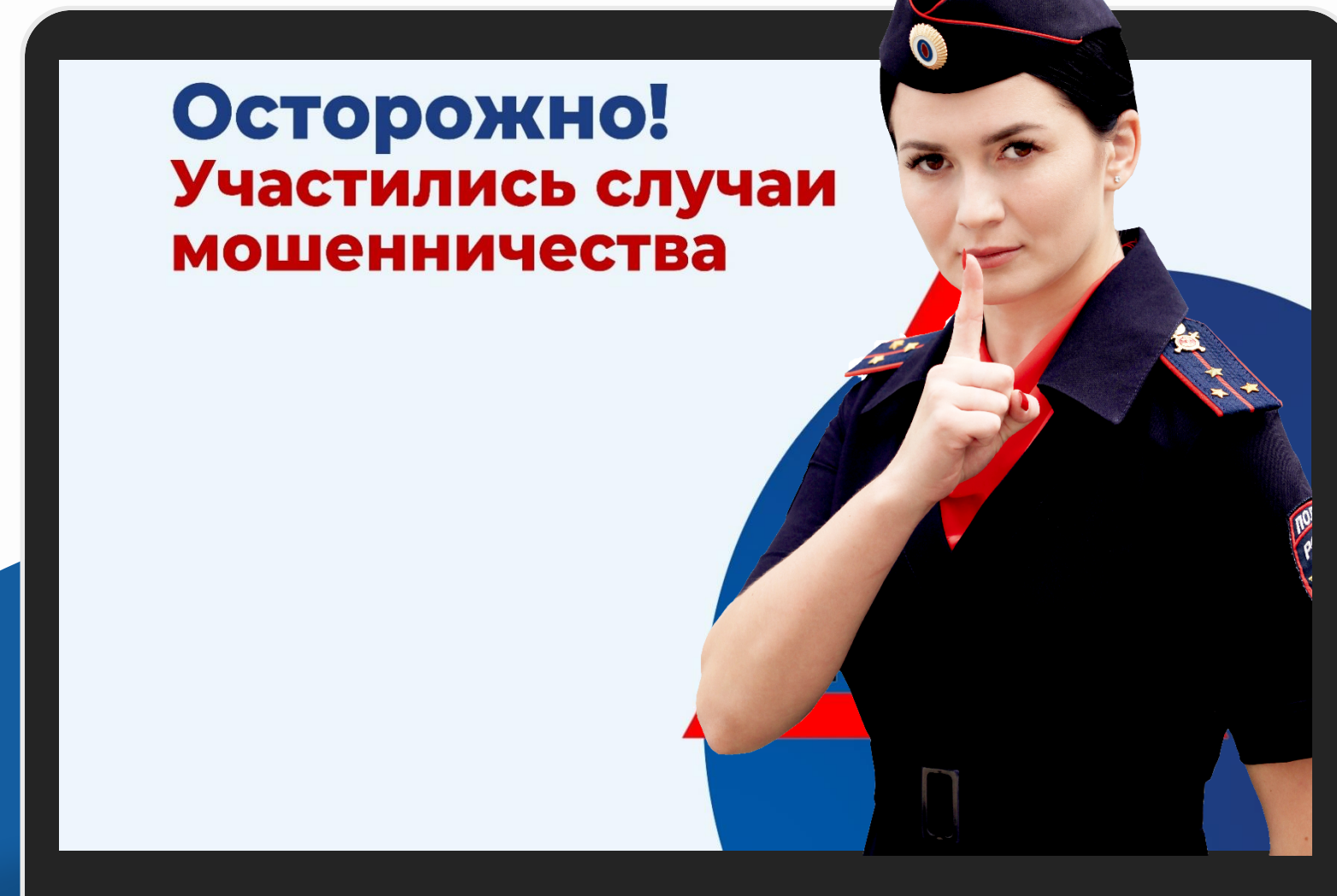




МУ МВД России «Иркутское»

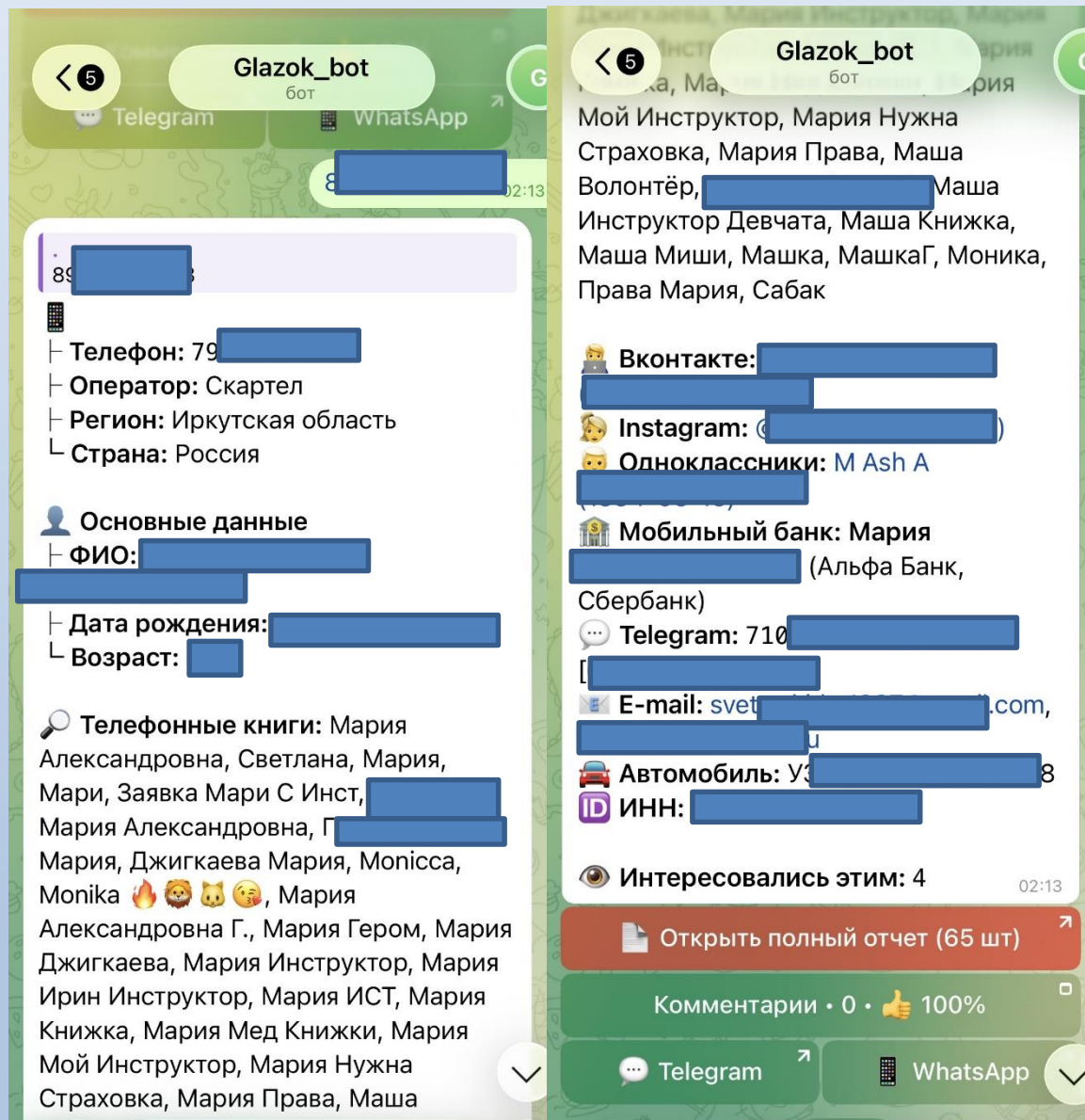
СТРУКТУРА МОШЕННИЧЕСТВ И ПРАКТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ





Структура мошенничества по средствам связи:

1. ПОДГОТОВКА



- А) Анализ открытых источников информации (проверка по ботам, анализ открытых страниц в социальных сетях, поиск родственников, увлечений, объявлений, отзывов на сайтах);**
- Б) Составление личного портрета жертвы, выявление слабых мест, подходов и поводов для общения;**
- В) Построение схемы обмана с несколькими вариантами поведения;**
- Г) Анализ выявленных платежных систем жертвы и подбор способа вывода денежных средств;**
- Д) Поиск средств связи для контакта с гражданином;**
- Е) Поиск «Дропа» для вывода похищенных средств.**



Структура мошенничества по средствам связи:

2. Контакт с гражданином и вход в доверие:

Создание повода и почвы для входа в доверие (Поступление звонка, в ходе которого представляются различными службами или организациями для создания или входа в ситуацию).

Инициативный звонок гражданина по высланным телефонным номерам (Госуслуги, тех. поддержка банков, организаций)

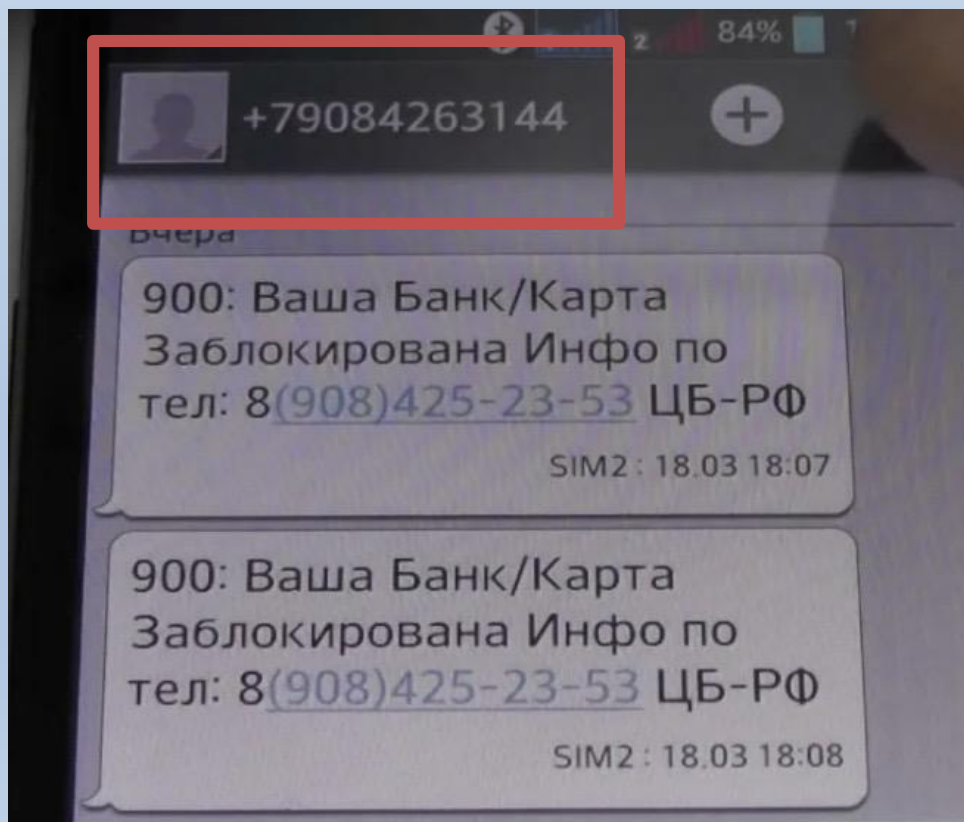
Формирование эмоционального фона
(Уменьшение времени на принятие решения, внушение страха под угрозой ответственности, внушение доверия)

Дистанционная помощь с переключением на специалистов других отделов или ведомств.

Попытка доказать реальность возникшей угрозы или обстоятельств

Предоставление документов в электронной или печатной форме (Доверенности, фотографии, удостоверения, декларации)

Видео звонок или общение в мессенджерах.
(сотрудники силовых ведомств, фирм, инвестиционных организаций)





Структура мошенничества по средствам связи:

3. Манипуляция:

Производится акцент на процессах и терминах, в которых гражданин не разбирается.

На данном этапе ведется пояснение о процессах или терминах, которые были выдуманы или искажены мошенником с целью донести необходимость в работе с банковскими счетами, картами, переводами, кредитами, обналичиванием, передачей, декларацией денежных средств.

Получение доступа к денежным средствам.

Установка сторонних приложений, которые предоставляют доступ к управлению телефоном, трансляции рабочего экрана. Установка кустарных приложений, переход по разработанным мошенниками сайтам. ПЕРЕДАЧА КОДОВ ИЗ СМС-СООБЩЕНИЙ.

Самостоятельный перевод денежных средств.

Осуществление переводов денежных средств на высланные мошенниками банковские реквизиты, номера телефонов, внесение наличных через банкомат на указанные реквизиты.

Затягивание времени и поддержание легенды на максимально возможный период.

Данный этап необходим для успешного вывода похищенных денежных средств до обращения гражданина в правоохранительные органы, а также для продления пользования имеющимися средствами связи и банковскими реквизитами.



Структура мошенничества по средствам связи:

4. Вывод денежных средств:

Осуществление подбора банка получателя (используются актуальные связки)

Получение денежных средств, решение проблем, связанных с их блокировкой в банке.

Трансфер денежных средств до организаторов мошеннической схемы.

После перевода или внесения наличных денежных средств на банковские реквизиты мошенников, средства, как правило, попадают на банковские карты или счета граждан, которые ранее оформили на свои данные платежные реквизиты и продали их третьим лицам. В течение нескольких дней денежные средства доходят до организаторов мошеннической схемы в различных формах. (криптовалюта, наличность, банковская карта)





Анализ примера из практики

1. **Мошенники изучили гражданина**, а именно установили абонентский номер, область проживания, ФИО, возраст, финансовое обеспечение, кредитную историю. Изучили местность и расположение отделений банков.
2. **Были созданы условия и почва для входа в доверие**. (поступил телефонный звонок, представились сотрудником поликлиники, сообщили, что необходимо пройти диспансеризацию. Попросили назвать ФИО, дату рождения. Далее голос звонящего был заменен на автоответчик, было сообщено, что голосовая биометрия окончена.)
3. **Далее поступила «дистанционная помощь» из государственного органа с переходом в мессенджеры**. (Спустя время поступил звонок от министерства цифрового развития сообщили, что составлена доверенность на гражданина, состоящего в реестре экстремистов. Общение перешло в конференцию «VK», где включалась демонстрация экрана в процессе входа в Госуслуги. Далее переход на сотрудника «Росфинмониторинга», который сообщил, что необходимо выполнять конкретный алгоритм действий.)
4. **Навязана опасность промедления в действиях и страх ответственности перед органами ФСБ посредством видео и аудио звонков**. (общение перешло в «zoom», где к разговору подключился сотрудник ФСБ. Далее гражданина убедили написать расписку о не разглашении государственной тайны, отправить фотографии в мессенджере «телеграмм». Сообщили, что телефон последующих 2 дней будет проверяться на предмет взаимодействия с Украиной, каждый час нужно было отписываться о том что гражданин сейчас делает.)
5. **По закреплению доверия мошенники перешли к этапу манипуляции одновременно с доступом к устройству жертвы**. (убедили приобрести сотовый телефон на базе «андроид» и новую sim-карту, через который мошенники проинструктировали о задаваемых вопросах в банке, в целом что необходимо, и как себя вести в банке, чтобы снять денежные средства в общей сумме 2 млн рублей)
6. **Хищение и вывод денежных средств**. (Через «zoom» гражданин направился к банкомату, где сделал переводы посредством NFC, установив при этом приложение «ЦБ». После переводов мошенники убедили гражданина оформить кредит на сумму около 1 млн рублей, однако получить денежные средства не удалось так, как сотрудниками банка был выявлен факт воздействия мошенников)

