К вопросу о мошенничестве с банковскими картами и методам борьбы с ними

On the issue of banking card fraud and its control

Сочнева Е.Н.
Канд. экон. наук, доцент, доцент кафедры судебных экспертиз Юридического института, ФГБОУ ВО «Красноярского государственного аграрного университета», г. Красноярск
e-mail: Sochneva.e@inbox.ru

Sochneva E.N.
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Forensic Examinations, Law Institute, Krasnoyarsk State Agrarian University, Krasnoyarsk
e-mail: Sochneva.e@inbox.ru

Четвериков Я.Д.
Студент Юридического института, ФГБОУ ВО «Красноярского государственного аграрного университета», г. Красноярск

Chetverikov Ya.D.
Student of the Law Institute, Krasnoyarsk State Agrarian University, Krasnoyarsk

Аннотация
Статья посвящена вопросам совершенствования методов борьбы с банковским мошенничеством. Актуальность темы связана с возросшим числом банковских мошенничеств за 2024 год, и новыми законодательными инициативами, принятыми весной 2025 г. В работе систематизированы подходы к совершению преступлений в банковской сфере, в частности, выделены: преступления, совершаемые с использованием социальной инженерии, кибермошенничество и мошенничество с банковскими картами и банкоматами. По каждой группе охарактеризованы основные способы совершения преступлений, проанализировано нормативно-правовое регулирование и законодательные инициативы, а, затем, предложены подходы к их пресечению. При формулировании предложений учтены психологические аспекты совершения преступлений и недоработки законодательства, в том числе, вступающего в силу. Статья будет интересна для тех, кто исследует современные методы защиты от банковского мошенничества, а также для тех, кто формирует государственную политику в этой сфере.
Ключевые слова: мошенничество в банковской сфере, социальная инженерия, кибермошенничество, мошенничество с банковскими картами и банкоматами, методы борьбы с мошенничеством.

Abstract
The article is devoted to the issues of improving methods of combating banking fraud. The relevance of the topic is related to the increased number of banking frauds in 2024, and new legislative initiatives adopted in the spring of 2025. The paper systematizes approaches to the commission of crimes in the banking sector, in particular, it highlights: crimes committed using social engineering, cyberbullying and fraud with bank cards and ATMs. For each group, the main methods of committing crimes are characterized, regulatory and legal regulation and legislative initiatives are analyzed, and then approaches to their suppression are proposed. When formulating proposals, the psychological aspects of the commission of crimes and the shortcomings of legislation, including the legislation that

is coming into force, are taken into account. This article will be of interest to those who study modern methods of protecting against banking fraud, as well as to those who form public policy in this area.
Keywords: fraud in the banking sector, social engineering, cyber fraud, fraud with bank cards and ATMs, anti-fraud methods.

Введение

Мошенничество в банковском секторе экономики прошло долгий путь развития, от древних цивилизаций, где зарождались первые формы финансовых операций, а, значит, и экономики, в целом, и одновременно с ними и методы экономического обмана.

Еще в Древнем мире мошенники использовали различные схемы для обмана, как государства, так и обычных граждан. Например, в Древнем Риме широко практиковалась фальсификация монет, когда недобросовестные монетные дворы подмешивали дешевые металлы в золотые и серебряные деньги. Это подрывало доверие к валюте и вызывало инфляцию, тем самым, обесценивая труд населения Рима.

Существующая же система, которая существует сейчас, начала развиваться примерно в XIV в., на севере Италии. Ярким примером выступает до сих пор существующий банк Монте де Паски ди Сиена, существующий с 1472 г., и он считается старейшим банком в мире. Он пережил не мало экономических и политических кризисов, однако существует и поныне [1].

Примером задокументированного мошенничества в банковском секторе, можно упомянуть случай, произошедший в XVIII в., так одним из крупнейших финансовых мошенников, стал Джон Ло, который в 1716 г. создал «Banque Générale» во Франции. Его «Миссисипская схема», которую сегодня бы окрестили «Финансовой пирамидой», была одной из первых спекулятивных афер в истории банковского дела, что привело к финансовому коллапсу и массовому обнищанию населения Франции [2].

