**Слайд 2**

Использование приемов и методов психологического воздействия остается одним из самых популярных инструментов злоумышленников для хищения денег у людей. В результате человек сам переводит деньги или раскрывает злоумышленникам личные и финансовые сведения, которые позволяют мошенникам совершить хищение. Проблема мошенничества актуальна как в отношении граждан, так и в отношении юридических лиц.

Мы совместно с банками противодействуем мошенническим операциям. Сейчас подавляющее большинство попыток злоумышленников похитить деньги у людей отражается защитными системами банков. Так, например, благодаря действию антифрод-систем кредитных организаций за 2025 год банки отразили 134,2 млн попыток злоумышленников похитить средства со счетов клиентов финансовых организаций. Это почти в два раза больше, чем за 2024 год. Таким образом банки сохранили 13,9 трлн рублей своих клиентов. Тем не менее, несмотря на впечатляющее количество предотвращенных хищений, за 2025 год размер потерь клиентов финансовых организаций от действий злоумышленников составил 29,3 млрд рублей, а количество удавшихся попыток осуществления незаконных операций – 1,6 млн. Рост к 2024 году составил 6% по объему хищений и 31% по их количеству.

*Справочно: более значительный рост количества хищений мы связываем с внедрением в мобильных приложениях крупных банков нового функционала – так называемой специальной кнопки – для пострадавших от действий мошенников. Он позволяет клиентам оперативно проинформировать банк о хищении, а также получить электронную справку о мошенническом переводе для обращения в полицию. Этот функционал вывел из тени мелкие хищения, о которых люди не сообщали ни в банк, ни в полицию. Таким образом, пострадавшие с небольшими суммами похищенных денег (до 20 тыс. рублей) все чаще обращаются в банки.*

**Слайд 3**

Мошенники подстраивают свои сценарии под актуальную новостную повестку. Например, когда основной новостью была коронавирусная инфекция, злоумышленники всячески использовали ее в качестве поводов для выманивания денег у граждан.

Есть поводы, которые повторяются ежегодно: например, сдача декларации о доходах за минувший год, начало отпускного сезона и нового учебного года и т.д.

Преступники оперативно реагируют на любые политические или экономические события и играют на эмоциях людей.

**Слайд 4**

Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события.

Сейчас «холодные звонки» якобы сотрудников банков совершаются уже редко. Атаки кибермошенников теперь все чаще направлены на конкретного человека. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. В большинстве случаев людям сложно распознать обман. Приведем некоторые распространенные способы обмана.

**Якобы сотрудник Пенсионного фонда, соцслужбы**. Мошенники сообщают, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда, индексация размера пенсии. Причем для получения этой выплаты никуда ходить не надо: все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.

**Якобы оператор мобильной связи.** Мошенники обращаются к человеку с предложением, например, продлить действие договора на оказание услуг мобильной связи, так как срок предыдущего якобы скоро истечет и номер телефона у человека перестанет действовать. Для этого необходимо продиктовать код, который они присылают якобы для продления обслуживания сим-карты. На самом деле, сообщив звонящим коды из полученного СМС, человек открывает мошенникам доступ к своему онлайн-банку или профилю на портале «Госуслуги».

**Якобы сотрудник банка** (как правило, представитель службы безопасности). Сценарии могут быть разные: от классического «с Вашей карты пытаются перевести деньги» до пугающего «по карте замечены подозрительные операции, и она заблокирована». В любом случае итогом будет просьба сообщить информацию по карте или счету, код из СМС или PUSH-уведомления.

**Якобы друг, родственник.** Мошенник может представиться родственником (другом), попавшим в неприятную ситуацию, или ставшим ее случайным свидетелем, а также представителем правоохранительных органов, который готов помочь гражданину с решением проблемы. Схема довольно старая, но мошенники продолжают ею пользоваться, так как страх за близкого человека – это очень сильная эмоция.

По-прежнему мошенники очень часто представляются **якобы сотрудниками Центрального банка (Банка России).** Гражданам звонят от имени Центробанка и сообщают, что по их карте зафиксирована подозрительная активность − пытаются перевести все деньги за рубеж. Чтобы сохранить свои

деньги и подтвердить, что это не сам человек совершает данную операцию, ему необходимо открыть в Центробанке «защищенный» («безопасный», «специальный») личный счет. Для этого уточняют паспортные данные, просят подтвердить данные по счету (карте). Для открытия счета просят подтвердить небольшой перевод на этот счет, который Центробанк якобы совершает для своих клиентов, то есть сообщить код из СМС. Следует помнить, что Банк России не работает с физическими лицами. При поступлении телефонного звонка якобы от сотрудника Банка России немедленно прервите разговор.

Также злоумышленники могут представляться **сотрудниками правоохранительных органов.** Они долго и подробно рассказывают об обстоятельствах уголовного дела, участником которого, по их словам, гражданин является. Далее для уточнения информации они просят сообщить личную и финансовую информацию. Это и является признаком того, что гражданин разговаривает с мошенником. Помните, что настоящие сотрудники полиции никогда не запрашивают личные и финансовые данные по телефону.

Распространенные мошеннические схемы, а также способы противодействия им Банк России публикует на своем официальном сайте в разделе «Противодействие мошенническим практикам»: https://cbr.ru/information_security/pmp/.

**Слайд 5**

Телефон остается основным инструментом, которым пользуются злоумышленники.

При этом они применяют различные психологические приемы и методы социальной инженерии: введение в заблуждение путем обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа (банковские карты, онлайн-банк) или побуждение владельцев самостоятельно совершить перевод денег, что приводит к их хищению.

Основные проявления социальной инженерии:

1. Обман или злоупотребление доверием (например, мошенники представляются сотрудниками банков, правоохранительных органов или родственниками).
2. Психологическое давление.
3. Манипулирование.

