistent Threat (or Informationized Force Operations).* USENIX. Retrieved from https://static.usenix.org/event/lisa09/tech/slides/daly.pdf.

Діордіца, І. В. (2020). Поняття та зміст кібершпигунства. *Наукові праці Національного університету «Одеська юридична академія»,* 26, 49–55.
DOI: https://doi.org/10.32837/npnuola.v26i0.660.

Horsman, G. (2021). Contemporaneous notes for digital forensic examinations. *Forensic Science International: Digital Investigation,* 37, 301173.
DOI: https://doi.org/10.1016/j.fsidi.2021.301173.

Інструкція про призначення та проведення судових експертиз та експертних досліджень в системі Служби безпеки України: затв. наказом Центрального управління Служби безпеки України № 371. (2015). Узято з https://zakon.rada.gov.ua/laws/show/z0738-15#Text.

Karafili, E., Cristani, M., & Viganò, L. (2018). A Formal Approach to Analyzing Cyber-Forensics Evidence. In: Lopez, J., Zhou, J., & Soriano, M. (Eds.), *Computer Security.* ESORICS 2018. Lecture Notes in Computer Science, vol. 11098. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-319-99073-6_14.

Karafili, E., Wang, L., Kakas, A. C., & Lupu, E. (2018). Helping Forensic Analysts to Attribute Cyber-Attacks: An Argumentation-Based Reasoner. In: Miller T., Oren N., Sakurai Y., Noda I., Savarimuthu B., Cao Son T. (Eds.), *PRIMA 2018: Principles and Practice of Multi-Agent Systems*. PRIMA 2018. Lecture Notes in Computer Science, vol. 11224. Springer, Cham.
DOI: https://doi.org/10.1007/978-3-030-03098-8_36.

Karafili, E., Wang, L., & Lupu, E. C. (2020). An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks. *Forensic Science International: Digital Investigation*, 32, 300925.
DOI: https://doi.org/10.1016/j.fsidi.2020.300925.

Холостенко, А. В., & Мотрук, В. А. (2020). Організаційно-тактичні основи призначення експертиз під час розслідування економічних злочинів. *South Ukrainian Law Journal,* 4, 285–289.
DOI: https://doi.org/10.32850/sulj.2020.4.48.

Кримінальний процесуальний кодекс України: Закон України № 4651-VI. (2012). Узято з https://zakon.rada.gov.ua/laws/show/4651-17#n1191.

Кулешов, М. В. (2019). Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України. *Інформація і право*, 2 (29), 115–122. Узято з http://nbuv.gov.ua/UJRN/Infpr_2019_2_15.

Лазебний, А. М., & Божук, І. І. (2021). Актуальні питання призначення криміналістичних судових експертиз в Україні. *Актуальні проблеми права: теорія і практика***,** 1 (41), 68–76.
DOI: https://doi.org/10.33216/2218-5461-2021-41-1-68-76.

Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень: затв. наказом Міністерства юстиції України № 53/5. (1998). Узято з https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

Нізовцев, Ю. Ю. (2013). Криміналістичне дослідження автоматизованих систем, що піддавалися віддаленій атаці на відмову в обслуговуванні: лог-файли сервісів та файли-звіти діагностичних утиліт як безпосередні об'єкти дослідження. *Криминалистика и судебная экспертиза*, 58, ч. 2, 452–455.

Нізовцев, Ю. Ю. (2016). *Судово-експертне дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні:* метод. рек. Київ: АртЕк. 118 с.

Нізовцев, Ю. Ю. (2021). *Пошук та дослідження шкідливих програмних засобів:* метод. рек. Київ: ІСТЕ СБУ. 192 с.

Ортинський, В. (2021). Сутність та цілі використання судових експертиз у досудовому розслідуванні кримінального провадження [The essence and purposes of the use of forensic examinations in the pre-trial investigation of criminal proceedings]. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki,* 8 (29), 1–9.
DOI: https://doi.org/10.23939/law2021.29.001.

