SIGUR

Приложение «Мобильный терминал Sigur». Руководство по настройке и работе

Редакция от 16.10.2026

«Промавтоматика», г. Н. Новгород, 2026 г.

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Оглавление

1. Введение ... 3
2. Версии документа ... 4
3. Используемые определения, обозначения и сокращения ... 5
4. Системные требования ... 6
5. Начало работы с приложением ... 7
6. Настройка на стороне ПО Sigur ... 9
   6.1. Общие настройки в ПО «Клиент» ... 9
7. Работа с приложением ... 12
8. Дополнительные функции приложения ... 16
   8.1. Санкционирование проходов сотрудников с мобильного терминала ... 16
   8.2. Сканирование QR-кодов и штрихкодов ... 19
9. TLS/mTLS шифрование трафика ... 23
   9.1. Настройка TLS/mTLS на мобильном устройстве ... 23
10. Контакты ... 28

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Введение

Документ содержит инструкции по настройке и использованию приложения «Мобильный терминал Sigur» в составе системы контроля и управления доступом (СКУД) Sigur.

Предприятие-изготовитель несёт ответственность за точность предоставляемой документации, и при существенных модификациях элементов системы обязуется предоставлять обновлённую редакцию данной документации.

Данный документ соответствует версии 3.1.0 приложения «Мобильный терминал».

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Версии документа

Данный документ имеет следующую историю ревизий.

Ревизия	Дата публикации	Что изменилось
0001	04 июля 2024 г.	Актуализация документа. Добавлены ссылки на скачивание мобильного приложения «Мобильный терминал Sigur» из магазинов приложений RuStore и AppGallery.
0002	11 декабря 2024 г.	Актуализация документа. Добавлено описание взаимодействия с использованием TLS/mTLS.
0003	21 июля 2025 г.	Актуализация требований в связи с изменением схемы лицензирования.
0004	15 сентября 2025 г.	Актуализирована информация о санкционировании проходов сотрудников с мобильного терминала.
0005	19 января 2026 г.	Актуализирован раздел «Системные требования»: добавлена информация о поддержке РЕД ОС М.
0006	24 марта 2026 г.	Актуализация документа. Добавлено описание функции сканирования QR-кодов и штрихкодов.
0007	23 сентября 2026 г.	Добавлена информация о поддержке идентификаторов формата W42. Актуализирована информация о настройке сканирования QR и штрихкодов. Обновлена минимальная поддерживаемая версия Android.
0008	16 октября 2026 г.	Уточнено название документа и терминология в связи с выпуском мобильного терминала Sigur MT.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно–аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
ПО	Программное обеспечение.
БД	База данных.
Приложение «Мобильный терминал Sigur»	Приложение для мобильных устройств, позволяющее использовать смартфон в качестве точки доступа в составе СКУД Sigur.

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Системные требования

- ОС мобильного устройства: Android 6.0 и выше / РЕД ОС М.
- Наличие NFC-чипа для использования смартфона в качестве считывателя.
- Свободное место на устройстве: от 8,8 МБ.
- Версия сервера СКУД Sigur: 1.8.5.69 и выше.
- Требуется наличие лицензии. Поддерживаются два режима работы:
    - Онлайн-режим — требует постоянного подключения мобильного устройства к серверу. Для работы в этом режиме необходимо наличие пакета лицензий Pro или Enterprise. В случае использования модульной схемы лицензирования дополнительные модули не требуются.
    - Офлайн-режим — допускает автономную работу мобильного устройства. Для работы в этом режиме также требуется пакет лицензий Pro или Enterprise и необходимое количество лицензий на работу с мобильным терминалом Sigur для регистрации проходов (Offline режим). В случае модульной схемы лицензирования достаточно только необходимого количества лицензий на работу с мобильным терминалом Sigur для регистрации проходов (Offline режим).
    - Сканирование QR-кодов и штрихкодов — функция доступна в пакетах лицензий Pro и Enterprise, а также при использовании соответствующего дополнительного модуля «Сканирование QR и штрихкодов в мобильном терминале» в рамках модульной схемы лицензирования.
- Поддержка OTG для подключения внешнего USB-считывателя.



Для работы с внешним USB-считывателем необходимо, чтобы сам считыватель имел режим эмуляции набора на клавиатуре считанного кода в десятичном формате (т. е. например, для пропуска «072,61947» это должно быть «0004780539» или «4780539»), с переводом строки в конце кода.

Известные ограничения.

Не поддерживается работа приложения «Мобильный терминал Sigur» на устройствах Samsung Galaxy совместно с использованием карт Mifare Classic. Данная проблема специфична для этого устройства, на нём не работает так же большинство других приложений, использующих NFC-модуль устройств.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Начало работы с приложением

Установите на телефон приложение «Мобильный терминал Sigur» из Google Play, RuStore или AppGallery.