Таким образом, мошенничество в банковском секторе экономики было всегда, просто с развитием технологий и введением средств зашиты, появлялись новые идеи для маневров мошенников. Если раньше жертвами действий мошенников были отдельные, как частные, так и государственные экономические системы, то сегодня с развитием технологий быстрой передачи информации и обработки данных, их удары стали более точечными и избирательными.

Вопросы мошеннических действий в банковской сфере и методов борьбы с ними поднимаются в работах многих авторов.

Социально-психологическими причинами мошенничества занимались такие авторы, как О.Е. Беркових, Е.Б. Матрешина, И.И. Павлова и др. [3]. Они дают обширный анализ типов мошенничеств, их динамики, мотивов, способов совершения и характеристик жертв. Также, авторы рассматривают влияние развитие цифровых технологий на увеличение финансовых махинаций.

Многие авторы пишут о способах и методах предотвращения мошенничеств, например, О.Ю. Ермоловская, Е.С. Яковенко и др. [4;5;6].

Однако, несмотря на такой интерес к указанной проблематике, интерес к теме мошенничества в банковской сфере не угасает в связи с тем, что формы и методы его осуществления постоянно трансформируются.

На основании вышеизложенного целью работы является анализ существующих методов современного электронного мошенничества в банковской сфере и предложение подходов по борьбе с ними.

Основная часть

В современной России банковское мошенничество остаётся одной из наиболее острых проблем финансовой безопасности. Достаточно взглянуть на статистику Центрального Банка, чтобы увидеть остроту проблемы. В 2024 г. произошел резкий скачок увеличения количества похищенных денежных средств.

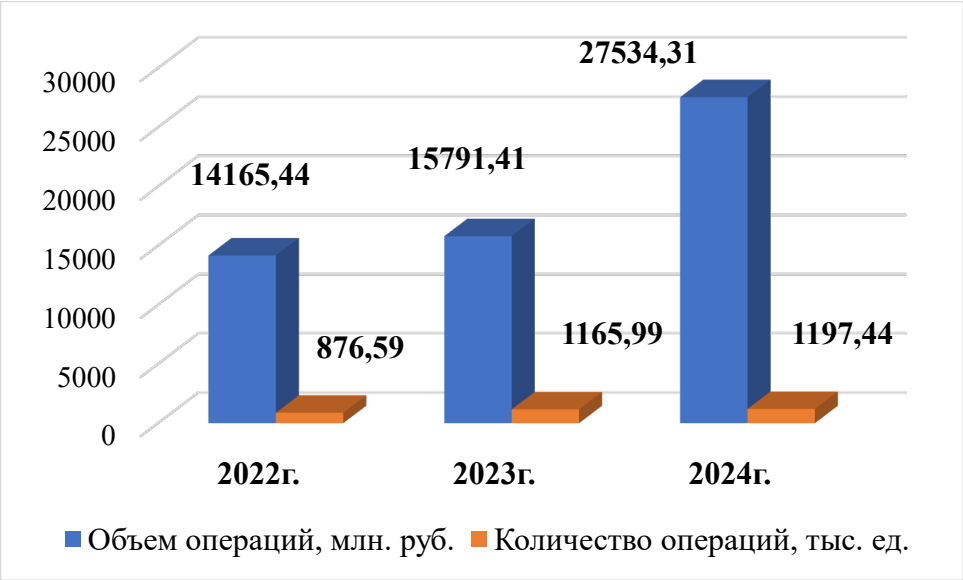

Рис. 1. Динамика общего объема количества операций без согласия клиентов [7]

Для анализа проблемы целесообразно выделить методики, которые используют мошенники и, в соответствии с их особенностями, разработать способы борьбы с ними.

Для удобства исследования все мошеннические схемы сгруппированы в три группы.

