УДК 343.72

Крюкова А.С.,
курсант
4 курс, факультет подготовки специалистов
по расследованию экономических преступлений
Федеральное государственное казенное образовательное учреждение
высшего образования «Нижегородская академия Министерства
внутренних дел Российской Федерации»
Россия, г. Нижний Новгород

ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Аннотация: *В статье рассматриваются особенности методики расследования мошенничества, совершенного в сети Интернет, обозначены виды мошенничеств в сети Интернет, современные проблемы, с которыми сталкиваются органы внутренних дел в своей работе и пути их решения.*

Ключевые слова: *мошенничество, Интернет, мессенджер, методика, электронные следы, преступление.*

Annotation: *the article discusses the features of the methodology for investigating fraud committed on the Internet, identifies the types of fraud on the Internet, the current problems faced by the internal affairs bodies in their work and ways to solve them.*

Keywords: *fraud, Internet, messenger, technique, electronic traces, crime.*

Начало нового тысячелетия ознаменовалось активным развитием информационных технологий, отразившееся на всех сферах жизни общества. Однако, в свою очередь, развитие информационных технологий привело и к

тому, что они все более часто стали использоваться для совершения хищений и иных противоправных действий [1, с.35].

Мошенничество, как одна из разновидностей хищения, характеризуется изъятием и обращением в свою пользу имущества путем обмана или злоупотребления доверием [2]. Анализ следственной практики показал, что в настоящее время при использовании информационно-телекоммуникационной сети «Интернет» появились следующие способы его совершения.

1. Фишинг – данный вид мошенничества заключается в получении злоумышленниками персональных данных людей, логинов, паролей или реквизитов карты под видом вымышленного интернет-сайта, целью которого является совершение хищения денежных средств.

2. Взлом аккаунта в социальных сетях с последующим написанием контактам пользователя, которого взломали, сообщений с просьбой одолжить в займы денежные средства. После этого мошенник сообщает реквизиты банковской карты, на которую необходимо перевести денежные средства.

3. Мошенничество в интернет-магазинах – преступник создает страницу или группу в социальной сети (Вконакте, Инстаграмм, Фейсбук и др.), позиционирует себя как интернет-магазин. В дальнейшем он принимает заказы, получая денежные средства за покупку, товар он не направляет покупателю [3, с.97].

4. Мошенничество с использованием IP-телефонии – мошенничество, которое заключается в подмене номера телефона и последующих звонках абонентам под предлогом службы безопасности кредитной организации, а также иных легенд с целью получения денежных средств от собеседника.

Каждый вид мошенничества оставляет следовую картину, которая наполнена электронными следами и их взаимосвязь образует «клубок», который необходимо распутывать сотрудникам ОВД. На конце этого «клубка» они ожидают найти преступника, однако в ходе расследования им редко

удается получить интересующую их информацию, потому что предстоит встретиться с нюансами, которые тормозят процесс изобличения злоумышленника, а также обнажает проблемы, которые испытывает система МВД России.

Проблемы, которые имеются на сегодняшний день в расследовании мошенничества в сети Интернет во многом связаны с компьютерно-техническим аспектом, и как правило, в одной из сложнейших следственных ситуаций – когда подозреваемый неизвестен и информация о нем отсутствует. В данной ситуации необходимо получить информацию от потерпевшего, а если конкретно, то всю следовую картину, которая присутствует в его гаджете, через который он связался с мошенниками.

Следы, которые появляются в процессе совершения мошенничества в сфере информационно-телекоммуникационных технологийделятся на три группы:

1. Электронные следы, которые появляются при размещении информации, применимо к мошенничествам в интернет-магазинах (спам-рассылки, следы взаимодействия с рекламными площадками, а также системами обмена баннерами, регистрационные данные на доменное имя, лог-файлы от взаимодействия с регистратором доменных имен; следы от проведения платежа этому регистратору, следы от взаимодействия с хостинг - провайдером, у которого размещен сайт мошенников и куда происходил залив контента и т.п.).

