DOI: http://dx.doi.org/10.21686/2411-118X-2024-2-81-84

Особенности первоначального этапа расследования мошенничества в сфере IT-технологий

Т. А. Сулейманов
кандидат юридических наук, доцент,
доцент кафедры уголовного процесса и криминалистики Академии ФСИН России.
Адрес: ФКОУ ВО «Академия права и управления Федеральной службы исполнения наказаний»,
390036, Рязань, Сенная ул., д. 1.
E-mail: suleymanov.talvat@yandex.ru

Features of the Initial Stage of Fraud Investigation in the Field of IT Technologies

T. A. Suleymanov
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminal Procedure and Criminalistics
of the Academy of the Federal Penitentiary Service of Russia.
Address: Academy of the Federal Penitentiary Service of Russia,
1 Sennaya str., Ryazan, 390036, Russian Federation.
E-mail: suleymanov.talvat@yandex.ru

Аннотация

В рамках настоящего исследования автор предпринимает попытку проанализировать первоначальный этап расследования мошенничества, совершенного с использованием IT-технологий. Одна из особенностей расследования мошенничества с использованием компьютерной информации заключается в том, что типичные следы преступления носят виртуальный характер, их следует искать в компьютерных устройствах и в сети Интернет, их обнаружение, изъятие и проведение последующего исследования предполагает привлечение к расследованию уголовного дела специалиста в области компьютерной информации. По данной категории дел в обязательном порядке проводится компьютерно-техническая экспертиза (КТЭ) для обнаружения следов преступления. Результаты экспертизы составляют основу доказательственной базы по этой категории дел. Вместе с тем принимаемые меры информационной безопасности не способны предотвратить совершение мошенничества в сфере компьютерной информации.

Ключевые слова: мошенничество в сфере компьютерной информации, расследование уголовного дела, компьютерно-техническая экспертиза (КТЭ), производство следственных действий.

Abstract

In the framework of this study, the author attempts to analyze the initial stage of the investigation of fraud committed using IT technologies. As the author notes, one of the peculiarities of investigating fraud using computer information is that typical traces of a crime should be searched for in computer devices and on the Internet, these traces are virtual in nature, their detection, seizure and subsequent research involves the involvement of a computer information specialist in the investigation of a criminal case. In this category of cases, a computer-technical examination (CTE) is mandatory to detect traces of a crime. The results of the examination form the basis of the evidence base for this category of cases. At the same time, as the author concludes, the information security measures taken are not able to prevent fraud in the field of computer information.

Keywords: fraud in the field of computer information, investigation of a criminal case, computer-technical expertise (CTE), the production of investigative actions.

Совершенствование информационных и цифровых технологий предопределило возникновение нового вида мошенничества, к которому, согласно статье 159.6 Уголовного кодекса Российской Федерации, относится мошенничество в сфере компьютерной информации. На первоначальном этапе расследования следователь должен собрать информацию о совершенном деянии, что предполагает наличие достаточных знаний о компьютерных устройствах и сети Интер-

нет. Компьютер содержит информацию о способе совершения и лице, совершившем мошенничество. Компьютерные устройства содержат элементы, способные сохранять, накапливать и обрабатывать информацию, при этом часть необходимой информации хранится в сети Интернет (облачные технологии, электронная почта). Компьютер и сеть Интернет используются мошенниками как средство, инструмент для совершения преступления. Следователь должен предвидеть, что ввод, удаление, блокировка, модификация компьютерной информации, совершаемые для хищения чужого имущества, оставляют виртуальные следы в памяти компьютера [3. – С. 26]. Типичными следами являются команды, которые отправлялись с компьютера виновного и через сеть Интернет поступали на компьютер потерпевшего, при этом в сети Интернет компьютер виновного и потерпевшего можно идентифицировать с помощью IP-адреса. При совершении данного способа хищения исключается личный контакт между потерпевшим и подозреваемым.

