УДК 343.985 DOI 10.51980/2686-939X_2023_4_77

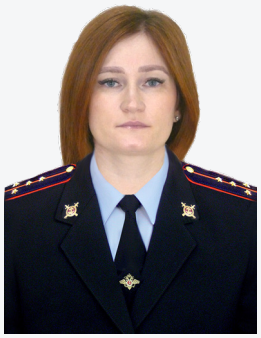
ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВАМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: СОВРЕМЕННОСТЬ И ПЕРСПЕКТИВЫ

COUNTERING FRAUD COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES: MODERNITY AND PROSPECTS

Анастасия Александровна Убоженко,

дознаватель отделения по расследованию преступлений против собственности, совершенных с использованием информационно-телекоммуникационных технологий отдела дознания МУ МВД России «Красноярское»

aubozhenko5@mvd.ru



Ключевые слова:
киберпреступность, мошенничество, информационно-телекоммуникационные технологии, информационная безопасность, раскрытие, расследование, противодействие, антифрод.

В статье проводится анализ статистических данных, характеризующих динамику преступности с использованием информационно-телекоммуникационных технологий, и мошенничества в частности, совершаемых на территории Российской Федерации. Рассматривается проблематика раскрытия и расследования мошенничеств указанной категории. Автор акцентирует внимание на отличительных признаках мошенничеств указанной разновидности, проблемах, возникающих при их раскрытии и расследовании, перспективных направлениях предупреждения, межведомственном взаимодействии для этой цели правоохранительных и иных органов государственной власти.

Keywords:
cybercrime, fraud, information and telecommunication technologies, information security, disclosure, investigation, counteraction, anti-fraud.

The article analyzes statistical data characterizing the dynamics of crime using information and telecommunication technologies, and fraud in particular committed on the territory of the Russian Federation. The problems of disclosure and investigation of frauds of this category are considered. The author of the article focuses on the distinctive features of fraud of this type, the problems that arise during their disclosure and investigation, promising areas of prevention, interdepartmental cooperation for this purpose by law enforcement and other public authorities.

Цифровая трансформация современного общества, появление и развитие новых технологий, затрагивающих все без исключения сферы его жизнедеятельности, доступ посредством сети Интернет к информационным ресурсам и, наконец, развитие искусственного интеллекта, несомненно, позволили за относительно недолгий период (примерно с 50-х годов прошлого столетия) сделать жизнь человека значительно удобнее и комфортнее. Компьютер и смартфон стали неотъемлемыми атрибутами повседневного быта, позволяющими не только слышать и видеть абонента, находящегося порой за тысячи километров, но и дали возможность дистанционного получения финансовых, банковских и государственных услуг, образования, покупки товаров и даже осуществления трудовой деятельности. Согласно отчету агентства We Are Social[1], по состоянию на 2022 год более 67,1% населения мира использовали мобильные телефоны, 62,5% имели доступ к сети Интернет. В России пользователями Интернета являлись 90% населения[2], а услуги мобильных операторов уже вошли в число потребностей первой необходимости.

К сожалению, столь быстрое движение по пути прогресса обусловило появление новых угроз в контексте информационной безопасности, когда достижения в сфере информационно-телекоммуникационных технологий все чаще стали использоваться для совершения преступлений. При этом наблюдается неутешительная закономерность: чем выше цифровизация, тем больше существует потенциальных возможностей для совершения преступных посягательств и тем выше уровень преступности с использованием информационно-телекоммуникационных технологий.

Наглядным подтверждением вышеуказанного являются результаты анализа криминогенной обстановки на территории Российской Федерации за 2018-2022 годы. Так, количественные показатели зарегистрированных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и компьютерной информации (далее – преступления ИТТ) имеют устойчивую тенденцию в сторону увеличения (174674 преступления – в 2018 году, 522065 – в 2022 году, рост почти в 3 раза за 5 лет)[3]. И, несмотря на то, что, по данным МВД России, в 2022 году отмечался незначительный прирост количества зарегистрированных преступлений ИТТ (всего на 0,8%), по состоянию на конец июля 2023 года преступлений указанной категории зарегистрировано уже на 27,9% больше, чем за аналогичный период прошлого года.

