УДК 343.9
DOI: https://doi.org/10.17308/law/1995-5502/2023/3/254–257

ФОРЕНЗИКА И АНТИФОРЕНЗИКА: КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ

Е. С. Орленко, И. Г. Гришаева

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Воронежский филиал)

FORENSICS AND ANTIFORENSICS: FORENSIC ASPECTS

E. S. Orlenko, I. G. Grishaeva

Russian Presidential Academy of National Economy and Public Administration (Voronezh Branch)

Аннотация: рассматриваются основные криминалистические аспекты форензики, её особенности, следственные действия и тактические приёмы, направленные на раскрытие киберпреступлений. Анализируются способы сокрытия цифровых следов.
Ключевые слова: криминалистика, форензика, антифорензика, киберпреступления, криминалистическая тактика, следственные действия.

Abstracts: the paper reveals the main forensic aspects of forensics, its features, investigative actions and tactical techniques aimed at uncovering cybercrimes. The methods of hiding digital traces are analyzed.
Key words: criminalistics, forensics, anti-forensics, cybercrime, forensic tactics, investigative actions.

Появление персональных компьютеров в 1970-х гг. привело к глобальной компьютеризации общества, а разработка и распространение сети Интернет дало толчок к дальнейшей цифровизации различных сфер жизнедеятельности человечества. Так, Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» определил такие задачи, как научно-техническое и социально-экономическое развитие страны, среди которых особое значение имеет процесс ускоренного внедрения цифровых технологий во все отрасли.

Технический прогресс стал одной из причин развития новых видов противоправных деяний, именуемых киберпреступлениями, против которых традиционные методы раскрытия и расследования уже не эффективны. По данным экспертно-аналитического центра InfoWatch, в 2022 г., по сравнению с предыдущим, преступлений в сфере компрометации финансов в цифровой форме стало больше практически в 3,7 раза, т. е. на 269,9 %[1]. Вследствие стремительных изменений в политиках мира в современных условиях множество отраслевых групп испытывают серьезное давление со стороны киберпреступности. Значительно увеличились умышленные нарушения «извне» : с 70,4 до 95,3 % в сравнении 2022 и 2021 гг.[2] В то же время специалисты предполагают, что «могла вырасти латентность инцидентов внутреннего характера»[3]. А это означает, что перенос незаконной деятельности в виртуальное пространство ставит перед криминалистами абсолютно новые задачи.

Решением проблемы активного роста цифровых преступлений стало введение нового раздела криминалистики – форензики. По своей сути

[1] См.: Исследование утечек конфиденциальной информации в финансовой сфере : Мир – Россия, 2022 г. (аналитический отчет) // Экспертно-аналитический центр InfoWatch, 2023.

[2] См.: Там же.

[3] Там же.

это прикладная наука, направленная на раскрытие и расследование деяний, непосредственно связанных с компьютерной информацией. Она изучает методы получения, исследования именно цифровых доказательств, а также применения для этого современных технологий. Форензика занимается решением таких задач, как «создание программных и аппаратных инструментов для исследования и сбора данных, разработкой плана оперативно-розыскных мероприятий»[4].

Особенность компьютерной криминалистики заключается в изучаемых следах преступления, которые в основном не имеют материальной оболочки, вследствие чего специалист, не обладающий специфическими знаниями в сфере IT-технологий, не сможет провести необходимые «процедуры выявления механизма следообразования»[5]. Часть 2 ст. 164.1 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) прямо устанавливает обязательный характер привлечения специалистов при производстве «изъятия электронных носителей информации»[6]. Из этого вытекает следующая отличительная черта форензики, а именно специфический субъект. Так, при осуществлении осмотра места происшествия, а также вещественных доказательств согласно ч. 1 ст. 57 УПК РФ специалист дает разъяснения по вопросам, которые входят в «его профессиональную компетенцию»[7].

Поскольку форензика значительно отличается от остальных направлений криминалистики, следственные действия по раскрытию и расследованию киберпреступлений, криминалистическая тактика их производства имеют ряд особенностей. Например, осмотр места происшествия, процедура которого регулируется ст. 176 и 177 УПК РФ, представляет собой исследование цифровых объектов, находящихся на персональном компьютере, в целях обнаружения, фиксации и изъятия следов преступления в информационном пространстве. Специфика данного действия связана с тем, что киберпреступление совершается не в реальном, материальном мире, а направлено на цифровое пространство. Поэтому для наиболее эффективной проработки механизма преступления в ходе расследования важно не упустить детали: обращение к DNS-серверу. Обращения к указанным данным могут признаваться доказательствами посещения конкретной веб-страницы, а значит, в дальнейшем играть важную роль. Также криминалисты в сфере IT-технологий зачастую обращаются к лог-файлам, содержащим сведения о событиях, фиксируемых сервером автоматически, без участия человека[8].

