УДК 34

Вирясова Наталья Васильевна,
канд. юрид. наук, доцент кафедры правовых дисциплин,
филиал ФГБОУ ВО «КубГУ» в г. Армавире;
Землянова Анастасия Николаевна,
старший следователь следственной части
по расследованию организованной преступной деятельности
Главного следственного управления
Главного управления МВД России по Краснодарскому краю

Проблемы раскрытия и расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Аннотация. В данной статье рассмотрены актуальные проблемы раскрытия и расследования мошенничеств в сфере IT-технологий и краж с банковских карт с использованием сети интернет.

***Ключевые слова*:** мошенничество, киберпреступность, IT-технологии, основные виды и схемы совершения хищений денежных средств, дистанционное мошенничество, счет банковской карты.

Рост преступности в сфере IT-технологий стал особенно заметен во время начала пандемии коронавируса в 2019 году, поскольку большая часть населения была переведена на дистанционную работу, осуществляемую посредством сети «Интернет». Лидирующую позицию среди противоправных деяний, совершенных путем обмана, манипуляций чувствами и доверчивостью людей, на протяжении нескольких лет занимают мошенничества и краж с банковских карт с использованием сети интернет.

Так, за первое полугодие 2020 года, количество совершенных преступлений подобного рода выросло на 91,7 % по сравнению с аналогичным периодом

2019 года, во втором полугодии 2020 года данный показатель составил 92,6 % [1].

Причинами такого необычайного роста преступлений данной сфере являются стремительное понижение доходов и, соответственно низкий уровень жизни граждан; снижение престижа труда; отсутствие у большей части населения познаний о соблюдении мер безопасности при работе и приобретении товаров в сети «Интернет»; технические ошибки и несовершенства систем интернет-банкинга; низкий уровень подготовки сотрудников правоохранительных органов в сфере раскрытия и расследования дистанционных преступлений; отсутствие должного взаимодействия сотрудников ОВД с интернет провайдерами, операторами мобильных сетей и службой безопасности банков. [2]

Сама суть противоправных деяний остается прежней, но в связи с проводимыми с гражданами профилактическими мероприятиями преступникам все чаще приходится разрабатывать новые схемы и способы совершения преступлений - злоумышленникам сложно удивить или напугать взрослого и здравомыслящего человека телефонным звонком от якобы задержанного сотрудниками полиции сына, за свободу которого требуется перевести денежные средства, или звонком сотрудника службы безопасности банка, повествующего о заблокированных счетах и необходимости перевода денежных средств на безопасный счет.

На практике в настоящее время выделяют пять основных видов и схем совершения хищений денежных средств с использованием сети «Интернет» и мобильных сетей:

1. Преступление с использованием телефонного звонка – совершаемое посредством установления личностного контакта злоумышленника с потерпевшим путем телефонного звонка при котором злоумышленник вводит в заблуждение потерпевшего, сообщая информацию о попавшем в беду родственнике, близком человеке и предлагая свою помощь в обмен на денежное вознаграждение.

2. Преступление с использованием безадресного перевода – преступление, при котором потерпевшим был осуществлен перевод денежных средств на лицевой счет абонентского номера или счет банковской карты.

3. Дистанционное мошенничество, совершенное с использованием информационно-телекоммуникационной сети Интернет – преступление, при котором виновный, используя компьютерные и телефонные сети, воздействуя на сознание потерпевшего путем обмана, склоняет потерпевшего к передаче имущества удаленным способом.

4. Дистанционное мошенничество, совершенное с использованием вредоносного программного обеспечения – это преступление, совершенное при помощи специально созданной компьютерной программы, наделенной функциями неправомерного воздействия на средства электронно-вычислительной машины, реализация которых приводит к несанкционированному уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации.

5. Мошенничество, совершенное путем использования похищенной или поддельной кредитной либо расчетной карты – это преступление, совершенное при помощи операции с использованием платежной карты или ее реквизитов, не инициированной или не подтвержденной ее держателем.

Под понятием «дистанционное мошенничество», надлежит понимать мошенничество, совершенное путем обмана и злоупотребления доверием в условиях, исключающих личный контакт, с использованием средств мобильной связи и (или) сети «Интернет» (путем распространения вредоносного программного обеспечения и иными способами), под воздействием которого владелец имущества или иное лицо передают имущество или право на имущество другому лицу, либо не препятствует его изъятию. Указанные преступления надлежит квалифицировать по статье 159 УК РФ [3, с. 110].