Значительную долю преступлений ИТТ составляют мошенничества (далее – IT-мошенничества). Согласно статистической информации за 2022 год, 49,3% общего объема зарегистрированных преступлений ИТТ приходилось на IT-

1 Digital 2022: another year of bumper growth. URL: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2. (дата обращения 01.09.2023).

2 Чернышенко: 90% населения России являются пользователями интернета. URL: https://rg.ru/2022/09/28/chernyshenko-90-naseleniia-rossii-iavliaiutsia-polzovateliami-interneta.html (дата обращения 01.09.2023).

3 Здесь и далее использованы статистические данные из сборника «Состояние преступности в России». URL: https://мвд.рф/reports/1/ (дата обращения 30.08.2023).

мошенничества, квалифицируемые по признакам составов преступлений, предусмотренных статьями 159, 159.3 и 159.6 УК РФ. Основными характерными чертами этой относительно новой разновидности мошенничеств являются:

– дистанционный характер совершения преступления. Указанное обстоятельство исключает непосредственный контакт потерпевшего и преступника, вероятных очевидцев и свидетелей, вызывает трудность или даже невозможность раскрытия преступления по «горячим следам» (не всегда на первоначальном этапе удается установить даже место совершения преступления);

– доступ злоумышленников к неограниченному количеству потенциальных жертв и высокая виктимность последних. Злоумышленники для «максимального охвата аудитории» активно используют эффективные маркетинговые технологии – «холодные» и «горячие» звонки, массовую рассылку информации и ссылок к ней без согласия получателей посредством электронной почты, СМС, мессенджеров, а также социальные сети и форумы;

– специфика следообразования. Следы рук, обуви, протекторы шин и т.п., как правило, имеют значение в расследовании IT-мошенничеств только на завершающем этапе, когда мошенник установлен и речь идет о закреплении полученных доказательств его причастности к совершенному преступлению. На первоначальном же этапе в качестве объекта пристального внимания и изучения оперативника или следователя выступает информация в электронном виде. Например, для звонков и вывода денежных средств мошенники часто используют «серые» SIM-карты операторов мобильной связи, не привязанные к действующему паспорту гражданина Российской Федерации, банковские карты, «электронные кошельки», оформленные на подставных лиц, сайты, например букмекерские сайты, сайты «казино» и прочее. Информация о проделанных манипуляциях или операциях сохраняется на серверах юридических лиц, предоставляющих соответствующие услуги. Чаще всего такая информация имеет ориентирующее или поисковое значение, предоставляется юридическим лицом по запросу в виде текстового файла установленной формы. Иногда все же информация позволяет идентифицировать преступника. Например, файлы с образцами голоса может предоставить оператор мобильной связи (если мошенник обращался за помощью на «горячую линию» либо контакт между мошенником и потерпевшим осуществлялся с использованием средств голосовых средств связи). Или видеофайлы, записанные с помощью камер, установленных в банкомате, где происходило обналичивание похищенных денежных средств. Также представляют интерес в качестве объекта изучения различные носители информации – смартфоны, компьютеры, серверы, запоминающие устройства, периферийные устройства, изъятые у преступника или на месте совершения преступления. Объектом поиска эксперта здесь будут файлы, программы или их фрагменты, имеющие отношение к преступлению. Например, в последнее время фиксируется применение мошенниками технологии голосовых роботов-операторов, телефонных звонков с использованием заранее разработанных «скриптов» для общения с абонен-

том. Для обнаружения искомой информации экспертом используется специальное программное обеспечение [1];

