Научная статья
УДК 343.98
DOI: 10.55001/2587-9820.2023.37.82.008

КЛАССИФИКАЦИЯ СПОСОБОВ ФАЛЬСИФИКАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕСТУПНОСТИ

Даниил Викторович Гирьятович
Академия управления МВД России, г. Москва, Российская Федерация, dv.gir@ya.ru

Аннотация. В статье рассматриваются научные взгляды на классификацию способов фальсификации доказательственной информации. Отмечается, что цифровая трансформация преступности обусловливает появление новых способов фальсификации, классификация которых не отражена в науке. В результате исследования автором предлагается классификация способов фальсификации доказательственной информации в зависимости от вида цифровой информации, содержащейся в электронных документах, медиафайлах, метаданных и сетевых данных.

Ключевые слова: доказательственная информация, цифровая трансформация преступности, способ фальсификации, классификация способов фальсификации

Для цитирования: Гирьятович, Д. В. Классификация способов фальсификации доказательственной информации в условиях цифровой трансформации преступности // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2023. Т. 28. № 4. С. 76–82. DOI: 10.55001/2587-9820.2023.37.82.008

CLASSIFICATION OF METHODS OF FALSIFICATION OF EVIDENTIARY INFORMATION IN THE CONTEXT OF DIGITAL TRANSFORMATION OF CRIME

Daniil V. Giryatovich
Academy of Management of the MIA of Russia, Moscow, Russian Federation, dv.gir@ya.ru

Abstract. The article discusses scientific views on the classification of methods for falsifying evidentiary information. It is noted that the digital transformation of crime causes the emergence of new methods of falsification, the classification of which is not reflected in science. As a result of the study, the author proposes a classification of methods for falsifying evidentiary information depending on the type of digital information contained in electronic documents, media files, metadata and network data.

Keywords: evidentiary information, digital transformation of crime, method of falsification, classification of methods of falsification

For citation: Giryatovich D.V. Klassifikaciya sposobov fal'sifikacii dokazatel'stvennoj informacii v usloviyah cifrovoj transformacii prestupnosti [Classification of methods of falsification of evidentiary information in the conditions of digital transformation of crime]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2023, vol. 28 no. 4, pp. 76–82 (in Russ.). DOI: 10.55001/2587-9820.2023.37.82.008

Введение

Фальсификация информации и ее источников является одной из центральных и дискуссионных тем в учении о противодействии расследованию преступлений и мер по его преодолению. В частности, вопросы о сущности и соотношении данного понятия с иными категориями указанного учения до сих пор не нашли своего единого понимания в науке и трактуются по-разному. Также остается нерешенной проблема классификации способов фальсификации информации, содержащейся на электронных носителях. Исследование данного вопроса видится исключительно актуальным. Необходимо отметить, что еще профессор Р. С. Белкин писал, что в настоящее время одной из перспективных и конкретных задачи криминалистической науки является классификация способов совершения преступлений [1, с. 53]. В настоящей статье мы предпримем попытку внести вклад в решение данной научной задачи и классифицировать способы фальсификации доказательственной информации на электронных носителях.

Основная часть

Прежде чем переходить к изложению непосредственного вопроса научной статьи, видится необходимым рассмотреть общую классификацию способов фальсификации и определить место «цифровых» способов в ней.

В результате анализа и обобщения научных трудов можно полагать, что самый распространенный и наиболее признанный в научных кругах перечень способов фальсификации разработан профессором Р. С. Белкиным и состоит в следующих способах:

1) заведомо ложное показание;

2) заведомо ложное сообщение, заявление, донос;

3) создание ложных следов и иных вещественных доказательств;

4) полная или частичная подделка документов;

5) подмена, дублирование объектов;

6) частичное уничтожение объекта, его переделка с целью изменить его внешний вид, фальсифицировать назначение и т. п. [1, с. 695].

Данный перечень до сих пор находит свое отражение в трудах многих исследователей. Вместе с тем, признавая высокую теоретическую и практическую научную значимость приведенных профессором Р. С. Белкиным способов, видится, что они уже далеко не в полной мере раскрывают содержание такого явления, как фальсификация, поскольку на фоне цифровой трансформации происходит расширение тех объектов, на которые она направлена. Помимо этого данный перечень не отражает классификацию всех разнообразных способов такого сложного явления, как фальсификация. Указанное обстоятельство детерминировало научный поиск более глубокого основания для классификации способов фальсификации информации и ее источников.

В дальнейшем различные исследователи предпринимали попытки построения такой классификации способов фальсификации, которая отражала бы все их многообразие. Например, в своем стремлении отыскать более глубокую дифференциацию способов фальсификации А. Г. Холевчук выделил следующие основания [2, с. 31]:

1) по объекту;

2) по виду;

3) по степени сложности;

4) по количеству лиц;

5) по субъекту совершения, по уровню преступных навыков;

6) по степени фальсификации объекта;

7) по времени осуществления фальсификации;

8) по количеству объектов;

9) по способам выражения;

10) по цели.