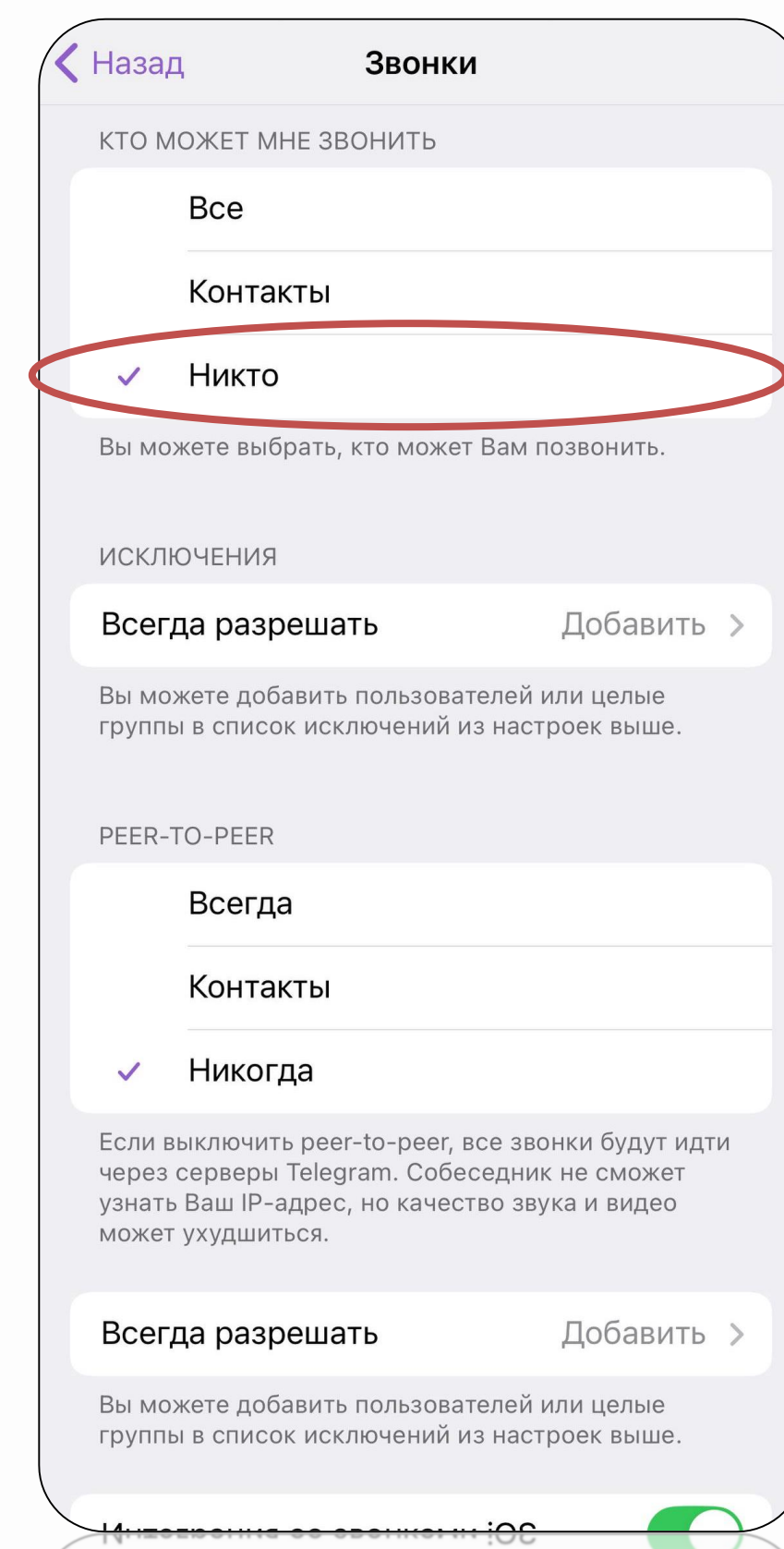
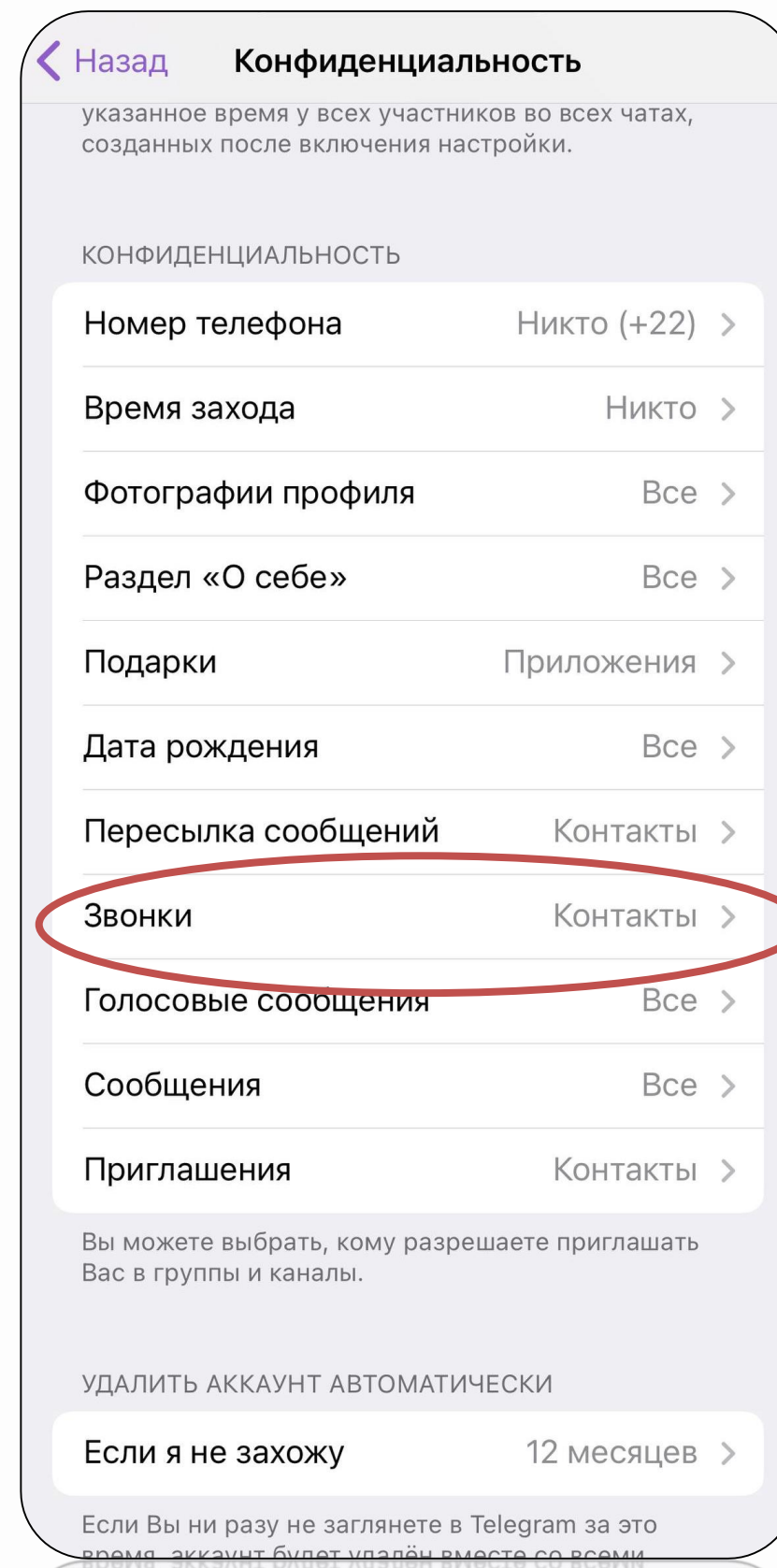
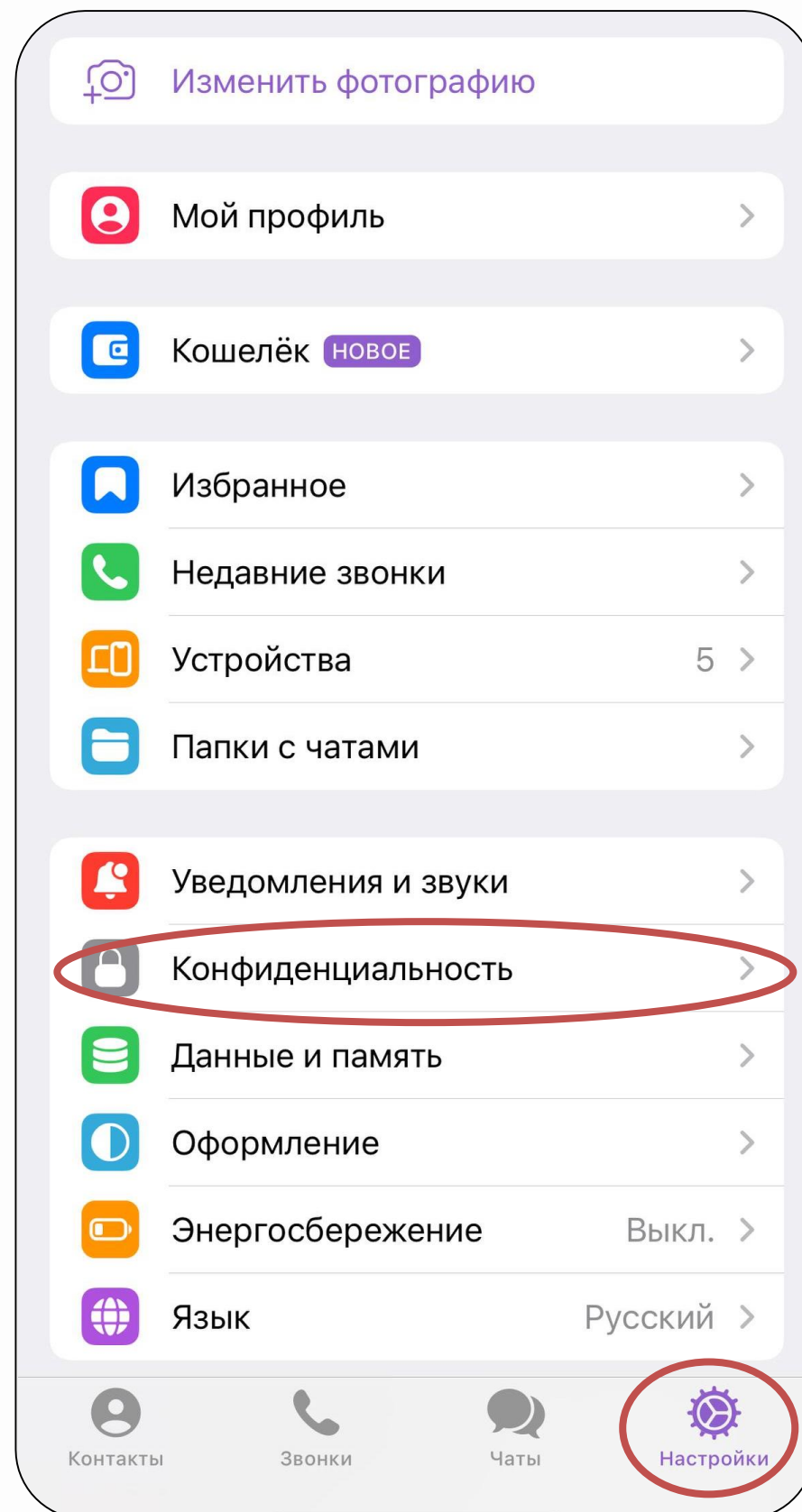
Защита от звонков в Telegram

Зайдите в Настройки → Конфиденциальность и безопасность → Номер телефона.

Выберите «Кто может видеть мой номер» → «Мои контакты» или «Никто».

В том же разделе «Конфиденциальность и безопасность» найдите пункт «Звонки».

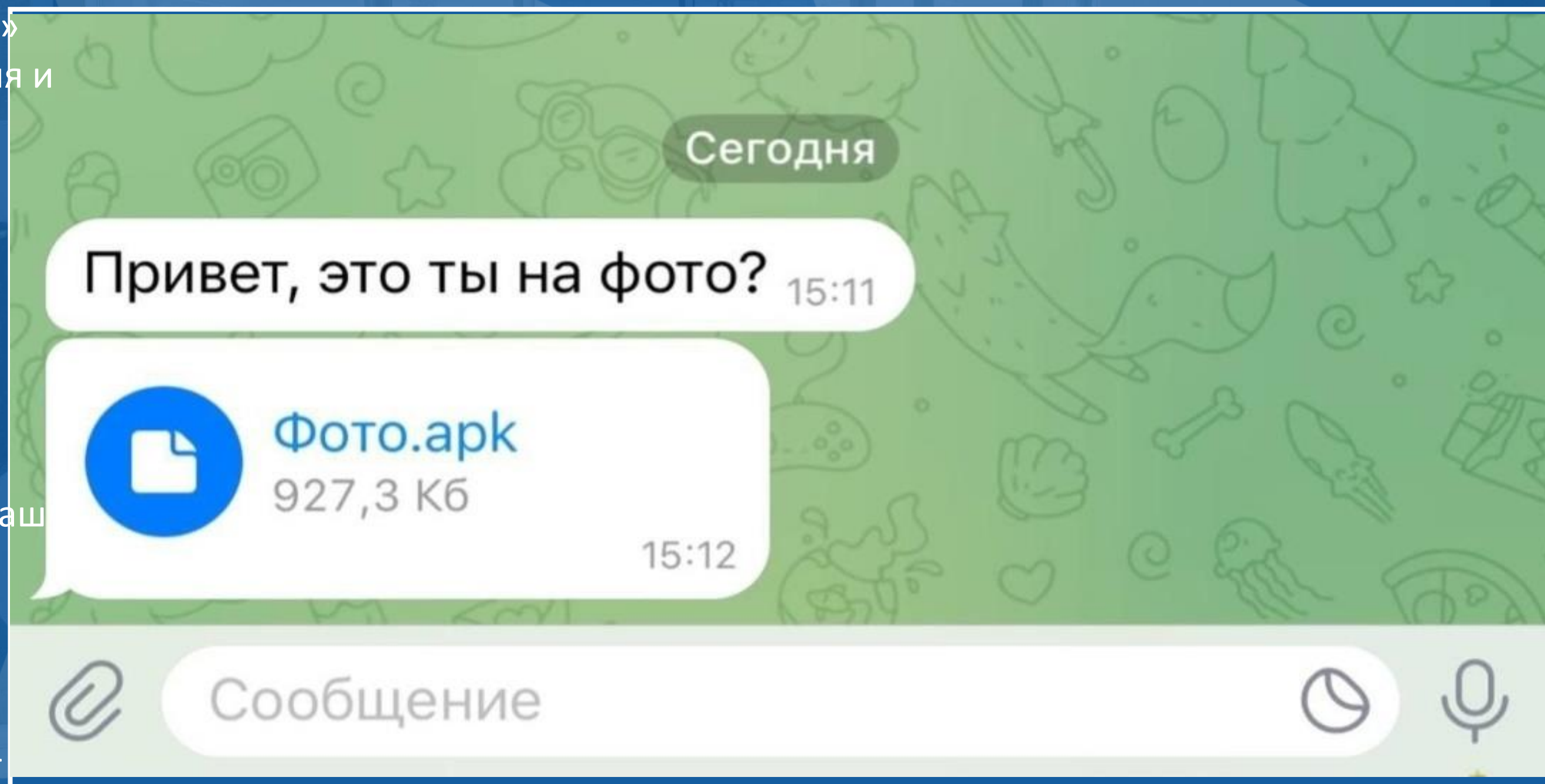
Установите «Кто может звонить мне» → «Мои контакты». Все звонки от незнакомых номеров будут автоматически отклоняться.



Новый вид мошенничества в мессенджерах

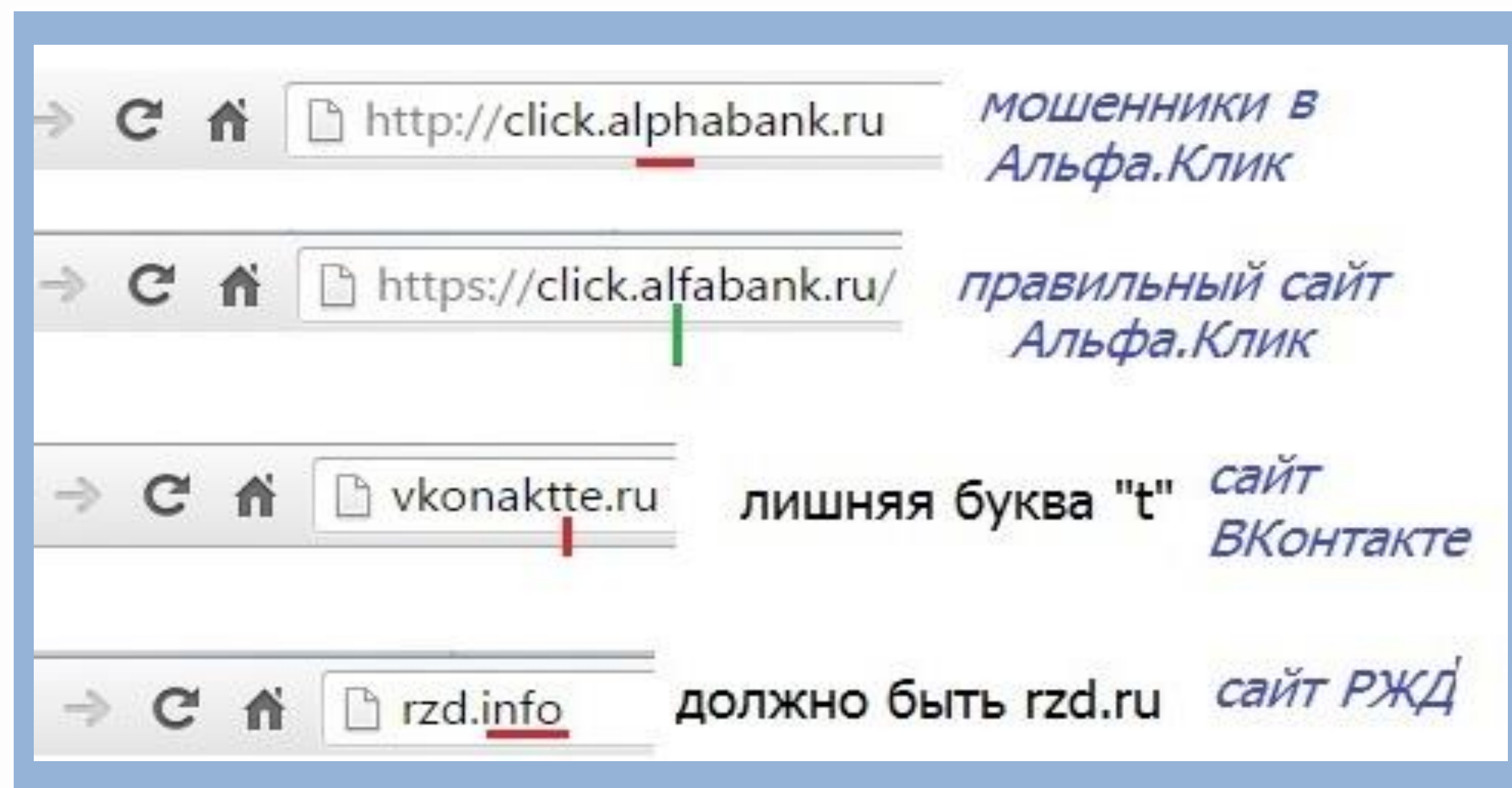
Арк – это формат файла, используемый операционной системой «Андроид» для распространения и УСТАНОВКИ мобильных приложений.

