

**PRO32**

# Mobile Security

Мобильная защита  
от киберугроз  
и потери данных

Руководство пользователя



## Оглавление

|  |    |
|--|----|
| I.   |    |
| Введение .....   | 2  |
| II. Системные требования.....                                    | 2  |
| III. Установка приложения.....                                   | 2  |
| IV. Первый запуск.....   | 4  |
| V. Активация приложения.....                                     | 9  |
| VI. Настройки и дополнительные разрешения .....                  | 10 |
| VII. Главный экран.....  | 14 |
| 1. Кнопка Сканировать .....                                      | 14 |
| 2. Защита от вредоносных программ .....                          | 14 |
| 3. Веб-защита .....  | 15 |
| 4. Фильтрация вызовов.....                                       | 15 |
| 5. Трекер .....  | 15 |
| VIII. Функции приложения.....                                    | 16 |
| 1. Сканирование.....   | 16 |
| 2. Аудит приложений .....  | 16 |
| 3. Управление ресурсами.....                                     | 16 |
| 4. Бэкап и восстановление.....                                   | 17 |
| 5. Проверка Wi-Fi.....   | 17 |
| IX. Сервисы .....  | 18 |
| 1. Обновление .....  | 18 |
| 2. Журнал.....   | 18 |
| 3. Настройки .....   | 18 |
| 4. О продукте .....  | 19 |
| 5. Техническая поддержка .....                                   | 19 |
| X. Функция Трекер и использование портала Трекер устройств ..... | 19 |
| XI. Управление лицензиями .....                                  | 23 |

## I. Введение

Вас приветствует команда PRO32!

Интернет дает вам доступ к большому количеству информации и открывает массу возможностей для бизнес, однако он также подвергает ваш компьютер множеству угроз, связанных с безопасностью и нарушением конфиденциальности, о которых большинство из нас даже не знает. Интернет-угрозы больше не ограничиваются одними лишь вирусами; они также включают в себя шпионское ПО, вредоносный активный код, спам, взломы и т. д. Каждый раз, когда ваш смартфон подключается к Интернету, он становится потенциальной целью для хакеров.

Используя легкодоступные инструменты, такие как шпионское ПО, черви и трояны, злоумышленники могут просматривать личные записи, похищать конфиденциальную информацию и получать контроль над вашим устройством без вашего ведома. Сложные и быстро распространяющиеся интернет-угрозы используют уязвимости программного обеспечения и операционной системы и распространяются с применением различных хакерских методов.

**PRO32 Mobile Security** помогает защитить ваше устройство от новых возникающих угроз, включая сетевые вирусы, неприемлемый контент и шпионское ПО, которые способны поставить под угрозу вашу конфиденциальность. Это позволяет вам полностью контролировать обмен данными как внутри вашего устройства, так и с внешними получателями.

## II. Системные требования

- 1) Смартфон или планшет с разрешением экрана от 320x480 пикселей.
- 2) 110 МБ свободного места в основной памяти устройства;
- 3) Операционная система Android 5.0 и выше.

- Для корректной работы портала «Антивор» требуется наличие установленных на смартфоне сервисов Google.
- Устройства Android TV не поддерживаются

## III. Установка приложения

Вы сможете установить PRO32 Mobile Security любым из удобных для вас способов:

- С помощью сервиса GPlay, перейдя по ссылке с вашего мобильного устройства:

<https://play.google.com/store/apps/details?id=com.k7computing.android.rusecurity>

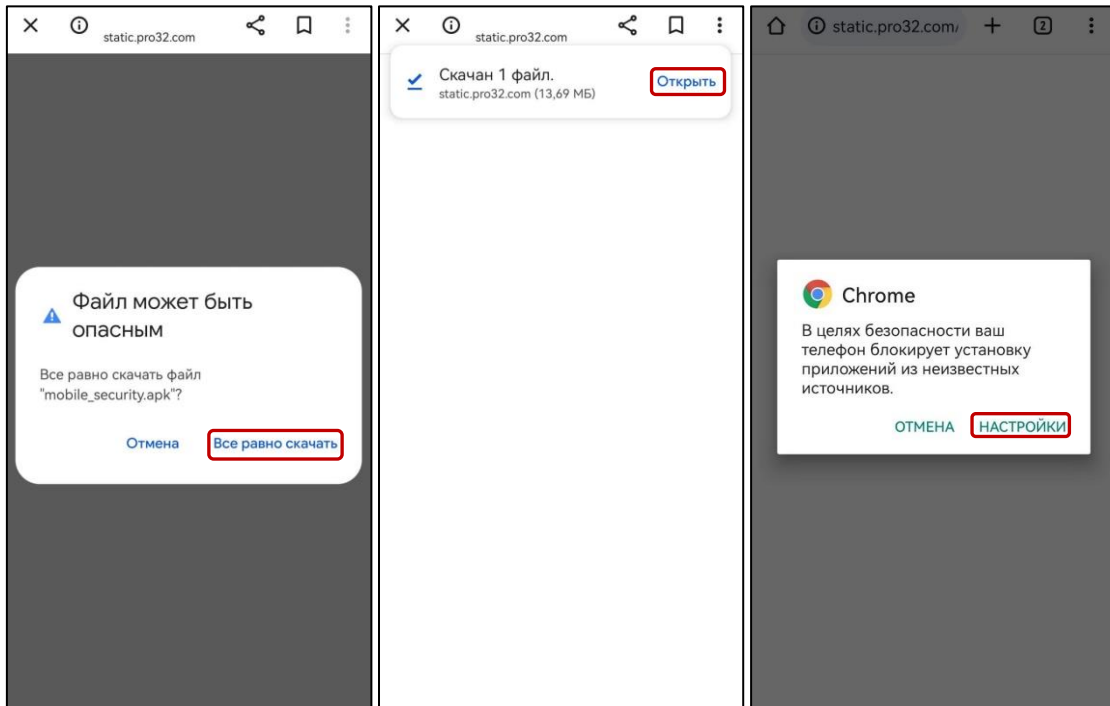
Пройдите по ссылке и следуйте указаниям сервиса.

- Скачав приложение с официального сайта PRO32 перейдя по ссылке с вашего мобильного устройства:

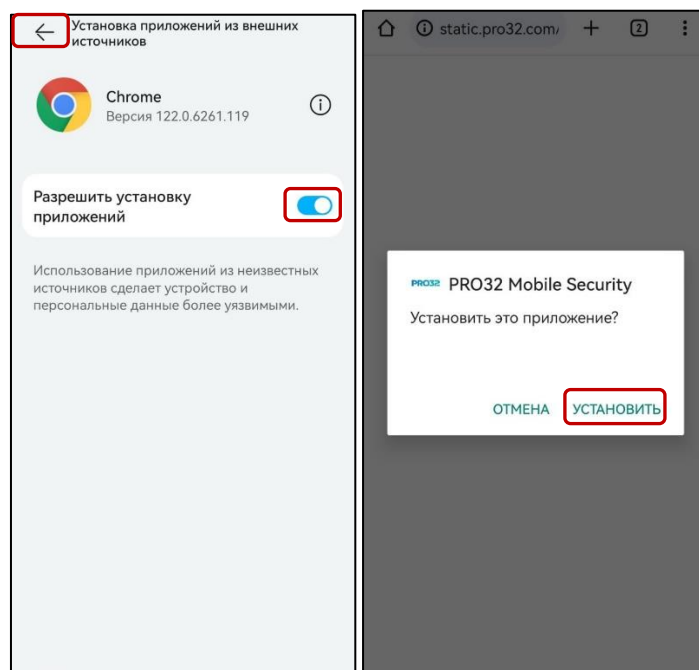
[https://static.pro32.com/download/installer/mobile\\_security.apk?\\_ga=2.6987639.413752937.1711034007-204561859.1711034007](https://static.pro32.com/download/installer/mobile_security.apk?_ga=2.6987639.413752937.1711034007-204561859.1711034007)

Установка с сайта потребует от вас нескольких шагов:

- 1) При скачивании браузер вашего мобильного устройства может вызвать предупреждение, что файл может быть опасен. Не переживайте, нажмите «Все равно скачать».
- 2) Скачав файл, нажмите «Открыть», в следующем окне вам предложат выдать разрешения на установку приложений из браузера. Перейдите в «Настройки».



- 3) Выдайте необходимые разрешения и вернитесь назад к шагу 2.
- 4) Установите приложение и запустите его.