Включите функции NFC и Wi-Fi (или мобильный интернет) на вашем смартфоне, запустите приложение и предоставьте ему все запрашиваемые разрешения.

При первом запуске приложения пользователю будет предложено ознакомиться с небольшой инструкцией.

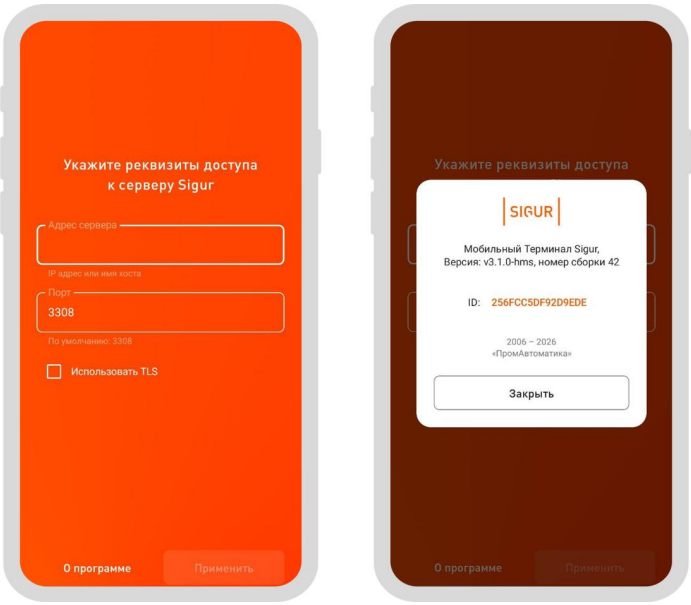


Первый запуск приложения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Во время ознакомления с инструкцией рекомендуется зафиксировать уникальный ID терминала, он потребуется при дальнейшей настройке терминала через ПО Sigur. ID терминала можно отправить на email/в мессенджер, нажав на соответствующий значок в строке справа от идентификатора.

ID терминала и версию приложения можно узнать, нажав кнопку «О программе» на странице ввода настроек сервера Sigur. В этом окне можно нажать на значение ID терминала и поделиться им предпочтительным способом.



Просмотр информации о терминале.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6. Настройка на стороне ПО Sigur

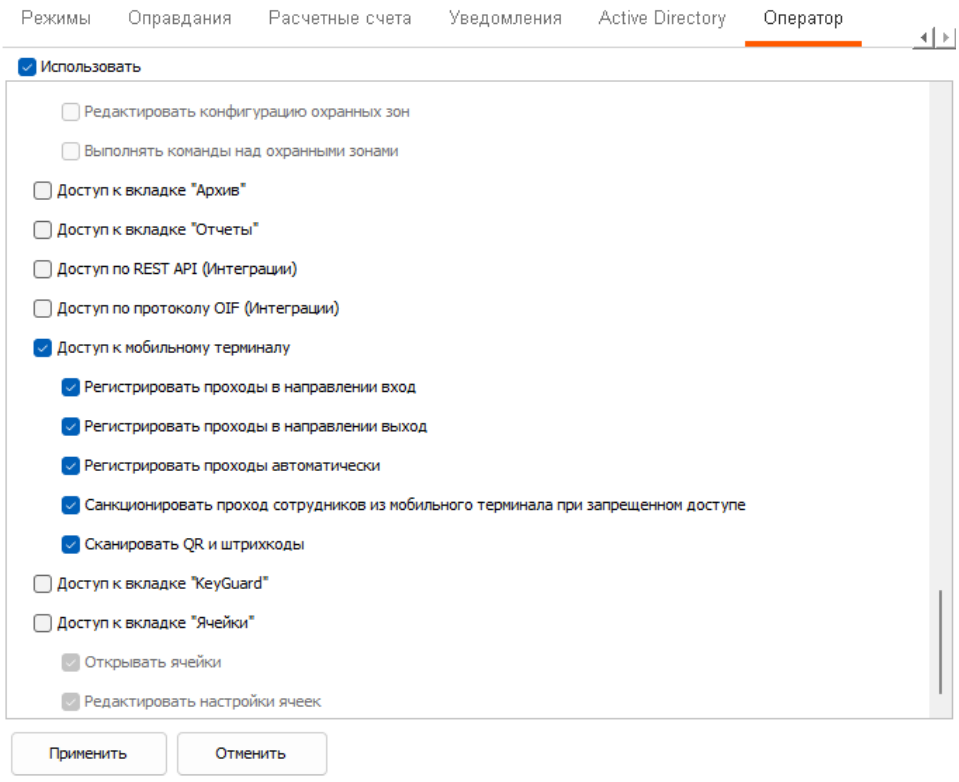
6.1. Общие настройки в ПО «Клиент»

1. Запустите ПО «Клиент» и перейдите на вкладку «Персонал».

