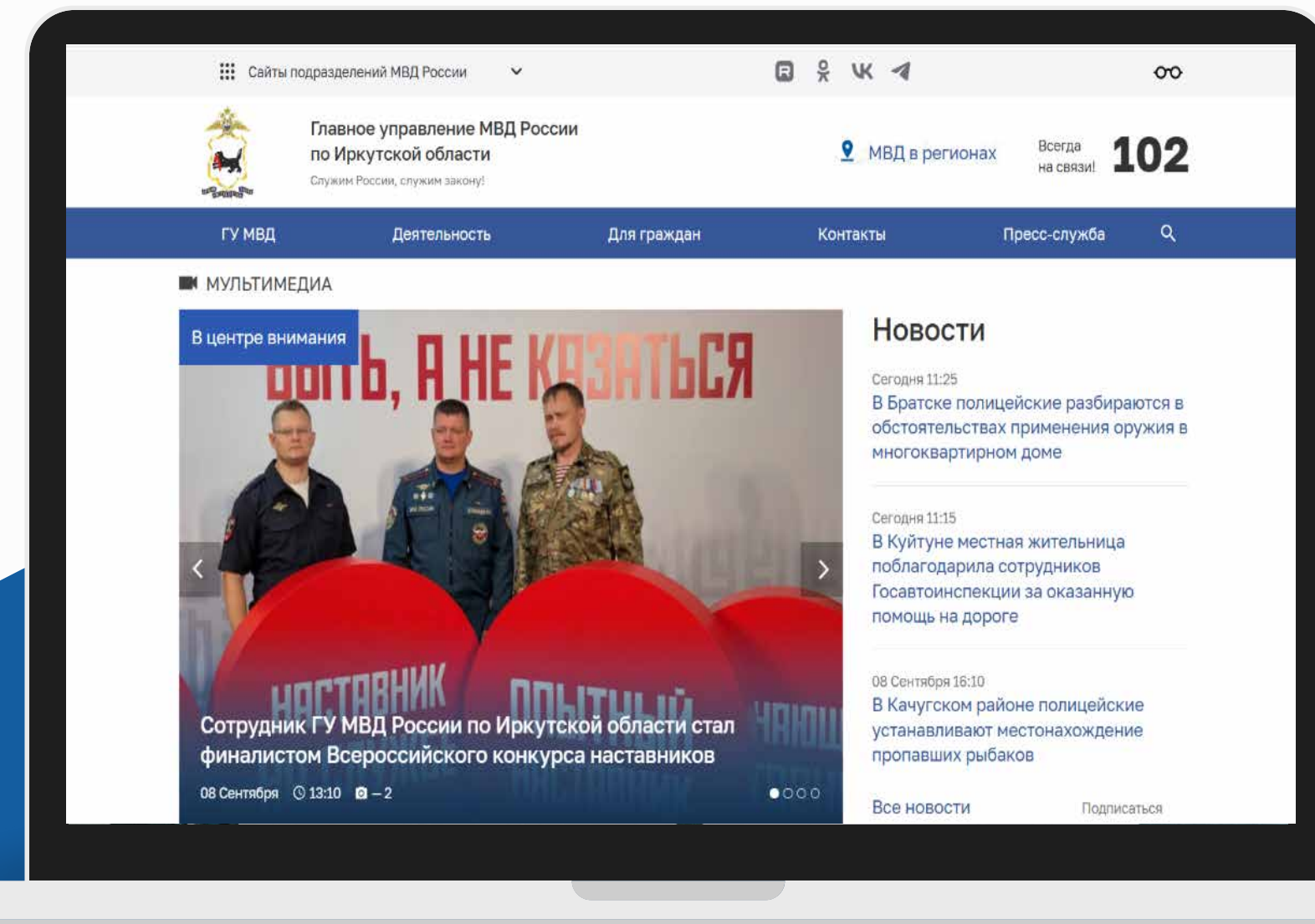




МУ МВД России «Иркутское»

ВИДЫ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ И ЗАЩИТА ОТ НИХ



**Общий ущерб составляет
Более 2,5 млрд. рублей
(за 2024 год)**



Иркутская область

Сумма похищенных средств в рублях на 2024г

Профессор института - 30 000 000 руб.

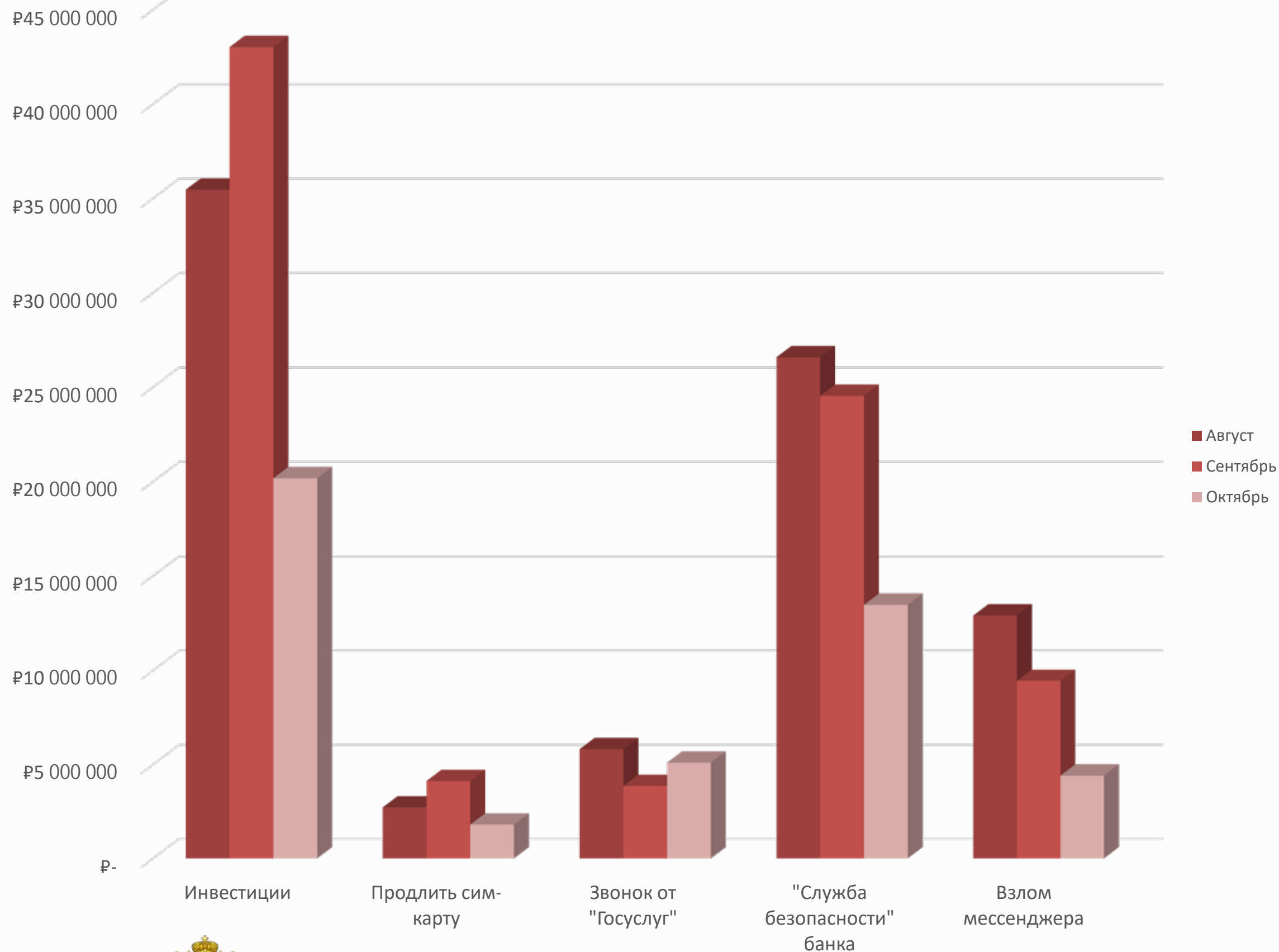
Индивидуальный предприниматель – 10 300 000 руб.

Домохозяйка - 6 700 000 руб.

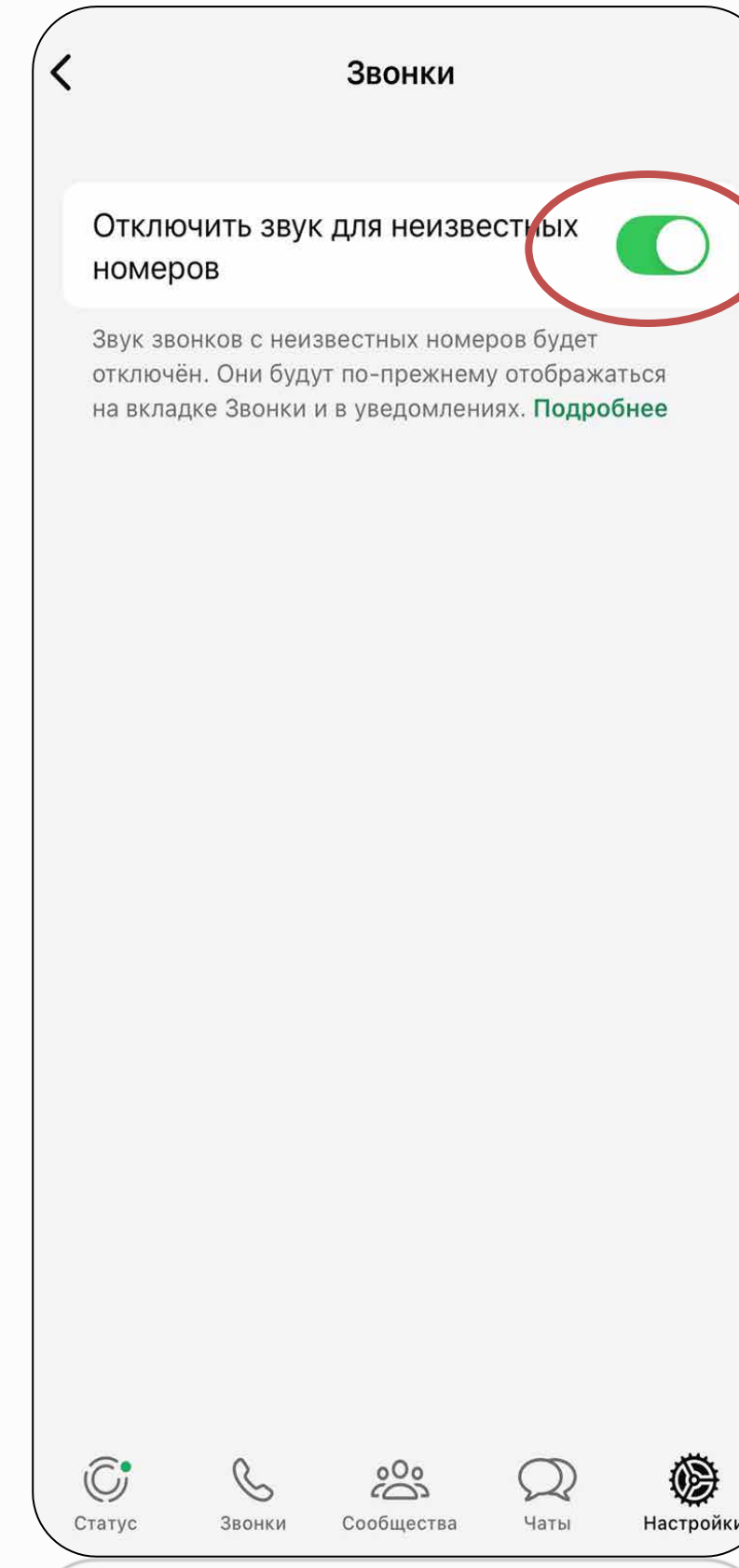
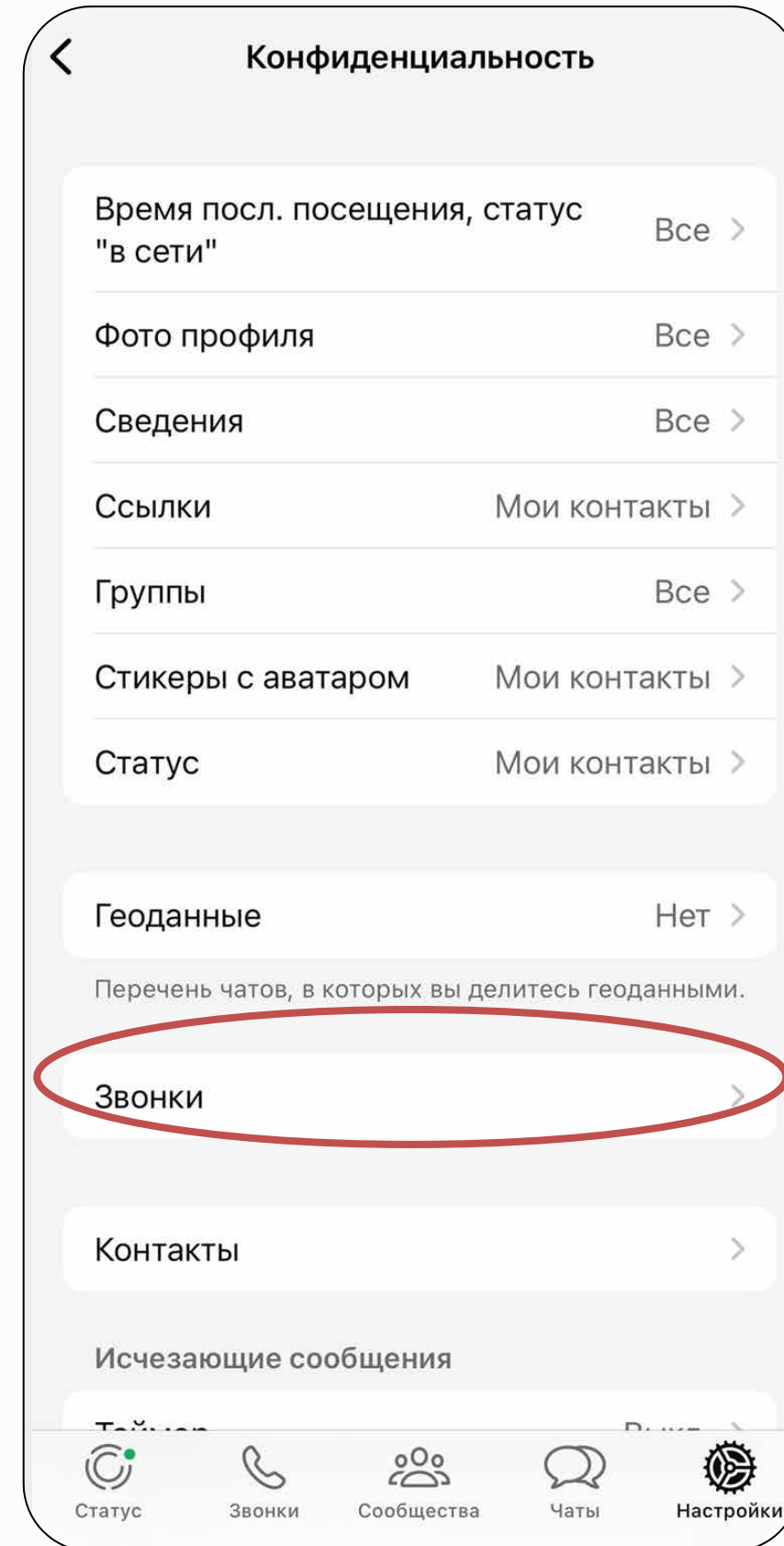
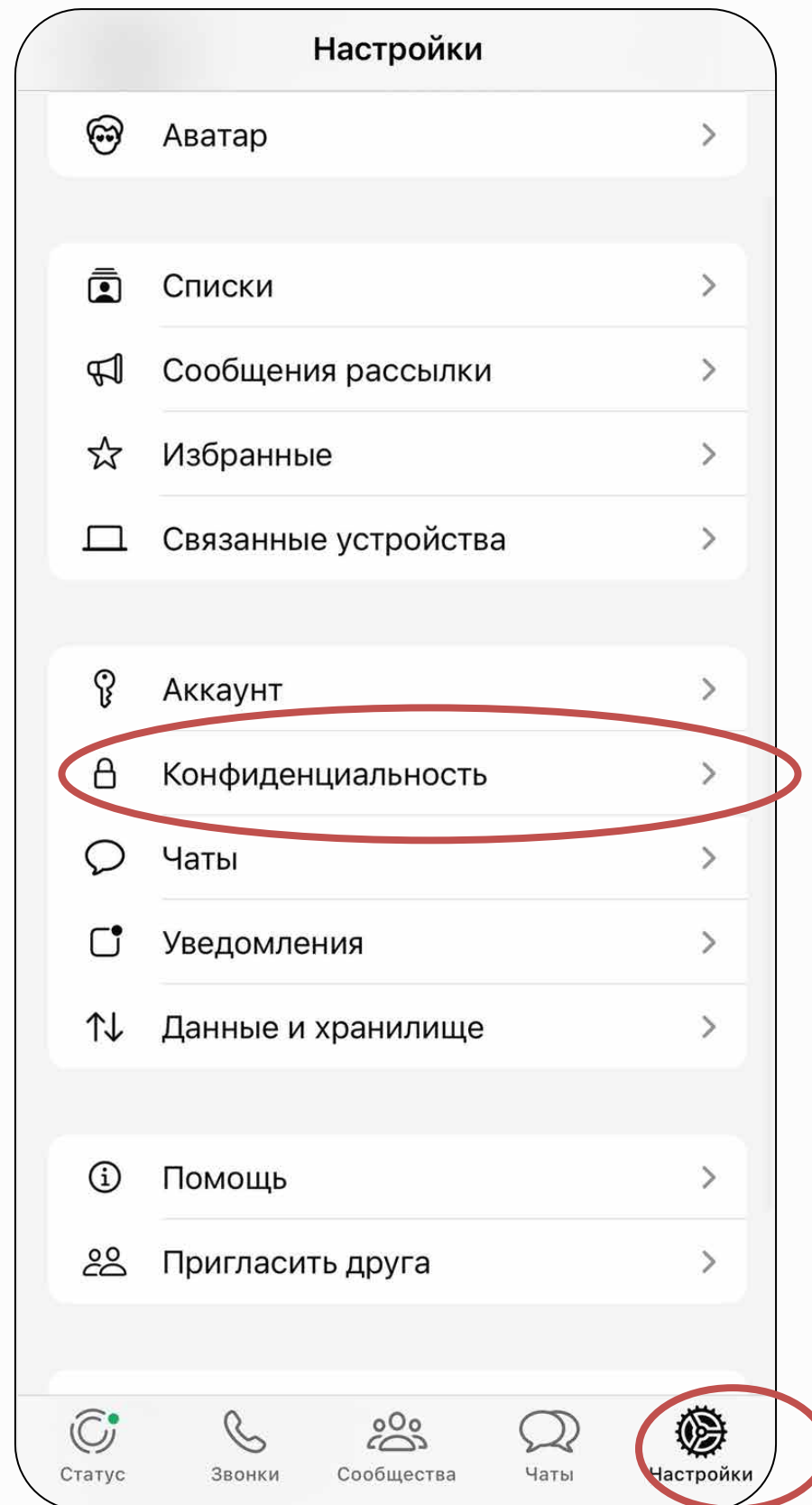
Врач - 6 000 000 руб.

Пенсионер – 5 200 000 руб.

Студент – 4 200 000 руб.



