Содержание

Введение

Мошенничество является одним из видов преступлений, который продолжает сохранять тенденцию к росту, несмотря на некоторую стабилизацию общей преступности. По данным Генпрокуратуры Российской Федерации, в России общее число случаев мошенничества за 2021 г. выросло на 6,5 %. Как сообщил заместитель начальника Следственного департамента МВД Данил Филиппов, сумма одного мошенничества варьируется от 15 тыс. до десятков миллионов рублей. Естественно, мошенники не останавливаются на достигнутом, с каждым днем совершенствуя уже известные и изобретая все новые способы обмана граждан[42].

Предупреждение интернет-мошенничества во многом зависит от того, насколько известен способ его совершения. Сегодня, правоохранители не успевают проанализировать все способы и предложить соответствующие меры профилактики, тем более довести эти профилактические меры до широкого круга лиц, которые потенциально могут стать жертвами интернет-мошенников.

Фактически профилактикой интернет-мошенничества занимаются как правоохранительные органы и государственные структуры, так и и субъекты предпринимательской деятельности — это банки, крупные корпорации, операторы сотовой связи, организации, занимающиеся разработками IT продуктов, другие организации и физические лица, так или иначе заинтересованные в информационной безопасности в сети Интернет.

Объектом исследования выступают общественные отношения, возникающие в связи с совершением, предупреждением и обеспечением профилактики современных видов мошенничества.

Предметом исследования в работе выступают система и механизмы профилактики мошенничества с использованием банковских карт и интернет ресурсов.

Целью данной работы является исследование проблем профилактики мошенничества с использованием банковских карт и интернет ресурсов.

Исходя из поставленной цели, в рамках данного исследования, предлагается решить следующие задачи:

- изучить обеспечительные меры профилактики мошенничества с использованием банковских карт и интернет ресурсов;

- рассмотреть способы совершения мошенничества с использованием банковских карт;

- выделить виды мошенничества с использованием интернет ресурсов;

- исследовать судебную практику по вопросам профилактики мошенничества с использованием банковских карт и интернет ресурсов;

- оценить эффективность профилактики мошенничества с использованием банковских карт и интернет ресурсов;

- выявить проблемы профилактики мошенничества с использованием банковских карт и интернет ресурсов;

- разработать меры профилактики мошенничества с использованием банковских карт и интернет ресурсов;

- определить перспективы развития направлений профилактики мошенничества с использованием банковских карт и интернет ресурсов.

Методологическую основу исследования составили исторический, сравнительно-правовой, формально-логический и системно-структурный методы.

Теоретической базой исследования послужили труды ученых в области профилактики мошенничества с использованием банковских карт и интернет ресурсов: Анненкова Е.А., Ахметов А.А., Балашев Н.Б., Балашова О.Б., Бжахов Г.М., Бытко С.Ю., Емельянов Д.А., Кабалина К.С., Лебедева И.А., Леваков А.К., Леун Е. В., Молдалиева К.З., Путанова О.А., Репецкая А.Л., Савинова Е.А., Смагоринский Б. П., Сычева А. В., Смирнов Д.Ю., Сычева А. В. и др.

Степень разработанности темы. Вопросы предупреждения преступлений корыстной направленности, включая и мошенничество, достаточно хорошо освещены в отечественной и зарубежной науке. Между тем основные фундаментальные исследования, посвященные вопросам совершения преступлений с использованием компьютерного и телекоммуникационного оборудования, в настоящее время требуют развития изложенных в них научных положений. Как отмечает А.А. Комаров, «глубоких всесторонних исследований, посвященных компьютерной преступности как явлению - следствию социальной трансформации общества, пока мало».

Рассматривая конкретные направления отечественной юриспруденции в целом и криминологической мысли в частности, можно отметить значительное внимание некоторых исследователей к вопросам «виктимологической профилактики» и «виктимологического предупреждения», обоснованным и активно разрабатываемым такими известными учеными, как К.Е. Вишневецкий, Т.В. Варнук, А.А. Гаджиев, В.И. Задорожный, Д.В. Ривман, Л.В. Франк и др. В работах названных авторов предприняты попытки разработки как отдельных элементов теоретической модели виктимологического воздействия на преступность, так и системы мер виктимологической профилактики преступлений. Однако, отсутствие законодательного закрепления и четко сформулированной государственной политики виктимологического воздействия до настоящего времени не позволяет в полной мере раскрыть потенциал указанных научных разработок.

Эмпирическую базу исследования составили статистические данные за 2017-2020 годы Главного информационно-аналитического центра МВД РФ, статистические и аналитические материалы по заявленной теме исследования. Кроме того, были проанализированы материалы уголовных дел, касающихся различных видов и отдельных этапов совершения

мошенничества, связанного с использованием телекоммуникационного и компьютерного оборудования.

Структура работы, обусловленная логикой исследования, его целью и задачами, представлена введением, тремя главами, заключением, списком использованных источников.

Первая глава посвящена теоретическим основам и изучению нормативно-правовой базы профилактики мошенничества с использованием банковских карт и интернет ресурсов.

Во второй главе представлена общая криминологическая характеристика цифрового мошенничества, проведен анализ судебной практики по вопросам профилактики мошенничества с использованием банковских карт и интернет ресурсов, а так приведены результаты оценки эффективности профилактики мошенничества с использованием банковских карт и интернет ресурсов.

В третьей главе выявлены проблемы профилактики мошенничества с использованием банковских карт и интернет ресурсов, и по результатам разработаны меры профилактики мошенничества с использованием банковских карт и интернет ресурсов.

1 Теоретические основы и нормативно-правовая база профилактики мошенничества с использованием банковских карт и интернет ресурсов

1.1 Теоретические разработки по проблемам профилактики мошенничества с использованием банковских карт и интернет ресурсов

По мнению многих специалистов, основной задачей для предупреждения и выявления мошенничеств с использованием пластиковых карт на ранней стадии их совершения является прежде всего обеспечение:

а) сопровождения операций с пластиковыми картами в рамках проводимой банками платежной системы;

б) безопасности операций с пластиковыми картами на национальном уровне;

в) безопасности операций с пластиковыми картами в рамках конкретного банка;

г) сотрудничества службы безопасности эмитентов и торговых организаций с правоохранительными органами.

Основным видом мошенничества в РФ на настоящий момент является мошенничество с утерянными и украденными картами. Карты используются для получения денежных средств в банкоматах в случае, если виновному лицу известен пин-код или в торговых точках при приобретении товара, когда кассир вследствие халатности или загруженности, нарушая правила, продает товар человеку, не являющемуся владельцем карты.

«К распространенному типу мошенничества относится также использование поддельной карты с данными магнитной полосы чужой карты (скимминг - skimming - копирование данных магнитной полосы карты). Существует несколько видов скимминга:

1) сетевое проникновение вкрупные процессинговые центры, компрометация данных карт;

2) подключение к POS-термина-лам техники в торговых точках или

использование переносных устройств в ресторанах;

3) организация фиктивных пунктов выдачи наличных (ПВН);

4) установка накладок на приемные устройства и клавиатуру банкоматов, перехватывающей спецтехники внутри них».

С каждым годом увеличивается число мошенничеств с использованием платежных карт в сети Интернет.

Наиболее распространенными местами совершения мошенничеств в сети Интернет являются места торговых операций (аукционов) и сделки по ним; различные службы и услуги Интернета; электронная торговля потребительскими товарами; компьютерное оборудование и программное обеспечение, схемы заработка на дому, аукционы, лотереи и другие. Для оплаты товара в интернет-магазинах достаточно указать реквизиты карточки, т. е. номер карты иС код, указанный на обороте. Данная информация может быть легко получена мошенниками, при осуществлении любой операции может произойти утечка информации, равно как и при утере или краже карты.

Возможности социальных методов профилактики интернет-мошенничества ограниваются восприятием субъектами профилактики профилактической информации и невозможностью раскрыть и донести до широкого круга пользователей, не только все схемы интернет-мошенничества, но и даже основные паттерны социальной инженерии используемые мошенниками.

В человеческих отношения, возможно всё, что угодно, восприятие людей сложно сориентировать на распознавание мошенничества, поэтому мошенники без особого труда находят своих жертв. Что касается технических способов профилактики интернет-мошенничества, то речь идет о разнообразных программных методах, призванных защитить устройства, выходящие в сеть Интернет от различного рода атак злоумышленников. Сюда можно отнести различные антивирусные программы, сервисы типа

CheckShortURL, используемые для проверки сайта на наличие вредоносных программ. Например, когда человек собирается перейти по ссылке на сайт.

Несмотря на разнообразие и всеобъемлющий характер профилактических мер, направленных профилактику и борьбу с мошенничеством в сети интернет, практика показывает, что сегодня, этих мер уже недостаточно, уровень интернет-мошенничеств за последние два года резко возрос. Как следует из отчета Центробанка, всего за период времени с января по март 2021 года мошенники украли путем несанкционированных переводов у граждан и компаний в России 2,9 миллиардов рублей, что на 57% больше, чем в первом квартале 2020 года [9, с. 112].

Профилактика мошенничества в сети Интернет в криминологическом аспекте, имеет некоторые затруднения вызванные тем, что интернет-мошенничество представляется, как мошенничество с использованием интернета как глобальной виртуальной сети, а также мошенничество с использованием интернет-связи. В последнем случае — это технология подключения к глобальной сети Интернет. При обсуждении вопроса анонимности в сети Интернет, понимание этих нюансов в контексте интернет-мошенничества необходимо для правильной квалификации деяний, образующих состав преступления.

Говоря об анонимности в сети, необходимо разграничивать анонимность в обыденном понимании, анонимность данных и анонимность в техническом аспекте. Эти аспекты хотя и связаны между собой, всё же имеются существенные различия по содержанию. Что касается анонимности в обыденном понимании, речь идет, прежде всего, о возможности использования псевдонимов, вымышленных имен, создания в социальных сетях страниц, не содержащих личных данных, таких как имя, фамилия, другой информации, в том числе фотографий, позволяющей идентифицировать пользователя или опознать его. Не всегда такие страницы

создаются с целью совершения мошенничества.

Для многих это шанс пообщаться без идентификации, возможность будучи не опознанным, просматривать чужие страницы, выражать свои мысли, без боязни быть, в чем-либо уличённым, или в иных целях. Это так называемые, «технические» аккаунты. В данном случае анонимность пользователей довольно условна, если речь идет о добропорядочных гражданах, ведь для регистрации в социальной сети, добропорядочным пользователям приходится оставлять какие-либо данные о себе. Другое дело, когда в социальных сетях и на торговых площадках, например, «Авито», под вымышленными именами скрываются профессиональные мошенники, которые регистрируют страницы по сим-картам,оформленным на подставных лиц, а в сеть выходят, используя специальные программы анонимайзеры, что существенно затрудняет их поиск [36, с. 88].

Однако, сами социальные сети, сайты знакомств и торговые площадки довольно быстро реагируют на такие подозрительные страницы, блокируя их деятельность. В данном случае можно говорить об ограничении или запрете анонимности с целью профилактики мошеннических действий, при которых потерпевшие лица, подвергшись обману, сами передают, принадлежащие им денежные средства мошенникам, например в счёт оплаты несуществующих товаров или услуг, на благотворительность, в долг или на другие цели.

Безопасность пользователей в социальных сетях, на сайтах знакомств, а также на торговых площадках, в большей степени зависит от выполнения ими несложных правил, касающихся общения и обращения с денежными средствами.

Полностью исключить обман и обезопасить каждого пользователя таких сайтов, запретив регистрацию анонимных страниц, представляется нам маловероятным. Добропорядочные граждане будут предоставлять паспортные данные при регистрации, предоставлять биометрические данные, а мошенники найдут способы, например, вскрыть чужие «настоящие»

страницы и, как это практикуется сейчас, совершать преступные действия через них. Формально, запрет анонимности в социальных сетях и на торговых площадках повысит уровень доверия пользователей, в результате чего, мошенники только выиграют.

В правовом плане, на выше упомянутые платформы будут возложены дополнительные обязанности по контролю и выявлению, ещё на стадии регистрации, недобросовестных пользователей, что неминуемо приведет к дополнительным затратам, которые скажутся на обычных пользователях, в отдельных случаях регистрация может стать платной или цена на регистрацию, если она была платной, возрастёт. Когда речь идет об анонимности данных, то имеется ввидуидентификация анонимных данных конкретного лица в сети Интернет [40, с. 54].

Необходимо отметить, что в настоящее время возможности идентификации данных физических и юридических лиц в сети Интернет [illegible] без применения каких-либо специфических технических методов.

Например, в социальных сетях, многие пользователи добровольно выкладывают информацию о себе. Здесь можно говорить об имени, дате рождения, семейном положении, номере телефона, транспортных средствах, включая государственные номера, данные геолокации и другую информацию, которую мошенники могут использовать в своих целях.

Юридические лица так же выкладывают в сеть свои данные, используя которые можно узнать большинство интересующей информации. Но когда речь идет о защите персональных данных, коммерческой тайны или данных, которые физическое или юридическое лицо не хотело бы придать огласке, например данные о наличии счетов в банках и тому подобные, необходимо иметь ввиду, что для сохранности этих данных применяются технологии анонимизации данных.