Еще одно важнейшее следственное действие – это обыск, закрепленный в ст. 182 УПК РФ. Данная процедура проводится с учетом определенных требований, среди которых можно выделить: установление «электрощита», который не допустит «приближение к данным объектам каких-либо лиц»[9]; запечатление компьютерной техники, а также наличие кабелей, места их положения и т. д. Также стоит отметить важность фиксирования информации, находящейся на мониторе в случае, если устройство включено. Выключение необходимо производить путем извлечения кабеля из корпуса компьютера или изъятия блока питания у ноутбука. Все технические средства опечатываются и упаковываются таким образом, чтобы исключить возможность утраты не только объектов физически, но и их информационной составляющей.

Выемка – следственное действие, необходимое для производства работы с электронными источниками и осуществления его осмотра не на месте происшествия. Перед началом проведения следственного действия следователь предлагает собственнику «выдать предметы и документы, подлежащие изъятию, а в случае отказа производит выемку принудительно»[10] согласно ч. 5 ст. 183 УПК РФ.

Для работы с электронными следами киберпреступлений криминалисты используют не только универсальные средства (компьютеры), но и специальные технические средства: устройства для клонирования жестких дисков и (или) иных носителей цифровой информации, определенные программы для проведения кримина-

[4] *Ломакин Д. Н.* Компьютерная криминалистика «Форензика» и киберпреступления в России в период пандемии // Молодой ученый. 2022. № 17 (412). С. 210.

[5] *Шуваева М. С., Николаева А. В.* Указ. соч. С. 235.

[6] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[7] Там же.

[8] См.: *Федотов Н. Н.* Форензика – компьютерная криминалистика. М., 2007. С. 204.

[9] *Шуваева М. С., Николаева А. В.* Указ. соч. С. 236.

[10] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

листического исследования, персональные компьютеры, направленные на получение информации в полевых условиях, набор хэшей, фильтрующих изучаемые файлы, и т. д.

Стремительное развитие компьютерной криминалистики привело к тому, что лица, совершающие действия преступного характера, в стремлении избежать раскрытия их умысла усложняют структуру деяния и разрабатывают новые способы «маскировки» следов, которые в совокупности дают такое понятие, как «антифорензика». Например, поскольку программа непосредственно «несет в себе волю программиста»[11], она не является объективной реальностью. Злоумышленник может использовать «логическую бомбу» для того, чтобы уничтожить всю критическую информацию, если компьютер попадет в руки иного лица[12]. Данная программа срабатывает при соблюдении конкретных условий: выполнении (или невыполнении) определенных действий. Указанная ситуация ставит перед криминалистами задачу – определить обстоятельства срабатывания «логической бомбы». Ключ к пониманию алгоритмов действия программы лежит через понимание замысла ее автора.

Помимо вышеописанной разработки, можно отметить такие антикриминалистические меры, как программы, направленные на шифрование информации, очистку дисков или же иных носителей, сокрытие преступных данных. Также применяются системы и серверы для анонимизации активности в сети. На данный момент времени лица, совершающие преступления, зачастую используют VPN-соединения. Пользователи соединяются с провайдером «по закрытому каналу»[13], обеспечивающему защиту путем шифрования передачи данных. Помимо этого, особую популярность имеют специальные браузеры, сохраняющие анонимность. Среди них наиболее используемым является TOR Browser[14]. Данные способы сокрытия цифровых следов все еще являются эффективными. Основной метод борьбы с ними – это выявление владельца сервера, у которого изымаются все необходимые для расследования данные. Однако такой вариант получения доказательств имеет серьезный недостаток: на практике возможна ситуация отсутствия возможности установления владельца. Еще один способ сокрытия цифровых следов киберпреступления – несоответствие реального географического местоположения и времени, установленного на используемом устройстве.

