УДК 343.985.1
ББК 67.52

© 2022 г. Маилян Ани Варужановна,
старший преподаватель кафедры криминалистики и оперативно-разыскной деятельности Ростовского юридического института МВД России, кандидат юридических наук.
E-mail: david.072014@mail.ru

ЦИФРОВАЯ КРИМИНАЛИСТИКА КАК ФАКТОР ЗАЩИТЫ ЦИФРОВОЙ ЭКОНОМИКИ

В данной статье проведен анализ наиболее уязвимых компонентов цифровой экономики, рассмотрены признаки цифровой информации, имеющие возможность стать доказательственной базой преступной деятельности. Определено значение понятия «цифровая криминалистика». Описаны основные способы анонимного проникновения в цифровую систему. Выделен перечень мер, принимаемых государством в целях противодействия цифровым преступлениям.

Ключевые слова: *экономика, цифровая, технология, носители, электронная, преступления.*

Mailyan Ani Varuzhanovna – Senior Lecturer, Department of Forensic Science and Operational-Search Activities, the Rostov Law Institute of the Ministry of Internal Affairs of Russia, PhD in Law.

DIGITAL CRIMINALISTICS AS A FACTOR OF PROTECTION OF THE DIGITAL ECONOMY

This article is devoted to the analysis of the most vulnerable components of the digital economics. The signs of digital information that have the opportunity to become the evidence base of criminal activity are considered. The meaning of the concept of «digital forensics» is defined. The main methods of anonymous penetration into the digital system are described. The list of measures taken by the state to counteract digital crimes is highlighted.

Keywords: *economics, digital, technology, media, electronic, crimes.*

Сегодня развитие передовых цифровых технологий в современном обществе позволяет в обязательном порядке внедрять их в широкий спектр сфер связей с общественностью. Однако с развитием цифровой экономики необходимо обратить внимание на активное использование цифровых технологий при осуществлении преступниками различных незаконных действий.

Осуществление безналичного способа оплаты стало наиболее удобным в связи с мгновенным поступлением денежных средств. В то же время электронные деньги не полностью защищены от незаконных нарушений, совершаемых преступниками. Наиболее распространенным методом мошенничества является обман со стороны преступников для получения паролей к карточкам или электронным кошелькам.

В российской стратегии развития информационных технологий подчеркивается, что одним из основных направлений является дальнейшее совершенствование информационных и цифровых технологий для решения сложных правовых, политических, экономических и социальных задач национальной политики [1].

В случае, когда преступники используют удаленный доступ для совершения квалифицированных преступлений, база доказательств значительно сокращается, т. е. наличие оставленных следов отражает признаки оставивших их предметов (отпечатки пальцев, следы хакеров, отпечатки колес и т. д.). Однако при использовании цифровых технологий для совершения мошенничества появляется новый тип следов – это цифровой след преступления.

В то же время существует еще два типа цифровых отпечатков. Во-первых, это отпечаток активности, сформированный в течение периода получения информации от самого пользователя-преступника, такой как его личные данные, фотографии, видео с комментариями, размещенные в социальных сетях, на веб-сайтах и на различных электронных онлайн-форумах.

Во-вторых, пассивные отпечатки пальцев, оставленные злоумышленником, использующим интернет. Например, они могут быть оставлены кем-то при просмотре истории в браузере.

Полученные цифровые отпечатки пальцев, если они признаны судом доказательствами, активно используются на заседаниях суда для подтверждения, опровержения фактов противоправной деятельности или показаний участников спора, а также для определения

фактов вины или невиновности преступника в этом деле.

Учитывая все вышеперечисленные обстоятельства, можно сделать вывод, что компьютерная криминалистика включает обнаружение, сбор и анализ электронных следов для борьбы с преступностью. В этом случае компьютер или смартфон могут быть инструментом или средством совершения противоправного деяния, стать объектом преступного посягательства или использоваться для хранения важных электронных доказательств преступления.

В процессе расследования уголовного дела необходимо установить роль, отведенную компьютерам в преступлении, чтобы собрать доказательства.

Если компьютер взломан через файл сетевого пароля, то необходимо определить местоположение файла, используемого для расшифровки пароля. Следовательно, после определения того, как компьютер участвовал в совершении преступления, можно определить конкретное направление расследования для сбора доказательств.

В современном мире компьютерная криминалистика – это новый вид деятельности, предназначенный для обработки цифровых следов преступных деяний. Разработка новых стандартов и принципов для оценки и проверки собранных доказательств (цифровых следов) требует новых знаний и развития криминалистических технологий. Проблема сбора цифровых следов заключается в том, что они могут изменяться, а также обнаруживаться и записываться только с помощью определенных методов и специального компьютерного оборудования.

