Как защитить и заблокировать сим-карту от мошенников

Мошенники, завладев вашими персональными данными, могут попытаться заключить от вашего имени договоры на выпуск новых сим-карт — как обычных пластиковых, так и электронных (eSIM). С их помощью злоумышленники смогут перехватывать СМС-коды для подтверждения операций в банках, регистрироваться на маркетплейсах или использовать ваш номер для противоправной деятельности.

Чтобы этого не случилось, необходимо настроить защиту на нескольких уровнях: на портале Госуслуг, у мобильного оператора и в самих цифровых сервисах. В этой памятке собраны пошаговые инструкции для каждого этапа.

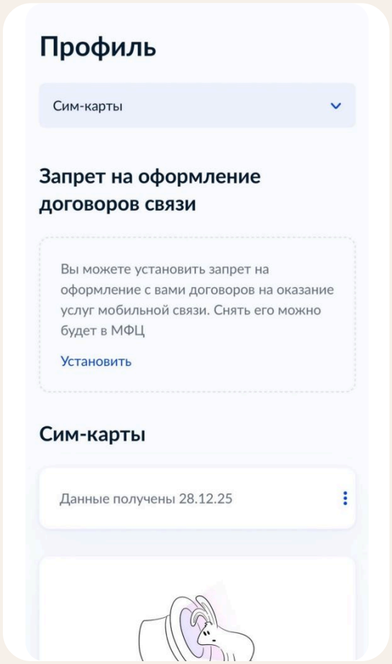


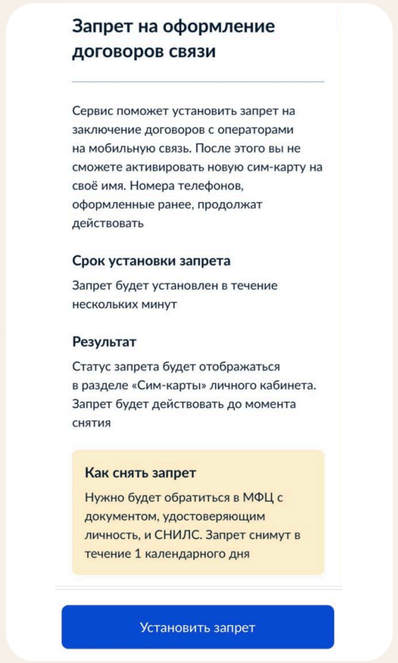
Как установить самозапрет на оформление новых сим-карт через Госуслуги

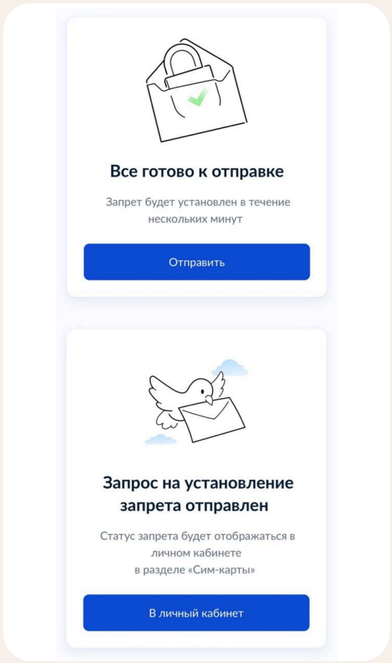
Мошенники, завладев вашими персональными данными, могут попытаться оформить на ваше имя новые сим-карты — как обычные пластиковые, так и виртуальные (eSIM). С их помощью они смогут подтверждать операции в банках, регистрироваться на маркетплейсах или даже использовать их для противоправной деятельности, например, для легализации (отмывания) денежных средств или дропперства, о чём вы можете даже не подозревать. Чтобы обезопасить себя, заранее установите запрет на оформление любых новых договоров связи от вашего имени. После включения этой функции ни один оператор не сможет зарегистрировать на вас СИМ-карту — ни в салоне, ни дистанционно.