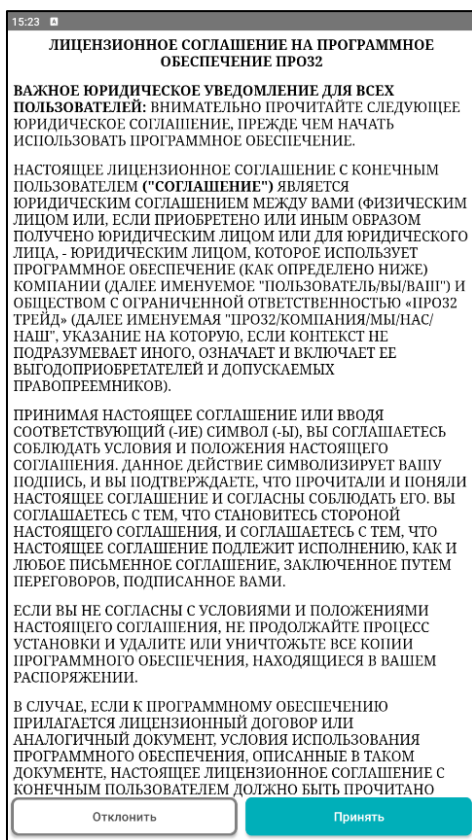


## IV. Первый запуск

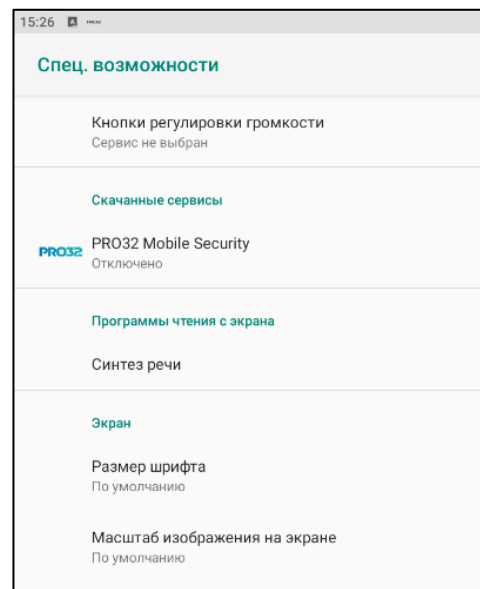
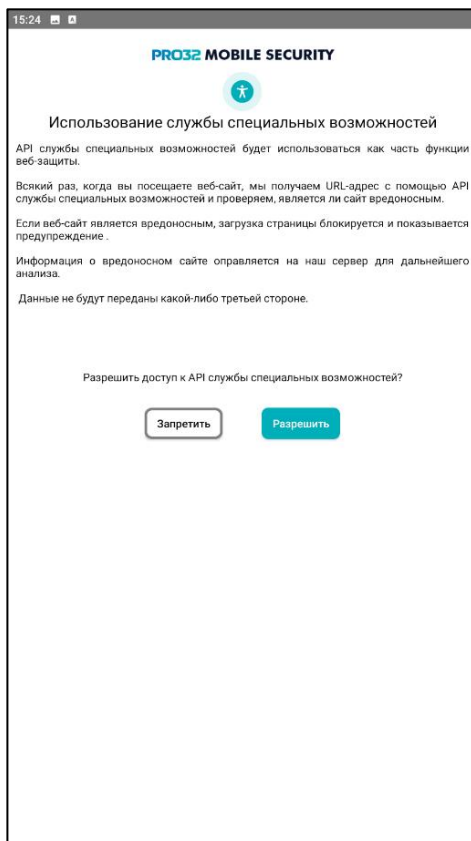
При первом запуске **PRO32 Mobile Security** вам будет необходимо выполнить некоторые настройки и предоставить приложению необходимые разрешения.

Выполните следующие действия:

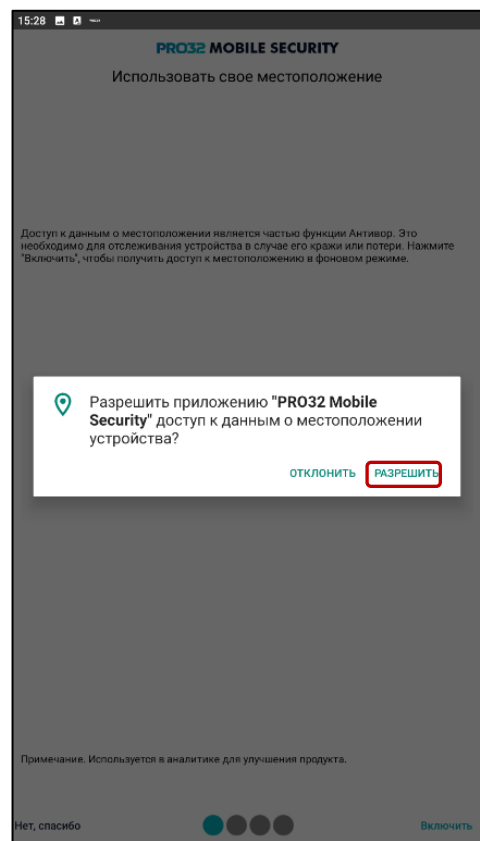
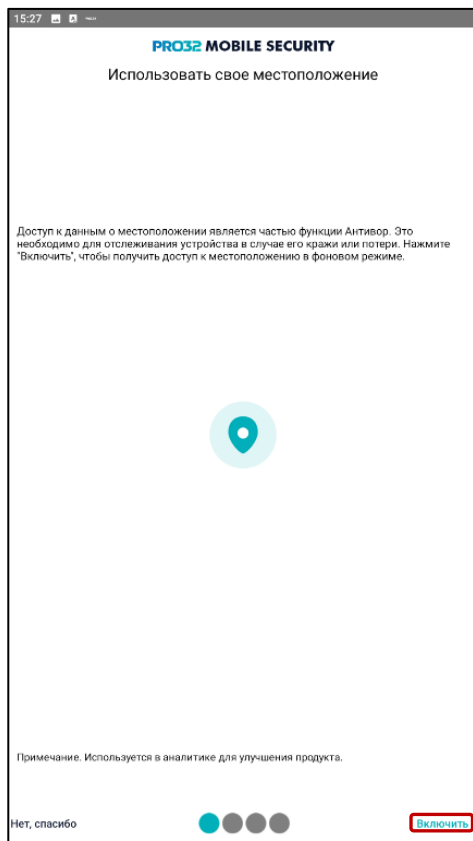
- Прочтите и примите лицензионное соглашение нажатием кнопки «**Принять**».
- На следующем экране нажмите «**Начать**».



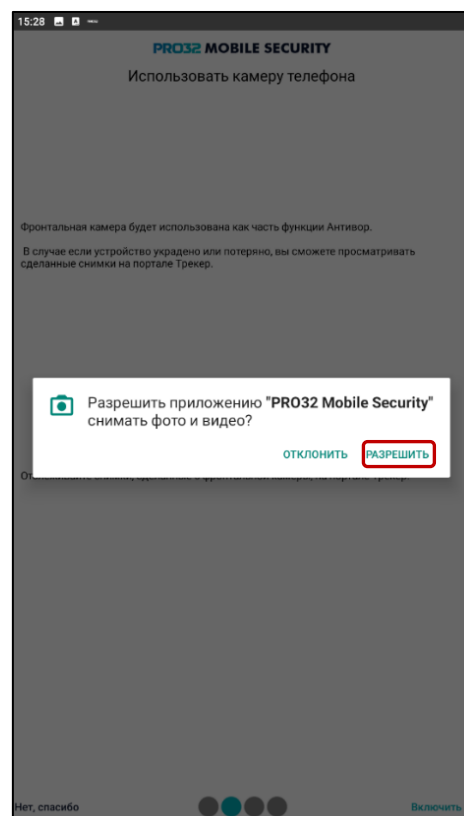
- Предоставьте приложению разрешение на использование API службы специальных возможностей (это необходимо для работы функции web-защиты: с помощью API службы специальных возможностей приложение получает адрес посещаемого сайта и проверяет, не является ли он вредоносным). Для этого на следующем экране нажмите кнопку «**Разрешить**». Откроется окно настроек Специальных возможностей телефона. Здесь необходимо выбрать PRO32 Mobile Security и установить ползунок в положение «**Использовать сервис**».



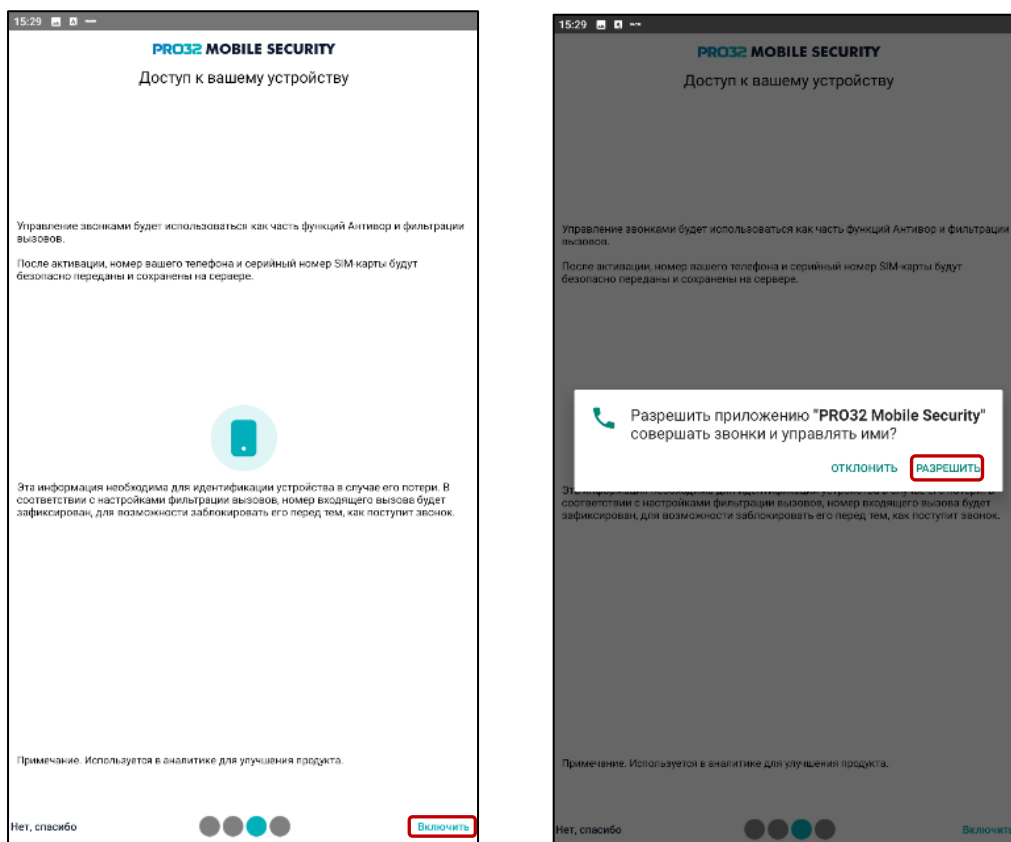
- Предоставьте приложению разрешение на доступ к данным о вашем местоположении (это необходимо для отслеживания местоположения устройства в рамках функции *Антивор*: вы сможете узнать местоположение своего устройства в случае потери). Для этого на следующем экране нажмите «**Включить**» в правом нижнем углу, а затем нажмите «**Разрешить**» в появившемся окне.



- Предоставьте приложению разрешение на использование камеры телефона (это необходимо для использования функции *Антивор* и предоставит вам доступ к снимкам с камеры в случае потери устройства). Для этого на следующем экране нажмите «**Включить**» в правом нижнем углу, а затем нажмите «**Разрешить**» в появившемся окне.