– использование преступниками приемов и методов социальной инженерии, то есть психологического манипулирования людьми для совершения ими конкретных действий или разглашения конфиденциальной информации[1]. Специально разработанные алгоритмы и сценарии обмана многократно применяются с целью хищения денежных активов в отношении граждан и юридических лиц, в связи с чем подавляющее число регистрируемых IT-мошенничеств имеют признаки серийности и обладают однотипным специфическим подчерком. В последнее время для совершения преступлений мошенники для звонков все чаще применяют IP-телефонию, технология которой позволяет «подделывать» абонентский номер входящего звонка, например на звонок из банка (таким образом осуществляется переадресация вызова). В этих условиях жертва, видя знакомый номер, охотнее вступает в диалог со «специалистом службы безопасности банка» или «следователем». Отдельно стоит отметить использование преступниками подменных сайтов, например, популярных маркетплейсов, государственных органов и банковских учреждений, для хищения персональных данных граждан и информации о их банковских картах.

Ряд исследователей обращают внимание на влияние на выбор методов и приемов манипуляций преступниками различных социально-экономических и политических факторов (событий), таких как, например, введение карантинных мер в связи с распространением вирусной инфекции COVID-19 в 2020 году, последствия усиления с начала 2022 года санкционного давления в отношении Российской Федерации со стороны западных стран, проведение специальной военной операции на Украине [2; 3] и прочие. Злоумышленники учитывают повышенный интерес населения к протекающим внутри и вне страны процессам, особенно получившим высокий общественный резонанс, и активно используют эту информацию в разработке стратегии и тактики обмана.

Еще одной чертой IT-мошенничеств является их латентность. В основном это связано с тем, что пострадавшие граждане не спешат обращаться в правоохранительные органы с заявлением. Мотивы могут быть разные: преступникам по не зависящим от них причинам не удалось довести преступление до завершения либо похищенная сумма, по мнению потерпевшей стороны, является незначительной, соответственно, действия пострадавшего объясняются нежеланием тратить свое время на разбирательство. Некоторые не обращаются в полицию из чувства стыда, понимая, что их «так легко обманули» и это может вызвать «осуждение и насмешки окружающих». Чаще всего латентные IT-мошенничества выявляются при расследовании серийных преступлений, например при анализе информации исходящих звонков преступников, пре-

1 Социальная инженерия. URL: https://ru.wikipedia.org/wiki/Социальная_инженерия (дата обращения к ресурсу 01.09.2023).

доставляемой по судебному разрешению операторами мобильной связи, изучения справок о движении денежных средств по «серым» счетам, получаемых в банковских и финансовых организациях.

В последние годы органами внутренних дел Российской Федерации достигнуты определенные успехи в предупреждении, раскрытии и расследовании IT-мошенничеств. С начала прошлого десятилетия на местах инициативно создавались следственно-оперативные группы, специализирующиеся на указанных видах преступлений. Указанными группами осуществлялся анализ и учет основных способов совершения преступлений ИТТ, способов вывода и обналичивания денежных средств, на их основе отрабатывалась методика сбора доказательств и расследования уголовных дел указанной направленности, проведения оперативно-розыскных мероприятий с учетом специфики IT-сферы. Результаты анализа информации на постоянной основе вносятся ИБД-Ф МВД России в подсистему «Дистанционное мошенничество», использование которой в раскрытии и расследовании преступлений показало свою эффективность. Изучение особенностей совершения IT-мошенничеств позволило выявить основные слои населения, обладающие высоким уровнем виктимности, и выработать и реализовать на практике методы профилактики мошенничеств.

В этот же период было организовано межрегиональное и межведомственное взаимодействие по вопросам противодействия IT-мошенничествам между правоохранительными и контролирующими органами, банковскими и финансовыми организациями, операторами мобильной связи, компаниями-владельцами интернет-порталов, маркетплейсов, сайтов и т.д. Основным аспектом этого взаимодействия стал обмен информацией (в том числе с использованием систем электронного документооборота), под который прорабатывается и постоянно совершенствуется отечественное законодательство. Здесь нельзя не упомянуть подписание Президентом РФ Федерального закона от 20 октября 2022 года № 408-ФЗ «О внесении изменений в статью 26 Федерального закона "О банках и банковской деятельности" и статью 27 Федерального закона "О национальной платежной системе"», который вступил в силу 21 октября 2023 года. Согласно указанному закону Банк России будет предоставлять МВД России информацию, содержащуюся в автоматизированной системе ФинЦЕРТ Банка России «о случаях и попытках осуществления переводов денежных средств без согласия клиента». Порядок информационного обмена, форма и перечень предоставляемых сторонами сведений будут определены в соглашении, заключаемом между Банком России и МВД России. По мнению экспертов, новый порядок информационного обмена существенно сократит временные затраты на получение органами, ведущими расследование, от банков информации, например, о том, на какие счета были выведены деньги, о размере похищенной суммы и т.д.[1]

