Сретенцев Д.Н., Калиничев А.Д.

НЕКОТОРЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

FEATURES OF INVESTIGATION OF CRIMES COMMITTED USING ELECTRONIC PAYMENTS

В данной статье затрагивается актуальная в настоящее время проблема расследования преступлений, совершённых с использованием систем электронных платежей, рассматриваются их виды, а также некоторые особенности расследования данной категории преступлений.

This article deals with the current problem of crimes committed using electronic payment systems, discusses their types, as well as some features of the investigation of this category of crimes.

Анализ преступлений, связанных с электронными платежами, позволяет разделить их на две группы: насильственные (грабежи, вымогательства) и денежные махинации, основанные на обмане. В отечественной правоприменительной практике вторая группа преступлений занимает особое место, поскольку сложность их раскрытия и выявления виновного субъекта зачастую вызывает существенные трудности у правоохранительных органов. Противоправная деятельность лиц направлена на извлечение денежных средств путём обмана или злоупотребления доверием. Законодатель в Уголовном кодексе РФ трактует эту категорию преступлений как мошенничество [1].

Если брать за основу криминалистическую классификацию данного рода преступлений, то можно выделить следующие виды: интернет мошенничества и кражи, вымогательства, легализация доходов, приобретённых незаконным путём, незаконная предпринимательская деятельность, получение взяток.

1. Интернет мошенничества – действия лица по построению фальшивых схем, пирамид, онлайн-аукционов и т.д., связанных с электронной оплатой; в результате злоумышленник путём обмана или злоупотребления доверием присваивает чужое имущество, пользуется и распоряжается им по своему усмотрению.

2. Интернет кражи – это хищения денежных средств путём взлома чужого электронного кошелька с полным предоставлением учётной записи злоумышленнику (логин и пароль). Данный взлом легко осуществляется, если на компьютере объекта преступления имеются какие-либо вредоносные программы.

3. Вымогательство – это противоправная деятельность лица, которая направлена на завладение чужим имуществом путём угрозы причинения насилия либо повреждения чужого имущества, либо распространения сведений, порочащих честь и достоинство лица или его близких. Данное преступление широко процветает в сети интернет и именуется как «DDoS атаки». Под угрозой этих атак подразумевается выдвижение злоумышленником предварительных требований к объекту посягательства (владельцу сервера) о выплате им определённых денежных средств на фальшивый счёт.

4. Легализация доходов, приобретённых незаконным путём. Данная деятельность достаточно подробно исследована Е.Л. Логиновым, он характеризует ее как процесс отмывания денег с помощью создания электронных счетов, через которые проходят денежные средства и впоследствии обналичиваются. Кредитные организации предпринимают множество действий для контроля данных процессов, но интерес преступников лишь увеличивается, и с каждым годом появляются всё новые способы отмывания денег [2].

5. Незаконная предпринимательская деятельность – это действия различных сайтов и контор (интернет-казино, лотереи, незаконные букмекерские компании и др.),

которые присваивают чужие денежные средства. Можно привести следующие примеры: с помощью интернет магазинов злоумышленники устраивают розыгрыши ценных призов между теми лицами, кто приобретает какой либо товар с их сайта, впоследствии выкладывают результаты не существующего розыгрыша между несуществующими лицами, тем самым обманывая клиентов; злоумышленники привязывают свой платный номер телефона к электронному кошельку, указывая вымышленное имя, и устраивают конкурс, по которому люди присылают на этот номер смс в надежде, что каждому 1000-ому будет предоставлена машина или путёвка для отдыха за границей. По итогу конкурса обещанные подарки не предоставляются.

Стратегия расследования вышеперечисленных преступлений во многом зависит от складывающихся типичных следственных ситуаций:

− выявлены все обстоятельства дела, зафиксированы показания потерпевшего, что за вирус использовал преступник, способ внедрения данного вируса, установлена личность преступника;

− установлен способ совершения преступления, исследован механизм преступления, известно предположительное местоположение преступника или преступник скрывается;

− следствию известен только результат преступления, способ и механизм его совершения не известен, личность преступника не установлена.

