Государственные меры защиты граждан от кибермошенничества в Российской Федерации: подробное руководство

Главное

По состоянию на июнь 2026 года в России сформирована многоуровневая система защиты граждан от кибермошенничества, включающая как превентивные механизмы (обязательный «период охлаждения» по кредитам, самозапрет на выдачу займов, автоматический мониторинг подозрительных операций), так и экстренные инструменты реагирования (функция оперативного сообщения о мошенничестве на портале «Госуслуги», обязанность банков блокировать подозрительные переводы на срок до 48 часов). С июня 2026 года вступил в силу новый пакет законов (Федеральный закон № 210-ФЗ), который вводит ответственность банков и операторов связи за ущерб при несоблюдении требований защиты, а также запускает «тревожную кнопку» на «Госуслугах» для уведомления о фактах мошенничества. Ключевые нововведения последнего года: обязательная маркировка звонков из-за границы, возможность самостоятельной блокировки всех международных вызовов, ужесточение контроля за сим-картами (новый срок расторжения договора — не ранее 90 дней), а также применение искусственного интеллекта для проверки переводов по расширенному списку признаков [1][2][3].

---

1. Действующие государственные механизмы и меры защиты

1.1. Основные законодательные акты

Федеральный закон от 26.06.2026 № 210-ФЗ — «второй пакет антифрод-поправок» — включает около 30 новых мер по борьбе с кибермошенничеством:

- новая функция на портале «Госуслуги» для оперативного направления сведений о возможном факте мошенничества («тревожная кнопка»);
- обязательная маркировка звонков из-за границы и возможность для абонента самостоятельно заблокировать любые телефонные звонки из-за рубежа;
- обязанность операторов связи и банков возмещать ущерб пострадавшему от мошенников при переводе денег против его воли, если они не соблюдали установленные требования;
- новые ограничения в отношении сим-карт: расторжение договора об оказании услуг связи — не ранее чем через 90 дней с даты его заключения

(абонентский платеж перестает взиматься с момента направления заявки о расторжении);
- возможность выпуска специальных «детских» сим-карт с дополнительными функциями защиты [1].

Федеральный закон от 26.06.2026 № 199-ФЗ вводит административную ответственность за неисполнение обязанностей по проведению авторизации пользователей в интернете при предоставлении доступа к информации. Штрафы для граждан — от 10 тыс. до 20 тыс. рублей [1].

Федеральный закон от 13.02.2025 № 9-ФЗ — внёс изменения в порядок выдачи потребительских кредитов и займов, установив обязательный «период охлаждения» [4].

1.2. Уполномоченные органы

- **Банк России (ЦБ РФ)** — регулирует деятельность банков и микрофинансовых организаций, формирует базу данных о случаях и попытках мошеннических переводов (ведётся специальным подразделением ФинЦЕРТ), устанавливает критерии подозрительных операций [2].
- **МВД России** (Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий — УБК) — расследует киберпреступления, ведёт мониторинг новых схем мошенничества [5].
- **Роскомнадзор** — контроль в сфере связи и обработки персональных данных.
- **Полиция** — приём заявлений по телефону 102 или 112 [6].

1.3. Каналы экстренного реагирования

- **«Тревожная кнопка» на портале «Госуслуги»** (запущена 9 июня 2026 года) — позволяет пользователю отправить сообщение в государственную информационную систему «Антифрод», если он подозревает, что с ним связались мошенники. Оповещение из системы передаётся банкам и операторам связи для пресечения действий злоумышленников. Аналогичная функция внедряется в мессенджере Max и приложениях банков [3].
- **Телефон полиции: 102 или 112** [6].
- **Горячая линия банка** — номер указан на обратной стороне карты и в мобильном приложении (круглосуточно).

---

2. Период охлаждения по кредитам

2.1. Что это такое и когда введено

«Период охлаждения» — это обязательная пауза между одобрением кредита или займа и фактической выдачей денег. Введён Федеральным законом № 9-ФЗ с **1 сентября 2025 года** [4].