Анонимизация является способом обработки данных, в результате

которого происходит преобразование идентификационной информации таким образом, чтобы по полученным данным нельзя было определить их принадлежность тому или иному субъекту. Анонимность данных рассматривается в качестве меры безопасности и должна, неукоснительно соблюдаться всеми субъектами оперирующими этими данными. Однако, как показывает практика, утечки данных происходят даже в крупных корпорациях. Попадая в руки мошенников, они используются ими в своих преступных целях. В этой связи необходимо учесть, что утечка данных происходят во многом благодаря тому, что они недостаточно анонимизированы, и вообще не защищены, часто они хранятся в незашифрованном виде, поэтому в определённых условиях становятся лёгкой добычей мошенников [32, с. 23].

Так в феврале 2022 года в Бурятии завершилось расследование уголовного дела против 22-летнего жителя республики, обвиняемого в совершении преступлений предусмотренных частью 2 статьи 138 Уголовного кодекса РФ — «Нарушение тайны переписки, телефонных переговоров и иных сообщений граждан, совершённое с использованием служебного положения», частью 3 статьи 272 «Неправомерный доступ к охраняемой законом компьютерной информации» и частью 3 статьи 183 УК РФ — «Незаконное получение и разглашение сведений, составляющих коммерческую тайну»[1].

По данным следствия, 8 февраля 2021 года молодой человек устроился продавцом-консультантом в торговую точку дилера оператора сотовой связи. На следующий день он разместил в нескольких группах в популярном мессенджере объявления о том, что имеет доступ к конфиденциальной информации абонентов и готов предоставить её всем желающим за определённое денежное вознаграждение.

В последующие несколько дней злоумышленник по запросам анонимных пользователей передал им сведения с детализацией телефонных

звонков и сообщений восьми клиентов из разных регионов. За это ему заплатили 21 тысячу рублей.

Данный пример свидетельствует, о том, как отсутствие анонимизации данных, способствует совершению разнообразных преступлений. Становиться очевидным, что если данные попадают к мошенникам, то число мошенничеств неизбежно растет. В целях профилактики такого вида преступности, необходимо возложить на компании повышенную ответственность за неправильное и незащищенное хранение персональных данных, стимулируя их, тем самым, применять более строгие меры к отбору сотрудников, имеющих доступ к персональным данным. Например, предлагать им проходить проверки на полиграфе при приёме на работу.

Однако наиболее проблемным и спорным аспектом в борьбе с интернет-мошенничеством, на сегодняшний день является инициатива ограничения анонимности в сети Интернет, в техническом аспекте. Идентификация в интернете или локальной сети возможна благодаря IP-адресам.

IP означает «Интернет-протокол» — это набор правил, регулирующих формат данных, отправляемых через сеть. IP содержит информацию о местоположении устройства, обеспечивая его доступность для связи. По IP-адресам идентифицируют компьютеры, маршрутизаторы и веб-сайты в сети Интернет.

IP-адрес назначается устройству интернет-провайдером. Любое действие в сети, любой запрос будет привязан к этому адресу. Отбросив технические тонкости про то, какие бывают IP -адреса как они работают, отметим, что скрытие IP-адреса для добропорядочного пользователя — это способ защитить персональные данные и личность в сети Интернет, а для мошенника шанс остаться незамеченным и безнаказанным за совершенные им преступления.

Зная IP-адрес, злоумышленники, с помощью специальных программ

могут вести сбор статистики пользователя для передачи третьим лицам, определять его месторасположение, получать сведения о каких-либо действиях пользователя, в том числе компрометирующих его. Так, преступник сможет подтвердить чью-либо личность по IP-адресу системы, с целью, например загрузки какого-либо контента с IP-адреса этого пользователя. Такие действия совершаются часто с намерением загружать пиратские фильмы, музыку, видео, что является нарушением условий использования услугами провайдера. Может быть загружен контент, связанный с экстремизмом, терроризмом или детской порнографией, а также контент, способствующий совершению мошенничества, например, объявления о продажах товаров и услуг.

Во всех случаях у правоохранительных органов возникают сложности с выявлением исполнителей. Отдельно отметим, что зная IP-адрес пользователя злоумышленники могут взломать устройство, заразить его вредоносными программами и использовать в своих преступных целях. Мошенники могут использовать социальную инженерию, чтобы обманом заставить пользователя раскрыть IP-адрес. Например, они могут найти субъекта в Skype или аналогичном приложении для обмена мгновенными сообщениями, использующем IP-адресадля связи. Общение с незнакомцами в этих приложениях, предполагает, понимание того, что они могут видеть IP-адрес. Злоумышленники могут использовать инструмент SkypeResolver, позволяющий определить IP-адрес по имени пользователя [30, с. 67].

Однако наиболее спорный метод профилактики, предлагаемый в настоящее время — это запрет операторам связи использовать «серые» IP-адреса, то есть публичные сетевые адреса, преобразованные по технологии NAT (NetworkAddressTranslation). Сторонники метода ссылаются на то, что технология NAT позволяет преступникам безнаказанно совершать все новые и новые преступления. Поэтому ввиду сложности их изобличения предлагается законодательно запретить операторам связи использовать

протокол «Ipv4», а протокол «IPv6» применять как его альтернативу.

Полагаем, что внедрение нового протокола может способствовать борьбе с преступлениями в сфере компьютерной информации, поскольку можно будет более точно выявить абонента, оставляющего электронные следы в сети Интернет. Важно отметить, что данное предложение имеет смысл в долгосрочной перспективе, в ближайшие 10– 15 лет, его реализация весьма затруднительна и экономически не обоснована. В настоящее время NAT (NetworkAddressTranslation) является базовой фундаментальной технологией и необходима для функционирования сети. А для перехода на протокол «IPv6» необходима замена аппаратно-технологической базы. То есть один IP-адрес должен соответствовать одному устройству, что на сегодняшний день технологически невозможно воплотить. Попытки же быстро осуществить данную политику могут повлечь обрушению сети Интернет.

Кроме того, NAT (NetworkAddressTranslation) не является, как таковой технологией анонимизации, анонимизация в данном случае, является ее побочным продуктом. К сожалению, что авторы таких предложений часто не приводят достаточных доказательств того, что запрет NAT (NetworkAddressTranslation) повысит уровень безопасности сети и снизит уровень преступлений в сфере обращения охраняемой законом информации. Более того, предлагая запретить NAT (NetworkAddressTranslation), необходимо ссылаться на исследования о экономической целесообразности такого запрета и провести оценки рисков для безопасности государства. Говоря об отмене NAT (NetworkAddressTranslation) необходимо понимать, что, во-первых, преступники могут использовать и другие технологии анонимизации, например VPN тоннель (англ. VirtualPrivateNetwork — виртуальная частная сеть) или Проект I2P. I2P. [24, с. 20].

На наш взгляд, для вынесения предложения о законодательном запрете NAT (NetworkAddressTranslation) необходимо привлечение экспертов в

сфере безопасности сетей к исследованию данного вопроса.

Нельзя игнорировать тот факт, что анонимность в сети Интернет имеет огромное значение для безопасности предприятий, компаний и государственных структур, так как анонимные каналы необходимы для передачи информации благонадежным участникам правоотношений. Именно анонимность в данном контексте, выступает гарантом безопасности от преступных посягательств. Большинство сервисов безопасности используют именно технологии NAT (NetworkAddressTranslation). На практике для того чтобы остаться не идентифицированными в сети Интернет, используется множество разнообразных методов.

Например, использование анонимайзеров, вход в интернет с зарубежных IP-адресов, использование серверов, получающих почтовые сообщения и переправляющих их по адресам, указанным отправителем, так называемые ремейлеры, когда при переадресовке, информация об отправителе уничтожается, использование Tor (TheOnionRouter — луковая маршрутизация) и VPN (VirtualPrivateNetwork — виртуальная частная сеть).

Использование VPN с Tor обеспечивает максимальную анонимность. Таким образом, можно сделать вывод, что для профессиональных интернет-мошенников, проблемы преодоления анонимности в сети Интернет не являются столь серьёзными, полагаем, что со временем преступники будут только совершенствоваться в уничтожении следов своей деятельности в сети Интернет. Поэтому для решения вопроса о законодательном запрете анонимности в сети Интернет, необходима тщательная оценка всех положительных и отрицательных последствий запрета. Для решения этого вопроса должны быть привлечены специалистов из разных сфер деятельности, начиная от IT и заканчивая криминалистами, криминологами и психологами [17, с. 41].

В противном случае запреты как мера профилактики мошенничества в сети Интернет приведут к ограничению возможностей и прав

добросовестных участников правоотношений, что является недопустимым. Что же касается профилактики интернет-мошенничества, полагаем, прежде всего, необходимо совершенствовать техническую защиту, проводить более глубокую профилактическую работу среди населения. Особенно со стороны субъектов, предоставляющих услуги сотовой сети и интернет, со стороны социальных сетей, торговых площадок. Очень важным является контроль за хранением и обработкой данных. Именно утечка данных даёт наибольшие возможности интернет-мошенникам осуществлять свои преступные намерения.

Эффективность предупреждения интернет-мошенничества зависит от проведения сбалансированной политики со стороны государства и общества в борьбе с киберпреступностью. Законодательная защита интересов бизнеса, электронной коммерции, неминуемо приведёт к тому, что бизнес-сообщество получит более широкие возможности по укреплению и развитию технологий защиты от интернет-мошенничества и других киберпреступлений.

1.2 Нормативно-правовая база противодействиямошенничества с использованием банковских карт и интернет ресурсов

В главе 21 Уголовного кодекса Российской Федерации (далее – УК РФ) закреплены нормы, устанавливающие уголовную ответственность за мошенничество с использованием электронных средств платежа (статья 159.3 УК РФ) и за кражу с банковского счета, а равно в отношении электронных денежных средств (пункт «г» части 3 статьи 158 УК РФ). Разграничение указанных составов между собой вызывает определенные трудности у правоприменителей.

Следует отметить, что в июне 2021 года из текста постановления Пленума Верховного Суда Российской Федерации (далее – ВС РФ),

разъясняющего вопросы квалификации мошенничества, присвоения и растраты, были исключены абзацы 1 и 2 пункта 17, в которых говорилось о том, что по статье 159.3 УК РФ следует квалифицировать действия лица в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой. При этом как кража квалифицировались действия лица, состоящие в хищении чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномоченного работника кредитной организации.

Однако, как уже отмечалось, эти разъяснения из текста постановления Пленума ВС РФ были исключены, в связи с чем правоприменительные органы вынуждены решать вопрос о том, какие же деяния следует квалифицировать по статье 159.3 УК РФ как мошенничество с использованием электронных средств платежа. Изучение правоприменительной практики за последние полтора года свидетельствует о том, что небезызвестное «дело Кактана» заложило определенное направление в решении поставленного вопроса. ЧТО ЗА ДЕЛО?

Эффективность механизма противодействия незаконным финансовым потокам возможна, только если финансовая система сама ставит заслон для экономической активности преступных элементов. Так, банки имеют право отказывать в открытии счетов, вкладов или проведении операций клиентам, чья добросовестность вызывает сомнения.

Для банков выявление подозрительных операций — сложная и дорогостоящая работа. Банк России постоянно оказывает им методологическую поддержку, например, определяет основные признаки

таких операций, а также предоставляет банкам информацию о лицах, которым ранее было отказано в банковском обслуживании из-за сомнений в их добросовестности.

С 1 июля 2022 года начала работать платформа для банков «Знай своего клиента» — система, которая предоставляет необходимую информацию об уровне риска вовлеченности в проведение подозрительных операций потенциальных и существующих клиентов. Платформа позволит сократить издержки банков и число необоснованных отказов их клиентам.

Незаконные финансовые операции часто носят трансграничный характер, поэтому борьба с отмыванием денег, полученных преступным путем, и финансированием терроризма ведется на международном уровне. Для эффективной борьбы с этими явлениями разработаны и постоянно актуализируются международные стандарты в сфере противодействия отмыванию денег, финансированию терроризма, распространению оружия массового уничтожения (ПОД/ФТ/ФРОМУ).

Разработкой стандартов и контролем за их выполнением всеми государствами занимается специализированная межправительственная организация — Группа разработки финансовых мер борьбы с отмыванием денег (FinancialActionTaskForce, FATF). Банк России принимает активное участие в работе FATF и активно взаимодействует с зарубежными партнерами в сфере ПОД/ФТ.

Основные положения, регламентирующие вопросы ПОД/ФТ/ФРОМУ, содержатся в Федеральном законе от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Банк России также контролирует проведение валютных операций кредитными и некредитными финансовыми организациями. Валютный контроль — часть государственной политики. Он направлен на обеспечение

устойчивости валюты Российской Федерации и стабильности внутреннего валютного рынка страны. Это направление деятельности регулируется Федеральным законом от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле».

Большое значение для борьбы с мошенниками, совершающими хищения с платежных карт, стало изменение 16.03.2015 «Положения о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…», утв. Банком России 09.06.2012 № 382-П. Указанные изменения фактически исключили использование платежных карт, на которых информация сохранена только на магнитной полосе: согласно п. 2.19 Положения, с 01.07.2015 возможна выдача дебетовых или кредитных карт, оснащенных и микропроцессором, и магнитной полосой. Это усложнило подделку кредитных карт на основе информации от скимминга.

Изучение нормативно-правовой базы противодействия мошенничеству с использованием банковских карт и интернет ресурсов показало, что современные способы совершения мошенничества в отношении физических лиц являются полноструктурными, так как мошенники тщательно готовятся к совершению преступления и предпринимают необходимые действия по его сокрытию.