Действительно, мошенники оказывают психологическое давление (торопят, сознательно пугают или, наоборот, приводят в состояние эйфории) и, используя вызванные положительные или отрицательные эмоции,

манипулируют действиями граждан. Существуют различные методы социальной инженерии.

**Слайд 6**

В чем заключается «успех» мошенников?

Их формула: неожиданность + сильные эмоции (положительные и отрицательные) + психологическое давление и создание паники + актуальная тема. И получается, что мы готовы сделать все, что у нас просят мошенники (перевести деньги, совершить финансовые операции, сообщить личную или финансовую информацию).

**Слайд 7**

Как действуют мошенники, чтобы человек, отбросив все свои знания, пошел у них на поводу?

Прежде всего злоумышленникам играет на руку эффект неожиданности. Застав человека врасплох (например, рано утром или поздно вечером, когда сложнее сосредоточиться), они подключают к действию эмоции:

− положительные: радость, желание быстрее получить деньги или выгоду (как правило, такие эмоции человек испытывает после таких фраз, как: «Вам положены социальные выплаты», «Вы выиграли крупную сумму денег» и других похожих);

− отрицательные: страх, испуг, желание помочь, спасти или родного человека, или свои сбережения (эти эмоции проявляются у человека после таких фраз, как: «Ваш сын попал в аварию», «С Вашей карты пытаются украсть деньги»).

Мошенники активируют базовые эмоции, обеспечивая быструю и необдуманную реакцию. Задача киберпреступников – вывести человека из спокойного состояния и отключить у него критическое мышление.

**Слайд 8**

Одной из распространенных мошеннических схем является ситуация, когда мошенники представляются сотрудниками Банка России или правоохранительных органов. Чтобы сохранить денежные средства, они предлагают перевести деньги на «специальный» или «безопасный» счет в Банке России. Чтобы человек окончательно поверил в реальность лжеситуации, мошенники могут прислать целый пакет якобы подтверждающих материалов: сканы официальных документов с подписями и печатями, фотографии удостоверений сотрудников и другие документы на официальных бланках органов государственной власти. К сожалению, такие сообщения могут содержать фамилии реальных работников – эти сведения злоумышленники могут брать с сайта Банка России (или с сайта той организации, сотрудниками

которой они представляются). Высылая фальшивое удостоверение или документы, они стремятся убедить человека в правдоподобности своих мошеннических действий, чтобы в дальнейшем лишить его денег или оформить на него кредит. На самом деле сотрудники Банка России не звонят людям и не направляют никому копии каких-либо документов, не запрашивают персональные и банковские сведения, не предлагают совершить какие-либо операции со счетом.

**Слайд 9**

Еще один вид мошенничества – это фишинг. Злоумышленники подделывают популярные сайты (к примеру, органов власти и различных ведомств, известных магазинов, маркетплейсов, туристических компаний и др.). В частности, на слайде представлен сайт, замаскированный под официальный сайт «Госуслуги». Несмотря на то что внешне он очень похож на настоящий, при внимательном рассмотрении можно заметить, что наименование сайта в адресной строке отличается от официального домена. Настоящий сайт «Госуслуги», а также официальные сайты финансовых организаций в популярных поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

**Слайд 10**

Для чего мошенники создают фишинговые сайты? Имитируя Интернет-ресурсы популярных компаний, они рассчитывают, что пользователи не заметят подделку и оставят на фальшивой странице важную информацию: личные или финансовые данные, логин и пароль, контактные сведения (номер телефона и электронную почту). При овладении чувствительной информацией мошенникам будет легче обмануть человека. А иногда такие сайты являются средством взлома аккаунтов на портале «Госуслуги» или в мессенджерах. Фишинг становится все более распространенным явлением. Внешний вид фишинговых сайтов может полностью совпадать с официальным сайтом, под который пытаются подделать свой сайт мошенники. Как тогда распознать фишинговый сайт?

Сделать это можно по нескольким признакам: адрес сайта может отличаться от настоящего лишь парой символов; в адресной строке отсутствуют https и значок закрытого замка; дизайн сайта скопирован некачественно, в текстах допущены ошибки, у сайта мало страниц или даже только одна – для ввода данных карты.

Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания.

**Слайд 11**

Существует довольно много уловок мошенников в Интернете: например, интернет-магазины и аукционы; восстановление кредитной истории; сообщение о крупном выигрыше или выплате от государства; заманчивое предложение о работе; льготные кредиты; туристические путевки со скидкой; сбор «пожертвований» для детей, больных, животных и т. д.; предложения в части высокодоходных инвестиций. Все они используют актуальную новостную повестку, а также воздействуют на базовые эмоции: положительные или отрицательные.

Будьте бдительны. Не верьте слепо предложениям в Интернете – проверяйте информацию на достоверность в официальных источниках!

**Слайд 12**

Есть распространенное заблуждение в том, что жертвами становятся в основном пожилые и доверчивые люди. На самом деле стать жертвой кибермошенников может любой человек, независимо от уровня образования и социального статуса.

Ежегодно Банк России проводит масштабное исследование – опрос о степени удовлетворенности населения уровнем безопасности услуг, которые оказывают финансовые организации. По его результатам составляется портрет пострадавшего от кибермошенников.

В 2025 году жертвами мошенников чаще всего становились работающие женщины со средним уровнем дохода и средним образованием, которые проживают в городе и имеют постоянную занятость.

С кибермошенниками сталкивались 29% респондентов, 9% из них лишились денег. При этом треть граждан, которые потеряли деньги, при контакте со злоумышленниками не вспомнили о правилах финансовой безопасности.

Да, стать жертвой кибермошенников может любой человек. Тем не менее, по итогам опроса, наибольший интерес для них представляют граждане, которые проявляют высокую экономическую активность и часто пользуются банковскими сервисами – люди в возрасте от 25 до 64 лет.