2.2. Условия применения

Сумма кредита/займа	Период охлаждения	Особенности
От 50 000 до 200 000 рублей	4 часа	Деньги не перечисляются до истечения срока
Свыше 200 000 рублей	48 часов	Деньги не перечисляются до истечения срока
Кредитные карты (при увеличении лимита)	Применяется «период охлаждения»	Лимит не активируется сразу
Займы с созаёмщиком или поручителем	Пауза не применяется	Деньги выдаются без задержки
Страховка по кредиту	30 календарных дней	Отдельный срок для отказа от добровольного полиса

2.3. Как работает

Если клиент передумал брать кредит в течение «периода охлаждения», он может отменить заявку через личный кабинет или по телефону. Проценты и комиссии за этот период не начисляются, договор теряет силу автоматически. Для МФО, где ранее микрозаймы оформлялись за 15 минут, теперь действуют такие же правила, как для банков [4].

---

3. Самозапрет на оформление займов

3.1. Где и как установить

Самозапрет (официально — «запрет на получение кредитов») устанавливается через портал **«Госуслуги»** или в отделении **МФЦ**. Услуга бесплатная [7].

Кто может установить:

- граждане России и иностранцы, имеющие подтверждённую учётную запись на «Госуслугах»;
- обязательно наличие ИНН в личном кабинете.

Важно: запрет можно установить только **на себя**. Сделать это за родственников (даже по доверенности) пока нельзя [7].

3.2. Виды запрета

Вид	Описание
Полный	Распространяется на получение кредита в кредитных и микрофинансовых организациях (МФО) при личном посещении и через интернет
Частичный	

Вид	Описание
	На получение кредита в определённом типе организаций (например, только МФО) и/или на определённый способ получения (например, только дистанционно)

3.3. Порядок действий на портале «Госуслуги»

1. Перейдите к услуге «Запрет на получение кредитов».
2. Проверьте данные: ФИО, серию и номер паспорта, ИНН.
3. Выберите тип запрета (полный или частичный).
4. Проверьте сформированное заявление и подпишите его электронной подписью (подойдёт любой вид).
5. Отправьте заявление. Срок рассмотрения — до 2 календарных дней.
6. Уведомления об установлении запрета придут от четырёх квалифицированных бюро кредитных историй (КБКИ) в личный кабинет.
7. Запрет начинает действовать на следующий день после получения первого уведомления [7].

Срок действия: бессрочно, в любой момент можно снять. **Отказ** в установлении запрета возможен, только если все четыре КБКИ не ответили на заявление в течение 2 календарных дней — в этом случае нужно подать заявление заново [7].

---

4. Сервисы мониторинга финансовых операций

4.1. Автоматический мониторинг банков (обязательный)

С **1 января 2026 года** банки обязаны проверять каждую операцию физических лиц (переводы по картам, через Систему быстрых платежей, операции с цифровыми картами и электронными деньгами) по расширенному списку признаков подозрительности. С марта 2026 года эти критерии применяются и к операциям с цифровым рублём [2].

Что происходит при блокировке:

- Банк приостанавливает перевод на срок до **2 рабочих дней (48 часов)**.
- Уведомляет клиента о приостановке через SMS, e-mail или push-уведомление с указанием причины.
- Запрашивает подтверждение добровольности операции.
- Для мгновенных платежей (СБП, электронные деньги) банк вправе сразу отказать в проведении.

Если клиент не отвечает на звонок банка или не подтверждает операцию — перевод отменяется [2].

Объём предотвращённых операций: в третьем квартале 2025 года банки предотвратили переводы без добровольного согласия клиента на сумму **3,51 триллиона рублей** [2].