2 Общая криминологическая характеристика цифрового мошенничества (КРИМИНОЛОГО_КРИМИНАЛИСТИЧЕСКАЯ?)

2.1 Способы совершения и виды мошенничества с использованием банковских карт

Рассмотрим основные способы мошенничества с картами и возможные меры противодействия им.

1. Способы мошенничества с картами. К настоящему времени самыми распространенными схемами мошенничества с непосредственным участием карт являются следующие:

Скимминг – хищение разными способами конфиденциальных данных (номер карты, ФИО владельца, срок действия карты, CVC-код) карты в сочетании с получением вводимого PIN-кода, например, с помощью накладной клавиатуры или при сьемке незаконно установленной рядом видеокамерой. Полный набор полученных данных позволяет мошенникам изготовить фальшивый дубликат карты для полного незаконного пользования счетом владельца [5, с. 546].

Бесконтактная кража – хищение средств со счета владельца карты при незаконном ношении и использовании в людных местах (транспорт, вокзалы, аэропорты, рынки и т.д.) мобильных считывателей или считывающих POS-терминалов. Фотография с незаконным ношением такого устройства в метро приведена на рисунок 1.

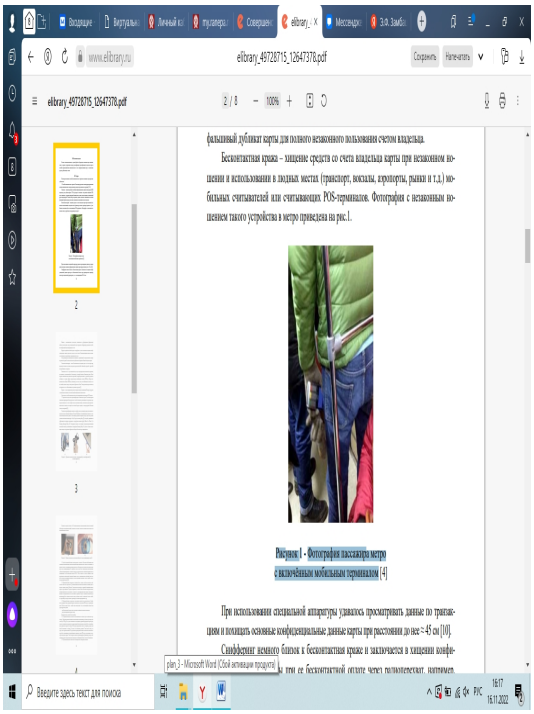

Рисунок 1 - Фотография пассажира метро с включённым мобильным терминалом [12, с. 20]

При использовании специальной аппаратуры удавалось просматривать данные по транзакциям и похищать основные конфиденциальные данные карты при расстоянии до нее ≈ 45 см.

Снифферинг немного близок к бесконтактная краже и заключается в хищении конфиденциальных данных карты при ее бесконтактной оплате через радиоперехват, например, используя специальный «радиожучок», в т.ч. и незащищенные Wi-Fi сети [33, с. 65].

Фишинг – мошеннические технологии, основанные на дублировании официальных сайтов, используемых для дистанционной оплаты картами и собирающих разными способами конфиденциальную информацию о них Вирусное заражение компьютеров и смартфонов с целью незаконных хищения конфиденциальных данных карты или доступа к счету карты [6, с. 85].

Совершенствование вирусов приводит к большому разнообразию мошеннических схем. Есть разновидности мошенничесва, связанных с организацией по определенным сценариям разных ситуаций с

психологическим воздействием или прямым обманом владельца карты. Социальная инженерия – способ мошеннического хищения денег со счета карты при, введении в шоковое состояние владельца карты какой-либо обманной ситуацией с просьбой или требованием о переводе.

Ливанская петля – вид мошенничества, когда в картоприемник вставляется кармашек, как правило, изготовленный из фотопленки, в который попадает банковская карта. Возле жертвы мошенничества появляется прохожий, который рассказывает о похожей ситуации и сообщает, что нужно набрать определенную комбинацию и ввести ПИН-код.

Жертва мошенничества сообщает ПИН-код мошеннику, но после того, как комбинация не помогла, тот же самый человек советует немедленно обратиться в банк. Этим временем карта изымается из кармашка и с нее обналичиваются денежные средства.

Кардинг – целое направление разных хакерских видов взламывания Интернет-ресурсов с попытками незаконного получения конфиденциальных данных карты. Существуют способы мошенничества через запрашивания одноразового СМС-пароля [28, с. 55].

В настоящее время типичными примерами биометрического способа являются распознавание следующих параметров человека и его тела: тембра голоса, отпечатков пальцев, отпечатков ладони, расположения вен на пальцах, на ладони, на тыльной стороне ладони, а также радужной оболочки глаза и голограммой.

Технология идентификации человека по тембру голоса в настоящее время уже активно используется при телефонном общении в России Сбербанком. Аутентификация человека по отпечаткам пальцев известна давно и к настоящему времени в широком доступе уже много разных датчиков отпечатков пальцев (рис. 2а-в).

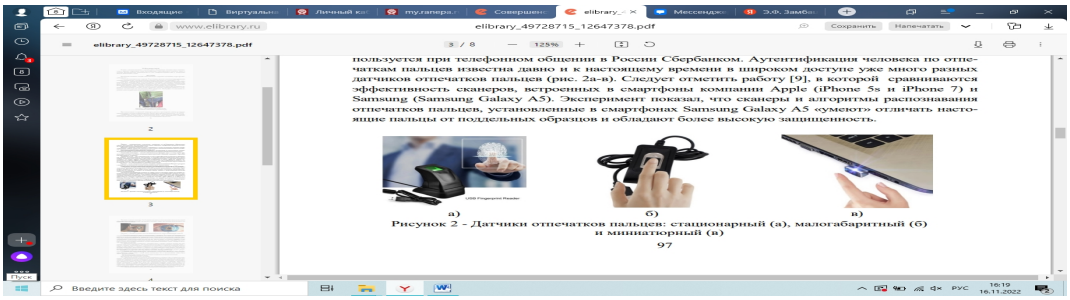

Рисунок 2 - Датчики отпечатков пальцев: стационарный (а), малогабаритный (б) и миниатюрный (в) [16, с. 87]

Датчики сетчатки глаза (рис. 3а, б) разных вариантов, распознающие рисунок радужной оболочки глаза индивидуальный для каждого человека, также уже активно используются для идентификации человека.

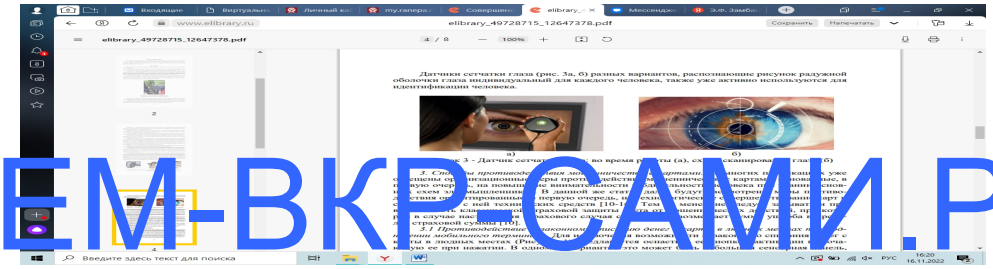

Рисунок 3 - Датчик сетчатки глаза: во время работы (а), схема сканирования глаза (б)

Следует отметить работу, в которой сравниваются эффективность сканеров, встроенных в смартфоны компании Apple (iPhone 5s и iPhone 7) и Samsung (SamsungGalaxy A5).

Эксперимент показал, что сканеры и алгоритмы распознавания отпечатков пальцев, установленные в смартфонах SamsungGalaxy A5 «умеют» отличать настоящие пальцы от поддельных образцов и обладают более высокую защищенность.

В современных условиях экономической нестабильности преступность в сфере информационно-телекоммуникационных технологий приобретает все новые направления. При этом сеть Интернет выступает не только удобным

инструментом, но и благоприятной средой для совершения мошеннических действий в отношении граждан. Рассмотрим некоторые способы такого обмана.

1. Заражение вирусом-вымогателем. Как известно, мошенники по всем у миру распространяют вирусы-вымогатели, которые попадают на компьютер потенциальной жертвы и зашифровывают все файлы, находящиеся на нем, что ставит под угрозу всю хранившуюся информацию и парализует работу компьютера. Для возврата необходимых жертве файлов, вирус выдает сообщение с требованием перевести денежные средства на криптовалютный кошелек.

Преступники поступают таким образом для того, чтобы остаться незамеченными, так как в данном случае их невозможно отследить. К сожалению, зачастую даже после уплаты «выкупа» информация на компьютере потерпевшего так и остается зашифрованной. Специалисты советуют регулярно обновлять антивирусные программы на своих компьютерах [3, с. 12].

2. Установка приложения на смартфон. Как известно, практически все современные люди пользуются смартфонами, что также способствует совершению преступных деяний мошеннического характера. Одним из способов такого обмана является установка приложений, внешне похожих на обычные программы, с помощью которых преступники получают доступ к личным данным потенциального потерпевшего [20, с. 65].

3. Кибермошенничество в социальных сетях. Данный вид мошенничества имеет множество вариаций. Так, преступники проводят опросы под видом одного из извебстных банков, предлагая потенциальному потерпевшему в конце разыграть приз. Для того, чтобы подтвердить, что жертва действительно является клиентом данного банка и получить выигрыш, мошенники просят отправить определенную сумму на их счет подтверждения.

4. Мошенничество с онлайн-играми. Многие современные дети, да и некоторые взрослые любят играть онлайн. Желание быть лучшим в игре нередко порождает зависимость к игре, которая проявляется в трате денег покупки улучшений для своих игровых персонажей. В целях экономии, многие сталкиваются в сети Интернет с мошенниками, которые не требуют предоплату, но в итоге не предоставляют никаких виртуальных улучшений.

В связи со сложившейся ситуацией на Украине, многие страны мира наложили на Российскую Федерацию множество санкций, из-за чего западные сервисы ограничили услуги для россиян (Intel, NVIDIA и AMD - прекратили поставки процессоров и видеокарт в Россию; многие игровые компании остановили продажи своей продукции в нашей стране - ActivisionBlizzard и др.).

5. Мошенничество с использованием бесконтактных платежей. Многие граждане пользуются бесконтактным способом оплаты покупок в магазинах, общественном транспорте и т.д. Мошенники создают самодельные портативные терминалы оплаты и, например, в общественном транспорте в часы пик подходят максимально близко к потенциальной жертве для того, чтобы бесконтактно списать денежные средства с карты последней [27, с. 85].

В целях предупреждения подобного рода хищений, целесообразно установить лимитированную сумму на денежные платежи по карте либо поставить необходимость ввода пин-кода для подтверждения любых транзакций.А СЕЙЧАС РАЗВЕ НЕ ТАК?

Рассмотренные нами криминалистически значимые сведения о способах совершения мошенничеств в сети Интернет, взаимосвязанные и взаимообусловленные с другими элементами криминалистической характеристики рассматриваемой категории преступлений, могут оказать помощь следователю(дознавателю) в выборе средств и методов расследования, выдвижении и отработке следственных версий, установлении

личности преступника и его розыске в целях своевременного раскрытия и расследования преступления.

Наиболее уязвимыми к мошенничеству по сети «Интернет» и сотовой связи являются пожилые люди. Причинами этого является отсутствие способности к критическому мышлению и объективному оцениванию ситуации, а также замедленной реакции на непредвиденные обстоятельства. Немаловажным выступает и тот факт, что большинство пожилых людей плохо оперируют в сети «Интернет» и сотовых телефонах, имеют страхи перед использованием современных технологий. Соответственно государству необходимо создавать программы обучения мобильной грамотности в различных регионах нашей страны, тем самым это позволит значительно снизить количество хищения денежных средств по сети «Интернет» и сотовой связи у самой подверженной мошенничеству категории граждан – людей пожилого возраста [21, с 65].

2.2 Судебная практика по вопросам профилактики мошенничества с использованием банковских карт и интернет ресурсов

Судебно-следственные органы в настоящее время квалифицируют по пункту «г» части 3 статьи 158 УК РФ как кражу с банковского счета деяния, в рамках которых посягатель для оплаты товаров бесконтактным способом незаконно использовал подделанное или принадлежащее другому лицу электронное средство платежа. Вменение состава преступления, предусмотренного статьей 159.3 УК РФ, в такой ситуации, с позиции Верховного суда РФ, признается «неправильным применением уголовного закона», о чем прямо указывается в судебных решениях.

НУЖНЫ ПРАВОВЫЕ ПОЗИЦИИ ВС РФ!!!!!!

Например, Судебная коллегия по уголовным делам Вологодского областного суда, изучив материалы уголовного дела и рассмотрев позицию,

отраженную в апелляционном представлении, пришла к выводу о необходимости отмены приговора в отношении гр-на Р. по причине несоответствия выводов суда, изложенных в приговоре, фактическим обстоятельствам уголовного дела, установленным судом первой инстанции, в связи с неправильным применением уголовного закона. Органом предварительного следствия действия гр-на Р. были квалифицированы по пункту «г» части 3 статьи 158 УК РФ как кража, совершенная с банковского счета.

Данная юридическая квалификация была поддержана государственным обвинителем в процессе судебного рассмотрения. Однако суд первой инстанции принял решение о необходимости изменения квалификации действий гр-на Р. на часть 1 статьи 159.3 УК РФ полагая, что в данном случае имеются все признаки состава мошенничества с использованием электронных средств платежа.

