СЛЕДОВАЯ КАРТИНА В МЕТОДИКЕ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

В. С. Якимёнок, Д. А. Гросс

Научный руководитель: В. С. Гальцов, доцент кафедры
государственно-правовых дисциплин, кандидат юридических наук, доцент

Развитие информационных технологий оказывает положительное влияние на все сферы жизни общества, однако в период стремительного развития цифровой экономики и глобальной информатизации общество столкнулось с серьезной проблемой – мошенничеством в сети Интернет. Децентрализованная структура сети Интернет и отсутствие национальных границ в киберпространстве предоставляют возможности для роста преступности и сдерживают механизмы социального и правового контроля в сфере использования информационных сетей для совершения преступлений.

На сегодняшний день наблюдается снижение числа преступлений в сфере информационных технологий, что подтверждается статистикой: в 2020 году следователями возбуждено 25 571 уголовное дело, в 2021 – 15 503. Количество зарегистрированных преступлений по ст. 212 Уголовного кодекса Республики Беларусь (хищение путем модификации компьютерной информации) в первом квартале 2022 года – 2 833, а в аналогичный период 2021 года – 5 734 преступления [1].

Однако, несмотря на положительную статистику киберпреступлений, проблема расследования мошенничества в сети Интернет остается актуальной, так как кибермошенники используют различные способы социальной инженерии. Специфику способа совершения преступления отражает следовая картина преступления.

В связи со сказанным выше, и итогов проведенных нами исследований, мы предлагаем свой взгляд на отдельные аспекты следовой картины в методике расследования мошенничества в сети Интернет.

Проведенный нами анализ публикаций на исследуемую тему, позволил определить наиболее распространенные виды мошенничества в сети Интернет на территории Беларуси. Так, Оперативно-аналитический центр при Президенте Республики Беларусь дает следующую их классификацию:

1) Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.);

2) Вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои

конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.

3) Смишинг – вид мошенничества (англ. smishing – SMS + phishing), целью которого является переход по ссылке из SMS или загрузки вредоносного программного обеспечения. Смишинг-сообщение обычно имеет схожий внешний вид сообщения от банка, государственного учреждения, оператора электросвязи, известного магазина, а также о внезапном выигрыше в лотерею или акции и т.д [2].

Добавляя к выше описанным способам мошенничества следует указать, что правоохранителями выявляются на территории Беларуси случаи мошенничества в интернет-магазинах, когда преступник создает страницу или группу в социальной сети и позиционирует себя как интернет-магазин: получая заказ от покупателя, принимает от него оплату за товар, а сам товар не направляет.

Изученный нами опыт правоохранителей позволяет говорить о том, что следовую картину мошенничества в сети Интернет составляют как традиционные, так и цифровые следы.

К традиционным следам мошенничества в сети Интернет можно отнести: следы человека в местах нахождения конкретного лица в момент совершения преступления (отпечатки пальцев рук на клавиатуре и других компьютерно-технических средствах, внешний облик при встрече с жертвой преступления или при совершении преступниками подготовительных действий, например, при заключении договора об услугах провайдера, по записи камеры видеонаблюдения); следы используемых транспортных средств; средств связи и т.п. [3, с. 14].

Для расследования мошенничества в сети Интернет следует в первую очередь обратить внимание на выявление и исследование следующих видов цифровых следов:

1) электронные следы, которые появляются при размещении информации, применимо к мошенничествам в интернет-магазинах (спам-рассылки, следы взаимодействия с рекламными площадками);

2) следы, которые создает потерпевший, которые связывают его со злоумышленником (следы при приеме заказов – по электронной почте, через веб-форму, социальные сети; копии сообщения на компьютере отправителя и получателя);

3) следы, которые появляются при переводе денежных средств (следы при осуществлении ввода, вывода и осуществления перевода денег в платежных системах [4, с. 227].