Поиск, фиксация, исследование, интерпретация цифровых следов подчиняются строгим правилам судопроизводства. Обычный файл для эксперта является не просто носителем текстовой и графической информации, это контейнер со сложной структурой, похожей на «матрешку», позволяющий увидеть скрываемые данные, получить дополнительные сведения об обстоятельствах его создания и редактирования. Поврежденный графический файл, который невосстановим для обычного пользователя, для эксперта лишь конструкция с дефектом, у которой нужно выявить и «отремонтировать» некорректные части, чтобы потом изучить как восстановленное изображение, так и техническую информацию (метаданные) о ситуации, в которой был создан файл. Перечисленные действия выполняются в соответствии с правилами компьютерно-технической экспертизы и проверенными методическими рекомендациями.

Компьютерная информация должна оставаться неизменной. Только так она может иметь доказательную ценность.

Что касается защиты цифровой экономики, то следует подчеркнуть, что, обеспечивая безопасность на рабочем месте как государственных, так и частных компаний, службы безопасности сосредотачиваются исключительно на защите, чтобы предотвратить несанкционированные атаки на их цифровую информацию. Эта ситуация привела к тому, что у специалистов нет технической возможности зарегистрировать информацию о доказательствах, а затем передать ее правоохранительным органам для идентификации злоумышленников.

Сегодня существуют проблемы, связанные с разработкой передовых технологий для обнаружения и загрузки необходимой информации из больших массивов компьютерных данных. Одной из проблем является технология, связанная с блокчейном, революционной технологией, предназначенной для хранения электронной информации на компьютере с большим объемом дисковой памяти.

Разработка квантовых компьютеров теоретически поможет взломать ключи шифрования системы. Злоумышленник может работать с большим количеством сообщников для атаки на систему блокчейнов и, следовательно, получит несанкционированный доступ к конфиденциальной информации. Важным фактом является отсутствие надлежащей правовой базы для использования технологии блокчейн и криптовалют. Это позволяет совершать транзакции анонимно, что является реальной возможностью использовать криптовалюты в преступных целях [2].

Что касается майнинга криптовалюты, то для тех, кто предоставляет дорогостоящее компьютерное оборудование, следует отметить, что алгоритм майнинга полностью известен своему создателю, а также то, как работает большое количество оборудования.

С 1 января 2021 г. в России начал действовать закон о цифровых финансовых активах, цифровой валюте (ФЗ от 31.07.2020 № 259-ФЗ), согласно которому криптовалюта имуществом не является, и данный термин заменен на «цифровую валюту» [3].

Что касается криптовалюты, то ее запрещено использовать для осуществления

платежей, но доходы от ее оборота должны декларироваться и облагаться налогом.

В современном обществе развитие цифровых технологий требует создания правовой и методологической основы для содействия использованию цифровых доказательств в уголовном судопроизводстве. В связи с этим необходимо провести обязательную стандартизацию и сертификацию при обработке цифровой информации, а также изменить и сформулировать соответствующие методы подготовки экспертов в области компьютерной экспертизы. В современном мире трудно представить, чтобы у человека не было мобильного телефона, компьютера, цифровой камеры или Интернета. Цифровые информационные технологии глубоко укоренились в жизни каждого человека и являются неотъемлемой частью работы или учебы. Преступники также используют информационные технологии для ведения незаконной деятельности и совершения преступлений на расстоянии. Чтобы положить конец такой преступной деятельности, государству необходимо усовершенствовать методы раскрытия информации.

Основным компонентом разработки новых методов и возможностей сбора и анализа доказательств этих преступлений является новая отрасль криминалистических знаний – цифровые криминалистические доказательства, которые представляют собой набор знаний, навыков и способностей (систем), позволяющих осуществлять криминалистическую экспертизу [4].

Целями цифровой криминалистики являются обнаружение, извлечение и анализ данных, а также использование цифровых технологий для сбора доказательств. Следует отметить, что объем цифровых криминалистических доказательств довольно широк. Он охватывает не только современные компьютерные технологии, но и их программное обеспечение, электронное хранение данных, мобильную связь и др.

Цифровые криминалистические доказательства характеризуются спецификой обнаружения, фиксации и удаления цифровых следов, которые могут передаваться на электронных носителях или через специальные средства связи, но на практике их довольно сложно найти. Следовательно, профессиональное оборудование и персонал, обладающие достаточными знаниями и навыками в этой области, необходимы для полного и быстрого раскрытия преступлений в цифровой сфере. Кроме того, следует отметить, что вещественное доказательство в уголовном процессе рассматривается как материальный носитель электронной информации (ноутбуки, телефоны, карты флэш-памяти, магнитные диски и т. д.) [5]. Например, когда бумажный документ, содержащий важную информацию, рассматривается как независимое доказательство, которое не требует проверки. Следовательно, вышеизложенное можно рассматривать как еще одну особенность цифровой криминалистики.

Если обратиться к статистике за период с января по июль 2020 г., то видно, насколько вырос уровень компьютерной преступности по сравнению с предыдущими годами и другими преступлениями [6].