Также свои классификации приводили А. В. Ушенин, В. П. Попов, А. В. Присекин и другие. Анализируя каждую из этих классификаций, можно сделать вывод, что многие авторы в зависимости от объекта выделяют и признают классификацию материальную и идеальную. Видится, что данная классификация гармонично сочетается с сущностью рассматриваемого явления, однако, учитывая цифровую трансформацию преступности, считаем необходимым дополнить такую классификацию способов фальсификации.

Для определения места «цифровых» способов фальсификации в общей структуре необходимо сказать о цифровой трансформации. Названное явление находит свое широкое распространение в различных сферах общественной жизни. Преступная деятельность отнюдь не является исключением, о чем свидетельствуют как многочисленные факты использования передовых цифровых технологий в процессе совершения преступлений, так и научные труды многих авторов, активно исследующих закономерности данного явления. Н. Н. Федотов, например, отмечал, что «неостановимый технический прогресс дает возможность совершать преступления новыми способами и при помощи новых орудий» [3, с. 14].

По мнению Ю. В. Гаврилина, одними из ключевых тенденций цифровой трансформации преступности выступают:

1. Развитие дистанционных способов совершения преступлений.
2. Использование криптовалют в криминальных взаиморасчетах.
3. Рост масштабов межрегиональной и трансграничной преступности, использование при совершении преступлений сетевой инфраструктуры, расположенной за пределами Российской Федерации.
4. Формирование криминального рынка противоправных услуг в информационно-телекоммуникационной сфере.
5. Использование возможностей искусственного интеллекта в противоправной деятельности.
6. Совершенствование способов сокрытия преступлений, основанных на использовании сервисов анонимизации личности в цифровом пространстве [4, с. 7].

Также автор отмечает, что данные тенденции предопределяют и появление новых способов противодействия расследованию преступлений, среди которых:

– использование ремейлеров (специальных программ, которые позволяют переадресовать отправлениие электронной почты);

– использование анонимайзеров и VPN-сервисов, позволяющих произвести подмену IP-адреса;

– применение TOR-браузеров;

– подмена абонентских номеров посредством использования возможностей IP-телефонии;

– использование криптовалют, оборот которых не подконтролен для уполномоченных государственных органов, в криминальных взаиморасчетах;

– распространение ложной информации негативного характера в целях инсинуации сотрудников и руководителей правоохранительных органов в различных социальных сетях и мессенджерах;

– проведение различных акций в средствах массовой информации, а также на объектах органов власти в целях воздействия на общественное мнение по тому или иному делу;

– использование интеллектуальных технологий синтезирования речи и видеоизображений с целью создания аудио- и видеозаписи для манипуляции людьми, распространения фальшивых новостей и видеосюжетов [5, с. 17].

При анализе указанных выше положений можно заключить, что одним из основных способов противодействия расследованию преступлений является фальсификация информации и ее носителей. Из данных обстоятельств следует тот факт, что в условиях цифровой трансформации

происходит стремительное развитие и распространение электронных носителей информации, которые содержат разнообразную информацию и позволяют производить над ней различные операции, в том числе в преступных целях. И фальсификация как один из способов совершения и сокрытия преступления аналогично направлена на данные объекты.

По мнению Ю. В. Гаврилина, «специфическим фактором, оказывающим влияние на выбор орудий и средств совершения преступления, является тип материального носителя, на котором зафиксирована информация» [6, с. 117]. Указанное положение в свою очередь детерминирует ухищрения злоумышленников в части разработки соответствующих способов, орудий и средств совершения фальсификации, используемой как для совершения преступлений, так и для противодействия расследованию преступлений.

Таким образом, в условиях цифровой трансформации преступности в качестве ключевого объекта фальсификации (как способа совершения и способа противодействия расследованию преступлений) выступает цифровая информация и электронные носители информации. А если учитывать, что электронные носители информации и хранящаяся на них информация имеют материальную природу, то представляется логичным отнесение их к материальным способам фальсификации информации и их источников.

Необходимо сказать, что некоторые авторы обозначали способы фальсификации информации, содержащейся на электронных носителях. Например, А. А. Рудых формулировал такие способы, как:

1) создание и представление следователю носителей с файлами, содержащими информацию или метаданные, не соответствующие действительности (фотографии, видео, документы в электронном виде);

2) создание ложной переписки или информации о транзакциях;

3) представление сотрудникам операторов связи ложных данных об IP-адресах, сессиях, пользователях, абонентах [6, с. 132].

