УДК 343.9

Ушаков Степан Иванович
Всероссийский государственный университет юстиции (РПА Минюста России)
Кафедра уголовного процесса и криминалистики
Россия, Москва
u_stepan@list.ru
Ushakov Stepan
All-Russian State University of Justice (RPA of the Ministry of Justice of Russia)
Department of Criminal Procedure and Criminalistics
Russia, Moscow

СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: в данной статье автором рассматриваются способы совершения мошенничеств с использованием информационных технологий, с точки зрения важности их для науки криминалистики. Приводится понятие данных способов, основная классификация, а также их актуальные примеры.

Ключевые слова: способы совершения, мошенничества, классификация, информационные технологии, фишинг, сеть интернет.

WAYS TO COMMIT FRAUD USING INFORMATION TECHNOLOGY

Annotation: in this article, the author examines the ways of committing fraud using information technology, from the point of view of their importance for the science of criminology. The concept of these methods, the main classification, as well as their actual examples are given.

Key words: methods of commission, fraud, classification, information technology, fishing, the Internet.

Одним из признаков объективной стороны состава преступления является способ совершения преступления, который в науке уголовного права зачастую является факультативным. Однако в некоторых составах, в том числе и в мошенничестве, данный признак является обязательным, поскольку на его основании законодатель проводит разграничение кражи и мошенничества [1, с. 155].

С точки зрения криминалистики, способ совершения преступления имеет более важное значение, чем в уголовном праве, поскольку при расследовании преступления следователю необходимо установить все обстоятельства, имевшие место, независимо от того, значим ли способ совершения преступления для квалификации деяния. Поскольку только после изучения способа совершения преступного деяния, можно с точностью сказать какими именно действиями началось совершение преступления, а какими - закончилось.

В науке криминалистике нет единого мнения о понятии способа совершения преступления, данный вопрос является крайне дискуссионным. Так, например, известный советский ученый-криминалист А.Н. Колесниченко под способом совершения преступления предлагал понимать: «образ действий преступника, выражающийся в определённой последовательности, сочетании отдельных действий, приёмов, применяемых субъектом» [2, с. 119].

Другую точку зрения по этому вопросу высказывала Э.Д. Куранова, которая определяла способ совершения преступления, как: «комплекс действий по подготовке, совершению и сокрытию преступления, избранный виновным в соответствии с намеченной целью и теми условиями, в которых осуществляется преступный замысел» [3, с. 165].

Нельзя не согласиться с данным определением, ведь предопределяющим фактором выбора способа преступного деяния выступает именно цель, которую преступник хочет достигнуть посредством осуществления своего замысла, а также некоторые объективные и субъективные обстоятельства и условия.

Также важно уточнить, что именно суть использования Интернета является фактором, который разграничивает мошенничество с использованием информационных технологий от других преступлений, совершаемых в сфере компьютерной информации. Так, при совершении данного вида преступлений, информационно-телекоммуникационная сеть Интернет, в первую очередь, выполняет одновременно две основные функции:

1. С помощью различных специализированных утилит, предоставляемых современными разработчиками (например, использования VPN-сервисов) позволяет мошеннику оставаться анонимным из любой точки планеты;

2. Выступает главным средством исполнения преступного замысла, посредством которого и совершаются мошенничества с использованием информационных технологий.

Основные особенности совершения мошенничества в сети Интернет зависят от избранного злоумышленником способа совершения преступного деяния т.е. схемы, вида мошенничества, а также круга лиц, на который в конечном итоге и будет направлено преступное деяние. Этот выбор предопределяет способ реализации и конечную цель преступных намерений [4, с. 172].

Все способы совершения мошенничества с использованием информационных технологий можно объединить в следующие группы:

1. Способы, при которых используются электронная почта (преимущественно на иностранных доменных именах), мессенджеры (Telegram, WhatsApp и т.д.) и другие способы непосредственного общения в сети Интернет.

2. Способы, когда мошенник создает, а также полностью или частично копирует WEB-сайты [5, с. 77].

Отметим, что данное разделение носит весьма условный характер, поскольку, на сегодняшний день, все чаще встречаются способы, когда

преступниками используются комбинированные способы совершения мошенничеств с использованием информационных технологий.

Для лучшего понимания рассмотрим каждую из представленных групп более подробно. Так, одним из самых многочисленных и распространенных, на сегодняшний день, являются мошенничества, в которых посягательство на объект осуществляется преимущественно с помощью электронной почты или мессенджеры. Входящие в эту группу преступления характеризуют тем, что почти вся работа с жертвой проходит в форме обмена текстовыми сообщениями, а в некоторых случаях для успешного для мошенника исхода может хватить одного единственного письма.

Сообщение, направляемые мошенниками своим жертвам, как правило, соответствуют следующим критериям:

1) читабельность, краткость и эмоциональность текста;

2) убедительность и анонимность написанного (направление сообщения от имени родственников жертвы, либо обращения от лица государственных органов или банков).

Большую популярность в последние годы приобрело мошенничество в социальных сетях. Суть его, схожа с мошенничеством в мессенджерах, и состоит в том, что мошенник посредством различных способов (взлома, покупки данных и т.д.) получает полный доступ к учётным записям пользователей, а также ко всей информации, которую содержит страничка «взломанного» пользователя, в том числе возможности направлять текстовые и голосовые сообщения людям из списка друзей.

Особенность такого способа мошенничества заключается в том, что пользователь не утрачивает возможность пользоваться своей учётной записью, поэтому потенциальные жертвы из списка его контактов с большей вероятностью поступят так, как того желает мошенник (например, дадут денег в

долг, либо пройдут по присланной им вредоносной ссылке, в результате чего данные человека могут быть также похищены).