Поліщук, В. А. (2018). Особливості експертного експерименту під час проведення судових комп'ютерно-технічних експертиз. *Криміналістичний вісник*, 2 (30), 116–121.
DOI: https://doi.org/10.37025/1992-4437/2018-30-2-116.

Про судову експертизу: Закон України № 4038-XII. (1994). Узято з https://zakon.rada.gov.ua/laws/show/4038-12#Text.

Русецький, А. А. (2018). Місце судових експертиз у системі протидії кіберзагрозам у сфері інформаційної безпеки України. *Теорія та практика судової експертизи і криміналістики*, 18, 263–271.
DOI: https://doi.org/10.32353/khrife.2018.29.

Самойленко, О. А. (2020). *Основи методики розслідування злочинів, вчинених у кіберпросторі:* монографія (за заг. ред. А. Ф. Волобуєва). Одеса: ТЕС. 372 с.
DOI: https://doi.org/10.32837/11300.13264.

Shrivastava, G., Gupta, D., & Sharma, K. (2021). *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*. Berlin, Boston: De Gruyter.
DOI: https://doi.org/10.1515/9783110677478.

Симоненко, Н. (2020). Особливості проведення окремих судових експертиз під час розслідування злочинів

минулих років. *Вісник Пенітенціарної асоціації України*, 1, 107–115.
DOI: https://doi.org/10.34015/2523-4552.2020.1.11.

Сиводєд, І. С. (2021). Використання спеціальних знань і проблеми призначення судових експертиз під час розслідування умисних убивств військовослужбовців під час проведення бойових дій. *Знання європейського права*, 4, 176–180.
DOI: https://doi.org/10.32837/chern.v0i4.152.

Torabi, S., Bou-Harb, E., Assi, C., & Debbabi, M. (2020). A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities. *Forensic Science International: Digital Investigation,* 32, Supplement, 300922.
DOI: https://doi.org/10.1016/j.fsidi.2020.300922**.**

Torabi, S., Dib, M., Bou-Harb, E., Assi, C., & Debbabi, M. (2021). A Strings-Based Similarity Analysis Approach for Characterizing IoT Malware and Inferring Their Underlying Relationships. *IEEE Networking Letters*, 3 (3), 161–165.
DOI: 10.1109/LNET.2021.3076600.

Жора, В. (2017). Українська група інформаційної безпеки: Кібернаступ не є нашою метою, хоча технічно ми на нього здатні. *Інтерв'ю з України.* Узято з https://rozmova.wordpress.com/2017/06/28/viktor-zhora/#more-20914.

Стаття надійшла до редакції 11.10.2021

Yu. Nizovtsev, *PhD (Law),*
Leading Researcher of the Research Laboratory
of the Center for Forensic and Special Expertise,
Ukrainian Scientific and Research Institute
of Special Equipment and Forensic Expertise
of the Security Service of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-7641-6403
email: nizovtsev.yurii@gmail.com
O. Omelian, *Postgraduate Student,*
National Academy of the Security
Service of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-4495-7835
email: omelan_ssu@ukr.net

ON THE PREPARATION AND APPOINTMENT OF FORENSIC EXPERTISE WITHIN THE INVESTIGATION OF CRIMINAL OFFENSES RELATED TO CYBERATRAKS