1 Центробанк поможет осложнить жизнь мошенникам. Интервью. URL: https://cbr.ru/press/event/?id=14108 (дата обращения: 01.09.2023).

Важной вехой в истории развития отечественных органов внутренних дел применительно к рассматриваемой теме является создание в структуре МВД России и на региональных уровнях в целях реализации Указа Президента РФ от 30 сентября 2022 года № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» подразделений по организации борьбы с противоправным использованием информационно-телекоммуникационных технологий. Перед новой структурой в системе МВД России поставлены ряд важных задач: организация предупреждения, выявления, пресечения и раскрытия преступлений, совершенных с использованием информационно-телекоммуникационных технологий, выявление и установление лиц, их подготавливающих, совершающих или совершивших; организация пресечения распространения в сети Интернет информации, создающей угрозу причинения вреда жизни, здоровью и имуществу граждан; организация международного взаимодействия по вопросам деятельности Управления; организация системного анализа криминалистически значимой информации.

Вместе с тем МВД России, на которое легла основная нагрузка по раскрытию и расследованию IT-мошенничеств, столкнулось с рядом проблем, решение которых, как нам представляется, является наиболее актуальным и первостепенным на современном этапе.

Во-первых, это качество подготовки кадрового состава, прежде всего сотрудников оперативных подразделений, дознавателей, следователей, экспертов. Система подготовки специалистов в области правоохранительной деятельности и юриспруденции системы МВД России по выявлению, раскрытию и расследованию «традиционных» преступлений оказывается неэффективной, когда речь идет о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий. Отсутствие представления о технических процессах и специальной терминологии, например в области банкинга, предоставления услуг сотовой связи, компьютерных технологий, технологий создания сайтов и принципов работы сети Интернет, влечет за собой «шаблонность» при разработке версий и планировании совместных следственных действий и оперативно-розыскных мероприятий. Отдельное место занимает подготовка специалистов цифровой или компьютерной криминалистики (форензика) [1].

Во-вторых, это проблемы, связанные с информационным взаимодействием с банковскими и финансовыми учреждениями и организациями, юридическими лицами, предоставляющими услуги в IT-сфере. Так, для установления преступников у сотрудников правоохранительных органов уходит значительное время на переписку (и не всегда результативную) с различными организациями и учреждениями. Преступники в то же время имеют достаточно времени для обналичивания денежных средств и уничтожения или реализации SIM-карт, телефонов и прочих средств совершения преступлений. За это время также истекает срок архивного хранения важной для раскрытия преступления информации.

В-третьих, разработка и внедрение новых методик раскрытия и расследования преступления, «цифровых» способов поиска и фиксации следов преступления для использования доказывании по уголовному делу, нормативное их закрепление.

В 2022 году раскрываемость IT-мошенничеств, несмотря на увеличение в 2022 году показателей расследованных преступлений почти на 40%, невелика и составляет 12%. Объективно оценивая указанные результаты, отметим, что это связано не только с озвученными выше проблемами, но и всплеском преступности, когда сотрудники правоохранительных органов физически не успевают реагировать на поступающие заявления о преступлениях. Мы полагаем, что наиболее эффективным способом противодействия IT-мошенничествам на современном этапе будет является создание и нормативное регулирование систем «Антифрод» (от англ. anti-fraud «борьба с мошенничеством»). «Антифрод» направлен на предупреждение основных способов IT-мошенничеств и вывода денежных средств, получивших наибольшую «популярность» и массовость в последние годы. Ключевая роль в реализации указанных систем отводится ЦБ РФ, Минцифры России, Роскомнадзору, банковским учреждениям и операторам мобильной связи.