Суд обосновал свое решение тем, что хищение денежных средств в данном случае было совершено путем обмана, поскольку гр-н Р. сознательно умолчал о неправомерности использования платежной карты для осуществления расчетов в торговой организации. Однако данный вывод суда первой инстанции суд апелляционной инстанции не поддержал, отметив, что по смыслу уголовного закона хищение денежных средств, совершенное с использованием электронного средства платежа, образует состав преступления, предусмотренного статьей 159.3 УК РФ, только в тех случаях, когда изъятие денег осуществлено путем обмана или злоупотребления доверием их владельца или иного лица.

Рассмотрев обстоятельства дела, суд пришел к выводу о том, что гр-н Р. после того, как незаконно завладел платежной картой другого лица, применял данное платежное средство для реализации расчетов за приобретаемые товары бесконтактным способом. При этом работники соответствующей торговой организации не принимали непосредственного

участия в операции по списанию денежных средств с банковского счета потерпевшего.

Таким образом, как отмечает суд апелляционной инстанции, гр-н Р. не сообщал уполномоченным специалистам и иным третьим лицам ложных сведений относительно принадлежности карты, и тем самым не вводил их в заблуждение. Исходя из этого, оснований для квалификации действий гр-на Р. по части 1 статьи 159.3 УК РФ нет.

Суд апелляционной инстанции квалифицировал действия обвиняемого по пункту «г» части 3 статьи 158 УК РФ4 . Вместе с тем в научном сообществе попрежнему нет единства мнений относительно квалификации рассматриваемых деяний

Возвращаясь к вопросу о том, какие деяния следует квалифицировать как мошенничество с использованием электронных средств платежа, отметим, что определенная часть приговоров по статье 159.3 УК РФ в настоящее время выносится в отношении деяний, в рамках которых злоумышленники используют сеть Интернет для размещения заведомо ложной информации о продаже товаров или услуг, не намереваясь при этом исполнять свои обязательства. Потерпевший в таких ситуациях, не подозревая о преступных намерениях лица, переводит с помощью своего электронного средства платежа денежные средства в счет оплаты данного товара или услуги для виновного.

Так, гражданин посредством своего смартфона, используя ложные данные, через Интернет зарегистрировался на платформе по размещению электронных объявлений «Авито» и разместил там информацию о продаже тепловизораFlir за 16 000 рублей, заведомо осознавая, что данный товар у него отсутствует. Кроме того, обвиняемый в целях реализации своего преступного умысла на финансовой платформе «Qiwi» зарегистрировал онлайн-кошелек, авторизировав его также на ложное имя.

В дальнейшем подсудимый ввел находящегося вдругом городе

потерпевшего в заблуждение относительно наличия тепловизораFlir и готовности продать указанный товар за сумму в 14 000 рублей, а также отправить тепловизор по адресу потерпевшего после получения оплаты в полном объеме. Потерпевший посредством мобильного банковского приложения перевел обвиняемому на указанный им номер виртуального кошелька оговоренную сумму. Подсудимый, с целью придания видимости законности своим действиям и уклонения от возможного уголовного преследования в дальнейшем, предоставил потерпевшему ложные сведения относительно отправки товара транспортной компании, а также истребовал от жертвы сумму якобы произведенных затрат на пересылку тепловизора в размере 1000 рублей. Указанные денежные средства потерпевший также посредством электронного средства платежа перевел на виртуальный кошелек посягателя. В дальнейшем злоумышленник распорядился полученными 15 000 рублей по своему усмотрению. Товар при этом потерпевшему не предоставил и предоставлять не намеревался. Действия обвиняемого были квалифицированы по части 2 статьи 159.3 УК РФ. В ситуации, когда потерпевшее лицо, находясь под воздействием ложной информации, предоставленной злоумышленником, самостоятельно осуществляет операцию по зачислению собственных наличных денежных средств на банковский счет виновного лица, такие действия подлежат квалификации по статье 159 УК РФ как мошенничество.

Однако обратим внимание на практику судов до июня 2021 года, когда, по сути, при тех же фактических обстоятельствах имела место переквалификация действий виновных со статьи 159.3 УК РФ на статью 159 УК РФ. Так, отдельные действия гр-на П. были квалифицированы по части 2 статьи 159.3 УК РФ.

Было установлено, что подсудимый, с целью хищения денежных средств путем обмана, при помощи телефонной связи связывался с потерпевшими, вводил их в заблуждение о том, что является представителем

ООО «...» и ООО «...» и что в продаже у них есть необходимые потерпевшим автомобильные детали. После этого гр-н П. вводил потерпевших в заблуждение о реальности, законности и добросовестности его деятельности, предоставлял потерпевшим номер счета для оплаты товаров. При этом подсудимый исполнять условия договора не намеревался.

Потерпевшие, обманутые обвиняемым, перечисляли на данный банковский счет денежные средства, которыми затем виновный распоряжался по своему усмотрению. Кроме того, гр-н П. с целью хищения чужого имущества путем обмана, используя информационно-телекоммуникационную сеть Интернет, разместил на сайте «...» объявление от имени ООО «…», сообщив заведомо ложные сведения о продаже запчастей для автомобилей и указав абонентский номер, находящийся в его пользовании, в действительности данным товаром не располагая. Действия виновного в суде были переквалифицированы с части 2 статьи 159.3 УК РФ на часть 1 статьи 159 УК РФ.

НИЖЕ НЕ СУДЕБНАЯ ПРАКТИКА, А СЛЕДСТВЕННАЯ. ЭТО БОЛЬШЕ ИМЕЕТ ЗНАЧЕНИЕ ДЛЯ КРИМИНАЛИСТИКИ

Изучение уголовных дел показало, что современные способы совершения мошенничества в отношении физических лиц являются полноструктурными, так как мошенники тщательно готовятся к совершению преступления и предпринимают необходимые действия по его сокрытию. Рассмотрим данные способы более подробно.

1. Роботизированные помощники. В последние месяцы преступные сообщества стали активнее использовать возможности машинного обучения и современных речевых технологий. Так, если в начале 2021 г. мошенники звонили на мобильные телефоны своим жертвам, то к концу 2021 — началу 2022 г. большая часть звонков стала совершаться с помощью голосовых роботов. Автоматизация обзвона потенциальных потерпевших, безусловно, облегчает мошенникам совершение преступления, так как охватывает

большее количество аудитории. По данным KasperskyWhoCalls, осенью 2021 г. по сравнению с январем — февралем 2021 г. в 35 раз выросло количество звонков с подозрением на мошенничество, когда злоумышленники применяли роботизированные обзвоны, похожие на те, которыми обычно пользуются финансовые организации.

Потенциальному потерпевшему поступает звонок от банковского робота-помощника, которого запрограммировали мошенники. Робот сообщает клиенту банка о том, что в его личном кабинете замечены подозрительные действия [11, с. 65].

Мошенники задают вопросы, которые требуют ответа «да» или «нет» (например:«Вы совершали операции с картой за последний месяц?»), и когда клиент отвечает: «Да», мошенники автоматически получают доступ к личному кабинету жертвы и, соответственно, возможность распоряжения денежными средствами последнего по своему усмотрению.

Если жертва отказывается подтверждать операции в тональном режиме, то происходит соединение с псевдосотрудником службы безопасности банка, который в разговоре пытается получить все данные абонента. В ходе телефонного разговора с потенциальной жертвой преступники стараются оказать давление на собеседника, торопят последнего и вынуждают принимать быстрые необдуманные решения, не давая возможности потенциальной жертве обсудить их с родственниками или близкими людьми.

Так, 12 декабря 2021 г. на мобильный телефон В. поступил звонок с неизвестного номера. В ответ В. услышала голос робота-помощника, который представлял один из известных банков. Далее робот спросил: «Это Светлана Александровна В. (назвав ее полную фамилию)?». Она ответила: «Да». Далее мошенники получили доступ к личному кабинету В. и похитили ее денежные средства [42].

Мошенники похищают деньги, создавая фишинговые сайты,

копирующие настоящие интернет-магазины (OZON, Wildberries, iHerb и др.). Так, 28 декабря 2021 г. на электронную почту А. пришло сообщение о скидке 70 % на большую группу товаров интернет-магазина OZON, которая действует в течение всего двух часов. В сообщении была указана ссылка для перехода на сайт данного магазина, где перечислялись товары, на которые действует скидка [42]. Тот факт, что адрес сайта магазина был немного изменен, А. сразу не заметила. Перейдя по ссылке, А. оформила заказ на сумму 36 тыс. рублей и оплатила заказ онлайн. Не дождавшись своего заказа, А. перешла на настоящий сайт магазина OZON, где обнаружила, что в ее личном кабинете никаких заказов нет.

Другая ситуация: потенциальным жертвам посредством социальных сетей либо электронной почты приходят навязчивые сообщения с просьбой получить денежные средства, выигранные в каком-либо конкурсе, в котором жертва даже не участвовала. Когда потенциальный потерпевший переходит по указанной ссылке, мошенники получают доступ к его личному кабинету и, соответственно, возможность распоряжения денежными средствами последнего по своему усмотрению.

В последние годы, особенно после начавшейся пандемии коронавируса COVID-19, большинство граждан пользуются интернет-сервисами, совершают покупки онлайн, и, соответственно, оставляют свои данные (Ф. И. О., номера телефонов, номера банковских карт и др.) на просторах Интернета. Зачастую эти данные попадают в базу черных брокеров, которые начинают регулярно звонить с предложением поторговать на выгодной бирже. Эти брокеры обещают делать прогнозы и указывать только выгодные ставки. Если потенциальная жертва соглашается, то брокер предлагает последней вложить немалую денежную сумму.

Вежливые брокеры настаивают взять кредит и даже предлагают свою помощь в его получении в случае плохой кредитной истории потенциальной жертвы. Далее за клиентом закрепляют персонального менеджера, который,

скорее всего, сидит у себя дома и делает вид, что работает в офисе, а фоном ставит запись с телефонными разговорами. Хотя возможно, он насамомделе находится в офисе, где такие же «сотрудники» вводят в заблуждение по телефону новых жертв.

Основная задача менеджера — заставить потенциальную жертву скачать некий софт и установить в свой телефон или компьютер. Он расскажет, как завести там аккаунт, вложить свои деньги и начать торги на бинарных опционах. Посмотрев на большие денежные суммы, подделанные в данной программе, потенциальная жертва начнет мечтать о покупке квартиры, машины и т. д.

Далее начинаются финансовые потери клиента. Главная цель персонального менеджера — чтобы клиент вложил как можно больше денежных средств. Для этого он будет постоянно уговаривать вложить еще деньги, ведь скоро все станет хорошо, и клиент якобы выйдет в плюс и получит большую прибыль. Но при этом клиент будет наблюдать очередные потери своих денег. А менеджер будет требовать получения очередного кредита клиентом.

Мошенничество с использованием сервиса «Авито Доставка». Всем известно, что платформа «Авито» является удобной площадкой для размещения объявлений о продаже товаров, предоставлении услуг и т. д. На данной платформе мошенники уже не первый год обманывают людей, изобретая все новые формы обмана. Преступники научились обманывать и покупателей, и продавцов.

Рассмотрим типичный пример с подменой ссылки через Авито Доставку. Мошенник оформляет подробное объявление о продаже, например, ноутбука, указывая причину продажи — по ненадобности. Стоимость ноутбука при этом занижена на 30—40 % от его рыночной цены [42].

Естественно, такое объявление привлекает большое количество покупателей. После убедительного разговора с продавцом подозрений у

потенциальной жертвы обычно не остается. Многие площадки объявлений внутри своего приложения или сайта блокируют чужие ссылки, чтобы продавец не смог перенаправить покупателя в другой мессенджер в целях обмана.

Опционами занимаются трейдеры, которые позиционируют себя успешными людьми, живущими на берегу океана, ни в чем себе не отказывающие, которые якобы тратят несколько часов в день на работу, а остальное время они совершенно свободны. В то же время трейдеры готовы поделиться своим секретом большого финансового успеха со всеми желающими. Трейдеры тратят большие деньги на рекламу своих аккаунтов в социальных сетях для того, чтобы иметь возможность завлечь как можно больше клиентов в целях получения материальнойвыгоды. Рассказав о своей красивой жизни, трейдер переходит к действиям. «Учитель» предлагает регистрацию по ссылке (см. рисунок 4) с обязательным открытием счета на платформе. Клиент при этом должен пополнить свой баланс на максимальную возможную сумму.

Далее трейдер высылает ссылку для доступа к закрытой группе, в которой он будет проводитьобучение. После этого начинается торговля по его сигналам. Схема обмана с трейдерами не представляет особой сложности: трейдер зарабатывает проценты от депозита клиента, но в большинстве случаев наживается именно на проигрышах. В итоге клиент проигрывает весь свой депозит.