В первом случае необходимо определить общественно опасное деяние (проникновением в компьютер), общественно опасные последствия (заражение вирусом) и причинно-следственную связь между ними и определить размер причинённого ущерба. Во втором – организовать розыск и поимку преступника. В третьем – установить способ и механизм совершения преступления, установить личность преступника [3].

Необходимо отметить, что при расследовании преступлений, совершённых с использованием электронных платежных систем, сотрудники правоохранительных органов сталкиваются со специфической особенностью следов, связанных с такого рода преступлениями. Эти следы не могут быть восприняты без применения программно-технических средств; для придания им доказательственного значения данные электронно-цифровые следы необходимо считать с носителя в наиболее короткий срок, так как они могут быть легко уничтожены. Процессуальное закрепление и фиксация подобных следов во многом отличаются от работы с традиционными материальными следами и требуют специальной квалификации субъекта расследования.

Как правило, вещественным доказательством в рассматриваемом случае был и остается накопитель информации, обладающий свойством хранить и предоставлять для интерпретации электронно-вычислительной системе информацию в электронно-цифровой форме. Непосредственным объектом исследования становятся электронные данные, выделение которых возможно только на основании присущих свойств занимать определенное место на носителе и изменять его состояние.

Таким образом, при расследовании преступлений, совершённых с использованием электронных платежных систем, следует уделять внимание поиску технических устройств, предназначенных для оперирования электронными данными, – следы-предметы. Обнаруженные устройства должны быть направлены на экспертное исследование с целью установления способа изготовления данного средства, его технических характеристик и возможного изготовителя.

В дальнейшем при производстве судебной экспертизы объектом исследования может являться не только компьютерная техника, но и задействованная в информационных процессах оргтехника и телекоммуникационное оборудование.

Зачастую раскрыть преступления подобного рода помогает анализ информации, содержащейся в электронных почтовых ящиках, это не только тексты сообщений, но и вложения, такие как документы, счета, графические изображения финансовых документов. Переписка представляет криминалистически значимый интерес как свидетельство намерений, событий, фактов, имен, документов. Электронная почта используется в

преступных целях для координации криминальной деятельности, распространения материалов преступного содержания, мошенничества, шантажа и в том числе для рассылки вредоносных программ и вирусов.

Чтобы исследовать сообщения электронной почты, необходимо получить следующую информацию:

− об устройстве, отправившем электронное сообщение;

− о сервере-отправителе и сервере-получателе электронной почты;

− об устройстве, получателе сообщения.

Почтовые программы хранят архив отправленных и полученных сообщений электронной почты в папках (файлах) на жестком диске компьютера. Письма хранятся до удаления пользователем, однако даже после этого тексты можно попытаться восстановить. Удаленные сообщения хранятся в папке удаленных писем, однако и оттуда они могут быть удалены пользователем или в результате автоматического удаления по истечении определенного времени. Пользователь может хранить корреспонденцию в других папках и файлах [4].

Чтобы исследовать электронную почту на компьютере, имеющем выход в сеть Интернет, надо изъять компьютер или жесткий диск, сделать копию диска для экспертного исследования данной информации [5].

Анализ практики раскрытия и расследования преступлений, сопряжённых с использованием электронных платежей, показывает, что собирание и исследование доказательств в данном случае невозможно без использования специальных познаний в области электронно-коммуникационных систем. Специальные познания в данной области могут использоваться как в процессуальной форме (участие специалиста в проведении следственных и процессуальных действий, производство судебных экспертиз), так и в непроцессуальной форме (консультационная деятельность специалиста, предварительные исследования и т.д.). От того, насколько полно и глубоко при производстве следственных действий и оперативно-розыскных мероприятий выявлены, зафиксированы и изъяты следы преступной деятельности в сфере движения платежной информации, зависит успех экспертного исследования [6].

Судебные экспертизы оказывают существенное влияние на процесс раскрытия и расследования указанных преступлений. Наиболее распространены следующие их виды:

1. Судебное исследование компьютерной системы, периферийных устройств, интегрированных систем и других комплектующих компьютера.