Защита от звонков в WhatsApp



Зайдите в Настройки →
Конфиденциальность →
Звонки → Отключить звук
для неизвестных номеров

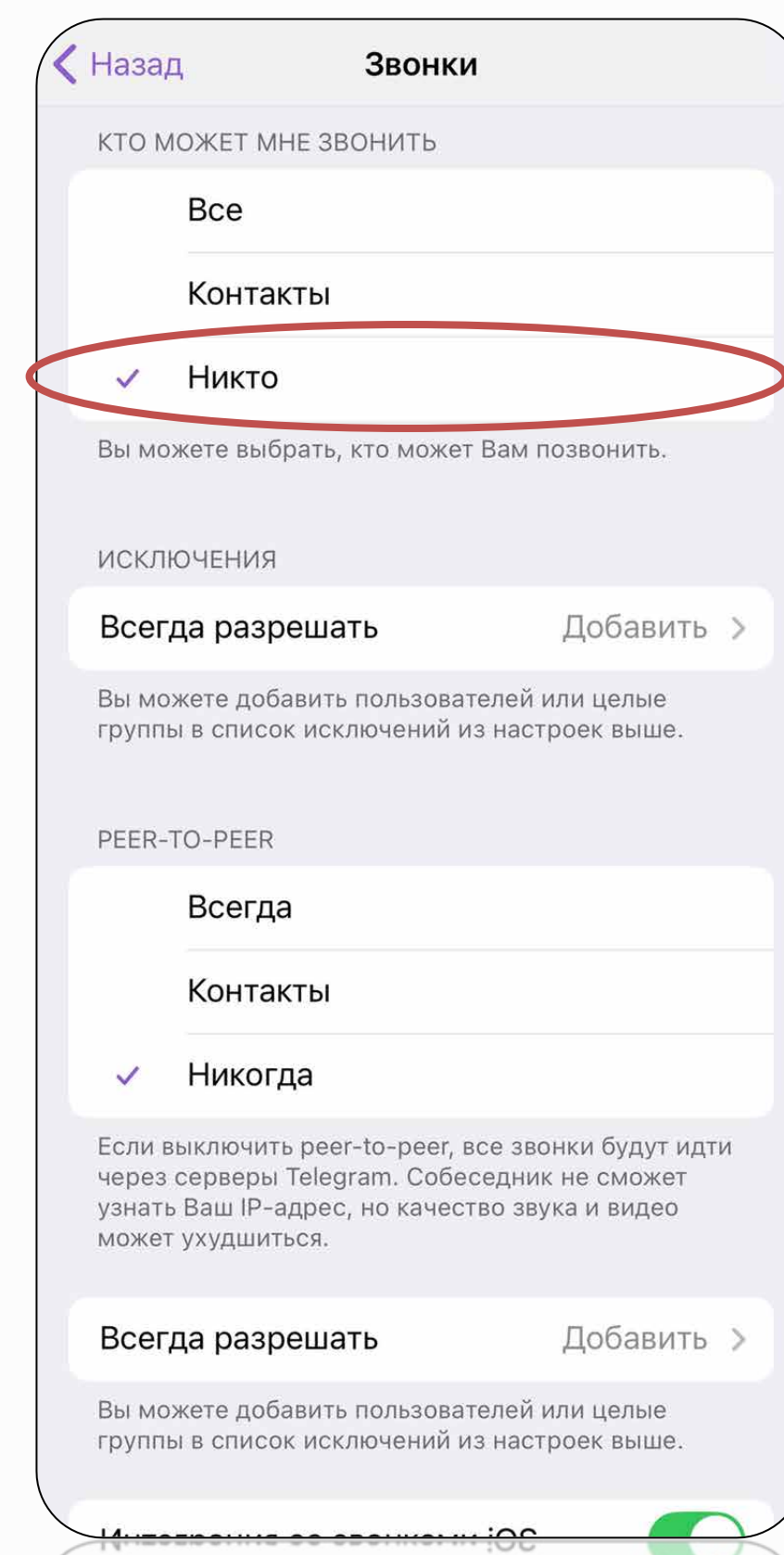
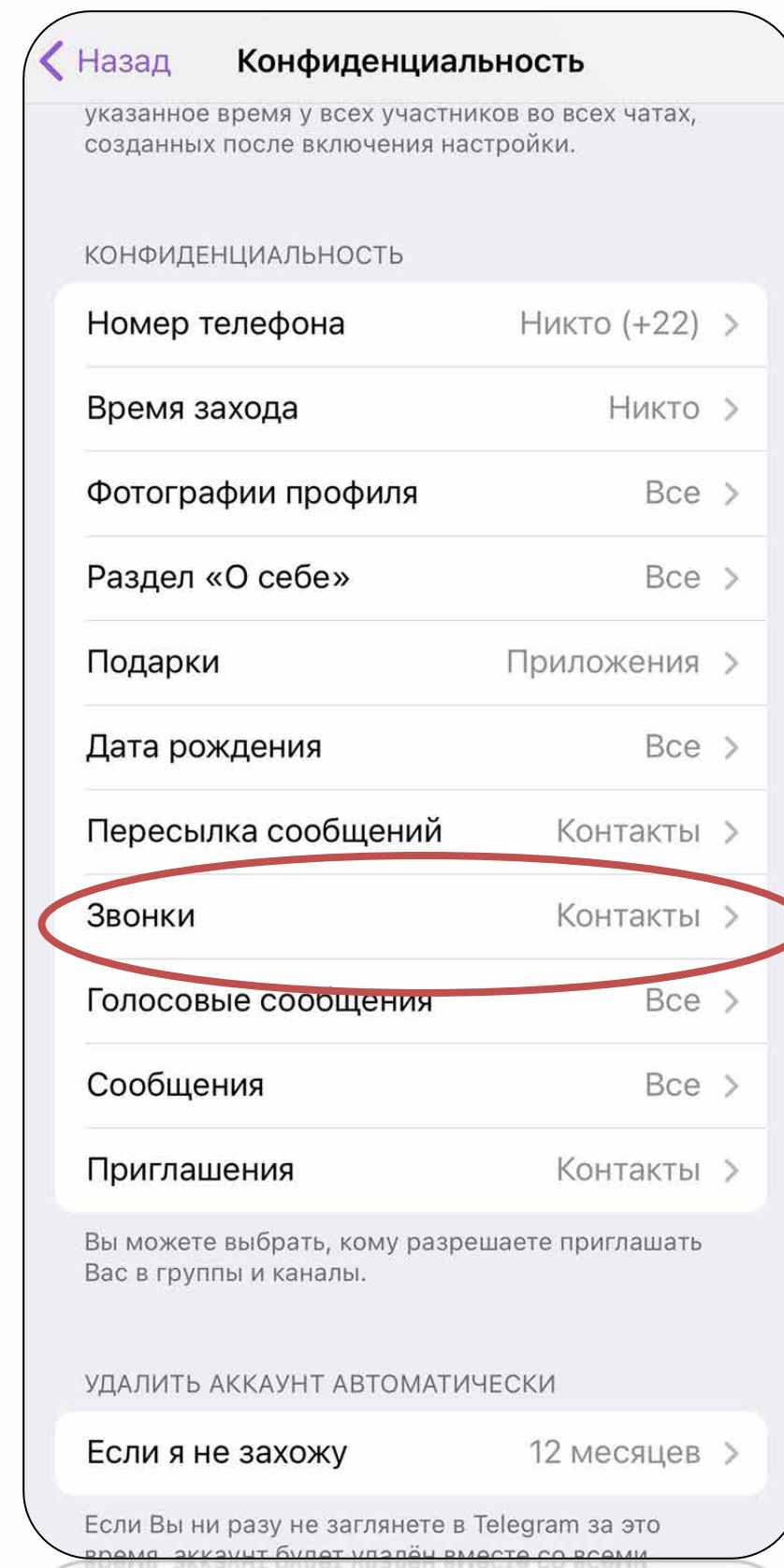
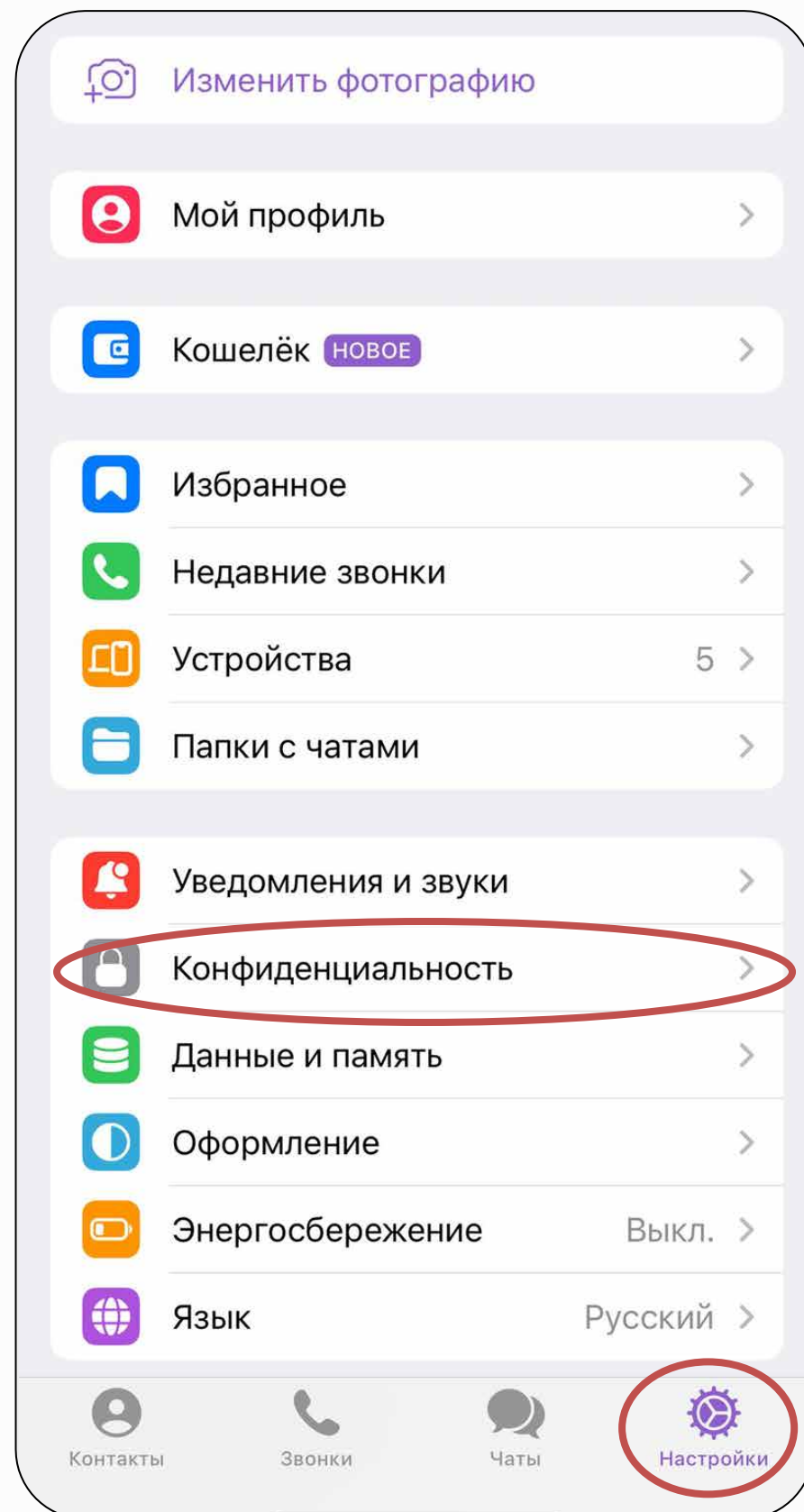
Защита от звонков в Telegram

Зайдите в Настройки → Конфиденциальность и безопасность → Номер телефона.

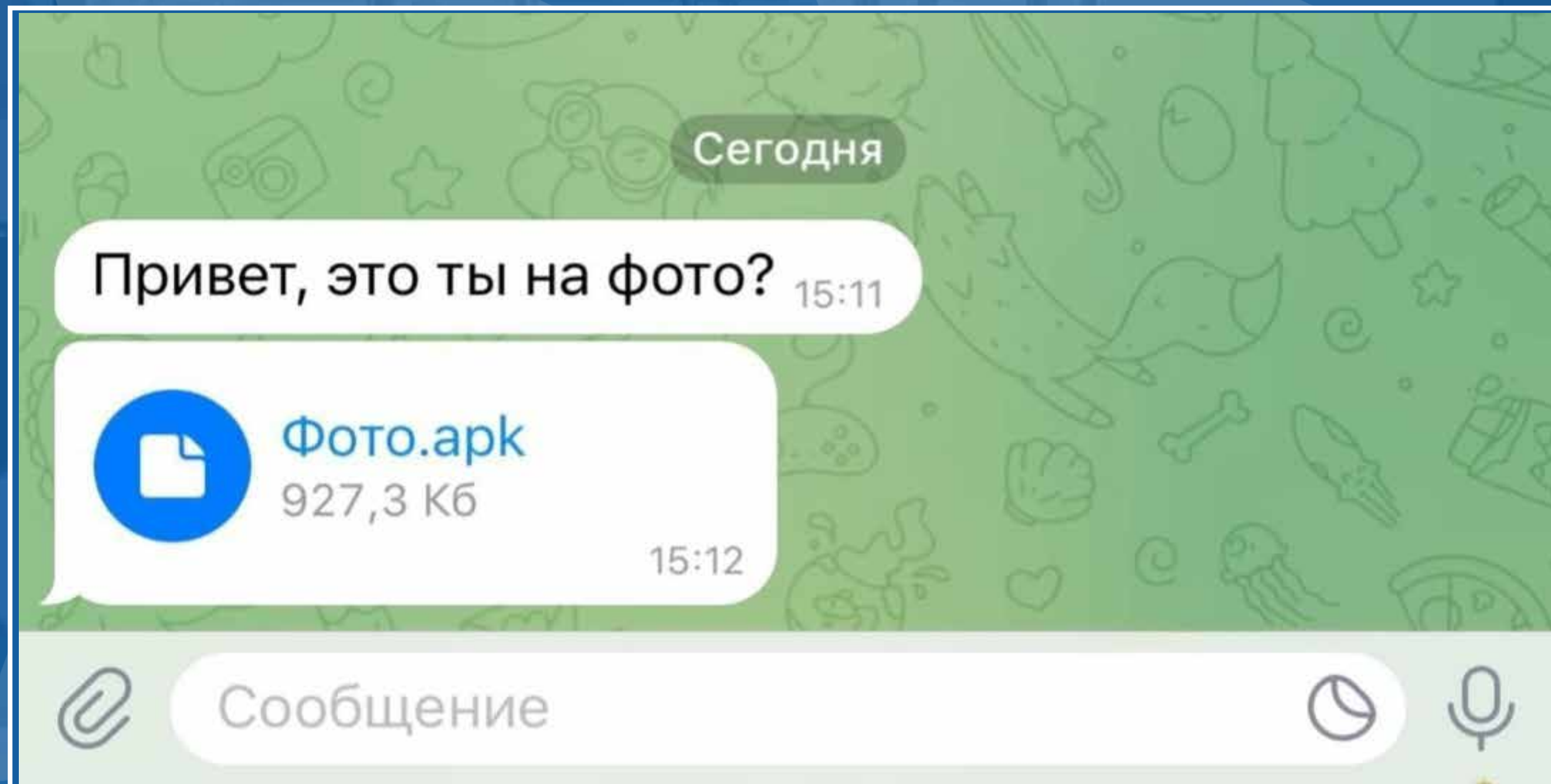
Выберите «Кто может видеть мой номер» → «Мои контакты» или «Никто».

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.

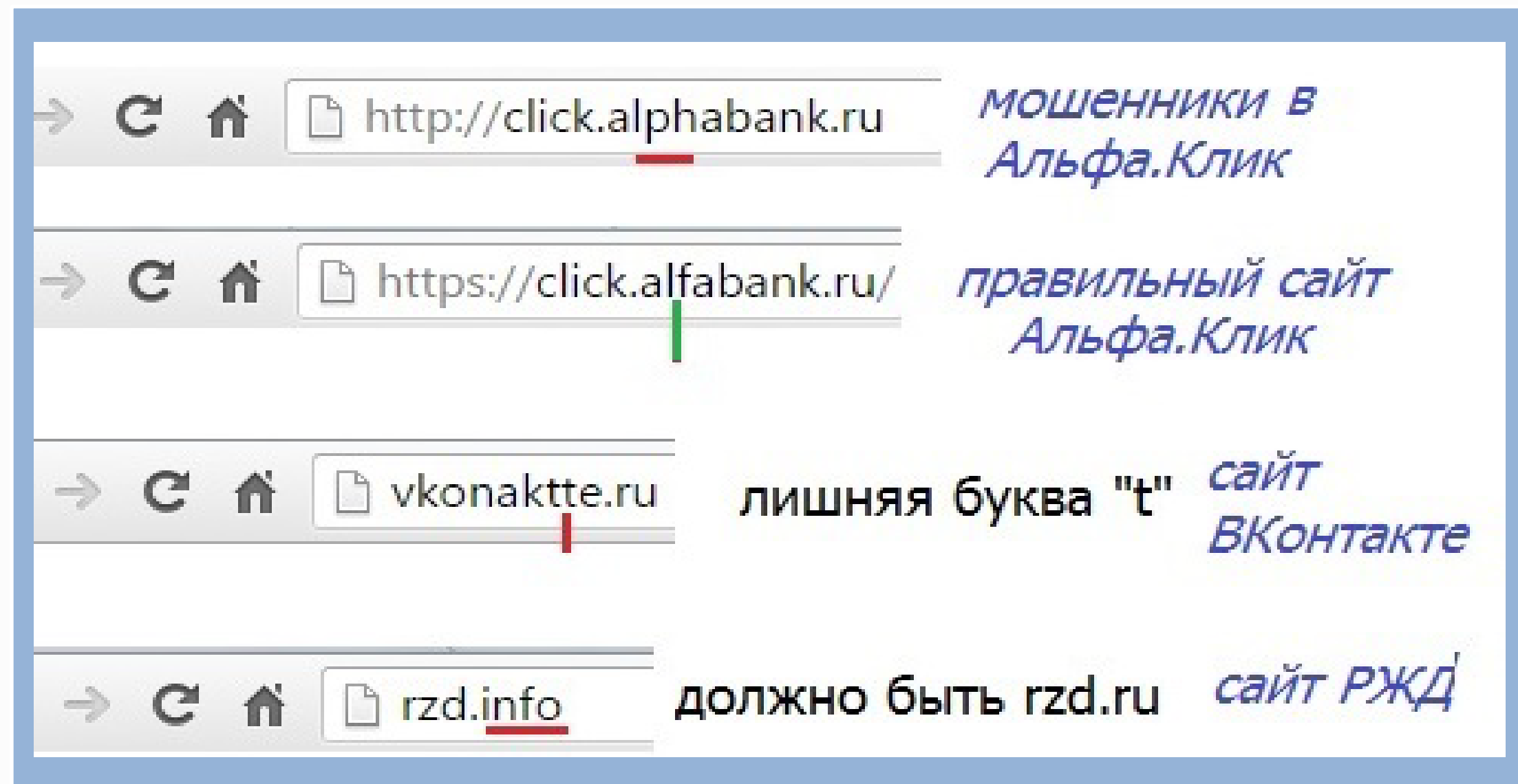


Новый вид мошенничества в мессенджерах



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

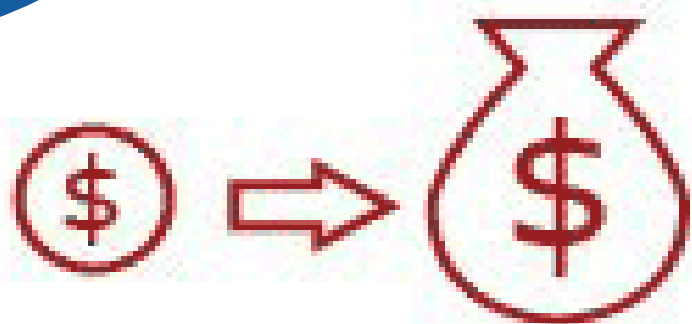
Телефоны

Адрес сайта

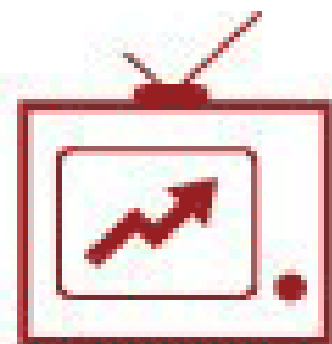


Проверьте продавца / покупателя при помощи различных сервисов. Например на сайте «Доверие в сети»

Признаки финансовой пирамиды



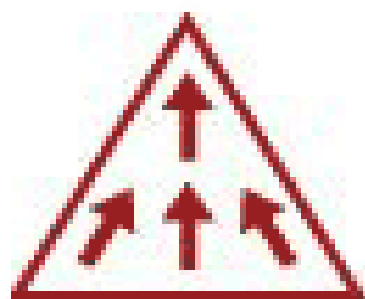
Вкладчикам обещают высокую доходность



В рекламе компании сообщается, что высокая доходность обусловлена новыми сверхприбыльными видами инвестирования



Вкладчиков призывают не раздумывать долго, а быстрее вкладывать деньги



Выплаты клиентам вычитаются не из прибыли компании, а из вкладов предыдущих клиентов



Скрывается информация о руководстве компании и ее реквизитах



Вкладчиков требуют уплатить регистрационный сбор, а размер прибыли зависит от количества привлеченных лично ими клиентов

Как себя обезопасить?

Финансовая пирамида (также инвестиционная пирамида, схема Понци) — мошенническая схема, которая имитирует успешный инвестиционный проект. Доход первым участникам выплачивается за счёт средств последующих. В отличие от реального бизнеса, пирамида не производит товары или услуги, а просто перераспределяет средства между участниками..

Совет 01

Проверять брокерскую компанию на сайте Банка России на наличие лицензии (<https://cbr.ru/finorg/>);

Совет 02

Не доверять рекламе о биржах в социальных сетях;

Совет 03

Не верить заманчивым и убедительным обещаниям о высокой доходности и отсутствии риска.

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.