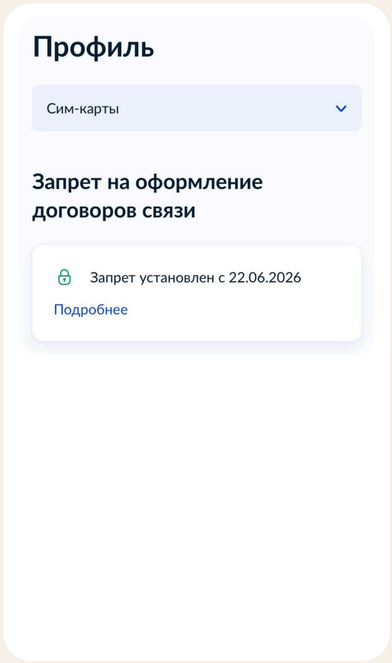
Как включить защиту:

- Зайдите в личный кабинет на портале госуслуг. Перейдите в меню «Профиль» → раздел «СИМ-карты».
- Найдите строку «Запрет на оформление договоров связи».
- Нажмите кнопку «Установить» и подтвердите действие.









Ограничение заработает во всех базах данных операторов страны в течение суток. Отменить этот запрет через личный кабинет на «Госуслугах» нельзя — это сделано специально для вашей безопасности. Если вам действительно понадобится новый номер, придется взять паспорт, СНИЛС и лично обратиться в любой центр «Мои Документы» (МФЦ). Это гарантирует, что мошенники не смогут отключить вашу защиту дистанционно.

Актуальная информация: подробности и возможные изменения в порядке установки запрета всегда можно уточнить на официальной странице помощи госуслуг.

Доверенный контакт: защитит ваш самозапрет на сим-карты

Для чего нужен доверенный контакт?

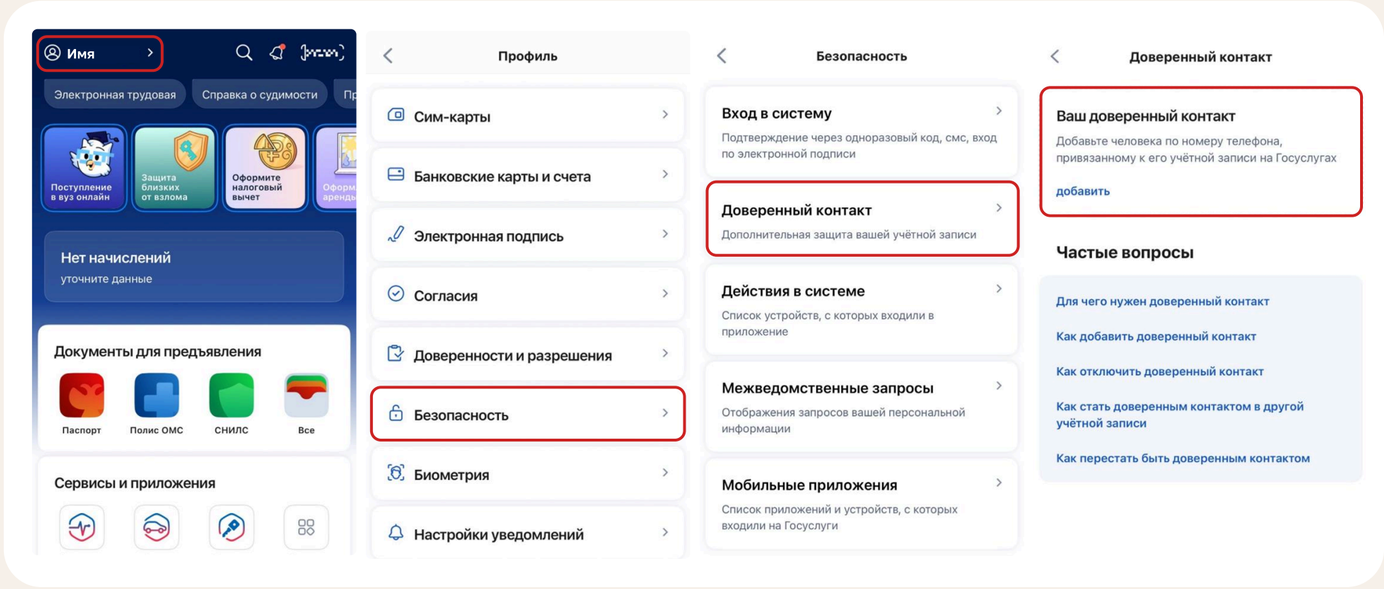
На госуслугах вы можете установить запрет на оформление новых сим-карт онлайн, без личного визита. Однако отменить этот запрет можно только при личном обращении в МФЦ с паспортом и СНИЛС — сделать это через личный кабинет на госуслугах невозможно.