При переходе по данному файлу на ваш мобильный УСТАНОВЛИВАЕТСЯ приложение или настройка по переадресации смс-сообщений, в которых содержатся коды.



ПРИ ПРОВЕРКЕ ОБРАТИТЕ ВНИМАНИЕ НА ДОМЕН (ИМЯ) САЙТА:

- ▶ Мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «l» (onL1ne вместо onLine);
- ▶ Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru);
- ▶ В некоторых случаях для написания домена используются буквы похожие на латинские из алфавита другого языка;
- ▶ Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU



ПРОВЕРКА НА МОШЕННИЧЕСТВО

[Сайты](#)[Соцсети](#)[Телефоны](#)

**Проверьте продавца / покупателя при помощи
различных сервисов. Например на сайте
«Доверие в сети»**

Как уберечь ребенка от преступных посягательств в цифровой среде



Настроить безопасный поиск в поисковых системах, который скрывает из результатов нежелательный контент (взрослые изображения, опасные сайты). При этом сохраняется доступ к образовательным ресурсам.



Использовать приложения для родительского контроля — они позволяют отслеживать, какие сайты посещает ребёнок и какие приложения использует, блокировать нежелательный контент.

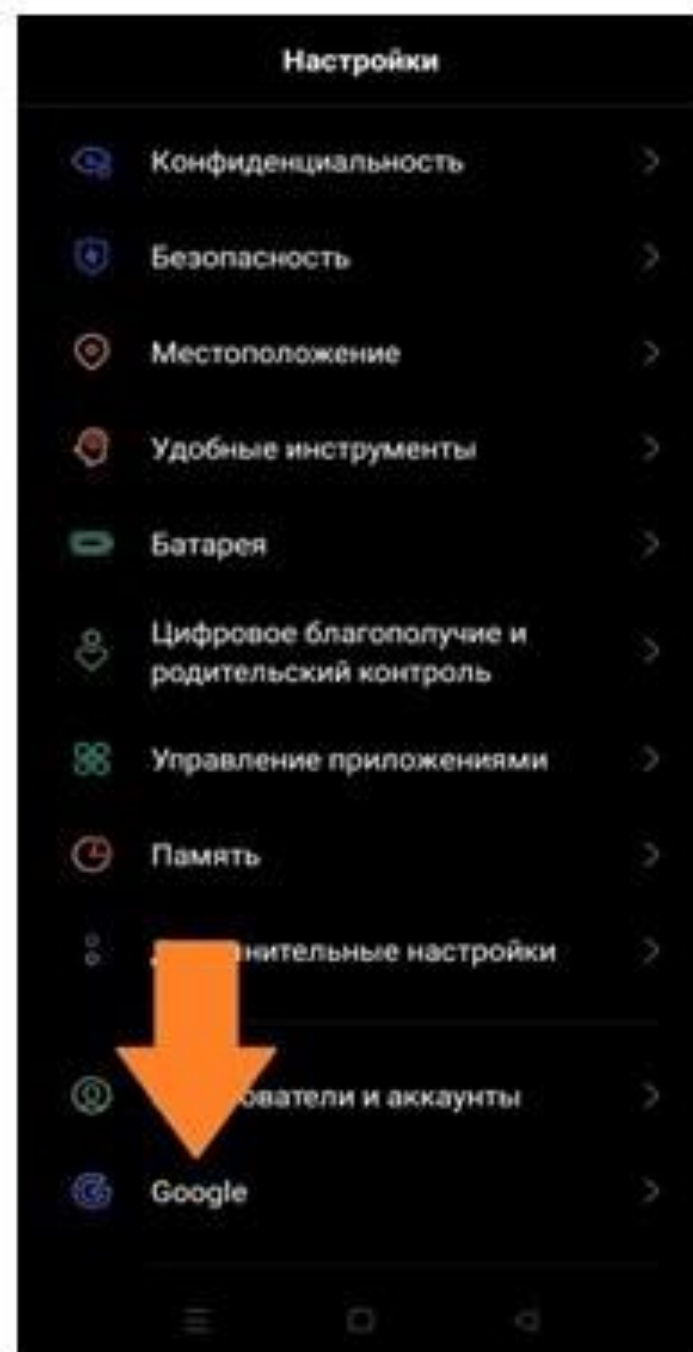


**Уделяйте больше внимания своему ребенку.
Чаще разговаривайте с ним, чтобы он делился с Вами о своем окружении, как прошел его день и внимательно следите за изменением в его поведении**

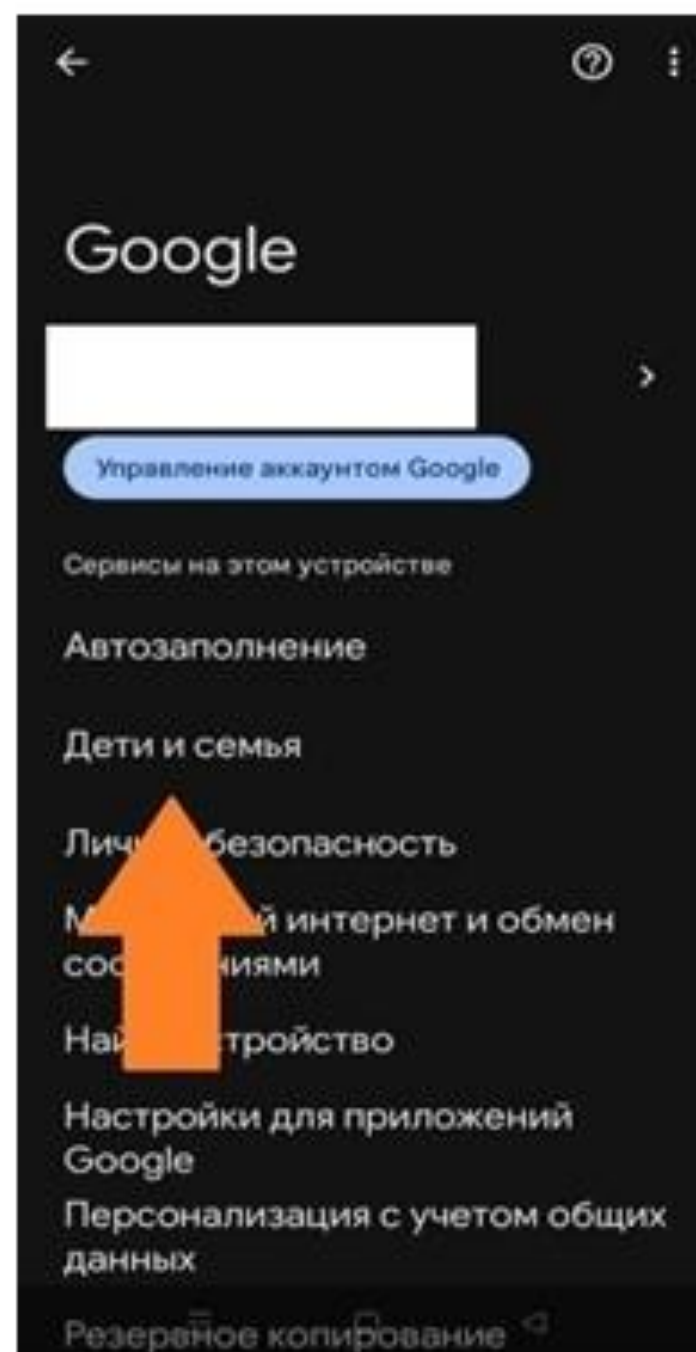
Установите дома родительский контроль на телевизор и его аккаунты в интернете.

1. Откройте «Настройки» на устройстве ребенка.

2. Выберите «Google»



3. «Дети и семья»



4. «Родительский контроль»



Установите дома родительский контроль на телевизор и его аккаунты в интернете.

Нажмите «Приступить»

Google

Настройте родительский контроль

Вы зададите возрастные ограничения, настройки конфиденциальности и время использования для этого устройства и аккаунта Google своего ребенка.



↓

Приступить

Выберите аккаунт ребенка или создайте новый.

Google

Вход

Используйте аккаунт Google.
[Узнать больше об использовании аккаунта](#)

Телефон или адрес эл. почты

Забыли адрес электронной почты?

Создать аккаунт

Далее

Войдите в свой «родительский»

Google

Аккаунт родителя

Переход в приложение "Family Link"

Войдите в аккаунт Google, с помощью которого вы будете управлять аккаунтом вашего ребенка.

Телефон или адрес эл. почты

Забыли адрес электронной почты?

Прежде чем начать работу с приложением "Family Link", вы можете ознакомиться с его политикой конфиденциальности и условиями использования.

Далее

Схемы взлома и защита от них



1. Звонок от работника сотового оператора

1. Поступает телефонный звонок от оператора сотовой связи, сообщают что необходимо продлить срок действия SIM-карты или обновить паспортные данные.

В это время мошенники, зная абонентский номер жертвы, на сайте «Госуслуги» открывают вкладку: «Восстановление пароля». Указывают номер жертвы и ждут когда им сообщат код из SMS.

2. После чего, в целях подтверждения личности или под другим предлогом просят сообщить / продиктовать SMS-код, поступивший на телефон с портала «Госуслуги»

Для личных кабинетов, где установлен вход на портал по SMS-коду, мошенники просят повторно сообщить код, якобы первый код не действителен и не проходит. **На самом деле повторно приходит КОД для изменения номера телефона.**

The screenshot shows the Gosuslugi website interface. At the top is the 'госуслуги' logo. Below it is the heading 'Восстановление пароля'. There is a text input field labeled 'Телефон / Email' containing the number '89000000000'. Below this is another 'госуслуги' logo. Underneath is the heading 'Изменение номера телефона +7 924'. At the bottom is a text input field labeled 'Новый номер телефона' with a placeholder '+7 () - - -'.

Как обезопасить личный кабинет от взлома?

01

Никому не сообщайте код из SMS-сообщения, поступившего с портала «Госуслуги»;

02

Настроить двухэтапную аутентификацию;