2. Выберите уже существующего сотрудника или создайте новую запись для оператора, от имени которого будет работать мобильный терминал Sigur. Подробнее о создании операторов см. в «Руководстве пользователя ПО Sigur».

3. Перейдите на вкладку «Оператор» и включите опцию «Доступ к мобильному терминалу». Доступны следующие права:

   - регистрировать проходы в направлении «вход»
   - регистрировать проходы в направлении «выход»;
   - регистрировать проходы автоматически;
   - санкционировать проход сотрудников из мобильного терминала при запрещённом доступе;
   - сканировать QR и штрихкоды.



Пример настройки прав для оператора мобильного терминала.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Первая пара прав позволяет оператору вручную выбирать направление отметки при каждом факте предъявления пропуска. Установка опции «Регистрировать проходы автоматически» в дополнение к первым двум позволяет предварительно выбрать направление, в котором будут автоматически регистрироваться последующие отметки.

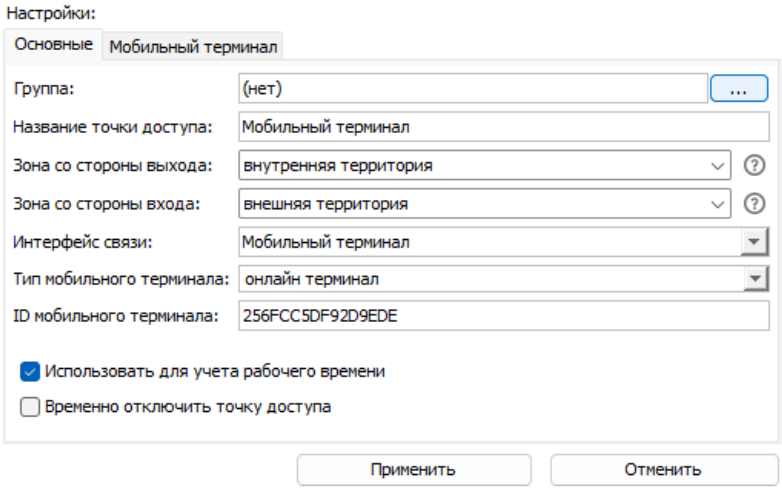
При необходимости оператору можно разрешить санкционировать проход сотрудников при запрещённом доступе. Эта функция подробно описана в отдельной главе. Также оператору можно назначить право на сканирование QR-кодов и штрихкодов. Подробное описание функции приведено в данном разделе.

После завершения настройки прав оператора нажмите «Применить».

4. Перейдите на вкладку «Оборудование» и создайте новую точку доступа. Необходимо настроить следующие параметры:

   - Интерфейс связи — Мобильный терминал.
   - Тип мобильного терминала:
     - онлайн — терминал находится на постоянной связи с сервером, при потере связи автономная работа невозможна;
     - офлайн — терминал не требует постоянного наличия связи с сервером, информация по картам доступа и совершаемым отметкам прописывается в память устройства, при восстановлении связи с сервером происходит синхронизация;
     - онлайн касса — терминал работает в специальном режиме, позволяющем продавать позиции меню (при использовании пакета лицензий Pro или Enterprise, или при установленном модуле «Платёжная система» в случае модульной схемы лицензирования), а также находится на постоянной связи с сервером.
   - ID терминала — укажите уникальный ID терминала. Его можно узнать в приложении «Мобильный терминал Sigur».

SEC.RU | Короткий путь к информации Скачано с sec.ru



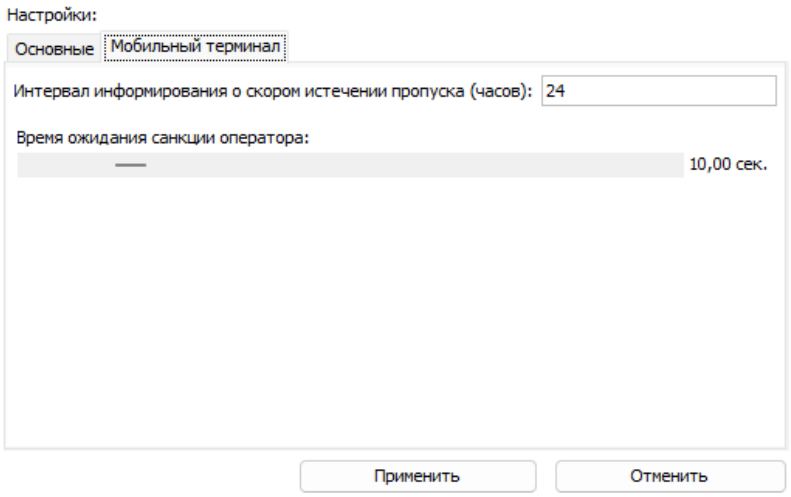
Пример настройки терминала на вкладке «Оборудование» в ПО «Клиент.