Расследование данного вида преступления, в соответствии со статьей 151 Уголовно-процессуального кодекса Российской Федерации, отнесено к подследственности следователей органов внутренних дел, возможно также расследование данного вида преступления следователями Следственного комитета и ФСБ России, если они выявили данное преступление. Общественная опасность данного вида мошенничества заключается в том, что она представляет угрозу информационной безопасности государства. Уровень латентности компьютерного мошенничества остается достаточно высоким, так как потерпевшие не всегда желают предавать огласке факт хищения их имущества (денежных средств). Поводом для возбуждения уголовного дела по факту мошенничества в сфере компьютерной информации является заявление потерпевшего о хищении у него электронных безналичных денежных средств. Основанием для возбуждения уголовного дела являются фактические данные, указывающие на признаки преступления, которые были добыты в ходе проведения оперативно-розыскных мероприятий или в ходе доследственной проверки.

В качестве потерпевшего, у которого похитили денежные средства, выступают физические и юридические лица (банки, предприятия торговли, коммерческие организации). Свидетели, в том числе очевидцы данного преступления, как правило, отсутствуют. На стадии возбуждения уголовного дела возможны две типичные ситуации: а) заявитель обнаружил хищение безналичных денежных средств с принадлежавших ему платежных систем, и сообщил о случившемся в полицию, сведения о виновном лице ему неизвестны; б) заявитель сообщает о хищении денежных средств путем мошенничества в сфере компьютерной информации, и ему известны установочные данные виновного. По полученному заявлению может проводиться предварительная проверка. Если в ходе проведения оперативно-розыскных мероприятий выявлен факт мошенничества, то проведение предварительной проверки не требуется. На данном этапе в распоряжении следователя могут быть материалы проведенных оперативно-розыскных мероприятий.

Во всех остальных случаях проводится предварительная проверка. Сложность ее проведения состоит в том, чтобы за короткий промежуток времени найти специалиста в области компьютерной информации, провести осмотр компьютерной техники, различных приложений и программ, обнаружить и изучить виртуальные следы преступления. До возбуждения уголовного дела отрабатывается версия о возможности неосновательного получения чужого имущества из-за неосторожных действий виновного или сбоя программы. Следователю рекомендуется установить с потерпевшим психологический контакт, чтобы получить от него первоначальную информацию об обстоятельствах происшедшего события. В ходе объяснений выясняют следующие обстоятельства: а) как потерпевший узнал о хищении денежных средств, какие события предшествовали этому, был ли этот эпизод единичным; б) каким компьютером пользуется потерпевший, какие пароли, логины установлены на этом компьютере, привязаны ли банковские карты к какой-либо компьютерной программе; в) кто, кроме потерпевшего, мог знать пароли и логины для доступа в программу, не отправлял ли потерпевший по запросу кому-либо свои пароли и логины; г) чьи указания и команды он выполнял, какую информацию и кому отправлял, как представлялся и что предлагал мошенник; д) допускал ли потерпевший возможность предоставления конфиденциальной информации кому-либо, осознавал ли, что эти действия могут привести к хищению денежных средств; е) установлена ли на компьютере программа, обеспечивающая информационную безопасность потерпевшего.

Если поступали телефонные звонки на номер потерпевшего, то следователь направляет запрос оператору сотовой связи для установления владельца абонентского номера. Также в период проверки могут быть проведены оперативно-розыскные мероприятия для получения дополнительной информации – чаще всего это оперативный эксперимент, наведение справок, контрольная закупка, снятие информации с технических каналов связи и т. д. Специалисту необходимо поручить изучение сети Интернет, сайтов для обнаружения виртуальных следов мошенничества. Для установления связей в сети Интернет между физическими лицами рекомендуется использовать программное обеспечение «Maltego 24», с помощью которого осуществляется сбор необходимой информации между доменами, IP-адресами, данных по истории запросов и действий пользователя ПК [2. – С.162]. По итогам проверки следователь анализирует основание для возбуждения уголовного дела и его достаточность, определяет первоначальные следственные действия и выдвигает версии событий.