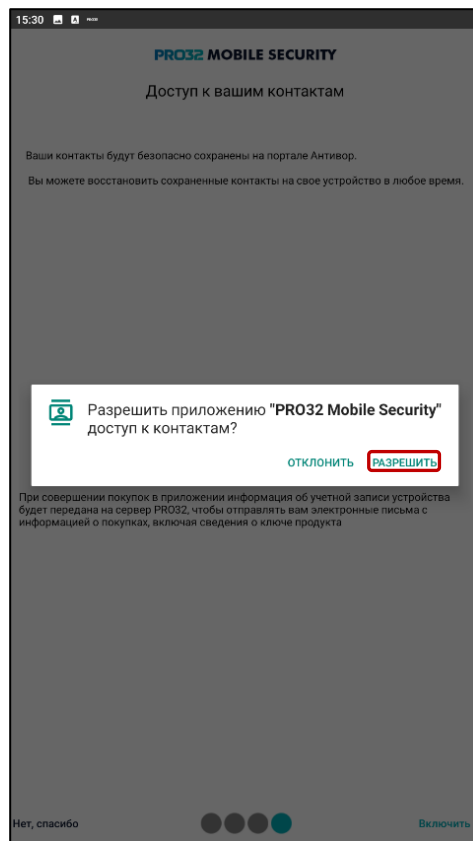
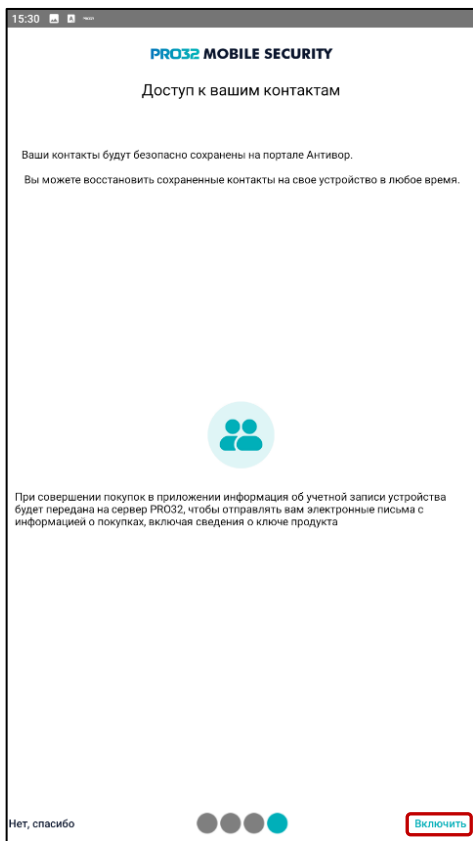


- Предоставьте приложению разрешение на управление звонками (это необходимо для использования функции *Антивор*, а также используется функцией фильтрации вызовов). Для этого на следующем экране нажмите «**Включить**» в правом нижнем углу, а затем нажмите «**Разрешить**» в появившемся окне.

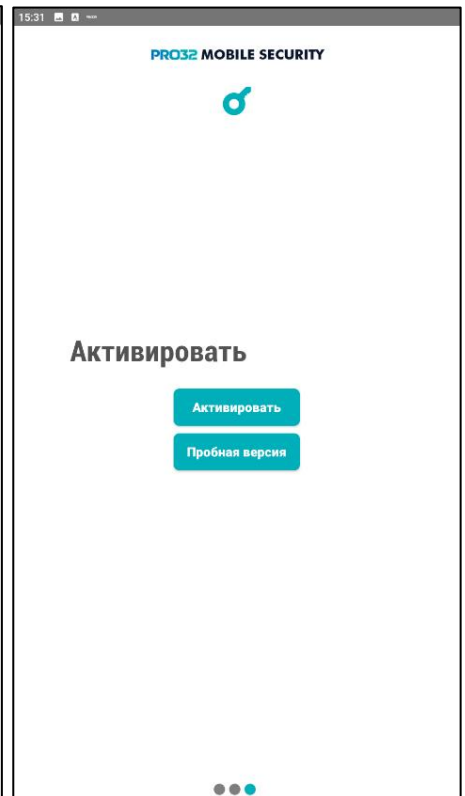
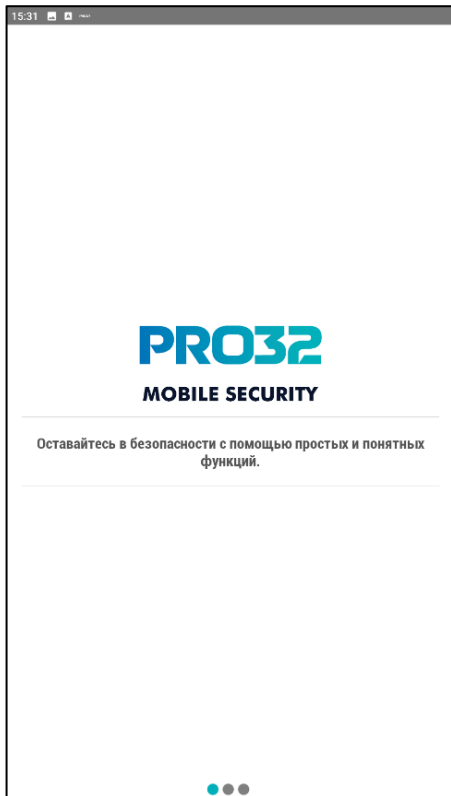


- Предоставьте приложению разрешение на доступ к вашим контактам. Контакты будут сохранены на портале *Антивор*, и вы сможете восстановить их в любое время, в частности, в случае потери устройства. Для этого на следующем экране нажмите «**Включить**» в правом нижнем углу, а затем нажмите «**Разрешить**» в появившемся окне.





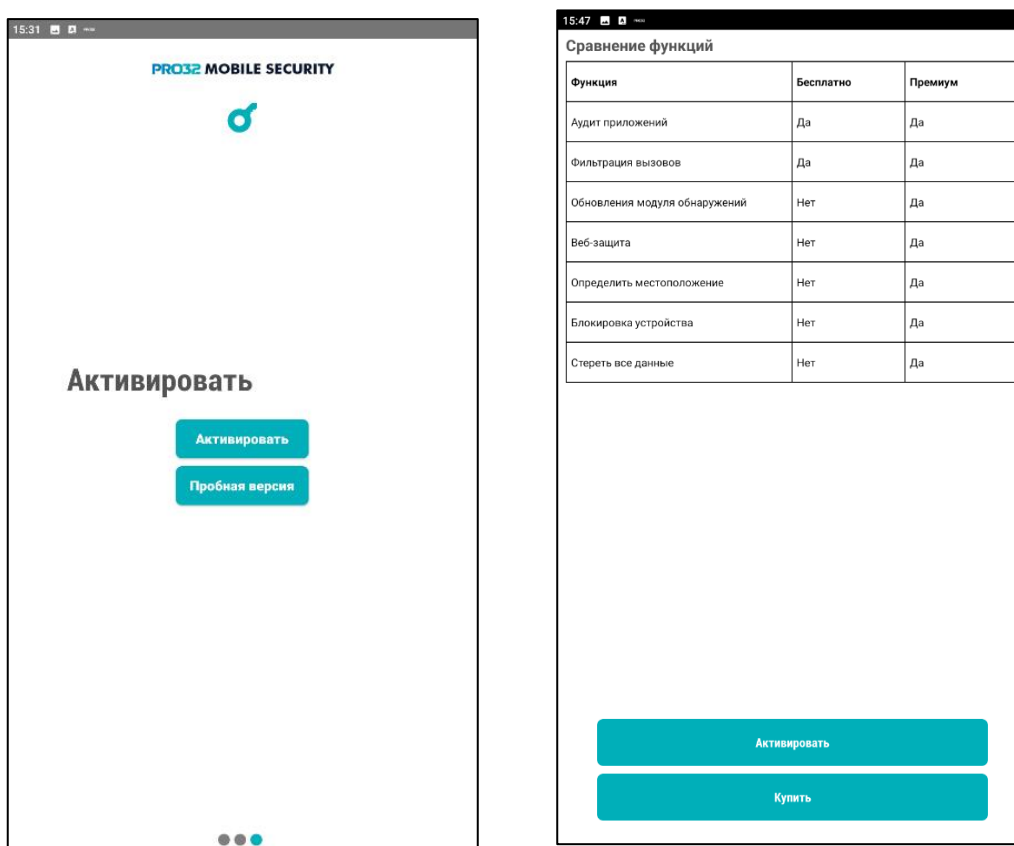
- Вы почти закончили. Прокрутите следующие экраны и переходите к активации приложения.



## V. Активация приложения

Вы можете активировать пробную, либо полную версию. В пробной версии доступна функция антивируса, фильтрации вызовов и аудита приложений. Функционал *Антивор* в пробной версии доступен не будет. Для активации пробной версии нажмите соответствующую кнопку, для активации полной платной версии нажмите **«Активировать»**.

При нажатии на кнопку **«Активация»** откроется экран с таблицей сравнения функций платной и бесплатной версии, и две кнопки – **«Купить»** и **«Активировать»**. Если у вас уже есть лицензионный ключ – выберите **«Активировать»**. При нажатии на кнопку **«Купить»** вы перейдёте на сайт, где можно будет приобрести лицензионный ключ.