После заполнения параметров нажмите «Применить».

5. На подвкладке «Мобильный терминал» можно указать дополнительные параметры работы терминала:

- «Интервал информирования о скором истечении пропуска (часов)» — поле для указания временного интервала, в рамках которого до наступления окончания срока действия пропуска объекта на мобильном терминале будет выводиться соответствующее предупреждение оператору системы.

- «Время ожидания санкции оператора» — актуально для санкционирования проходов сотрудников при запрещённом доступе. Более подробно этот функционал описан в отдельной главе.



Пример настройки терминала на подвкладке «Мобильный терминал» в ПО «Клиент.

Добавление пропусков производится на вкладке «Персонал», подробнее см. в «Руководстве пользователя ПО Sigur».

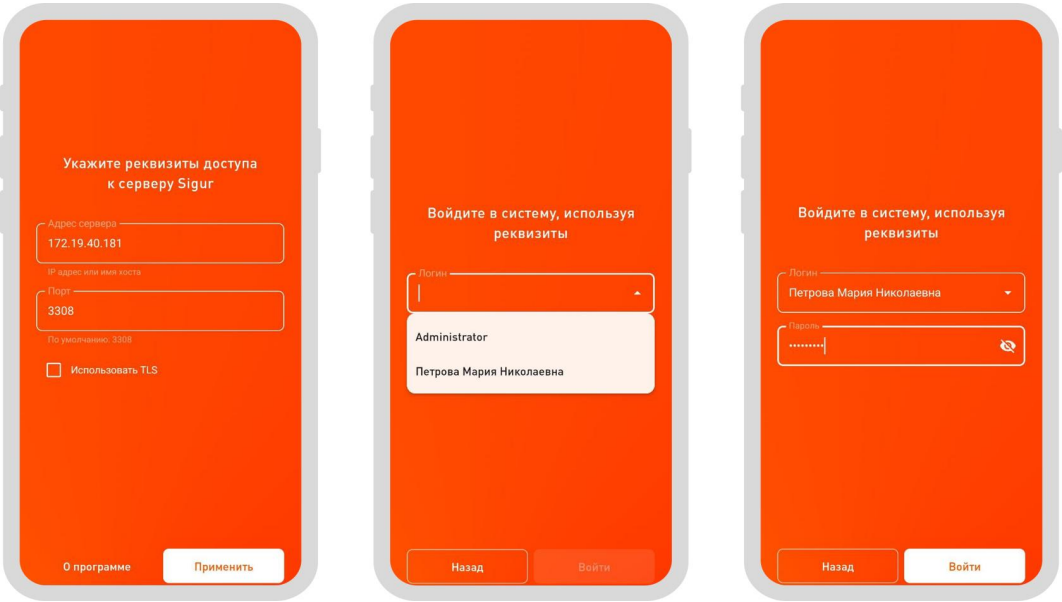
SEC.RU | Короткий путь к информации Скачано с sec.ru

7. Работа с приложением

Если подключение к серверу ранее не было установлено, то пользователю будет предложено ввести реквизиты для подключения к серверу Sigur: IP-адрес и TCP-порт (по умолчанию — 3308). После ввода параметров необходимо нажать кнопку «Применить».

Далее при успешном подключении к серверу будет предложено выбрать одного из операторов, которым разрешён доступ к мобильному терминалу. Выберите оператора, введите его пароль и нажмите «Войти».

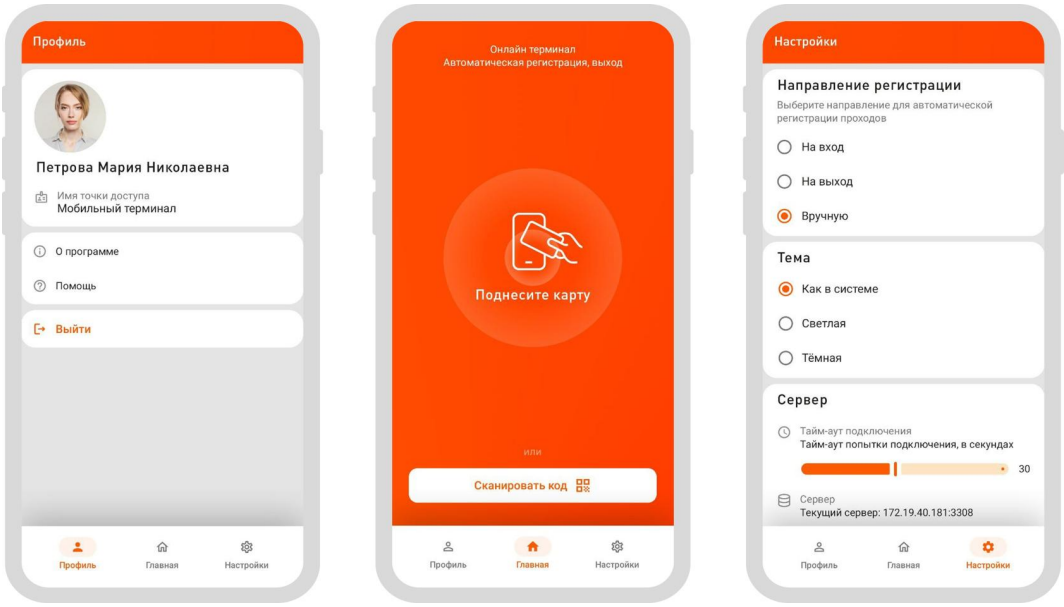
После добавления устройства в ПО Sigur, создания оператора и логина от его имени на устройстве, терминал готов к работе.