Следующей группой мошенничеств являются преступления, в которых посягательства на объект осуществляются с использованием возможностей WEB-сайтов, как основного инструмента воздействия на жертву. В частности, такими возможностями выступают создание или копирование известных интернет сайтов, на которых возмездно предоставляются товары или услуги.

Примером будут являться, способы, когда мошенники осуществляют клонирование сайта, принадлежащего какой-либо организации или органу власти (например, сайты различных ведомств, отелей, известных маркетплейсов и т.д.), клонированию подлежит вся доступная информация, вплоть до использования схожего доменного имени WEB-страниц. В данном случае для реализации преступных действий мошенником используется только интернет сайт, без использования возможностей других электронных ресурсов (например, мессенджеров). Такие сайты-клоны используются мошенниками для запутывания своих жертв, а также выманивания персональных данных или данных о кредитных картах, счетах и т.д.

Также ярким примером мошенничества являются различные способы заработка и «инвестиционные схемы», предлагаемые мошенниками на различных, созданных ими, интернет-сайтах. Способы совершения данного преступного деяния могут носить самый различный характер. В качестве примера реализации данного способа можно привести следующую общую схему.

Мошенниками создаётся сайт, предлагающий быстрый заработок и высокий доход, например, на торговле криптовалютой. Процесс описывается таким образом, чтобы у жертвы не возникло вопросов и сомнений в честности и порядочности данного предложения. Для достижения этой цели используется специальная лексики и узкопрофильные термины, которые, в конечном счёте,

могут не нести какой-либо смысловой нагрузки, однако, усложняя своим присутствием текст, способны ввести потенциальную жертву в заблуждение. После чего у жертвы, под предлогом, расходов на осуществление начала деятельности на данной платформе выманивается определённая денежная сумма. В конечном итоге, после того, как набралась достаточная сумма, либо WEB-сайт дискредитировал себя (например, наличием плохих отзывов) – интернет страница перестает существовать [6, с. 78].

Несколько слов, хотелось бы сказать, также о комбинированных способах совершения мошенничеств с использованием информационных технологий. Так, одним из популярнейших видов мошенничества в сети Интернет является фишинг (от англ. «fishing» - уловка). Суть его заключается в воровстве номеров платёжных карт и создании мошенниками самостоятельного сайта, либо клонов популярных сайтов (например, сайты популярных платежных систем), с полной сервисной поддержкой и возможностью перехода в мессенджеры от имени компании, сайт которой скопировали мошенники.

Фишинг как разновидность мошенничества имеет следующую особенность, а именно: может быть реализован с помощью сервисов обмена сообщениями, сайтов, средств сотовой либо телефонной связи, тем самым комбинируя способы совершения преступных действий.

Важно уточнить, что для достижения целей данного преступного способа важна массовость, что предполагает использование различных способов захвата большей аудитории потенциальных жертв, например, используется спама (массовая, рассылка текстовых сообщений). Его особенность заключается в следующем.

1) сообщения присылаются, как правило, от известных жертвам организаций;

2) сообщения носят массовый характер и посылаются большому количеству людей;

3) сообщения носят неперсонифицированный характер (не имеют конкретного адресата и рассылаются группам лиц);

4) очень часто письмо содержит ссылку на сайт, который либо является точной копией оригинала, либо перенаправляет пользователя на нужную преступнику страницу [7, с. 36].

Иногда вместо рассылок преступники применяют метод прозвона через мессенджеры. Данный метод применяется в тех случаях, когда мошенники получают базу данных телефонных номеров, которая по различным причинам была утеряна у различных компаний, а также банков. Данный способ заключается в том, что потенциальной жертве звонит человек или робот и сообщает, например, о фактах несанкционированного использования их кредитной карты и необходимости сообщить CVV-код карты с целью «блокировки нежелательного перевода». Таким же способом могут собираться также персональные данные людей.

Подводя итог, хотелось бы сделать вывод о том, что развитие интернет-технологий в современном мире несет, помимо положительного влияния на различные сферы жизни человека, еще и много негативных явлений, одним из которых является – мошенничество с использованием информационных технологий. Хотелось бы сказать, что вышеописанные способы совершения преступных действий не статичны и постоянно видоизменяются и совершенствуются. Это обуславливает высокую сложность в раскрытии и расследовании данного вида преступлений.

Список литературы:

1. Миникаев А.М. Проблемы разграничения составов мошенничества и отграничения их от смежных составов преступлений. Экономика и социум. 2021. № 3-2 (82). С. 154-161.

2. Колесниченко А.Н. Общие положения методики расследования отдельных видов преступлений. Харьков: Харьков. юрид. инт, 1965. – 294 с.

3. Куранова Э.Д. Об основных положениях методики расследования отдельных видов преступлений // Вопросы криминалистики. 1962. № 6-7. С. 165-166.

4. Бессонов, А. А. Способ преступления как элемент его криминалистической характеристики. Пробелы в российском законодательстве // Юридический журнал. 2014. № 4. С. 171-173.

5. Стеценко Ю. А., Холодковская Н. С. Мошенничество в сети интернет // Вестник Таганрогского института имени А. П. Чехова. 2021. № 16. С. 75-80.

6. Яковлева Л. В. Современные способы совершения дистанционного мошенничества \\ Вестник Краснодарского университета МВД России. 2021. № 11. С. 77-80.

7. Завьялов А. Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal, 2022. 13 (2). С. 36-37.