УДК 004.056

Л.О. Майданевич
М. Б. Тарасюк

КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА: ОСНОВНІ АСПЕКТИ ПІДГОТОВКИ ДО ПРОВЕДЕННЯ

Вінницький національний технічний університет

Анотація

В доповіді розглянуто основні аспекти підготовки до проведення комп'ютерно-технічної експертизи. Доведено, що ефективне розслідування кіберзлочинів потребує проведення комп'ютерно-технічної експертизи, оскільки кіберзлочинці постійно вдосконалюють методи протидії криміналістичному аналізу. З'ясовано, що впровадження «антикриміналістичних дій» ускладнює процес збору та аналізу електронних доказів. Вирішення цієї проблеми можливе шляхом залучення спеціалістів на ранніх етапах розслідування, забезпечення належних процедур фіксації та передачі електронних доказів на експертизу. Недотримання цих заходів може призвести до активації «антикриміналістичних технологій», що значно ускладнить доступ до ключових доказів або зробить його неможливим.

Ключові слова*: кіберпростір, розслідування кіберзлочинів, комп'ютерно-технічна експертиза, електронні докази.*

Abstract

This report examines the main aspects of preparation for conducting a computer-technical examination. It is proven that effective investigation of cybercrimes requires conducting a computer-technical examination, since cybercriminals are constantly improving methods of counteracting forensic analysis. It is found that the introduction of anti-forensic measures complicates the process of collecting and analyzing electronic evidence. This problem can be resolved by involving specialists at the early stages of the investigation, ensuring proper procedures for recording and transferring electronic evidence for examination. Failure to comply with these measures may lead to the activation of anti-forensic technologies, which will significantly complicate access to key evidence or make it impossible.

Keywords: *cyberspace, investigation of cybercrimes, computer-technical examination, electronic evidence.*

Вступ

Сучасні методи криміналістики відіграють ключову роль у протидії кіберзлочинності. Використання результатів експертиз та міжнародна кооперація допомагає правоохоронним органам оперативно реагувати на нові загрози у сфері кібербезпеки. Так, комп'ютерно-технічна експертиза є невід'ємною у процесі досудового розслідування кіберзлочинів. Її проведення дозволяє встановити природу, статус об'єкта посягання в кіберпросторі, детально проаналізувати технічні та функціональні аспекти тощо. Водночас, кіберзлочинці все більше використовують «антикриміналістичні методи» (видалення, приховування та в інший способів перешкоджання відшукання та оброблення електронних доказів при проведенні комп'ютерно-технічної експертизи), і це є викликом.

Результати дослідження

Кіберзлочинці постійно вдосконалюють свої методи та тактики приховання «слідів», застосовуючи новітні технології, зокрема штучний інтелект, машинне навчання та блокчейн. Це дає їм змогу створювати нові види атак, які складно виявити та знешкодити. Додаткові труднощі у розкритті злочинів створює використання анонімайзерів, VPN-сервісів і методів шифрування, які ускладнюють встановлення особи правопорушника. Крім того, злочинці можуть застосовувати ботнети як посередників для приховування своєї діяльності, що значно ускладнює їхню ідентифікацію та притягнення до відповідальності.

Дослідження «антикриміналістичних методів» є нагальною науковою проблемою. Насамперед, вона обумовлена тим, що в сфері «антифорензики» постійно розробляються нові «організаційно-технічні засоби та методи» протистояння законодавчим процедурам у розслідуванні кіберзлочинів. Ці способи протистояння не мають чіткої та уніфікованої класифікації. Водночас, незважаючи на це, можна виокремити основні підходи та методи, що використовуються в «антифорензичній

діяльності», які мають значний вплив на процес збору та аналізу електронних (цифрових) доказів: 1) приховування даних; 2) знищення артефактів; 3) заплутування слідів; 4) атаки на процес або інструменти комп'ютерної експертизи [1].

Приховування даних: стеганографія (від грецького слова «приховане письмо») є методом приховування інформації, часто шляхом маскування файлів як інші типи даних; цей метод використовується для уникнення виявлення, зокрема, шляхом приховування файлів у системних чи незайнятих областях жорстких дисків, а також в метаданих різних типів файлів; дані можуть бути приховані у звукових файлах, зображеннях або текстах, що ускладнює автоматичне виявлення за допомогою інструментів комп'ютерно-технічної експертизи [2].

Знищення артефактів: видалення артефактів включає в себе методи очищення або змінювання слідів, залишених в ЕОМ; це може включати зміну або видалення файлів журналів, зміну дат файлів, а також видалення інформації з серверів чи системних подій; використання таких інструментів, як Timestamp і Transmogrify, дозволяє маніпулювати даними таким чином, щоб приховати їх реальний характер і ввести в оману [3].