Анализируя иные, несомненно, значимые труды авторов по вопросу способов фальсификации информации, содержащейся на электронных носителях, стоит констатировать отсутствие их классификации.

В связи с изложенными выше обстоятельствами мы полагаем, что способы фальсификации информации и ее источников в условиях цифровой трансформации преступности возможно классифицировать в зависимости от вида цифровой информации. Необходимо отметить, что доказательственная информация, содержащаяся в электронных документах, медиафайлах, метаданных и сетевых данных, зачастую позволяет раскрыть преступление и доказать виновность конкретных лиц. Факт существования такой информации является нежелательным для злоумышленников в связи с чем они предпринимают различные способы ее фальсификации.

Таким образом, предлагаем следующую классификацию способов фальсификации доказательственной информации, содержащейся в электронных документах, медиафайлах, метаданных и сетевых данных:

1. Электронные документы, в том числе электронная подпись, которая включает в себя:

– изменение содержимого документа (изменение текста, данных или метаданных в электронных документах);

– создание фальшивых документов (создание документов, которые выглядят подлинными, но содержат ложную информацию).

2. Медиафайлы:

2.1. *Фото:*

– редактирование изображения в графическом редакторе: изменение значений цвета, яркости, контрастности, наложение фильтров и эффектов, удаление или добавление элементов, изменение размеров и пропорций и т. д.;

– использование специального

программного обеспечения;

– использование генеративно-состязательных сетей (GAN) (технология позволяет создавать синтетические изображения, которые могут быть похожи на настоящие фотографии).

2.2. *Видео:*

– Deepfake (технология, основанная на использовании искусственного интеллекта, которая позволяет создавать реалистичные видеоролики с лицами людей, которые на самом деле не участвовали в съемке);

– монтаж (редактирование видео с использованием программного обеспечения, чтобы изменить содержание съемки или добавить элементы, которые не имели место быть на самом деле);

– создание передачи обратной связи, т. е. использование специального оборудования или программного обеспечения для подделки видеозаписи таким образом, чтобы она выглядела, как будто она была записана на объекте, который не является источником видео (например, снятый на дистанции с помощью беспилотного летательного аппарата).

***3. Метаданные*:**

– изменение временных меток (злоумышленник может фальсифицировать временные штампы в метаданных, чтобы изменить информацию о времени создания или изменения файла);

– изменение GPS координат, например в фотографиях или видеозаписях, чтобы создать ложное впечатление о нахождении в определенном месте или времени;

– изменение авторской информации о файле, чтобы приписать его кому-либо или изменить источник;

– изменение EXIF данных, таких как модель камеры, дата или время съемки (это позволяет создать или изменить ложную историю события);

– добавление или удаление метаданных, чтобы скрыть или изменить информацию о файле (например, удаление информации о размере файла или его источнике).

4. Сетевые данные:

4.1. Сетевые идентификаторы:

а) IP-адрес (изменение или подделка IP-адреса для ложного представления настоящего отправителя или обмана системы идентификации (IP-спуфинг, VPN и др.)).

б) MAC-адрес:

– изменение MAC-адреса в настройках сетевого адаптера на своем устройстве;

– использование специализированного программного обеспечения;

– использование аппаратных устройств (например, некоторые беспроводные адаптеры позволяют изменять свой MAC-адрес);

– использование прокси-серверов, которые позволяют скрывать или изменять MAC-адрес устройства;

– спуфинг MAC-адреса (техника, при которой отправляющая сторона отправляет пакеты с поддельным MAC-адресом).

4.2. Сетевой трафик:

а) Электронная почта и мессенджеры:

– фальшивое подделывание отправителя (подделка адреса электронной почты для создания впечатления, что сообщение было отправлено другим лицом, например программы-ремейлеры);

– изменение содержимого письма (изменение текста или прикрепленных файлов в электронной почте).

б) Интернет-страница:

– изменение исходного кода (злоумышленник может использовать консоль разработчика браузера, чтобы изменить содержимое страницы, включая текст, изображения, ссылки и другие элементы);

– подделка URL-адреса (мошенник может создать URL-адрес, который похож на официальный, чтобы сделать страницу выглядящей подлинной, но на самом деле являющейся поддельной или фишинговой);

– спам и вредоносные программы (мошенник может использовать вредоносные программы для изменения содержимого страницы).

4.3. Веб-логи:

– манипуляция серверным журналом (злоумышленник может изменить лог-файлы, добавив или удалив записи);

– взлом аккаунтов с правами администратора (если злоумышленник получает доступ к аккаунту администратора системы, он может изменять или удалять логи).

Выводы и заключение

Полагаем, что предложенная нами классификация отражает наиболее общие способы фальсификации доказательственной информации, содержащейся в электронных документах, медиафайлах, метаданных и сетевых данных, которые в последующем, с учетом развития цифровых технологий, могут и должны дополняться различными частными способами.