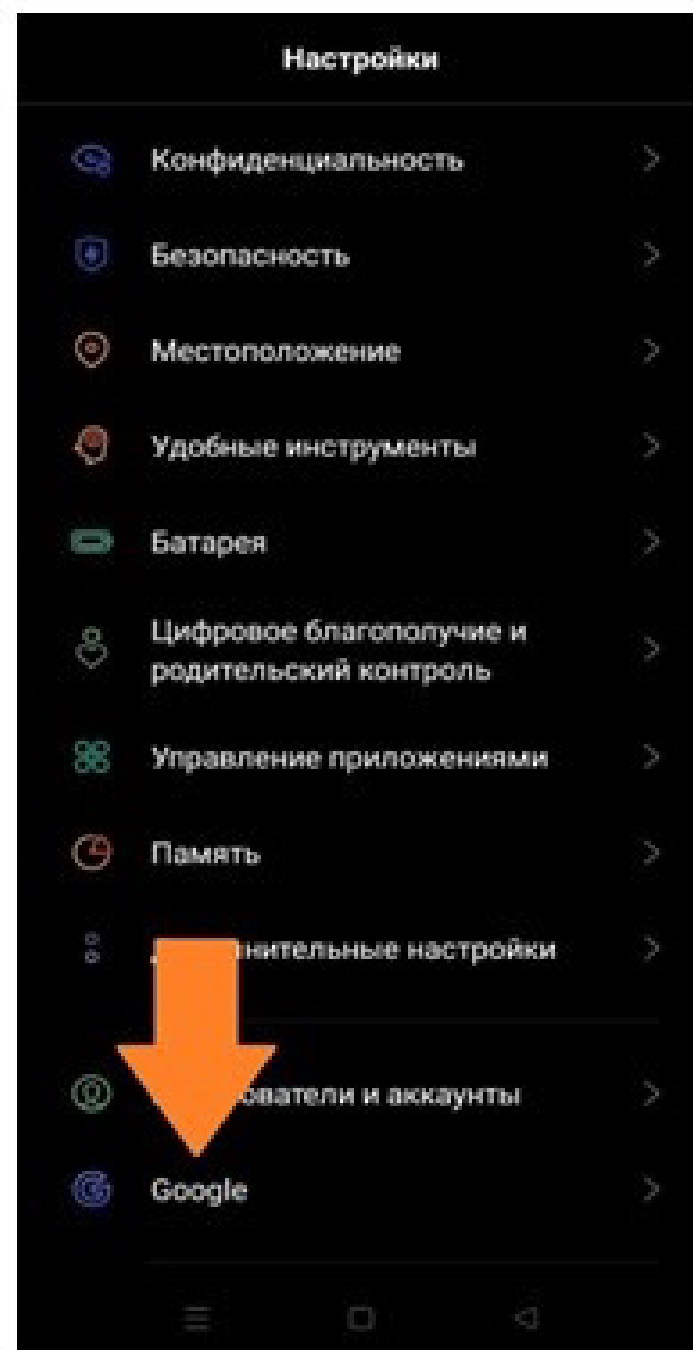


Уделяйте больше внимания своему ребенку. Чаще разговаривайте с ним, чтобы он делился с Вами о своем окружении, как прошел его день и внимательно следите за изменением в его поведении

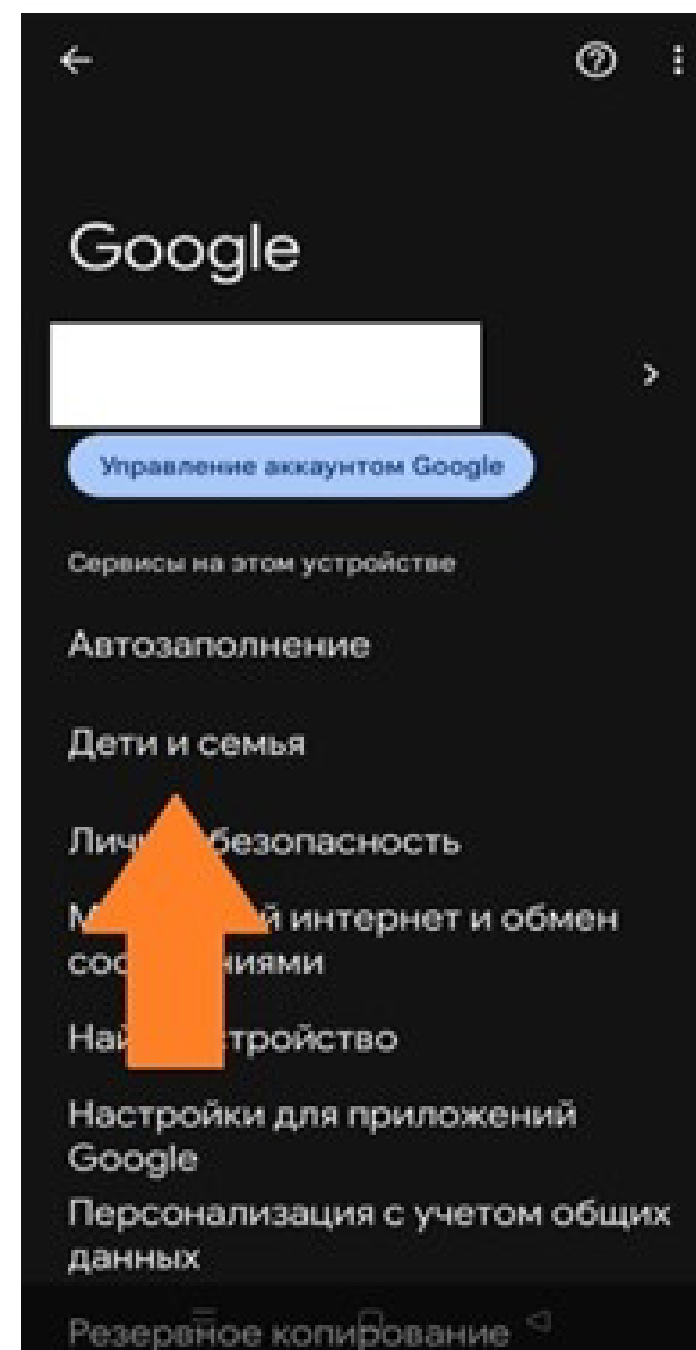
Установите дома родительский контроль на телевизор и его аккаунты в интернете.

1. Откройте «Настройки» на устройстве ребенка.

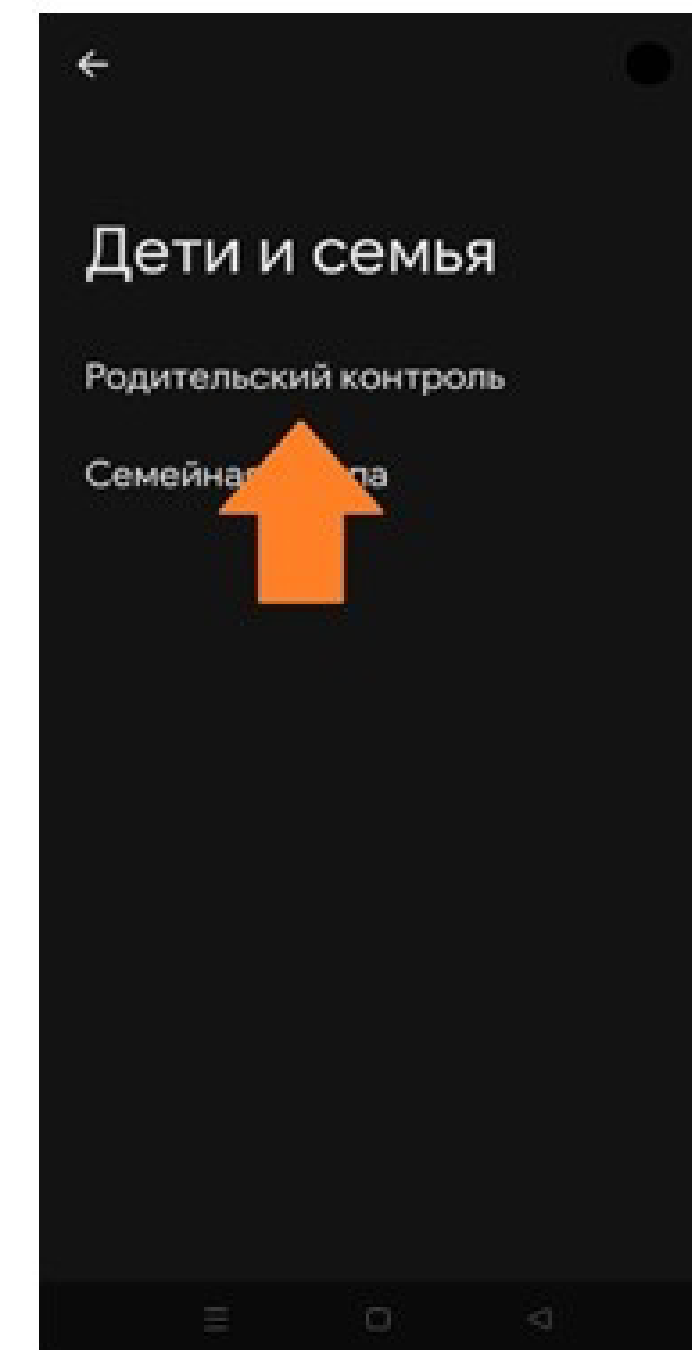
2. Выберите «Google»



3. «Дети и семья»



4. «Родительский контроль»

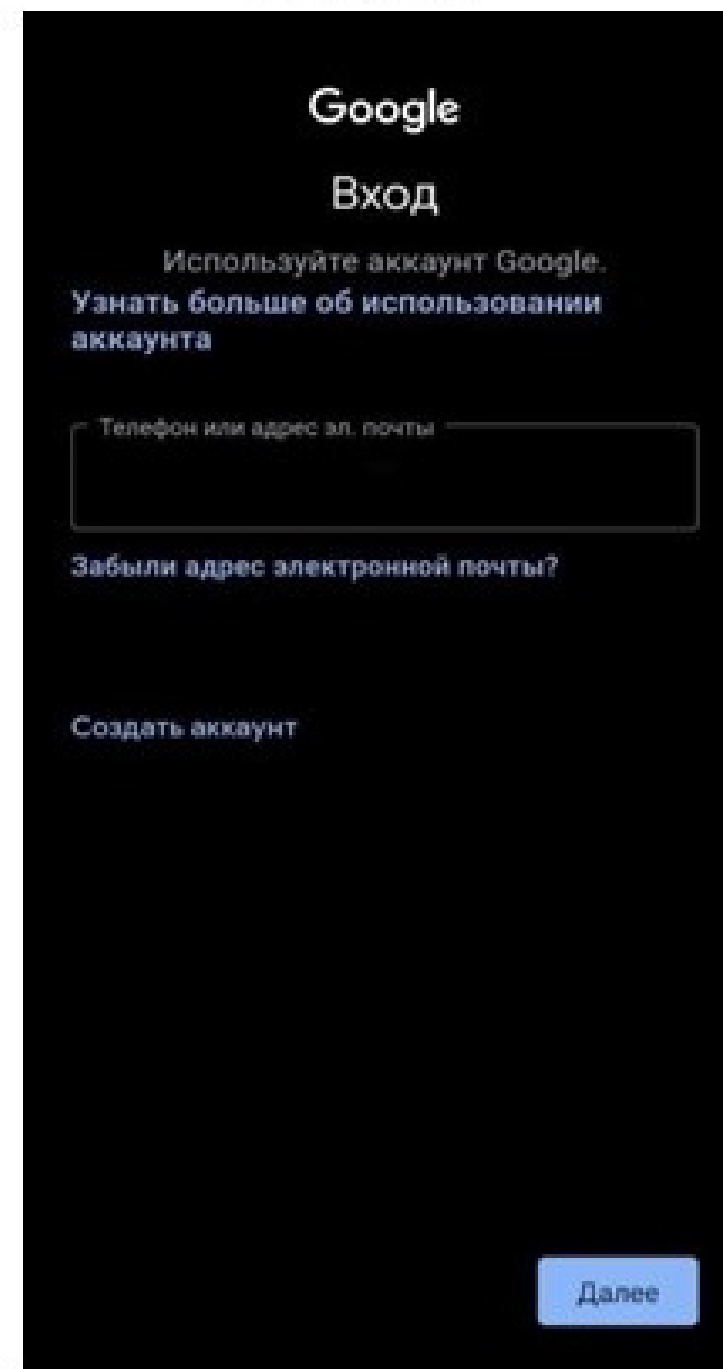


Установите дома родительский контроль на телевизор и его аккаунты в интернете.

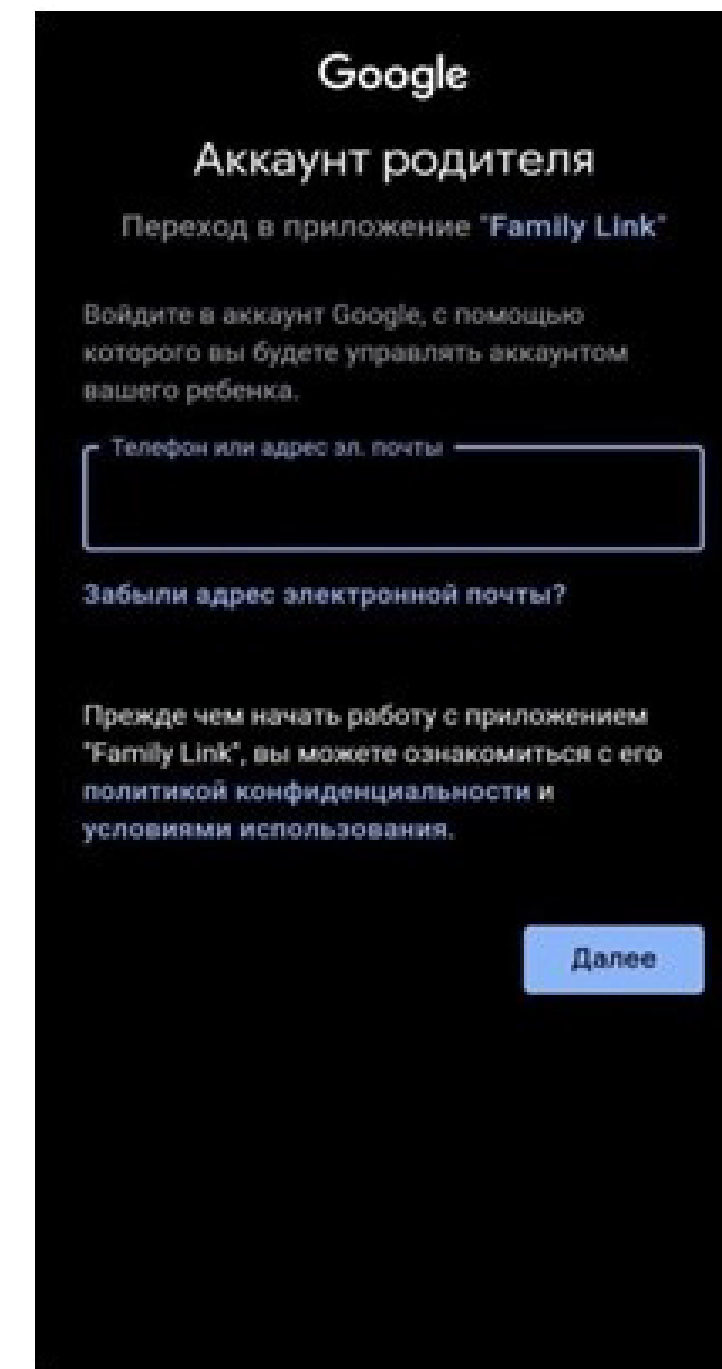
Нажмите «Прислупить»



Выберите аккаунт ребенка или создайте новый.



Войдите в свой «родительский»



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, the logo 'ГОСУСЛУГИ' is displayed. Below it, the heading 'Восстановление пароля' (Password recovery) is visible. A text input field labeled 'Телефон / Email' contains the number '89000000000'. Below this, the heading 'Изменение номера телефона +7 924' (Change phone number +7 924) is shown. A second text input field labeled 'Новый номер телефона' (New phone number) contains the partial number '+7 () - - -'.

Как обезопасить личный кабинет от взлома?

01

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

02

Настроить двухэтапную аутентификацию;

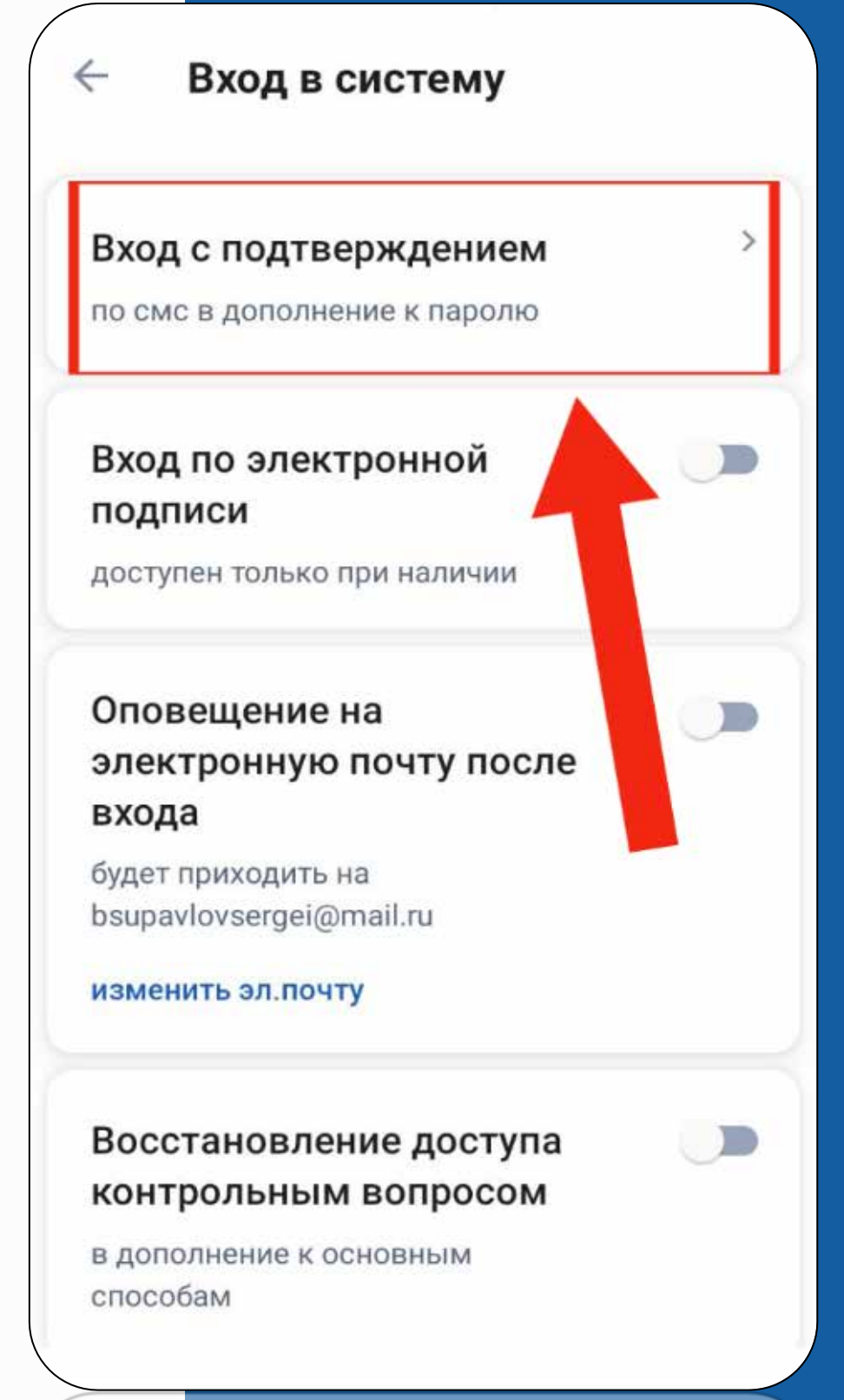
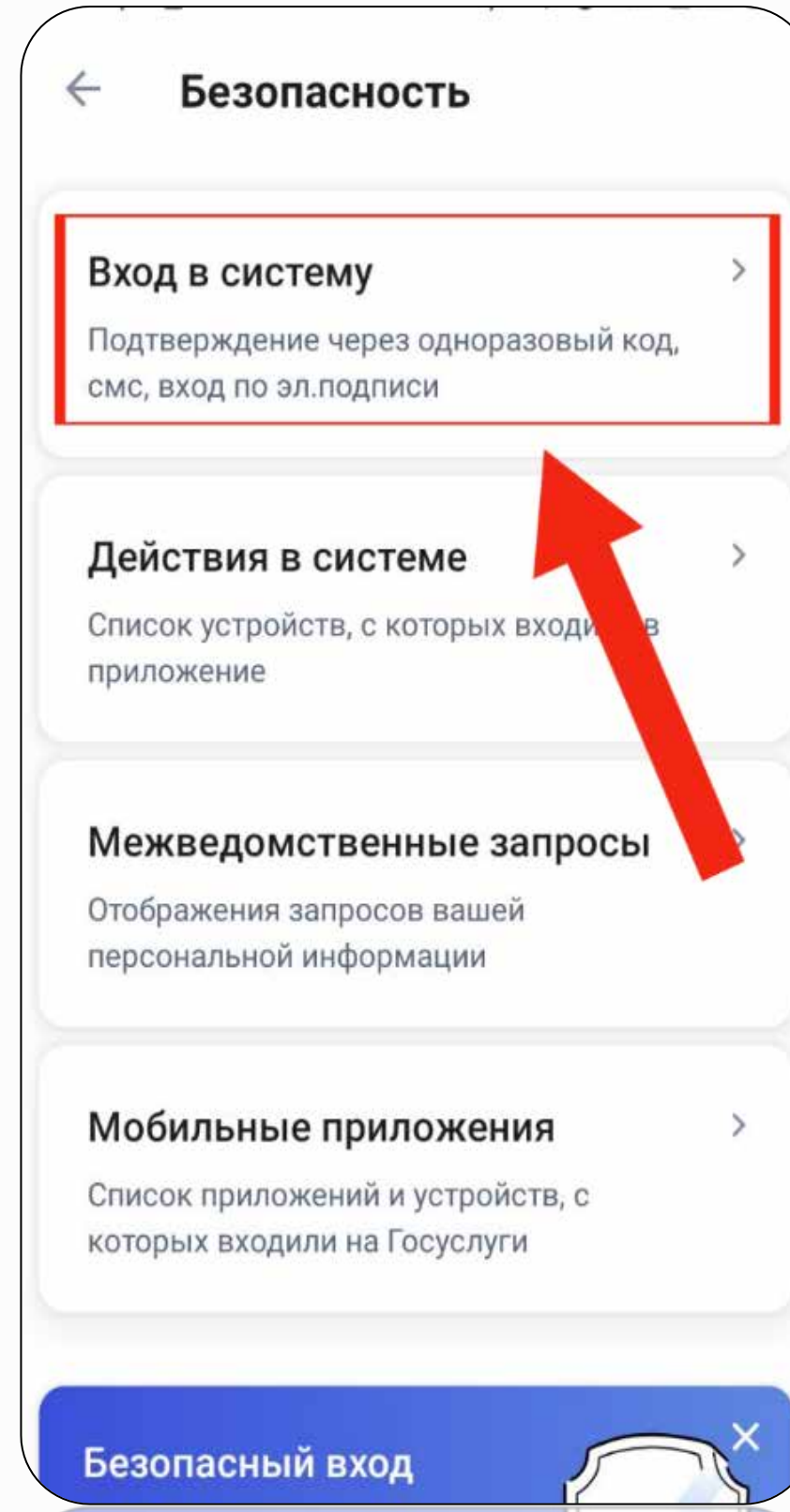
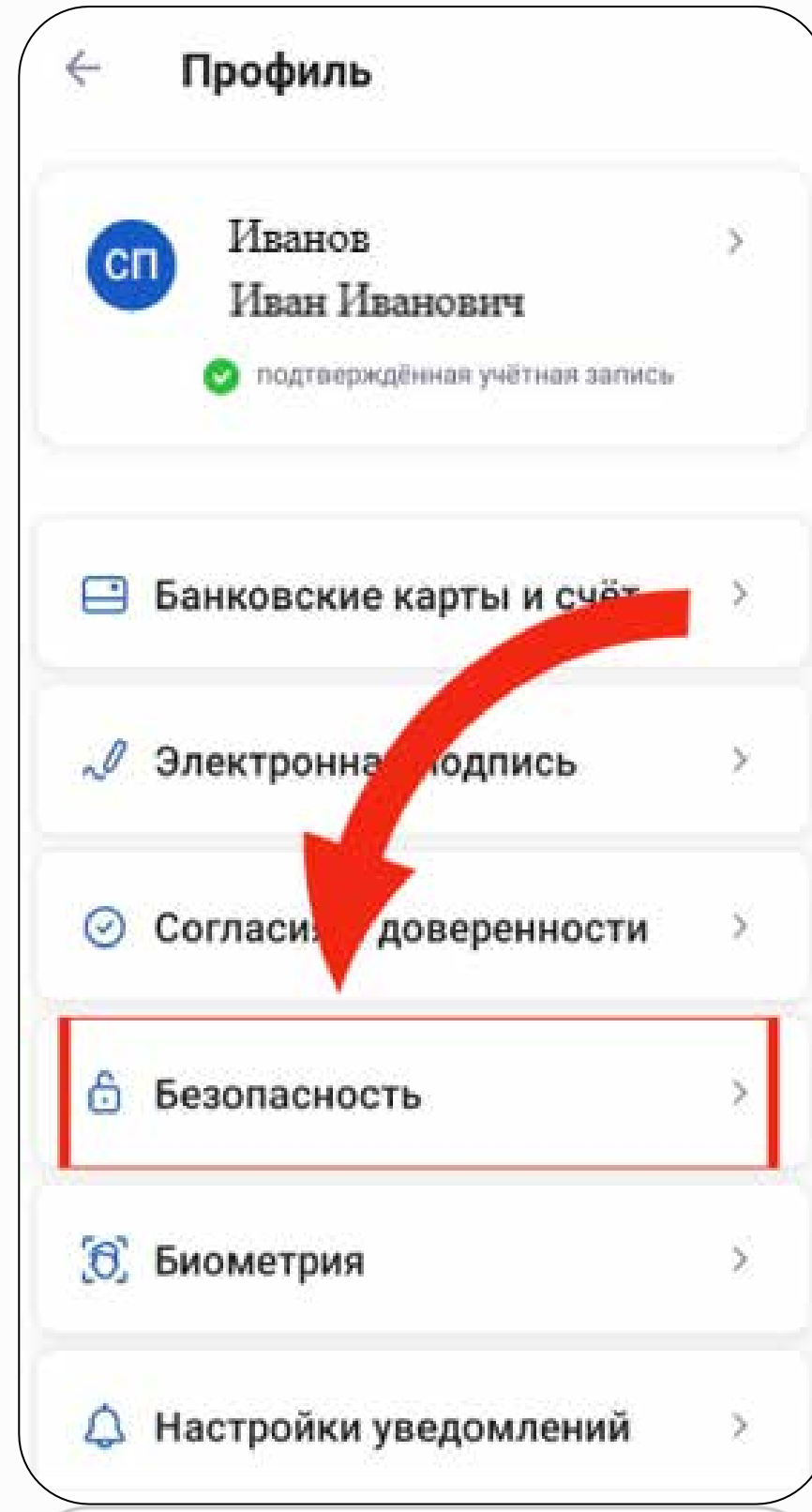
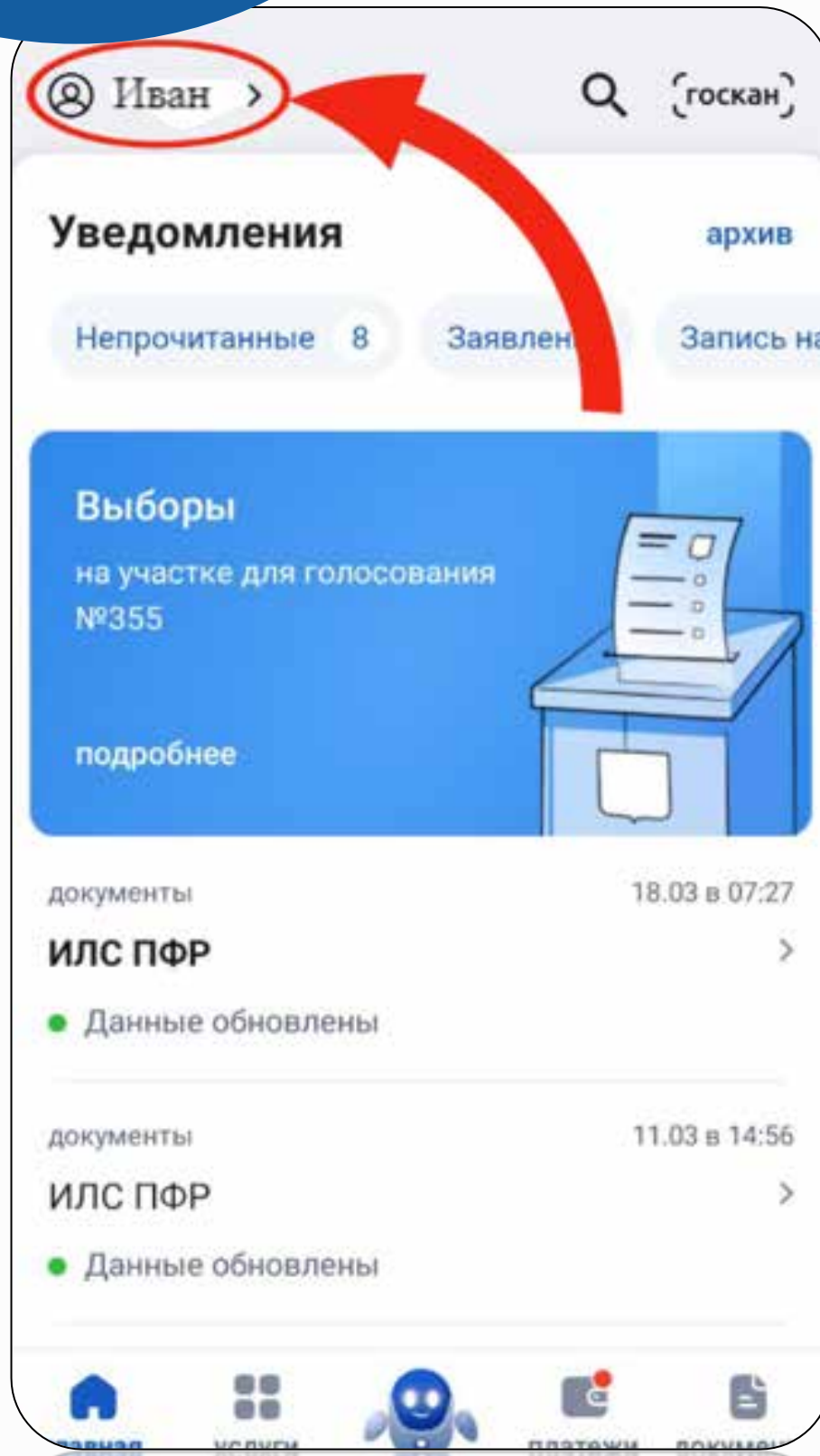
03