При нажатии на кнопку **«Активировать»**, вы попадёте на экран, где нужно будет заполнить форму. Введите следующие данные:

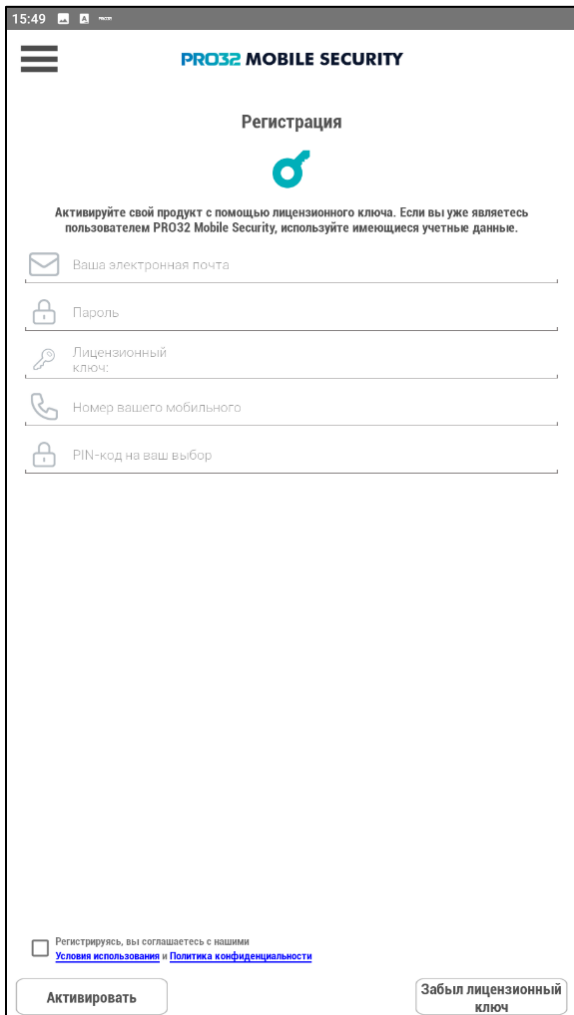
- ваша электронная почта
- пароль

**!** *Эти данные в дальнейшем будут использоваться для входа на Портал, поэтому выберите надёжный пароль и запомните его!*

- имеющийся у вас лицензионный ключ
- номер вашего мобильного телефона
- PIN-код на ваш выбор

 **Придумайте и запомните PIN-код, он необходим для разблокировки устройства!**

После заполнения, отметьте пункт о согласии с Условиями использования и Политикой конфиденциальности в левом нижнем углу и нажмите кнопку «**Активировать**». Поздравляем, вы активировали приложение, и теперь вам доступен его полный функционал.



15:49

PRO32 MOBILE SECURITY

Регистрация

Активируйте свой продукт с помощью лицензионного ключа. Если вы уже являетесь пользователем PRO32 Mobile Security, используйте имеющиеся учетные данные.

Ваша электронная почта

Пароль

Лицензионный ключ

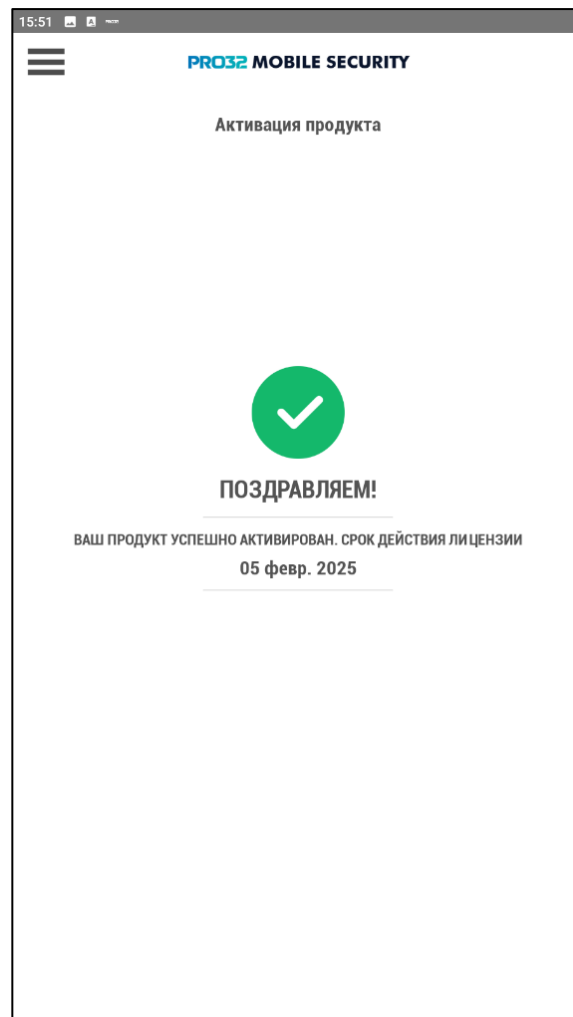
Номер вашего мобильного

PIN-код на ваш выбор

Регистрируясь, вы соглашаетесь с нашими [Условиями использования](#) и [Политикой конфиденциальности](#)

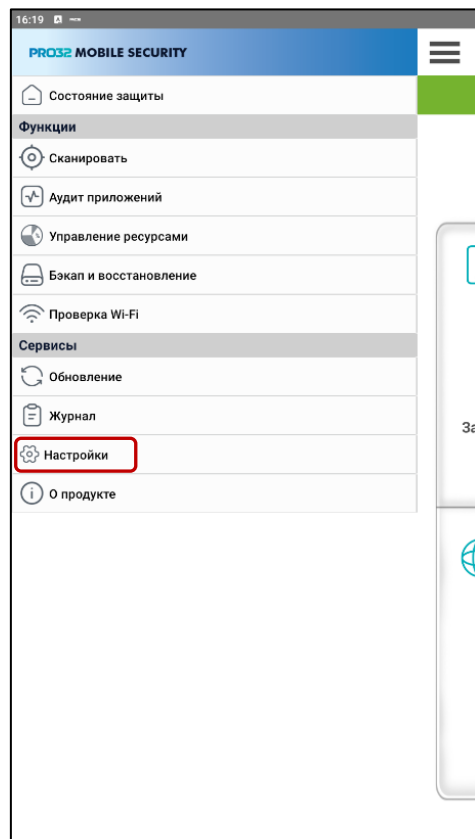
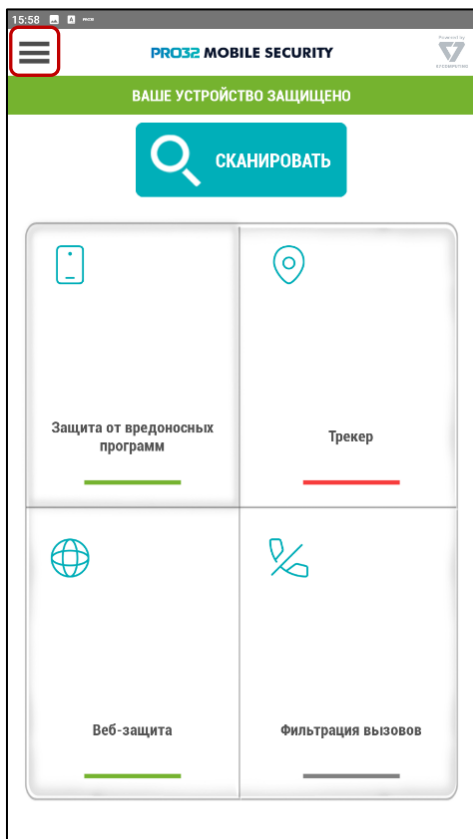
Активировать

Забыл лицензионный ключ

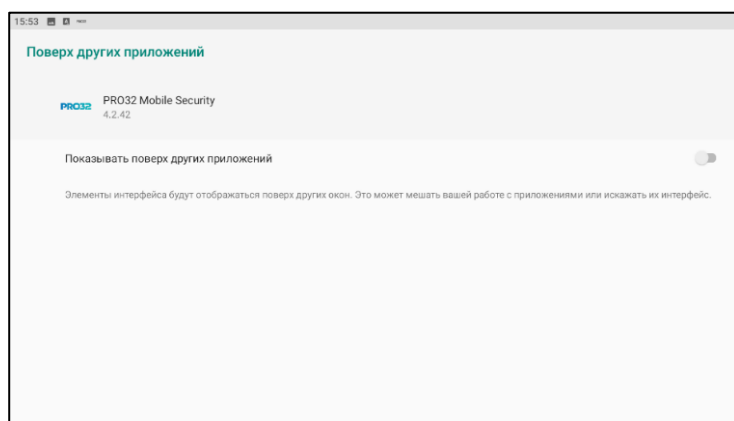
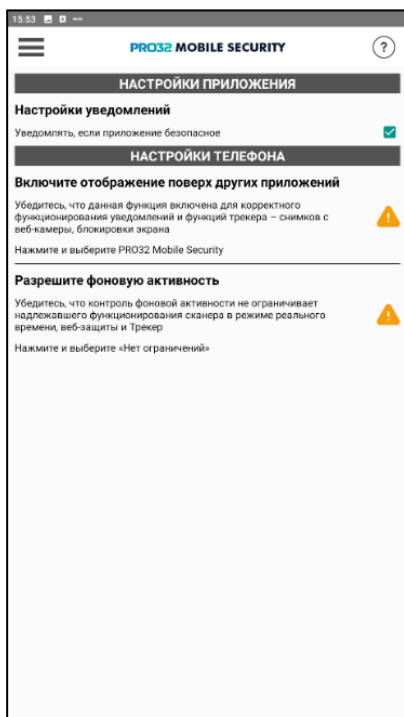