Окно для настройки параметров подключения к серверу Sigur.

SEC.RU | Короткий путь к информации Скачано с sec.ru

В нижей части экрана расположена навигационная панель приложения.



Навигационная панель приложения.

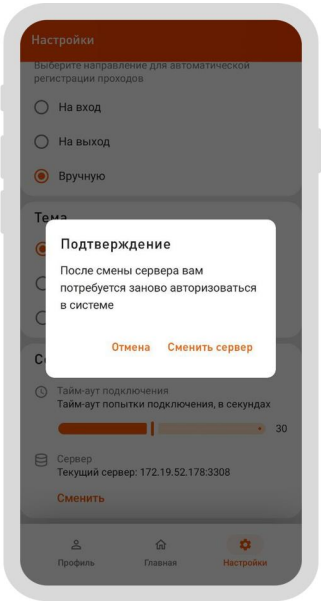
В разделе «Профиль» содержится информация об операторе и приложении. Также в этом разделе с помощью кнопки «Помощь» можно задать вопрос или отправить файлы журнала на электронную почту технической поддержки Sigur.

В разделе «Главная» отображаются режим работы терминала (онлайн или офлайн), режим регистрации проходов, а также кнопка сканирования кодов.

В разделе «Настройки» можно:

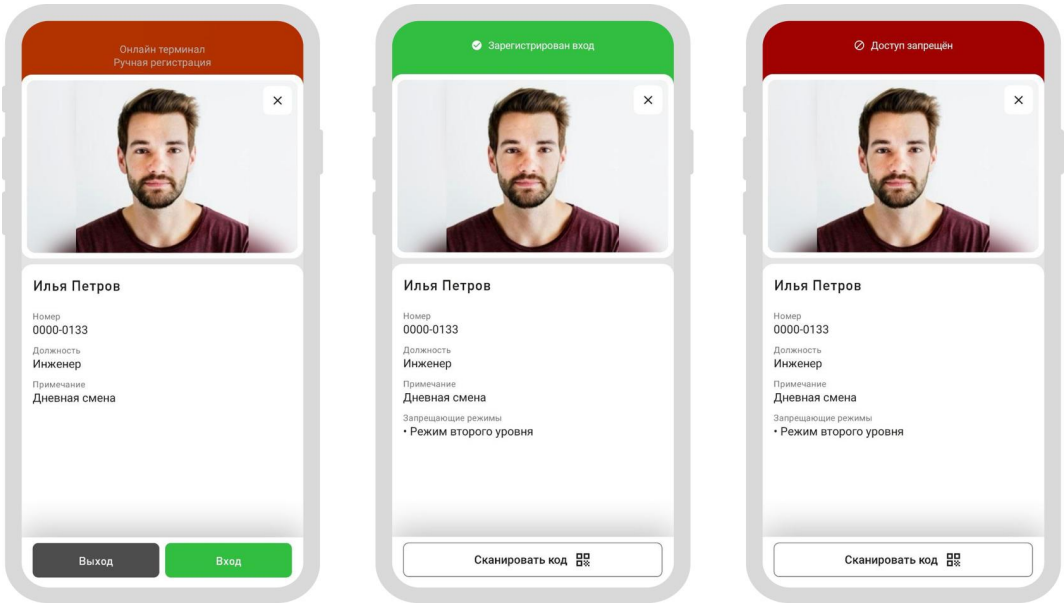
- выбрать направление для автоматической регистрации проходов (если оператору разрешено регистрировать проходы и на вход, и на выход, а также доступна автоматическая регистрация);
- изменить тему приложения;
- задать тайм-аут подключения к серверу — время, в течение которого терминал будет пытаться подключиться к серверу по указанным IP-адресу и порту;
- изменить параметры подключения к серверу. Для этого в разделе «Сервер» нажмите кнопку «Сменить» и подтвердите действие.