Отозвать неизвестные для вас согласия в личном кабинете;

04

Регулярно, раз в полгода необходимо менять пароли доступа.

Дополнительная защита личного кабинета

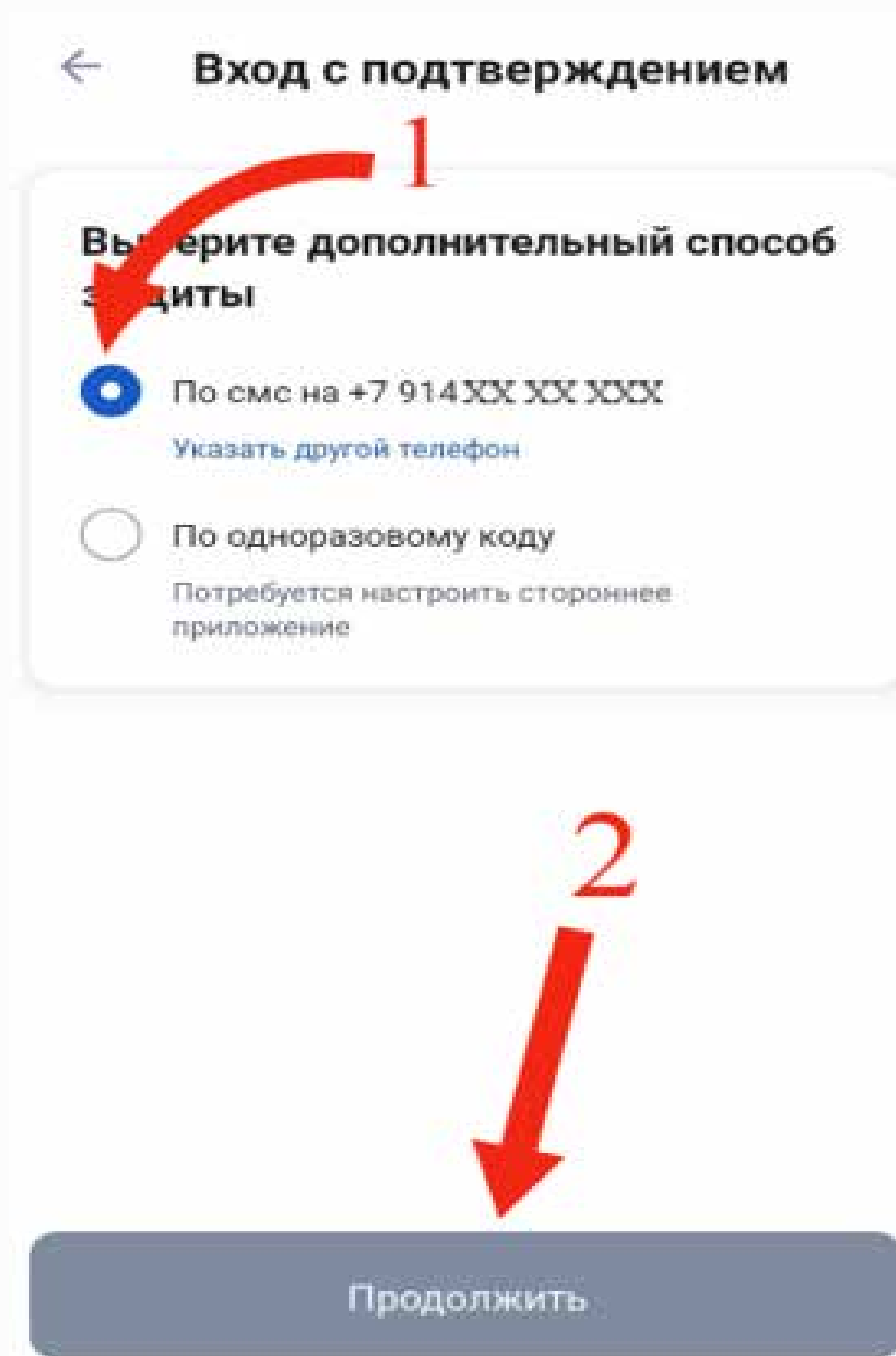




Дополнительная защита личного кабинета

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.



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

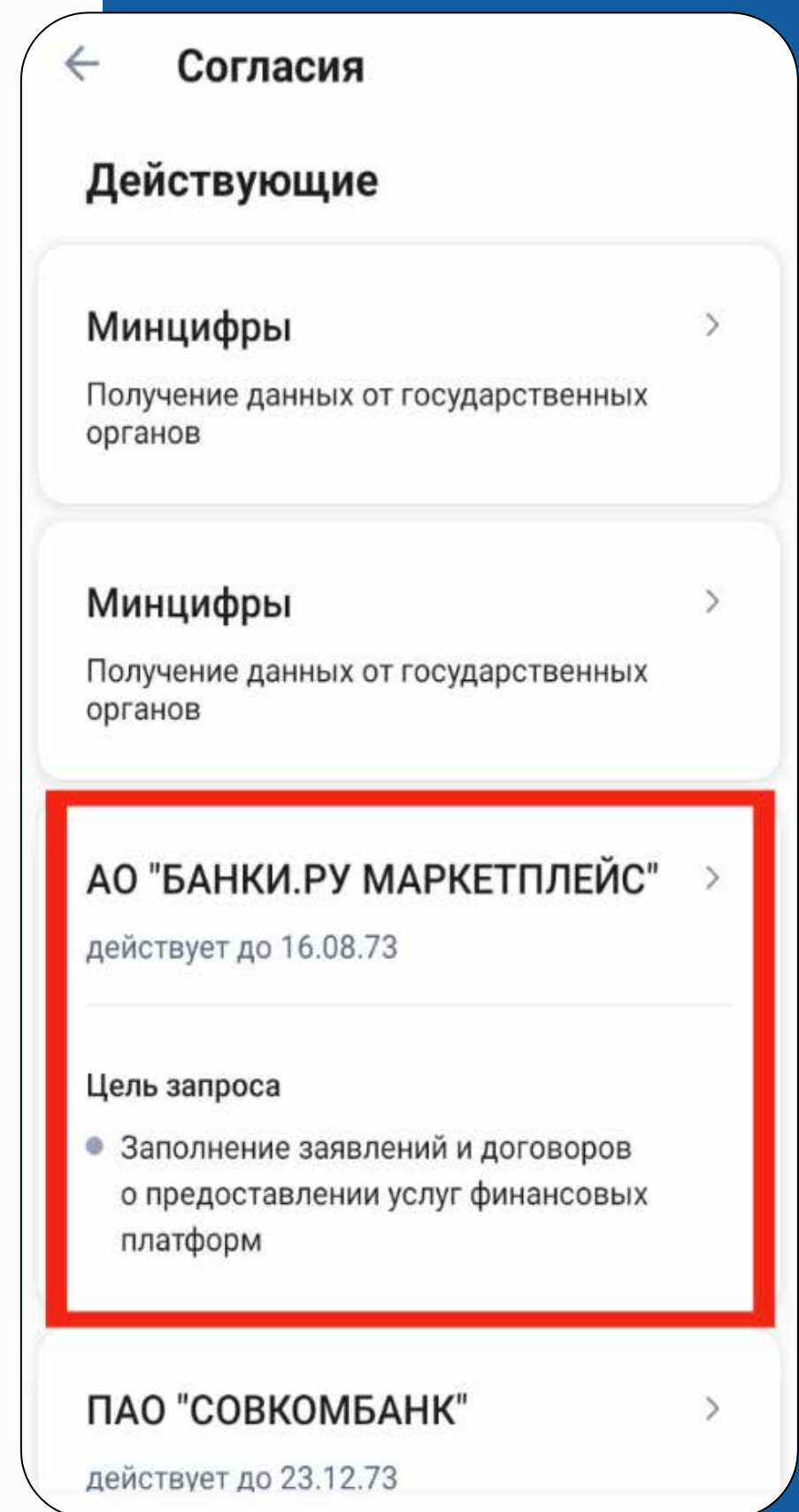
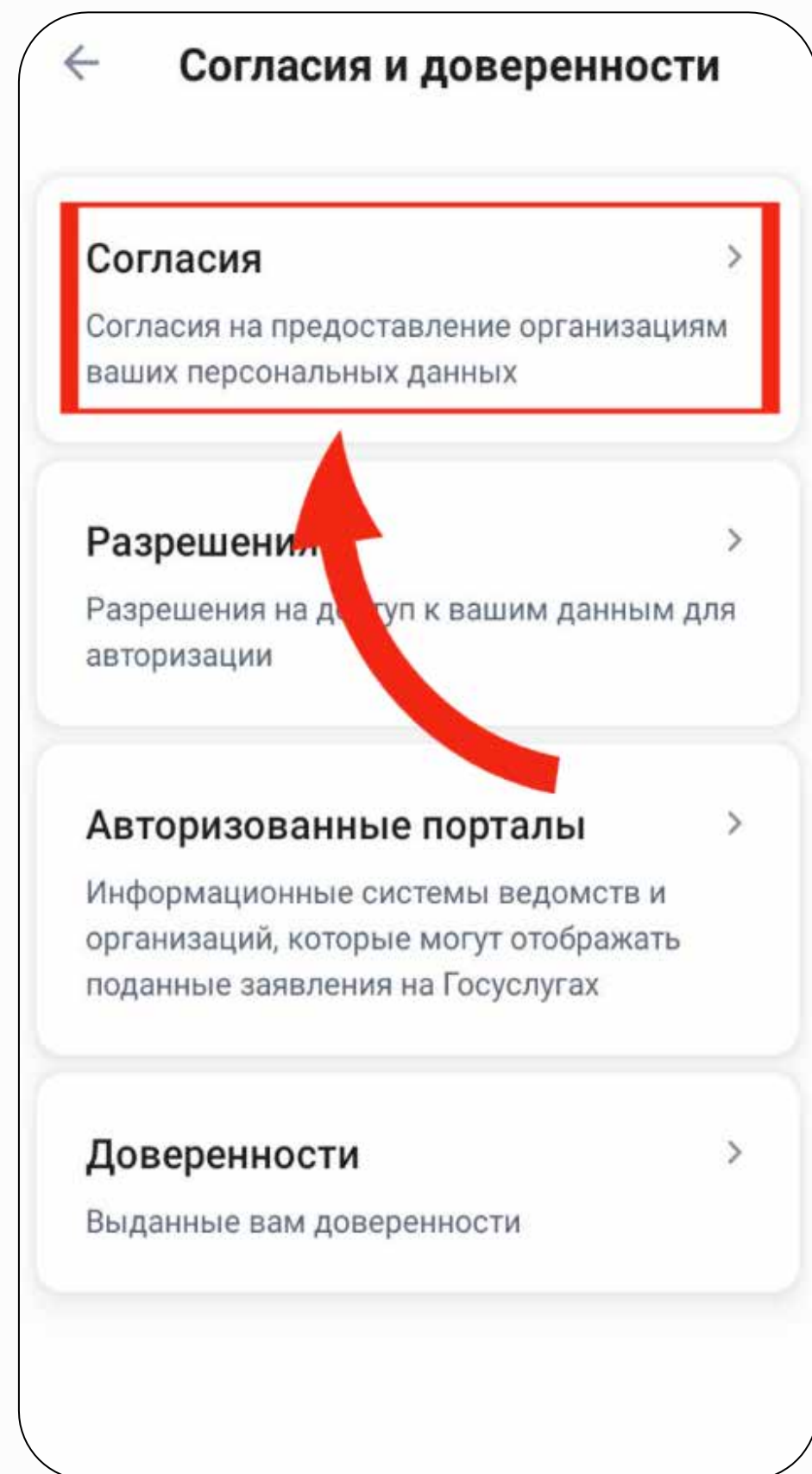
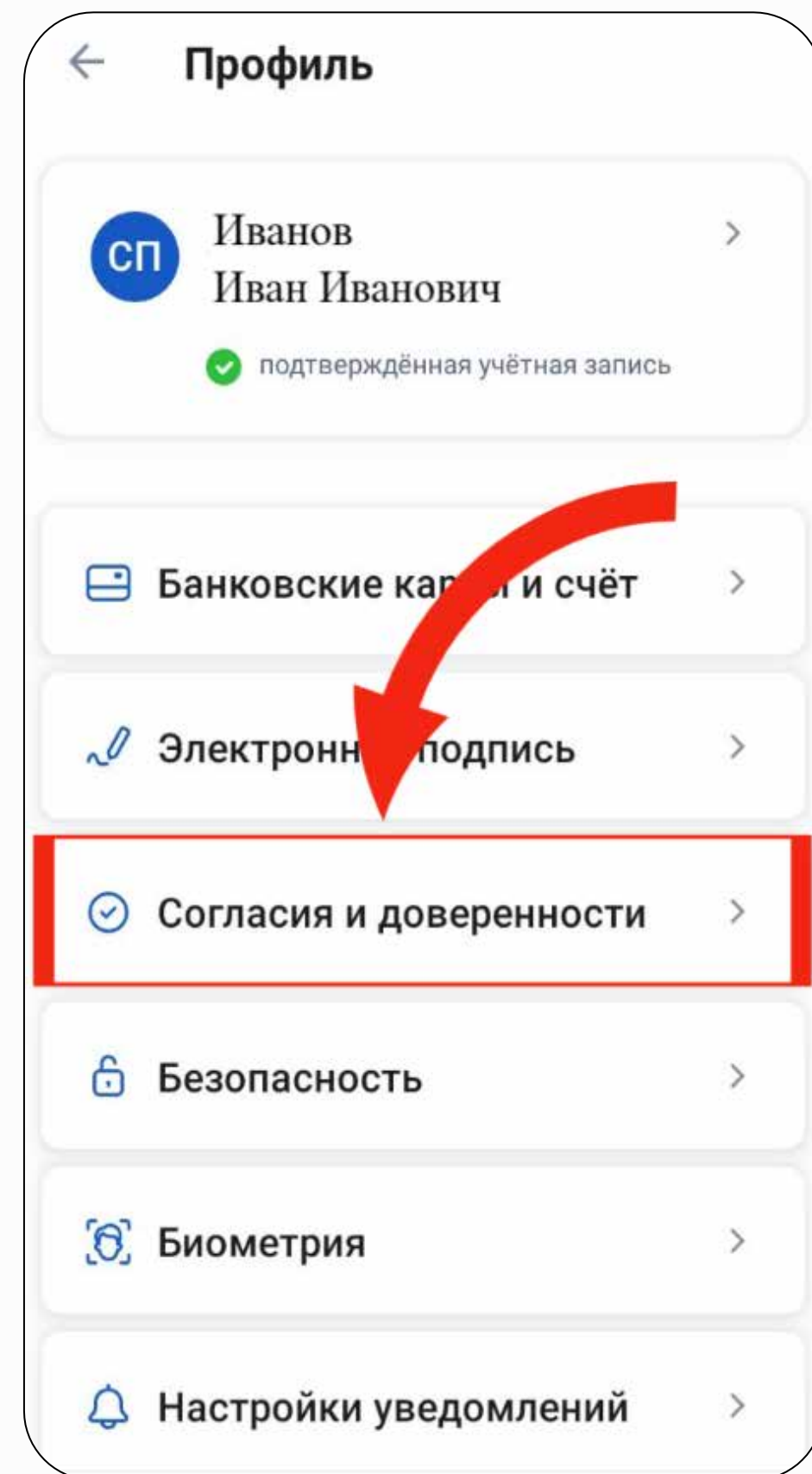
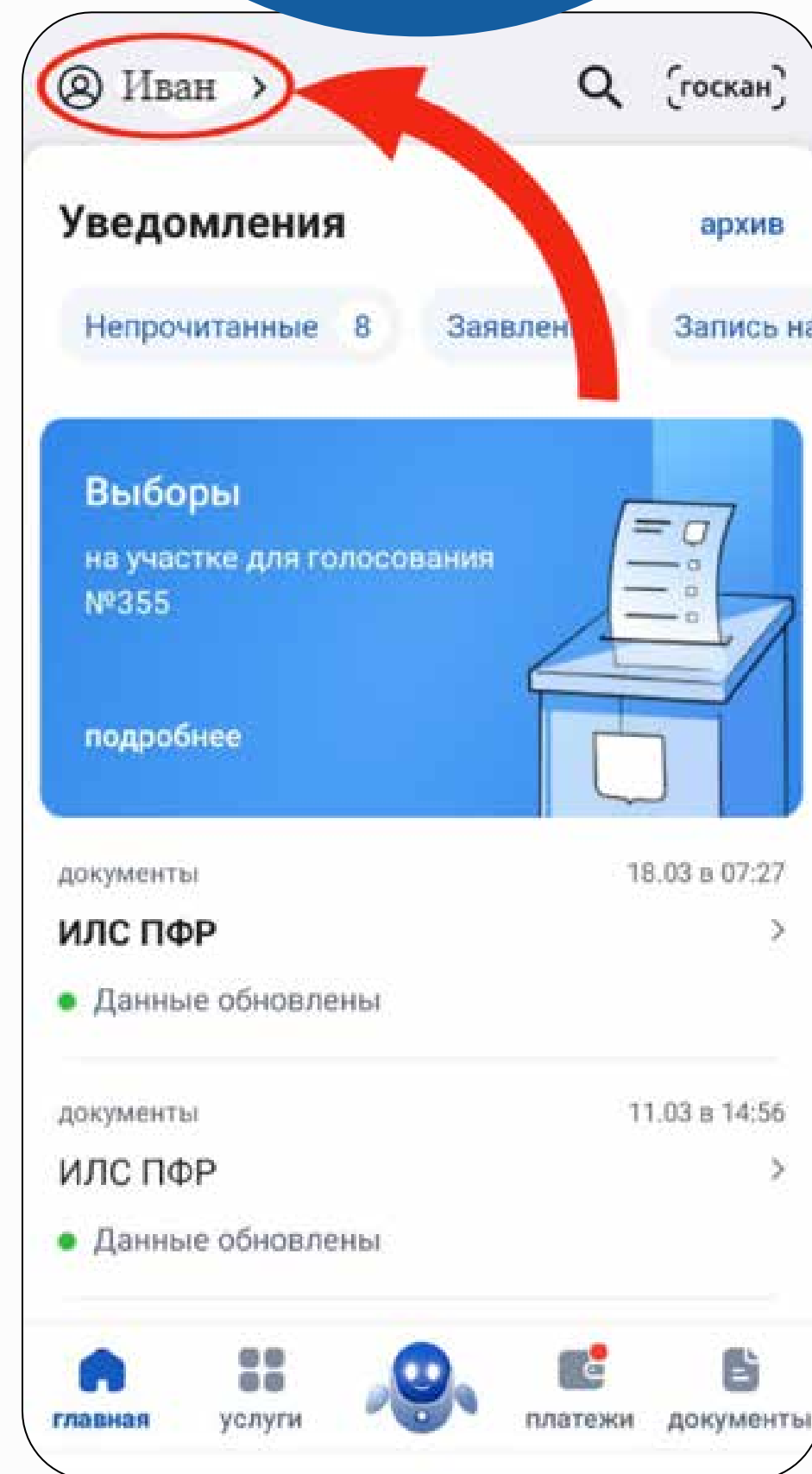
Введите ответ 2

