



УДК 346.22

ПРАВОВЫЕ МЕХАНИЗМЫ БОРЬБЫ С МОШЕННИЧЕСТВОМ СИЛАМИ БАНКА**Абсатарова Виктория Олеговна**

4 курс, бакалавриат

Оренбургский институт (филиал) Московской государственной юридической академии

О.Е. Кутафина (МГЮА), г. Оренбург

Аннотация. В данной статье рассматриваются основные понятия мошенничества в банковской сфере, анализ противодействия банками мошенничеству, статистика мошенничества в банковской сфере, способы, которые, предлагают банки по борьбе с мошенничеством на примере двух банков Российской Федерации.

Ключевые слова: банк, мошенничество, банковская сфера

Под определение «мошенничество» попадают многие незаконные действия в самых различных сферах, в том числе и в сфере банковской деятельности. Практика преступной деятельности выработала много способов хищения, но наиболее распространенными видами мошенничества стали кредитные, с использованием банкоматов и с применением банковских карт.

Единого мнения о понятии мошенничества нет. Некоторые авторы под мошенничеством в банковской сфере понимают деяние, посягающее на законный порядок банковской или иной экономической деятельности и интересы в сфере банковского кредитования¹

Другие предлагают более широкое толкование мошенничества в банковской сфере, понимая под ним обманное обращение в собственность (владение) любого имущества или права на него; имущества, принадлежащего банку или иной кредитной организации: – совершенное с использованием банковских операций или документов; – совершенное с использованием своего служебного положения; – совершенное с использованием лжебанка или иной лжекредитной организации².

А. В. Бондарь полагает, что мошенничество в банковской сфере необходимо рассматривать в рамках, которые очерчены в Федеральном законе «О банках и банковской деятельности». Анализируя данный федеральный закон, можно определить объект мошенничества в банковской сфере, которым выступает право собственности конкретных

¹ Карпович О. Г. Понятие, признаки и виды финансового мошенничества // Юрид. мир. 2010. № 8. С. 39

² Эльзессер В. В. Борьба с мошенничеством в банковской сфере: Уголовно правовой и криминологический аспекты : авто реф. дис. ... канд. юрид. наук. СПб., 2005. С. 7.



банков и право собственности клиентов этих банков, которыми могут быть не только физические лица, но и юридические³

Как всем известно, граждане часто сталкиваются с проблемой звонков с неизвестных номеров, которые, как правило представляются различными сотрудниками. Ориентироваться кому звонить им не приходится, они набирают все номера подряд, если один сбросил или отказал в предоставлении своих банковских данных, то другой предоставит все, что нужно.

Статистика на сайте Сбербанка с 2018 года, показывает, что уже с 2019 года, стало на 68,5 % больше преступлений с использованием информационных технологий. На 130%, стало больше преступлений связанных с использованием банковских карт. На 91% с применением мобильных телефонов.

Банки, в первую очередь в целях предотвращения доверия к посторонним звонкам, информируют граждан.

В статье, будем анализировать, достаточно интересные термины, употребляемые на сайтах банков.

Помимо звонков в мире мошенничества существует еще один способ обмана граждан, так называемый спуфинг. Спуфинг- это подмена номера на телефоне, каких либо официальных учреждений или сотрудников органов.

Банки разрабатывают внутренние приемы борьбы с мошенничеством. Проведем сравнение нескольких банков и их сайтов Российской Федерации.

Сбербанк: если обратиться на его сайт, в раздел кибербезопасности частных клиентов , то можно увидеть раздел : «Ваша кибербезопасность» , в нем рассказывается:

- Куда пожаловаться на мошенников
- Как заблокировать спам и проверить подозрительный телефон
- Приёмы самозащиты от жуликов

Так же, Сбербанк, разработал приемы жалоб на мошенников: сообщение о мошенничестве ,проверка мошенника

Сервисы кибербезопасности в приложении СберБанк Онлайн

В разделе «Безопасность Сбербанк впустил всё, что поможет вам защитить себя от мошенников: сервисы проверки данных, настройки безопасности, обучающие статьи, видео и тесты.