1) Социальная инженерия — методы, основанные на психологическом воздействии на жертву с целью получения конфиденциальной информации (например, паролей, кодов подтверждения, данных банковских карт и т.п.). Это направление приобретает всё большую значимость в условиях цифровизации, когда контакт между клиентом и банком часто осуществляется удалённо.

2) Кибермошенничество — сюда входят методы, реализуемые с помощью вредоносного программного обеспечения, фишинговых сайтов, взлома баз данных и других IT-инструментов. Учитывая рост объёма онлайн-операций и электронной коммерции, данная категория остаётся ключевой угрозой в финансовом секторе.

3) Мошенничество с банковскими картами и банкоматами — включает в себя клонирование карт, скимминг, установка фальшивых банкоматов или устройств съёма данных. Несмотря на то, что этот вид мошенничества уступает по масштабам киберпреступлениям, он по-прежнему остаётся актуальным, особенно в регионах с недостаточной защищённостью оборудования.

Выбор этих трёх категорий обусловлен как их актуальностью, так и различиями в механизмах реализации преступлений и способах противодействия им. Такой подход позволяет не только систематизировать существующие угрозы, но и предложить дифференцированные меры по борьбе с каждым из типов мошенничества.

В качестве первой группы по способам совершения преступлений в области электронной коммерции отнесем «социальную инженерию».

В основе социальной инженерии лежит использование психологических уязвимостей, таких как доверие, страх, спешка и любопытство. В любом случае это метод манипуляции людьми с целью получить конфиденциальную информацию (пароли, логины, банковские данные и пр.), или заставить жертву выполнить определённые действия (например, открыть вредоносную ссылку или передать доступ к системе).

Рассмотрим, какие методы социальной инженерии существуют и как с ними можно бороться:

1) Фишинг – подразумевает собой создание подложных писем, ссылок, сообщений, с целью передачи личных данных мошеннику.

2) Претекстинг – метод, при котором мошенник манипулирует жертвой, с целью выдачи себя за того, кто пользуется наибольшим доверием жертвы, с целью получения данных, денежных средств и других интересующих мошенника данных.

3) Метод «услуга за услугу» – мошенник предлагает вознаграждение, за выполнение определенной, поставленной мошенником задачи, с целью войти в доверие к жертве.

Главная проблема в борьбе с преступлением в данной группе заключается в том, что мошенники чаще всего атакуют самые незащищённые слои населения, которые больше всего доверяют непроверенной или незнакомой им информацией. Так мошенники, пользуясь этим, часто представляются сотрудниками государственных органов, знакомыми близких родственников, разыгрывая выдуманные сцены с целью вхождения в доверие к жертве, чтобы вынудить её передать конфиденциальную информацию, перевести деньги или предоставить доступ к важным ресурсам.

И, именно, на данную группу преступлений сейчас в большей мере нацелено нормотворчество в РФ. В текущем году был принят ряд нормативно-правовых актов, что должны усложнить работу мошенников и защитить наиболее незащищённые слои населения.

В частности, были приняты следующие меры:

1) Ограничения на количество сим-карт у физических лиц. С 1 апреля 2025 г. гражданам РФ запрещено иметь более 20 абонентских номеров (сим-карт) [8]. Такая мера направлена на борьбу с мошенническими схемами, связанными с массовым использованием анонимных сим-карт для звонков и рассылок фишинговых сообщений.

2) Принятие пакета документов, направленного на противодействие телефонным мошенникам. В марте 2025 г. был принят законопроект, под № 842276-8 «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [9]. Он предусматривает целый ряд новшеств.

Во-первых, со вступлением в силу этого ФЗ с поправками, появится возможность онлайн-обмена информацией между государственными органами, банками и операторами связи, для быстрого реагирования, связанного с выявлением и блокировкой подозрительной транзакции. Также будет разрешен доступ органов, ведущих оперативно-розыскную деятельность к информационным системам операторов связи для быстрого реагирования и расследования преступления.