Введите пароль, чтобы подтвердить использование контрольного вопроса для восстановления доступа

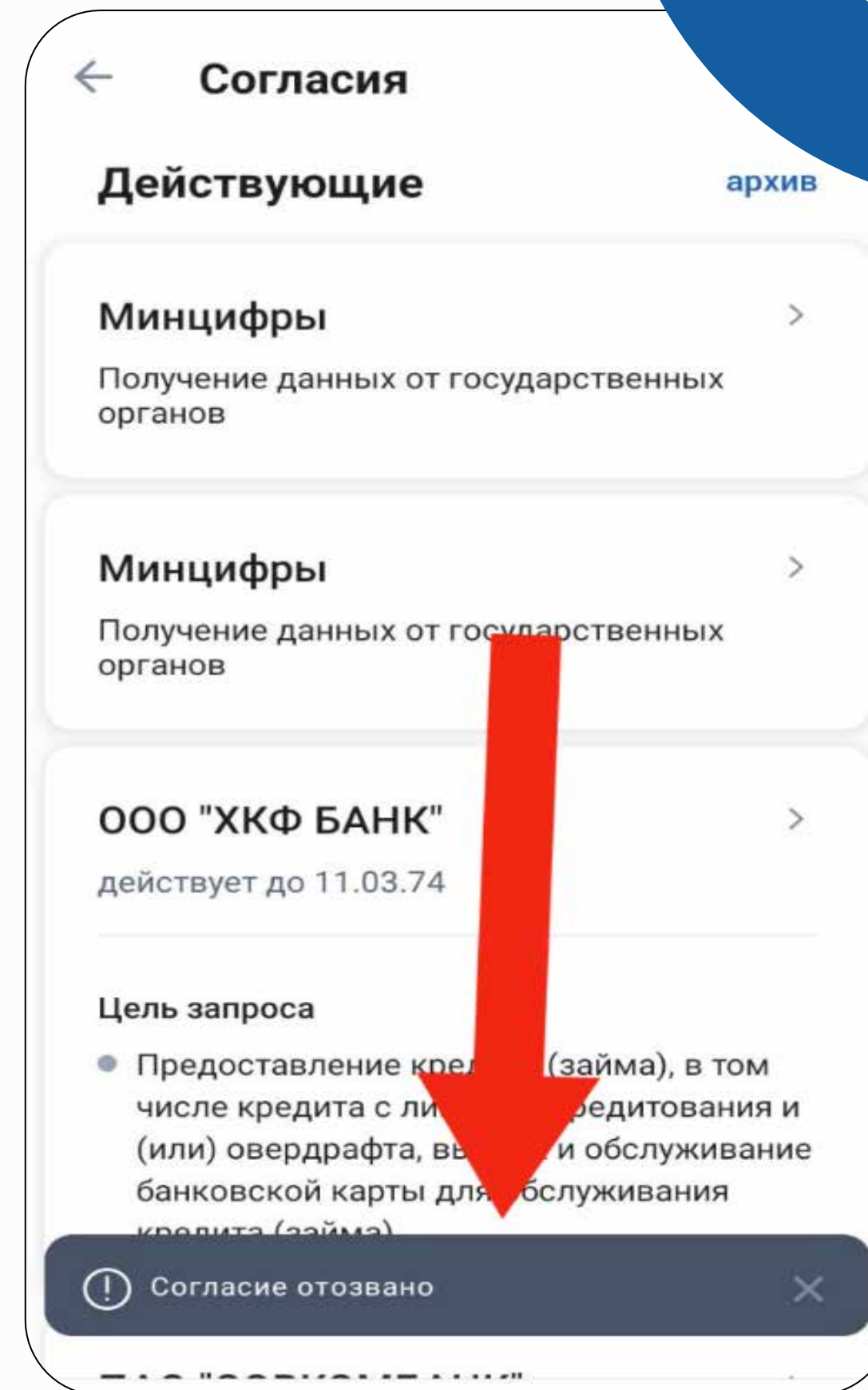
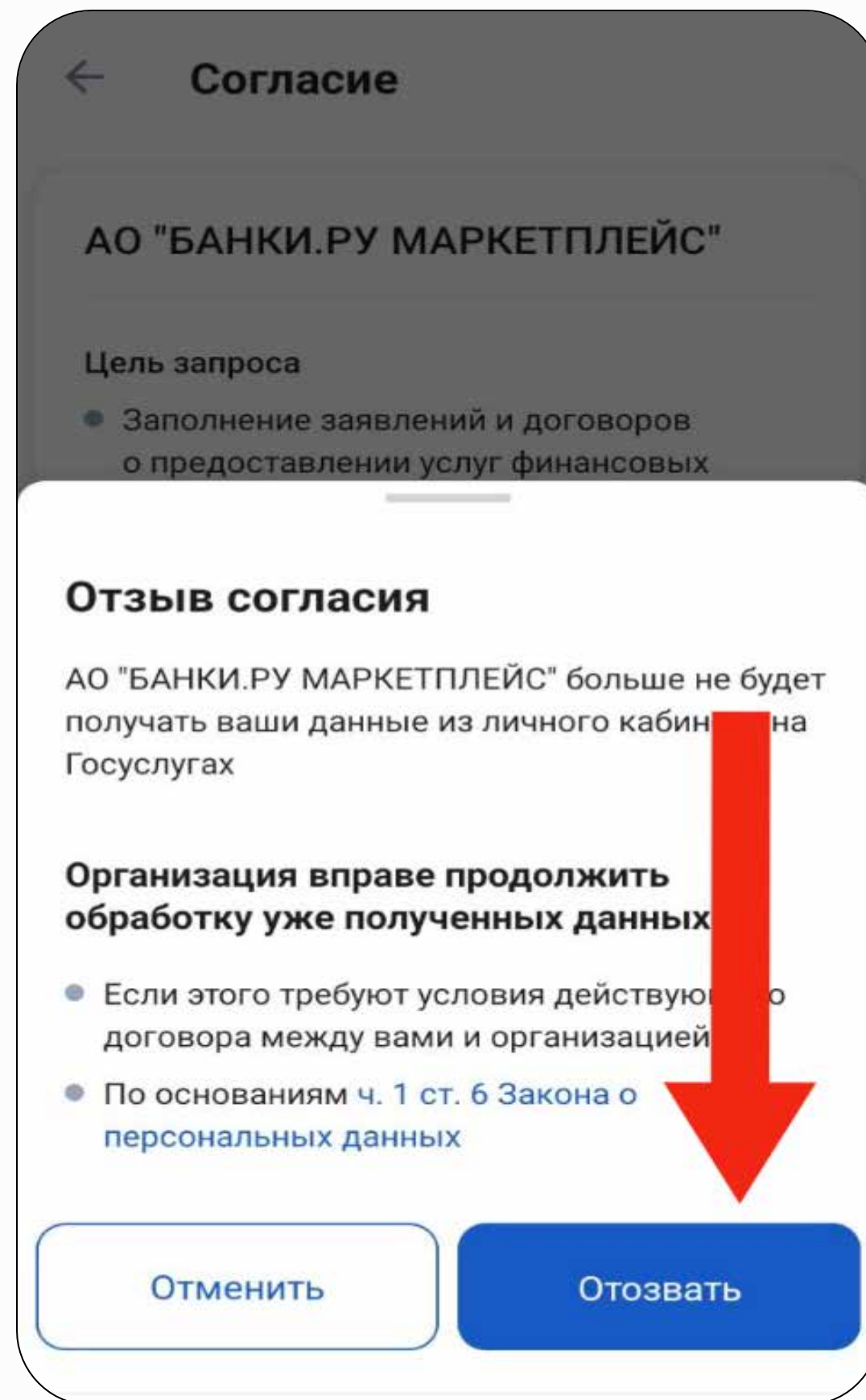
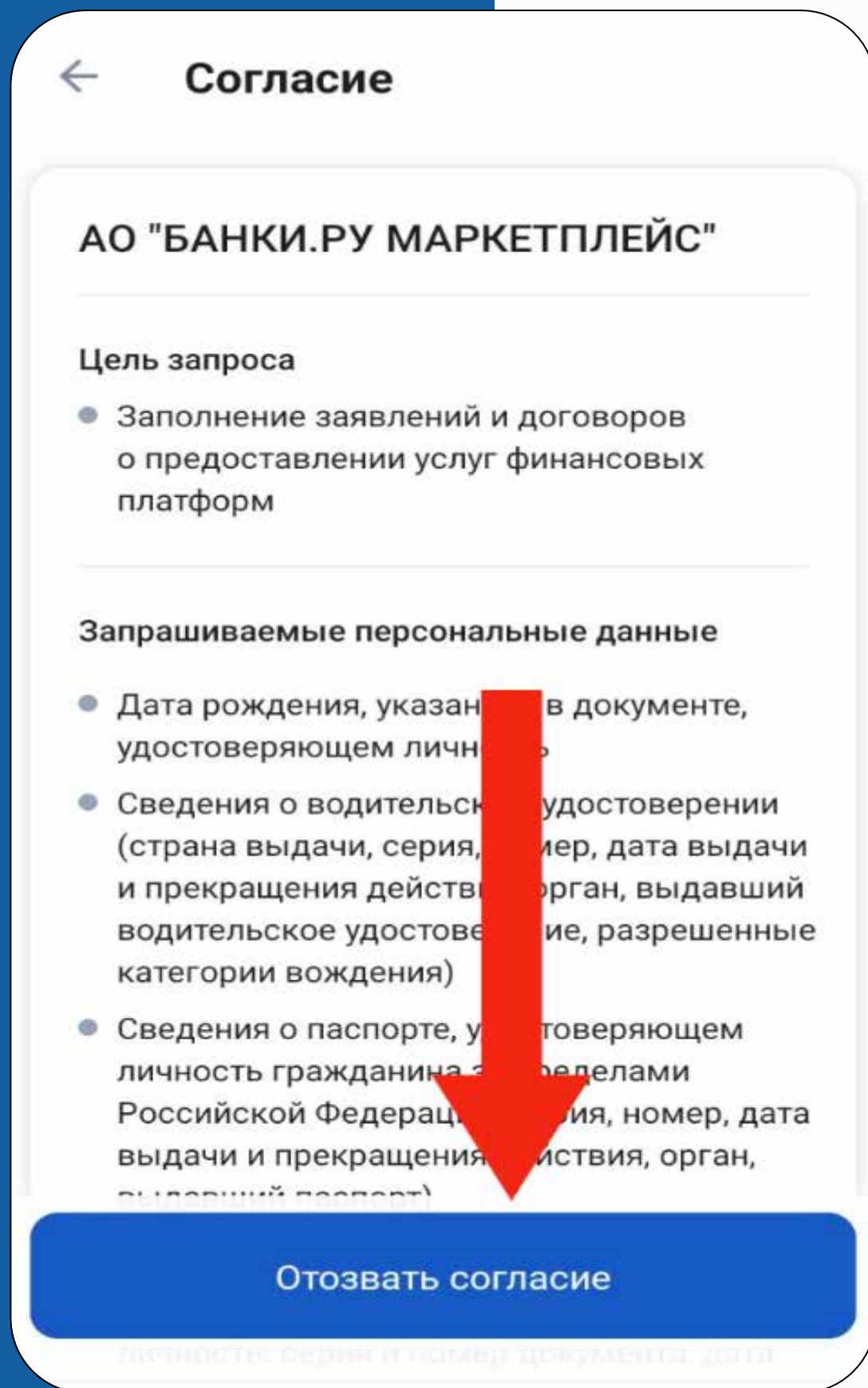
Введите пароль 3