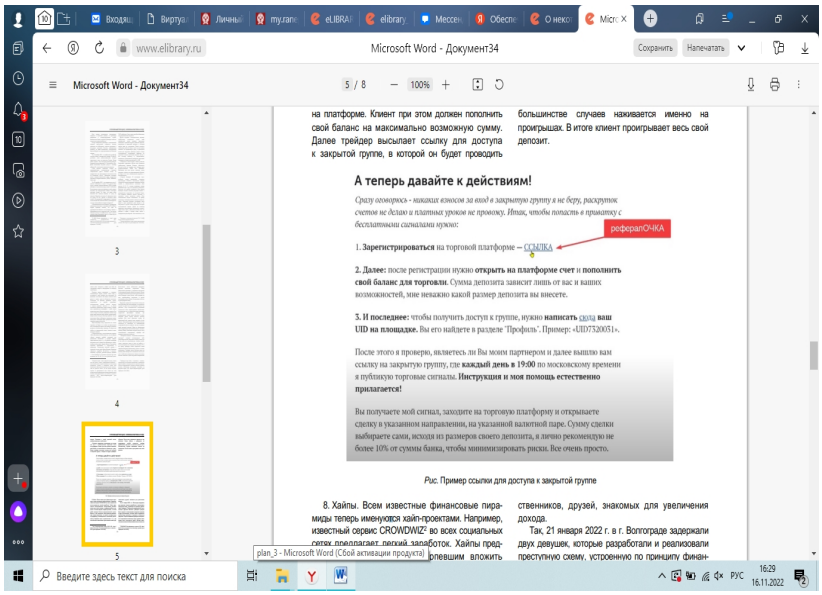

Рисунок 4 - Пример ссылки для доступа к закрытой группе

Всем известные финансовые пирамиды теперь именуются хайп-проектами. Например, известный сервис CROWDWIZ2 во всех социальных сетях предлагает легкий заработок. Хайпы предлагают потенциальным потерпевшим вложить деньги под очень высокие, нереалистичные проценты.

Сначала жертвы создают депозит, а потом якобы выводят больше первоначальной суммы. Вместе с тем создатели хайп-проектов рассказывают своим вкладчикам, что деньги последних идут на разработку инновационных технологий, криптовалюту, биржевые торги, строительство и т. д., при этом активно навязывают приглашение своих родственников, друзей, знакомых для увеличения дохода [25, с. 97].

Так, 21 января 2022 г. в г. Волгограде задержали двух девушек, которые разработали и реализовали преступную схему, устроенную по принципу финансовой пирамиды [42].

Сотрудницы микрокредитной организации «Депозит Капитал» убеждали граждан брать кредиты и инвестировать денежные средства в свою организацию, которая якобы занимается прибыльными проектами и нуждается в оборотных средствах. В целях завоевания доверия

потенциальных потерпевших мошенницы сразу отдавали заемщикам часть полученных денег, обещая самостоятельно вносить в банки ежемесячные платежи закредит. Как правило, в течение первых двух месяцев они выполняли обещание, но далее платежи прекращались. В полицию поступило более 200 заявлений от пострадавших, каждый из которых отдал микрокредитной организации от 1 до 8,5 млн рублей [37, с. 21].

2.3 Оценка эффективности профилактики мошенничества с использованием банковских карт и интернет ресурсов

ЭТО КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА!

Оценка эффективности профилактики мошенничества с использованием банковских карт и интернет ресурсов проводилась с помощью следующих показателей:

- динамика численности зарегистрированных случаев мошенничества в банковской сфере;

- динамика коэффициента интенсивности мошенничества в банковской сфере в Российской Федерации, в федеральных округах;

- динамика уровня и структуры зарегистрированных мошенничеств в банковской сфере по видам (ст. 159.1 и 159.3 УК РФ) в РФ;

- динамика уровня и структуры выявленных и осуждённых лиц, совершивших мошенничества в банковской сфере, по видам (ст. 159.1 и 159.3 УК РФ) в РФ;

- структура способов мошенничества с использованием электронных средств платежа;

- структура способов совершения мошенничествас использованием электронных средств платежа (ст. 159.3 УК РФ) в РФ;

- структура способов совершения мошенничества в кредитной сфере (ст. 159.1 УК РФ).

Непосредственный анализ динамики уровня исследуемых мошенничеств за последние пять лет (2016–2020 гг.) в РФ в целом свидетельствует о неуклонном его росте. Так, за изученный период абсолютное количество мошенничеств увеличилось в 3,7 раза: с 8 713 преступлений, зарегистрированных в 2016 г., до 32 186 в 2020 г. Эту же тенденцию подтверждают и относительные показатели.

Так, коэффициент интенсивности данных преступлений увеличился за рассматриваемый период на такую же величину (в 3,7 раза) – с 5,9 преступлений, приходящихся на 100 тыс. чел. в 2016 г., до 21,9 в 2020 г. (см. таблицу 1).

Таблица 1 - Динамика состояния зарегистрированных случаев мошенничества в банковской сфере (ст. 159.1 и 159.3 УК РФ) по федеральным округам за 2017–2020гг [41]

Год	ЦФО	СЗФО	ЮФО	СКФО	ПФО	УФО	СФО	ДФО	РФ
2017	2589	572	846	524	1846	788	1353	156	8713
2018	2480	668	1177	525	2160	912	1230	290	9480
2019	2883	1250	1730	889	3439	1089	1974	479	13733
2020	5407	3192	2747	1435	7765	2093	4545	1640	28904

Вместе с тем территориально по стране мошенничества данного вида распределены неравномерно. Так, по совокупным абсолютным показателям мошенничеств в банковской сфере, зарегистрированных в период 2016–2019 гг., лидируют Приволжский и Центральный федеральные округа (ПФО, ЦФО), что имеет логичное объяснение, поскольку на указанной территории проживает большая часть населения РФ, здесь находится наиболее развитая сеть банковских учреждений.

Соответственно, в федеральных округах с невысокой численностью населения, где огромные территории вообще не заселены, рассматриваемых преступлений было зарегистрировано в несколько раз меньше.

Так, например, в федеральных округах, находящихся за Уралом и

занимающих по территории две трети страны, совокупные абсолютные показатели за исследуемый период были ниже максимального показателя по ПФО (15 210): в Сибирском федеральном округе (СФО) – в 1,7 раза (9 102), в Уральском федеральном округе (УФО) – в 3 раза (4 882), в Дальневосточном федеральном округе (ДФО) – фактически в 6 раз (2 565) (см. таблицу 2).

Таблица 2 - Динамика коэффициента интенсивности мошенничества в банковской сфере в Российской Федерации, Сибирском, Уральском, Дальневосточном федеральных округах в 2017–2020 гг. (на 100 тыс. человек) [41]

Год	РФ	СФО	УФО	ДФО
2017	5,9	7	6,4	2,5
2018	6,5	6,4	7,4	4,7
2019	9,3	10,2	8,8	3,9
2020	19,7	26,5	16,9	20

Между тем динамика состояния в абсолютных показателях по федеральным округам имеет неоднозначный характер. Например, в ДФО, демонстрирующем самые низкие абсолютные показатели за рассматриваемый период, мошенничества в банковской сфере развивались самыми высокими темпами в стране: их количество увеличилось в 10,5 раз, тогда как в ЦФО – только в 2 раза, что оказалось самым низким приростом.

Иными словами, в ДФО темпы прироста были в 3 раза выше, чем в целом по стране, и в 5 раз выше, чем в ЦФО, где регистрируется большинство рассматриваемых преступлений. Указанные тенденции подтверждают и относительные показатели, которые свидетельствуют о том, что мошенничества рассматриваемого вида на указанных территориях развивались более высокими темпами, чем в Российской Федерации в целом, и по уровню интенсивности даже превышали общероссийский коэффициент. Например, в СФО в 2019 г. он был на 7 единиц выше, чем в РФ (26,5 против 19,7). При этом сам общероссийский коэффициент продолжает расти. В 2020

г. он увеличился ещё на 2 единицы и составил 21,9 (см. таблицу 2).

Анализ удельного веса мошенничеств, совершённых в банковской сфере, по видам свидетельствует о значительных изменениях, произошедших в структуре этих преступлений за исследуемый период. Так, если на начало периода 95 % в структуре мошенничеств в банковской сфере составляли мошенничества, совершённые в сфере кредитования, то к концу периода (2020 г.) таким мошенничеством было только каждое пятое. Снижение уровня мошенничеств произошло на 79 %. Напротив, доля мошенничеств с использованием электронных средств платежа выросла в 16 раз, а темпы прироста данного вида мошенничеств составили 1500 %. Иными словами, количество зарегистрированных преступлений за исследуемый период выросло в 45,7 раз (см. таблицу 3).

Таблица 3 - Динамика уровня и структуры зарегистрированных мошенничеств в банковской сфере по видам (ст. 159.1 и 159.3 УК РФ) в РФ за период 2015–2020 гг. [41]

Вид мошенничества в банковской сфере	Зарегистрировано мошенничеств в банковской сфере		Темпы прироста удельного веса мошенничеств в банковской сфере, %	Удельный вес видов мошенничеств в структуре мошенничеств в банковской сфере, %	
	2015 год	2020 год	2015-2020 гг.	2015 год	2020 год
Ст. 159.3 С использование м электронных средств платежа	565	25820	+1500	5	80

Следует отметить, что и в общей структуре мошенничеств доля рассматриваемого вида преступлений растёт. Так, в 2020 г. она составила 9,6

%, тогда как в 2015 г. – только 5,6 %. Это значит, что каждое десятое мошенничество в РФ в 2020 г. было совершено в банковской сфере. Для полноты характеристики количественных показателей преступлений рассматриваемого вида необходимо обратиться к количественным показателям выявленных по ним преступников.

Их анализ свидетельствует о снижении уровня выявления мошенников, совершающих преступления в банковской сфере.

Так, если в 2015 г. выявляли каждого второго, а осуждался каждый пятый мошенник, то в 2020 г. выявляли уже каждого третьего, а осуждали только шестого-седьмого (см. таблицу 3, 4).

Таблица 4 - Динамика уровня и структуры выявленных и осуждённых лиц, совершивших мошенничества в банковской сфере, по видам (ст. 159.1 и 159.3 УК РФ) в РФ за период 2015–2020 гг. [41]

Вид мошенничества в банковской сфере	Выявлено лиц, совершивших мошенничество в банковской сфере		Темпы прироста выявленных лиц	Удельный вес лиц, совершивших мошенничество, %		Осуждено лиц за совершение мошенничества в банковской сфере		Темпы прироста осуждённых, %
	2015 год	2020 год	2015–2020 гг	2015 год	2020 год	2015 год	2020 год	2015–2020 гг
Ст. 159.3 С использованием электронных средств платежа	375	8362	2130	5,6	68,7	154	3084	1902

Анализ видов мошенников в банковской сфере показал, что здесь

изменения имели сходный, но более выраженный характер. Так, при снижении доли мошенников, совершивших преступления в сфере кредитованияв 3 раза доля лиц, совершивших мошенничество с использованием электронных средств платежа, увеличилась в 12 раз, а темпы прироста как выявленных, так и осуждённых за этот вид мошенничества лиц составили 2 130 и 1902 % соответственно (см. табл. 4). Всё это в целом свидетельствует об общем росте мошенничеств в банковской сфере и фантастических темпах роста мошенничеств с использованием электронных средств платежа.

Такая динамика, на наш взгляд, связана с изменением методов совершения данных преступлений, произошедшим за исследованный период. Всё чаще мошенники предпочитают использование малозатратных психологических способов обмана жертвы.

В 2020–2021 гг. аналитики банка Тинькофф провели исследование мошенничества в российской банковской сфере и выявили самые распространённые методы хищений средств у клиентов российских банков, а также описали типичные схемы обмана. Согласно их исследованиям, доля мошенничеств с использованием социальной инженерии7 в 2018 г. составляла 36 %, в 2019 г. – около 70 %, в 2020 г. – 80 %, т. е. за 3 года эта доля выросла более чем в 2 раза. В 2020 г. 50 % всех денег, полученных мошенниками, люди перевели им сами (в 2019 г. эта доля составляла только 30 %). Ещё 28 % составили потери от того, что клиенты раскрывали данные карт или секретные коды.

Анализ сценариев мошенничества с использованием электронных средств платежа показал, что в 42 % случаев, когда мошенники пытаются узнать смс-коды и данные карт, они представляются службой безопасности сторонних банков (т. е. не того банка, операции по карте которого планируют совершить); в 25 % случаев – службой безопасности банка, по карте которого впоследствии будут запрашивать информацию; 11 % приходится на схемы с

покупкой и продажей товаров в сети; 22 % – на другие сценарии (инвестиции, комиссии за получение выигрыша, вознаграждения за опрос и т. д.)

Средняя сумма успешного мошенничества на одного клиента в 2019 г. варьировала (в зависимости от способа банковского мошенничества) от 48,8 тыс. руб. до 4,7 тыс. руб., в 2020 г. – от 45 тыс. руб. до 4,5 тыс. руб.

Стоит заметить, что некоторое снижение суммы оправдано, поскольку чем она ниже, тем меньше вероятность обращения потерпевшего в правоохранительные органы и выше вероятность компенсации этой суммы банком, если клиент «не виноват».

Анализ динамики способов мошенничества с использованием электронных средств платежа с момента его регламентации в 2014 г. до 2020г., по итогам региональных исследований авторов, свидетельствует, что в Сибирском федеральном округе изменение способов совершения указанного вида мошенничеств также менялось, но несколько иным образом.

Так, например, в 2014 г. больше половины преступлений, регламентированных ст. 159.3 УК РФ, совершалось с использованием поддельных карт (53 %) [1]. Между тем в 2020 г. уже каждое второе мошенничество совершалось с использованием подлинных карт или их реквизитов, похищенных путём обмана у владельцев (50 %). Почти не изменилась только доля преступлений, совершённых с использованием подлинных карт, заведённых злоумышленниками: 2014 г. – 10 %, 2020 г. – 11,5 % (см. рисунок 5).