## VI. Настройки и дополнительные разрешения

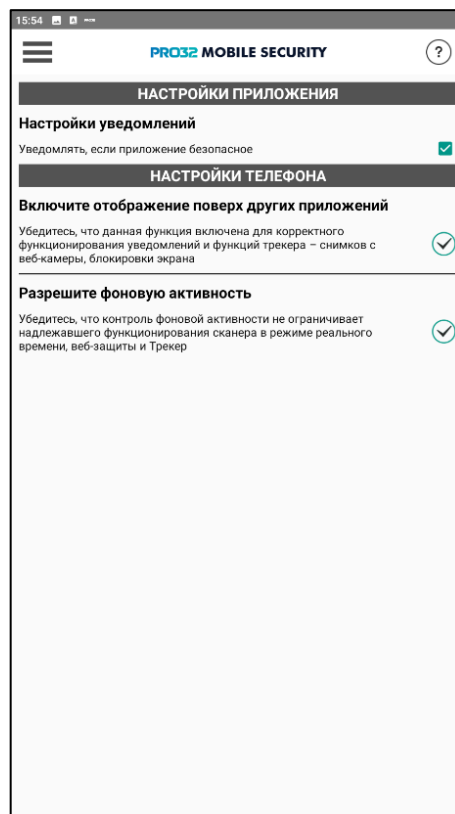
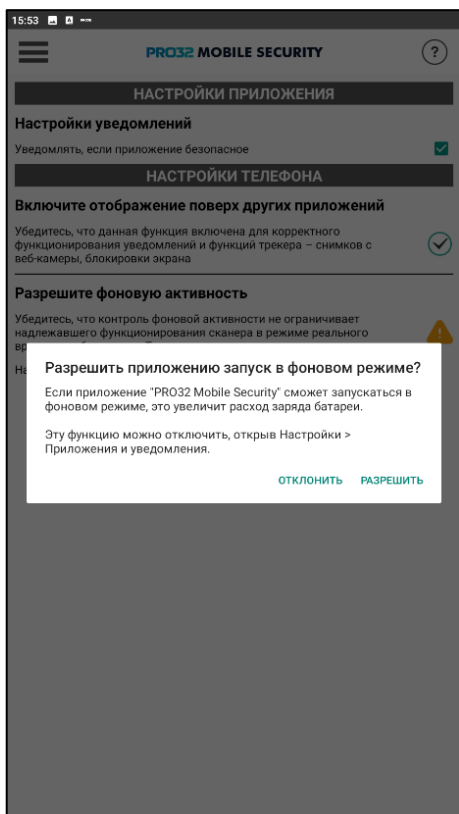
После первого запуска необходимо произвести настройки и предоставить приложению ещё несколько разрешений. Перейдите в меню «**Настройки**». Для этого на главном экране нажмите три черты в левом верхнем углу и выберите «**Настройки**».



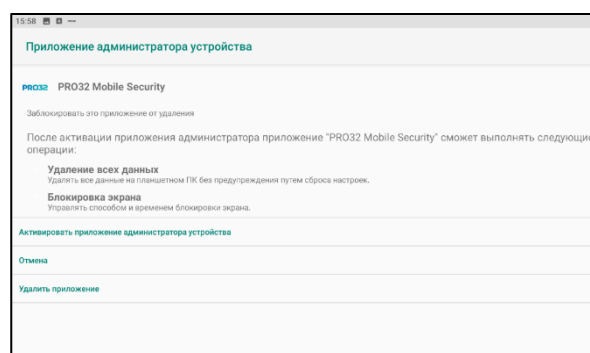
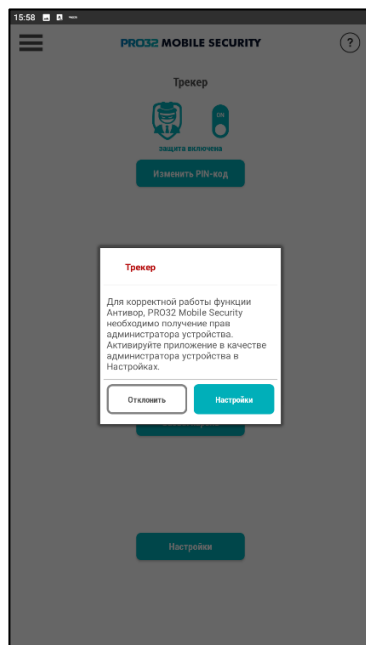
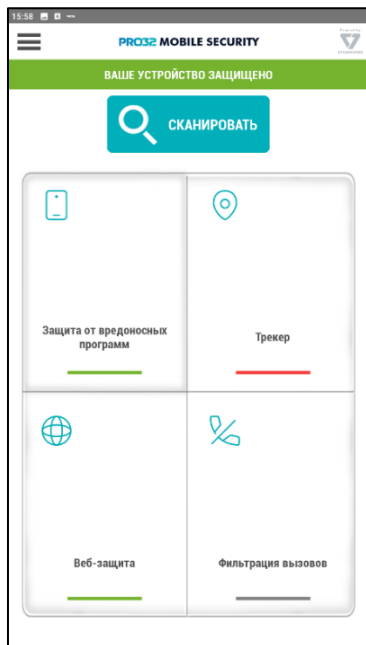
В открывшемся окне нажмите **«Включите отображение поверх других приложений»** и затем в появившемся окне системных настроек активируйте ползунок **«Показывать поверх других приложений»**. Таким образом, приложение получит возможность заблокировать устройство в случае его потери.



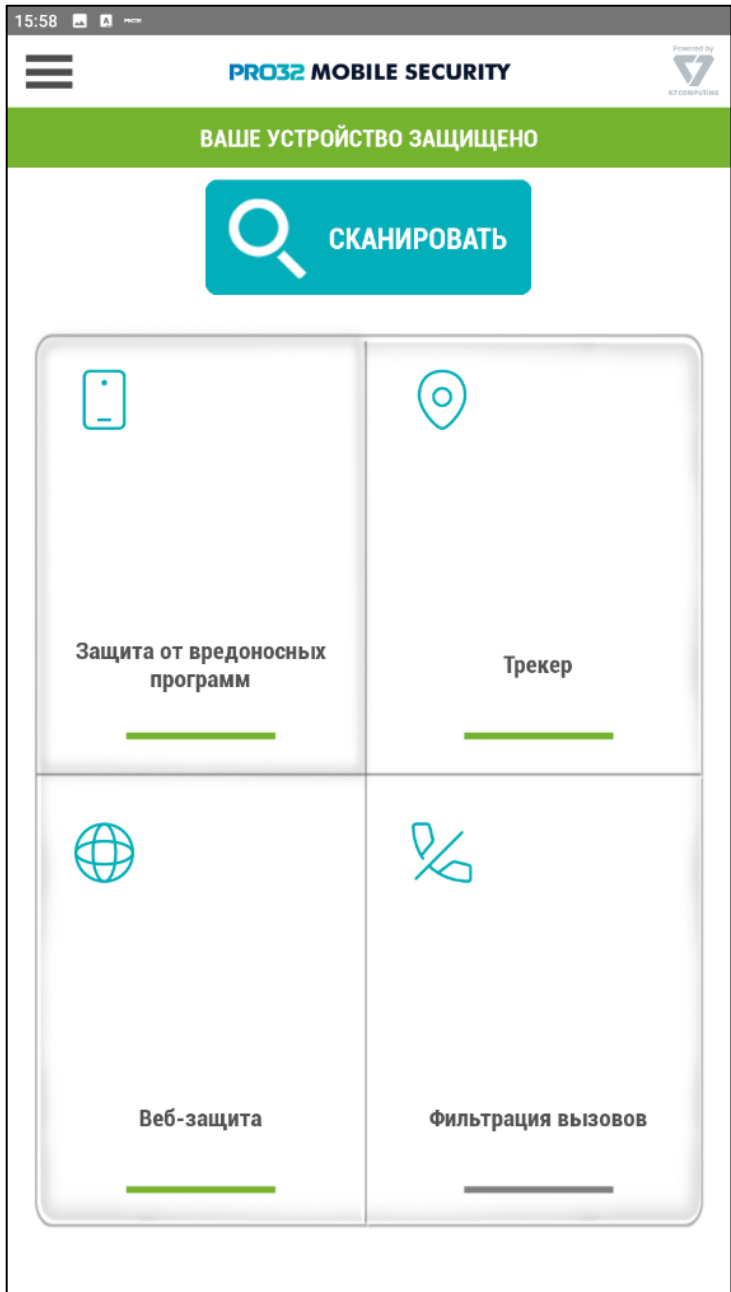
Далее, в том же окне нажмите **«Разрешите фоновую активность»** и нажмите **«Разрешить»** в появившемся окне. Работа в фоновом режиме позволит приложению защищать устройство в режиме реального времени. Восклицательные знаки в Настройках сменились галочками – всё сделано правильно.



Теперь необходимо предоставить права администратора устройства функции **Трекер**, необходимой для работы *Антивора*. Вернувшись на главный экран, нажмите на кнопку Трекер, подсвеченную красным. В открывшемся окне нажмите «**Настройки**». Перейдя в меню настроек телефона, выберите «**Активировать приложение администратора устройства**». Это разрешение позволит вам получить доступ к ряду функций устройства, таких как удаление пользовательских данных, включение сирены и т.п. в случае его потери.



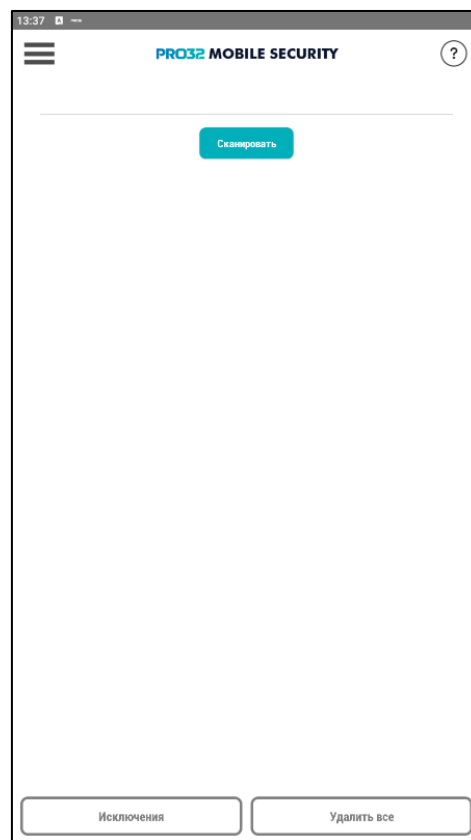
Теперь приложение полностью настроено и готово к работе.