**Слайд 13**

По-прежнему самым популярным инструментом, с помощью которого мошенники связываются с потенциальной жертвой, остается телефон. Это отметили 55% опрошенных. Кроме того, сохраняют лидирующие позиции атаки на людей через мессенджеры, а также сообщения в социальных сетях и электронной почте. Причем сравнение результатов опроса в отношении мужчин и женщин показало различия в их уязвимостях. Так, например, женщины чаще

оказываются пострадавшими от мошеннических звонков и СМС-сообщений, а мужчины более уязвимы перед более технологичными формами мошенничества: атаками через мессенджеры, а также поддельные сайты и приложения.

Таким образом, вопрос защиты телефонов граждан, через которые в основном происходят коммуникации мошенников, обретает особое значение.

Больше всего опрошенных граждан, пострадавших от действий мошенников, потеряли в итоге сумму до 20 тыс. рублей. Ту же тенденцию фиксирует отчетность, которую Банк России получает от банков: средняя сума ущерба от мошеннической операции по итогам 2025 года составила 18,7 тыс. рублей.

**Слайд 14**

По сравнению с 2024 годом на 6% увеличилось число людей, которые обращались одновременно и в свой банк и в полицию – до 40%. В 2025 году сократилось количество граждан, которые в результате обмана никуда не обращались для защиты своих прав. Среди них в основном пострадавшие, у которых похищенная сумма составила менее 20 тыс. рублей.

Подчеркнем, что, даже если похитили незначительную сумму, надо обязательно обратиться и в обслуживающий банк, и в правоохранительные органы.

В банк нужно обратиться, чтобы информация о переводе средств, который человек совершил под влиянием мошенников, поступила в базу данных Банка России «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента» (далее – база данных о мошеннических операциях, база данных Банка России о мошеннических операциях). Она формируется на основе данных, которые банки передают в Банк России после каждого обращения клиента о несогласии с операцией, в том числе совершенной под влиянием злоумышленников. Информацию из базы данных о мошеннических операциях мы ежедневно направляем во все кредитные организации. Перед тем как осуществить перевод, они обязаны проверять, не находятся ли в ней реквизиты получателя средств. Таким образом, реквизиты, которые один раз «засветились» при проведении мошеннической операции, будут известны всем банкам, что не позволит злоумышленникам обмануть с их помощью других людей.

В полицию надо обратиться, чтобы повысить вероятность привлечения злоумышленника к ответственности.

Таким образом, нужно обратиться в банк и в полицию сегодня, чтобы завтра этот же мошенник не обманул родных и близких.

Чтобы сделать процедуру обращения в банк и полицию удобнее и проще для пострадавших, Банк России обязал крупные банки внедрить в свои мобильные приложения специальный функционал. Он позволяет клиентам оперативно проинформировать банк о хищении, а также получить электронную справку о мошенническом переводе для обращения в полицию. Этот функционал вывел из тени мелкие хищения, о которых люди не сообщали ни в банк, ни в полицию.

Таким образом, пострадавшие с небольшими суммами похищенных денег (до 20 тыс. рублей) все чаще обращаются в банки.

**Слайд 15**

Чтобы не попасть на уловки мошенников, надо соблюдать простые правила поведения:

− не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и др.) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам, они могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

− не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера как минимум могут быть чреваты списанием значительной суммы с Вашего мобильного счета, а как максимум − стать поводом для мошенников реализовать в отношении Вас мошенническую схему;

− не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны установкой вредоносного ПО на Ваш гаджет, а скачивание программ с неофициальных источников может предоставить мошенникам доступ к Вашему устройству;

− установите антивирусные программы на все свои гаджеты и постоянно обновляйте такие программы. Данное ПО предупредит Вас в случае установки подозрительного продукта на Ваш гаджет;

− заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получат доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.

И самое главное правило – будьте бдительны: не действуйте второпях и проверяйте информацию в официальных источниках. Советуйтесь со своими близкими и родными, не оставайтесь наедине с требованиями мошенников.

**Слайд 16**

Если Вам позвонили и представились якобы сотрудником банка, положите трубку и самостоятельно позвоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка. Не нужно перезванивать на номера, с которых вам звонили, – Вы рискуете столкнуться с мошенниками.

Чтобы обезопасить свои данные, установите двухфакторный способ аутентификации (например, логин и пароль, а также подтверждающий код из СМС или PUSH-уведомления) – это, как правило, бесплатно. Пользуйтесь только проверенными и официальными сайтами финансовых организаций в поисковых системах (например, Яндекс, Mail.ru), помеченными цветным кружком с галочкой.

**Слайд 17**

Что делать, если мошенники все же похитили с Вашей карты деньги?

Как только Вы это обнаружите, сразу же заблокируйте карту. Сделать это можно через мобильное приложение банка, а также позвонив в контактный центр или обратившись в отделение банка. В течение суток напишите заявление в отделении банка о несогласии с операцией и возьмите выписку по счету. Банк обязан принять это заявление и предоставить выписку. Если Вы клиент крупного банка, то можете направить обращение о мошеннической операции в свой банк в его мобильном приложении. Там можно сформировать справку о такой операции для предъявления в полицию.

Затем как можно скорее напишите заявление в полицию, лично обратившись в ближайший территориальный орган внутренних дел с заявлением о возбуждении уголовного дела и предоставив документы, полученные в банке.

**Слайд 18**

Как противостоять телефонным мошенникам?

Не отвечайте на звонки с незнакомых номеров. Как правило, если Вам звонят с работы или из другой организации, от которой Вы ожидаете звонка, Вам дополнительно напишут СМС-сообщение или сообщение в мессенджере. Никогда не перезванивайте по незнакомым вам номерам.

Если разговор касается финансовых вопросов, не продолжайте разговор и положите трубку. Сотрудники банков или правоохранительных органов не запрашивают Ваши личные и финансовые данные по телефону.

