Шабанов Антон Александрович,
Магистрант 2 курса очной формы обучения
Центральный филиал,
Российский государственный университет
правосудия им. В.М. Лебедева

Научный руководитель:
Комбарова Елена Леонидовна,
Доцент кафедры судебной экспертиза и криминалистики
кандидат юридических наук, доцент, Центральный филиал,
Российский государственный университет
правосудия им. В.М. Лебедева

ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ И КРИМИНАЛИСТИЧЕСКИЕ ВЕРСИИ, ВОЗНИКАЮЩИЕ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Аннотация. В работе анализируются наиболее характерные следственные ситуации, возникающие в процессе расследования мошенничества, связанного с использованием электронных средств платежа. Рассматриваются особенности формирования криминалистических версий на различных стадиях предварительного расследования, выявляются проблемы, связанные с получением и закреплением цифровых доказательств, а также предлагаются практические рекомендации по организации следственных действий.

Ключевые слова: Мошенничество, электронные платежи, следственная ситуация, криминалистическая версия, цифровые доказательства, расследование.

Современный этап развития финансовых технологий сопровождается активным внедрением электронных средств платежа в повседневную жизнь. Банковские карты, онлайн-банкинг, мобильные приложения и цифровые валюты существенно упростили проведение финансовых операций, однако одновременно стали инструментом совершения новых форм преступлений.

Мошенничество в данной сфере отличается высокой динамичностью, использованием сложных технических решений и значительным объемом цифровой информации, оставляемой злоумышленниками. В связи с этим расследование подобных преступлений требует междисциплинарного подхода, сочетающего правовые, технические и аналитические знания.

Следственные ситуации по таким делам нередко быстро изменяются, что обусловлено постоянным совершенствованием преступных схем и средств сокрытия следов.

Под мошенничеством с использованием электронных средств платежа следует понимать противоправное завладение денежными средствами посредством обмана или злоупотребления доверием с применением электронных платежных инструментов.

К числу таких инструментов относятся:

- банковские карты;
- системы дистанционного банковского обслуживания;
- электронные кошельки;
- мобильные платежные сервисы;
- криптовалютные платформы.

Характерными признаками данных преступлений являются:

- использование электронного платежного инструмента в качестве средства или объекта посягательства;

- совершение финансовых операций без осознанного согласия владельца средств;
- применение технологий, направленных на обход систем защиты и сокрытие следов;
- наличие цифровых данных, фиксирующих действия злоумышленника (логи, IP-адреса, метаданные).

Указанные особенности определяют специфику расследования: необходимо установить не только сам факт хищения, но и механизм получения доступа к денежным средствам, а также траекторию их движения.

Типичные следственные ситуации

Следственная ситуация представляет собой совокупность исходной информации и условий, в которых принимаются решения о направлении расследования.

Н.В.Олиндер выделяет следующие типичные ситуации первоначального этапа расследования:

1) «информация о мотивах, способе совершения преступления и личности преступника отсутствует (полная информационная неопределенность) (например, пропажа денег из электронного кошелька).

2) имеются сведения о мотиве, способе совершения преступления, но нет сведений о личности преступника (частичная информационная неопределенность) (видно, на какой счет перечислили электронные средства, но не видно, как и кто).

3)известны мотивы, способы совершения и сокрытия преступления, личность преступника и другие обстоятельства (информационная определенность) (когда есть возможность проследить всю цепочку перечислений электронных платежных средств и предположительно выявить виновное лицо)» [1, с.88].

Криминалистические версии

Криминалистическая версия представляет собой обоснованное предположение о механизме совершения преступления, подлежащее проверке в ходе расследования.

Наиболее часто выдвигаются следующие версии о механизме события:

1). Использование методов социальной инженерии.

Одной из наиболее распространённых является версия о получении злоумышленником конфиденциальных данных путем психологического воздействия на потерпевшего.

Для её проверки анализируются:

- коммуникации (сообщения, звонки);
- обстоятельства передачи данных;
- используемые мошенниками сценарии.

2). Эксплуатация технических уязвимостей.

В случае отсутствия действий со стороны потерпевшего рассматривается возможность несанкционированного доступа вследствие недостатков в системе защиты.

Проверка включает:

- анализ серверных логов;
- исследование программного обеспечения;
- проведение технических тестов.

3). Причастность сотрудников организаций.