С этой целью уже принят ряд федеральных законов, например:

от 30 декабря 2020 года № 533-ФЗ «О внесении изменений в Федеральный закон "О связи"». Согласно принятым поправкам Роскомнадзор с использованием информационной системы мониторинга осуществляет мониторинг соблюдения операторами связи обязанности по проверке достоверности сведений об абоненте и сведений о пользователях услугами связи абонента – юридического лица либо индивидуального предпринимателя. В случае неподтверждения в течение пятнадцати суток соответствия персональных данных фактических пользователей сведениям, заявленным в абонентских договорах, оператором связи предоставление услуг прекращается. Указанные меры направлены в том числе против использования так называемых «серых» SIM-карт;

от 24 июля 2023 года № 369-ФЗ «О внесении изменений в Федеральный закон "О национальной платежной системе"», который вступит в законную силу с 24 июля 2024 года. Согласно принятому закону оператор по переводу денежных средств будет обязан возместить в полном объеме сумму операции, совершенной без добровольного согласия клиента.

Кроме того, в декабре 2022 года Роскомнадзор запустил единую платформу верификации телефонных вызовов (ЕПВВ) «Антифрод», предназначенную для борьбы с телефонным мошенничеством, с помощью которой будет решаться проблема с подменными номерами[1]. Минцифры России запущена в эксплуатацию ИС «Антифишинг». Указанная информационная система мониторинга фишинговых сайтов предназначена для автоматизации и повышения эффективности процессов сбора, систематизации, обработки, анализа и хранения

1 Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством. URL: https://digital.gov.ru/ru/events/42390/?utm_referrer=https%3a%2f%2fyandex.ru%2f (дата обращения 01.09.2023).

сведений о фишинговых ресурсах и фишинговой активности на территории Российской Федерации[1]. В рамках функционирования системы компетентные участники взаимодействуют друг с другом с целью обеспечения противодействия мошенничеству с использованием фишинговых инструментов. Результатом работы данной системы является блокирование вредоносных ресурсов, которые признаны фишинговыми на территории Российской Федерации. Для ускорения процедуры Минцифры России ведет совместную работу с Генеральной Прокуратурой РФ по блокировке ресурсов в соответствии с Федеральным законом 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Резюмируя изложенное, отметим, что на современном этапе вследствие массовости и специфики IT-мошенничества представляют серьезную угрозу безопасности общества и государства, требующую комплексного и много-уровневого подхода к реализации мероприятий, направленных на противодействие им, а также защиту прав, свобод и собственности человека и гражданина от преступных посягательств. В качестве ключевых направлений для успешного противодействия IT-мошенничествам следует выделить дальнейшее совершенствование деятельности по предупреждению, раскрытию и расследованию преступлений указанной категории, внедрение и развитие систем «Антифрод» с целью снижения количества наиболее массовых и распространенных способов совершения преступления, повышение эффективности взаимодействия государственных органов, банковских и финансовых учреждений, юридических лиц, предоставляющих IT-услуги, и, наконец, дальнейшее развитие нормативно-правовой базы для реализации указанных направлений.

1 URL: https://paf.occsirt.ru/(дата обращения 01.09.2023).

Библиографический список

1. Медведев, И.В. Компьютерная криминалистика «форензика» и киберпреступность в России / И.В. Медведев // Пролог: журнал о праве. – 2013. – № 3. – С. 66-69.

2. Сычева, А.В. О способах совершения мошенничеств посредством социальной инженерии в современных условиях и методах их предупреждения / А.В. Сычева // Вестник Волгоградской академии МВД России. – 2022. – № 4 (63). – С. 127-132.

3. Костенко, Н.С. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе / Н.С. Костенко, Г.М. Семененко, А.А. Пшеничкин // Вестник Волгоградской академии МВД России. – 2020. – № 4. – С. 192-196.