SEC.RU | Короткий путь к информации Скачано с sec.ru



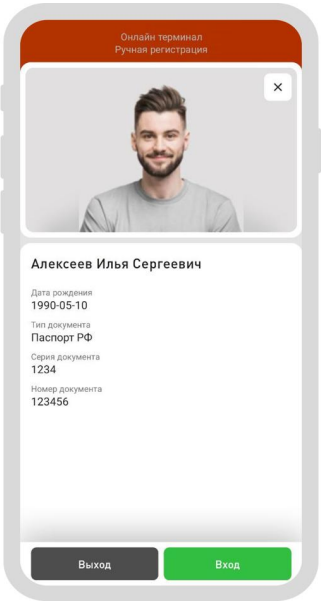
Окно подтверждения смены сервера.

При поднесении карты или считывании QR-кода объекта доступа оператору терминала будет предложено вручную зафиксировать проход в нужном направлении, либо проход будет зарегистрирован автоматически, либо появится сообщение о запрете доступа.



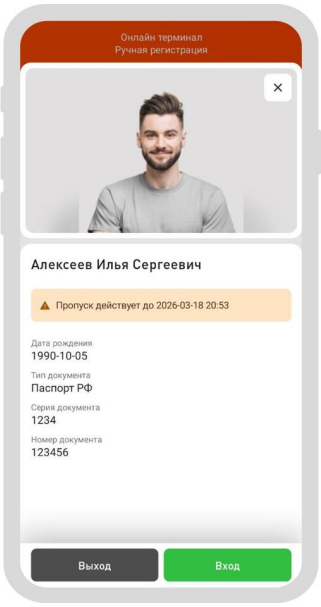
Примеры успешной идентификации с возможностью выбора направления прохода, успешной регистрации прохода и запрета доступа.

SEC.RU | Короткий путь к информации Скачано с sec.ru



Пример отображения пропуска посетителя.

При считывании пропуска с истекающим сроком действия приложение издаст звуковой сигнал и покажет оповещение об окончании срока действия пропуска.



Вид оповещения о приближении окончания срока действия пропуска.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8. Дополнительные функции приложения

8.1. Санкционирование проходов сотрудников с мобильного терминала

Оператор может санкционировать проходы сотрудников из мобильного приложения в том случае, если сотруднику запрещён доступ согласно назначенному режиму.

Данная функция доступна только при работе мобильного терминала в онлайн-режиме.

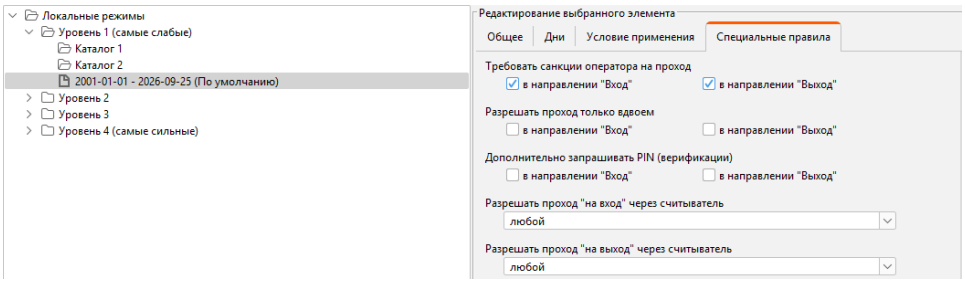
Для настройки необходимо выполнить следующее:

1. В правах оператора-пользователя мобильного терминала должна быть активирована функция «Санкционировать проход сотрудников из мобильного терминала при запрещённом доступе».

2. Сотруднику должен быть назначен режим доступа, в специальных правилах которого включена опция «Требовать санкции оператора на проход» в необходимом направлении. Подробнее с настройкой режимов доступа можно ознакомиться в соответствующем разделе «Руководства пользователя ПО Sigur».

   Санкция запрашивается, если выполнены следующие условия:

   - сотруднику запрещён доступ согласно назначенному режиму доступа;
   - в карточке сотрудника разрешён проход на данную точку доступа;
   - срок доступа и срок действия пропуска не истёк.