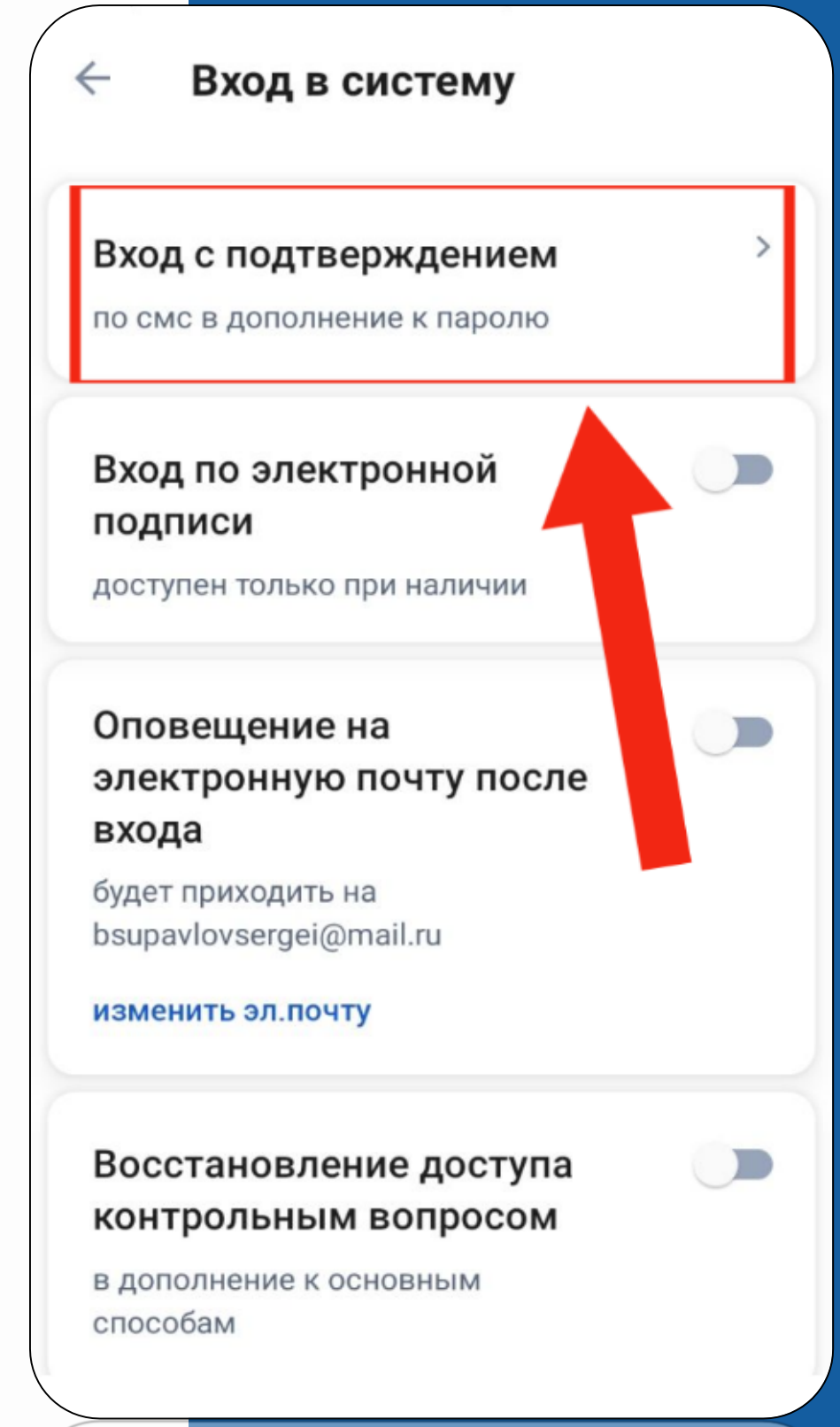
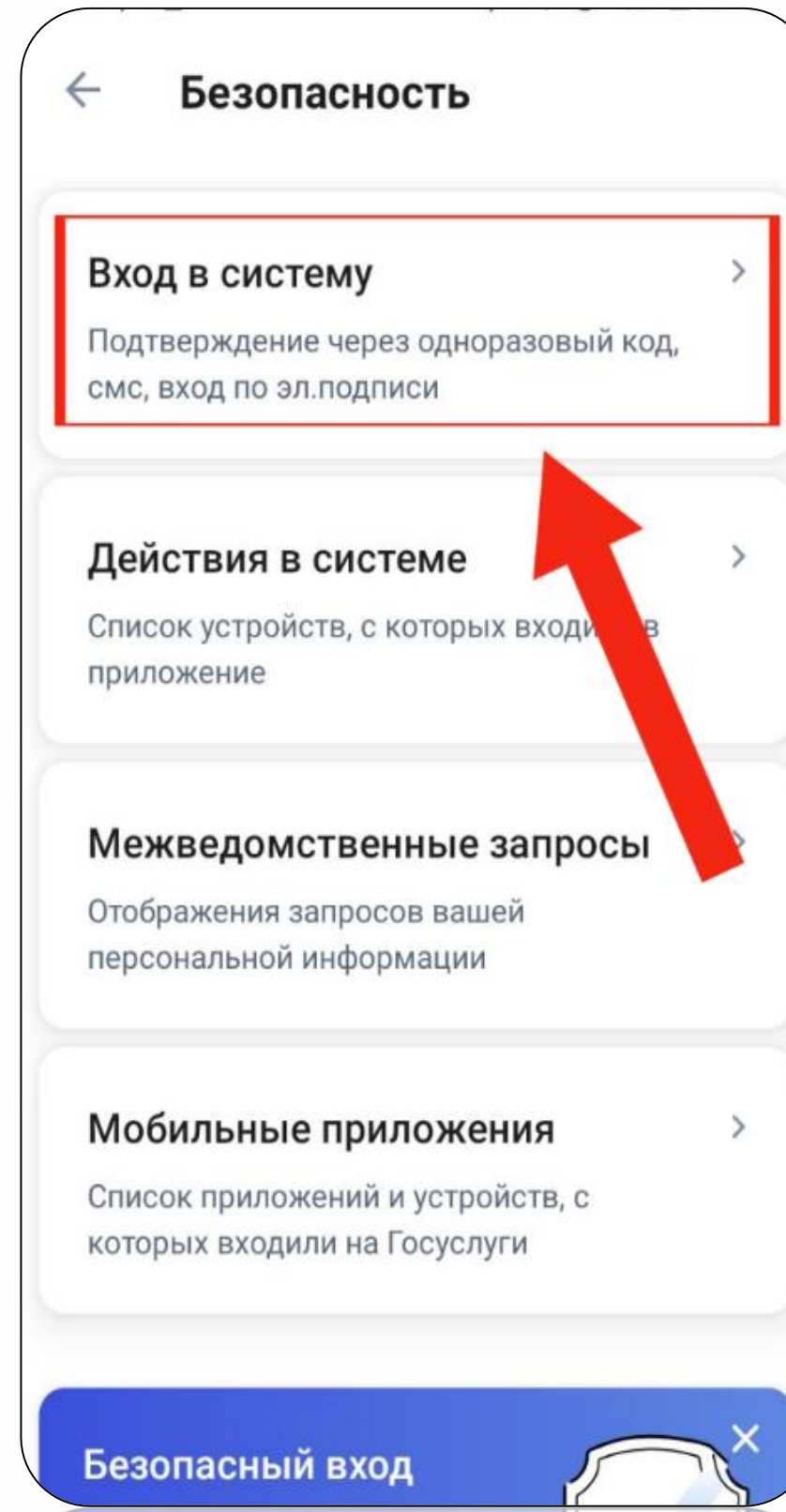
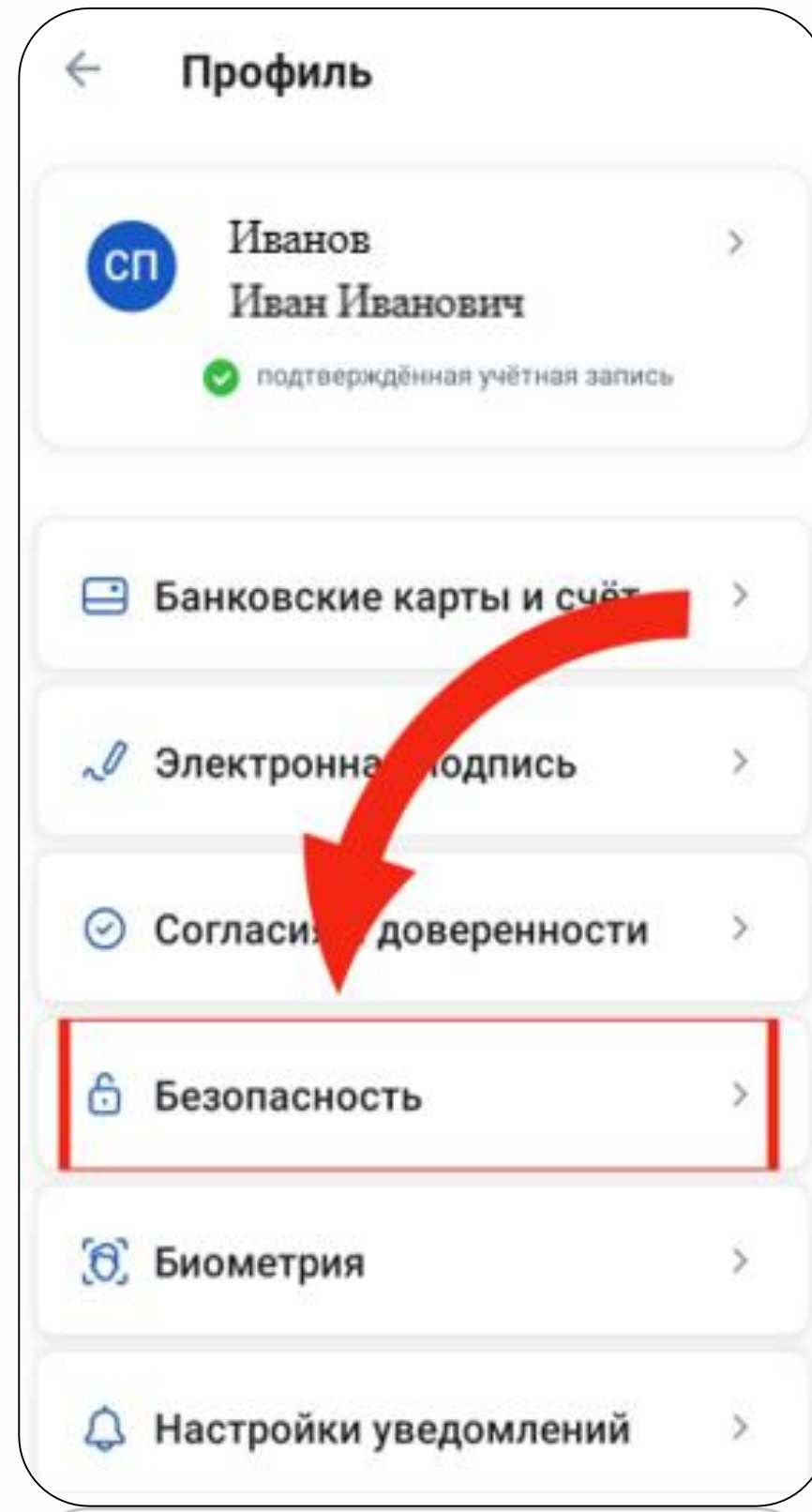
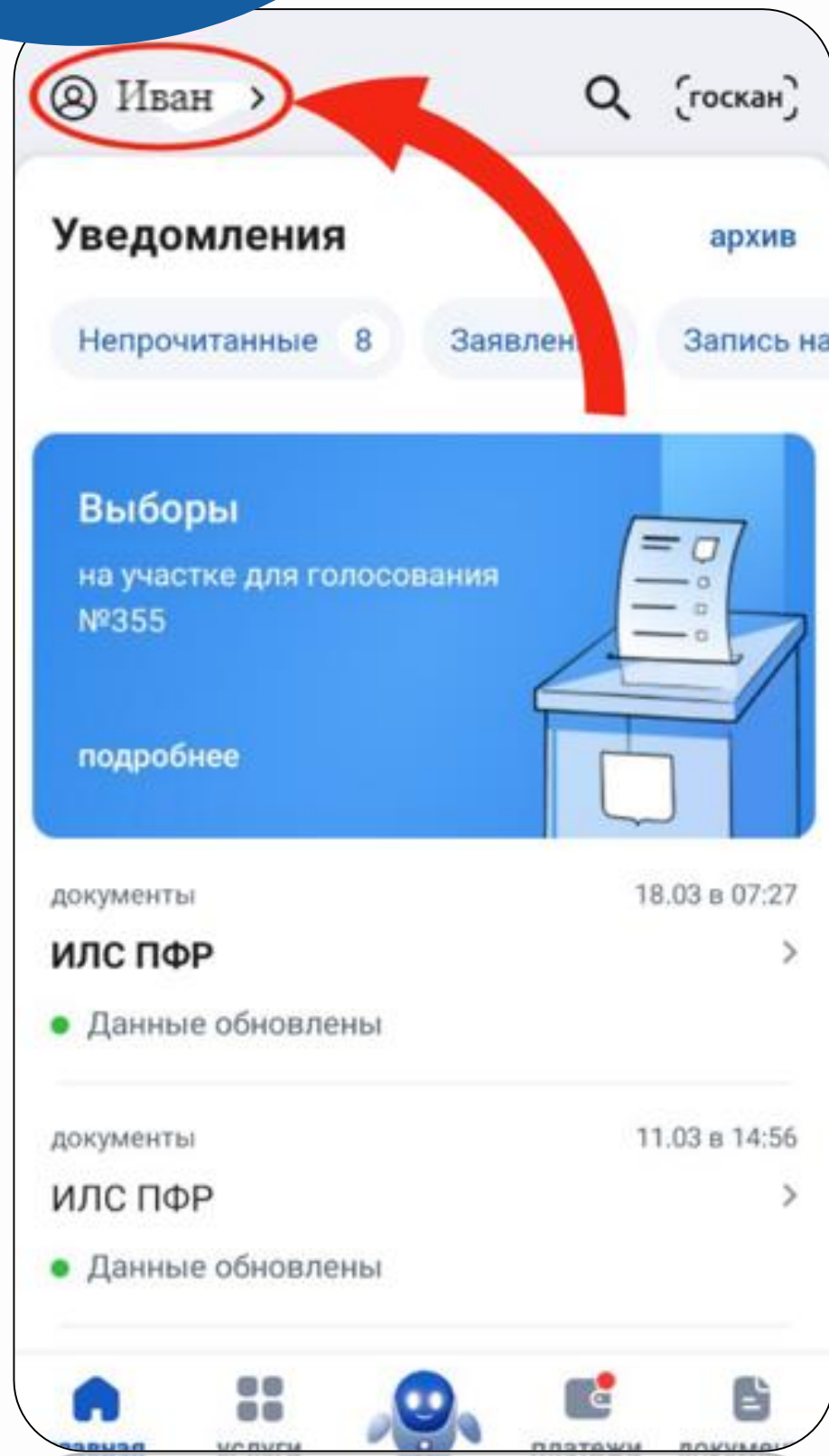
03

Отозвать неизвестные для вас согласия в личном кабинете;

04

Регулярно, раз в полгода необходимо менять пароли доступа.

Дополнительная защита личного кабинета





Дополнительная защита личного кабинета

Функция входа с двухэтапной
аутентификацией.

Войти в личный кабинет с
помощью одного только логина
и пароля будет недостаточно,
при каждом входе в личный
кабинет необходимо вводить
одноразовый код, поступающий
в виде SMS-сообщения.

← Вход с подтверждением

1

Выберите дополнительный способ защиты

☒ По смс на +7 914 XX XX XXX
Указать другой телефон

☐ По одноразовому коду
Потребуется настроить стороннее приложение

2

Продолжить

Дополнительная защита личного кабинета

Функция восстановления доступа контрольным вопросом.

После переоформления SIM-карты, мошенники не смогут восстановить доступ к личному кабинету, так как они не знают ответ на контрольный вопрос.



← Вход в систему

Вход с подтверждением
по смс в дополнение к паролю

Вход по электронной подписи
доступен только при наличии

Оповещение на электронную почту после входа
будет приходить на
bsupavlovsergei@mail.ru
[изменить эл.почту](#)

Восстановление доступа контрольным вопросом
в дополнение к основным способам

← Вход в систему

Восстановление доступа контрольным вопросом
в дополнение к основным способам

Ваш контрольный вопрос

Выберите вопрос 1

Ответ на контрольный вопрос

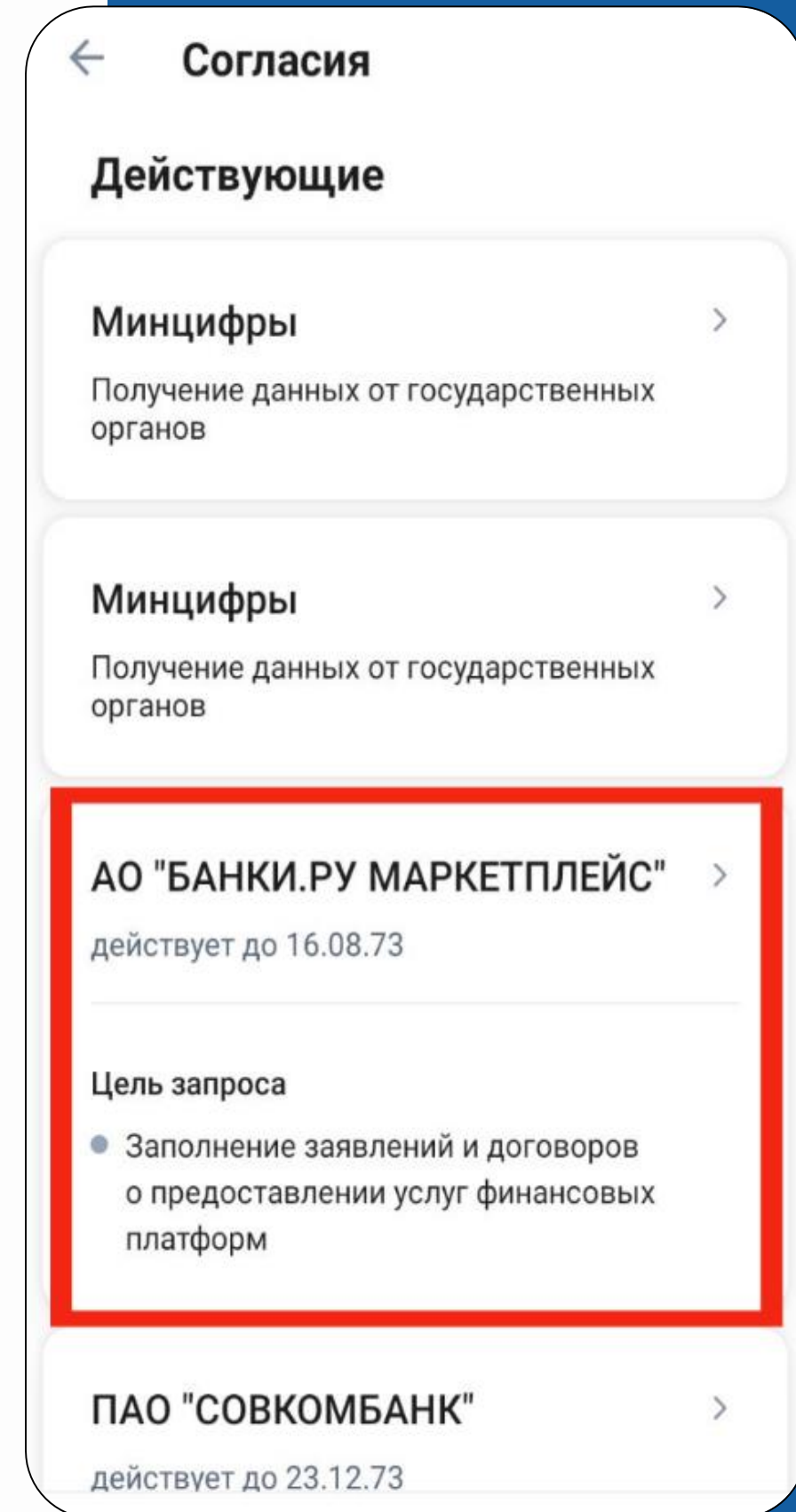
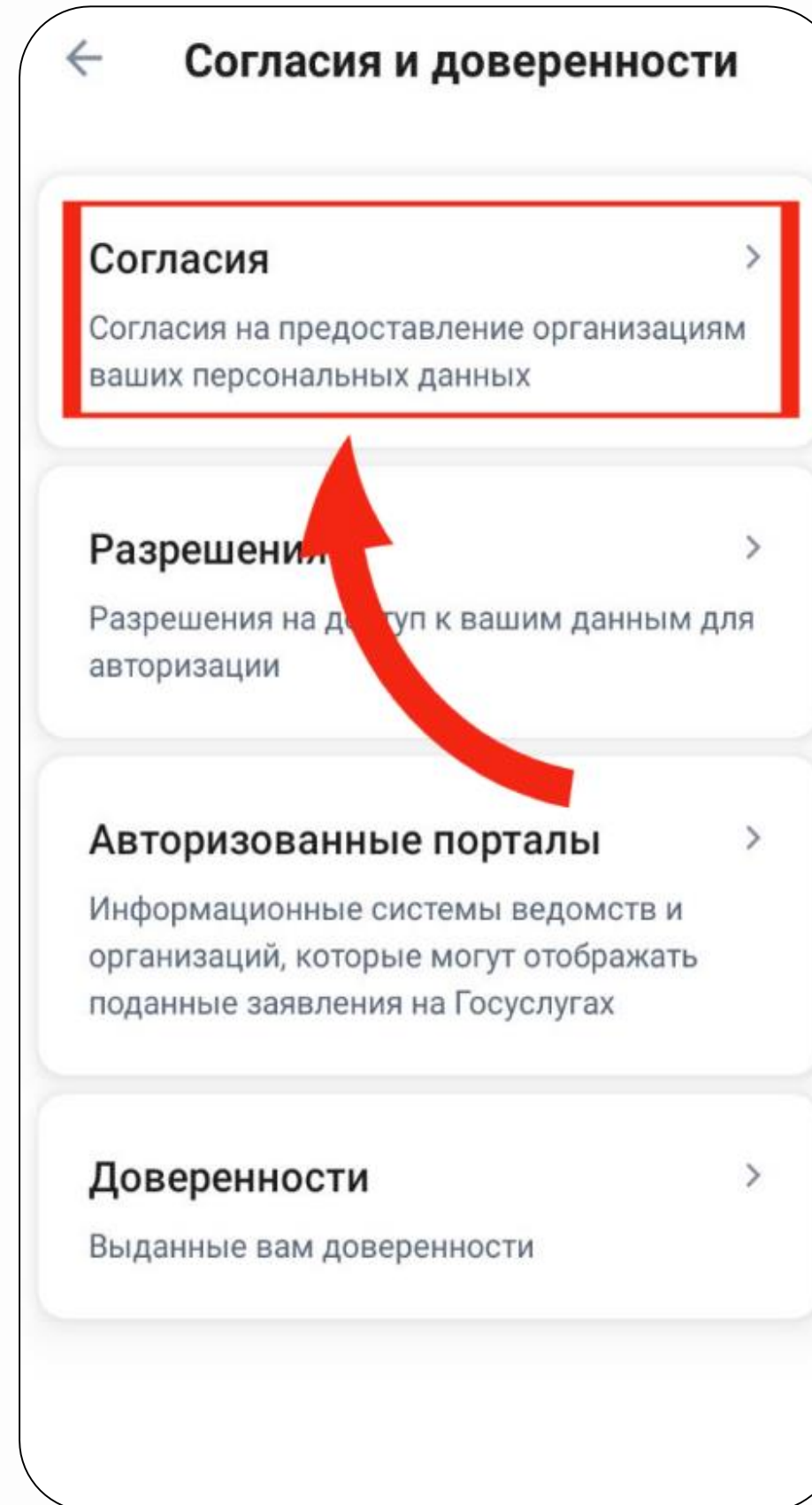
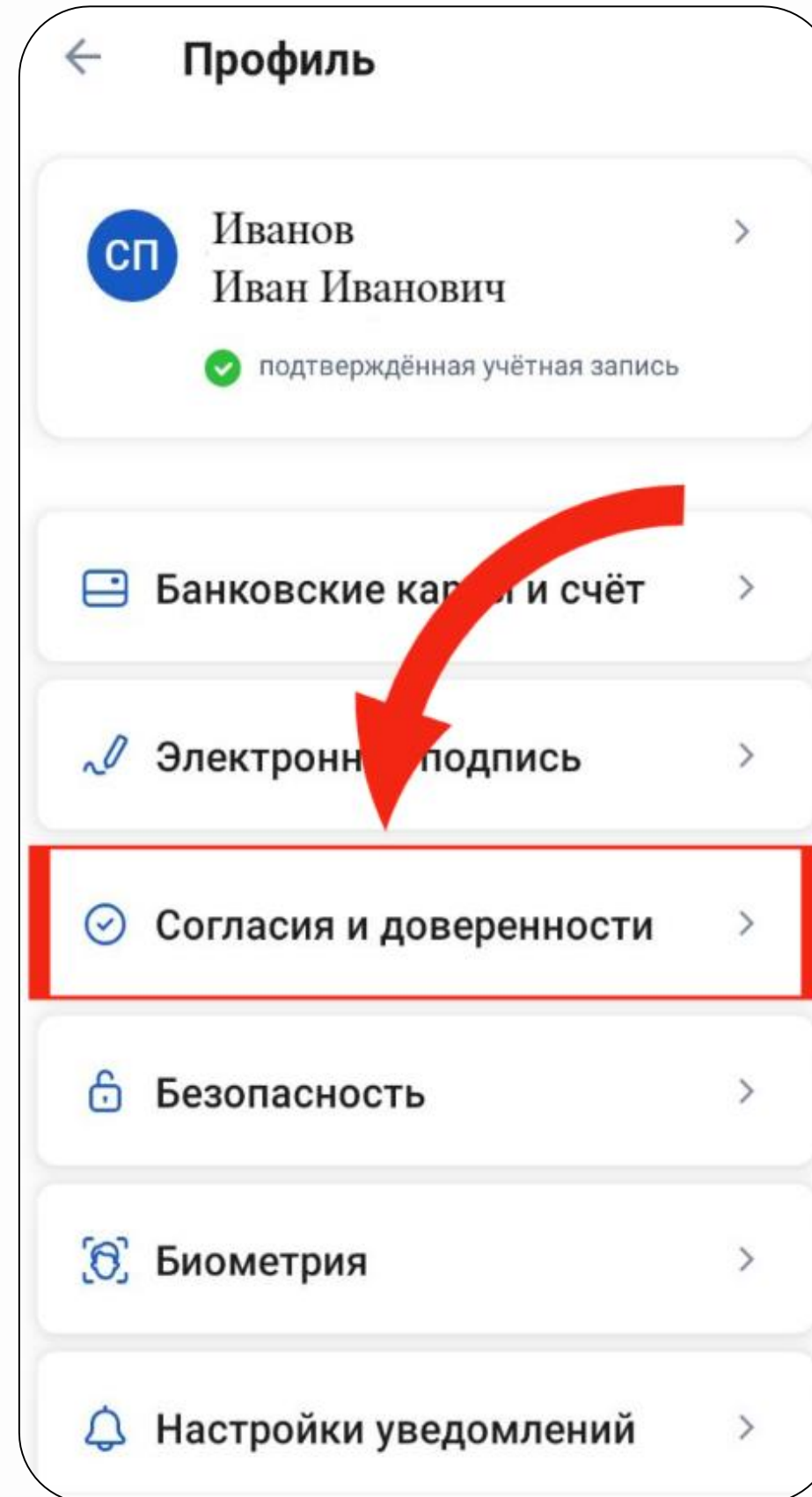
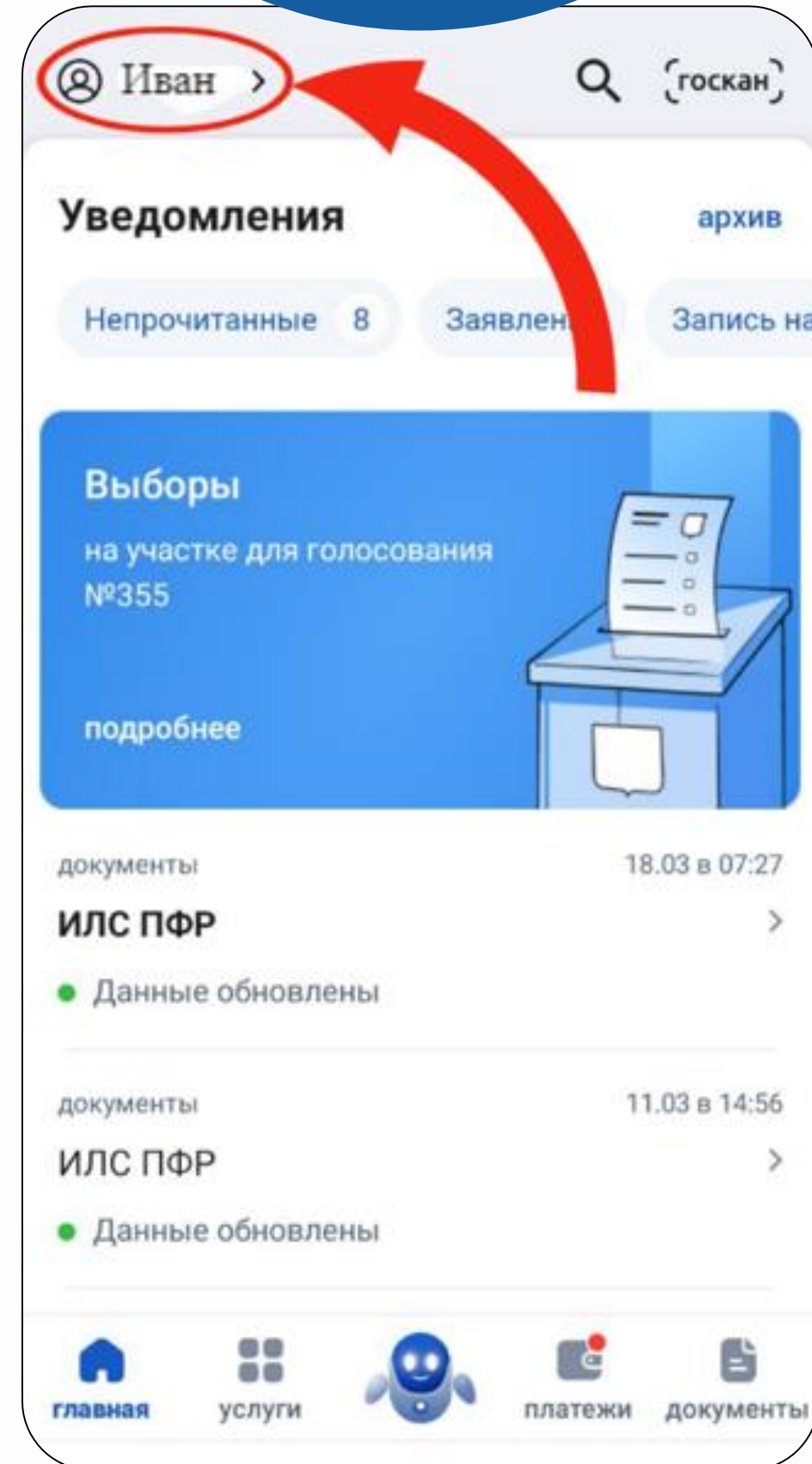
Введите ответ 2