Первоначальные следственные действия ориентированы на собирание следов преступления и вещественных доказательств по уголовному делу. Проводится осмотр места происшествия и компьютерной техники в рамках единого следственного действия. Одновременно допрашивается потерпевший и, в качестве свидетелей, все лица, которые имели доступ к компьютеру. Необходимо установить факт и способ совершения мошенничества, признаки хищения (как правило, мошенники пытаются получить сведения о банковской карте, реализуют какое-либо имущество через социальные сети, требуют перевести деньги якобы с целью оказания помощи близким потерпевшего, оказывают психологическое давление на него), размер ущерба, виновное лицо или группу лиц (соучастие). Для этого надо, желательно со специалистом, провести осмотр компьютера, его элементов, связанных с памятью, изъяв (а в случае невозможности изъятия – скопировав на флеш-накопители) имеющуюся информацию. На ее основании назначается компьютерно-техническая экспертиза (КТЭ) [1. – С. 25]. Ее главная задача – ответить на вопросы, требующие специальных познаний в области форензики (компьютерной криминалистики), т. е. знаний о методах поиска, закрепления и исследования цифровых доказательств по преступлениям, связанным с компьютерной информацией (киберпреступлениям) [5. – С. 17]. Для этого собранные следы, материалы, объекты передаются в распоряжение эксперта, который исследует сетевые и лог-файлы (в них содержится информация о всех интернет-соединениях пользователя, выполненных входящих и исходящих запросах) и устанавливает IP-адреса, с которых делались запросы на компьютер потерпевшего [4. – С. 406]. Зная IP-адрес компьютера, следователь устанавливает, кому принадлежит данный адрес. Провайдер, предоставляющий интернет-услуги физическим и юридическим лицам, обязан регистрировать сервер владельца с указанием адреса, телефона, паспортных данных, что позволяет установить местонахождение компьютера и личность виновного. Правда, это не всегда возможно, так как регистрация владельцев сервера осуществляется на динамический IP-адрес, а он может принадлежать неопределенному кругу лиц. Эксперт также устанавливает возможность использования виновным вредоносных программ для хищения чужого имущества.

Производство экспертизы позволяет собрать доказательную базу по уголовному делу. Значимую помощь в расследовании кибермошенничества могут оказать специализированные организации, противодействующие мошенничеству в сфере компьютерной информации. В штате данных организаций имеются высококвалифицированные специалисты по информационным и цифровым технологиям. По итогам первоначальных следственных действий и заключения эксперта возможно проведение розыскных мероприятий для задержания подозреваемого. В жилых и служебных помещениях, занимаемых виновным, проводятся обыски с целью обнаружения и изъятия техники, следов преступления, доказательств. При наличии подозреваемого проводятся его задержание, обыск, а затем допрос.

Успех допроса кибермошенника зависит от тщательности подготовки к нему[1] и имеет свои особенности. Типичный портрет подозреваемого: мужчина 25–45 лет, умен, изворотлив, расчетлив, имеет дар убеждения, как правило, готов к задержанию, практически всегда у него заготовлены «легенды» для допрашивающих относительно происшедшего. Для обеспечения результативно-

[1] Пупцева А. В., Курин А. А. Методика расследования мошенничества: учебное пособие. – Волгоград : ВА МВД России, 2022. – С. 35.

сти допроса следует провести психодиагностику подозреваемого, учитывать его психотип. Предметом допроса подозреваемого выступают обстоятельства совершения и сокрытия преступления. Тактические приемы должны быть подобраны с учетом необходимости преодоления противодействия подозреваемого в ходе допроса.

В финансовых организациях проводится выемка документов, подтверждающих перевод денежных средств, количество транзакций. Возможно также проведение иных следственных действий для формирования доказательной базы и предъявления обвинения виновному. Целью первоначального этапа расследования кибермошенничества является обнаружение и закрепление доказательной базы, установление обстоятельств совершенного деяния, розыск и задержание подозреваемого.

Список литературы

1. *Егерева О. А., Коломинов В. В., Сизова М. С.* Некоторые вопросы методики расследования киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. – 2018. – № 4 (22). – С. 24–32.

2. *Жижина М. В., Завьялова Д. В.* Возбуждение уголовного дела по факту преступления в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы российского права. – 2021. – Т. 16. – № 12. – С. 156–166.

3. *Коломинов В. В.* Мошенничество в сфере компьютерной информации: криминалистический аспект // Baikal Research Journal. – 2015. – Т. 6. – № 1.

4. *Левченко Е. М., Корнева А. А.* Компьютерно-техническая экспертиза: предмет, объект и задачи // Вестник науки. – 2023. – Т. 3. – № 5 (62). – С. 405–409.

5. *Смолина А. Р.* Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы. Дисс. … канд. тех. наук. – Томск, 2017.