Во-вторых, в целях борьбы с телефонным мошенничеством стала обязательной маркировка звонков, отображающая на экране телефона наименование организации, совершающей вызов, что позволяет гражданам быстрее ориентироваться в подлинности входящих контактов.

В-третьих, введён запрет на информирование граждан через мессенджеры для сотрудников государственных органов, банков, операторов связи, маркетплейсов и сервисов по поиску работы, что минимизирует возможность фальсификации сообщений.

В-четвертых, важным шагом в защите прав граждан стало прекращение массовых вызовов и спам-звонков при подаче абонентом оператору связи официального отказа от их получения.

В-пятых, заключение договоров на обслуживание радиотелефонной связи теперь будет возможно только при личном участии абонента, либо посредством портала государственных услуг.

В-пятых, будет введено ограничение на выдачу наличных средств в размере до 50 000 руб. в течение 48 часов, если банк фиксирует признаки незаконного снятия денег без добровольного согласия владельца. Для дополнительной защиты предусмотрена возможность назначения уполномоченного лица, который подтверждает выполнение операций по переводу денежных средств. Граждане теперь смогут самостоятельно назначать доверенных лиц, которые, в случае необходимости, будут подтверждать, что перевод денежных средств идет по воле владельца счета.

Как мы видим, социальная инженерия остаётся мощным инструментом мошенников, использующих психологические слабости людей. Однако, благодаря новым законодательным инициативам, государство стремится минимизировать количество таких атак, тем самым

ограничивая действия злоумышленников. Совместно с активной пропагандой по выработке недоверия к неизвестным номерам телефонов, а также активным введением определителя номера от разных организаций, в том числе от банков, как например секретарь «Олег» от Т-Банка, создаются новые барьеры на пути мошенников.

Эти технологии позволяют не только оперативно выявлять подозрительные звонки, но и предупреждать граждан о возможной угрозе. Подобные меры, в сочетании с повышением цифровой грамотности населения, формируют комплексный подход к борьбе с социальной инженерией, что в долгосрочной перспективе способствует снижению числа успешных мошеннических атак.

Считаем целесообразным дополнить существующие методы борьбы с мошенниками, использующими факторы социальной инженерии, следующими методами:

1) Отложенное исполнение денежных переводов с возможностью аннулирования.

Так как злоумышленники этого раздела используют социальные факторы, действуя внезапно, чтобы напугать свою жертву и заставить делать какие-либо действия, то с введением «отложенной обработки денежных переводов» для физлиц, не имеющих активной истории переводов крупными суммами со сроком исполнения в несколько часов. В таком случае у жертвы будет время, в течении которого человек может осознать случившиеся и отменить перевод через мобильное приложение или банк.

2) Введение обязательной «цифровой паузы» перед высокорисковыми действиями.

Так, с недавнего времени, на портале «Госуслуги» можно установить запрет на получение кредитов [10]. Считаем целесообразным сделать подобную меру и в мобильных приложениях банков, в виде механизма «пауза безопасности». Это должна быть не постоянная мера, а временная, так как многие пользуются кредитной картой для частых покупок, и, введя такую меру, они обезопасят свои активы, но при этом смогут пользоваться картой. Сам же механизм будет работать так: перед оформлением кредита или выдачей доверенности клиенту будет предлагаться подождать 30 мин. и ознакомиться с предупреждением о возможных методах воздействия на них сценариев «социальной инженерии».

В качестве второй группы в части подходов к совершению преступлений было выделено кибермошенничество.

Технологический прогресс, который принес в повседневную жизнь много благ, начиная от просмотра интересующего нас фильма до возможности заказать какой-либо товар, и все это, не выходя из дома. Также, появилось много удобных приложений, что помогают людям в повседневной жизни. Однако, необходимо отметить, что при установке и регистрации в этих приложениях, человек дает согласие на «передачу и обработку персональных данных», так как сайты собирают персональную информацию «Cookie file».