Цифровые следы остаются на машинных носителях информации и отражают изменения в хранящейся в них информации. Их особенность заключается в возможности легкого удаления или модификации, высокой скорости трансформации. А также цифровые следы характеризуются как легко распространяемые, так как они могут быть распространены в компьютерных

сетях из любой точки мира, их локализация осуществляется не в одном конкретном месте, а по пути прохождения всего информационного сигнала.

Специфика цифровых следов определяет сложность работы с такими следами и вызывает необходимость в специальной подготовке правоохранительных органов.

Первого апреля 2021 года на заседании координационного совещания по борьбе с преступностью и коррупцией в Витебской области участники совещания отметили, что отрицательное влияние на состояние киберпреступности оказали упущения в работе органов дознания и следствия по выявлению, раскрытию и расследованию таких преступлений [5].

Опыт правоохранительных органов показывает, что особенности цифровых следов не позволяют лицу, осуществляющему производство по делу, самостоятельно, грамотно и эффективно работать с ними.

А. И. Васильев, заместитель председателя Следственного комитета Республики Беларусь, рассказал корреспонденту об использовании следователями автоматизированной информационной системы «След», которая представляет собой учет всех следов, оставленных преступником в сети и позволяет исходя из цифровых следов выявить закономерность и находить другие эпизоды. Однако А.И. Васильев подчеркнул, что «След» - это своего рода ориентирующая информация, а аналитической деятельностью обязан заниматься следователь [1].

Использование автоматизированных информационных систем представляется нам перспективным направлением в расследовании мошенничества в сети Интернет. Однако несмотря на помощь следователю в поиске информации, которую оказывают информационные системы, анализировать ему ее предстоит самостоятельно. В связи с этим, нами разделяется предложение, выдвинутое Е. Р. Россинской, о расширении информационно-компьютерной составляющей в подготовке будущих следователей либо в рамках основных образовательных программ, либо путем профессиональной подготовки или повышения квалификации в области расследования преступлений, сопряженных с использованием компьютерных средств и систем [6, с. 35-36].

Таким образом, следовую картину мошенничества в сети Интернет составляют традиционные и цифровые следы. Наличие цифровых следов определяет специфику методики расследования мошенничества в сети Интернет. Выявление, фиксация и исследование таких следов представляют непростую задачу для правоохранительных органов. Использование информационных систем в расследовании исследуемого вида мошенничества является инновационным направлением, однако так как анализ информации из этих систем осуществляется следователями, нам представляется целесообразным организовать подготовку следователей в области информационных технологий.

Список использованных источников:

1. Васильев, А. И. Коррупция, киберпреступность, терроризм: Зампред СК о текущей обстановке и работе [Электронный ресурс] / А. И. Васильев // БЕЛТА. – 2022. – Режим доступа: <https://www.belta.by/interview/view/korruptsija-kiberprestupnost-terrorizm-zampred-sk-o-tekuschej-obstanovke-i-rabote> 8147?ysclid=1c61b8q236273892378. – Дата доступа: 26.12.2022.
2. Оперативно-аналитический центр при Президенте Республики Беларусь [Электронный ресурс]. – Режим доступа: <https://www.oac.gov.by/fighting-telecom-fraud/phishing>. – Дата доступа: 15.12.2022.
3. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: автореф. дис. ... д-ра юрид. наук : 12.00.12 / В. В. Коломинов; Байкальский госуд. ун-т. – Краснодар, 2017. – 25 с.
4. Крюкова, А. С. Особенности методики расследования мошенничества в сети Интернет / А. С. Крюкова // Аллея науки. – 2022. – Т.1. – № 2(65). – С. 225–230.
5. Генеральная прокуратура Республики Беларусь [Электронный ресурс]. – Режим доступа: <https://prokuratura.gov.by/ru/media/sobytiya-i-meropriyatiya/prokuratura-vitebskoy-oblasti-na-koordinatsionnom-soveshchanii-о bsudili-voprosy-borby-s-kiberprestup/>. – Дата доступа: 26.12.2022.
6. Россинская, Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е. Р. Россинская // Вестник университета имени О.Е. Кутафина (МГЮА). – 2019. – № 5. – С. 35–36.