Однако если злоумышленники взломают ваш личный кабинет, они смогут похитить ваши паспортные данные, СНИЛС и ИНН для их использования в других преступных схемах. Чтобы полностью исключить риск кражи личных данных, настройте функцию **«Доверенный контакт».**

Это близкий человек, который помогает восстановить доступ к вашей учётной записи. Если мошенники узнают ваш пароль и попытаются сбросить его, система не откроет им доступ сразу. На телефон вашего доверенного контакта придёт СМС с кодом подтверждения. Ваш доверенный контакт должен связаться с вами, убедиться, что вы действительно запрашиваете восстановление пароля, а затем ввести полученный код в своём личном кабинете на госуслугах. Только после этого вы получите временный пароль для входа. Без этого кода посторонние не смогут захватить контроль над вашим профилем.

Как добавить доверенного человека в профиль:

- Зайдите в личный кабинет на портале госуслуг.
- Перейдите в раздел «Профиль» → «Безопасность» → «Доверенный контакт».
- Нажмите кнопку «Добавить».
- Укажите имя и номер телефона доверенного лица (у него должен быть подтверждённый профиль на портале).
- Отправьте приглашение — оно отобразится в личном кабинете вашего близкого человека, где он должен его принять.



Что нужно обсудить с доверенным контактом?

Доверенный контакт не имеет доступа к вашим документам, персональным данным и не может управлять вашими услугами. Данная функция используется исключительно для подтверждения сброса пароля.

Договоритесь со своим доверенным контактом, чтобы он **никогда не одобрял запросы автоматически.** Если ему в личный кабинет пришло уведомление о восстановлении вашего доступа, он должен сначала связаться с вами по телефону. Продолжать операцию можно только после того, как вы лично подтвердите, что действительно восстанавливаете пароль.

Официальные инструкции портала

Подробнее о работе сервиса можно прочитать в справке госуслуг:

- Для чего нужен доверенный контакт
- Как добавить доверенный контакт



Услуги операторов связи для защиты сим-карты от мошенников

Защиту можно и нужно усилить на стороне мобильного оператора. У всех крупных операторов есть внутренние алгоритмы и услуги, которые защищают ваш номер на сетевом уровне, ещё до того, как вызов или СМС дойдут до вашего телефона.

Что обычно предлагают операторы для вашей безопасности:

- **Блокировка спам-звонков и подозрительных номеров:** автоматическая фильтрация входящих вызовов по базам оператора и жалобам абонентов. Антифрод-системы в реальном времени проверяют номера и сбрасывают звонки с поддельных или мошеннических номеров.
- **Защита от фишинговых ссылок:** блокировка перехода на мошеннические сайты при использовании мобильного интернета (работает на сетевом уровне).
- **Запрет на замену сим-карты без подтверждения:** при попытке перевыпуска номера требуется дополнительный код (приходит на электронную почту или в приложение). Это не даёт мошенникам получить вашу сим-карту даже при наличии поддельных документов.
- **Отключение международных звонков:** полный запрет входящих вызовов из-за границы, что отсекает значительную часть мошенников, использующих подставные международные номера.
- **Запрет по доверенности:** настраивается при личном обращении к оператору. После этого любые важные действия с номером (замена сим-карты, смена тарифа) будут возможны только при подтверждении личности по паспорту.
- **Двойная проверка при входе:** доступ к личному кабинету и сервисам оператора защищён дополнительными уровнями аутентификации.
- **Временный запрет на СМС от банков:** если вы меняете сим-карту, оператор на некоторое время отключает доставку банковских СМС. Это не даёт мошенникам перехватить коды подтверждения, даже если они завладели вашим номером.
- **Период охлаждения:** временная блокировка интернета и СМС, которая автоматически срабатывает, например, при возвращении из поездки за границу (в том числе из отпуска) или после долгого отсутствия в сети. Голосовые звонки при этом остаются доступны. Чтобы снять ограничение досрочно, можно перейти по ссылке из СМС.
- **Добровольная заморозка номера:** если вы уезжаете надолго и хотите сохранить номер, но при этом защитить его от списаний или кражи, можно оформить временную блокировку. Услуга доступна в приложении оператора, на сайте или при личном обращении. Обычно она бесплатна первые дни, затем может взиматься небольшая плата за сохранение номера.
- **Проверка устройства на угрозы:** сканирование телефона на наличие вредоносного ПО и фишинговых приложений (встроено в приложения некоторых операторов).