## VII. Главный экран

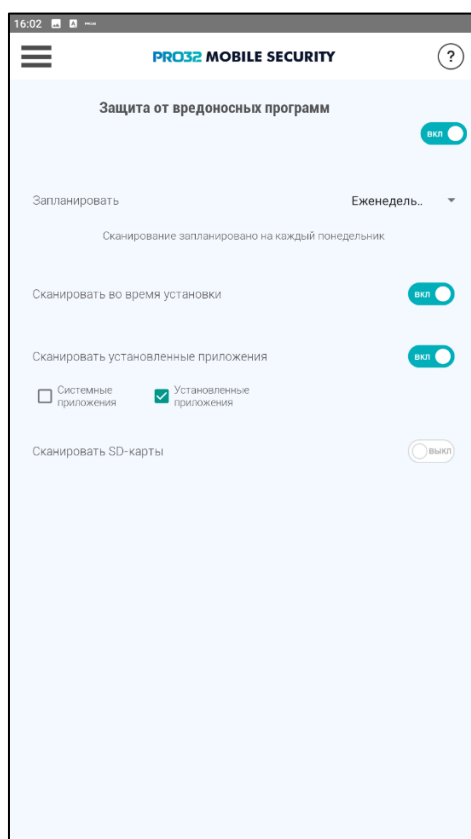
Рассмотрим элементы управления, расположенные на главном экране приложения:

1. **Кнопка Сканировать** позволяет вручную запустить проверку устройства на наличие вредоносных программ. Если будут найдены заражённые объекты, вы можете либо добавить его в исключения (таким образом, приложение больше не будет рассматривать его в качестве угрозы) соответствующей кнопкой внизу экрана, либо удалить его. Кнопка **«Удалить всё»** удалит все обнаруженные угрозы.



2. **Защита от вредоносных программ.** Здесь находятся основные настройки антивирусного модуля:

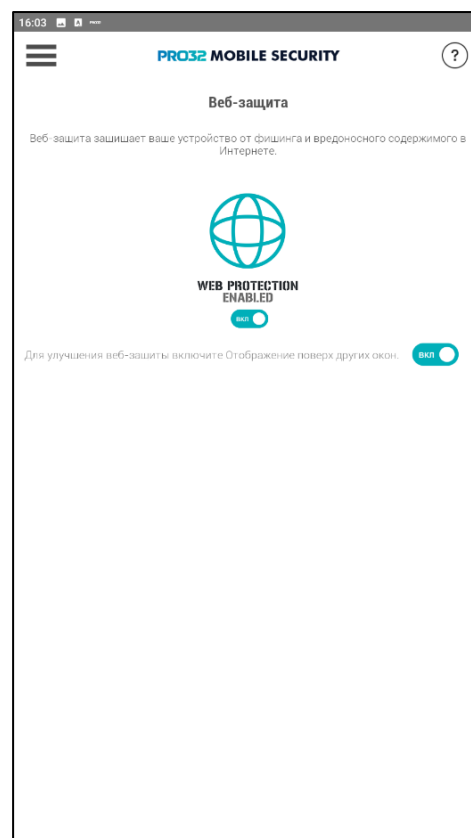
- Верхний переключатель позволяет полностью выключить антивирус. По умолчанию находится в положении **вкл.**
- **Запланировать** – автоматическое сканирование устройства по расписанию. Выберите периодичность сканирования – ежедневно, еженедельно либо ежемесячно. Нет – сканирование будет запускаться только в ручном режиме (с помощью кнопки **«Сканировать»** на главном экране).
- **Сканировать во время установки** – проверяет приложение на наличие вредоносного содержимого непосредственно во время его установки.
- **Сканировать установленные приложения** – будет проводиться проверка и тех приложений, которые



уже были установлены. При этом можно выбрать, нужно ли сканировать системные приложения, либо только те, что были установлены отдельно.

- **Сканировать SD-карты** – включает проверку содержимого внешнего накопителя.

3. **Веб-защита.** Модуль веб-защиты предназначен для защиты устройства от фишинговых сайтов и вредоносного содержимого в Интернет, блокируя потенциально опасное содержимое. Модуль включён по умолчанию. Для улучшения работы модуля веб-защиты, включите функцию **Отображение поверх других окон** (если не сделали этого ранее).

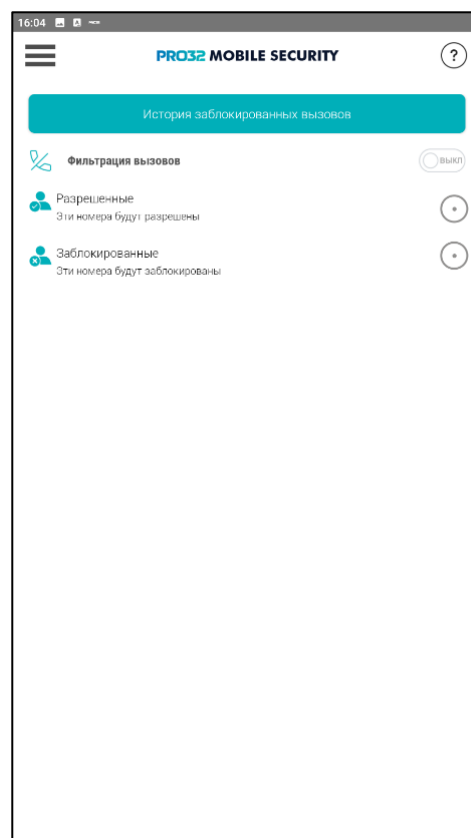


4. **Фильтрация вызовов.** Функция фильтрации вызовов может быть использована либо для блокировки вызовов с отдельных номеров, либо для разрешения вызовов с определённого списка номеров (при этом звонки с остальных номеров будут блокированы).

- **История заблокированных вызовов** показывает список вызовов, которые были заблокированы.
- **Фильтрация вызовов** – включает или полностью выключает функцию. По умолчанию функция выключена.
- **Разрешенные** – добавьте номера, вызовы с которых будут разрешены (при этом звонки с остальных номеров будут блокироваться).
- **Заблокированные** – добавьте номера, вызовы с которых будут блокироваться.

5. **Трекер** – настройки и функционал модуля *Антивор*. За подробным описанием обратитесь к разделу **X.**

**Функция Трекер и использование портала Трекер устройств** этого руководства.





## VIII. Функции приложения

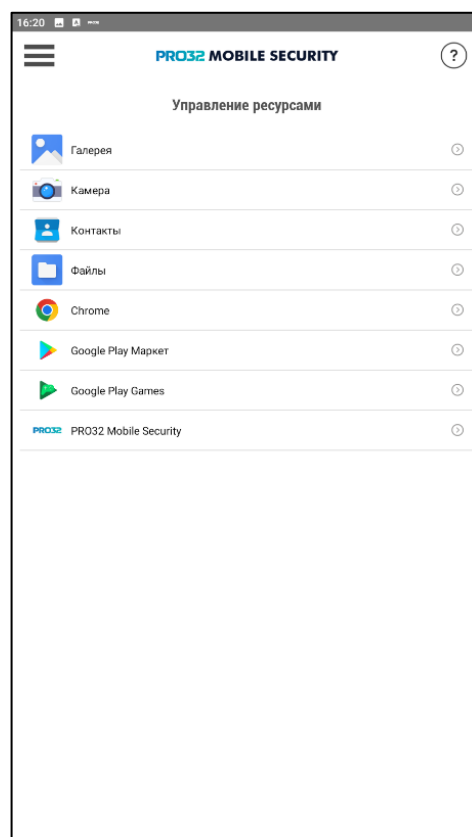
Рассмотрим раздел **Функции** главного меню приложения.

1. **Сканирование.** Аналогично кнопке **Сканировать** на главном экране, запускает ручную проверку устройства на вирусы. За подробностями обратитесь к соответствующему разделу данного руководства.

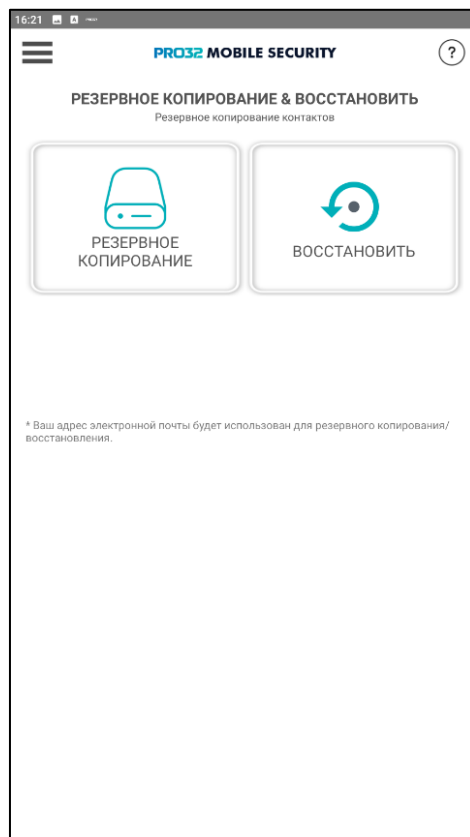
2. **Аудит приложений.** Данная функция предоставляет информацию о приложениях, имеющих разрешения на доступ к данным о местоположении устройства, SMS и звонкам. Откройте интересующий вас раздел, чтобы посмотреть список приложений.



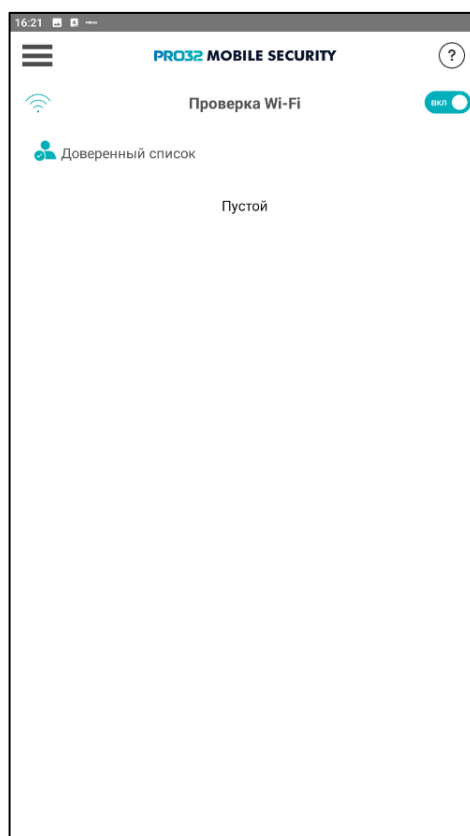
3. **Управление ресурсами.** Функция предоставляет данные об использовании приложениями оперативной памяти устройства, процессора, и объеме данных, передаваемых/получаемых по мобильной сети и Wi-Fi. Для просмотра сведений, нажмите на интересующее вас приложение.