Введите пароль, чтобы подтвердить использование контрольного вопроса для восстановления доступа

Введите пароль 3

4 [изменить](#) [включить](#)

Отзыв согласий



Отзыв согласий

←

Согласие

АО "БАНКИ.РУ МАРКЕТПЛЕЙС"

Цель запроса

- Заполнение заявлений и договоров о предоставлении услуг финансовых платформ

Запрашиваемые персональные данные

- Дата рождения, указанная в документе, удостоверяющем личность
- Сведения о водительском удостоверении (страна выдачи, серия, номер, дата выдачи и прекращения действия, орган, выдавший удостоверение, разрешенные категории вождения)
- Сведения о паспорте, удостоверяющем личность гражданина Российской Федерации (серия, номер, дата выдачи и прекращения действия, орган, выдавший паспорт)

Отозвать согласие

←

Согласие

АО "БАНКИ.РУ МАРКЕТПЛЕЙС"

Цель запроса

- Заполнение заявлений и договоров о предоставлении услуг финансовых платформ

Отзыв согласия

АО "БАНКИ.РУ МАРКЕТПЛЕЙС" больше не будет получать ваши данные из личного кабинета на Госуслугах

Организация вправе продолжить обработку уже полученных данных

- Если этого требуют условия действующего договора между вами и организацией
- По основаниям ч. 1 ст. 6 Закона о персональных данных

Отменить

Отозвать

←

Согласия

Действующие

архив

Минцифры

>

Получение данных от государственных органов

Минцифры

>

Получение данных от государственных органов

ООО "ХКФ БАНК"

>

действует до 11.03.74

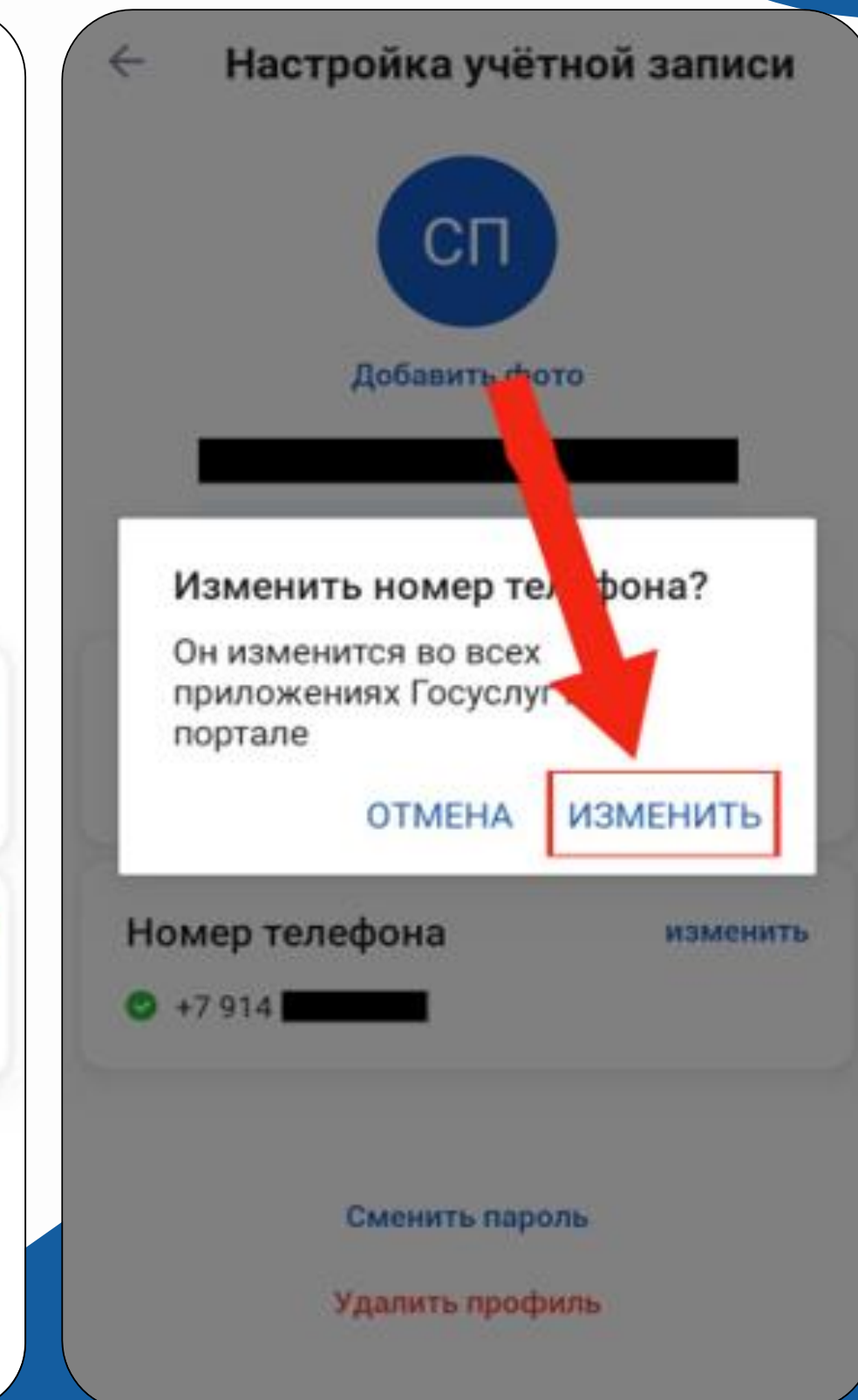
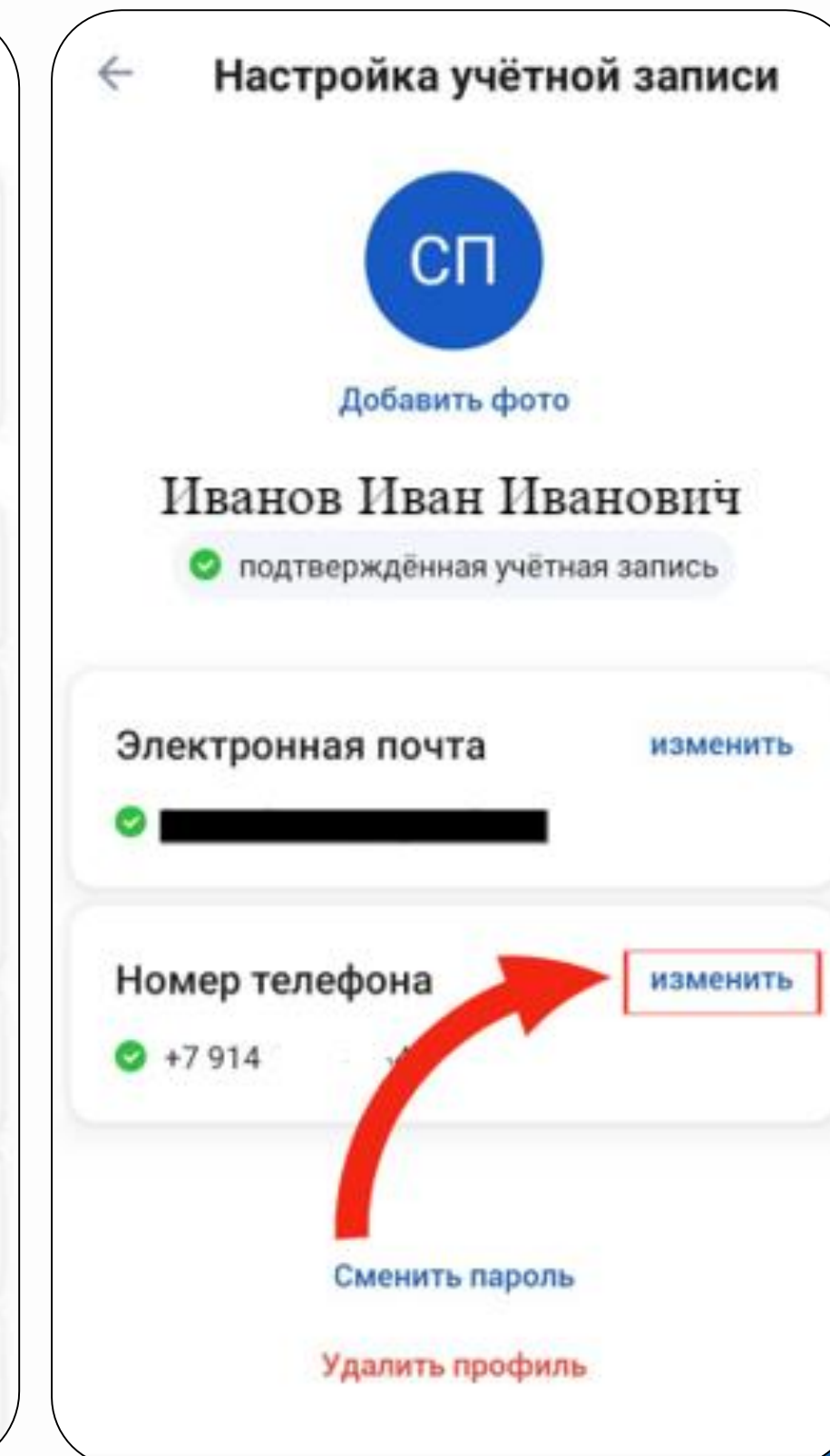
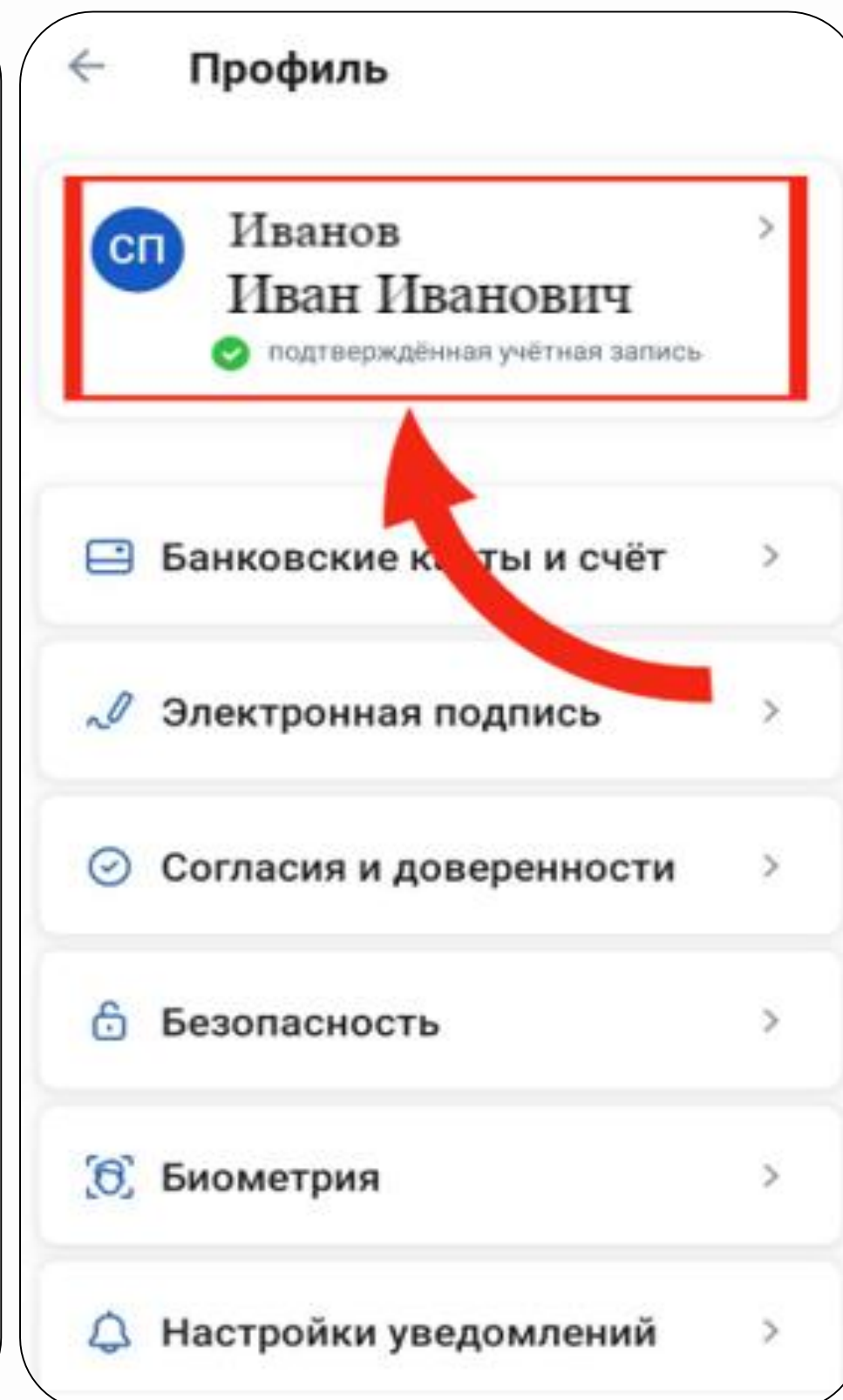
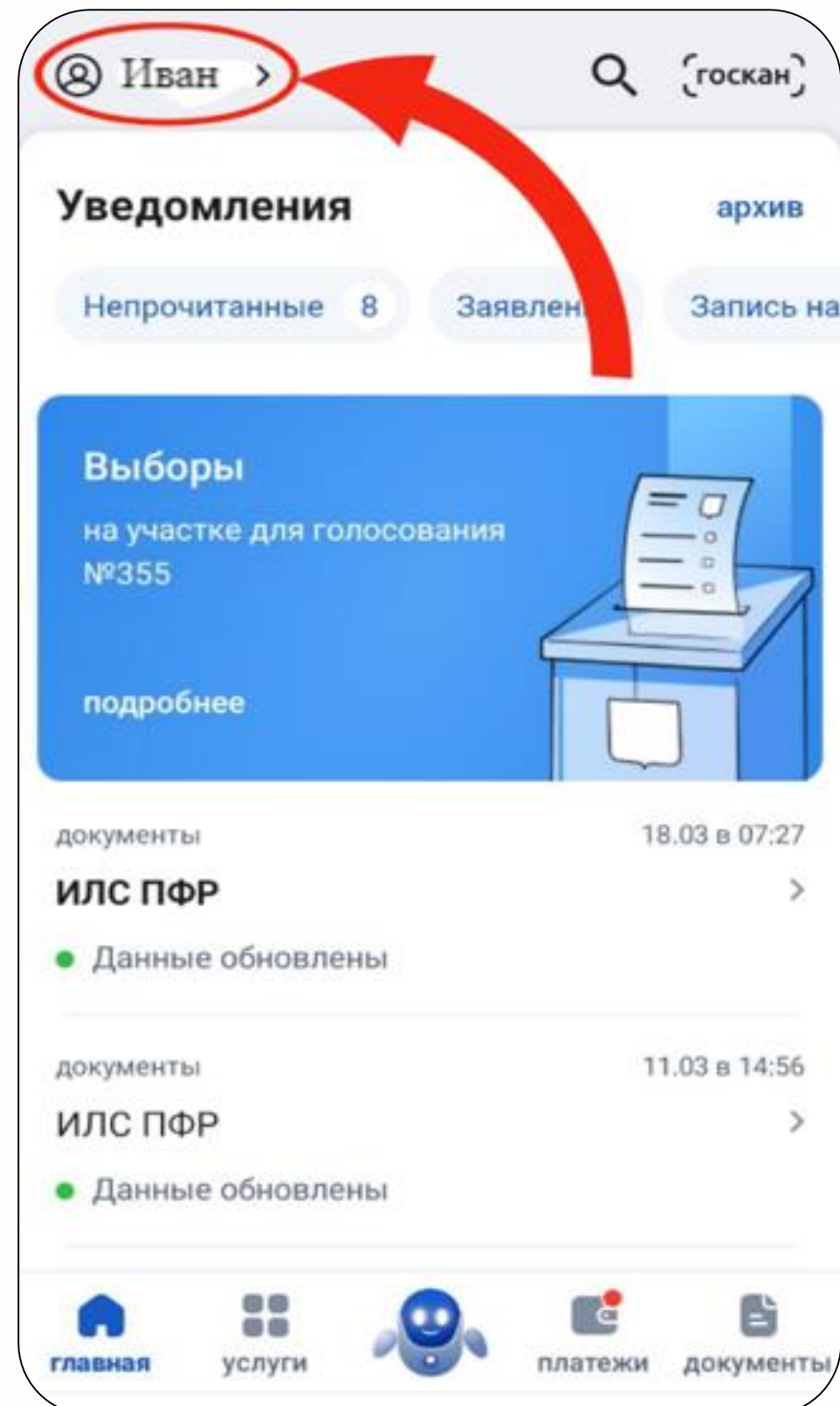
Цель запроса