Не торопитесь принимать решение, которое касается Ваших денег. Мошенники добиваются именно того, чтобы Вы приняли быстрое и необдуманное решение. Они используют методы социальной инженерии: торопят Вас, пугают, вызывают панику. Не стоит поддаваться такому давлению:

проверьте информацию в официальном источнике или обратитесь за помощью к близким родственникам.

Прежде чем принять какое-то решение, связанное с финансами, позвоните близкому человеку, в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий. Важно получить подтверждение информации именно из официального источника, контактные номера при этом берите из доверенных источников: если это знакомый – из своей записной книжки, если организация – с ее официального сайта.

Будьте бдительны и оставайтесь в безопасности!

**Слайд 19**

Банк России проводит постоянную работу по выявлению и блокировке телефонных номеров, которые используют злоумышленники, и мошеннических Интернет-ресурсов. После выявления он направляет для последующей блокировки телефонные номера операторам связи, а Интернет-ресурсы – в адрес уполномоченных организаций, которыми являются регистраторы доменных имен и Генеральная прокуратура Российской Федерации. За 2025 год Банк России инициировал блокировку более 69 тыс. телефонных номеров и 38,4 тыс. мошеннических сайтов, страниц в социальных сетях и приложений.

**Слайд 20**

Банк России принимает комплексные меры, направленные на:

− повышение качества работы антифрод-систем банков;

− противодействие совершению мошеннических переводов;

− противодействие кредитному мошенничеству;

− противодействие дропперству.

В основе принимаемых мер лежит база данных о мошеннических операциях, которую ведет Банк России.

Указанная база данных формируется на основе сведений, полученных от банков и других участников информационного обмена, и содержит большое количество параметров – уникальных идентификаторов, в том числе сведения о совершенных операциях, о плательщиках и получателях денежных средств. В основе ее формирования лежит заявление пострадавшего человека в свой банк о совершении мошеннической операции. Банки передают в Банк России информацию обо всех случаях или попытках совершения переводов без добровольного согласия клиентов, они обязаны учитывать сведения из базы в своих защитных системах и не допускать новые переводы на счета злоумышленников. Кроме того, в своей базе данных о мошеннических операциях Банк России учитывает сведения, которые поступают от МВД России, а именно в случаях, когда человек, пострадавший от мошенников, уже обратился

с заявлением в полицию. В этом случае МВД России может направить запрос в Банк России, чтобы получить необходимую для расследования информацию о получателе похищенных денег. Количество обращений в Банк России от МВД России по автоматизированным каналам за 2025 год выросло в 1,5 раза, сейчас мы получаем порядка 20 тыс. запросов ежемесячно. И, кстати, это позволяет нам быстрее наполнять базу данных о мошеннических операциях и видеть более полную картину о хищениях. Если запрос связан с мошенническим переводом, сведения о котором есть в нашей базе данных, время ответа Банка России не превышает одной минуты. Если такие сведения ранее в базу еще не поступали, мы запрашиваем их у банков в автоматизированном режиме и направляем в МВД России.

Сведения о получателе платежа попадают в базу данных о мошеннических операциях на основании информации, поступающей и от банка – отправителя платежа, и от банка – получателя платежа. Предоставленную банками информацию регулятор проверяет и включает в базу данных о мошеннических операциях на основе определенных правил и алгоритмов.

Банк России осуществляет постоянный мониторинг за включением сведений о получателях средств, в том числе о юридических лицах, в базу данных о мошеннических операциях, которая ежедневно обновляется. Сведения из нее доступны всем банкам, и кредитные организации обязаны учитывать их в своих антифрод-системах.

**Слайды 21, 22**

Для этого регулятор определяет признаки мошеннических операций, которыми должны руководствоваться банки для предотвращения подозрительных переводов. Если перевод соответствует хотя бы одному из этих признаков, банк должен приостановить операцию и предупредить клиента о риске обмана. На основании результатов анализа эффективности их применения и с учетом возможного появления новых схем, с помощью которых мошенники пытаются обойти установленные барьеры, Банк России расширяет перечень действующих признаков. С начала 2026 года число признаков, которыми руководствуются кредитные организации, было увеличено с 6 до 12.

Новые признаки:

1. Попытка внесения наличных в банкомате с помощью токенизированной карты на счет человека, который за последние 24 часа до этого сделал трансграничный перевод другому человеку на сумму больше 100 тыс. рублей.

2. Перевод человеку, которому ни разу за последние полгода не осуществлялись переводы. Этот критерий учитывается, только если переводу

менее чем за 24 часа предшествовал перевод самому себе из другого банка по СБП на сумму более 200 тыс. рублей.

**Важно: подозрительным считается не перевод самому себе по СБП, а последующая операция человеку, с которым давно не было финансовых взаимоотношений. На оплату товаров и услуг юридическим лицам критерий не распространяется.**

3. На телефоне клиента обнаружены подозрительные события (вредоносная программа, изменение операционной системы, провайдера связи и др.), либо за 48 часов до перевода произошла смена номера телефона в онлайн-банке или на портале «Госуслуги».

4. Превышено время обмена данными между картой, в т. ч. токенизированной, и банкоматом при бесконтактной операции в банкомате (временной интервал устанавливает АО «НСПК»).

5. Банк получил от АО «НСПК» информацию о риске мошенничества при совершении переводов.

6. Сведения о получателе денег есть в государственной информационной системе противодействия правонарушениям, которые совершаются с использованием ИКТ (срок вступления в силу – 01.03.2026).

«Старые» признаки, которые продолжают действовать:

1. Реквизиты получателя есть в базе данных Банка России.

2. Нетипичная операция (по сумме перевода, периодичности, времени и месту и т. д.).

3. Операция с устройства, которое ранее использовалось мошенниками, и сведения о нем есть в базе данных о мошеннических операциях.

4. Сведения о получателе денег есть в собственной базе данных банка о подозрительных переводах.

5. Есть информация о возбуждении уголовного дела по факту мошенничества.

