РЯСОВ АЛЕКСАНДР АЛЕКСЕЕВИЧ
Ставропольский филиал Краснодарского университета МВД России
(Ставрополь, Россия)
identifiks@mail.ru

Способы обнаружения и исследования скрытой информации на электронных носителях

Аннотация. Современные технологии позволяют хранить огромные объемы информации на различных носителях данных, начиная от жестких дисков и USB-накопителей и заканчивая облачными сервисами. С развитием технологий и расширением возможностей хакеров и киберпреступников защита конфиденциальных данных становится все более сложной задачей. В этой связи люди все чаще задаются вопросом о необходимости сокрытия на электронных носителях конфиденциальной информации от посторонних глаз, которыми могут являться как близкие родственники, так и преступники. Для этого, исходя из уровня своей компьютерной грамотности, они осваивают все новые и новые способы сокрытия информации. Не остаются в стороне и преступники, которым действительно есть, что скрывать.

Данные обстоятельства диктуют новые, повышенные требования к сотрудникам правоохранительных органов не только по изучению способов сокрытия информации, но и к способам ее обнаружения.

Стоить отметить, что данный вопрос является очень узким и требующим специальных познаний в области как компьютерной техники, так и организации хранения файлов на электронных носителях. Проблему поиска скрытой информации отчасти затрагивали такие авторы, как: Л.А. Бураева [1], В.А. Гаужаева [2], Р.Р. Карданов [3], О.П. Грибунов [4], Н.С. Зиновьева [5] и др. Однако в этом направлении делается лишь попытка привлечь внимание к данному вопросу, но полноценных работ, посвященных его рассмотрению, практически нет.

Ключевые слова и словосочетания: информация, сокрытие компьютерной информации, поиск скрытой компьютерной информации, расследование преступлений, компьютерная экспертиза, компьютерно-техническая экспертиза, стеганография, криптоконтейнеры, восстановление удаленной компьютерной информации

Для цитирования: *Рясов А. А. Способы обнаружения и исследования скрытой информации на электронных носителях // Вестник ВИПК МВД России. – 2024. – № 4 (72). – С. 78-83; doi: 10.29039/2312-7937-2024-4-78-83*

RYASOV ALEXANDER A.
Stavropol branch of Krasnodar University of the Ministry of Internal Affairs of Russia
(Stavropol, Russia)

METHODS OF DETECTING AND RESEARCHING HIDDEN INFORMATION ON ELECTRONIC MEDIA

Annotation. Modern technologies allow you to store huge amounts of information on various data carriers, ranging from hard drives and USB drives, and ending with cloud services. With the development of technology and the expansion of the capabilities of hackers and cybercriminals, the protection of confidential data is becoming an increasingly difficult task. In this regard, people are increasingly wondering about the need to hide confidential information on electronic media from prying eyes, which may be both close relatives and criminals. In order, based on their level of computer literacy, they master more and more new ways of hiding information. Criminals who really have something to hide do not stay away from this issue either.

These circumstances dictate new and increased requirements for law enforcement officers not only to study ways to conceal information, but also to ways to detect it.

It is worth noting that this issue is very narrow and requires special knowledge in the field of both computer technology and the organization of file storage on electronic media. This issue was partially addressed by individual authors such as: L.A. Buraeva [1], V.A. Gauzhaeva [2], R.R. Kardanov [3], O.P. Gribunov [4], N.S. Zinovieva [5] and others. However, they only made an attempt to draw attention to this issue, but there are practically no full-fledged works devoted to its consideration.