4.2. Сервисы в мобильных приложениях банков (на примере СберБанк Онлайн)

В разделе «Безопасность» (значок в виде щита) доступны следующие инструменты [8]:

Сервис	Функция
Закрыть доступ к счетам	Скрыть вклады и счета в приложении и банкоматах при утечке паролей
Управление устройствами	Просмотр всех устройств, с которых был вход в приложение; удаление чужих устройств
Куда привязаны счета и карты	Просмотр всех магазинов и подписок, списывающих деньги; возможность отключить ненужные
Утечки данных	Проверка, не попали ли в сеть персональные данные (телефон, адрес) из-за утечек на сторонних сервисах
Мониторинг кредитной истории	Уведомления о ключевых изменениях, связанных с оформлением кредитов (помогает вовремя заметить попытки кредитного мошенничества)
Антивирус	Защита мобильного устройства (доступен для Android версии 16.2 и выше)

4.3. База данных ЦБ РФ

Центробанк формирует базу данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента на основе сведений от банков и МВД. Проверку проводят как банк-отправитель, так и банк-получатель («двойная заслонка») [2][9].

---

5. Порядок возврата средств при мошеннических списаниях

5.1. Обязанности банков (новые правила 2026 года)

Согласно Федеральному закону № 210-ФЗ, банки обязаны возмещать ущерб пострадавшему от мошенников при переводе денег против его воли, если они не соблюдали установленный порядок проверки и подтверждения операции. Заявление клиента рассматривается в течение **30 дней**. Доказательством для возврата служит заявление клиента; стандарт доказывания корректности действий банка пока уточняется правоприменительной практикой [1][9].

5.2. Алгоритм действий пострадавшего

Шаг 1. Свяжитесь с банком немедленно

- Заблокируйте карту или учётную запись в онлайн-банке.
- Попробуйте отменить транзакцию (если операция ещё не завершена).

- Банк отправителя свяжется с банком-получателем для блокировки счёта подозрительного лица.
- Шанс вернуть деньги выше, если обратиться в течение суток [9].

Шаг 2. Подайте заявление в полицию

- Можно подать в отделение полиции по месту жительства или онлайн на сайте МВД.
- К заявлению приложите выписку о движении средств (заказывается в банке). Чем больше подробностей, тем выше вероятность раскрытия [9].

Шаг 3. Обратитесь в суд (при необходимости)

- При сумме ущерба до 50 тыс. рублей — мировой суд.
- Свыше 50 тыс. рублей — районный суд.
- При значительных суммах — подайте заявление в прокуратуру (лично или заказным письмом).
- Срок рассмотрения дела: от двух месяцев до нескольких лет [9].

Шаг 4. Сообщите в Центробанк

- Особенно актуально, если мошенничество связано с действиями компании (например, лжебанка или лжеинвестиционной платформы).
- Обращение в ЦБ может помочь в расследовании [9].

Шаг 5. Если мошенничество массовое

- Найдите других пострадавших через соцсети и тематические форумы.
- Коллективный иск обычно привлекает больше внимания и снижает расходы на юридическое сопровождение [9].

---

6. Новые тенденции и виды кибермошенничества (2025–2026 гг.)

6.1. Дипфейк-звонки (голосовые клоны)

Мошенники с использованием искусственного интеллекта подделывают голоса родственников, друзей или публичных сотрудников Следственного комитета и МВД в режиме реального времени. Атаки максимально персонализированы и рассчитаны на мгновенную эмоциональную реакцию, отключающую критическое мышление [10][5].

Как защититься: голос и номер телефона больше не являются надёжными идентификаторами личности. Введите в семье кодовое слово или пароль для экстренных ситуаций. При любом звонке с просьбой о деньгах перезвоните человеку сами на известный вам номер.

6.2. Фишинг под видом служб доставки

Жертве приходит реалистичное SMS с официального номера магазина или сообщение в мессенджере о невозможности доставить заказ. Сообщение содержит ссылку на фишинговую страницу, которая крадёт платёжные реквизиты или устанавливает вредоносное ПО. Возможна просьба назвать код из сообщения для «подтверждения доставки» [10].

6.3. Фейковые видеоролики со знаменитостями

Мошенники создают поддельные видео с участием известных личностей, которые якобы объявляют о «государственных выплатах», акциях или розыгрышах. Видео используются для сбора персональных данных или принуждения к переводам [5].