4. **Бэкап и восстановление.** Функция позволяет выполнить резервное копирование контактов с устройства в облако, а также восстановить контакты из ранее сделанной копии. Для выполнения резервного копирования, нажмите кнопку «**Резервное копирование**» и введите имя копии. Для восстановления, нажмите «**Восстановить**» и выберите копию из существующих.



5. **Проверка Wi-Fi.** Добавьте данные доверенных Wi-Fi сетей в список разрешённых, которые можно безопасно использовать.



## IX. Сервисы

Рассмотрим раздел Сервисы главного меню приложения.

1. **Обновление.** В этом разделе находятся настройки обновления приложения. Нажмите кнопку «**Обновить**», чтобы выполнить обновление вручную. Переключатель «**Автоматическое обновление**» позволяет включить либо выключить автоматическую проверку обновлений. Активируйте переключатель «**Обновлять только по Wi-Fi**», чтобы избежать расхода мобильного трафика. Активируйте переключатель «**Отключить в роуминге**», чтобы избежать расхода трафика в роуминге.

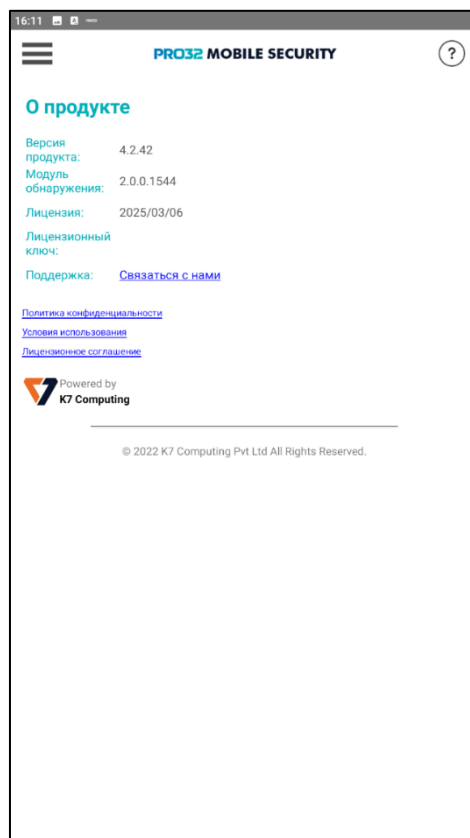


2. **Журнал.** Предоставляет доступ к журналу сканирования устройства на вирусы.



3. **Настройки.** Настройки приложения. Подробно описано в разделе [VI. Настройки и дополнительные разрешения](#) данного руководства.

4. **О продукте.** Здесь содержится информация о версии приложения и сроке действия вашей лицензии.
5. **Техническая поддержка** с радостью поможет вам. Нажмите **«Связаться с нами»** в разделе «О продукте», для перехода на портал технической поддержки.



## Х. Функция Трекер и использование портала Трекер устройств

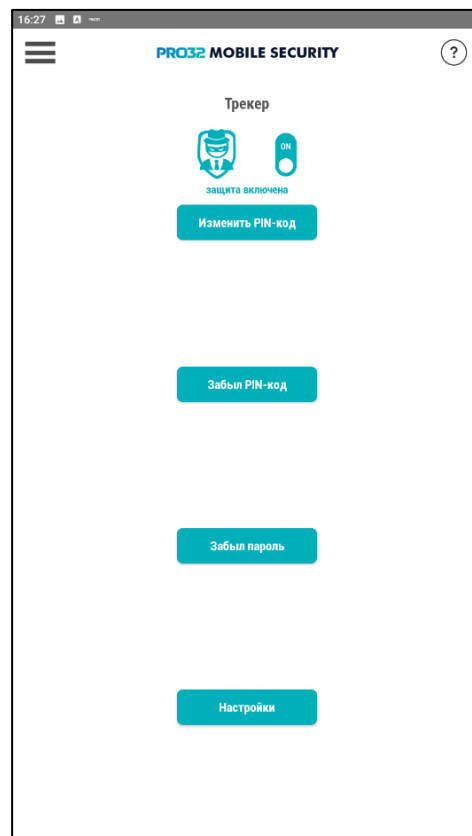
Подробно рассмотрим функцию **«Трекер»** (*Антивор*) и использование портала Трекер устройств.

*Примечание. Под PIN-кодом, паролем и адресом электронной почты подразумеваются данные, указанные при активации приложения (раздел*

### **V. Активация приложения)**

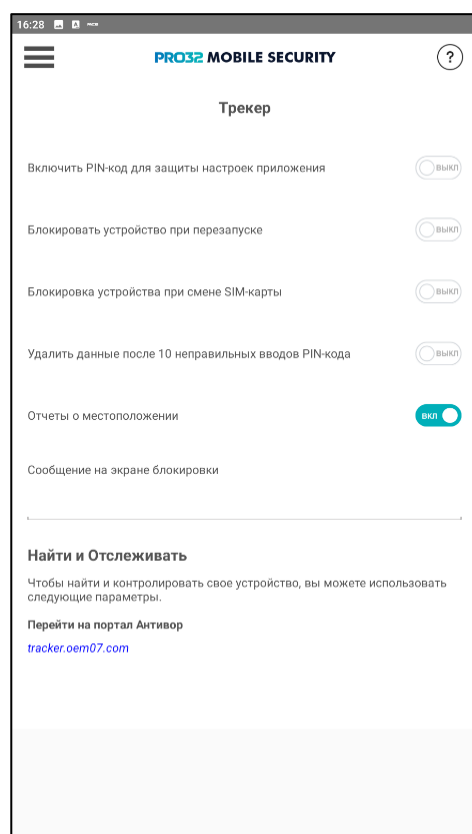
Перейдите на главный экран приложения и выберите «Трекер». На этом экране вы можете:

- Переключателем «On/Off» включить или полностью выключить функцию трекера
- Кнопкой «Изменить PIN-код» задать новый PIN-код (для этого будет необходимо ввести старый)
- Кнопкой «Забыл PIN-код» выслать напоминание о PIN-коде на адрес электронной почты, указанный при активации
- Кнопкой «Забыл пароль» выслать напоминание о пароле от личного кабинета на Портале на адрес электронной почты, указанный при активации



Меню **Настройки**:

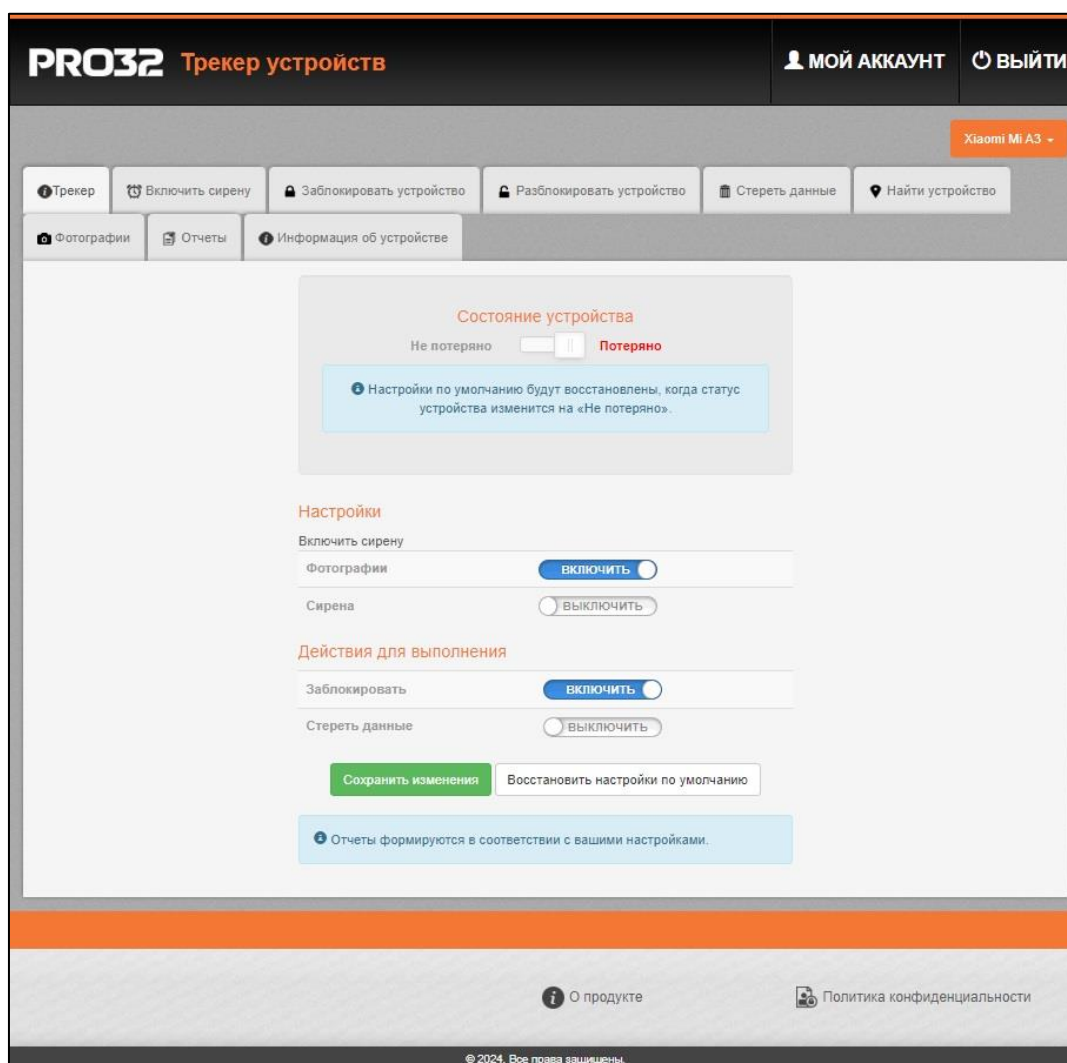
- **Включить PIN-код для защиты настроек приложения** – включает обязательный ввод PIN-кода при попытке изменить настройки
- **Блокировать устройство при перезапуске** – после перезагрузки устройство будет заблокировано и потребуются ввод PIN-кода
- **Блокировка устройства при смене SIM-карты** – при смене SIM-карты устройство будет заблокировано и потребуются ввод PIN-кода
- **Удалить данные после 10 неправильных вводов PIN-кода** – после 10 безуспешных попыток ввода PIN-кода все данные с устройства будут удалены
- **Отчёты о местоположении** – отправлять отчёты о местоположении устройства
- **Сообщение на экране блокировки** – введите сообщение, которое будет отображаться на экране блокировки устройства
- **Перейти на портал Антивор** – открыть страницу портала в браузере