На примере оператора «Билайн»: как подключить основные услуги защиты

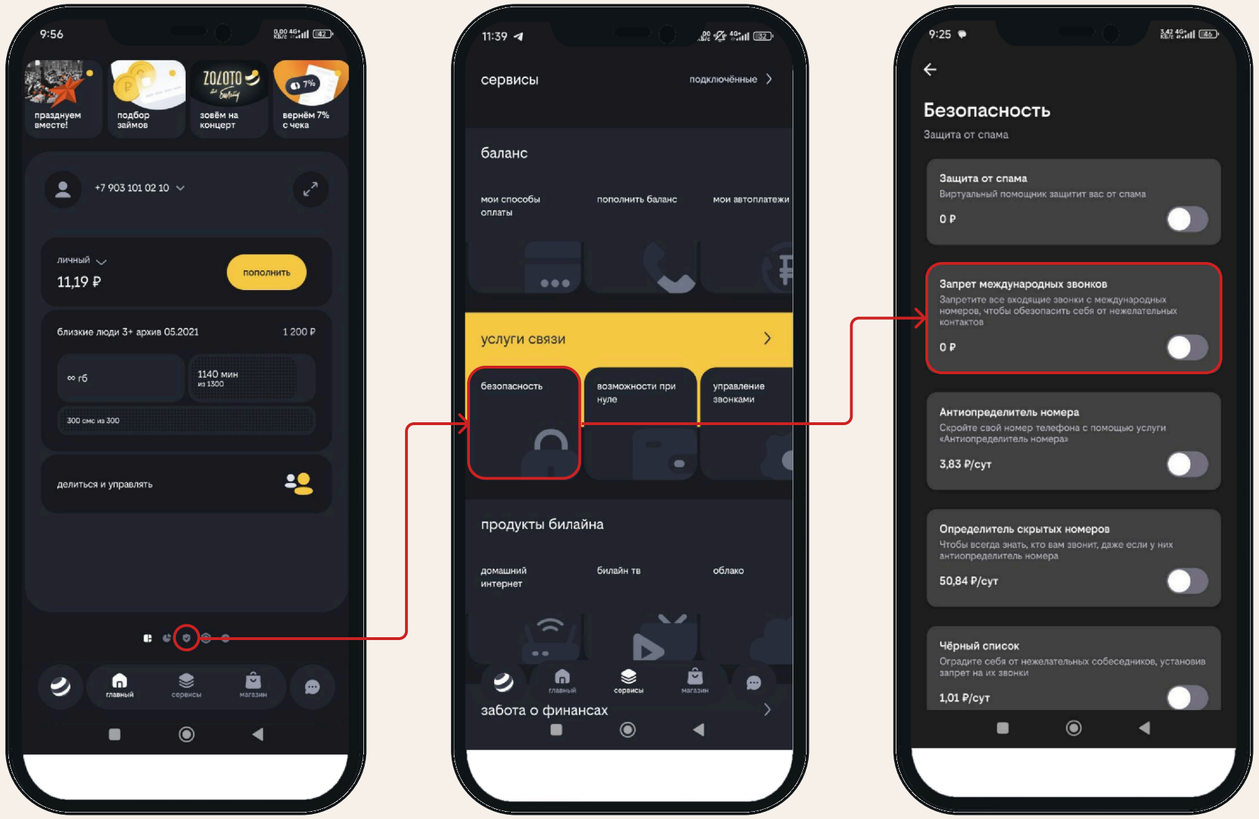
Все три услуги подключаются в мобильном приложении «Мой Билайн» в разделе «Услуги» или «Безопасность». Это пример для «Билайна» — у других операторов названия и порядок действий могут отличаться, но суть обычно та же.