- Предоставление кредита (займа), в том числе кредита с лимитом кредитования и (или) овердрафта, выдача и обслуживание банковской карты для обслуживания кредита (займа)

! Согласие отозвано

×

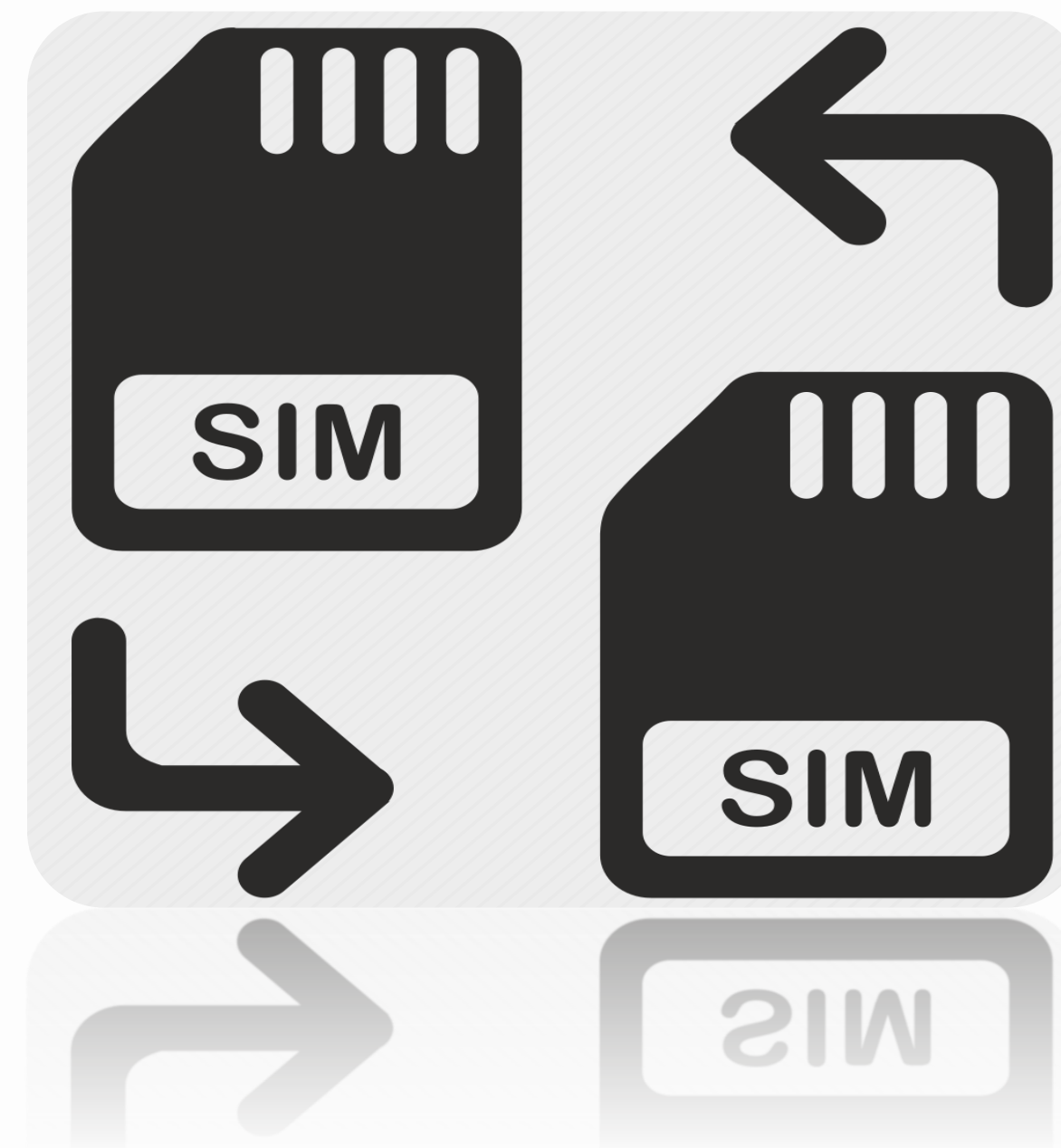
Способ открепления номера телефона



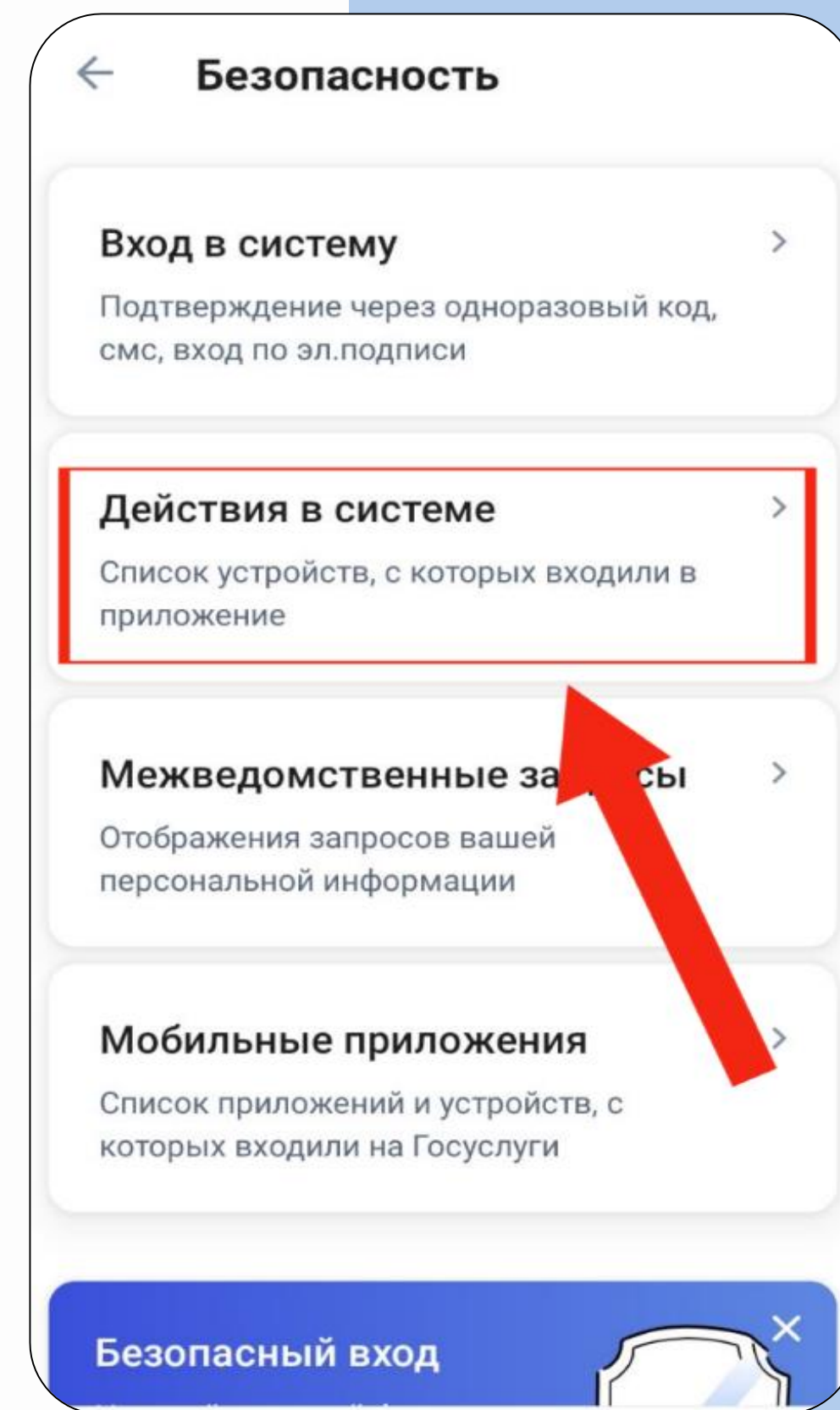
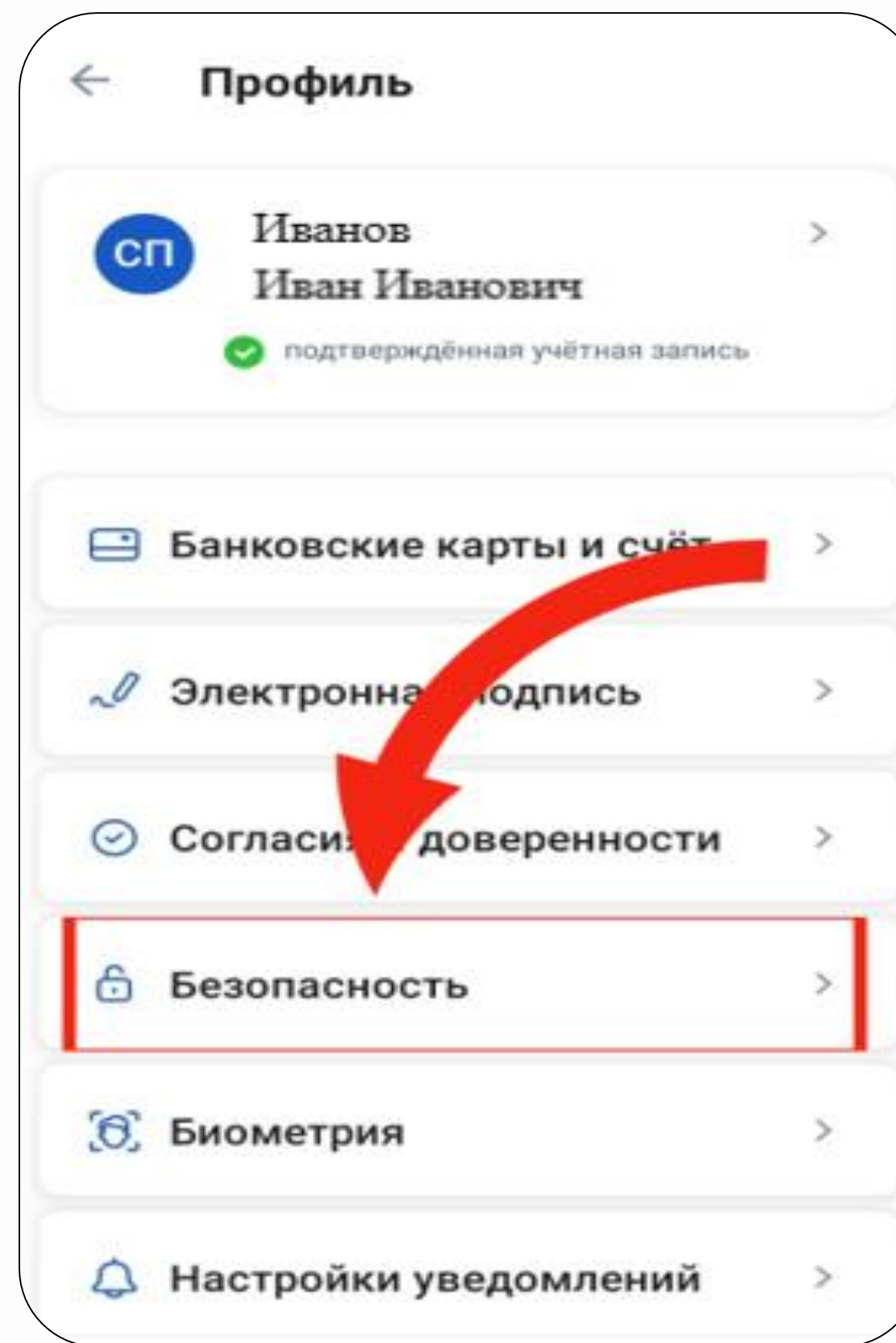
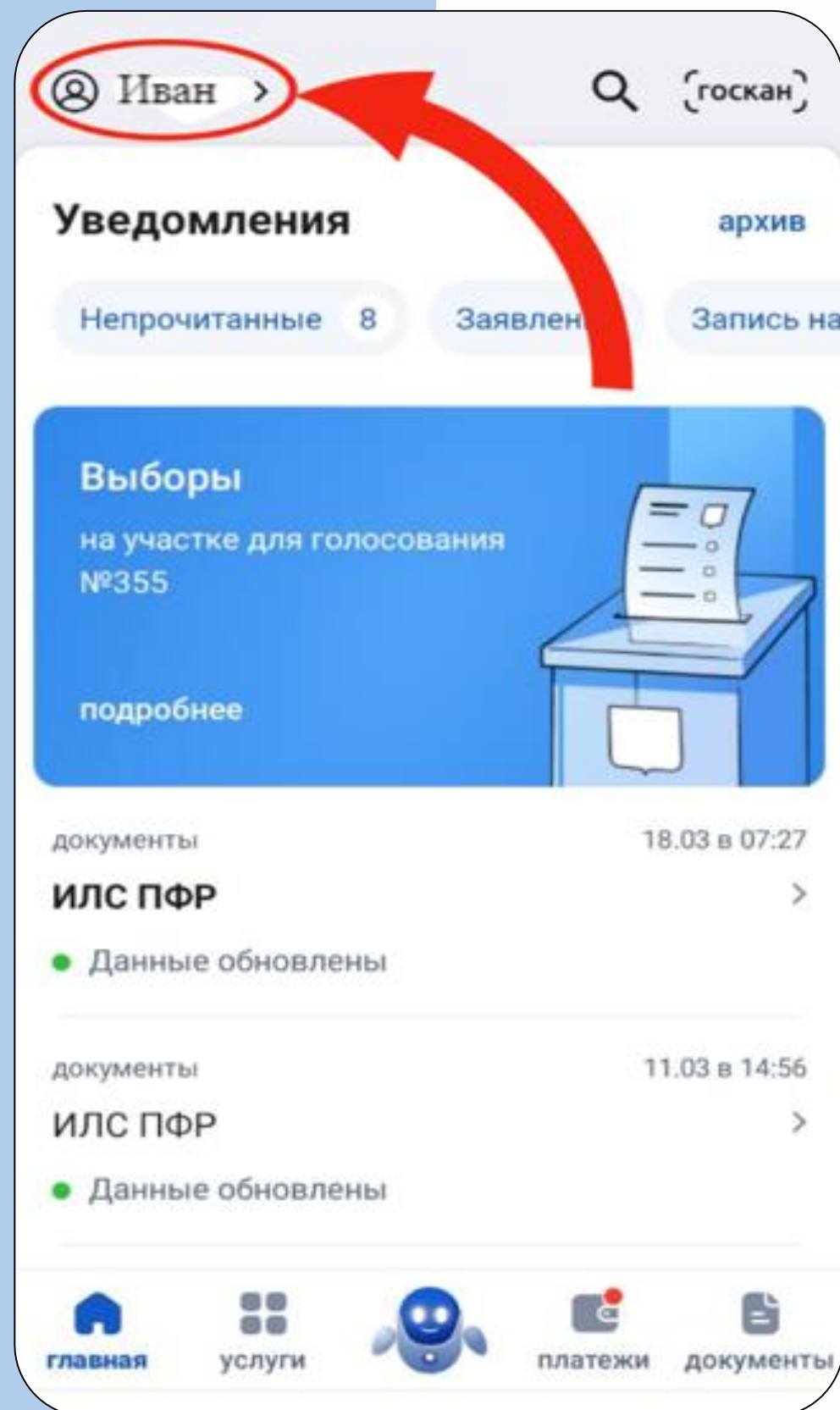
Переоформление SIM-карты