6. Есть поступившая как минимум за 6 часов до перевода информация от других организаций (например, от операторов связи) о возможном мошенническом переводе (телефонная активность, рост числа входящих СМС и т. д.).

**Слайд 23**

Закон, который вступил в силу 25.07.2024, ввел двухдневный «период охлаждения». В течение этого времени банк не переводит деньги на подозрительный счет, если его реквизиты находятся в базе данных Банка России о мошеннических операциях. За эти 2 дня человек может понять, что имеет дело с мошенниками, и отказаться от перевода. Если банк все-таки совершит такой

перевод раньше и не известит клиента о том, что его перевод может быть направлен на мошеннический счет, то он должен компенсировать клиенту потери. Крупные банки ежемесячно «охлаждают» (приостанавливают на 2 дня) порядка 330 тыс. переводов на счета из базы данных Банка России. Банки перестали без «периода охлаждения» переводить деньги на счета из нашей базы.

Банки могут ограничить пользование электронным средством платежа (карты, онлайн-банкинг) клиенту, если его реквизиты содержатся в базе данных Банка России о мошеннических операциях. По закону они обязаны это сделать, если информация о совершенных клиентами противоправных действиях поступила от МВД России. При этом человек может воспользоваться деньгами и совершить любые банковские операции, но для этого ему необходимо обратиться в отделение банка с паспортом или другим документом, удостоверяющим личность.

С 2025 года, если банк не заблокировал карту или доступ к онлайн-банкингу клиенту, сведения о котором находятся в базе данных о мошеннических операциях, для такого человека действует лимит на переводы — он не может переводить себе или другим людям с использованием электронного средства платежа больше 100 тыс. руб. в месяц. Кроме того, он не сможет снять в банкомате больше 100 тыс. рублей в месяц.

**Слайд 24**

Ограничение на использование электронных средств платежа действует все время, пока сведения о клиенте (человеке или юридическом лице) находятся в базе данных регулятора. При этом он может обжаловать включение в нее реквизитов.

Это можно сделать двумя способами:

1. Обратиться с заявлением в любой из банков, клиентом которого является заявитель. Банк обязан перенаправить обращение клиента в Банк России не позднее следующего рабочего дня (при отсутствии основания для отказа в передаче заявления в Банк России). Если человек не имеет возможности лично подать заявление, это может сделать его представитель по нотариально оформленной доверенности.
2. Направить заявление в Банк России через Интернет-приемную, выбрав в качестве темы обращения «Информационную безопасность» и соответствующий тип проблемы.

Банки могут и самостоятельно, без участия клиента, направить в Банк России мотивированное заявление об исключении сведений о клиенте из базы данных регулятора. Этой возможностью они могут воспользоваться, если у

них будут основания полагать, что включение сведений о клиенте в базу данных о мошеннических операциях необоснованно.

Регулятор в течение 15 рабочих дней рассмотрит заявление и примет мотивированное решение о целесообразности исключения реквизитов из базы данных о мошеннических операциях.

Рассматривая каждый случай об исключении, Банк России взаимодействует с кредитными организациями, чтобы минимизировать риски принятия необъективного и необоснованного решения. По результатам рассмотрения большинства обращений об исключении сведений из базы данных Банка России о мошеннических операциях принимаются отрицательные решения – основания для исключения сведений из базы данных отсутствуют, так как банки подтверждают признаки мошенничества. Кроме того, ряд обращений поступает от заявителей, сведения о которых отсутствуют в базе данных регулятора (например, в случаях, если клиент не понимает причину приостановки платежа или желает проверить, находятся ли его реквизиты в базе данных Банка России, и проч.). В остальных случаях, если по результатам взаимодействия с банками подтверждается обоснованность обращения заявителей, сведения о них исключаются из базы данных регулятора.

В соответствии с Федеральным законом «О национальной платежной системе» решение об отказе в удовлетворении заявления об исключении сведений из базы данных Банка России о мошеннических операциях может быть обжаловано в суде.

Если регулятор принимает решение не исключать сведения из базы данных, он в своих ответах дает человеку подробную информацию о транзакции, из-за которой информация о нем попала в базу данных Банка России. С ней человек может самостоятельно обратиться в банк плательщика для урегулирования вопроса, чтобы вернуть деньги, похищенные у других людей, и устранить первопричину проблемы.

Когда возбуждено уголовное дело по факту мошенничества, Банк России также предоставляет человеку информацию о номере уголовного дела и о территориальном органе МВД России, который ведет расследование. Связавшись с ним, человек может уточнить возможность обращения в отделение полиции по месту своего жительства или по месту расследования уголовного дела и дать необходимые пояснения, даже если дело заведено в другом регионе. Мы начали апробацию этого механизма в декабре 2025 года. Сейчас он работает в соответствии с Указанием Банка России от 19.01.2026 № 7287-У и рекомендательным письмом Банка России в кредитные организации от 11.02.2026 № 017-56/1167.

*В среднем ежедневно в адрес регулятора поступают десятки обращений от МВД России об урегулировании таких ситуаций, что позволяет исключать реквизиты человека из базы данных. Сведения исключаются из базы данных Банка России с учетом ответов кредитных организаций о необоснованности включения информации о клиенте в базу данных Банка России.*

**Слайд 25**

Мошенники постоянно придумывают новые схемы обмана. Миновало время «холодных обзвонов». Сейчас атаки становятся все более персонифицированными, тщательно подготовленными. Злоумышленники предварительно изучают жертву: ее профиль в социальных сетях, круг друзей, увлечения, место работы, а также в соответствии с этим оценивают, на какую сумму человек может оформить кредит. Часть информации берется с сайтов, на которых человек сам оставляет данные о себе, а некоторые сведения становятся доступными из-за утечек.