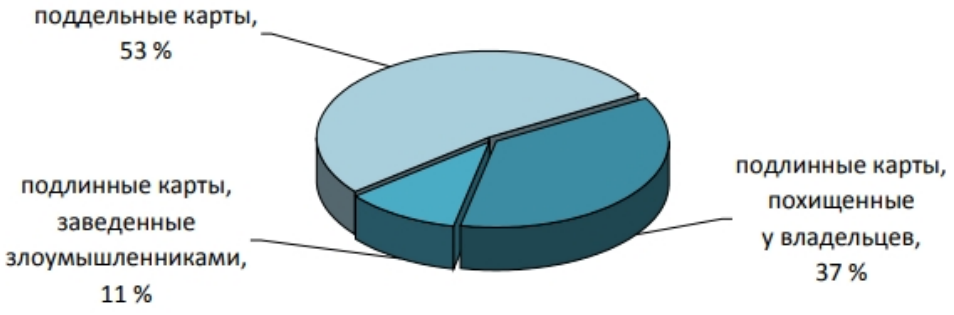

Рисунок 5 - Анализ динамики способов мошенничества с использованием электронных средств платежа в 2014, % [41]

Таким образом, при сравнении с общероссийскими результатами исследований доля мошенничеств, совершённых в 2019 г. с использованием подлинных карт или их реквизитов в СФО, была меньше на 20 %, при этом стоит учитывать, что сюда входят как случаи использования подлинных карт, которыми мошенники завладели обманным путём, так и случаи, когда потерпевшие сами предоставили мошенникам реквизиты платежей по своим картам.

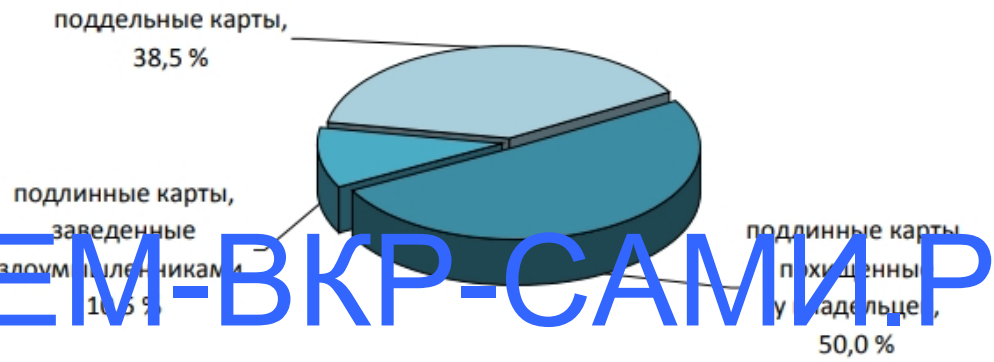

Рисунок 6 - Динамика способов совершения мошенничествас использованием электронных средств платежа (ст. 159.3 УК РФ) в РФв2019 гг. в СФО, % [41]

Такую региональную специфику подтверждают и эксперты10. Согласно их исследованиям, наименьший индекс подверженности мошенничеству (FraudIndex) демонстрируют регионы Сибири (Тува, Алтай, Хакасия, Кемеровская и Иркутская области, Забайкальский край, Бурятия) и Дальнего Востока (Чукотка, Саха (Якутия), Сахалинская область). Самые высокие значения этого индекса в Москве, Санкт-Петербурге, Московской и Ленинградской областях.

Лидерство с ними делят Калининградская область и Севастополь. Увеличение доли мошенничеств, совершённых с использованием подлинных

карт, связано прежде всего с изменением банковских технологий. Так, в последние несколько лет банки предложили своим клиентам новые карты, оснащённые технологией бесконтактной оплаты: VisaPayWave, MasterCardPayPass. Цель их выпуска – облегчение проведения платежей для клиентов. Достаточно лишь поднести такую карту к считывающему устройству, и деньги будут списаны со счёта без введения ПИН-кода, что сделало их лёгкой добычей для мошенников.

Следует отметить, что из способов совершения мошенничеств с использованием электронных средств платежа практически исчез скримминг (использование специальных технических устройств для считывания данных карты клиента) из-за высокой стоимости и сложности использования для мошенников. Несколько иная ситуация с изменением способов совершения мошенничеств в сфере кредитования. Если в начале исследуемого периода преобладало получение кредита путём использования чужих паспортов (43,5 %), то в 2020 г. каждое второе мошенничество в этой сфере совершено физическими лицами при предоставлении заведомо ложных документов (49,9 %). В 2,5 раза выросло получение кредитов без цели возвращения. В 2020 г. таким было практически каждое третье мошенничество (30 %). Снизилось количество мошенничеств, совершённых через подставное лицо, с 19 до 13 % (см. рисунок 7).

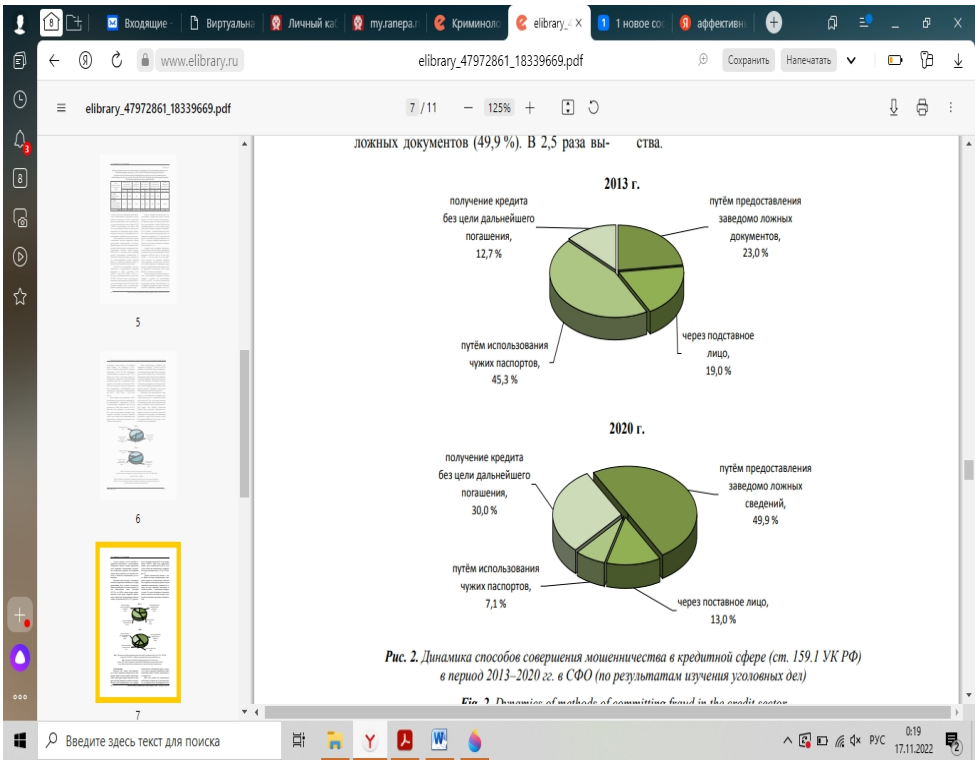

Рисунок 7 - Динамика способов совершения мошенничества в кредитной сфере (ст. 159.1 УК РФ) в период 2013–2020 гг. в СФО (по результатам изучения уголовных дел) [41]

Данные обстоятельства связаны с тем, что банки постоянно совершенствуют механизмы защиты от мошеннических действий. Так, например, используются разные методы выявления мошенничества, основной из которых на этапе обработки полученных от клиентов данных – предоставление заведомо ложных сведений.

3 Проблемы эффективности и разработка направлений совершенствования профилактики мошенничества с использованием банковских карт и интернет ресурсов

3.1 Проблемы профилактики мошенничества с использованием банковских карт и интернет ресурсов

Использование электронных денег, замена расчетов наличными деньгами на безналичные с помощью электронных средств платежа, возможность управлять своими финансами онлайн с компьютера, планшета или смартфона становится все более актуальными, удобными и распространенными среди потребителей.

Разработка и повсеместное внедрение технологии и оборудования для бесконтактных платежей и практически мгновенного зачисления платежей на расчетные счета позволило ускорить транзакции и соответственно оборачиваемость денежных средств, что, несомненно, способствует дальнейшему развитию электронных платежных технологий [39, с. 6].

Мошенничество является одной из самых критичных проблем рынка платежных карт. Именно риски мошенничества являются основной причиной, по которой население, не имеющее платежных карт, выражает недоверие к ним, а уже действующие держатели карт опасаются проводить операции по ним. Решение данной проблемы полностью невозможно, поскольку риск мошенничества есть всегда, а вслед за развитием технологий, прямо или косвенно влияющих на платежные карты и операции по ним, развиваются новые технологии и способы мошенничества. Но минимизации рисков мошенничества и эффективные способы борьбы с ним позволяют привлекать новых клиентов, увеличивать эмиссию платежных карт, стимулировать оборот операций, проводимых с их помощью [8, с. 96].

Для борьбы со скиммингом банкам следует активнее использовать следующие способы:

1. Физический мониторинг, который представляет собой осмотр банкоматов на их целостность и наличие на нем нештатных устройств.

2. Активныйантискиммер, который представляет собой установку антискиммера внутрь банкомата. Он позволяет сразу выявить попытку установить несанкционированное устройство. К тому же такой антискиммер может создавать помехи для передачи данных на посторонние электронные устройства [23, с. 14].

На данный момент такими устройствами, в основном, оснащаются только новые банкоматы в то время, как старые устройства (которых подавляющие большинство), остаются уязвимыми для скимминга. Даже Сбербанк с его огромными возможностями не всегда обновляет свое оборудование до нужного уровня, не говоря уже о малых и средних игроках.

3.Законодательным органам необходимо внести поправки в закон, представить правовую регламентацию мошенничества в интернете и с банкоматами и подробно описать виды особенности меры борьбы и ответственность за данный вид мошенничества с пластиковыми картами. Например, при усовершенствовании статей УК РФ следует обратить внимание на следующие статьи.

Во-первых, это статья 138.1. «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации». Здесь говорится об уголовной ответственности за незаконное производство, продажу или покупку специальных технических устройств, помогающих получить конфиденциальную информацию[1].

С одной стороны, скиммер является как раз таким незаконным устройством, позволяющим получить конфиденциальную информацию о владельце пластиковой карты, но, к сожалению, в законе не дается точной характеристики, что представляет собой данное техническое устройство, поэтому данное обобщенное описание позволяет производителям и покупателям скиммеров уходить от ответственности. В целях безопасности

законодатель должен дать описание, чем конкретно является незаконное средство, и в каких именно случаях оно используется.

Во-вторых, следует усовершенствовать раздел уголовного кодекса о преступлениях в экономической сфере, а именно статей 183 и 187, поскольку здесь говорится о банковской тайне и использованию платежных карт. В статью 183 следует добавить «собирание сведений, составляющих… банковскую тайну …путем похищения документов, подделки платежных карт, подкупа или угроз…».

Данное изменение позволит наказывать скиммеров, так как они как раз занимаются тем, что подделывают конфиденциальную информацию о владельце карты, являющуюся банковской тайной. В статье 187 следует изменить то, что злоумышленник будет наказан не только за то, что изготавливает или сбывает платежную карту, но и использует ее в своих или чужих корыстных интересах.

В-третьих, нужно модернизировать статью 159 «Мошенничество», а именно статью 159.3 «Мошенничество с использованием платежных карт», поскольку здесь говорится лишь о том, что махинации происходят путем обмана сотрудника банка [1].

Усовершенствовать необходимо, так как злоумышленник-скиммер не общается с сотрудником, а лишь с банкоматом, а он является техническим средством, который не может анализировать и распознать обман (что вместо настоящей пластиковой карты используется поддельная пластиковая карта). Поэтому в статью следует добавить, что мошенничество с использованием платежных карт происходит путем обмана сотрудника банка, банковской системы, технических устройств. Важно отметить, что на законодательном уровне происходят активные и эффективные изменения.

Так, одним из важнейших шагов к стимулированию борьбы самих банков с мошенничеством были реализованы изменениями в Федеральном законе N 161-ФЗ «О национальной платежной системе», где статья 27

обязывает банки (и других участников платежной системы и инфраструктуры) обеспечивать защиту информации при осуществлении переводов денежных средств, защиту персональных данных.

Еще одним важным законодательным решением в области решения проблемы мошенничества на рынке платежных карт стало то, что в апреле 2018 года Государственной Думой Российской Федерации принят закон, который ужесточает ответственность за кражу денежных средств с банковских карт, усилена уголовная ответственность за воровство платежных карт, за хищение денег с банковских счетов и со счетов электронных кошельков. Такой закон, однозначно, окажет положительное воздействие на ситуацию с киберпреступностью и кардингом.

Федеральный Закон № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» от 23 апреля 2018 года поднимает также и размеры штрафов за кражу денег с банковских счетов и электронных кошельков граждан до 100 000 – 500 000 рублей. Ужесточены наказание в виде принудительных работ, ограничения или лишения свободы преступников. Теперь за кражу денежных средств с банковских карт закон предусматривает принудительные работы на срок до 5 лет, ограничение свободы до 1,5 лет, и наказание в виде лишения свободы до 6 лет [43].