1. Защита от международных звонков

Мошенники часто звонят из-за границы, подставляя номера, похожие на российские. Если вы не ждёте звонков из-за рубежа, лучше отключить их совсем: это остановит значительную часть мошеннических вызовов.

Как подключить:

- в мобильном приложении «Мой Билайн» в разделе «Услуги» или «Безопасность» найдите переключатель «Запрет международных вызовов» и активируйте его;
- или позвоните на горячую линию «Билайна» и попросите оператора отключить входящие вызовы из-за границы.



Важно: услуга бесплатная. Если у вас есть родственники за границей, имейте в виду, что запрет блокирует все входящие международные звонки — заранее предупредите близких о других способах связи.

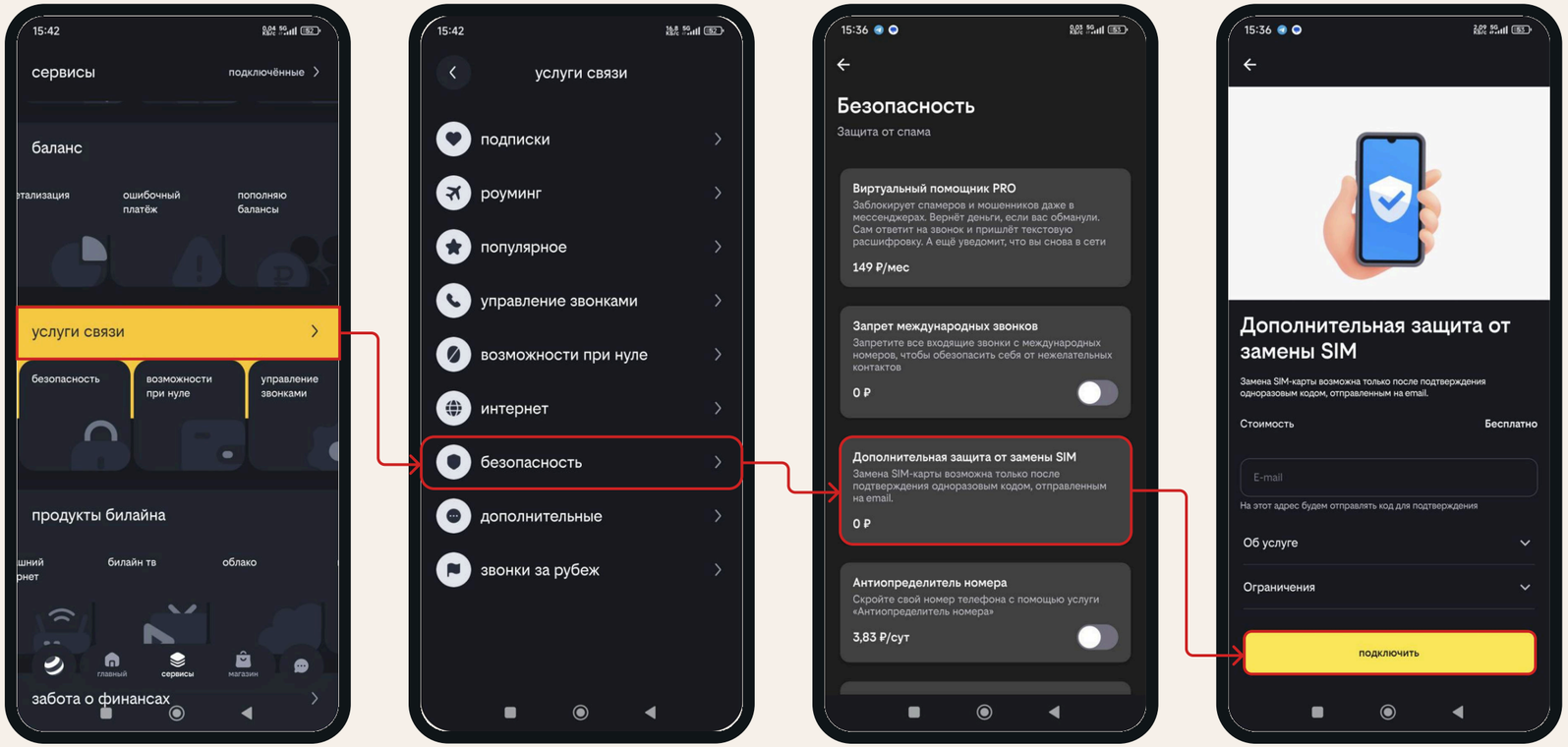
На примере оператора «Билайн»: как подключить основные услуги защиты