Сбербанк, в том числе на сайте , создал раздел - кибрарий, т.е. библиотеку знаний о кибербезопасности. Там представлены статьи о том , как : « мошенники обманывают

³ Бондарь А. В. Мошенничество как вид преступного посягательства против собственности и особенности его проявления в сфере банковской деятельности: Уголовно правовой аспект : авто реф. дис. канд. юрид. наук. Красноярск, 2003. С. 7



юридических лиц или помощи себе сам» Для определенности, попробуем раскрыть одну из примеров статей.

Статья «помоги себе сам» подробно рассказывает, как защититься от мошенников пенсионеру. Базовые правила кибербезопасности :

- помните, сотрудник банка никогда не попросит вас продиктовать номер карты, код из СМС или секретный код на обороте карты (CVV);
- никогда не выполняйте действия под диктовку незнакомцев, даже если они представляются сотрудниками служб безопасности банков или правоохранительных органов;
- всегда сообщайте банку о мошеннике, если столкнулись с ним в Сети или по телефону;
- проверяйте реквизиты переводов и платежей, которые приходят в СМС;
- не переходите по подозрительным ссылкам в СМС и письмах;
- устанавливайте приложения только из официальных магазинов.

Напоминаются о правилах общих кибербезопасности и приводятся схемы мошенничества и способы самозащиты.

Схема № 1 . Обман по телефону.

Защита:

Прежде всего возьмите паузу, с какой бы новостью вам ни позвонили. Не совершайте никаких операций с деньгами под диктовку незнакомцев.

Если вам сообщили о том, что друг или родственник в беде, попытайтесь связаться с ним или его близкими. Если предложили получить компенсацию — перепроверьте информацию на портале Госуслуг. А по поводу здоровья консультируйтесь с лечащим врачом, а не с телефонными мошенниками.

Кроме того, настройте проверку телефонного номера при входящем звонке в мобильном приложении СберБанк Онлайн. Система определит, является ли абонент жуликом, и предупредит вас об этом. Чтобы включить функцию, на главном экране приложения выберите раздел «Безопасность», далее перейдите по строчке «Проверка входящих звонков» и нажмите на кнопку «Подключить».

И помните, что сотрудники банка не запрашивают полный номер карты, срок её действия и трёхзначный код на обратной стороне. У них есть вся необходимая информация

Схема № 2. Коварные смс.

Как защититься: к любым СМС с незнакомых номеров стоит относиться с подозрением, особенно если в них вас просят куда-то перезвонить или перейти по ссылке. Велика вероятность того, что, сделав это, вы или свяжетесь с мошенником, который начнёт



«обрабатывать» вас, или попадёте на поддельный интернет-сайт (если ввести на нём свои платёжные данные, можно потерять деньги).

Если вам пришло сообщение о том, что с вашего счёта якобы списана крупная сумма, не спешите паниковать. Возьмите паузу, сделайте глубокий вдох и выдох и перезвоните в свой банк по номеру телефона, указанному на карте, чтобы уточнить информацию.

Помните, что бесплатный сыр бывает только в мышеловке, а люди не всегда оказываются теми, за кого себя выдают. Будьте бдительны с незнакомыми отправителями, которые говорят, что якобы ошиблись номером. Не пересылайте им информацию, которую они просят, а посоветуйте обратиться в банк или службу поддержки сайта, на котором произошла «ошибка».

А чтобы наверняка обезопасить себя от кражи денег с карты, установите суточный лимит трат в приложении СберБанк Онлайн. Для этого в разделе «Безопасность» выберите опцию «Настройте безопасность», а дальше — пункт «Изменить суточный лимит».

Рассмотрев примеры мошенничества и способы защиты, можно сделать вывод о том что, банки очень подробно расписывают и объясняют как не попасться на уловку мошенников.