Все это представляет собой сбор и обработку информации о пользователе. К таким могут относиться интересы человека, потребности и примерные финансовые возможности. Таким образом, владелицы сайтов могут понимать свой контингент, и предлагать таргетированную рекламу, в которой будет заинтересован конкретный пользователь.

Рассмотрим, какие ситуации могут возникнуть в таких случаях:

1) Существует вероятность взлома базы данных компании, что отвечает за хранение персональных данных пользователей.
2) Создание сайтов/приложений - «зеркал» популярных сайтов, что выглядят также, но это может ввести пользователя в заблуждение. И мошенники получают возможность похитить данные пользователя, который вводит их самостоятельно.
3) Межсайтовый скриминг – внедрение вредоносного кода, с целью похищения данных на устройстве пользователя при открытии ссылки, зараженной этим вредоносным кодом.
4) Фишинг – это распространение вредоносных приложений, в виде электронных, почтовых сообщений, где может, как содержатся вредоносный код, так и использование социальной инженерии, для убеждения пользователя в том, что ему за определенные действия полагается какая-либо награда.

Это небольшой список методик, которые используют мошенники в сети интернет для получения данных пользователя и дальнейшего их использования в мошеннических схемах.

Рассмотрим, как мошенники могут применить данные, и как можно решить эти проблемы.

В современной ситуации формат сертификатов сайтов в формате «SSL» перестали поддерживается в России. Они необходимы для шифрования данных между клиентским устройством и сервером. Министерство цифрового развития выступила осенью 2024, с инициативой создания своего формата сертификатов [11], но пока проблема остается открытой, а, это значит, что вероятность утечки данных может быть высокой.

Как нам кажется, в цифровой сфере это главные направления, на которые должен быть направлен взор законодателей и компетентных органов Российской Федерации. Сегодня пользователям приходится использовать двухфакторную аутентификацию (2FA), которая обеспечит безопасность от того, что данные и пороли могут попасть в руки мошенников.

Собирая информацию о пользователе, мошенники могут узнать о социальном и финансовом положении пользователя, тем самым создать определенный «цифровой образ пользователя», помимо этого в руки мошенников могут попасть пароли, «код-слово», необходимое для входа в банковскую систему, а также в сеть могут попасть документы. Тем самым, мошенники имеют много возможностей того, как они будут использовать полученные данные. Это может быть взятие кредитов на обманутых граждан, создание поддельных аккаунтов на различных биржах, для выведения незаконно полученных денежных средств.

По вопросам кибермошенничества можно уже говорить о сложившейся судебной практике. Например, в 2022 г. произошла массовая «утечка» данных граждан, которые пользовались сервисами «Яндекс Еда». Информация попала в сеть, и это привело к тому, что потенциальные мошенники получили базу данных, состоящую из: номеров телефонов, ФИО, домашних адресов, а также, возможно, данные дебетовых карт клиентов. За этот инцидент Московский суд назначил штраф в размере всего 60 тыс. руб. в соответствии с ч. 1 ст. 13.11 КоАП РФ [12]. И это не единичный случай, когда в сеть попадают данные граждан.

По оценке Сбербанка, на момент 06.11.2024 оценивалось, что данные в сети доступны о 90% населения России [13]. Это является показателем того, что компании не выполняют возложенные на них обязательства. При этом наказание идёт несоизмеримое. Чем чаше происходят утечки, тем свежее данные у мошенников и, единственное, что можно было бы предложить сделать — это увеличить размер ответственности для юридических и физических лиц. И даже это не гарантирует того, что компании избавятся от подобных утечек данных, но вполне может повлиять на их количество.

Далее рассмотрим, что можно сделать для уменьшения числа утечек персональных данных жителей нашей страны в сеть.

Предлагаем введение отдельной статьи в УК РФ за создание вредоносных сайтов и программ, имитирующих легальные ресурсы.