При выявлении цифровых преступлений и преступлений, совершенных стандартным образом, также используется ряд оперативных расследований и поисковых мер. Однако, в отличие от доказательств с материальным обозначением, цифровые доказательства (вся информация, особенно зашифрованная) сложнее восстановить и удалить.

Следовательно, цифровые криминалистические доказательства также характеризуются специальными оперативными исследовательскими мерами, которые представляют собой комплекс мероприятий, направленных на перехват и расследование данных о трафике, а также на создание журналов веб-серверов и почтовых серверов, системных журналов, доменов трафика и т. д.

Специальные ОРМ для борьбы с цифровой преступностью включают в себя:

– восстановление удаленных файлов;

– определение источника вредоносных программ или атак (компьютеры, другие устройства);

– установление исходного IP-адреса;

– настройку оборудования для съемки фотографий, видеозаписей, а также установление даты, время и места;

– создание информации об устройстве: контакты, пропущенные/исходящие/входящие звонки, сообщения;

– отслеживание местоположения устройства с системой GPS или без нее;

– установление времени создания или редактирования файла;

– взлом пароля на телефоне, компьютере, жестком диске или заблокированном/зашифрованном файле;

– отслеживание истории посещений вебсайта и установку загруженных файлов;

– идентификацию лица, взломавшего беспроводную сеть, или лица, которое не было авторизовано в качестве пользователя и т. д [7].

В современном мире цифровые и компьютерные технологии занимают важное место практически во всех областях человеческой деятельности, результатом чего является развитие цифровой криминалистики как отдельной отрасли криминалистики. Несколько лет назад высокотехнологичные преступления считались потенциальными, т. е. преступления готовились и совершались с использованием компьютерных технологий и цифровой информации. Это означает, что не следует ожидать быстрой идентификации людей и раскрытия информации о случаях. В этой ситуации присутствуют многие факторы: отсутствие специализированного оборудования для обнаружения, регистрации и расследования цифровых следов; недостаточная разработка методов расследования таких преступлений; отсутствие людей с достаточными знаниями и навыками в этой области.

Таким образом, можно сделать вывод, что разработка и формирование цифровых криминалистических доказательств и защита цифровой экономики являются неотъемлемыми областями национальной деятельности.

Литература

1. Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 гг. и на перспективу до 2025 г.: распоряжение Правительства РФ от 01.11.2013 № 2036-р [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_82959 (дата обращения: 14.10.2021).

2. Цой В.В., Царев Е.О., Омбровский Ю.Е. Обеспечение безопасности при использовании криптовалюты // Банковское дело. 2017. № 11.

3. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31.07.2020 № 259-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_82959/ (дата обращения: 14.10.2021).

4. Афанасьев А.Ю., Репин М.Е. Некоторые особенности расследования компьютерных преступлений. Уфа, 2015.

5. Русанова Д.Ю. Цифровая криминалистика: возможности и перспективы развития // Международный журнал гуманитарных и естественных наук. 2019. № 12–4(39).

6. Соловьева С.М. Применение цифровых технологий в криминалистике // Молодой ученый. 2019. № 51(289).

7. Репин М.Е. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия // Молодой ученый. 2015. № 15(95).

8. Статистический сборник «Состояние преступности в России за июль 2020 г.» // Сайт Генеральной Прокуратуры Российской Федерации [Электронный ресурс]. URL: https://genproc.gov.ru/stat/data/1888262/ (дата обращения: 14.10.2021).

Bibliography

1. On the approval of the Strategy for the development of the information technology industry in the Russian Federation for 2014–2020 and for the future until 2025: decree of the Government of the Russian Federation of 01.11.2013 № 2036-d [Electronic resource]. URL: http://www.consultant.ru/document/cons_doc_LAW_82959 (date of access: 14.10.2021).

2. Tsoi V.V., Tsarev E.O., Ombrovsky Yu.E. Ensuring security when using cryptocurrencies // Banking. 2017. № 11.

3. On Digital Financial Assets, digital currency and Amendments to Certain Legislative Acts of the Russian Federation: fed. law of 31.07.2020 № 259-FL [Electronic resource]. URL: http://www.consultant.ru/document/cons_doc_ LAW_82959/ (date of access: 14.10.2021).

4. Afanasyev A.Yu., Repin M.E. Some features of the investigation of computer crimes. Ufa, 2015.

5. Rusanova D.Yu. Digital criminalistics: opportunities and prospects for development // International Journal of Humanities and Natural Sciences. 2019. № 12–4(39).

6. Solovyova S.M. Application of digital technologies in criminalistics // Young scientist. 2019. № 51(289).

7. Repin M.E. Crimes in the field of computer information: problems of detection and disclosure // Young scientist. 2015. № 15(95).

8. Statistical collection «The state of crime in Russia for July 2020» // Website of the Prosecutor General's Office of the Russian Federation [Electronic resource]. URL: https://genproc.gov.ru/stat/data/1888262 / (date of access: 14.10.2021).