Key words and word combinations: information, concealment of computer information, search for hidden computer information, crime investigation, computer expertise, computer-technical expertise, encryption, encryption, steganography, cryptographic containers, recovery of deleted computer information

For citation: *Ryasov A. A. Methods of detecting and researching hidden information on electronic media // Vestnik Advanced Training Institute of the MIA of Russia. – 2024. – № 4 (72). – P. 78-83; doi: 10.29039/2312-7937-2024-4-78-83*

Современные технологии передачи данных позволяют осуществлять удаленное взаимодействие между участниками преступной деятельности, безопасно передавать и хранить сведения о подготовке, совершении и сокрытии преступлений, что предопределяет увеличение числа неочевидных преступлений и позволяет избегать ответственности за совершенные преступные деяния в силу сложностей установления лиц, причастных к их совершению. Сведения, распространяемые посредством информационно-коммуникационных технологий, являются источником криминалистически значимой информации о преступлении, обнаружение, изъятие и исследование которой является необходимым условием для закрепления доказательств в ходе расследования. Несмотря на целенаправленную выработку правоохранительными органами мер противодействия преступным проявлениям в информационно-телекоммуникационной среде, наблюдается рост отдельной категории рассматриваемых преступлений.

С развитием возможностей хранения и передачи данных возникают все новые способы скрытой передачи информации, как в цифровом, так и в физическом виде. В связи с чем сегодня особую актуальность у правоохранителей приобретает задача по развитию методов обнаружения и исследования скрытой информации для расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Особую значимость приобретает данный вопрос в связи с катастрофической нехваткой кадров во всех сферах системы МВД, о чем заявляет даже Владимир Колокольцев [6], и особенно в области компьютерной безопасности. Несмотря на то, что в соответствии с ч. 2 ст. 164.1 УПК РФ изъятие электронных носителей осуществляется с участием специалиста на основании соответствующего постановления следователя, на практике осуществить данное положение далеко не всегда представляется возможным, именно по вышеуказанной причине. Познания в данной области, по нашему

мнению, должны постепенно выходить из области специальных и становиться общедоступными. В этой связи возникает необходимость реформирования системы подготовки кадров для системы МВД России, которое позволит сотрудникам следствия и дознания самостоятельно выявлять удаленные файлы, закодированные данные, скрытые разделы на жестком диске и другую информацию, которая может быть ключевой в проведении расследования.

При помощи данных способов обнаружения скрытой информации можно установить мотивы и методы преступников, выявить связи между различными событиями и даже предотвратить дальнейшие атаки и преступления.

Исследование скрытой информации на носителях данных позволяет выявлять угрозы для безопасности и принимать меры по их предотвращению. Такие методы обнаружения могут включать в себя анализ цифровых следов, проверку метаданных, использование специализированного программного обеспечения и оборудования, криптоанализ и другие технологии.

Поэтому изучение и разработка новых способов обнаружения и исследования скрытой информации на носителях данных является важной задачей для специалистов в области информационной безопасности, кибернетики и криптографии.

Однако, для того чтобы рассматривать проблемы выявления сокрытой информации, требуются знания о способах ее сокрытия. Полный перечень таковых назвать очень трудно из-за их многообразия. Выбор конкретного способа зависит от уровня познаний лица, его применяющего, от вида и степени секретности скрываемой информации. К основным таким способам можно отнести следующие:

1. Наиболее простым способом сокрытия является перемещение данных в один из системных каталогов, например «C:\Windows\System32\Com\dmp» или «C:\Users\Admин\AppData\Local\Temp_avast_\unp_low». Основная цель в таких случаях – спрятать информацию там, где ее никто не будет искать. Однако такой способ чаще всего выбирают дилетанты, т.к. для специалиста найти спрятанную информацию не составит труда, если, конечно, он знает, что хочет найти. Достаточно использовать простой запрос по маске расширения файлов.

2. Другим способом сокрытия может являться сокрытие данных в архиве «zip, rar и др.». Выявить такую информацию можно тем же способом, однако сложности могут возникнуть, если на архив был предварительно установлен пароль. В таком случае при обнаружении архива мы можем посмотреть его содержимое (название каталогов, папок, типы файлов, их размер), однако для открытия самих файлов потребуется пароль, получить который можно у его создателя или попробовать подобрать его по словарю либо простым перебором. С этой целью используется специальное программное обеспечение «PassFab for RAR», набор программ от компании «ElcomSoft», разработавшей целую линейку программного обеспечения для подбора паролей под различные типы файлов, либо иную подобную программу. Успех подбора пароля во многом будет зависеть от мощности компьютера, на котором будет подбираться пароль, и от того, какими правилами создания криптостойких паролей пользовался его автор. Для подбора пароля при помощи вышеуказанных программ может потребоваться от нескольких минут до нескольких десятков лет.