2. Защита от замены сим-карты

Эта услуга не даёт мошенникам получить вашу сим-карту, даже если они придут в офис с поддельными документами. При попытке замены сим-карты на вашу электронную почту приходит одноразовый код подтверждения — без него сотрудник не имеет права выдать новую карту.

Как подключить:

- откройте мобильное приложение «Мой Билайн»
- перейдите в раздел «Услуги» → «Безопасность»
- найдите услугу «Дополнительная защита от замены сим-карты» и активируйте её.



Важно: услуга бесплатна для всех абонентов. При подключении нужно указать электронную почту, на которую будет приходить код подтверждения.

На примере оператора «Билайн»: как подключить основные услуги защиты

3. Виртуальный помощник

«Виртуальный помощник» — это антифрод-сервис, который блокирует спам и мошеннические звонки, в том числе в мессенджерах. Базовая версия подключена по умолчанию для всех абонентов бесплатно.

Что делает базовая версия:

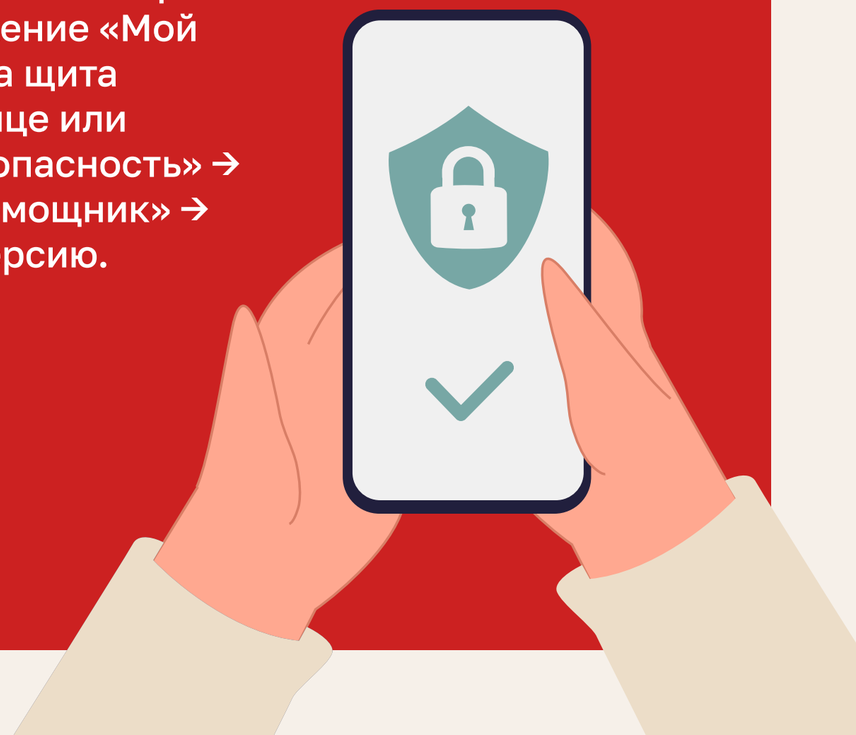
- Блокирует спам-звонки и подозрительные вызовы.
- Блокирует СМС с кодами авторизации во время разговора, чтобы вы случайно не продиктовали их мошеннику.
- Защищает от мошеннических звонков в мессенджерах (эту функцию нужно активировать отдельно в приложении).