4

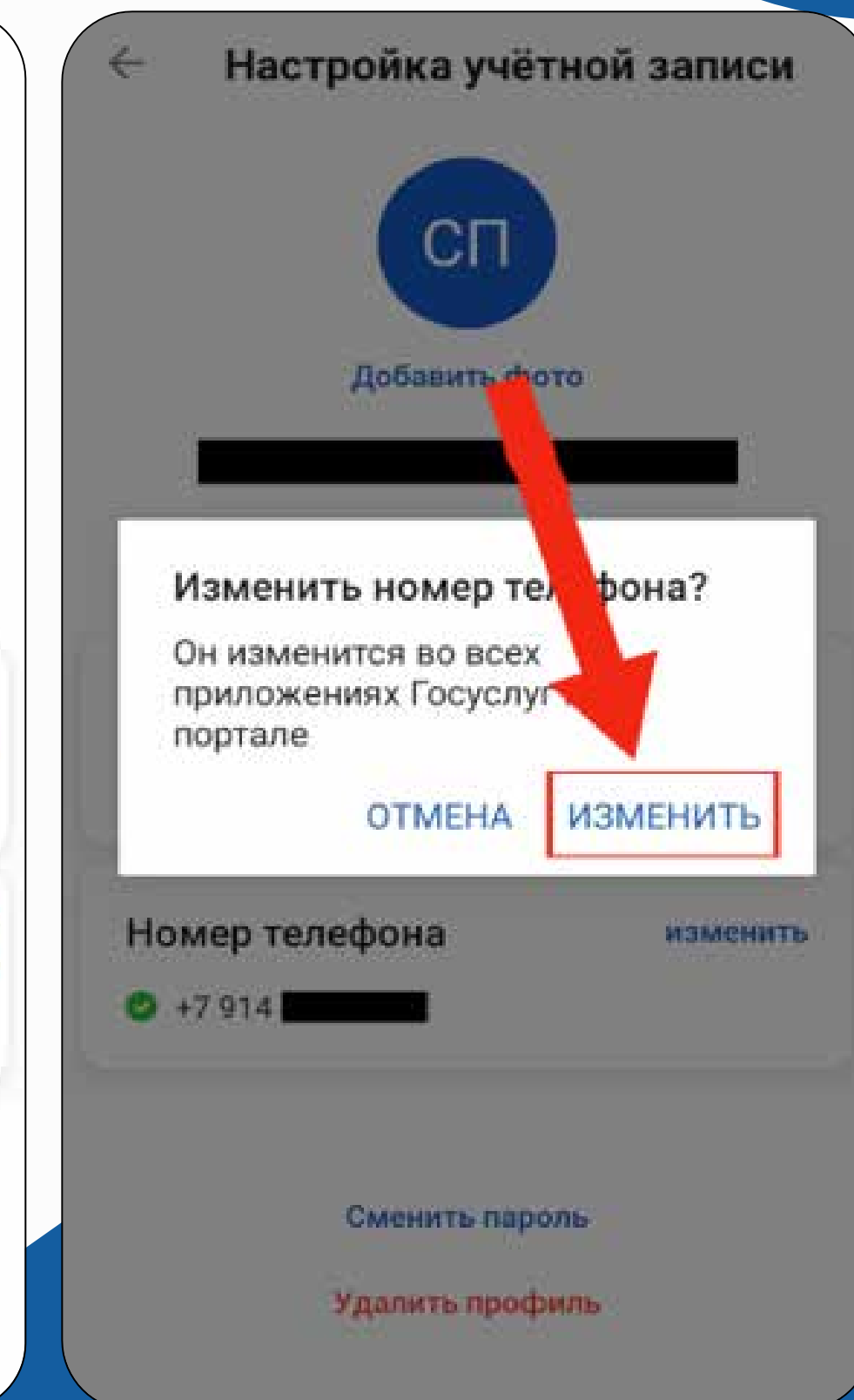
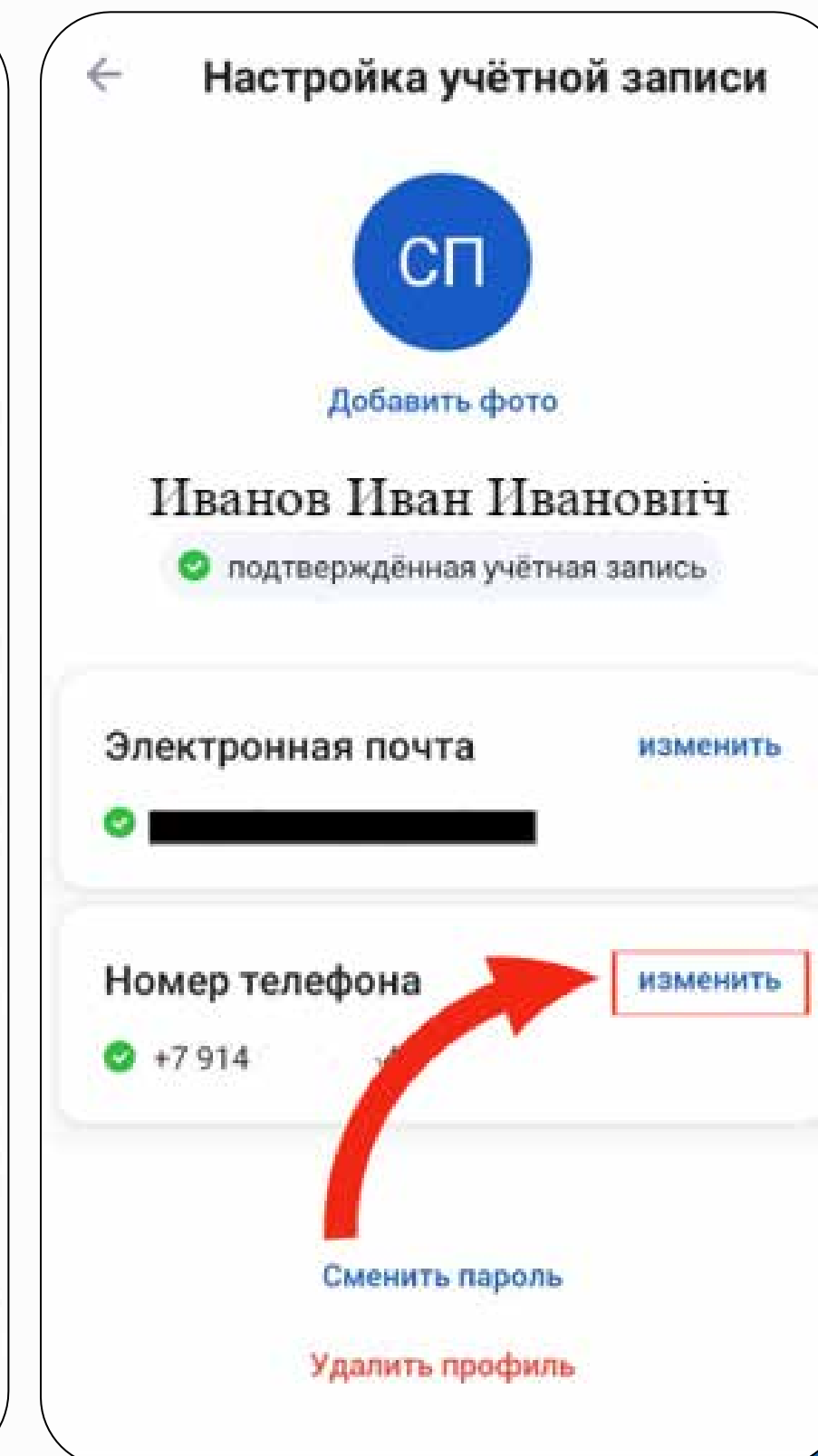
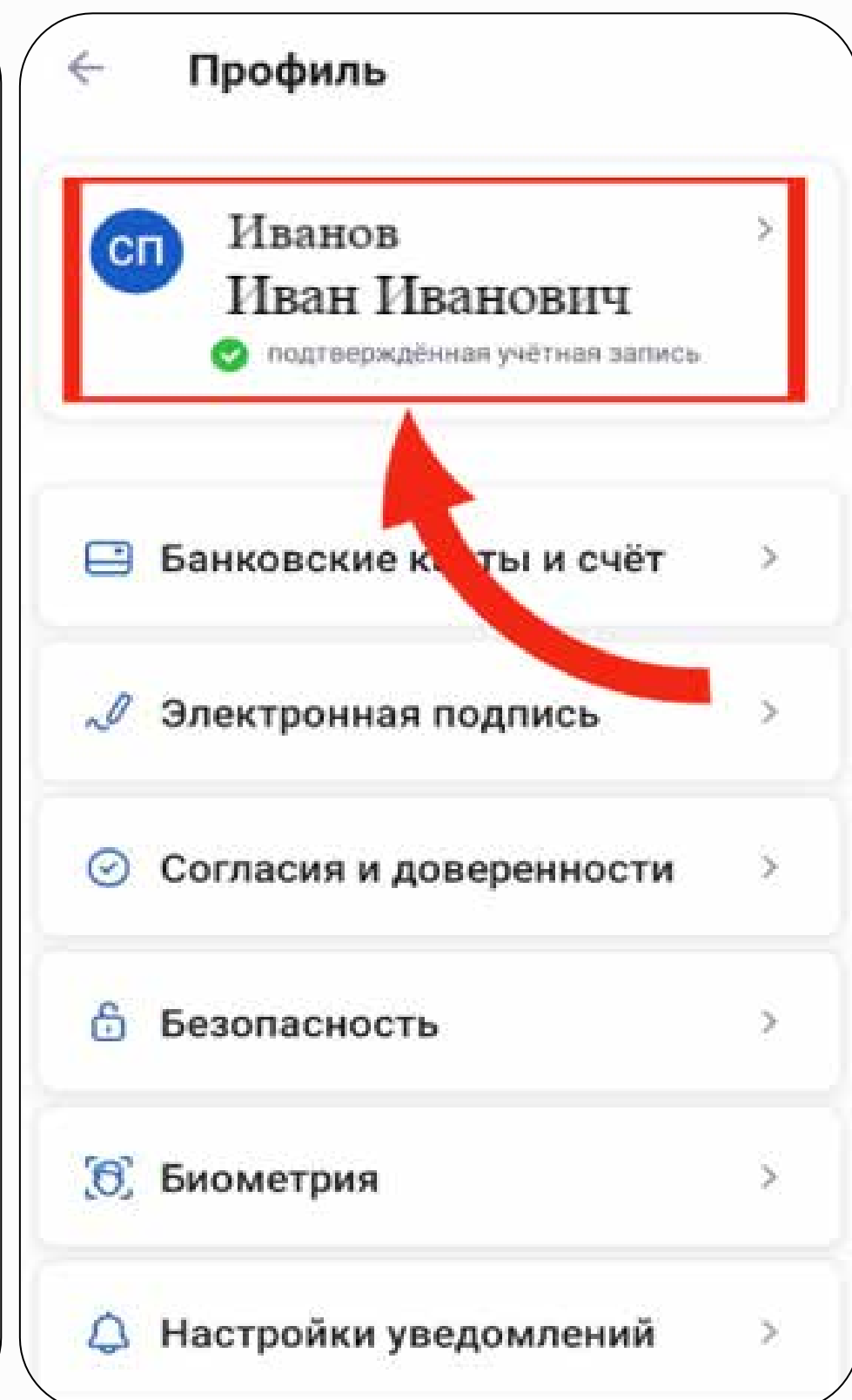
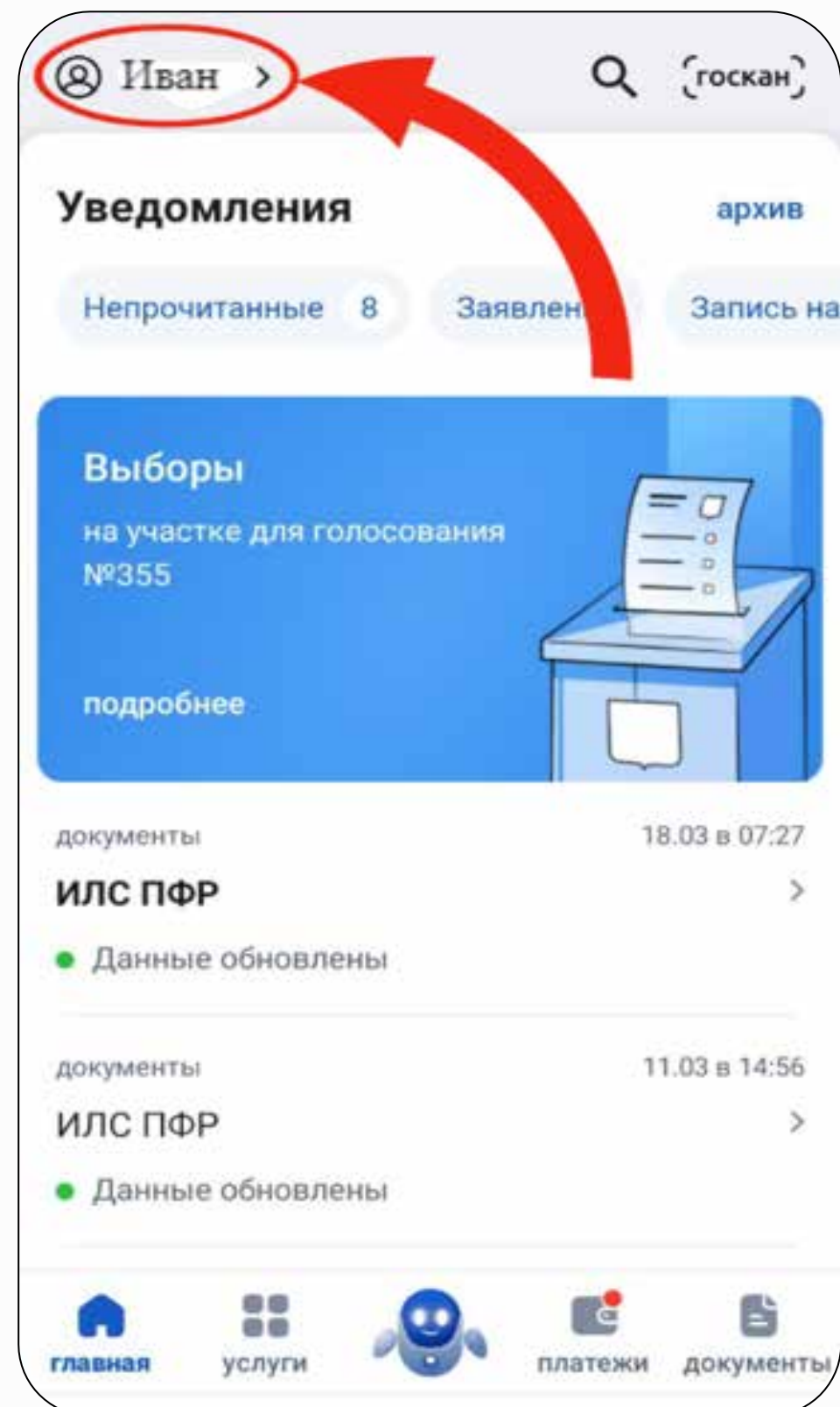
Отзыв согласий



Отзыв согласий



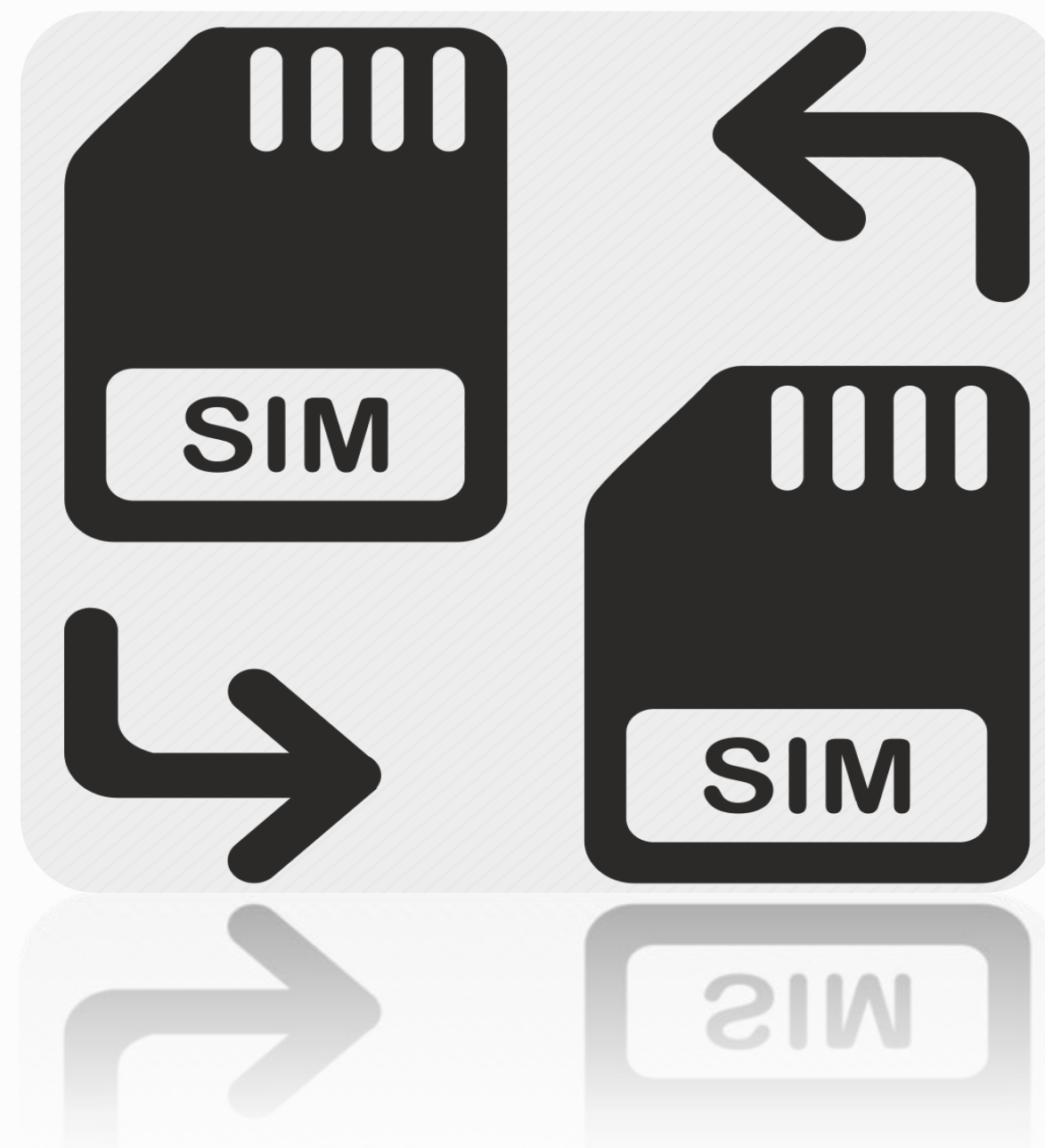
Способ открепления номера телефона



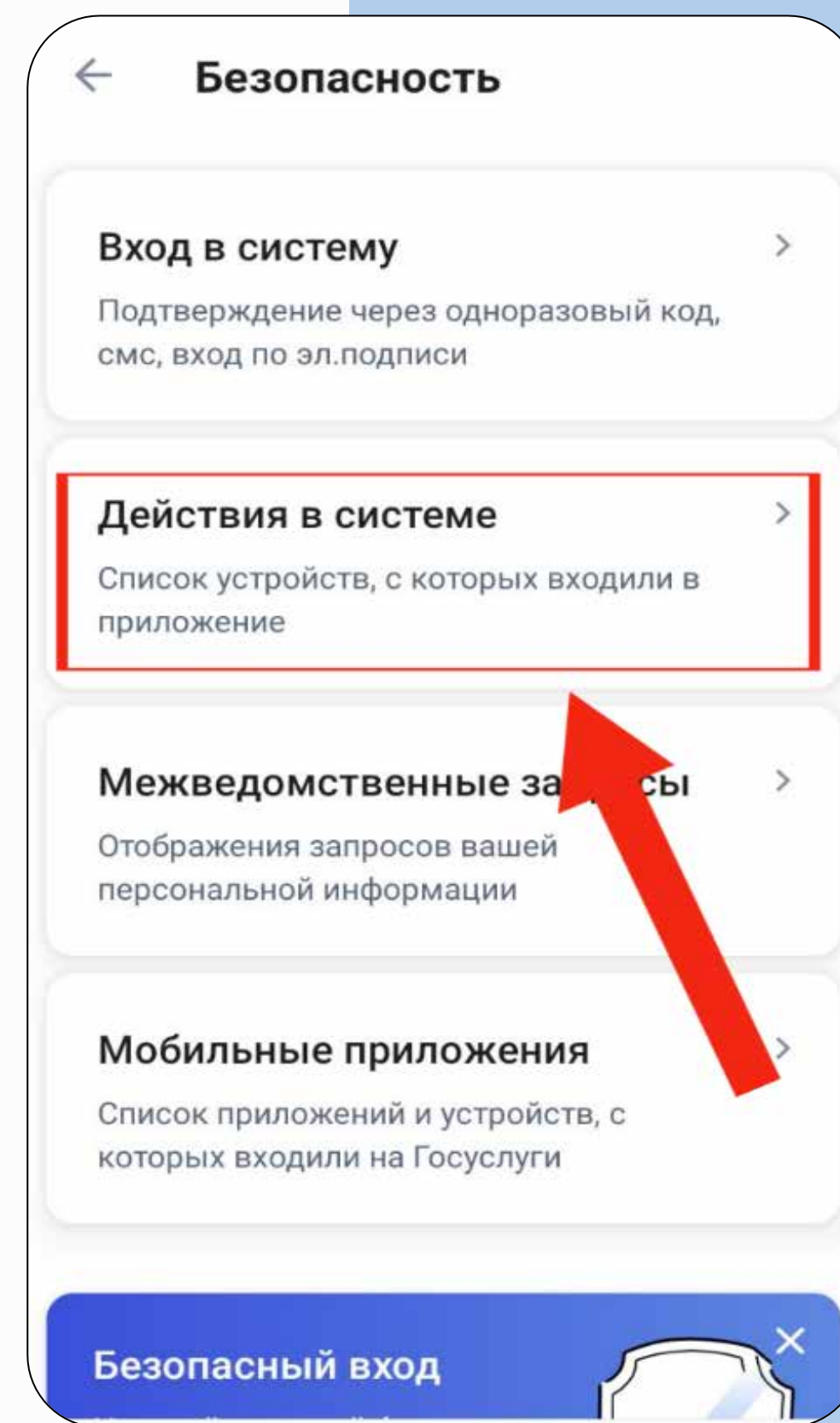
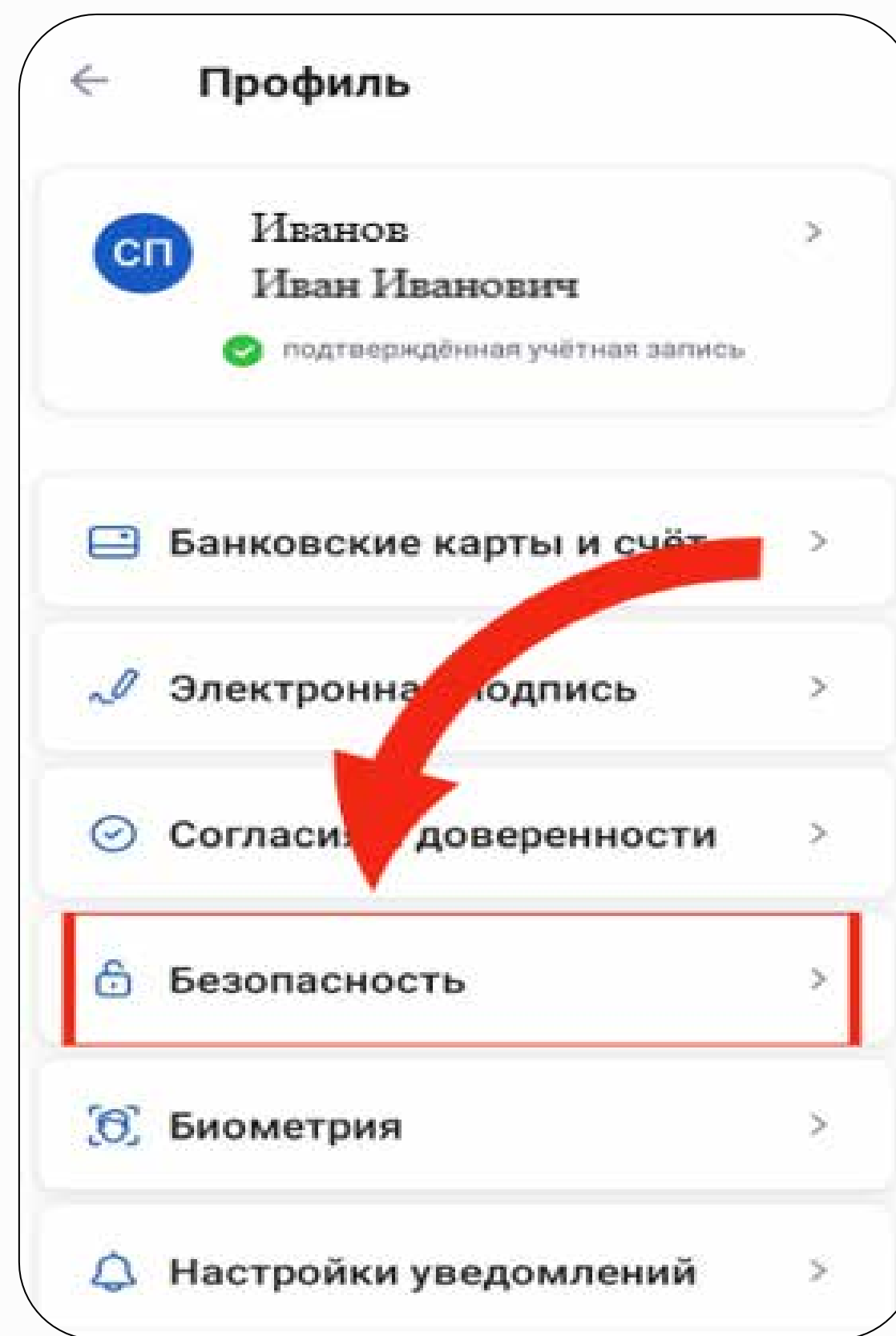
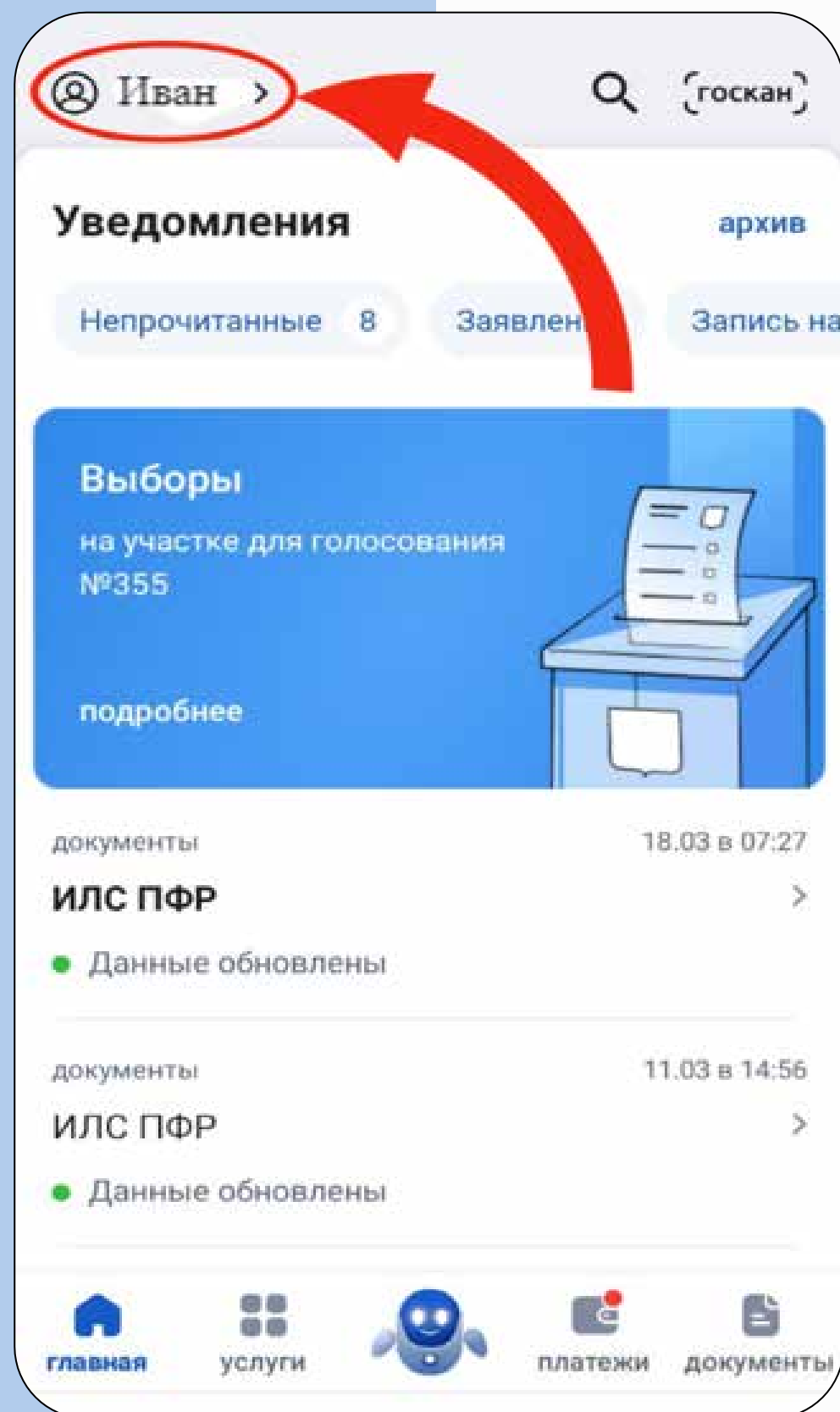
Переоформление SIM-карты

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.