Заплутування слідів: дії які спрямовані на ускладнення ефективного процесу комп'ютерно-технічної експертизи, використовуючи методи, такі як підробка логів, використання зомбі-акаунтів та підміна команд [3]; наприклад, інструменти Transmogrify, дозволяють змінювати заголовки файлів, що призводить до їх помилкового трактування під час пошуку, ускладнюючи виявлення справжніх даних [4].

Атаки на процес або інструменти комп'ютерної експертизи: атаки на цілісність хешів, що використовуються для перевірки цілісності образів дисків (зокрема, це відбувається під час підготовки та процесу проведення комп'ютерно-технічної експертизи); спеціалізовані скрипти можуть маніпулювати файловими системами, змінюючи вміст файлів або підписів, що викликає сумнів у правдивості зібраних доказів [3].

Таблиця 1 – Основні аспекти протистояння щодо відшукання та оброблення електронних доказів при розслідуванні кіберзлочинів [4, 5]

Експертиза (основні акценти)	**Антикриміналістична діяльність**
Відновлення видалених файлів	Надписування даних, використання безпечного видалення (Wipe), шифрування перед видаленням
Журнали подій та системні логи	Видалення логів, підміна записів, використання log-cleaner
Файлові метадані (часові мітки, авторство тощо)	Маніпуляція часовими мітками (Timestomp), видалення метаданих
Аналіз файлових систем (FAT, NTFS, ext тощо)	Приховування даних у незайнятих секторах, зміна файлових заголовків (Transmogrify)
Стеганографічний аналіз	Використання вдосконалених алгоритмів стеганографії, приховування у малопомітних носіях даних
Криптографічний аналіз (розшифрування даних)	Використання сильного шифрування (AES, RSA), приховування ключів, шифрування з автознищенням
Аналіз мережевого трафіку	Використання VPN, TOR, проксі-серверів, шифрування трафіку
Хешування та контроль цілісності	Маніпуляція контрольними сумами, додавання шуму до файлів, атаки на хеш-функції
Аналіз RAM та дамп пам'яті	Шифрування оперативної пам'яті, використання антивідладкових технік, очищення пам'яті перед вимкненням
Віртуалізація та аналіз образів системи	Використання rootkits, приховування активності у гостьових ОС

Висновки

Ефективне розслідування кіберзлочинів передбачає проведення комп'ютерно-технічної експертизи в ході розслідування. Водночас, в сфері «антикриміналістичної діяльності» постійно розробляються нові «організаційно-технічні засоби та методи» протистояння щодо відшукання, фіксації та подальшого оброблення інформації (електронних доказів). Цю проблему можна вирішити шляхом своєчасного залучення спеціалістів (на стадії підготовки до призначення експертизи) та вчинення всіх необхідних дій щодо відшукання, фіксації та передачу на експертизу електронних доказів, оскільки недотримання належних процедур може спровокувати активацію антифорензичних засобів, що ускладнить або навіть унеможливить доступ до важливих цифрових доказів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Anti–computer forensics. Wikipedia. https://en.wikipedia.org/wiki/Anti%E2%80%93computer_forensics
2. Комп'ютерна стеганографія : навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець. Вінниця : ВНТУ, 2017. 155с.
3. Rogers, D. M. (2005). Anti-Forensic Presentation given to Lockheed Martin. San Diego. : https://www.researchgate.net/profile/Marcus_Rogers/publication/268290676_Anti-Forensics_Anti-Forensics/links/575969a908aec91374a3656c.pdf?__cf_chl_tk=aP3h4wZ3eDLpwg3gW6V_pzsr3LkOMs5.m0bL9b9ducc-1742374543-1.0.1.1-QiWBoQytKoF0cSq_suEiNm4Vak0ndnOVWdG2fKkyNVc
4. Berinato, S. (2007). The Rise of Anti Forensics. CSO (Jun 08, 2007): https://www.csoonline.com/article/521254/investigations-forensics-the-rise-of-anti-forensics.html
5. Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник / Л.О. Майданевич, О.П.Войтович, Г.В.Шелепало. Вінниця : ВНТУ, 2025. 117с.

Майданевич Леонід Олександрович – канд. філос. наук, старший викладач кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Тарасюк Микола Борисович – студент групи 1БС-24М кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, м. Вінниця, e-mail: tarasyuk.m12@gmail.com

Maidanevych Leonid – Candidate of Philosophical Sciences, Senior Lecturer, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com

Tarasiuk Mykola – Student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, email: tarasyuk.m12@gmail.com