PRO-версия (платная опция):

- Помощник может принять звонок, если вам неудобно говорить, записать разговор и отправить аудио в приложение и Telegram.
- Текстовая расшифровка пропущенных вызовов.
- Выбор голоса помощника.
- Гарантия возврата денег по двум документам в случае успешной атаки мошенников.

Как подключить и настроить:

- Базовая версия уже работает — ничего делать не нужно.
- Чтобы активировать защиту в мессенджерах, зайдите в приложение «Мой Билайн» и предоставьте необходимые доступы.
- Для подключения PRO-версии: откройте приложение «Мой Билайн» → иконка щита на первой странице или раздел «Моя безопасность» → «Виртуальный помощник» → выберите PRO-версию.

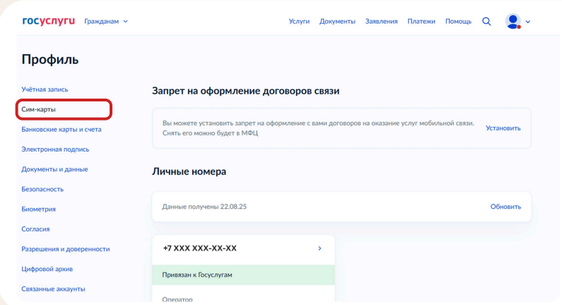


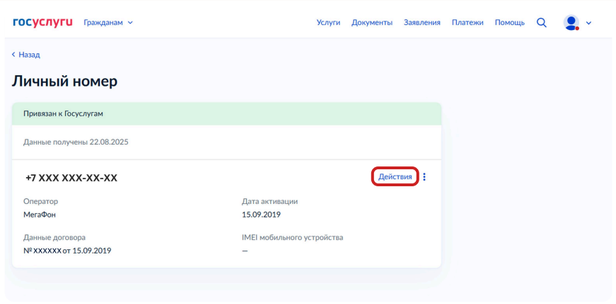
Как заблокировать сим-карту при потере или краже телефона

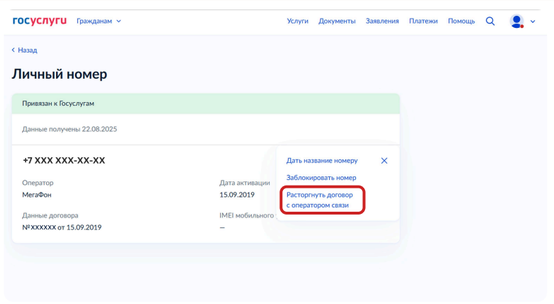
Если вы потеряли телефон, его украли или вы вдруг нашли в своём списке на портале госуслуг незнакомый номер — действовать нужно быстро. Неиспользуемые или чужие сим-карты нужно закрывать сразу, чтобы мошенники не использовали их для подтверждения операций в онлайн-банках. Избавиться от нежелательного номера можно тремя простыми способами.

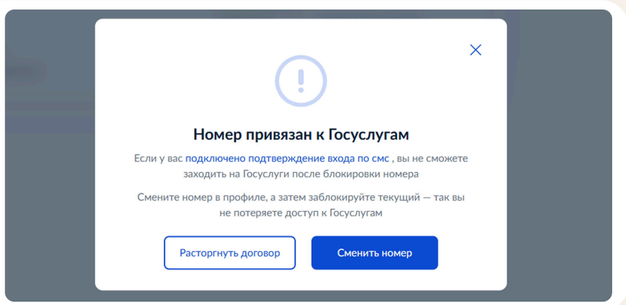
Способ 1 Онлайн через портал госуслуг

1. Перейдите в меню «Профиль» → раздел «Сим-карты».
2. Выберите подозрительный или ненужный номер из списка.
3. Нажмите «Расторгнуть договор с оператором связи» (или попросите временную блокировку у Робота Макса).