2. Следы, которые создает потерпевший, которые связывают его со злоумышленником (следы при приеме заказов – по электронной почте, по ICQ, через веб-форму, социальные сети; копии сообщения на компьютере отправителя и получателя, следы в логах провайдеров (например, статистика трафика), запись в логе каждого MTA, через который сообщение прошло,

логины антивирусов и программ, предназначенных для фильтрации информации и защиты от спама, иные следы.

3. Следы, которые появляются при переводе денежных средств (следы при осуществлении ввода, вывода и осуществления перевода денег в платежных системах – Webmoney, e-gold, StormPay, RUpay, RBKMoney, Qiwi, Яндекс-деньги, МОНЕТА.РУ и другие; на серверах платежных систем остаются данные об операциях с интересующими нас счетами, данные пользователей, конкретное время проведения операций со счетами, следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия, а также многие другие сведения; реквизиты счетов, на которые осуществлен перевод денежных средств, полученные как от потерпевшего, так и из рассылок, рекламы, на сайте мошенников и другими способами).

При совершении мошенничества в сфере информационно-телекоммуникационных сетей необходимо организовать алгоритм проведения первичных и последующих следственных действий и оперативно-разыскных мероприятий. В первую очередь при поступлении заявления о дистанционном мошенничестве необходимо связаться с пострадавшим и потребовать не удалять информацию, которая остается после совершенного преступления. Необходимо получить документы, представленные потерпевшим в подтверждение фактов оплаты, перевода денежных средств и т.п., что послужит доказательством для установления причиненного ущерба.

Далее с участием специалиста необходимо провести изъятие персонального компьютера потерпевшего для его детального последующего осмотра, при этом изъятие необходимо проводить с созданием условий, препятствующих подключению электронного устройства к электрической сети или другим электрическим устройствам [4, с.54]. Также необходимо провести процессуальные действия, направленные на получение от кредитно-финансовых учреждений информации об открытии расчетных счетов, на

которые были переведены денежные средства, а также кем были открыты расчетные счета.

Также требуется получить информацию о соединениях между абонентами путем проведения выемки у сотовых компаний, предоставляющих услуги связи, а также информацию о сим-картах, после чего провести комплекс необходимых оперативно-разыскных мероприятий, направленных на установление местонахождения предполагаемых злоумышленников. После чего принять меры к их задержанию.

Анализ криминалистической характеристики рассматриваемой группы преступлений позволяет сделать вывод, что кроме основных следов, которые присущи широкому кругу преступлений, для мошенничества в сети Интернет характерна особая группа следов – цифровые следы.

Их особенность характеризуется возможностью легкого удаления или модификации. Еще одна особенность характеризует цифровые следы как легко распространяемые, иными словами, они могут быть распространены в компьютерных сетях из любой точки мира. Особенно актуально это в эпоху цифровизации информационного общества, когда организации переходят на удаленный способ осуществления трудовой деятельности.

При этом локализация цифровых следов осуществляется не в одном конкретном месте, например, в месте нахождения преступника, а по пути прохождения всего информационного сигнала, что, в свою очередь, позволяет правоохранительным органам выявлять и фиксировать их.

Основными характеристиками цифровых следов являются (рисунок 1): [5, с.20-26].