Сбербанк, так же предлагает пройти тесты на то что как вы знаете кибербезопасность. Так же, можно пройти марафон: «Смотрите короткие ролики и проходите тесты. Они помогают научиться отличать в разговоре и переписке киберпреступников от сотрудников банка. Кто пройдет марафон до конца, не оставит мошенникам шансов украсть деньги.»

Помимо вышеперечисленных видов мошенничества, существуют еще разные способы, например: вишинг⁴ – это телефонное мошенничество, когда злоумышленники пытаются обманным путём под разными предлогами выманить у клиентов банков деньги или конфиденциальную информацию. Чаще всего мошенники представляются сотрудниками банка или госструктур (МВД, ФСБ, Центробанк, Прокуратуры и т.д.)

Фишинг⁵ – это вид интернет-мошенничества, целью которого является получение конфиденциальных данных пользователя, таких как логин, пароль, номер телефона или платёжная информация. Например: выигрыш в лотерее, в которой вы не участвовали;

У банка ВТБ есть памятка «Клиентам банка ВТБ (ПАО) о соблюдении финансовой безопасности», при пользовании банковскими картами, интернет-банком и другими услугами банка⁶. В ней говорится о том как поступать, если :

- Если Вам поступают звонки от имени «банковских работников», а также СМС-сообщения;

⁴ <https://www.sberbank.ru/ru/person/kibrary/vocabulary/vishing>

⁵ <https://www.sberbank.ru/ru/person/kibrary/vocabulary/fishing>

⁶ https://www.vtb.ru/-/media/Files/PDF/bezopasnost/pamyatka_fl.pdf



- При использовании карты в Интернете;
- При проведении операции в Интернете обращайте внимание на содержание СМС-сообщения с кодом подтверждения операции
- Если Вы выходите в Интернет через смартфон или планшет, настоятельно рекомендуем использовать антивирусное ПО и тд

Так же « ВТБ напоминает, что нельзя сообщать третьим лицам персональные данные, данные банковских карт, пароли, коды из СМС-сообщений и любую информацию, которая может быть использована для списания ваших средств с банковских карт. Банк ВТБ никогда не обзванивает клиентов с предложением перевести деньги «на безопасный счет» под различными предложениями. Настоящие менеджеры банка ВТБ не имеют возможности переключать звонок клиента на другие организации: сторонние банки, МВД или ЦБ»⁷

ВТБ, выделяет следующие виды мошенничества:

1. Дорогое СМС;
2. Опасная продажа;
3. Лжесотрудник;
4. Розыгрыш;

Банк, предупреждает, что: Не осуществляют звонки с просьбой предоставления персональных данных, номеров карт, одноразовых паролей из СМС для подтверждения финансовых операций. Не просят коды из СМС для отмены совершённых «мошеннических операций». Не предлагают для сохранности перевести деньги на специальные счета или установить специальные программы для обеспечения удалённого доступа и управления компьютерами (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin)⁸

Анализируя выводы банка ВТБ, наиболее распространенными схемами мошенничества остаются социальная инженерия и фишинг. Одновременно увеличилось количество случаев социальной инженерии, когда клиенты под воздействием мошенников оформляют кредиты через дистанционные каналы и в банковских офисах, отметили в банке.

Банк России⁹, так же предоставил на сайте статистику об операциях без согласия клиентов: опрос Банка России позволил сформировать среднестатистический портрет клиента банка, наиболее уязвимого для обмана:

- Возраст от 25 до 44 лет;
- Проживает в городе;

⁷ <https://www.vtb.ru/bezopasnost/>

⁸ <https://www.vtb.ru/bezopasnost/>

⁹ https://cbr.ru/analytics/ib/operations_survey_2022/



- Работающий мужчина со средним уровнем дохода и средним образованием;
- Активно пользуется банковскими онлайн-сервисами.