Задачи, решаемые при данной экспертизе:

− устанавливается состояние компьютера, его фактическое и первоначальное состояние;

− производится анализ компьютера и выявления в нём каких-либо изменений в работе;

− определяется способ и механизм взлома, производится диагностика компьютера целиком и отдельных его частей.

2. Исследование программной системы компьютера.

Задачи, решаемые при данной экспертизе:

− установление характеристик программной системы, анализ состояния программного обеспечения, изучение работы программного обеспечения с аппаратными платформами;

− установление причины изменения работы программного обеспечения, изучение начальных версий программ и их копий, соотнесение и распределение программного обеспечения по группам, выявление индивидуальных факторов, позволяющих установить владельца компьютера.

3. Судебное исследование информации компьютера в целях обнаружения необходимой информации. Основная задача здесь одна – установить состояние информации и действия, направленные на её изменение, изучение информации до её удаления.

4. Судебное исследование компьютерных средств, функционирующих в сети интернет. Задачами этой экспертизы являются все задачи перечисленных выше экспертиз, разница лишь в том, что все объекты между собой связаны и функционируют в определённой сетевой технологии.

Также могут быть назначены и другие дополнительные экспертизы: судебно-трасологические, экономические, технологические и другие [3].

В основе успешного расследования преступлений, совершённых с использованием систем электронных платежей, лежит знание следователем возможностей современных информационных технологий, их уязвимых мест для злоумышленников, особенностей работы с электронно-цифровыми данными для придания им доказательственного значения, способов получения криминалистически значимой информации путем использования специальных познаний, экспертиз и исследований.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: с посл. изм. и доп. // Собр. законодательства Рос. Федерации. 1996, № 25, ст. 2954.
2. Логинов Е.Л. Отмывание денег через интернет технологии // Методы использования электронных финансовых технологий для легализации криминальных доходов и уклонения от уплаты налогов: учебное пособие. М., Юнити-Дана, 2012.
3. Расследование преступления в компьютерной сфере [Электронный ресурс]. URL: http://www.grandars.ru/college/pravovedenie/r-kompyuternyh-prestupleniy.html.
4. Гаврилов М.В., Иванов А.Н. Осмотр и предварительное исследование электронной почты на компьютере // Информатика в судебной экспертизе: сборник трудов. Саратов: СЮИ МВД России, 2003.
5. Жигалова Г.Г., Рясов А.А. К вопросу об осмотре и изъятии электронных почтовых сообщений при расследовании преступлений, совершенных с использованием средств телекоммуникации // Криминалистика: актуальные вопросы теории и практики Ростов-на-Дону, 2019.
6. Зайцев И. Е. Инновационные технологии в выявлении следовой картины "цифровых" преступлений // Инновации: Издательство: "Трансфер-Инновации" СПб, 2009.

СВЕДЕНИЯ ОБ АВТОРАХ

Сретенцев Денис Николаевич. Старший преподаватель кафедры криминалистики и предварительного расследования в ОВД. Кандидат юридических наук.

Орловский юридический институт МВД России имени В.В. Лукьянова.

Служебный адрес: 302027, г. Орел, ул. Игнатова, д. 2.

Sretentsev Denis Nikolaevich. Senior teacher of the chair of Criminalistics and Preliminary Investigation in the Internal Affairs Bodies. Candidate of legal sciences.

Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.

Work address: 302027, Orel, st. Ignatova 2.

Калиничев Андрей Дмитриевич. Курсант 3 курса факультета подготовки следователей.

Орловский юридический институт МВД России имени В.В. Лукьянова.

Служебный адрес: 302027, г. Орел, ул. Игнатова, д. 2.

Kalinichev Andrey Dmitrievich. 3 rd year cadet of the faculty of training investigators.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
Work address: 302027, Orel, st. Ignatova, 2.

Ключевые слова: электронные счета; преступления; мошенничество, информация; тактика следственных действий; судебные экспертизы.
Keywords: electronic accounts; crimes; fraud; information; tactics of investigative actions; forensic examinations.

УДК.343.1