Жестче стали наказания и за мошенничество с использованием электронных средств, теперь за подобные преступление предусмотрены такие меры как лишение свободы до 3 лет (ранее это было всего лишь арест до 4 месяцев). Хотя мошенник может отделаться и альтернативным наказанием в виде штрафа до 120 000 рублей, либо ограничением свободы до 2 лет, либо исправительными работами до 1 года. Отныне уголовная ответственность установлена и за такие преступления как присвоение посторонним собственностью либо материальными правами с помощью блокировки, изменения либо другого влияния на ресурсы хранения, передачи либо обработки электронных данных, либо информационно-

телекоммуникационных сетей [32, с. 67].

Помимо законодательного решения проблемы мошенничества и реализации банком технических возможностей препятствования противоправным действиям, банкам-эмитентам следует проводить работу, направленную на повышение вовлеченности и грамотности населения в области использования платежных карт.

Данная проблем в РФ стоит достаточно остро. Во многом, вероятно, это связано и с некой некомпетентностью и «халатностью» как сотрудников банков, так и банков в целом. При открытии банковской карты, в основном, клиенты не получают никакого должного инструктажа по использованию банковских карт. Сотрудники банка не рассказывают о мерах предосторожности и основах безопасности при использовании платежных карт. В основном, выдача карты сопровождается лишь подписанием документов [19, с. 65].

Существенное сокращение уровня мошенничества можно добиться, если банковские сотрудники будут проводить обязательную консультацию по использованию платежных карт, а также будет выдаваться распечатанная памятка, в которой информация будет представлена крупным шрифтом и наглядно.

Не менее важной является и проблема вовлеченности населения в рынок банковских карт. Для решения этой проблемы необходимо создавать все более благоприятные условия для функционирования банковских карт, особый упор делая на зарплатные проекты, потому что именно таким способом и происходит подавляющее большинство подключений новых клиентов. Также стоит развивать систему семейных проектов, благодаря чему появляются новые клиенты даже вне зарплатных проектов, в том числе и достаточно молодые клиенты.

Необходимо проводить активные маркетинговые кампании, нацеленные на привлечение новых клиентов. В этих кампаниях необходимо

убедить людей в удобности и выгоде использовании банковских карт, а также изменять представления людей о безопасности карт в положительную сторону. Уменьшение процентных ставок по кредитным картам позволит увеличить притягательность этого варианта платежного инструмента, что повысит обилие выпущенных карт и операции по ним, а значит, сможет повысить доходность банковской организации.

Эффективным инструментом привлечения новых клиентов являются кобрендинговые проекты. Расширение списка партнеров и предлагаемых программ может послужить хорошим стимулом для распространения не только дебетовых, но и кредитных карт. Чтобы минимизировать риски просрочек задолженности по кредитным картам, стоит более внимательно относиться к выпуску кредитных карт. Здесь подразумевается более тщательная проверка клиента на его способность погасить долг, поскольку сейчас выдача кредитной карты представляет собой более простой процесс, нежели выдача кредита наличными [13, с. 65].

Решить данные проблемы можно с помощью более активного использования нового оборудования, устройств, позволяющих пресечь мошеннические попытки, расширение законодательства и внедрение новых инновационных технологий.

3.2 Разработка мер профилактики мошенничества с использованием банковских карт и интернет ресурсов

В последние годы получил распространение такой вид мошенничества с использованием банковских карт, как спуфинг идентификатора вызывающего абонента (англ. spoofing – подменять) – маскировка под другую личность путём фальсификации личных данных, позволяющая получать незаконные преимущества.

Разумеется, службы безопасности банков осведомлены оподобного

рода мошенничестве и предпринимают меры по защите вкладов своих клиентов, например, предлагают им использовать кардридеры для сканирования QR-кодов для авторизации входа и платежей. Это делает таких клиентов менее уязвимыми в сравнении с клиентами, отправляющими обычные текстовые сообщения, поскольку имитировать QR-коды на фишинговом сайте банка сложнее, чем создать поле ввода для кода подтверждения.

Еще одним способом надежной защиты кладов потенциальных жертв являются использование лимитов на трансакции, которые установлены по умолчанию для некоторых банков. Часто они ограничиваются довольно небольшими суммами, и клиентам придется увеличить лимит, если они хотят произвести более крупные платежи. Когда банк просит клиента увеличить этот лимит, а не наоборот, это должно стать для последнего тревожным сигналом [34, с. 84].

В одних банках предусмотрена страховка от банковского мошенничества, но другие банки могут заявить, что жертва сама перевела средства, и банк в том случае не несет ответственности за убытки. В большинстве стран клиенты защищены законом от мошеннических платежей при определенных условиях. Одно из этих условий обычно можно сформулировать как «клиент не должен быть беспечным», и клиент может считаться беспечным, если он добровольно предоставит свои учетные данные для входа.

Вопрос о том, является ли ввод этих учетных данных на фишинговом сайтефальшивого банка, который выглядит точно также, как сайт реального банка, неосторожным, остается предметом споров.

Следует помнить о таких способах виктимологического противостояния мошенникам, как психологическая самозащита, критичность (осмотрительность) в собственных действиях (главным образом, финансового характера), безопасное поведение в нестандартной ситуации,

критический уровень доверия, осознание возможных рисков. Телефонные звонки мошенников сегодня становятся все более распространенным способом противоправного посягательства [29, с. 17].

Мошенники обучены профессионально разговаривать с потенциальными жертвами. Во многих случаях мошенники выдают себя за сотрудников сервисных центров и часто создают фальшивые уведомления, в которых они создают у потерпевших ощущение срочности в отношении исполнения услуги. Мошеннические звонки могут поступать откуда угодно – из-за границы, из других регионов, из мест лишения свободы [38, с. 97].

Существует несколько способов узнать, кто звонил по номеру телефона, даже если номер был скрыт. Поиск номера через поисковые сервисы – один из самых доступных способов определения звонка с незнакомого номера. На эту процедуру затрачивается несколько минут, одной проверки бывает достаточно, чтобы опознать входящий номер. Чтобы эффективно пробить номер телефона в «Google» или «Yadex», его рекомендуется вводить в разных форматах, например 79xxxxxxxxx, 8 (9xx) xxx-xx-xx, 79xxxxxxxxx, +7 (9xx) xxx-xx-xx. Определенный формат номера можно обнаружить на различных сайтах, включая те, на которых хранятся сведения о физических лицах в открытом доступе. Эффективным способом определения подозрительных номеров является их проверка через специальные бесплатные сервисы, например: neberitrubku.ru,кто-звонит.рф, zvonkoff.net, zvonili.com. [22, с. 69]

На этих сайтах происходит подборка таких номеров и размещаются отзывы граждан о них, которые часто делятся подробными комментариями о таких номерах, в том числе предупреждают о мошенниках. После запроса становится понятно, важен ли был звонок, либо это были мошенники.

Проверка номеров через популярныемессенджерыViber и WhatsApp, в которых зарегистрировано большинство абонентов сотовых операторов. Однако не всем известно, что Viber и WhatsApp свободно раскрывают

некоторые сведения о своих пользователях. Для того, чтобы «пробить» номер по одному из мессенджеров, достаточно начать добавлять его в контакты. Практически сразу можно узнать имя того, кто звонил вам со скрытого номера и получить его фотографию.

Проверка номера через «Сбербанк Онлайн» позволяет узнать имя и отчество человека, которому принадлежит неизвестный номер. Если номер не зарегистрирован в Viber и WhatsApp, для его проверки через сервис «Сбербанк Онлайн» необходимо начать выполнение процедуры перевода по номеру телефона. Можно указать в качестве суммы перевода 1 рубль и нажать «Продолжить». Этот рубль не будет снят со счета до подтверждения, выполнять которое не потребуется. После нажатия кнопки «Продолжить» нужно перейти в меню подтверждения оплаты, где будут указаны имя и отчество получателя. Определение звонков по «Avito» и «Юле» через доску объявлений – специальный сервис, в котором собирается база объявлений по номерам телефонов. Так можно установить имя абонента, где он живет, какие объявления он подавал на популярные доски объявлений. Иногда в тексте объявлений размещается дополнительная информация.

Определение звонков через приложения для iPhone и Android. Для iPhone и Android-смартфонов есть много приложений со встроенными определителями номеров. В базах таких приложений насчитываются тысячи номеров, по каждому из которых пользователю предоставляется дополнительная информация, в том числе предупреждения в случае, если номер принадлежит мошенникам.

Существуют приложения с определителями номеров, например, «Яндекс» (iOS, Android). Приложение полностью бесплатное, содержит огромную базу номеров и умеет выдавать полезные предупреждения, например, о мошенниках или рекламе. Для оценки незнакомого номера «Яндекс» использует собственную базу «Яндекс.Справочника», отзывы пользователей приложения [18, с. 112].

Механизмы приложения оценивают частоту звонков с номеров, продолжительность разговоров и другие параметры. Все это позволяет приложению выдавать максимально точные рекомендации даже по незнакомым номерам, которых нет в базе. Определитель номеров от «Лаборатории Касперского» – KasperskyWhoCalls (iOS, Android). В приложении огромная база номеров, которая пополняется еженедельно. Вся база хранится прямо на смартфоне пользователя. За счет этого определение номера выполняется и при отсутствии подключения мобильного устройства к Интернету. Приложение может блокировать звонки от мошенников и других нежелательных лиц еще до появления вызова. Пользователь может просмотреть заблокированные подозрительные звонки. Достаточное количество, о них необходимо доводить информацию до граждан. И, разумеется, своевременно сообщать о фактах мошенничества в правоохранительные органы.

3.3 Перспективы развития направлений профилактики мошенничества с использованием банковских карт и интернет ресурсов

За последние несколько лет большое внимание уделялось вопросу безопасности и конфиденциальности. Стоит отметить, что цифровой прогресс работает в обе стороны: совершенствуются как законные способы и методы развития, так и модернизируется преступное общество.

В условиях современной реальности очевидно, что вычислять поддельные сайты с каждым днем становится все сложнее, их адреса все больше похоже на подлинные, при этом в некоторых случаях они находят контакт даже с защищенным соединением HTTPS, а если говорить о использовании сайтов через мобильные устройства, то здесь риск столкнуться с фишинговым сайтов еще больше увеличивается ввиду технических особенностей смартфонов. Компании и банки стараются

бороться с действиями злоумышленников [10, с. 96].

Конечно, при работе с сайтами в корпоративной среде риск столкнуться с фишингом крайне невелик, ввиду ограничения нецелевого использования, а также применения различных встроенных инструментов в используемый браузер. Однако такие меры являются базовыми и в редких случаях гарантируют безопасность персональных данных. Очевидно, что необходимо прибегать к использованию внешних ресурсов, применять комплексный подход, который будет включать в себя комбинацию действий: от технических инструментов, до проведения организационных мероприятий по защите сайтов.

В рамках противодействия преступности в рассматриваемой области, а также осуществления надзора за реализацией нацпроекта «Цифровая экономика» в Генеральной прокуратуре Российской Федерации создан отдел по надзору за исполнением законодательства в ИТ-сфере.

Анализ статистических данных показал, что наиболее частым фишинговым атакам подвергаются официальные сайты Пенсионного фонда и Фонда социального страхования. Данный факт обусловлен тем, что указанные сайты работали без соблюдения условий безопасности, в частности, установлено отсутствие нормативных правовых актов, позволяющих определять актуальные угрозы безопасности данных [26, с. 103].

Очевидно, что такие фишинговые сайты имеют огромные возможности по получению личных данных граждан Российской Федерации и борьба с их созданием и использованием должна вестись на достаточно серьезном уровне.

Крайне актуально здесь применять все возможные меры профилактики, предупреждение этих деяний должно стать первостепенной задачей, в этой связи созданный специальный отдел по надзору за исполнением законодательства в ИТ-сфере станет одной из мер по контролю за

внедрением искусственного интеллекта, целью которого является обеспечение защиты и хранения информации.

Еще одной мерой по борьбе с фишинговыми сайтами стало предложение Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, которое заключается в объединении Единого портала государственных и муниципальных услуг с государственной биометрической системой, что позволит также повысить безопасность пользователей сайтов государственных органов. По словам ведомства, биометрия является наилучшей защитной системой в данном случае.

Кроме того, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации в настоящее время занимается созданием единой системы по борьбе с кибератаками, которая будет включать в себя возможности поиска фишинговых сайтов, а также функции автоматизированной обработки на признаки мошенничества в сфере ИКТ, поиск мер по блокировки вредоносных программ, сайтов и т.д. [14, с. 96].

Кроме того, регулярными проверками занимается и Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор), направленными на защиту и обработку персональных данных. Многообразие фишинговых атак показывает, что существует огромное число средств, позволяющих получить от пользователя сети Интернет любую конфиденциальную информацию.

Безусловно, чем больше технологически развита страна, чем больше используются современные инфокоммуникационные технологии — тем выше риск, а, соответственно, меры безопасности должны работать на опережение. Современная преступность, являясь неотъемлемой частью общественных отношений, все больше приобретает характерные черты высокотехнологического процесса.

В этой связи трудно не согласиться с высказыванием О.П. Грибунова,

который отметил, что в настоящее время без современных технологий процесс противодействия противоправным деяниям уже практически невозможен.

Очевидно, что противодействие фишинговым атакам должно проводится на всех уровнях, здесь должна вестись совместная работа организаций, различных государственных структур, правоохранительных органов, граждан.

Борьбу с данным видом мошенничества можно осуществлять только с применением комплексного подхода. Однако, очевидно, что защита своих персональных данных во многом зависит от пользователя, от его умения критически анализировать поток информации [35, с. 66].