Отдельного внимания требует версия о внутреннем содействии. Она предполагает участие сотрудников финансовых или обслуживающих организаций.

В этом случае изучаются:

- права доступа;
- служебные связи;
- возможные мотивы.

Как отмечает а.и.анапольская, версия о наличии сговора преступника с сотрудником банковского учреждения выдвигается в 49% случаев [2, с.135].

4). Деятельность организованной группы.

Нередко преступления совершаются группами с распределением функций (создание инфраструктуры, взаимодействие с жертвами, обналичивание средств). Проверка данной версии требует комплексного подхода и координации действий различных подразделений.

Основные направления расследования.

1. Обнаружение несанкционированных операций.

Как правило, поводом для возбуждения дела служит обращение потерпевшего или представителя банка, выявившего подозрительные списания.

На начальном этапе следователь располагает следующими сведениями:

- параметры транзакций (время, сумма, получатель);
- технические данные соединения (ip-адреса, устройства);
- сведения о географическом расположении точек доступа.

Основной задачей является установление способа компрометации данных: фишинг, подбор учетных данных, утечка информации либо внедрение вредоносного программного обеспечения.

2. Исследование цифровых носителей.

При изъятии электронных устройств проводится их криминалистическое исследование. Внимание уделяется:

- истории интернет-активности;
- данным авторизации в платежных сервисах;
- следам установки подозрительных программ;
- активности вредоносных приложений.

Эффективность данной работы напрямую зависит от качества проведённой компьютерно-технической экспертизы.

3. Установление схемы движения денежных средств.

Значительная сложность возникает при анализе цепочек транзакций, поскольку похищенные средства, как правило, быстро распределяются между различными счетами.

В рамках этой ситуации необходимо:

- проследить финансовые потоки;
- выявить взаимосвязи между участниками;
- получить информацию от банков и платежных систем.

4. Наличие иностранного элемента.

При использовании зарубежных сервисов расследование осложняется необходимостью международного взаимодействия. В таких случаях требуется:

- направление запросов о правовой помощи;
- взаимодействие с иностранными финансовыми структурами;
- учет особенностей зарубежного законодательства.

Ключевое значение имеет правильное изъятие и фиксация цифровой информации. Важно обеспечить:

- сохранность исходных данных;
- документирование процесса изъятия;
- соблюдение требований к хранению доказательств;
- взаимодействие с провайдерами.

Нарушение указанных требований может привести к утрате доказательственной силы информации.

Многоуровневые схемы переводов требуют применения специализированных аналитических инструментов, позволяющих визуализировать движение средств.

Использование средств анонимизации (vpn, прокси-серверы, подставные аккаунты) существенно затрудняет идентификацию злоумышленников, что требует комплексного анализа цифровых и поведенческих признаков.

При этом сбор доказательств часто вызывает определенные проблемы. Необходимо знание технологий защиты банковских карт, содержания положений об их использовании, но не всегда такими специальными познаниями обладают следователи. Снижает оперативность расследования и необходимость получения судебного решения для установления банковских операций ввиду наличия банковской тайны [3, с.35].

В целях повышения эффективности расследования целесообразно:

- оперативно фиксировать цифровые следы;
- привлекать специалистов в области информационных технологий;
- выдвигать и проверять альтернативные версии;
- использовать экспертные знания в сфере криптовалют;
- активно применять механизмы международного сотрудничества.

Таким образом, расследование мошенничества с применением электронных средств платежа представляет собой сложную и многоаспектную деятельность, требующую высокой профессиональной подготовки. Успех расследования во многом определяется способностью следователя правильно оценить исходную ситуацию, выдвинуть обоснованные версии и эффективно организовать процесс сбора доказательств. Представленные в статье подходы и рекомендации могут быть использованы как в практической деятельности, так и в образовательных целях.

Список литературы:

1. Олиндер Н.В. Следственные ситуации на первоначальном этапе расследования преступлений, совершенных с использованием электронных платежных средств и систем // Юридический вестник СамГУ. – 2015. – Т.1- №4. – С.87-91.

2. Анапольская А.И. Типичные следственные ситуации и версии первоначального этапа расследования мошенничеств с электронными счетами // Вестник ТГУ. – 2015. - №8 (148). – С.133-138.

3. Данильян А.С. Вопросы квалификации и расследования преступлений, совершенных с использованием электронных средств платежа // Общество и право. – 2022. - №3 (81). – С.32-36.