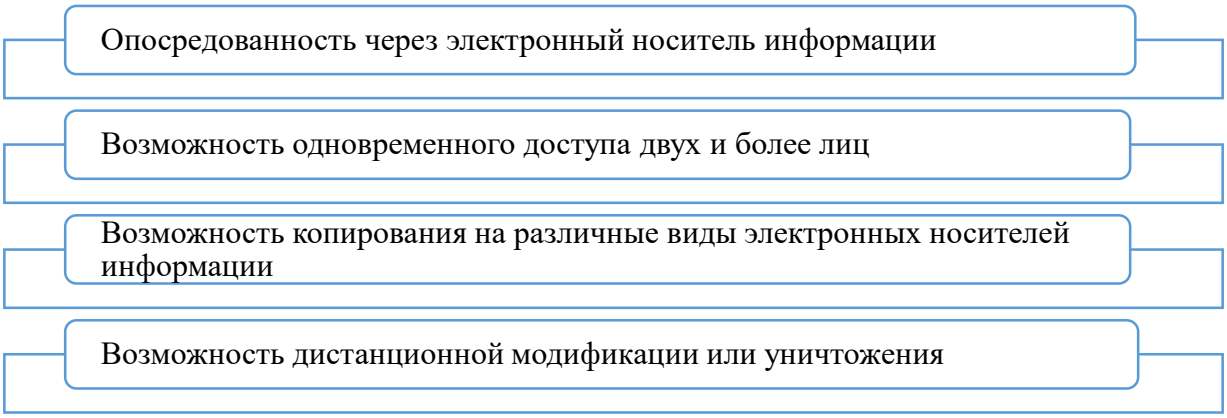

Рисунок 1 – Характеристика цифровых следов мошенничества в сети Интернет

Наличие указанных особенностей свидетельствует о том, что лицо, которое осуществляет их фиксацию, должно обладать специальными знаниями. Не каждый сотрудник правоохранительных органов сумеет грамотно и эффективно использовать их в целях расследования и раскрытия уголовного дела.

Необходимо отметить, что на данный момент, несмотря на высокие темпы развития общества и существующего технического прогресса, можно выделить следующие основные проблемы, связанные с расследованием мошенничества в информационно-телекоммуникационной сети Интернет:

1. слабая научная база;
2. недостаточная квалификация лиц, занимающихся расследованием данных преступлений;
3. недостаточность практики расследования некоторых видов Интернет-мошенничества;
4. относительно большое количество преступлений, остающихся нераскрытыми;

5. отсутствие взаимодействия с иностранными компаниями, предоставляющими услуги, связанными с IT-технологиями;

6. утечка в сеть информационных баз с персональными данными;

7. излишняя доверчивость граждан, так как по статистике в большинстве случаев люди теряют свои деньги, потому что сообщают мошенникам свои полные реквизиты банковской карты.

Таким образом, для решения проблемы расследования мошенничеств в информационно-телекоммуникационной сети Интернет необходимо:

1. усовершенствовать техническую базу системы МВД России;

2. обучить сотрудников органов внутренних дел теоретическим аспектам, позволяющим понимать оперативную обстановку, а также понимать следовую картину, возникающую при совершении дистанционного мошенничества;

3. наладить взаимодействие с организациями, предоставляющими услуги связи интернет-соединений по всему миру;

4. продолжать вести профилактическую работу с гражданами, постоянно информировать о новых видах мошенничества.

Таким образом, при встрече с мошенниками гражданам необходимо критически воспринимать любые предложения и условия, перепроверять информацию и никогда не торопиться при принятии решений. Никому ни при каких обстоятельствах не сообщать полные реквизиты банковской карты, а для покупок в интернет-магазинах приобрести отдельную банковскую карту, на которой будет храниться небольшая денежная сумма необходимая для совершения покупки.

Библиографический список:

1. Зайцев А.А., Смолин А.В. О некоторых элементах криминалистической характеристики киберпреступлений // Криминалистика: вчера, сегодня, завтра, 2019. № 3 (11). С. 35-41.

2. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021)

3. Шут, О.А. Мошенничество в социальных сетях и способы его осуществления / О.А. Шут // Вестник Омского университета. Серия право. – 2020. - №4. – С. 97-106.

4. Смолин А.В., Зайцев А.А. Тактика производства отдельных следственных действия по преступлениям, совершенным с применением компьютерной техники // Криминалистика: вчера, сегодня, завтра, 2019. № 4 (12). С. 52-57.

5. Давыдов, В.С. Цифровые следы в расследовании дистанционного мошенничества / В.С. Давыдов, И.В. Тишутина // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. - №3. – С. 20-26.