Стоит сразу отметить еще одну проблему, с которой могут столкнуться правоохранители при работе с иностранным программным обеспечением. В большинстве случаев это отсутствие лицензий на использование таких программных продуктов в связи с введением санкций в отношении Российской Федерации со стороны некоторых иностранных государств. Если для сотрудников органов дознания при проведении ими оперативно-розыскных мероприятий это не столь существенно, т.к. к большинству из них можно найти нелицензионные ключи, то для экспертов, проводящих экспертизы, использование такого программного обеспечения недопустимо. Им приходится искать аналоги от российских компаний либо обращаться в частные

экспертные организации, у которых есть возможность приобрести такие ключи в обход санкций.

3. Еще одним из простых способов сокрытия файлов может быть переименование имени или атрибутов скрываемого файла. Например, создание не привлекающего внимания имени файла, изменение расширения файла, изменение атрибутов файла с пометкой скрытого файла. При этом в системе должен быть установлен параметр «не показывать скрытые файлы и папки». Такой способ может также сочетаться с вышеописанными способами сокрытия. Противодействием такому сокрытию может быть поиск по содержимому, по дате и другим атрибутам.

4. Достаточно простым способом сокрытия информации является создание на рабочем столе невидимого каталога. С этой целью папку на рабочем столе необходимо переименовать в 255 при нажатом ALT. При этом имя папки будет пустым. А иконку папки сменить на пустую картинку. Таким образом папка становится визуально невидимой. Однако если мы, удерживая кнопку мыши, выделим всю область рабочего стола, то данная папка также выделяется и становится видимой. Видимой она также будет и при просмотре содержимого рабочего стола через файловые менеджеры.

5. Очередным, достаточно эффективным, хотя и опасным для содержимого скрываемых данных, может быть удаление скрываемых файлов и папок. Не секрет, что при удалении файлов они не исчезают с диска. Местонахождение удаленного файла на диске система помечает как свободное для записи, и при использовании соответствующего программного обеспечения, предназначенного для восстановления удалённых данных, они могут быть без труда восстановлены. Правда, при этом есть риск того, что место на диске, где находился удаленный файл, может быть перезаписано другими данными операционной системы или пользователем. Данный метод сокрытия не станет проблемой не только для эксперта, но и для любого пользователя, обладающего минимальными знаниями по восстановлению удаленных данных. Программ для восстановления удаленной информации разработано огромное множество. Наибольшую популярность у пользователей приобрели такие как «R-Studio», «Recuva», «Hetman Partition Recovery» и др.

В том случае, если следствие интересуют фото- либо видеофайлы, которые открывались на осматриваемом компьютере, существенную помощь может оказать использование программы «ThumbnailExpert», предназначенной для поиска эскизов графических файлов. Далеко не все знают, что просматриваемые нами картинки или видеофайлы сохраняют свои эскизы в уменьшенном разрешении в папке «C:\Users\Admin\AppData\Local\Microsoft \Windows\Explorer» в файлах «thumbcache_96.db» либо в файлах с другими цифрами вместо 96. Данная цифра обозначает разрешение хранящихся в них эскизов. Найденные на исследуемом компьютере эскизы позволят доказать, что на нем открывались фото поддельных или украденных банковских карт, с детской порнографией, местами закладок наркотических средств и т.д. Причем сделать это можно даже в том случае, если файлы находились на отсутствующем на момент исследования электронном носителе или были безвозвратно уничтожены.

6. Сокрытие данных в скрытых от операционной системы логических дисках также не представляет особой сложности в их выявлении. Наибольшую популярность для этих целей приобрели такие программы, как «Hidden Disk», «Secret Disk» и др., а также стандартные утилиты Windows. Однако используемое экспертами при анализе электронных носителей программное обеспечение позволяет без труда обнаружить и извлечь их содержимое.