6.4. Автоматизированные фишинговые рассылки

Адаптируются под конкретного человека на основе данных из открытых источников (соцсети, форумы, утечки баз данных). Вызывают больше доверия, чем массовые рассылки [5].

6.5. Голосовое подтверждение на начальном этапе

Злоумышленник звонит якобы из поликлиники, страховой компании, от оператора связи или госоргана, сообщает о необходимости «подтвердить данные» и просит повторить заранее заготовленную фразу (например, «Я согласен на перенос данных»). Записанный голос затем используется для подтверждения операций в системах, где внедрена голосовая биометрия [5].

6.6. Принуждение к преступлениям

Мошенники под предлогом «задания», «лёгкого заработка» или «возврата украденного» толкают жертв на тяжкие преступления: поджоги, подрывы, порчу имущества. В группе риска — пожилые люди и подростки, ищущие заработок в сети [6].

6.7. Поддельные документы, сгенерированные нейросетями

Удостоверения, справки, постановления — отличить можно по отсутствию мелких элементов, искажённому фону и несоответствиям текста [5].

---

7. Алгоритм действий при выявлении признаков мошенничества

7.1. Если поступил подозрительный звонок или сообщение

1. **Немедленно прекратите разговор.** Любой телефонный звонок с сообщением о проблемах с деньгами, счётом или документами от лица банка, полиции или иного ведомства — это мошенник [6].
2. **Не выполняйте инструкции** по снятию наличных, оформлению кредитов, сбору ценностей или передаче денег и вещей неизвестным (курьерам).
3. **Никому не сообщайте** коды подтверждения из SMS, пароли и данные доступа к банковским приложениям и личным кабинетам.
4. **Посоветуйтесь с родственниками** или лично обратитесь в отделение банка или полиции для проверки информации.
5. **Используйте «тревожную кнопку»** на портале «Госуслуги» (или в приложении Max / мобильном банке) для отправки сообщения в систему «Антифрод» [3].

7.2. Если обнаружили несанкционированное списание

1. **Заблокируйте карту/счёт** в мобильном приложении или позвоните в банк (круглосуточная горячая линия).
2. **Сообщите банку** о мошеннической операции — банк попытается отменить перевод и заблокировать счёт получателя.
3. **Сохраните доказательства:** скриншоты, SMS, записи разговоров, выписки по счёту.
4. **Подайте заявление в полицию** (102, 112 или онлайн на сайте МВД).
5. **Направьте обращение в Центробанк** (через интернет-приёмную).
6. **Подайте заявление в банк** на возврат средств — банк обязан рассмотреть его в течение 30 дней. Если банк нарушил процедуру проверки, он возмещает ущерб [1][9].

7.3. Если мошенники принуждают к незаконным действиям (угрозы, шантаж)

- **Не выполняйте незаконные указания**, даже под угрозой близким.
- **Немедленно прекратите общение**.
- **Срочно звоните в полицию** — 102 или 112 [6].

7.4. Особое внимание детям и подросткам

- Родителям: следите за кругом общения ребёнка в интернете.
- Объясните, что предложения «просто передать посылку» или «выполнить задание за деньги» — первый шаг к соучастию в преступлении.
- Создайте доверительную атмосферу, чтобы ребёнок мог рассказать о любом давлении или сомнительном предложении [6].

---

8. Подробные советы по защите от кибермошенничества

8.1. Базовые правила цифровой гигиены

- **Установите самозапрет на получение кредитов** через «Госуслуги». Это бесплатно и занимает несколько минут. Даже если мошенники получат доступ к вашим документам, они не смогут оформить на вас заём [7].
- **Подключите мониторинг кредитной истории** в мобильном приложении банка — вы будете получать уведомления о попытках оформления кредитов на ваше имя [8].
- **Проверьте утечки своих данных** через сервисы банков или специализированные сайты. Если данные утекли — смените пароли.
- **Настройте уведомления о всех операциях** по картам и счетам — SMS или push-уведомления от банка должны приходить мгновенно.
- **Используйте отдельную карту для интернет-покупок** с небольшим лимитом (или виртуальную карту с возможностью заморозки).
- **Установите лимиты на операции** в мобильном приложении банка (суточный лимит на переводы, на снятие наличных).