Затем мошенники ищут варианты наиболее эффективного установления коммуникации с этим человеком. Под него разрабатывается индивидуальный сценарий обмана с использованием современных компьютерных программ. Например, распространяется схема с созданием поддельных телеграм-аккаунтов руководителей: чтобы завоевать доверие, людям пишут от имени их начальников, заранее изучая, кто именно ими руководит. Мошенники могут использовать современные программы и технологии, в том числе искусственный интеллект, чтобы создавать голосовые сообщения от имени родственников человека или его близких. Затем, войдя в доверие, злоумышленники могут разыгрывать многоходовые сценарии: на протяжении нескольких часов или суток с человеком поочередно связываются лжесотрудники Министерства внутренних дел, Следственного комитета или Генеральной прокуратуры, а также Центрального банка. Его максимально запутывают, отправляют фотографии поддельных удостоверений личности, приказов Центробанка, документы с синей печатью. Такие адресные атаки мошенников опасны тем, что человеку еще сложнее распознать обман. Злоумышленники и рассчитывают на то, что, используя приватную информацию, они «пробьют» барьер недоверия, вынудят человека совершить необходимые им действия и получат доступ к деньгам.

**Слайд 26**

Все чаще злоумышленники для хищения денег стали использовать дипфейки, созданные с использованием современных технологий. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его коллегам, друзьям или родным через мессенджеры или социальные сети. В коротком фальшивом видеоролике

виртуальный образ, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. В некоторых случаях мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той сферы деятельности, в которой трудится их потенциальная жертва.

Чтобы создать цифровую копию конкретного человека, злоумышленники используют фото и видео, а также запись голоса, полученные в основном из открытых источников либо в результате взлома его аккаунта в социальных сетях или мессенджерах.

**Слайд 27**

Проявляйте осторожность при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи − его аккаунт могли взломать злоумышленники. Иногда для рассылки таких сообщений мошенники создают поддельные аккаунты с именем и фото человека. Не спешите переводить деньги! Обязательно сами свяжитесь по альтернативному каналу с человеком, от имени которого поступило сообщение, и перепроверьте информацию. Если такой возможности нет, то задайте собеседнику проверочный личный вопрос, ответ на который может знать только он.

Да, качество дипфейков растет. Но их можно распознать, уделяя внимание деталям. Например, у собеседника могут быть неестественная, несвойственная ему мимика, монотонная речь, а также могут присутствовать дефекты звука или изображения.

**Слайд 28**

Вовлечение в дропперство – очень острый вопрос, который имеет крайне высокое социальное значение. Ведь нередко в эту деятельность вовлекают школьников и студентов, а те, надеясь на мгновенный сомнительный доход, могут понести серьезное наказание и заработать «пятно» на всю жизнь. Кроме того, очень часто дропами становятся: жители небольших населенных пунктов, приехавшие учиться или работать в крупные города; люди, находящиеся в сложном финансовом положении (например, взявшие много кредитов), а также уязвимые слои населения (сироты, многодетные семьи, безработные, пенсионеры, молодые мамы).

Кто же такие дропы (дропперы)?

Это участники деятельности по обналичиванию денежных средств, полученных преступным путем, в том числе с использованием своих электронных средств платежа (карты, онлайн-банкинг и т. д.). Дроп не инициатор преступления, он выполняет указания злоумышленников, переводит

похищенные деньги на другие счета и карты, проводит операции с наличными в банкоматах и терминалах (снятие или внесение) либо оформляет на себя банковские карты и отдает их злоумышленникам. За это дроп получает определенное вознаграждение.

Чем занимаются дропперы:

− получают на свои карты деньги и передают их дальше по цепочке другим людям наличными или переводом;

− принимают наличные деньги, вносят их на свои счета для последующего перевода или передают другим людям;

− предоставляют мошенникам в пользование свои карты или доступ к онлайн-банку.

**Слайд 29**

Чаще всего дропов вовлекают в преступную деятельность через Интернет. Преступники могут связаться с человеком через социальные сети, мессенджеры, всплывающие окна в Интернете, а также лично и по электронной почте. Сценариев может быть много: например, предложение работы, участие в лотерее. Также могут обращаться от имени банков, правоохраны; попросить вернуть якобы ошибочно переведенные деньги.

Как определить, что Вас пытаются вовлечь в дропперскую деятельность?

Стоит насторожиться, если Вам предлагают:

- оформить банковскую карту и отдать ее неизвестным лицам;
- получить перевод денег от неизвестного лица, обналичить средства и передать их другому человеку;
- получить от неизвестного человека наличные деньги, внести их на свой банковский счет и совершить перевод третьему лицу;
- предоставить неизвестным лицам доступ к уже существующим банковским картам или онлайн-банку.

Чтобы не стать дроппером поневоле, не соглашайтесь использовать личные счета для пересылки денег, не отдавайте карту посторонним людям и не раскрывайте им доступ к своему онлайн-банку. Никуда не переправляйте деньги, которые пришли вам по ошибке. Обратитесь в свой банк и попросите сделать обратный перевод по реквизитам отправителя.

Иногда дропами становятся по незнанию: люди даже не понимают, что злоумышленники используют их средства платежа для обналичивания похищенных денег. Но независимо от того, сознательно человек участвует в дропперской деятельности или его вовлекли в этот процесс обманным путем, он является участником преступной схемы. Он не только будет испытывать

неудобства при проведении банковских операций, но и понесет уголовную ответственность.

Что делать, если человек понял, что его вовлекли в дропперскую деятельность?

Первым делом надо прекратить все контакты с мошенниками. Если человек под влиянием злоумышленников передал незнакомцам свою карту или раскрыл им данные для входа в свой банковский кабинет, надо немедленно обратиться в свой банк, заблокировать карту и дистанционный доступ к счетам. Также необходимо обратиться в правоохранительные органы и подробно описать сложившуюся ситуацию.

**Слайд 30**

Информацию о получателе, на чей счет пострадавший от мошенников человек переводит деньги, банки и полиция передают в базу данных Банка России о мошеннических операциях. Когда человек попадает в нее, все его карты могут быть заблокированы, а дистанционный доступ к счетам через мобильное приложение и личный кабинет на сайте – приостановлен. Если информацию о дропе передает полиция, это случится обязательно. Совершать любые банковские операции, в том числе снимать деньги со своих счетов и вкладов, клиент сможет только лично в офисе банка.