SIM-карта оператора сотовой связи может быть переоформлена через 2-6 месяцев после прекращения пользования предыдущим абонентом.

Тем самым, предоставляя возможность новому пользователю восстановить доступ к личному кабинету от портала «Госуслуги», путем ввода **SMS-кодов**, поступивших на перевыпущенный номер **SIM-карты**, что и делают злоумышленники.



Признаки взлома личного кабинета портала «Госуслуги»



Признаки взлома личного кабинета портала «Госуслуги»

Без признаков взлома

← Действия в системе [фильтры](#)

Авторизация по номеру телефона

IP 19 [REDACTED]
Мобильное приложение Госуслуги

20.03.24 в 11:03

Вход в систему Портал государственных услуг Российской Федерации

Авторизация по номеру телефона

IP 19 [REDACTED]
Android, Chrome

20.03.24 в 11:02

Вход в систему Портал государственных услуг Российской Федерации

Авторизация по номеру телефона

С признаками взлома

2023-09-01T19:06:17.120+0300	Вход в систему Vivus.SMSFinance. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:54:47.939+0300	Вход в систему Портал государственных услуг Российской Федерации. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:51:03.165+0300	Вход в систему Срочноденьги ЦПГ. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:45:07.170+0300	Вход в систему ООО МФК "ВЭББАНКИР". Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49
2023-09-01T18:44:10.675+0300	Вход в систему Срочноденьги ЦПГ. Авторизация по номеру телефона. Личный кабинет физического лица	128.204.65.49

Восстановите пароль от личного кабинета

Перейдите на сайт или
в приложение одного
из своих банков.

Повторите
регистрацию на
«Госуслуги» через
банк-номер из личного
кабинета банка будет
перенесен в личный.
Банк вышлет пароль
для входа в аккаунт.

ИЛИ



Обратитесь в офис
МФЦ и попросите
оператора
восстановить пароль.

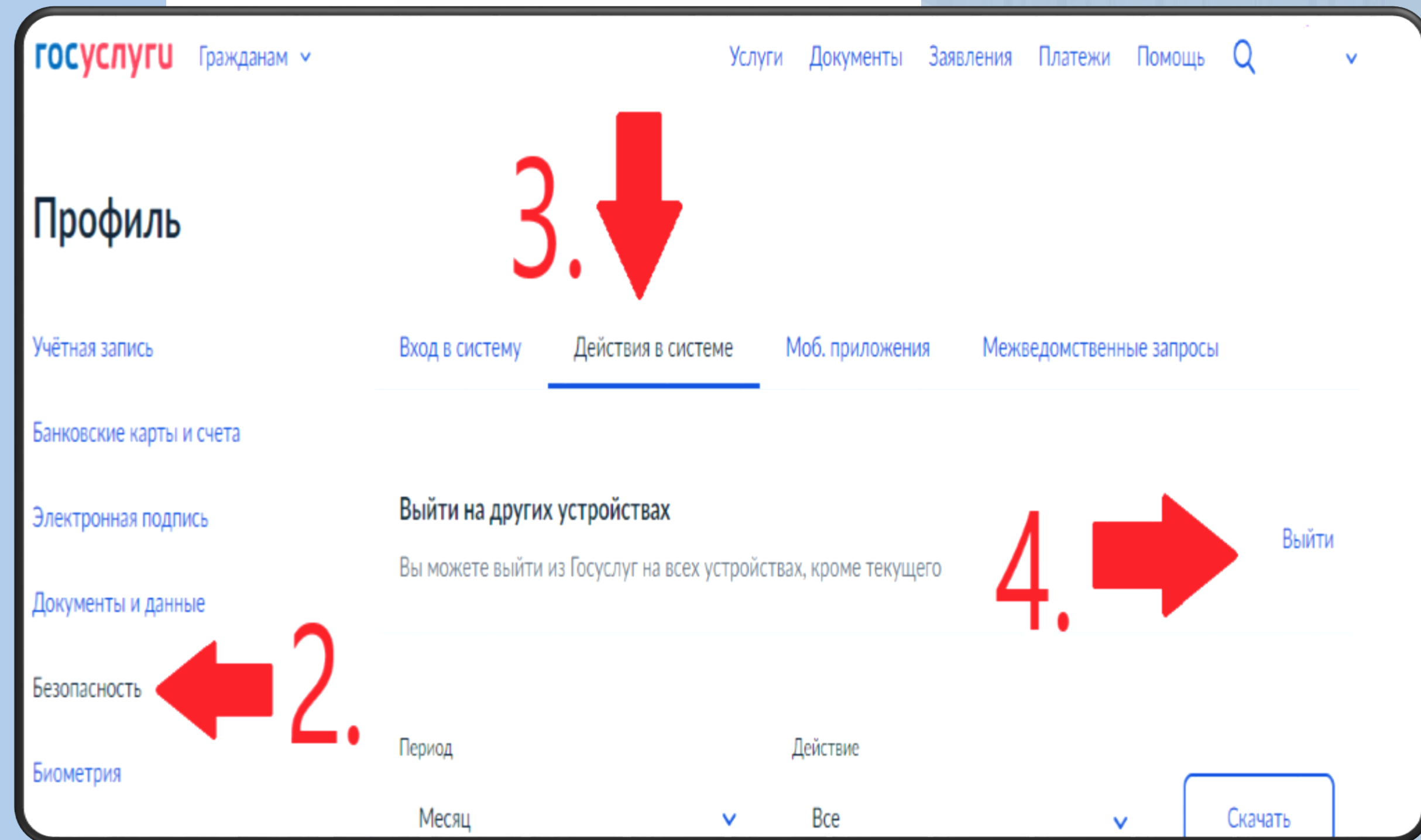
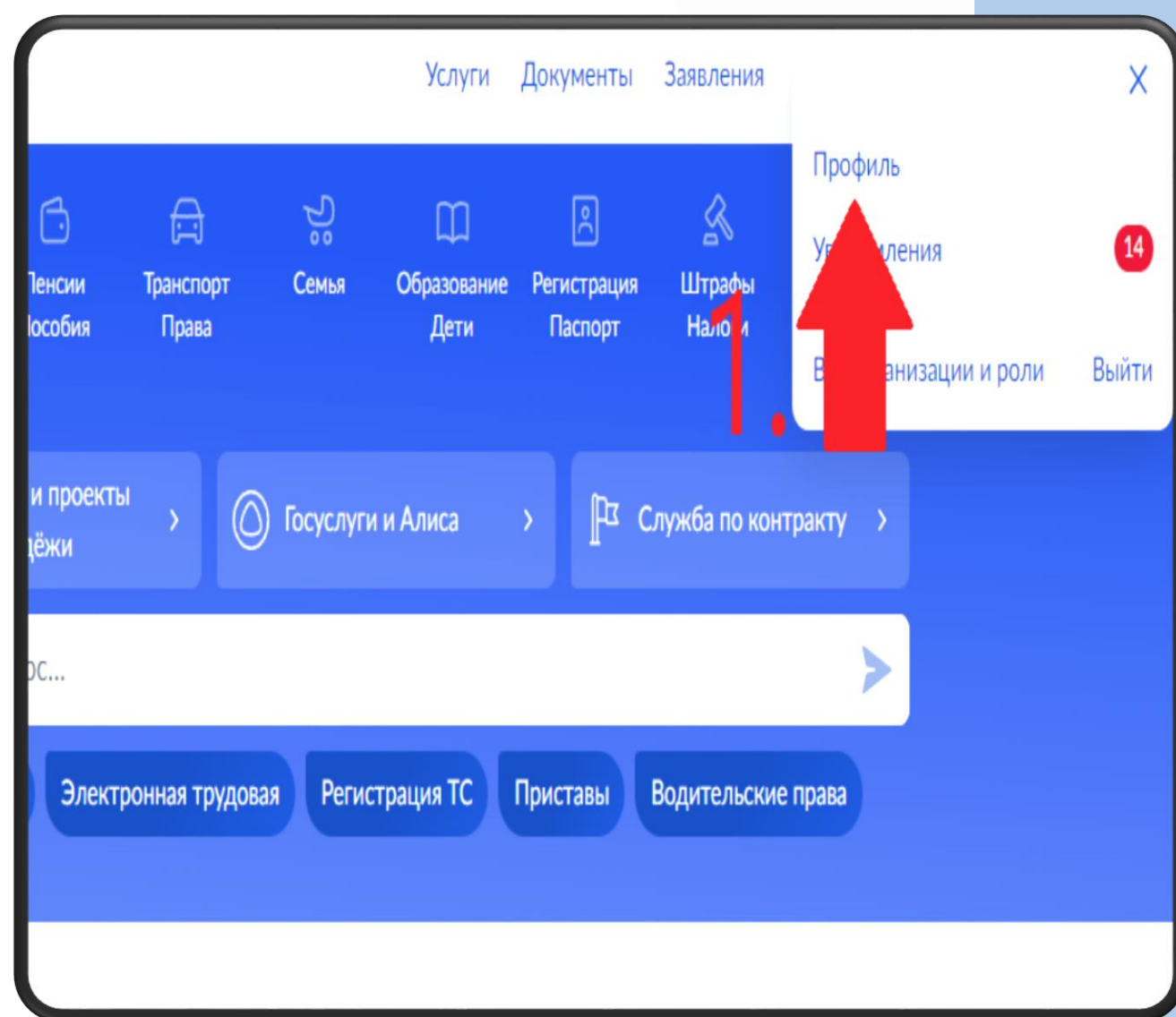
Сотрудники проверят
вашу личность,
помогут восстановить
доступ к аккаунту и
сменить пароль.