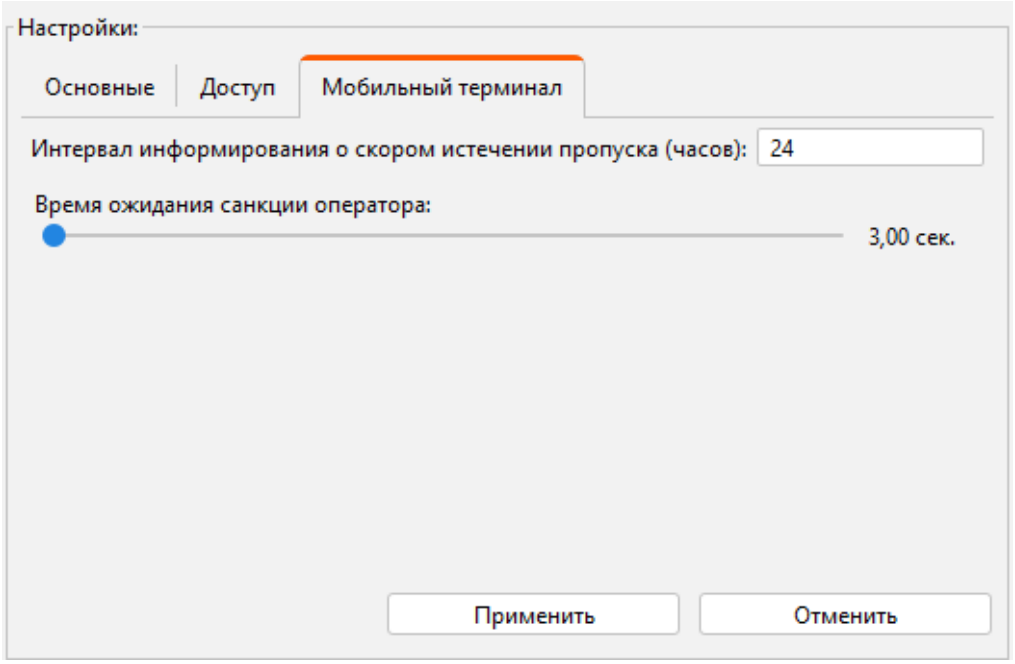


Пример настроек режима, требующего санкции оператора при проходе.

3. Время ожидания санкции оператора можно отрегулировать в настройках точки доступа на вкладке «Оборудование», подвкладка «Мобильный

SEC.RU | Короткий путь к информации Скачано с sec.ru

терминал».

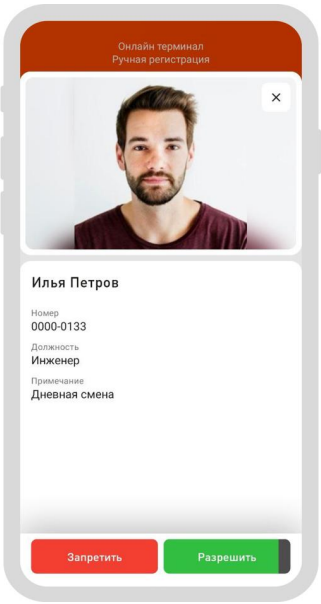


Настройка времени ожидания санкции оператора на подвкладке «Мобильный терминал».

Если сотрудник идентифицировался на точке доступа «Мобильный терминал», санкцию на проход может предоставить только оператор этого мобильного терминала — предоставить санкцию иными способами (через ПО «Клиент», нажатием на физическую кнопку, через USB-считыватель) в такой ситуации нельзя.

SEC.RU | Короткий путь к информации Скачано с sec.ru

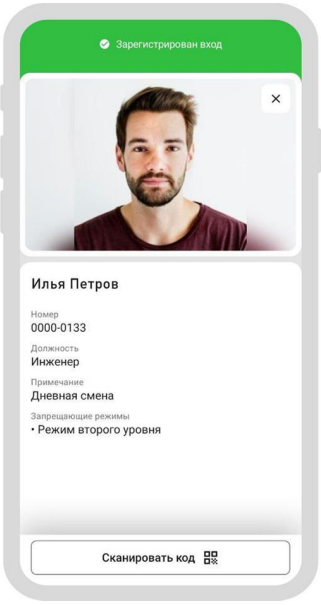
В результате по факту идентификации сотрудника оператору будет предложено санкционировать проход:



Пример отображения запроса санкции оператора в приложении.

После разрешения или запрета прохода на экране терминала появится информация о сотруднике, включая параметр «Запрещающие режимы». В нём указан режим верхнего уровня, в соответствии с которым вызвана санкция оператора. Это может быть полезно в ситуациях, когда сотруднику назначено сразу несколько режимов и необходимо определить, какой из них стал причиной вызова санкции. Например, если сотруднику назначены режимы 1-го и 2-го уровней и в каждом из них для прохода требуется санкция оператора, в карточке отобразится только режим 2-го уровня. Если при проходе санкция оператора не запрашивалась, параметр «Запрещающие режимы» отображаться не будет.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Пример отображения параметра «Запрещающие режимы».

В системе регистрируются события ожидания санкции при запрещённом доступе, а также события запрета доступа в том случае, если санкция на проход не была предоставлена. Просмотреть события можно через программу «Клиент» на вкладках «Наблюдение» или «Архив».

Список событий:

Время	Точка	Событие
2026-03-18 12:48:34	Мобильный терминал	Ожидание санкции оператора (доступ запрещен). Объект: Илья П. . Напр.: вход.
2026-03-18 12:48:35	Мобильный терминал	Доступ запрещен. Оператор отказал в доступе. Объект: Илья П. . Напр.: вход.
2026-03-18 12:48:53	Мобильный терминал	Ожидание санкции оператора (доступ запрещен). Объект: Илья П. . Напр.: вход.
2026-03-18 12:48:53	Мобильный терминал	Зарегистрирован проход. Объект: Илья П. . Напр.: вход.