The purpose of the article is to scientifically substantiate the theoretical principles of preparation and appointment of forensic expertise within the investigation of criminal offenses related to cyberattacks, to form appropriate scientific and applied recommendations. ***Methodology***. The reliability of the obtained results and conclusions are ensured by a set of methods of general scientific and specific scientific levels. In particular, the main is the general dialectical method of scientific knowledge of phenomena, processes and objects, as well as modeling and forecasting, formal-logical, system-structural methods. ***Scientific novelty***. The list of questions that can be put to a forensic expertise in case of interference in the work of information and telecommunications systems through remote attacks on denial of service and the use of malicious software has been clarified. ***Conclusions***. It was stated that the objects of research in the investigation of cybercrime include media or their clones or bit images; RAM dumps; log files; diagnostic utility report files; login settings; setting up diagnostic utilities; schemes of structure of automated systems and networks; hardware and software settings; email correspondence; source code of malicious programs and the most malicious programs, means of their development and administration. The peculiarities of the seizure of research objects within the framework of the investigation of cybercrimes, which consist in the fact that forensically significant information is seized both from the computers under attack and from the computers of the suspects, are highlighted. It should be borne in mind that cybercriminals, as a rule, try to hide the traces of a cyberattack on the attacked computer, and take «countercriminalistic» measures on their own computer. Scientific and applied recommendations for the preparation and appointment of forensic expertise in the framework of investigating cybercrimes have been developed, promising directions for expanding the possibilities of forensic expertise have been identified with a competent formulation of the questions that are posed for its solution.

Keywords: forensic expertise; computer and technical expertise; telecommunication expertise; informational security; cyber threat; cybercrime; cyberattack; cyber incident; malicious software; log file.

Ю. Ю. Низовцев, *кандидат юридических наук,*
ведущий научный сотрудник научно-
исследовательской лаборатории
Центра судебных и специальных экспертиз,
Украинский научно-исследовательский інститут
специальной техники и судебных экспертиз
Службы безопасности Украины, г. Киев
ORCID: https://orcid.org/0000-0002-7641-6403
email: nizovtsev.yurii@gmail.com
А. С. Омельян, *аспирант,*
Национальная академия
Службы безопасности Украины, г. Киев
ORCID: https://orcid.org/0000-0003-4495-7835
email: omelan_ssu@ukr.net

О ПОДГОТОВКЕ И НАЗНАЧЕНИИ СУДЕБНЫХ ЭКСПЕРТИЗ В РАМКАХ РАССЛЕДОВАНИЯ КРИМИНАЛЬНЫХ ПРАВОНАРУШЕНИЙ, СВЯЗАННЫХ С КИБЕРАТАКАМИ

Цель статьи – научно обосновать теоретические основы подготовки и назначения судебных экспертиз в рамках расследования криминальных правонарушений, связанных с кибератаками, сформировать соответствующие научно-прикладные рекомендации. ***Методология***. Достоверность полученных результатов и выводов обеспечены совокупностью методов общенаучного и конкретно-научного уровней. В частности, основным является общий диалектический метод научного познания явлений, процессов и объектов, а также моделирование и прогнозирование, формально-логический, системно-структурный методы. ***Научная новизна***. Уточнен перечень вопросов, которые могут быть поставлены на решение судебной экспертизы в случае вмешательства в работу информационно-телекоммуникационных систем путем удаленных атак на отказ в обслуживании и применения вредоносных программ. ***Выводы***. Констатировано, что к объектам исследования в рамках расследования киберпреступлений принадлежат носители информации или их клоны или битовые образы; дампы оперативной памяти; лог-файлы; файлы-отчеты диагностических утилит; настройки логирования; настройки диагностических утилит; схемы построения автоматизированных систем и сетей; настройки оборудования и программного обеспечения; переписка электронной почтой; исходные коды вредоносных программ и сами вредоносные программы, средства их разработки и администрирования. Выделены особенности изъятия объектов исследования в рамках расследования киберпреступлений, которые состоят в том, что криминалистически значимая информация изымается как из атакованных компьютеров, так и из компьютеров подозреваемых лиц. При этом следует учитывать, что злоумышленники, как правило, пытаются скрыть следы кибератаки на атакованном компьютере, а на своем компьютере применить средства «контркриминалистики». Разработаны научно-прикладные рекомендации о подготовке и назначении судебных экспертиз в рамках расследования киберпреступлений, выявлены перспективные направления расширения возможностей судебной экспертизы при грамотном формулировании вопросов, которые ставятся на ее решение.

Ключевые слова: судебная экспертиза; компьютерно-техническая экспертиза; телекоммуникационная экспертиза; информационная безопасность; киберугроза; киберпреступление; кибератака; киберинцидент; вредоносные программные средства; лог-файл.