8.2. Защита от телефонного мошенничества

- **Заблокируйте все звонки из-за границы**, если вы не ждёте международных звонков — такая возможность предусмотрена новым законодательством [1].
- **Не отвечайте на звонки с незнакомых номеров.** Если ответили и слышите предложение от «банка», «полиции» или «госорганов» — повесьте трубку. Перезвоните сами по официальному номеру организации.
- **Помните правило:** настоящие сотрудники банков, правоохранительных органов и госслужб никогда не используют телефон для организации передачи наличных денег или ценностей [6].
- **Не называйте коды из SMS никому.** Даже если звонящий представляется сотрудником банка и говорит, что «код нужен для отмены подозрительной операции».

8.3. Защита при использовании мессенджеров и соцсетей

- **Не переходите по ссылкам из подозрительных сообщений**, даже если они пришли от имени друга (аккаунт мог быть взломан).
- **Не участвуйте в «голосованиях» и «розыгрышах»** с переходом по внешним ссылкам.
- **Проверяйте достоверность информации** о «государственных выплатах», «акциях» и «компенсациях» — официальные объявления публикуются только на сайте правительства, Госуслуг и в официальных аккаунтах ведомств.
- **Установите двухфакторную аутентификацию** на всех важных аккаунтах (Госуслуги, почта, соцсети, банк).

8.4. Что делать, если вас пытаются обмануть

- **Используйте «тревожную кнопку» на «Госуслугах»** — сообщение уходит в систему «Антифрод», которая блокирует действия мошенников на уровне банков и операторов связи [3].
- **Прервите разговор** — не пытайтесь переубедить мошенника, не вступайте в дискуссию, не следуйте инструкциям.
- **Сообщите близким** — предупредите родственников, особенно пожилых, о новой схеме. Мошенники часто звонят повторно, используя ту же легенду.
- **Подайте заявление в полицию**, даже если вы не понесли материального ущерба — это поможет в общей борьбе с мошенничеством.

8.5. Дополнительные рекомендации

- **Используйте отдельный банковский счёт для крупных сумм** (депозит, накопительный счёт), к которому не привязана карта и который не подключён к онлайн-банку для переводов.
- **Проверяйте, не оформлен ли на вас кредит** — раз в год можно бесплатно запрашивать кредитную историю в любом бюро кредитных историй.
- **Настройте «период охлаждения» для всех финансовых продуктов**, где это возможно (например, отказ от страховки в течение 30 дней после оформления кредита) [4].
- **Расскажите пожилым родственникам** о правилах безопасности. Пожилые люди — основная группа риска. Мошенники часто используют легенды о «замене полиса ОМС», «проверке счётчиков», «льготах и компенсациях».
- **Установите семейный пароль** — кодовое слово, которое вы и ваши близкие используете в экстренных ситуациях для подтверждения личности по телефону [10].

Ссылки:

[1] https://bft.ru/expert-bft/50138/

[2] https://gba.business.ru/blog/novye-kriterii-podozritelnyh-operacii-s-1-yanvarya-2026-goda-banki-massovo-blokiruyut-perevody/

[3] https://www.1tv.ru/news/2026-06-09/544421

[4] https://bankiros.ru/wiki/term/kak-rabotaet-period-ohlazdenia-po-kreditam-i-zajmam-v-curryear-godu

[5] https://iz.ru/2103113/2026-05-25/v-mvd-soobshchili-o-poddelyvanii-moshennikami-zvonkov-ot-silovykh-vedomstv

[6] https://sam.mos.ru/info/kak-deystvuyut-moshenniki-rekomendacii-po-zaschite

[7] https://www.gosuslugi.ru/help/faq/credit_lock/262252

[8] https://www.sberbank.ru/ru/person/cybersecurity/sberbank_online

[9] https://www.kp.ru/money/lichnye-finansy/pereveli-dengi-moshennikam/

[10] https://dzen.ru/a/aWerEBD7VhuwQzIA