Кроме того, квалификации по статье 159 УК РФ, подлежат действия злоумышленника, при которых:

- потерпевший под влиянием сообщенной ему ложной информации самостоятельно перечисляет денежные средства преступнику, при этом осознавая, что принадлежащие ему денежные средства получит другое лицо;

- потерпевший под влиянием обмана самостоятельно перечисляет на счет другого лица принадлежащие ему денежные средства, но не осознает этого;

Вместе с тем, квалификации по статье 159.3[3, с. 114] подлежат случаи хищения денежных средств со счета банковской карты, фактически находящейся у потерпевшего, либо выбывшей из его пользования (например, в связи с утратой); хищение совершается под предлогом продажи товара посредством сеть «Интернет», осуществления пожертвований на счет организации либо под иными предлогами.

Кроме того, квалификации по статье 159.6[3, с. 116] подлежат случаи совершения мошенничества с использованием различных вредоносных программ, с помощью которых осуществляется целенаправленное воздействие на серверы, компьютеры, смартфоны, снабженные соответствующим программным обеспечением, которое позволяет злоумышленнику незаконно завладеть чужим имуществом или приобрести право на него.

При этом, часть аналогичных преступлений с использованием информационно-телекоммуникационных технологий, подлежат квалификации по п. «г» ч. 3 ст. 158 УК РФ – кража с банковского счета, а равно в отношении электронных денежных средств:

- если потерпевший под влиянием обмана самостоятельно называет преступнику данные своей банковской карты, в результате чего последний получает доступ к хранящимся на счете денежным средствам и совершает их хищение (при этом потерпевший в момент совершения в отношении него преступления не осознает, что в результате его действий принадлежащие ему денежные средства поступят в распоряжение другого лица);

- если лицо, путем незаконного получения доступа к мобильному банку потерпевшего, приложению «Сбербанк Онлайн», либо иному аналогичному

приложению, тайно похитило денежные средства со счета потерпевшего;

- если хищение произошло с банковской карты, выбывшей из владения потерпевшего, путем обналичивания денежных средств через банкомат.

При росте преступности в сфере IT-технологий, сотрудники правоохранительных органов до настоящего времени не обладают необходимым для предотвращения, раскрытия и расследования указанных преступлений техническим оснащением. Кроме того, взаимодействие сотрудников ОВД с интернет провайдерами, операторами сотовых сетей, а также службами безопасности банков, находится на низком уровне, что не позволяет в полном объеме оперативно получать и использовать информацию, необходимую для установления личности преступника.

Для решения указанной проблемы в системе МВД России созданы обособленные подразделения, специализирующиеся на раскрытии и расследовании преступлений в сфере IT-преступлений, однако до настоящего времени сотрудники правоохранительных органов не наделены полномочиями, позволяющими в полном объеме получать все необходимые сведения, что влечет неумолимый рост количества совершаемых в данной сфере преступлений, а также уход от уголовной ответственности лиц, их совершивших. В связи с этим, большинство указанных преступлений остаются не раскрытыми, а преступники уходят от уголовной ответственности и создают новые способы и схемы совершения преступлений.

Список литературы

1. Распоряжение врио начальника Главного следственного управления ГУ МВ России по Краснодарскому краю А.С. Степанькова №5р от 07.03.2019: Об организации проведения доследственной проверки и производства предварительного следствия по уголовным делам о «дистанционных» мошенничествах. – Краснодар. – Текст: непосредственный.

2. Уголовный кодекс Российской Федерации: УК: текст с изменениями и дополнениями: [принят Государственной думой 24 мая 1996 года: одобрен Советом Федерации 5 июня 1996 года]. – Москва. – 10000 экз. – ISBN 978-5-39233579-4. – Текст: непосредственный.

3. Василенко, Н.А. Преступления в сфере информационных технологий (киберпреступность)

/ Василенко, Н.А. – Текст : электронный // Старт в науке : [https://science-start.ru]. – 2016. – № 5. – URL: https://science-start.ru/ru/article/view?id=428 (дата обращения: 25.01.2021).