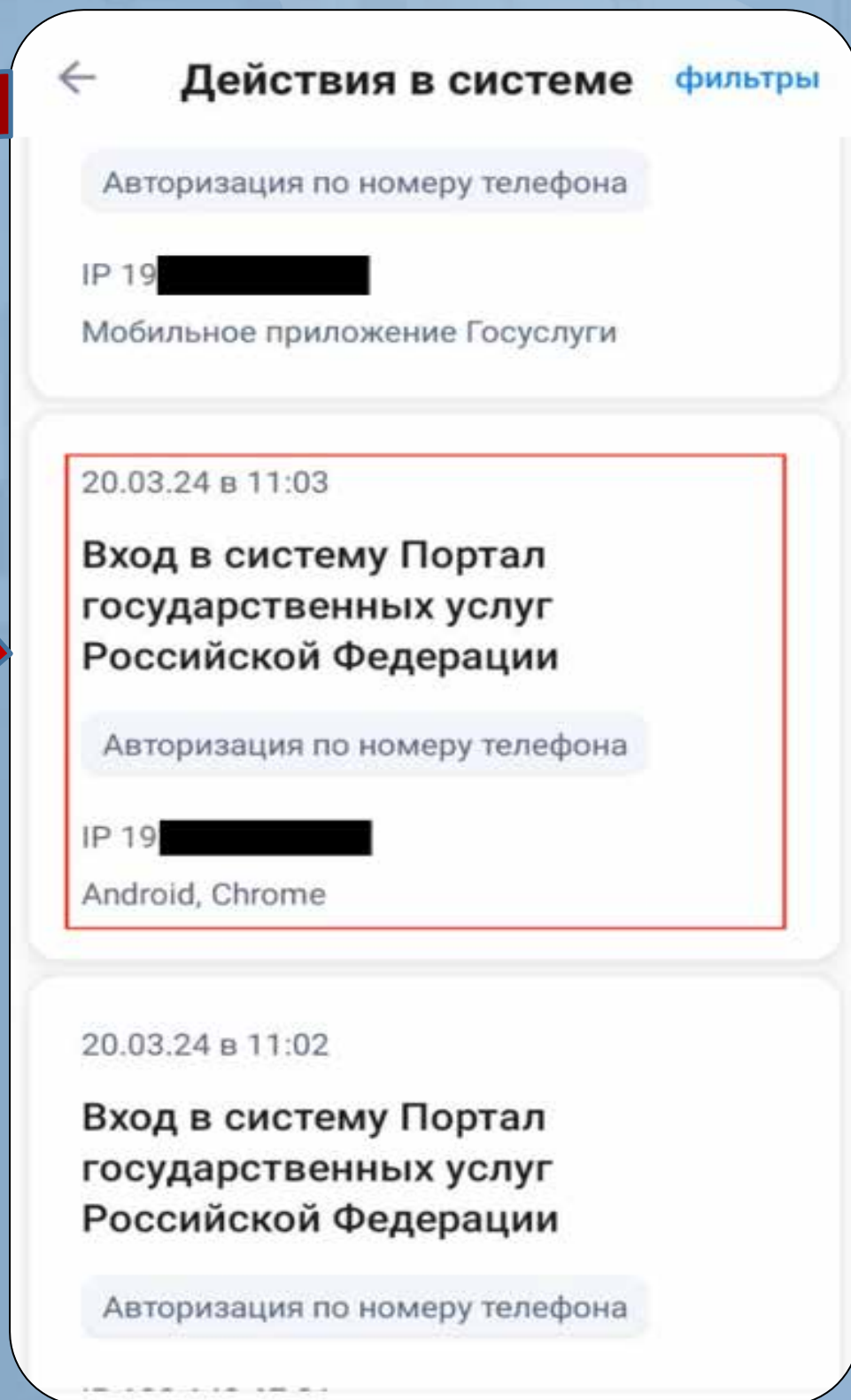


Признаки взлома личного кабинета портала «Госуслуги»



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.

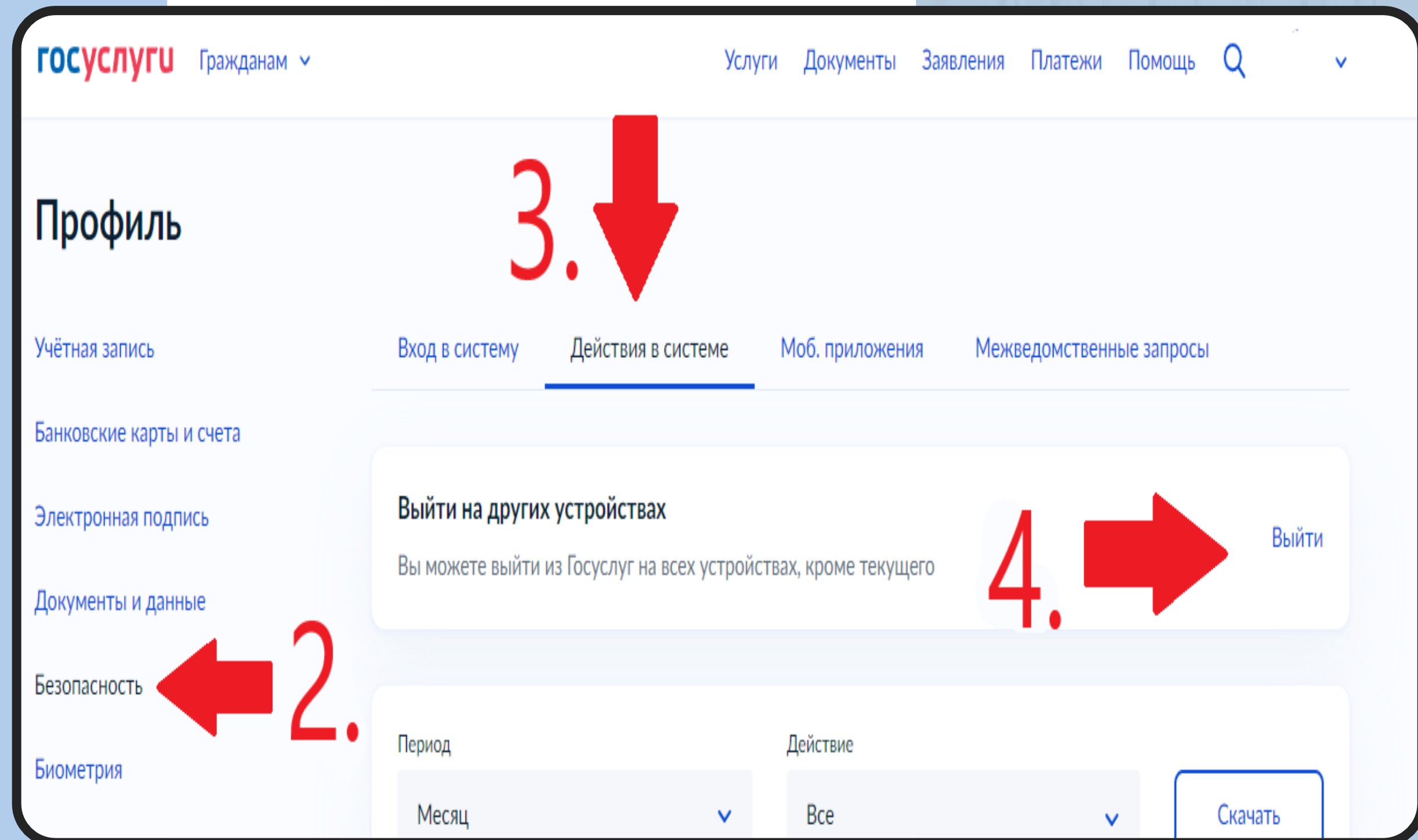
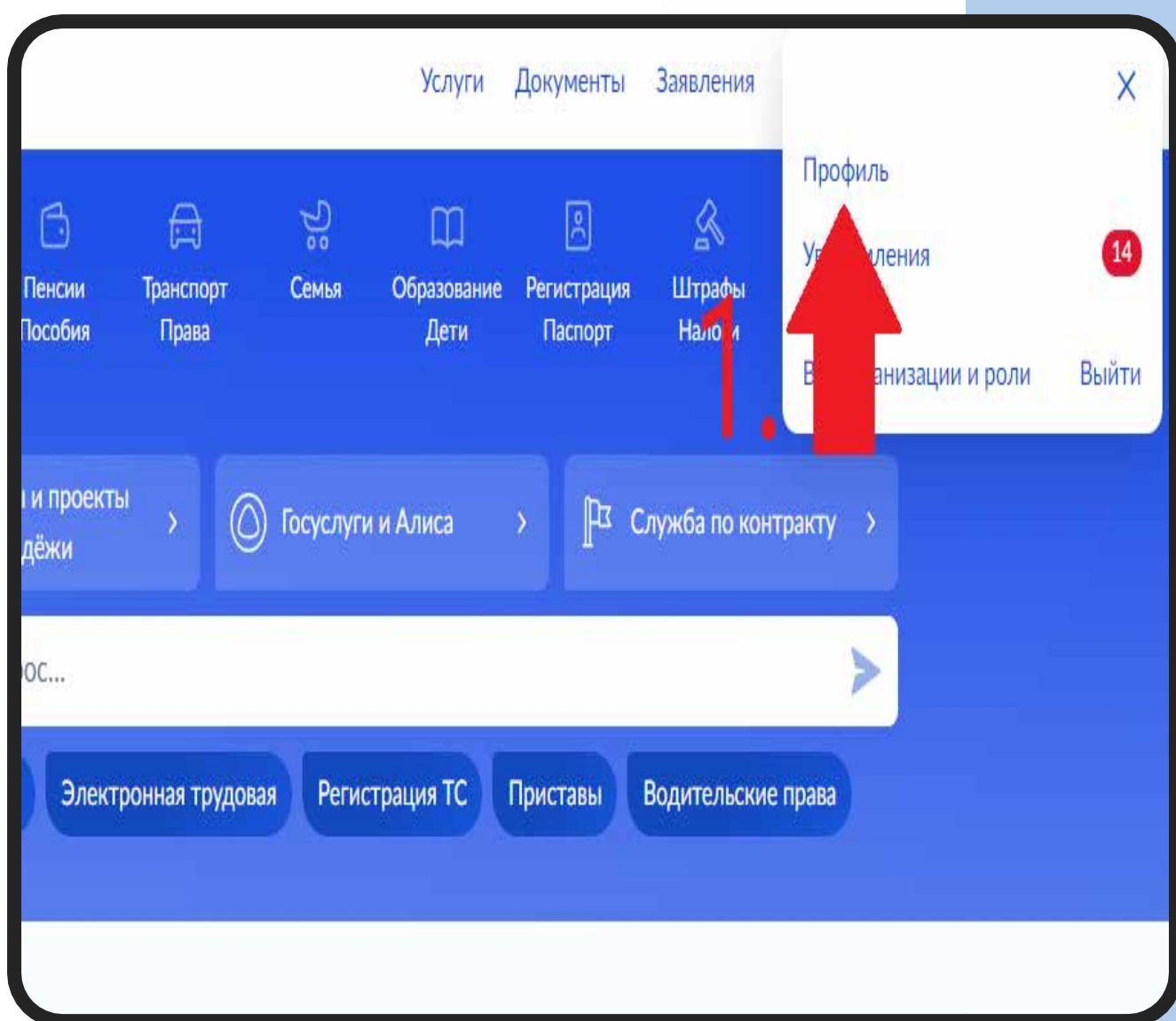
Сотрудники проверят вашу личность, помогут восстановить доступ к аккаунту и сменить пароль.

Возьмите с собой паспорт и СНИЛС

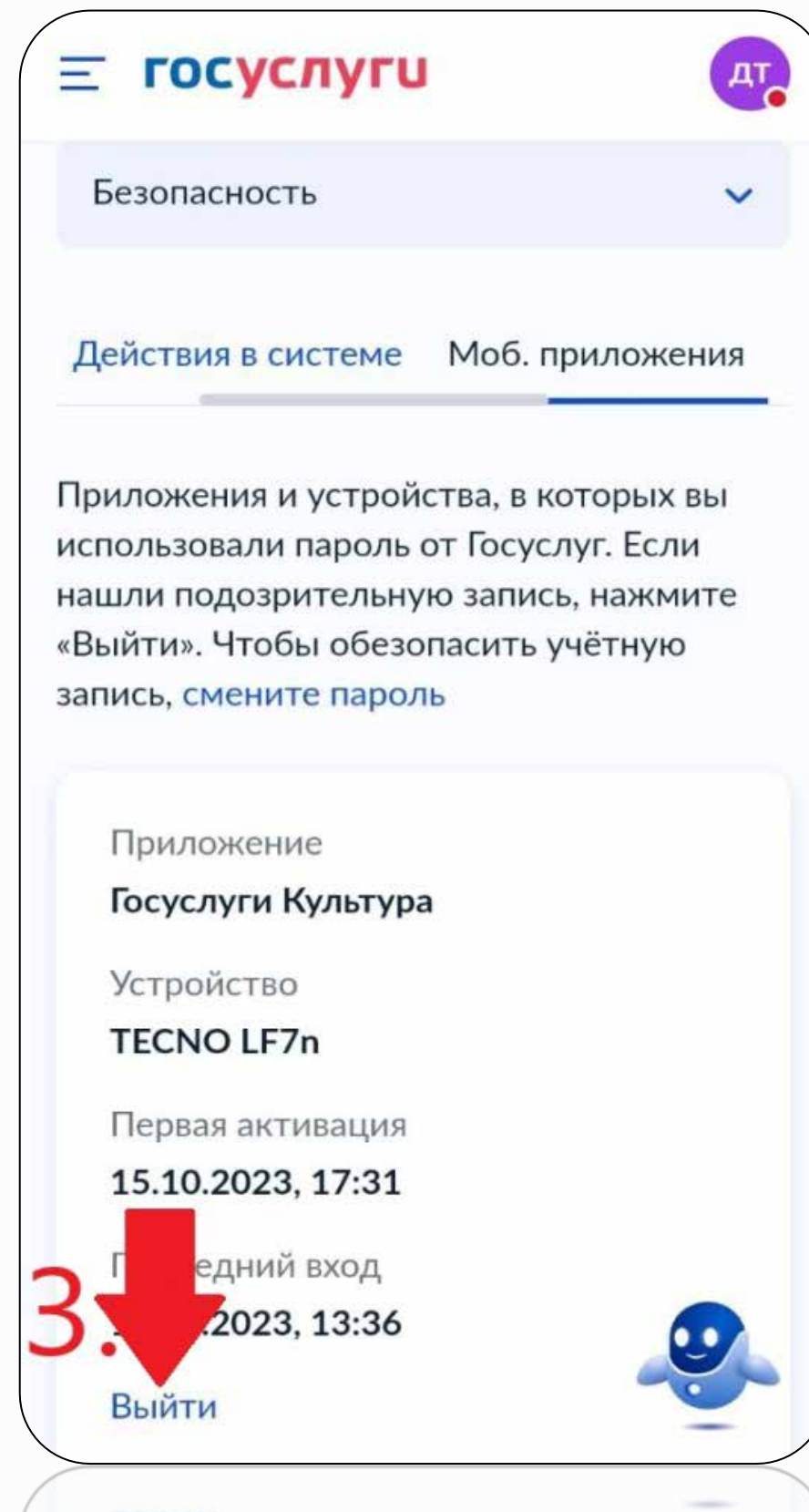
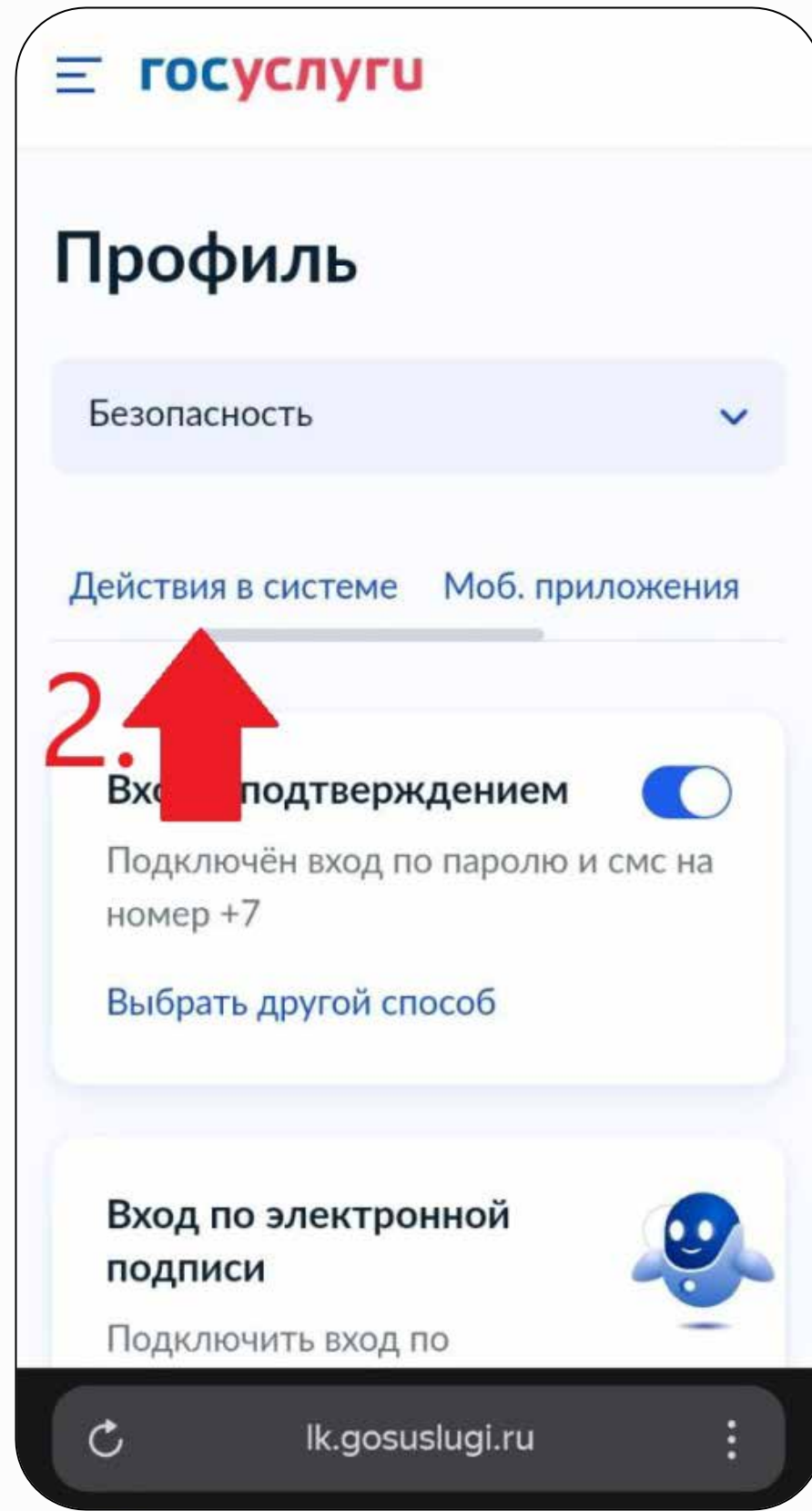
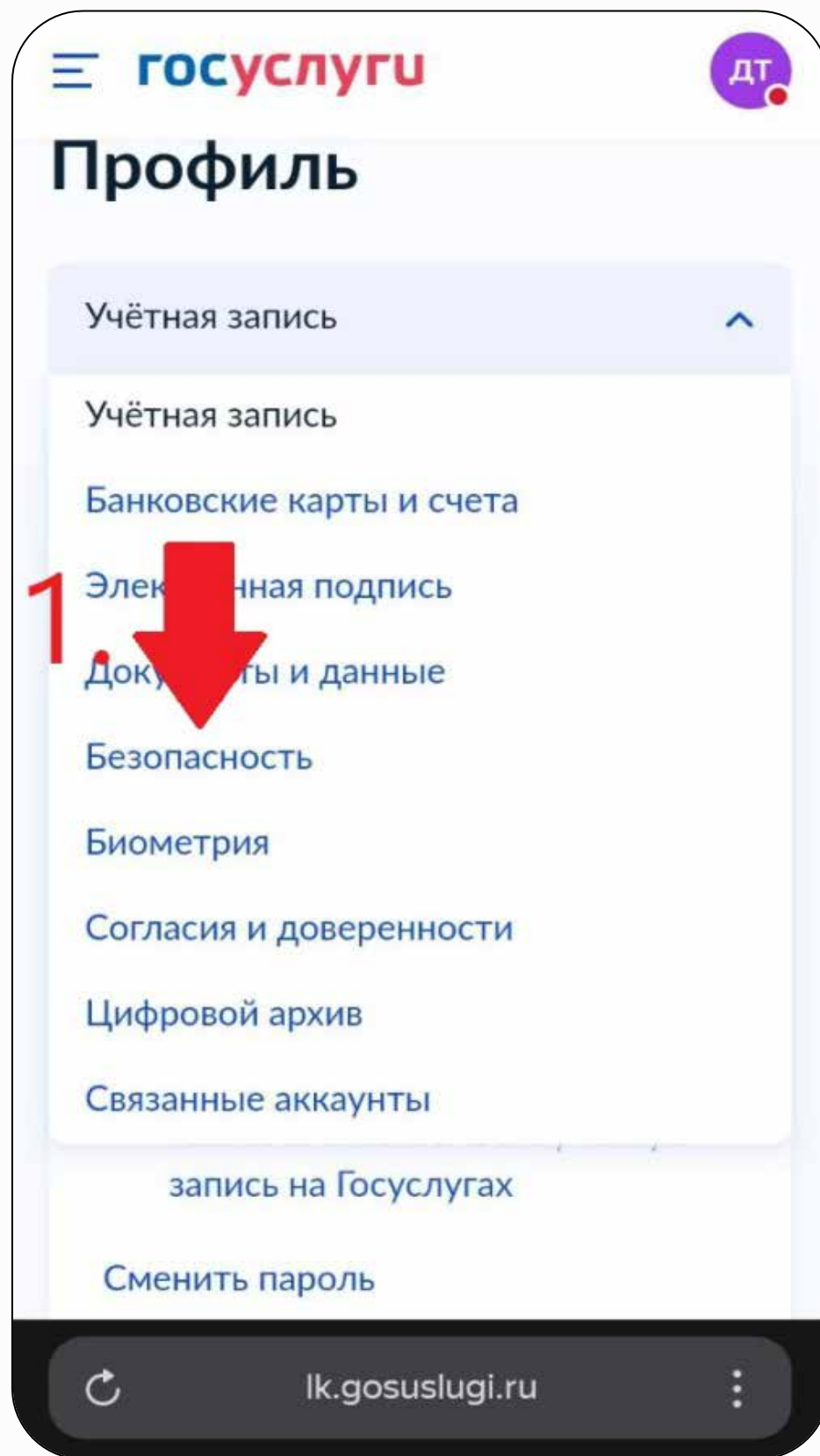