Все переводы на счета дропа «замораживаются» на 2 дня. У отправителя средств запросят подтверждение такой операции, и, если он откажется от ее совершения, деньги на счет дропа не поступят. Исключение составляют операции по зачислению заработной платы и социальных выплат – они в любом случае без промедления будут зачислены на счет получателя.

Если банк не заблокировал карту или доступ к онлайн-банкингу клиенту, сведения о котором находятся в базе данных о мошеннических операциях, для такого человека действует лимит на переводы − он не может переводить себе или другим людям с использованием электронного средства платежа больше 100 тыс. руб. в месяц. Кроме того, он не сможет снять в банкомате больше 100 тыс. рублей в месяц.

Ограничение действует, пока сведения о человеке находятся в базе данных Банка России. Чтобы совершить перевод на сумму, превышающую установленный законом лимит, или снять наличные деньги, человеку необходимо обратиться в отделение банка с паспортом или другим документом, удостоверяющим личность.

На переводы в адрес юридических лиц ограничение не распространяется. Это значит, что человек, сведения о котором или информация о платежных средствах которого есть в базе данных Банка России о мошеннических

операциях, по-прежнему может с использованием карт и онлайн-банкинга покупать товары в магазинах или на маркетплейсах, оплачивать жилищно-коммунальные и другие услуги.

Кроме того, банки не открывают лицам, информация о которых содержится в базе данных Банка России о мошеннических операциях, новые электронные средства платежа (платежные карты, онлайн-банкинг).

В результате применяемых мер банки в 100% случаев приостанавливают действие карт и онлайн-банкинга всем лицам, сведения о которых поступили в Банк России от МВД России. Транзакционная активность по платежным инструментам, сведения о которых содержатся в базе данных о мошеннических операциях, многократно снижается – в 40 раз. Это влечет за собой рост издержек мошенников на поиски новых инструментов для вывода похищенных денег.

**Слайд 31**

Банк России совершенствует свою нормативную базу, чтобы как можно больше пострадавших от действий мошенников обращались с заявлениями в свои банки и информация о злоумышленниках поступала в базу данных Банка России.

Так, регулятор обязал крупные банки внедрить в мобильные версии своих приложений новый функционал, чтобы гражданин мог:

– подать заявление о мошеннической операции без посещения банка;

– получить справку об этой операции для предоставления в полицию;

– ответить на вопрос банка, является ли операция мошеннической, если такой запрос поступил в Банк России из МВД России.

Этот функционал вывел из тени небольшие хищения, о которых граждане ранее не заявляли ни в банк, ни в полицию. По результатам проведенного Банком России опроса, доля пострадавших, обратившихся и в кредитную организацию, и в полицию, увеличилась за год на 6% − до 40%. Мы ведем постоянный мониторинг реализации банками этого функционала. Наша задача – сделать так, чтобы сервис был максимально удобен и имел простой клиентский путь.

**Слайд 32**

В результате принимаемых Банком России мер злоумышленникам становится все сложнее выводить похищенные деньги, используя переводы. Поэтому в рамках различных сценариев обмана злоумышленники все чаще пытаются убедить человека снять в банкомате и передать им наличные. То есть мошенники пытаются вывести похищенные деньги из периметра платежной инфраструктуры, где антифрод-системы банков достаточно эффективно приостанавливают подозрительные переводы.

Поэтому при участии Банка России были разработаны нормы закона[1], которые направлены на противодействие мошенническим схемам с использованием банкоматов.

Сейчас банки, которые оформили клиенту платежную карту, перед выдачей наличных через банкоматы обязаны проверять, не находится ли человек под воздействием мошенников, а также не совершает ли эту операцию злоумышленник. Для этого перед каждой операцией они проверяют наличие специальных признаков, которые определил Банк России.

Если операция соответствует хотя бы одному из них, банк немедленно сообщит об этом клиенту и на 48 часов введет временный лимит на выдачу наличных денег в банкомате – до 50 тыс. рублей в сутки. Если человек находится под влиянием мошенников, эта мера даст ему время, чтобы обдумать свое решение и отказаться от операции. Способ информирования предусмотрен договором клиента с банком. Как правило, это СМС-сообщение или PUSH-уведомление. Снять более крупную сумму в этот период можно в отделении банка.

Мы наблюдаем, что к концу 2025 года по сравнению с пиковыми значениями в июне − июле 2025 года объем хищений через банкоматы снизился на 40%.

Признаки выдачи наличных денежных средств без добровольного согласия клиента с использованием банкоматов устанавливает Банк России.

**Слайд 33**

Какие это признаки?

В их основе лежат конкретные критерии, а также анализ нехарактерного поведения человека при снятии наличных. Например, непривычные время суток или местонахождение банкомата, нетипичные сумма или количество операций.

Банк также обращает внимание на попытки клиента снять деньги непривычным для него способом, например, когда вместо платежной карты он использует QR-код или цифровую карту.

Кредитная организация вводит лимит на снятие наличных через банкомат, если клиент пытается снять деньги в течение 24 часов с момента:

получения им кредита, займа или кредитной карты,

увеличения лимита на выдачу наличных или увеличения лимита по кредитной карте,

[1] Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

зачисления на свой счет более 200 тыс. рублей по СБП со своего счета в другом банке,

досрочного расторжения договора банковского вклада на аналогичную сумму.

Выявление одного из признаков направлено на противодействие схеме, при реализации которой человека убеждают установить на своем устройстве приложение и токенизировать карту мошенников. Для отклика банкомата на карту, токенизированную с использованием мошеннического приложения, необходимо больше времени. Таким образом, увеличение времени ожидания отклика банкомата на токенизированную карту или телефон является признаком совершения операции без добровольного согласия клиента.