*Примечание. Рекомендуем сохранить в закладках браузера на вашем ПК адрес Портала, чтобы в случае потери устройства оперативно получить к нему доступ.*

## Как действовать в случае потери устройства?

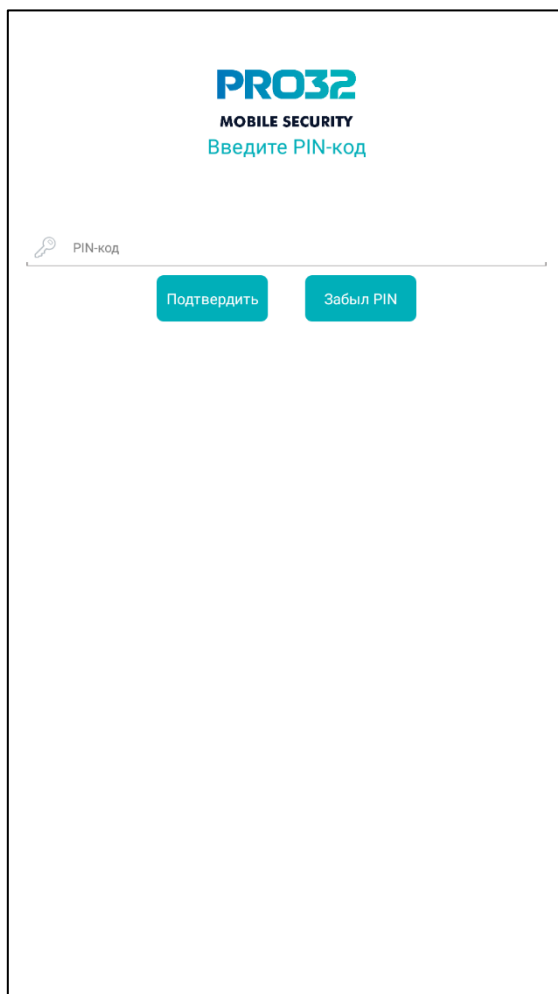
- Перейдите с любого устройства (ПК, телефон) на страницу портала по адресу, указанному выше ([tracker.oem07.com](http://tracker.oem07.com)), нажмите кнопку «**Войти**» в правом верхнем углу и введите свой адрес электронной почты и пароль, указанные при активации приложения
- Если на вашу учётную запись зарегистрировано несколько устройств, выберите нужное в выпадающем списке в правом верхнем углу
- Переведите переключатель «**Состояние устройства**» в положение «**Потеряно**»



На странице Трекер (та страница, на которой вы сейчас находитесь) вы можете:

- Переключателем «**Фотографии**» включить доступ к фронтальной камере устройства, чтобы получить возможность делать снимки
- Переключателем «**Сирена**» включить возможность включения сирены на устройстве
- Переключателем «**Заблокировать**» заблокировать устройство до ввода PIN-кода
- Переключателем «**Стереть**» данные удалить все данные на устройстве

Когда устройство будет заблокировано, использовать его будет невозможно, а на экране появится окно ввода PIN-кода:



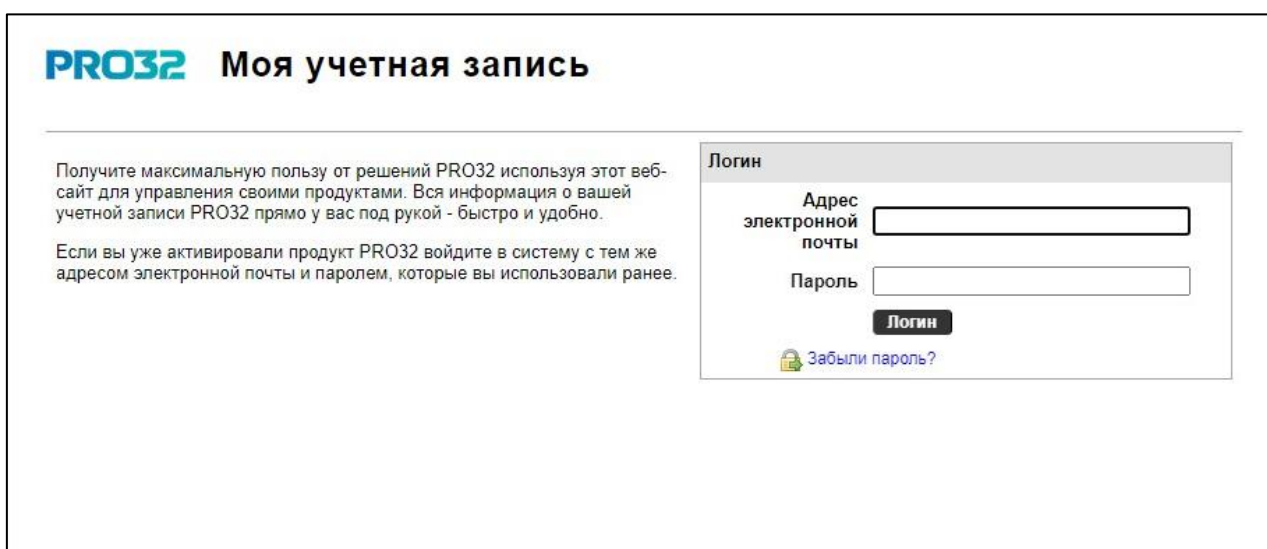
Рассмотрим остальные вкладки Портала:

- **Включить сирену** – на устройстве будет включена сирена, отключить которую можно будет только вводом PIN-кода
- **Заблокировать устройство** – устройство будет заблокировано, разблокировать его будет можно только вводом PIN-кода
- **Разблокировать устройство** – отключает блокировку устройства
- **Стереть данные** – удаляет все данные на устройстве
- **Найти устройство** – показывает карту с местоположением устройства
- **Фотографии** – позволяет сделать снимок с фронтальной камеры устройства
- **Отчёты** – сводный отчёт, содержащий информацию об устройстве, его местоположении, последних снимках с камеры, состоянии сетевого соединения, заряда аккумулятора и так далее
- **Информация об устройстве** – базовая информация об устройстве (версия ОС, оборудование и т.п.)

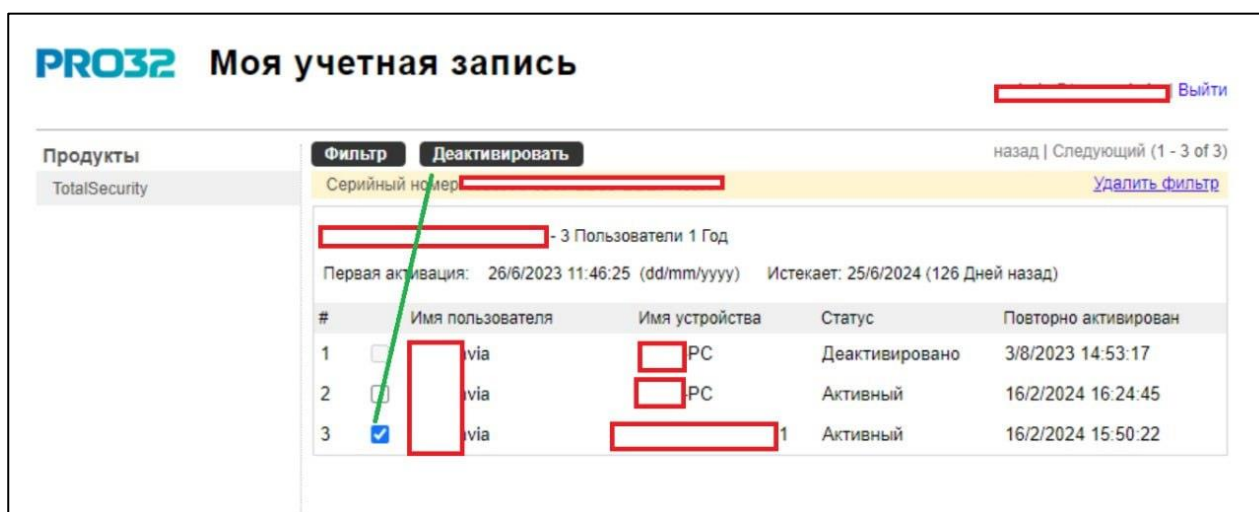
## XI. Управление лицензиями

PRO32 предлагает широкий ассортимент лицензий. Вы можете приобрести лицензию на несколько устройств. В определённых случаях (например, при потере или невозстановиваемом повреждении) требуется перенести лицензию с одного устройства на другое. Для этого воспользуйтесь порталом управлениями лицензиями.

<https://register.oem07.com/Pro32/Subscriptions/MyAccount.asp?lang=ru-ru>



Используйте адрес электронной почты и пароль, который вы задали при активации приложения (см. раздел [V. Активация приложения](#) настоящего документа).



| # | Имя пользователя | Имя устройства | Статус         | Повторно активирован |
|---|------------------|----------------|----------------|----------------------|
| 1 | [redacted] via   | [redacted] PC  | Деактивировано | 3/8/2023 14:53:17    |
| 2 | [redacted] via   | [redacted] PC  | Активный       | 16/2/2024 16:24:45   |
| 3 | [redacted] via   | [redacted] 1   | Активный       | 16/2/2024 15:50:22   |

Выберите устройство, на котором не планируете использовать продукт и нажмите кнопку «Деактивировать».

Теперь вы можете использовать имеющийся ключ активации на новом устройстве.