В заключение также необходимо отметить, что в современном мире, где цифровая информация приобретает высокую значимость и широкое распространение, актуализируется проблема борьбы с неправомерным воздействием на нее. Фальсификация как один из таких способов на сегодняшний день представляет собой опасное явление, поскольку позволяет ввести в заблуждение должностных лиц правоохранительных органов и повлиять в конечном счете на исход дела.

СПИСОК ИСТОЧНИКОВ

1. *Белкин, Р. С.* Криминалистика : учебник для вузов. М. : НОРМА, 2001. 990 с.

2. *Холевчук, А. Г.* Фальсификация как объект криминалистического исследования : дис. ... канд. юрид. наук. М., 2010. 225 с.

3. *Федотов, Н. Н.* Форензика – компьютерная криминалистика. М. : Юридический Мир, 2007. 432 с.

4. *Гаврилин, Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. М. : Академия управления МВД России, 2021. 72 с.

5. *Гаврилин, Ю. В.* Развитие криминалистического учения о противодействии расследованию и мерах по его преодолению в условиях цифровой трансформации // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации : сб. науч. ст. по мат-лам международ. науч.-практич. конф., Москва, 21 мая 2021 года / под ред. Ю. В. Гаврилина, Ю. В. Шпагиной. М. : Академия управления МВД России, 2021. С. 16–25.

6. *Гаврилин, Ю. В.* Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы : дис. ... д-ра юрид. наук. Москва, 2009. 404 с.

7. *Рудых, А. А.* Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : дис. ... канд. юрид. наук . Иркутск, 2019. 239 с.

REFERENCES

1. *Belkin, R.S.* Kriminalistika [Criminalistics]. M.: NORMA, 2001, 990 p. (in Russian).

2. *Kholevchuk, A.G.* Fal'sifikacija kak ob`ekt kriminalisticheskogo issledovanija : dis. ... kand. jurid. nauk [Falsification as an object of forensic research: diss...cand. jurid. Sciences.]. M., 2010, p. 225. (in Russian).

3. *Fedotov, N.N.* Forenzika – komp'yuternaya kriminalistika [Forenzika – computer criminalistics]. M.: Legal World, 2007, 432 p. (in Russian).

4. *Gavrilin, Yu.V.* O nauchnyh podhodah k probleme ispol'zovaniya informacionno-telekommunikacionnyh tekhnologij v prestupnyh celyah: nauchno-prakticheskoe posobie [On scientific approaches to the problem of using information and telecommunication technologies for criminal purposes: a scientific and practical guide]. Moscow, 2021, 72 p. (in Russian).

5. *Gavrilin, Yu.V.* [Development of the criminalistic doctrine on countering the investigation and measures to overcome it in the conditions of digital transformation]. Razvitie uchenija o protivodejstvii rassledovaniju prestuplenij i merah po ego preodoleniju v uslovijah cifrovoj transformacii : sb. nauch. st. po mat-lam mezhdunarod. nauch.-praktich. konf., Moskva, 21 maja 2021 goda [Development of the doctrine on countering the investigation of crimes and measures to overcome it in the conditions of digital transformation: Collection of scientific articles based on the materials of the international scientific and practical conference, Moscow, May 21, 2021]. Moscow, 2021, pp. 16-25. (in Russian).

6. *Gavrilin, Yu.V.* Rassledovanie prestuplenij, posjagajushhih na informacionnuju bezopasnost' v sfere jekonomiki: teoreticheskie, organizacionno-takticheskie i metodicheskie osnovy : dis. ... d-ra jurid. nauk. [Investigation of crimes encroaching on information security in the field of economics: theoretical, organizational, tactical and methodological foundations: dissertation... Doctor of Law]. Moscow, 2009, 404 p. (in Russian).

7. *Rudykh, A.A.* Informacionno-tehnologicheskoe obespechenie kriminalisticheskoj dejatel'nosti po rassledovaniju prestuplenij v sfere informacionnyh tehnologij : dis. ... kand. jurid. nauk. [Information and technological support of criminalistic activities for the investigation of crimes in the field of information technology: dissertation... Candidate of Legal Sciences.]. Irkutsk, 2019, 239 p. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Гирьятович Даниил Викторович, адъюнкт. Академия управления МВД России. 125993, Российская Федерация, г. Москва, ул. Зои и Александра Космодемьянских, 8.

INFORMATION ABOUT THE AUTHOR

Giryatovich Daniil Viktorovich, postgraduate. Academy of Management of the MIA of Russia, 8, str. Zoya and Alexander Kosmodemyanskikh, Moscow, Russian Federation, 125993.