Также банк обязан учитывать информацию об уровне риска осуществления мошеннической операции, которую получает от оператора услуг платежной инфраструктуры (АО «НСПК»).

**Слайд 34**

Еще один из признаков, установленных регулятором, – наличие у банка информации, которая может свидетельствовать о том, что клиент пытается снять наличные через банкомат под влиянием мошенников, например не менее чем за 6 часов до запроса на снятие денег зафиксированы несвойственная человеку активность телефонных разговоров, рост числа входящих СМС-сообщений с новых номеров или сообщений в мессенджерах.

Сигналом для банков служит информация:

об изменении или нетипичности параметров мобильного устройства, с помощью которого человек делает запрос на выдачу наличных денег (это может быть смена провайдера связи, использование VPN-сервисов);

о вредоносных программах, имеющихся на этом устройстве;

о смене номера телефона в личном кабинете мобильного приложения банка или на портале «Госуслуги».

Критерием для введения лимита является наличие информации о 5 и более отказах клиенту в выдаче наличных денег в течение одного календарного дня (например, из-за ошибок при вводе ПИН-кода или превышения лимита кредитования).

**Слайд 35**

В фокусе повышенного внимания Банка России находится ситуация с кредитным мошенничеством. В 2025 году был введен целый пакет мер, направленный на противодействие ему.

Какие это меры?

Каждый гражданин может добровольно установить в своей кредитной истории запрет на заключение с ним договоров потребительского кредита или займа. Сделать это он может как через портал «Госуслуги», так и в многофункциональных центрах. Запрет может быть разным: по виду кредитора (банк или микрофинансовая организация) или по способу обращения за кредитом или займом (в офисе и дистанционно либо только дистанционно). Если запрет установлен, кредитор должен отказать в выдаче кредита или займа. Этот механизм востребован – по состоянию на 08.04.2026 граждане установили более 24 млн таких запретов.

**Слайд 36**

При участии Банка России в 2025 году был принят закон[2] о противодействии кредитному мошенничеству.

В соответствии с его положениями банки и микрофинансовые организации (МФО) обязаны проводить антифрод-мероприятия при заключении договоров потребительского кредита и займа.

Если банк или МФО нарушат антимошеннические нормы и будет возбуждено уголовное дело по факту хищения полученных денег, то заемщик освобождается от исполнения обязательств и уплаты процентов до вступления в силу приговора суда по уголовному делу.

Так, заработал «период охлаждения» – время между подписанием заемщиком договора потребительского кредита (займа) и выдачей ему денег. Кредиты и займы от 50 тыс. до 200 тыс. рублей доступны для использования через 4 часа после подписания договора с клиентом, а свыше 200 тыс. рублей – через 48 часов.

Пока действует «период охлаждения», человек вправе отказаться от заемных денег. Для этого ему необходимо уведомить об отказе банк или МФО. Способ уведомления кредитора предусмотрен договором потребительского кредита (займа).

Во время «периода охлаждения» проценты по договору потребительского кредита (займа) не начисляются.

**Слайд 37**

Для «периода охлаждения» есть исключения. Он не применяется при оформлении кредитов и займов до 50 тыс. рублей, а также в случаях, когда риски мошенничества минимальны: при оформлении ипотечных, образовательных кредитов и автокредитов (если деньги перечисляются продавцу автомобиля – юридическому лицу). Также можно быстро приобрести товары и услуги

[2] Федеральный закон от 13.02.2025 № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

в кредит, если человек лично пришел в магазин или организацию. Без задержек можно рефинансировать ранее выданные кредиты и займы, если при этом не увеличивается сумма долга. Норма не касается кредитов, которые оформляются при участии созаемщика или поручителей, а также доверенного лица заемщика.

**Слайд 38**

В соответствии с нормами закона МФО при дистанционном оформлении займа зачисляют деньги на счет, только если сведения о заемщике и получателе денег совпадают. Признаки совпадения сведений о заемщике и получателе денежных средств устанавливаются Банком России. Эта мера направлена на противодействие схеме, при которой мошенники оформляют договоры на ничего не подозревающих граждан, а деньги получают сами.

Также МФО отказывают в выдаче займа, если информация о заемщике содержится в базе данных Банка России о мошеннических операциях.

Банкам по закону не запрещается предоставлять кредит человеку, сведения о котором содержатся в этой базе. Но кредитная организация не может перечислять заемные средства на счет такого человека, если клиент указал его реквизиты в качестве третьего лица для получения денег. Поэтому если по результатам проверки банк выявит, что сведения о получателе денег находятся в базе данных Банка России о мошеннических операциях, то он откажет заемщику в перечислении денег на счет третьего лица. Банк должен незамедлительно уведомить клиента о причине отказа в перечислении денег и о том, что они могут быть переведены только на банковский счет самого заемщика.

Чтобы избежать случаев, когда человек в короткий срок оформляет сразу несколько кредитов и займов в разных банках и МФО под влиянием мошенников, будет ускорен обмен информацией между кредиторами и бюро кредитных историй (БКИ). С 01.07.2026 БКИ будут обязаны принимать информацию, которую направляют банки и МФО, и передавать ее им в онлайн-режиме. А банки и МФО с 31.12.2026 будут обязаны получать информацию из БКИ, фиксировать факт ее получения, хранить и учитывать ее в своих антифрод-процедурах.

**Слайд 39**

В результате реализуемых мер общая сумма кредитов и займов, оформленных клиентами крупных банков без добровольного согласия, за год снизилась на 39,2%. По данным крупных банков, в 2025 году доля кредитных денег, переведенных на счета злоумышленников, составила 18% **в сравнении** с общим объемом хищений. Для сравнения – в 2024 году этот показатель составлял 37%. Но несмотря на достигнутые успехи, проблема остается. И необходимо продолжать деятельность в этом направлении, чтобы ее искоренить.