Определите, где использовалась учетная запись

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.

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.

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»



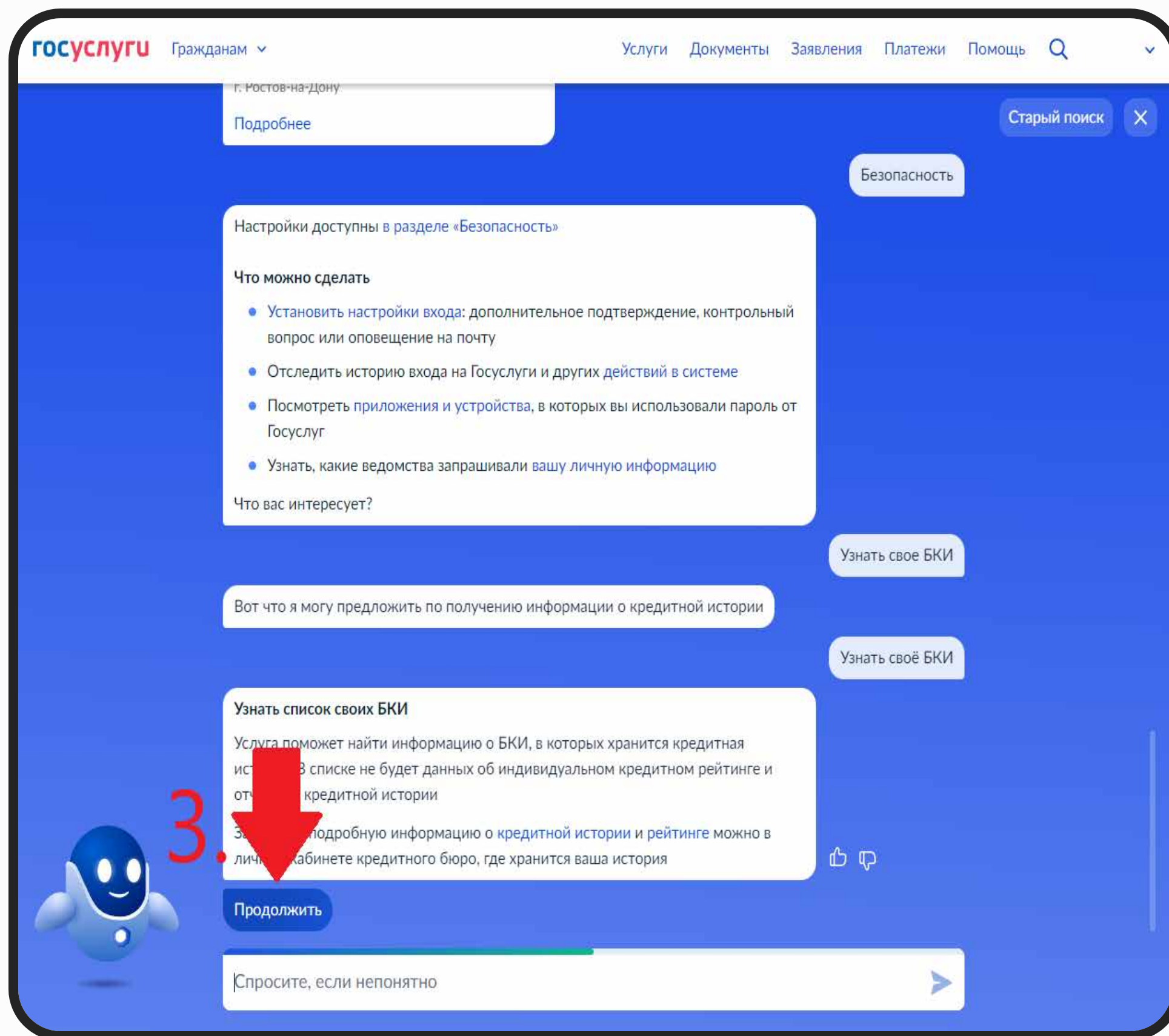
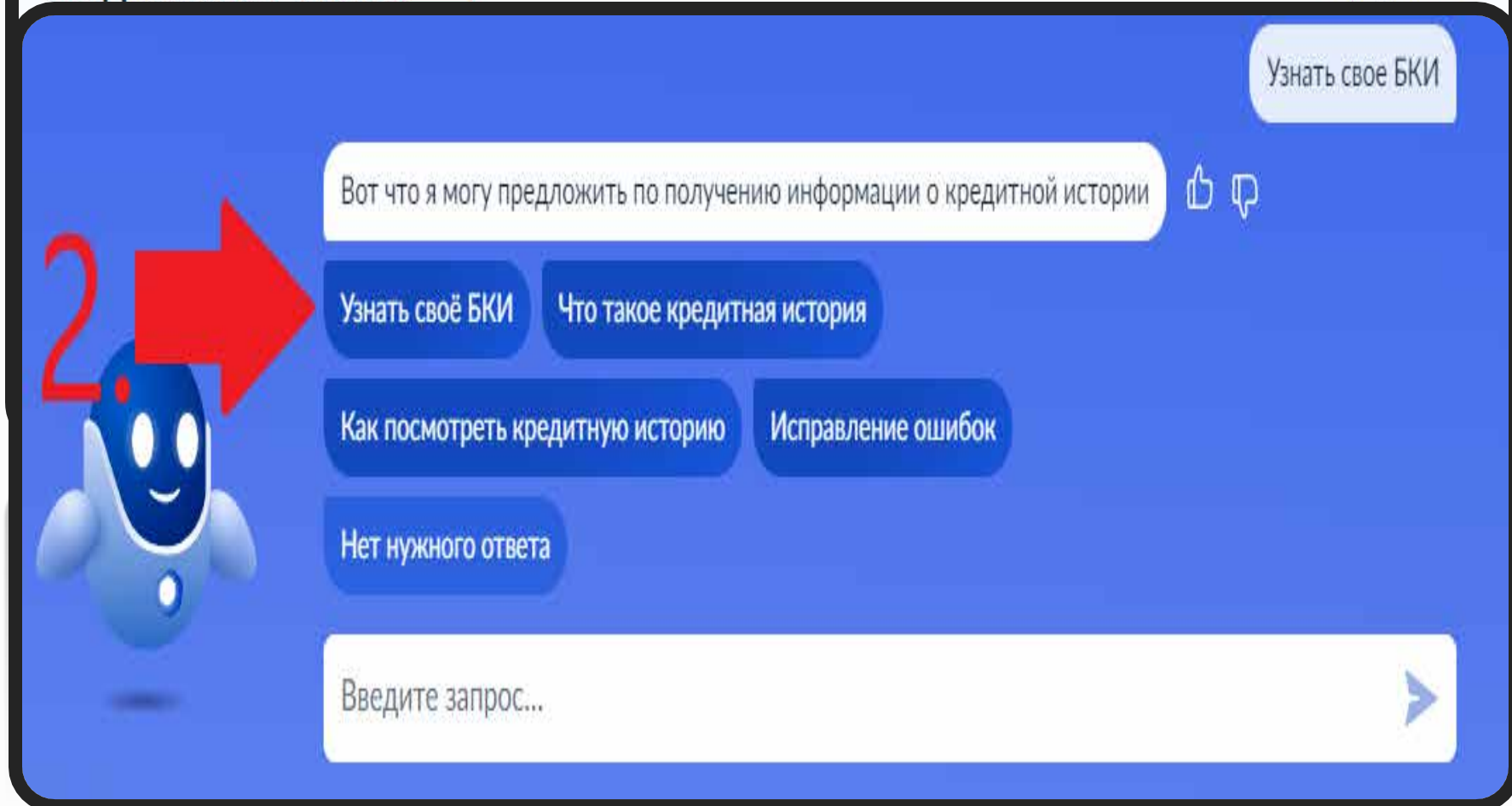
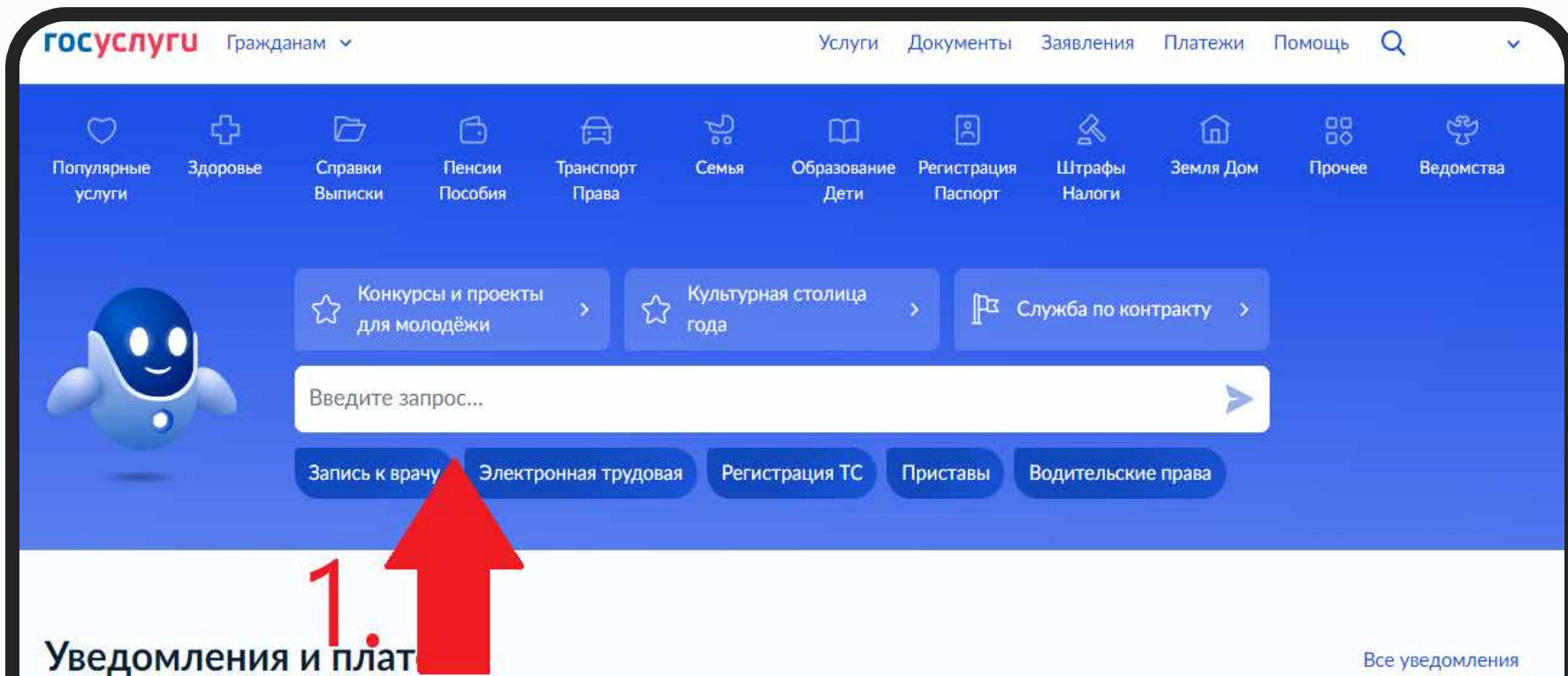
Введите в строке поиска запрос «узнать свое БКИ».



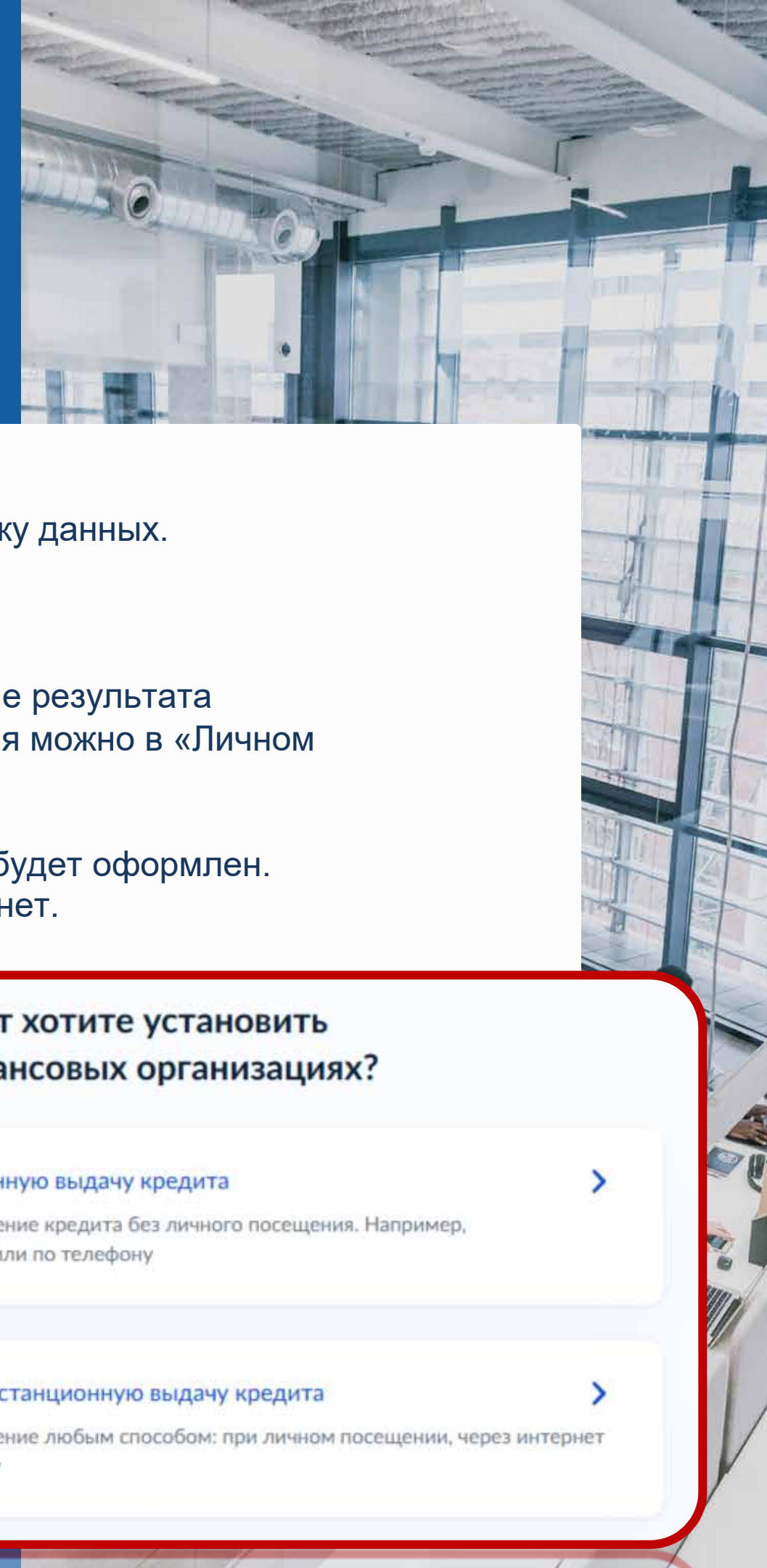
Далее зарегистрируйтесь на сайте каждого бюро* и запросите свою кредитную историю (рекомендуем направить запрос через 2 недели после взлома аккаунта).

*Можно авторизоваться с помощью учетной записи «Госуслуги».

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



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



Скриншоты экрана мобильного приложения «Госуслуги» для установки самозапрета на кредиты и микрозаймы.

Экран 1: Выбор организаций

На какие организации будет распространяться запрет?

- Кредитные: Чаще всего это банки, которые предоставляют крупные кредиты на длительный срок – более месяца
- Микрофинансовые: Это организации, которые выдают в долг небольшие суммы на короткий срок. Как правило, не более 1 месяца
- Кредитные и микрофинансовые

Экран 2: Выбор типа запрета

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

Экран 3: Выбор подписи

Какую подпись хотите использовать?

Что такое ПЭП, УНЭП и УКЭП

- ПЭП: Формируется с помощью личной электронной подписи на Госуслугах
- УНЭП в приложении «Госулок»: Потребуется телефон или планшет с приложением «Госулок». Если сертификата УНЭП ещё нет, это будет предложено выдать
- УКЭП в приложении «Госулок»: Потребуется телефон или планшет с приложением «Госулок». Если сертификата УКЭП ещё нет, это будет предложено выдать. Для этого потребуется либо подтверждающая биометрия, либо заграничный паспорт нового образца и телефон с NFC, либо поход в МФЦ или банк

Экран 4: Подтверждение отправки

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

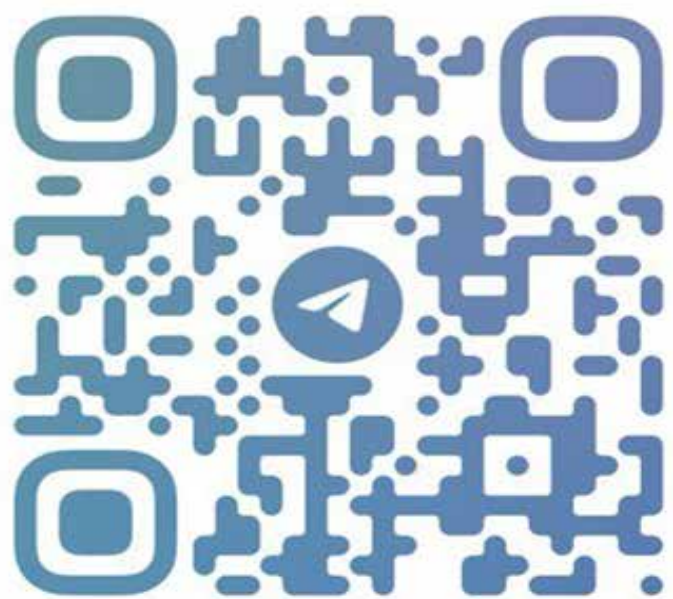
Запрет действует бессрочно. Снять его или узнать статус запрета можно также через Госуслуги

Экран 5: Итог

Заявление готово к отправке

Вы ввели все необходимые данные и можете отправить заявление

Отправить заявление



@TEBYA_OBMANIVAYU
T

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