В настоящий момент такие действия могут квалифицироваться по общим статьям о мошенничестве или незаконном доступе к информации. Однако, специфики создания вредоносных фейковых сайтов в законе нет. Считаем целесообразным внести изменения в 28 главу Уголовного Кодекса Российской Федерации «Преступления в сфере компьютерной информации» посредством появления новой статьи, например, ст. 273.1 «Создание, распространение и эксплуатация фальшивых цифровых ресурсов с целью хищения данных» с санкцией до 4 лет лишения свободы. Эта статья будет работать за создание сайтов-двойников или фальшивых приложений, независимо от наступления последствий. Такое решение может служить фактором уменьшения количества создаваемых вредоносных сайтов на территории РФ.

Также, считаем необходимым внести изменения в Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ, сделав обязательным требованием для компаний условие об уведомлении пользователей о взломе или утечке данных. Кроме того, нужно увеличить

ответственность компаний за эти самые утечки данных пользователей. При введении таких мер, те, кто пользуются продукцией или приложением компании, будут в курсе о данном инциденте, и смогут принять необходимые меры безопасности.

Третьим подходом в группировке преступлений в электронной сфере выступает мошенничество с банковскими картами и банкоматами.

Этот тип мошенничества имеет особенность в виде физического взаимодействия мошенника с устройством банка или жертвы с целью получения необходимых ему данных.

Конкретные методы, здесь следующие:

1) Скимминг – это установка на банкомат специальных устройств (скиммеров), которые считывают данные карты с магнитной полосы. Часто злоумышленники также размещают скрытые камеры или накладные клавиатуры для кражи PIN-кода. Скопированные данные используются для создания дубликата карты и кражи средств со счета.

2) Картинг - мошенники покупают или похищают данные банковских карт в результате утечек информации, и используют их для покупок в интернете.

3) Кэш-треппинг - при этом методе мошенники устанавливают в банкомате специальные накладки, которые блокируют выдачу наличных. Клиент уходит, думая, что произошел сбой, а преступники затем извлекают застрявшие деньги.

4) Перехват SMS-кодов – взлом мобильных устройств или подмена SIM-карт для получения кода подтверждения банковской операции.

Для эффективной борьбы с такими преступлениями требуется комплексный подход, включающий не только технические меры защиты, но и совершенствование законодательства Российской Федерации.

Прежде всего, необходимо ужесточить уголовную ответственность за мошеннические действия, связанные с производством, распространением и использованием скиммингового оборудования, а также за незаконный оборот данных платежных карт. Кроме того, необходимо пресекать торговлю украденными данными в «даркнете». Под последним понимается часть интернета, которой пользуются люди, когда хотят быть анонимными и скрыть свое местоположение от посторонних или правоохранительных органов) [14]. Также, нужно усилить контроль за киберпреступностью.

На уровне банковской системы важно обязать кредитные организации внедрять современные технологии защиты, такие как антискимминговые устройства, биометрическую идентификацию клиентов и многофакторную аутентификацию для всех онлайн-операций. Также следует разработать механизм возврата денежных средств жертвам мошенничества, например, за счет арестованных средств преступников.

Также, считаем целесообразным предложить следующие действия, которые можно предпринять, для борьбы с данным типом мошенничества:

1) Запрет на перевыпуск SIM-карт без личного присутствия владельца и биометрическая идентификация пользователя, на чей номер привязан банковский счет.
2) Дополнительные меры должны быть направлены на контроль за работой мобильных операторов, поскольку мошенники часто используют подмену номеров и перехват SMS-кодов.
3) Ужесточение контроля за оборотом данных платежных карт.

Сегодня кража данных банковских карт (картинг) в большинстве случаев остается безнаказанной — преступники используют утечки, выкупают данные в даркнете, и совершают транзакции с подложными идентификаторами. В этом вопросе необходимо обратить внимание на зарубежный опыт.