Возьмите с собой
паспорт и СНИЛС

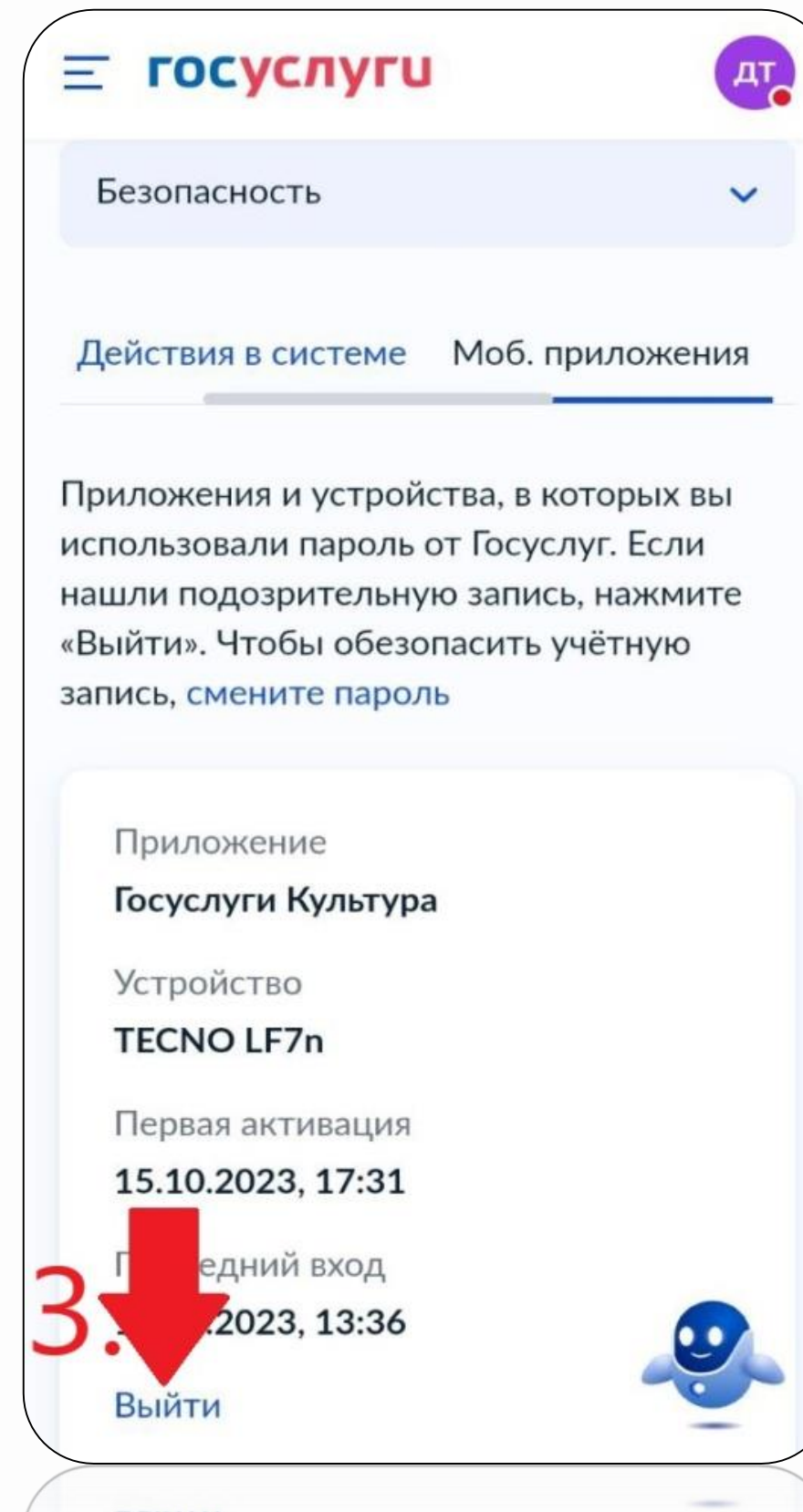
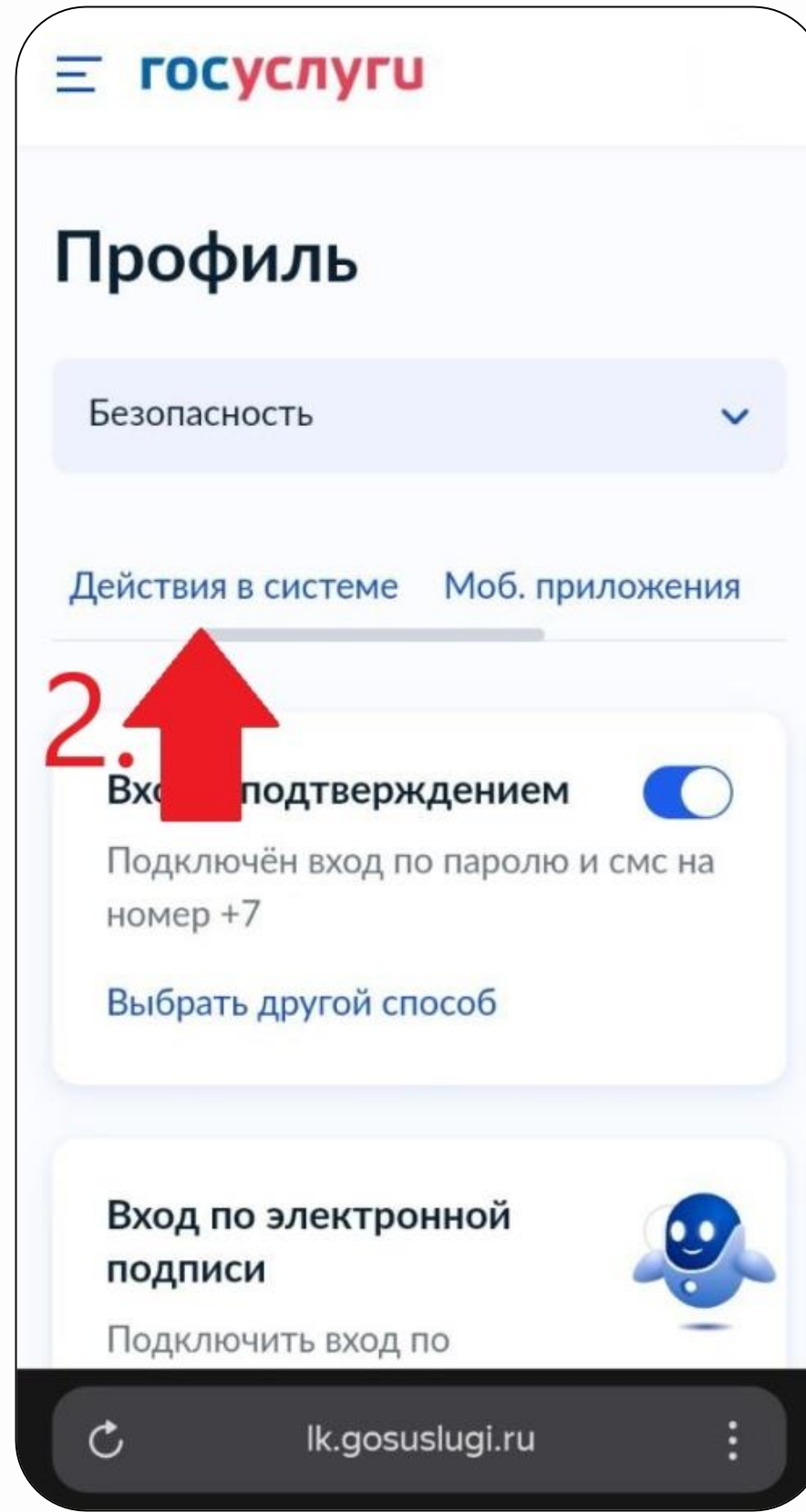
Определите, где использовалась учетная запись

Вы можете выйти одновременно на всех устройствах, кроме
текущего

НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ:



НА МОБИЛЬНОМ ТЕЛЕФОНЕ:



Отзовите разрешения, которые не выдавали.

Проверьте поданные заявления. Это поможет выявить, какие действия хотели совершить мошенники от вашего имени.

Проверьте кредитную историю и узнайте, направлялись ли от вашего имени заявки на займы



Выясните, в каких
бюро хранится ваша
кредитная история
(их может быть
несколько).
Сделать это можно
на портале
«Госуслуги»



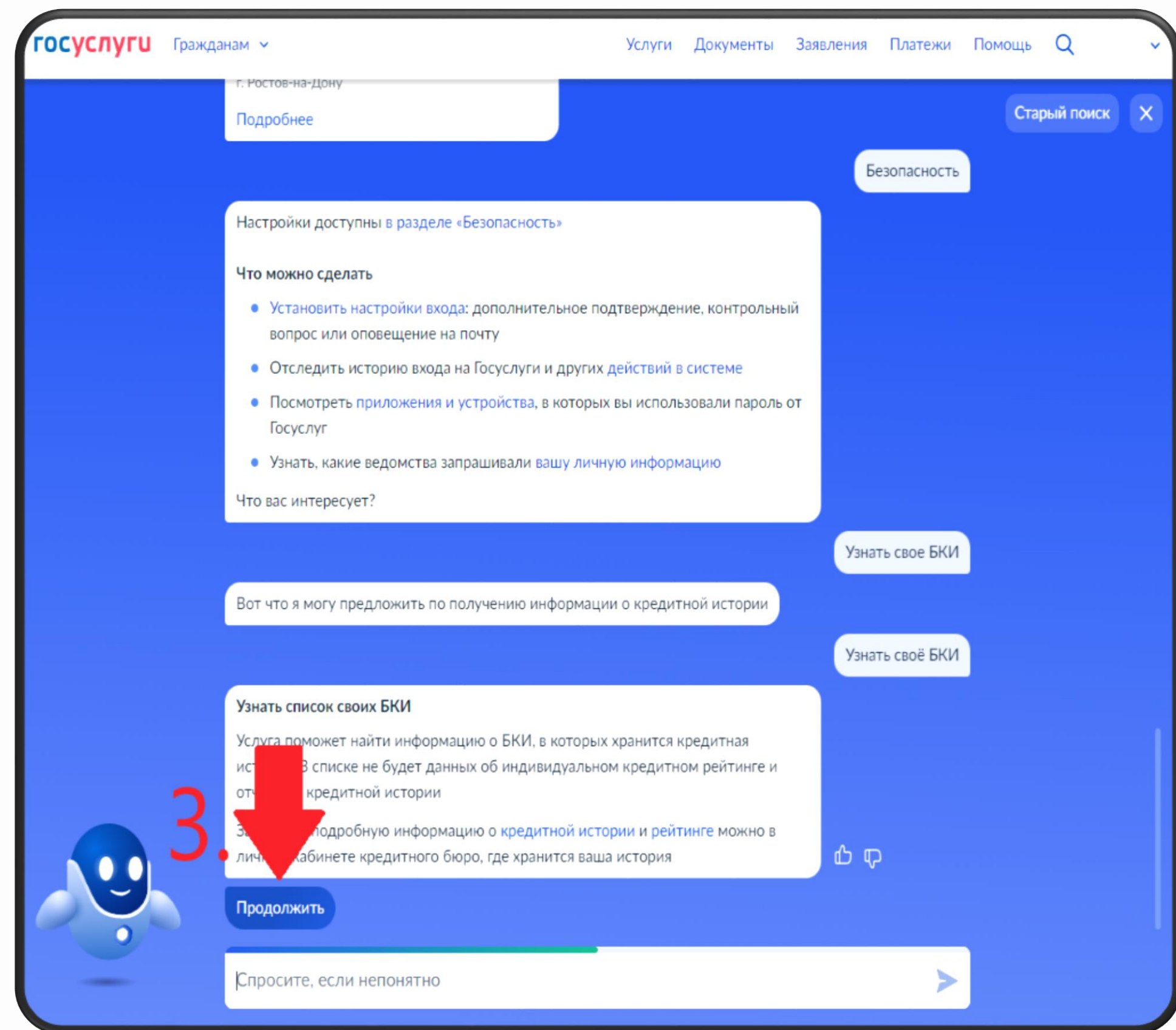
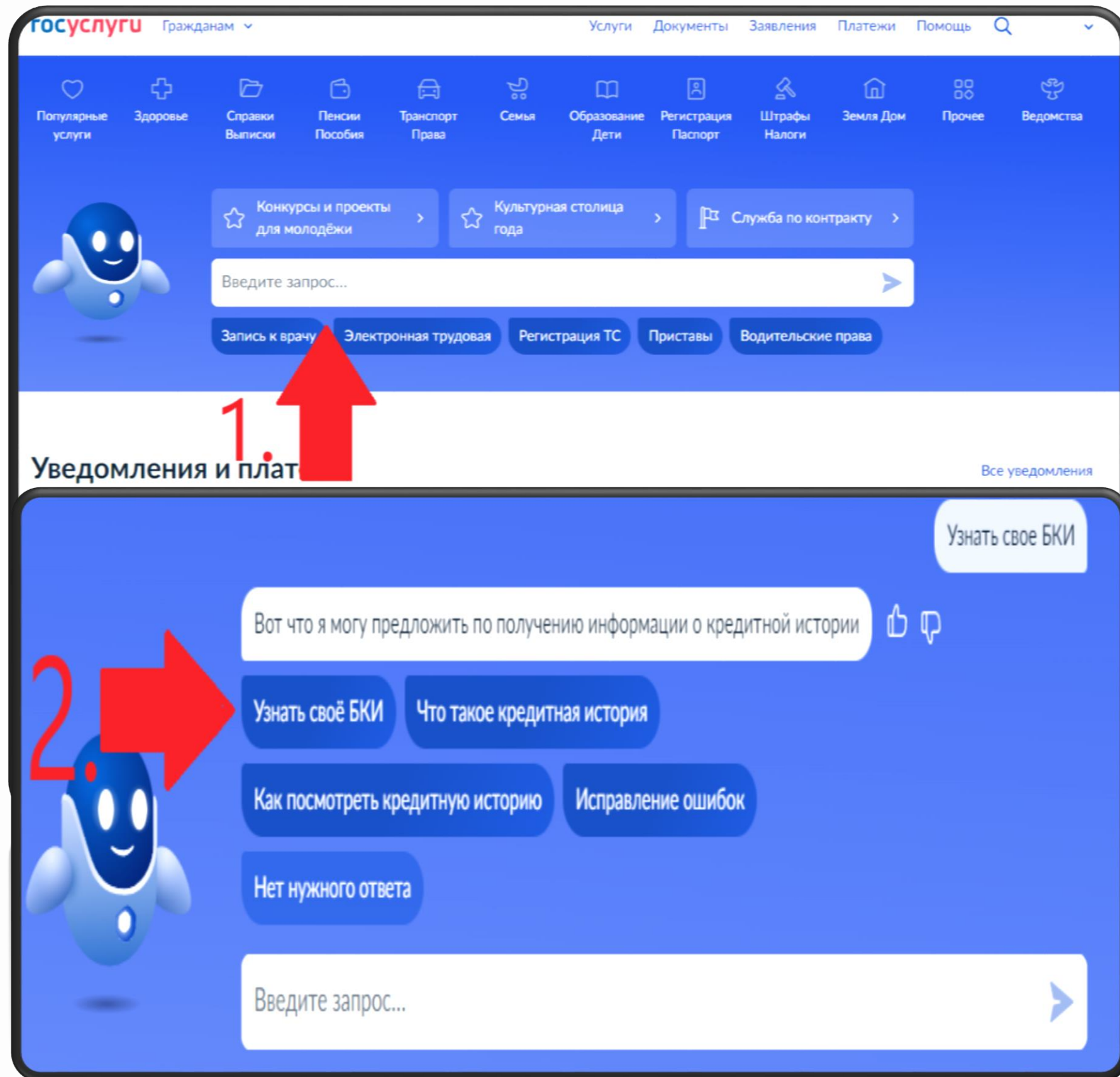
Введите в строке
поиска запрос
«узнать свое БКИ».



Далее
зарегистрируйтесь на
сайте каждого бюро* и
запросите свою
кредитную
историю
(рекомендуем направить
запрос через 2 недели
после взлома аккаунта).

***Можно авторизоваться с помощью учетной записи «Госуслуги».**

Узнать на портале «Госуслуги» в каких бюро хранится ваша кредитная история.



Самозапрет на госуслугах: цифровая гигиена и защита от мошенников

?

Установить запрет может любой гражданин, нужны только ИНН и документ, удостоверяющий личность

?

Установление запрета бесплатно

?

Запрет можно установить и снять неограниченное количество раз

?

Установленный запрет действует бессрочно

?

Наличие действующих кредитов не мешает установлению запрета

?

Лучше, чтобы запрет был установлен, при необходимости его можно снять в любой момент

?

Действующие кредиты останутся, нельзя будет брать новые

?

Запрет не препятствует получению денежных средств по ранее выданным кредитным картам

?

Наличие запрета не снижает кредитоспособность и не влияет на рейтинг кредитоспособности

Как установить самозапрет на кредиты и микрозаймы



1. Поиск услуги

Войдите в свой аккаунт на portal.gosuslugi.ru или в мобильном приложении.

В строке поиска введите: «Установка самоограничения» или «Запрет на выдачу кредитов».

2. Либо найдите услугу в каталоге: «Нотариат, регистрация, право» → «Сведения из бюро кредитных историй».

3. Заполнение заявления

Нажмите кнопку «Получить услугу».

Внимательно прочитайте информацию о последствиях (запрет можно будет снять только через 3, 6 или 12 месяцев).

Выберите срок, на который хотите установить запрет (3, 6 или 12 месяцев).

4. Подача заявления

Дайте согласие на обработку данных. Нажмите «Отправить».

5. Подтверждение и получение результата

Проверить статус заявления можно в «Личном кабинете» → «Уведомления».

В течение 1-3 рабочих дней запрет будет оформлен. Уведомление придет в личный кабинет.

Какой запрет хотите установить
в микрофинансовых организациях?

На дистанционную выдачу кредита



Запрет на получение кредита без личного посещения. Например, через интернет или по телефону

На очную и дистанционную выдачу кредита



Запрет на получение любым способом: при личном посещении, через интернет или по телефону

Как установить самозапрет на кредиты и микрозаймы



заккрыть

← Назад

На какие организации будет распространяться запрет?

Кредитные

Чаще всего это банки, которые предоставляют крупные кредиты на долгий срок — более месяца

Микрофинансовые

Это организации, которые выдают в долг небольшие суммы на короткий срок. Как правило, не более 1 месяца

Кредитные и микрофинансовые

заккрыть

← Назад

Какой запрет хотите установить в микрофинансовых организациях?

На дистанционную выдачу кредита

Запрет на получение кредита без личного посещения. Например, через интернет или по телефону

На очную и дистанционную выдачу кредита

Запрет на получение любым способом при личном посещении, через интернет или по телефону

заккрыть

← Назад

Какую подпись хотите использовать?

Что такое ПЭП, УНЭП и УКЭП

ПЭП

Формируется с помощью вашей учётной записи на Госуслугах

УНЭП в приложении «Госключ»

Понадобится телефон или планшет с приложением «Госключ». Если сертификата УНЭП ещё нет, его будет предложено выдать

УКЭП в приложении «Госключ»

Понадобится телефон или планшет с приложением «Госключ». Если сертификата УКЭП ещё нет, его будет предложено выдать. Для этого понадобится либо подтверждающая биометрия, либо заграничный паспорт нового образца и телефон с NFC, либо поход в МФЦ или банк

заккрыть

Заявление отправлено

⌚ Срок оказания услуги — до 2 календарных дней

Что дальше

Уведомление о получении заявления придёт в личный кабинет в течение 2 календарных дней. Запрет начнёт действовать на следующий день после получения уведомления

Запрет действует бессрочно. Снять его или узнать статус запрета можно также через Госуслуги

В личный кабинет

заккрыть

← Назад

Заявление готово к отправке

Вы ввели все необходимые данные и можете отправить заявление

Отправить заявление

Обратитесь в полицию и
подайте заявление.

**При наличии данных, указывающих на
совершение противоправных действий, в
том числе связанных с мошенничеством,
подайте заявление в полицию.**

**Возьмите с собой копию заявления из
МФЦ,
скриншоты СМС – сообщений и другие
доказательства.**



обманывают

el_vas_obmanivayut



01

Публикует актуальную информацию о новых схемах обмана, уловках злоумышленников и способах защиты.

02

Помогает узнать о рисках заранее и не стать жертвой, распознав обман по описанным признакам.

03

Оповещает о свежих видах мошенничества и получают конкретные инструкции, как себя обезопасить.

04

Оперативно предупреждает, повышая финансовую и цифровую грамотность