7. Стеганография является еще одним методом сокрытия данных на электронных носителях. Стеганография представляет собой метод сокрытия информации внутри другой информации таким образом, чтобы никто, кроме получателя, не мог даже подозревать о наличии скрытых данных. Одним из способов использования

стеганографии для сокрытия компьютерных данных является внедрение информации в графические, видео- или звуковые файлы.

Например, можно скрыть текстовое сообщение или картинку внутри другого изображения, изменив значения пикселей таким образом, чтобы невооруженный глаз не мог заметить изменений, но при этом получатель сможет извлечь скрытую информацию с помощью специального программного обеспечения. Также данные можно скрыть в аудио- и видеофайлах путем изменения частот, видеопотока или громкости звуковых сигналов.

Для сокрытия данных при помощи стеганографии разработано множество программ: S-Tools, OpenPuff, OpenStego, RedJPEG deepsound-2-0-en-win, ImageSpyer и др. OpenPuff позволяет не только скрывать текст или одно изображение внутри другого, но и устанавливать пароль на извлечение и даже делать контейнер с двойным дном, когда при вводе одного пароля извлекается один файл, а при вводе другого пароля извлекается другой.

Стоит признаться, что стеганография является достаточно эффективным методом сокрытия данных, однако в арсенале экспертов есть и меры его преодоления, к которым можно отнести в первую очередь выявление косвенных признаков, свидетельствующих о стеганографии, например наличие на компьютере установленного, либо следов установки, либо инсталляционных пакетов специального программного обеспечения для осуществления стеганографии. Кроме того, существуют и программные средства поиска стеганоконтейнеров, такие как StegoHunt MP, Stegdetect и др.

К примеру, программа Stego Watch анализирует набор файлов и с большой вероятностью определяет, какие из них являются носителями стеганографии, вероятный алгоритм, используемый для сокрытия (который, в свою очередь, дает подсказки относительно наиболее вероятного используемого программного обеспечения). В анализе используются различные выбираемые пользователем статистические тесты, основанные на характеристиках файла-носителя, которые могут быть изменены различными методами стеганографии. Знание программного обеспечения для стеганографии, доступного на компьютере подозреваемого, поможет аналитику выбрать наиболее вероятные статистические тесты.

Наиболее простым и не требующим специального программного обеспечения вариантом стеганографии может быть сокрытие текста внутри другого текста. Так, например, в текстовом документе, созданном при помощи программы Microsoft Word, можно сокрыть текст в колонтитулах или в самом тексте, применив к нему размер шрифта № 1 и обесцветив его. Однако при конвертировании данного документа в формат .txt все эти ухищрения будут нивелированы.

8. Наиболее эффективным с точки зрения безопасности и в то же время наиболее сложным с точки зрения форензического анализа является использование для сокрытия данных закодированных файлов, дисков или криптоконтейнеров.

Закодированные файлы – это файлы, которые были преобразованы с использованием специальных алгоритмов кодирования, таких как AES, RSA или др. Кодирование делает данные недоступными для прочтения без специального ключа, который нужен для декодирования информации.

Криптоконтейнерами называются специальные файловые контейнеры, которые могут содержать закодированные файлы и папки. Проще говоря, это файл, в котором можно разместить огромное количество других файлов, нечто вроде файлового архива, для открытия которого нужны специальное программное обеспечение и знание пароля.

Для создания криптоконтейнеров можно использовать специальные программы, такие как TrueCrypt, VeraCrypt, BitLocker. Эти программы предлагают различные методы кодирования и настройки безопасности, позволяя выбрать наиболее подходящий вариант для защиты данных.

Данные программы позволяют создавать как отдельные файловые контейнеры, так и контейнеры с двойным дном, когда при вводе одного пароля открывается одно его

содержимое, а при вводе другого открывается закодированная часть. Кроме того, вышеуказанные программы позволяют кодировать целые диски.