Так, например, в Европейском союзе существует Общий регламент по защите данных (GDPR), который включает в себя требования к компаниям об обеспечении высокого уровня защиты персональных данных, включая данные платежных карт, а также предусматривает существенные штрафы (до 20 млн евро) за нарушение этих требований [15]. Наряду с этим, в рамках Второй платежной директивы (PSD2) установлены дополнительные меры

безопасности для платежных операций, такие как обязательное использование сильной аутентификации клиента [15]. Эти меры не только регулируют доступ к платежным данным, но и создают правовые и технические барьеры для их незаконного оборота.

Основываясь на данном примере, считаем целесообразным, внести изменения в законодательство, например, создав новую статью 159.8 УК РФ «Незаконное приобретение и использование данных платежных средств (даже без факта списания денежных средств)» с санкцией до 5 лет лишения свободы, что позволит пресекать преступные намерения на раннем этапе.

Заключение

Таким образом, по результатам исследования можно сформулировать следующие выводы.

1) В части социальной инженерии целесообразны методы борьбы с преступностью, приведенные ниже:

Во-первых, отложенное исполнение переводов с возможностью аннулирования. Данный механизм позволяет создать временной буфер между принятием решения и его реализацией. Это особенно актуально в ситуациях, когда жертва находится под психологическим давлением. Возможность отмены перевода в течение нескольких часов позволит человеку осознать ситуацию и предотвратить ущерб.

Во-вторых, введение обязательной «цифровой паузы» перед высокорисковыми действиями. Подобная мера может быть реализована в мобильных приложениях банков в виде «паузы безопасности». Перед оформлением кредита или совершением других, потенциально опасных, действий пользователю будет предложено подождать 30 мин., ознакомиться с предупреждением о рисках социальной инженерии и ещё раз подтвердить своё решение. Это снизит вероятность принятия импульсивных решений под давлением злоумышленников.

2) В части кибермошенничества целесообразно использовать такие следующие методы борьбы с преступностью:

Во-первых, введение отдельной статьи в Уголовный кодекс РФ за создание вредоносных сайтов и программ, имитирующих легальные ресурсы. На сегодняшний день подобные действия квалифицируются по общим нормам, что не учитывает всей специфики цифровых преступлений. Введение статьи, например, ст. 273.1 «Создание, распространение и эксплуатация фальшивых цифровых ресурсов с целью хищения данных» в гл. 28 УК РФ, позволило бы точнее классифицировать такие деяния и установить уголовную ответственность даже при отсутствии факта нанесённого ущерба. Это стало бы действенной мерой профилактики и сдерживания цифровых преступников.

Во-вторых, ужесточение регулирования в сфере защиты персональных данных. Необходимо внести изменения в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», обязав компании незамедлительно уведомлять пользователей о фактах взлома и утечки их персональных данных. Кроме того, следует повысить ответственность за допущенные утечки. Это не только повысит прозрачность, но и позволит гражданам своевременно принимать меры по защите своей цифровой идентичности, а также будет способствовать улучшению информационной безопасности со стороны компаний.

3) В части мошенничества с банковскими картами и банкоматами целесообразно использовать следующие методы борьбы с преступностью:

Во-первых, запрет на перевыпуск SIM-карт без личного присутствия владельца и внедрение биометрической идентификации. Учитывая, что одна из популярных схем мошенничества связана с подменой SIM-карт и перехватом SMS-кодов для входа в банковские приложения, необходимо ввести обязательное требование личного присутствия владельца при перевыпуске SIM-карты. Также следует предусмотреть биометрическую идентификацию при оформлении номеров, к которым привязаны банковские счета, что усложнит действия мошенников и повысит уровень безопасности.

Во-вторых, ужесточение контроля за оборотом личных данных платёжных карт. В настоящее время утечки данных банковских карт и их последующее использование в преступных целях зачастую не влекут за собой серьёзной ответственности. Необходимо ужесточить контроль за оборотом этих данных, включая мониторинг даркнета, а также усилить ответственность за распространение, покупку и использование краденых карточных данных.