Таким образом, здесь важны и меры профилактики, заключающиеся в информировании граждан о существующих угрозах и о мерах по защите своих персональных данных, и систематические проверки по соблюдению законодательства в сфере информационно-телекоммуникационных технологий.

В результате рассмотрения судебной практики мы пришли к выводу о том, что чаще всего фишинг неочевиден: неизвестны данные о конкретном лице, которое совершило преступление, известен лишь факт совершения преступления. Проведение оперативно-розыскных мероприятий и следственных действий при расследовании фишинга осложняется тем, что часть получаемых при их производстве данных добывается из источников виртуальной информации (компьютер потерпевшего или преступника, удаленный локальный сервер, сеть Интернет и т.д.).

Исходя из всего вышесказанного, можно сделать вывод о том, что проблема фишинга на сегодняшний день особенно актуальна в современном Российском киберпространстве. Не существует универсального средства борьбы с фишингом. Злоумышленники постоянно увеличивают свой арсенал и находят новые способы обхода технических средств защиты. Однако

специалисты информационной безопасности продолжают создавать новое программное обеспечение, чтобы снизить шанс успешного проведения атаки. Помимо этого, сейчас также идет активная борьба со злоумышленниками на законодательном уровне. Однако уровень квалификации и опыт следственных органов в расследовании подобных преступлений пока остается на невысоком уровне.

Следовательно, государству необходимо обеспечить правоохранительные органы наиболее современными техническими средствами, программным обеспечением, высококвалифицированными специалистами для успешной борьбы с новыми вызовами в киберпространстве в условиях цифровой экономики.

Подводя итог, хочется отметить, что борьба с преступностью играет важную роль в формировании и поддержании устойчивого правового государства. Соблюдение должного уровня правопорядка и законности – одна из приоритетных задач современного общества.

К проблемам профилактики мошенничества с использованием банковских карт и интернет ресурсов, выявленным в работе, относятся: пробелы в законодательстве, посвященном профилактике мошенничества; некомпетентность и «халатность» как сотрудников банков, так и банков в целом; технические проблемы (сбои в оборудовании); внешнее воздействие (атаки, взломы), что обусловлено внешнеполитическими отношениями.

Анализ преступности показал, что информационно-телекоммуникационные технологии постепенно становятся неотъемлемой частью практически любой сферы деятельности, что напрямую ставит вопрос о необходимости повышения роли информационной безопасности. При этом такой вид преступной деятельности является крайне специфичным, и положительный исход по делу во многом зависит от качества проведения предварительного следствия.

Обеспечение безопасности в сфере информационного поля, пространства, информационных ресурсов и информационных систем в настоящее время является одной из приоритетных задач, эти вопросы представляют собой крайне актуальную область исследования и требуют постоянного развития и совершенствования.

Заключение

Профилактика мошенничества с использованием банковских карт и интернет ресурсов во многом зависит от того, насколько известен способ его совершения.

Основными способами мошенничества с картами, рассмотренными в работе, выступают: скимминг; бесконтактная кража; снифферинг; фишинг; социальная инженерия; кардинг.

Изучение уголовных дел показало, что современные способы совершения мошенничества в отношении физических лиц являются полноструктурными, так как мошенники тщательно готовятся к совершению преступления и предпринимают необходимые действия по его сокрытию.

Непосредственный анализ динамики уровня исследуемых мошенничеств за последние пять лет (2016–2020 гг.) в РФ в целом свидетельствует о неуклонном его росте. Так, за изучаемый период абсолютное количество мошенничеств увеличилось в 3,7 раза: с 8 718 преступлений, зарегистрированных в 2016 г., до 32 186 в 2020 г. Эту же тенденцию подтверждают и относительные показатели.

Вместе с тем территориально по стране мошенничества данного вида распределены неравномерно. По совокупным абсолютным показателям мошенничеств в банковской сфере, зарегистрированных в период 2016–2019 гг., лидируют Приволжский и Центральный федеральные округа (ПФО, ЦФО), что имеет логичное объяснение, поскольку на указанной территории проживает большая часть населения РФ, здесь находится наиболее развитая сеть банковских учреждений. Соответственно, в федеральных округах с невысокой численностью населения, где огромные территории вообще не заселены, рассматриваемых преступлений было зарегистрировано в несколько раз меньше.

К проблемам профилактики мошенничества с использованием

банковских карт и интернет ресурсов, выявленным в работе, относятся: пробелы в законодательстве, посвященном профилактике мошенничества; некомпетентность и «халатность» как сотрудников банков, так и банков в целом; технические проблемы (сбои в оборудовании); внешнее воздействие (атаки, взломы), что обусловлено внешнеполитическими отношениями.

В рамках противодействия преступности в рассматриваемой области, а также осуществления надзора за реализацией нацпроекта «Цифровая экономика» в Генеральной прокуратуре Российской Федерации создан отдел по надзору за исполнением законодательства в ИТ-сфере.Еще одной мерой по борьбе с фишинговыми сайтами стало предложение Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, которое заключается в объединении Единого портала государственных и муниципальных услуг с государственной биометрической системой, что позволит также повысить безопасность пользователей сайтов государственных органов.

Противодействие мошенничества должно проводиться на всех уровнях, здесь должна вестись совместная работа организаций, различных государственных структур, правоохранительных органов, граждан.

Борьбу с данным видом мошенничества можно осуществлять только с применением комплексного подхода. Однако, очевидно, что защита своих персональных данных во многом зависит от пользователя, от его умения критически анализировать поток информации.

Библиографический список

1. Уголовный кодекс Российской Федерации» от 13.06.1996 N63-ФЗ (ред. от 28.01.2022 N3-ФЗ) // Российская газета от 31 января 2022г. N202.

2. Федеральный закон от 28.12.2009 N381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации» (ред. от 02.07.2021) // Собрание законодательства Российской Федерации от 5 июля 2021г. N27 (часть I) ст. 51823. 7.

3. Федеральный закон от 27.07.2006 N152-ФЗ «О персональных данных» (ред. от 02.07.2021) // Собрание законодательства Российской Федерации от 5 июля 2021г. N27 (часть I) ст. 5159. 8.

4. Федеральный закон от 07.07.2003 N126-ФЗ «О связи» (ред. от 30.12.2021) // Собрание законодательства Российской Федерации от 3 января 2022г. N1 (часть I) ст. 34.

5. Абалтарав Э.Г. Проблемы безопасности бесконтактных платежей // Угрозы и риски финансовой безопасности в контексте цифровой трансформации. 2021. С. 546–551.

6. Анненкова Е.А. Использование банковских карт: вызовы и современность // Цифровизация экономики России: институты, механизмы, процессы. Яшин Н.С., Устинова Н.Г., Тучина Н.А., Орехова Е.А. и др. Коллективная монография. Саратов, 2019. С. 147–159.

7. Ахметов А.А.Защита банковских карт от мошенничества // Современные вопросы естествознания и экономики. 2022. С. 32-34.

8. Балашев Н.Б., Александрова А.С., Барабанова Ю.С.Проблемы рынка банковских карт // Вестник Тульского филиала Финуниверситета. 2022. № 1. С. 16-18.

9. Балашев Н.Б., Пономарев Д.В. Динамика развития электронных платежных технологий в РФ. Международный журнал гуманитарных и естественных наук. 2019. № 11-3. С. 119-123.

10. Балашев Н.Б., Суслова О.А. Бесконтактные платежи и их использование в России и Европе. Вестник Тульского филиала Финуниверситета. 2019. № 1-2. С. 19-21.

11. Балашова О.Б., Балашев Н.Б. Сущность и виды банковских карт. Вестник Тульского филиала Финуниверситета. Демидовские чтения: экономика и образование. Тула: Издательство ТулГУ, 2018. № 1, С. 27-30.

12. Бжахов Г.М.Об актуальных вопросах, возникающих при раскрытии дистанционных мошенничеств и краж с банковских карт // Пробелы в российском законодательстве. 2022. № 4. С. 39-43.

13. Бойцова Е.В., Мамонова В.В., Пупкова В.И., Шелкоплясова Н.И.Мошенничество в сети "интернет" // Академическая публицистика. 2022. № 5-2. С. 183-187.

14. Бородкина Т. Н., Лавлюк А. В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. 2018. № 1. С. 135—13

15. Быть О.Ю. Эффективность мер предупреждения преступлений в сети Интернет // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 2 (48). С. . DOI

16. Грачев С. А. Проверка сообщений о мошенничестве в сети интернет и принятие решения о возбуждении уголовного дела / С. А. Грачев, А. С. Крюкова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2022. – № 2(91). – С. 164-171.

17. Гурьянов К.В. Современные риски бесконтактных платежей с использованием RFIDтехнологий // Базис. 2019. № 1 (5). С. 50–63.

18. Давыдов В.В. Анализ метода биометрической аутентификации для системы Paypass // Региональная информатика и информационная безопасность. 2017. С. 402–406.

19. Емельянов Д.А.Предупреждение мошенничества в сети интернет // Право и законность: вопросы теории и практики.сборник материалов XII

Всероссийской научно-практической конференции. Абакан, 2022. С. 87-88.

20. Кабалина К.С. Мошенничество с использованием банковских карт: основные способы совершения и методы противодействия // Научно-педагогические чтения 101 молодых ученых имени профессора С.В. Познышева. 2020. С. 26–31.

21. Кецко К.В. Преступность в сфере электронной коммерции // Российский следователь. 2021. N9. С. 58–63. 2.

22. Лебедева И.А., Пантелеева А.О. Актуальные вопросы совершенствования мер безопасности при проведении операций с использованием банковских карт // Технологическая перспектива в рамках евразийского пространства: новые рынки и точки экономического роста. 2018. С. 417–422.

23. Леваков А.К. Телефонное мошенничество: трудности противодействия // Вестник связи. 2020. № 12. С. 15-16.

24. Леун, Е. В. Совершенствование банковских карт и технических средств, работающих с ними, для повышения информационной безопасности финансовых операций / Е. В. Леун, Т. Н. Гупалова, С. Е. Пчелкин // Социально-экономические проблемы и перспективы развития трудовых отношений в инновационной экономике. 2022. – С. 95-102.

25. Миляев Г.А., Дворянкин О.А.Методы борьбы с мошенничеством банковских карт в информационной сфере органами внутренних дел // Правопорядок в России: проблемы совершенствования. 2022. С. 79-82.

26. Молдалиева К.З.Современные технологии развития банковского сектора // Реформа. 2022. № 1 (93). С. 53-58.

27. Попова А.А. Незаконные способы снятия денежных средств со счета платежной карты владельца // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2020. № 2 (54). С. 86–89.

28. Путанова О.А. Современные виды мошеннических действий и

способы борьбы с ними на рынке безналичных платежей Российской Федерации // Инновационная деятельность. 2019. № 4 (51). С. 100–108.

29. Рекунова Л.Д.Социальное проектирование в сфере мошеннических действий в интернет пространстве // Исторические, философские, методологические проблемы современной науки. 2022. С. 415-420.

30. Репецкая А.Л., Петрякова Л.А.Криминологический анализ современного состояния мошенничеств в банковской сфере России // Вестник Омского университета. Серия: Право. 2022. № 1. С. 62-72.

31. Решняк О. А., Ковалев С. А. Организация расследования мошенничеств, совершенных с использованием сети «Интернет», на первоначальном и последующем этапах // Вестник Волгоградской академии МВД России. 2020. № 2 (53). С. 106—111.

32. Савинова Е.А., Жевора В.В.Технические способы мошенничества с банковскими картами и направлениях повышения безопасности расчетов // Цифровой регион: опыт, компетенции, проекты. 2021. С.537-540.

33. Сапрыкина А.С.Применение искусственного интеллекта для обнаружения мошенничества с банковскими картами и платежами // Международная студенческая научно-техническая конференция. 2022. С. 415-416.

34. Семенова, Н. А. Запрет анонимности в сети интернет как мера профилактики мошенничества / Н. А. Семенова // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. – 2022. – № 4. – С. 206-210.

35. Смагоринский Б. П., Сычева А. В. О некоторых актуальных способах совершения мошенничества в отношении физических лиц в современных условиях // Вестник Волгоградской академии МВД России. 2022. № 2 (61). С. 172—178.

36. Смирнов Д.Ю. Комплексный подход к формированию защиты

денежных средств на банковских картах физических лиц // Проблемы и пути социально- экономического развития: город, регион, страна, мир. 2020. С. 105–109.

37. Сорокина Е.А.Цифровая грамотность как способ защиты от интернет-мошенничества // Инновации. Наука. Образование. 2022. № 50. С. 852-856.

38. Сычева А. В. Некоторые способы совершения «дистанционного» мошенничества // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 167—173.

39. Уваров А.А. Проблемы использования цифровых технологий при реализации прав и свобод граждан // Право и цифровая экономика. 2020. N2. С. 5–11. 3.

40. Шуваева М.С.Особенности организации расследования и предупреждения некоторых видов интернет-мошенничеств // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства. 2022. С. 328-332.

41. Статистика преступности. URL: http://epp.genproc. gov.ru/ (дата обращения: 18.10.2022).

42. За 2021 г. мошенники похитили у россиян 45 млрд руб. URL: http://pravo.ru/ (дата обращения: 18.10.2022).

43. Эксперты рассказали о новых схемах мошенничества в России. URL: http://iz.ru/ (дата обращения: 1810.2022).