В целях создания механизма выплаты банками и кредитными организациями компенсаций гражданам, у которых мошенники украли деньги со счетов в Государственную Думу внесены Предложения по усовершенствованию механизма ¹⁰противодействия хищению денежных средств с банковских карт ("антифрода") внесены в Госдуму. Проект Федерального закона N 197920-8 "О внесении изменений в Федеральный закон "О национальной платежной системе"

Законопроектом предлагается, в частности:

закрепить обязанность оператора по переводу денежных средств, обслуживающего плательщика, осуществить возврат клиенту- физическому лицу сумму перевода денежных средств или увеличить остаток электронных денежных средств в полном объеме в случае, если оператор получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов без согласия клиента, указывающую на операцию без согласия клиента, и исполнил распоряжение клиента в нарушение установленных требований;

Предоставить банкам право не принимать к исполнению распоряжения по явно мошенническим операциям в течение 2 дней независимо от согласия клиента в случаях, если оператор по переводу денежных средств получил от Банка России информацию, указывающую на операцию без согласия клиента;

Обязать банк получателя средств осуществлять проверку операций на признаки мошенничества наряду с банком плательщика;

Обязать операторов по переводу денежных средств, операторов платежных систем, операторов услуг платежной инфраструктуры направлять в Банк России информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия клиента.

Антифрод- это « (от англ. *anti-fraud* — борьба с мошенничеством) — программные комплексы для предотвращения мошеннических транзакций. Антифрод-решения анализируют каждую транзакцию и присваивают ей метку, характеризующую ее надежность».

На основе анализа, внутреннего регулирования на примере нескольких банков мошенничества, можно сделать вывод, что банки совершенствуются в ногу с появлением новых видов мошенничества. Подробно описывают и рассказывают, как не попасть в руки мошенников. Но к сожалению, время идет, а новые уловки мошенников, вырабатываются с новой скоростью. По нашему мнению, попадание мошенникам, зачастую основывается на психологическом

¹⁰ <https://www.consultant.ru/law/hotdocs/77116.html>



факторе. Чтобы преодолеть или уменьшить доверие людей мошенникам, нужно больше, публично демонстрировать, как работают банки, в том числе в социальных сетях более часто рассылать памятки, о том как действуют мошенники и что их приемы, постоянно меняются.

Список литературы:

1. Бондарь А. В. Мошенничество как вид преступного посягательства против собственности и особенности его проявления в сфере банковской деятельности: Уголовно правовой аспект : авто реф. дис.канд. юрид. наук. Красноярск, 2003. С. 7
2. Карпович О. Г. Понятие, признаки и виды финансового мошенничества // Юрид. мир. 2010. № 8. С. 39
3. Эльзессер В. В. Борьба с мошенничеством в банковской сфере: Уголовно правовой и криминологический аспекты : авто реф. дис. канд. юрид. наук. СПб., 2005. С. 7.
4. Проект Федерального закона N 197920-8 "О внесении изменений в Федеральный закон "О национальной платежной системе"// [Электронный ресурс] URL.<https://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=225034#H39pGcTtb28dQ1ND>(дата обращения: 23.03.2023).
5. Финансовая безопасность: советы по работе с интернет банком и мобильным приложением ВТБ//[Электронный ресурс]. URL: <https://www.vtb.ru/bezopasnost/> (дата обращения: 23.03.2023)
6. Банк России: Обзор операций, совершенных без согласия клиента, финансовых организаций//[Электронный ресурс].URL. https://cbr.ru/analytics/ib/operations_survey_2022/(дата обращения 23.03.2023)
7. Фишинг-Сбербанк// [Электронный ресурс]. URL. <https://www.sberbank.ru/> (дата обращения: 23.03.2023)
8. Энциклопедия Лаборатории Касперского // [Электронный ресурс]. URL. <https://encyclopedia.kaspersky.ru/glossary/antifraud/> (дата обращения : 23.04.2023).