В-третьих, внесение изменений в Уголовный кодекс РФ. Предлагается дополнить главу о мошенничестве новой статьёй — например, ст. 159.8 «Незаконное приобретение и использование данных платёжных средств». Такая норма позволит наказывать не только за совершённые кражи средств, но и за сам факт незаконного оборота данных карт, даже при отсутствии списания денег. Это обеспечит профилактику преступлений на более ранних стадиях и усилит защиту граждан.

Таким образом, мы видим, что для борьбы с мошенничеством требуются скоординированные действия государства, банковского сектора, мобильных операторов. Только комплексный подход, включающий строгий контроль, технологические нововведения и осведомленность граждан, позволит значительно сократить уровень финансовых преступлений и повысить доверие к банковской системе.

Литература

1. Беркович О.Е. Социально-психологические причины и способы совершения мошенничества в современном обществе / Беркович О.Е., Матрёшина Е. Б., Павлова И.И. (Криминология). Российский следователь. - 2024. - № 6. - С. 46-48.
2. В Сбербанке оценили долю утекших данных взрослых россиян в 90%. Официальный сайт журнала Forbs. Режим доступа: https://www.forbes.ru/tekhnologii/524629-v-sberbanke-ocenili-dolu-uteksih-dannyh-vzroslyh-rossian-v-90 (дата обращения: 22.04.2025г.).
3. Группа ВТБ. История повеления Банков. Режим доступа: https://www.vtb.ru /articles/finansovaya-gramotnost/kak-poyavlyalis-banki/ (дата обращения: 25.05.2025г.).
4. Государственный портал ГОСУСЛУГИ. Раздел «Как установить запрет на получение кредитов». Режим доступа: https://www.gosuslugi.ru/help/faq/rft/103816 (дата обращения: 16.05.2025г.).
5. Добрецов Г.Б. Цифровая хакупка. Рабочая тетрадь. Выпуск 1/2023. Красноярск, 2024.
6. Ермоловская О.Ю. Предотвращение мошеннических транзакций в финансовой сфере / О.Ю. Ермоловская // Экономическая безопасность. – 2025. – Т. 8, № 4.
7. Минцифры может поддержать использование отечественных SSL-сертификатов. Официальный сайт журнала «Сбер». Официальный сайт: https://sber.pro/publication/ mintsifri-mozhet-podderzhat-ispolzovanie-otechestvennih-ssl-sertifikatov/ (дата обращения: 17.04.2025г.).
8. 300 лет кризисов: как аферист и убийца довел Францию до голода. Официальный сайт газеты «Финмаркет». Режим доступа: https://www.finmarket.ru/finances/article/3633498 (дата обращения: 25.05.2025г.).
9. Официальный сайт ЦБ РФ. Режим доступа: https://cbr.ru/analytics// (дата обращения: 17.05.2025г.).
10. Проект Федерального закона N 842276-8 «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 15.02.2025); Режим доступа: https://www.consultant.ru /cons/cgi/online.cgi?req=doc&base=PRJ&n=257477#T9w2JhUgBJMgwfbo1.
11. Решение Московского Мирового Судьи, участка № 101, по делу № 5-413/2022. Режим доступа: https://mos-sud.ru/101/cases/admin/details/f6ffad43-95ae-4186-8d87-5e0ab277e669?respondent=Яндекс.Еда.

12. Регламент (ЕС) № 2016/679. Европейского парламента и Совета от 27 апреля 2016 года О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, отменяющий Директиву 95/46/ЕС (Общий регламент по защите данных) URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
13. Федеральный закон от 08.08.2024 N 303-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации» (пп. «г» п. 2 ст. 1).
14. Что такое Дакркент». Режим доступа: https://support.google.com/websearch/answer/ (дата обращения: 20.05.2025г.).
15. Яковенко Е.С. Решение графовых классификационных задач как инструмент обнаружения мошеннических банковских транзакций / Е.С. Яковенко, В.М. Сушков, П.Ю. Леонов // Информатизация в цифровой экономике. – 2024. – Т. 5, № 2. – С. 231-244.