Особый интерес в настоящее время вызывает цифровой отпечаток устройства. Он является уникальным электронным идентификатором, который содержит набор важных данных. После анализа браузера или конкретного устройства программное обеспечение для снятия отпечатков устройства сохраняет сведения на стороне сервера, вне контроля пользователя. Это позволяет идентифицировать и отслеживать пользователей интернета, даже когда они принимают обходные меры против файлов cookie. В то же время лица, желающие скрыть сведения о совершенных незаконных деяниях, разработали способы изменения таких данных. Зачастую они используют код, написанный на JavaScript, или же Canvas Blocker, однако наиболее эффективным является предоставление фиктивного отпечатка устройства. Существуют программы, которые случайным образом меняют данные при попытке браузера идентифицировать пользователя, в частности, Canvas Fingerprint Defender. Четких методов определения факта подделки цифрового отпечатка нет, однако специалисты могут сравнить используемые данные при совершении преступного деяния и, например, входа в личный аккаунт социальной сети.

Таким образом, можно сделать вывод, что форензика активно развивается в современных реалиях. Появление новых технологий ведет к образованию иных видов преступлений, раскрытие и расследование, а также пресечение и предупреждение которых невозможно без трансформации традиционных методов и выявления специальных способов. Киберпреступления – серьезная проблема современного общества, прогрессирующая с каждым годом все больше. Это проявляется в активном росте антифорензики, т. е. развитии методов и способов сокрытия цифровых следов незаконного деяния. Важно подчеркнуть, что эффективно организованная работа правоохранительных органов, создание новых действенных методов расследования, а также привлечение к работе компетентных кадров в сфере информационных технологий обе-

[11] *Федотов Н. Н.* Указ. соч. С. 18.

[12] Там же. С. 35.

[13] *Усманов Р. А.* Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 139.

[14] Там же.

спечит снижение общего количества киберпреступлений.

Библиографический список

Исследование утечек конфиденциальной информации в финансовой сфере: Мир-Россия, 2022 г. (аналитический отчет) // Экспертно-Аналитический центр InfoWatch, 2023.

Ломакин Д. Н. Компьютерная криминалистика «Форензика» и киберпреступления в России в период пандемии // Молодой ученый. 2022. № 17 (412). С. 210.

Усманов Р. А. Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 139.

Федотов Н. Н. Форензика – компьютерная криминалистика. М. : Юридический мир, 2007. С. 204.

Шуваева М. С., Николаева А. В. Роль форензики в расследовании киберпреступности. Криминалистический аспект // Международный журнал гуманитарных и естественных наук. 2021. № 6-2 (57). С. 235–236.

References

Fedotov N. N. Forensics is computer forensics. Moscow : Legal World, 2007. P. 204.

Lomakin D. N. Computer forensics «Forensic» and cybercrime in Russia during the pandemic // Young scientist. 2022. No. 17 (412). P. 210.

Shuvaeva M. S., Nikolaeva A. V. The role of forensics in the investigation of cybercrime. Forensic aspect // International journal of the humanities and natural sciences. 2021. No. 6-2 (57). P. 235–236.

Study of leaks of confidential information in the financial sector : World-Russia, 2022 (analitical report) // InfoWatch Expert Analytical Center, 2023.

Usmanov R. A. Characteristics of criminal activity carried out on the Internet through anonymizing services // Legal Science and Law Enforcement Practice. 2018. No. 4 (46). P. 139.

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Воронежский филиал)

Орленко Е. С., студент

E-mail: evgeniy.orlenko17@yandex.ru

Гришаева И. Г., кандидат биологических наук, доцент, доцент кафедры уголовного и гражданского права и процесса

E-mail: grishaeva-ig@yandex.ru

Поступила в редакцию: 12.07.2023

Для цитирования:

Орленко Е. С., Гришаева И. Г. Форензика и антифорензика: криминалистические аспекты // Вестник Воронежского государственного университета. Серия: Право. 2023. № 3 (54). С. 254–257. DOI: https://doi.org/10.17308/law/1995-5502/2023/3/254–257.

Russian Presidential Academy of National Economy and Public Administration (Voronezh Branch)

Orlenko E. S., Student

E-mail: evgeniy.orlenko17@yandex.ru

Grishaeva I. G., Candidate of Biology Sciences, Associate Professor, Associate Professor of the Criminal and Civil Law and Process Department

E-mail: grishaeva-ig@yandex.ru

Received: 12.07.2023

For citation:

Orlenko E. S., Grishaeva I. G. Forensics and antiforensics: forensic aspects // Proceedings of Voronezh State University. Series: Law. 2023. № 3 (54). P. 254–257. DOI: https://doi.org/10.17308/law/1995-5502/2023/3/254–257.