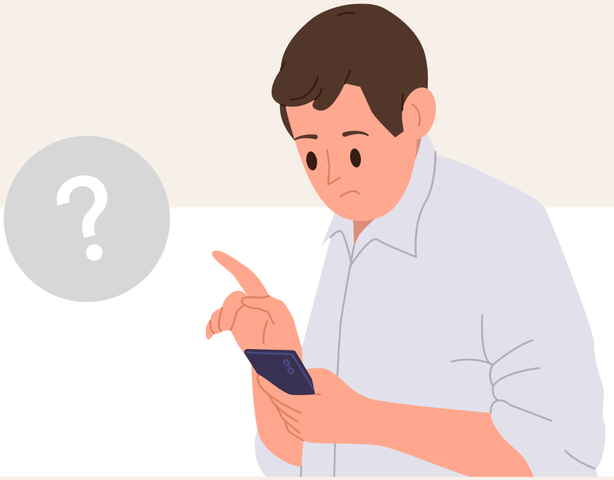
Способ 2 Обратиться к оператору связи (любым удобным способом)

- **В мобильном приложении:** авторизуйтесь, найдите раздел управления номером и выберите блокировку (временную или постоянную).
- **По телефону горячей линии:** наберите номер поддержки (он указан на официальном сайте или в приложении). Сообщите, что потеряли карту и её нужно заблокировать, назовите паспортные данные и кодовое слово (если оно установлено).
- **Лично в салоне связи:** возьмите с собой паспорт, зайдите в ближайший офис вашего оператора и попросите сотрудника заблокировать номер.

Помните важную разницу:

если телефон просто потерялся, но вы хотите сохранить свой номер на будущее — просите именно временную блокировку. А вот если вы увидели на портале госуслуг чужую сим-карту, которую никогда не покупали, — сразу оформляйте расторжение договора, чтобы полностью снять с себя ответственность за этот номер и защититься от возможных неприятностей, связанных с его использованием.

Почему важно отвязать номер телефона от всех сервисов после смены сим-карты



Это самое главное правило, про которое почти все забывают. Физически заблокировать сим-карту недостаточно. Если вы перестали пользоваться номером, он всё ещё остается в базах данных мессенджеров, банков и сайтов. Через полгода оператор имеет право передать этот номер новому абоненту. Если вы не уберете невостребованный телефон из настроек, новый владелец вашей бывшей сим-карты сможет нажать кнопку «Забыли пароль?» и зайти в ваши аккаунты.

Где нельзя оставлять старый номер

- **Банковские приложения** — зайдите в настройки каждого мобильного банка, где использовался номер, и смените контактный телефон для входа, СМС-оповещений и подтверждения операций. Если доступ к приложению уже потерян — обратитесь в отделение банка с паспортом.
- **Госуслуги** — авторизуйтесь в личном кабинете, перейдите в раздел «Настройки» или «Профиль» и измените номер телефона. Если старый номер недоступен и войти не получается — потребуется личное обращение в МФЦ с паспортом и СНИЛС для восстановления доступа.
- **Видеохостинги и медиа** — проверьте настройки аккаунта на всех платформах, где вы загружали видео или оставляли комментарии. Смените привязанный номер телефона или удалите его, если он использовался только для входа.
- **Маркетплейсы и интернет-магазины** — проверьте настройки профиля и способы доставки на всех популярных онлайн-площадках, где вы совершали покупки. Удалите старый номер из контактных данных, чтобы курьеры и службы доставки не звонили по недействительному телефону, а мошенники не могли восстановить пароль.
- **Мессенджеры и приложения для звонков** — в каждом используемом мессенджере найдите функцию «Изменить номер» в настройках аккаунта. Ваши чаты и контакты перенесутся на новый номер, а на старом все сессии автоматически завершатся. Дополнительно проверьте список привязанных устройств и завершите сессии, если номер остался на старых гаджетах.
- **Социальные сети** — обновите номер в настройках безопасности всех соцсетей, где он используется для входа или двухфакторной аутентификации.
- **Почтовые сервисы** — зайдите в настройки каждого почтового ящика, который вы используете, и привяжите новый номер для восстановления доступа. Если к почте привязан старый номер, мошенники могут через него сбросить пароль и получить доступ к вашей переписке, а через неё — и ко многим другим аккаунтам.
- **Онлайн-сервисы и подписки** — проверьте, где ещё вы использовали номер для входа: стриминговые платформы, облачные хранилища, сайты бронирования отелей и авиабилетов, приложения каршеринга и такси. Удалите старый номер из контактной информации везде, где это возможно.