Стоит отметить, что криптоконтейнеры очень тяжело обнаружить, так как их можно маскировать под любой тип файла и внешне они ничем не будут выделяться среди других таких же файлов. При грамотном выборе пароля для контейнера шансов подобрать его практически нет. Наиболее предпочтительными способами выяснить настоящий пароль являются методы социальной инженерии и тактические приемы, применяемые сотрудниками органа дознания.

Однако нельзя сказать, что экспертно-криминалистические методы тут бессильны. В распоряжении специалистов имеется программное обеспечение для поиска ключей кодирования и декодирования криптоконтейнера, которое предоставляет возможность восстановить доступ к закодированным данным.

К числу наиболее популярных программных продуктов для поиска ключей кодирования и декодирования криптоконтейнера можно отнести: Passware Kit Forensic, Elcomsoft Forensic Disk Decryptor, John the Ripper и Hashcat. Перечисленные программы поддерживают широкий спектр форматов криптоконтейнеров: TrueCrypt, BitLocker, FileVault и др. Данные инструменты позволяют проводить атаки на различные типы кодирования, включая DES, MD5, SHA-1 и др.

Однако применение этих программных продуктов занимает очень много времени и, как мы уже говорили, при грамотном выборе кодировщиком пароля результат их применения не гарантирован.

Значительную помощь в процессе поиска скрытой информации могут оказать знания о косвенных признаках, свидетельствующих о тех или иных способах ее сокрытия.

К числу косвенных признаков сокрытия информации можно отнести изменения в системных файлах и временных файлах компьютера. Программы кодирования могут создавать временные файлы для хранения закодированных данных, а также изменять системные файлы для обеспечения своей работы.

Следующим признаком, на который следует обращать внимание, является изменения в реестре операционной системы. При его анализе можно выявить наличие подозрительных программ и действий на компьютере, которые осуществлялись при сокрытии данных или подготовке к данному процессу. В нем можно найти в том числе и остатки ранее установленных, а затем удаленных программ, использованных для кодирования или иного способа сокрытия данных.

Другим косвенным признаком может быть наличие установленного в системе программного обеспечения, которое используется для сокрытия информации. При этом стоит обратить внимание на установленные программы, такие как VeraCrypt, TrueCrypt, BitLocker, программы для стеганографии, о которых мы уже писали выше, и другие, которые могут использоваться для кодирования файлов и дисков. Следует также проанализировать историю использования программ и открывавшихся в последнее время документов, несоответствие размера файла его расширению, изучить эскизы графических файлов и т.д.

Для более точного обнаружения признаков сокрытия информации эксперты-криминалисты могут использовать специализированные инструменты и программы, такие как EnCase Forensic или FTK Imager. Они позволяют проводить более глубокий анализ компьютера и выявлять скрытые программы, осуществляющие кодирование.

Криминалисты должны быть внимательны при анализе косвенных признаков и не делать поспешных выводов. Наличие закодированных файлов или программ кодирования на компьютере не всегда свидетельствует о преступной деятельности.

Таким образом, мы можем констатировать, что существует множество способов обнаружения и исследования скрытой информации на носителях данных. Однако для успешного проведения таких исследований требуются специализированное

оборудование и программное обеспечение, а также опытные специалисты в области информационной безопасности.

Список источников.

1. Бураева Л.А., Шогенов Т.М. Роль информационных технологий в обеспечении общественного порядка и общественной безопасности // Социально-политические науки. 2019. Т. 9. № 5. С. 190-192.

2. Курин А.А., Гаужаева В.А. Электронно-цифровые следы как объекты криминалистической регистрации // Право и управление. 2023. № 7. С. 141-147.

3. Курин А.А., Карданов Р.Р., Евстифеева Е.П. Направления развития системы информационно-аналитического обеспечения раскрытия и расследования преступлений // Право и управление. 2022. № 8. С. 113-118.

4. Грибунов О.П., Старичков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие. – М.: ДГСК МВД России, 2017.

5. Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: автореф. дис. … канд. юрид. наук. – Краснодар, 2021.

6. https://ria.ru/20230810/mvd-1889293603.html.