Пример отображения событий на вкладке «Наблюдение» для санкционированного прохода и отказа в предоставлении санкции на проход.

8.2. Сканирование QR-кодов и штрихкодов

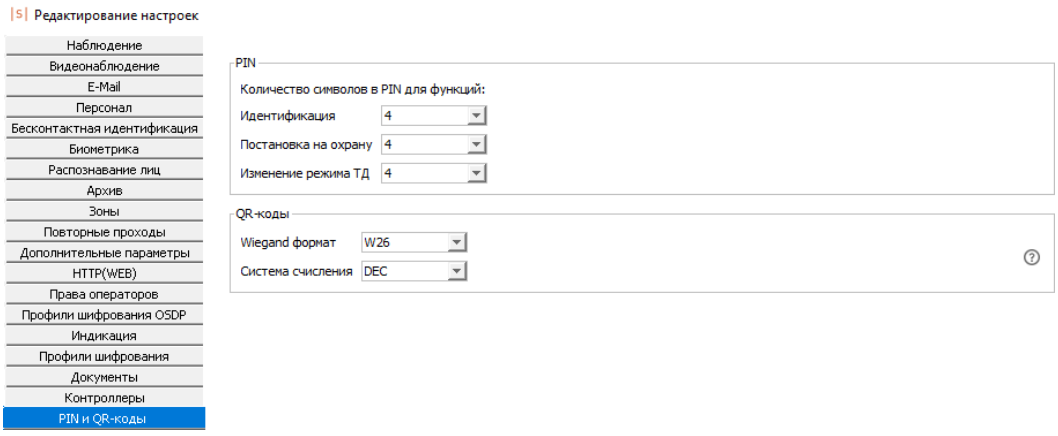
Приложение поддерживает сканирование QR-кодов и штрихкодов для идентификации сотрудников и посетителей. Функция доступна в онлайн и офлайн режимах работы терминала.

Приложение распознаёт штрихкоды формата Code 128 и QR-коды, содержащие идентификаторы формата Wiegand:

- W26, W34, W42, W58 в HEX — шестнадцатеричная запись кода;
- W26, W34, W42, W58 в DEC — десятичная запись кода;
- W26 в DEC, записанный с запятой (с Facility Code), например 123,12345 — только в штрихкодах Code 128.

Формат чтения QR-кодов и штрихкодов определяется в ПО «Клиент» в меню «Файл» — «Настройки» — «PIN и QR-коды».

SEC.RU | Короткий путь к информации Скачано с sec.ru



Окно настройки формата QR-кодов.

При изменении настроек ранее выданные QR-коды и штрихкоды перестанут распознаваться приложением «Мобильный терминал Sigur».

Сканирование доступно при одновременном выполнении следующих условий:

1. Наличие активной лицензии. Активировать её можно через партнёрский портал. Подробная инструкция приведена в руководстве, в разделе «Расширение лицензий».

2. В правах оператора-пользователя мобильного терминала активирована функция «Сканировать QR и штрихкоды». Данное право будет доступно только при наличии лицензии.

При выполнении этих двух условий в приложении станет доступна кнопка «Сканировать код».

SEC.RU | Короткий путь к информации Скачано с sec.ru



Отображение кнопки «Сканировать код».

При нажатии кнопки «Сканировать код» приложение запросит разрешение на доступ к камере устройства. Необходимо предоставить доступ, после чего откроется режим сканирования. Также допускается использование ранее сделанного изображения: вместо сканирования с камеры можно выбрать фотографию с QR-кодом или штрихкодом из галереи устройства с помощью кнопки, расположенной в правом верхнем углу.



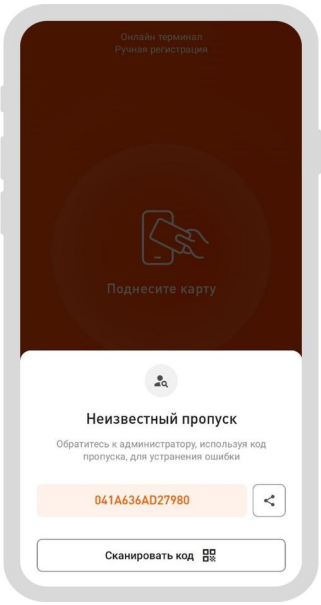
Режим сканирования в приложении.

При считывании QR-кода или штрихкода в приложении в системе формируется событие «Считан код: <считанная строка>». Событие не отображается на вкладке «Наблюдение» в ПО «Клиент» и доступно только в журнале событий системы и на вкладке «Архив».

SEC.RU | Короткий путь к информации Скачано с sec.ru

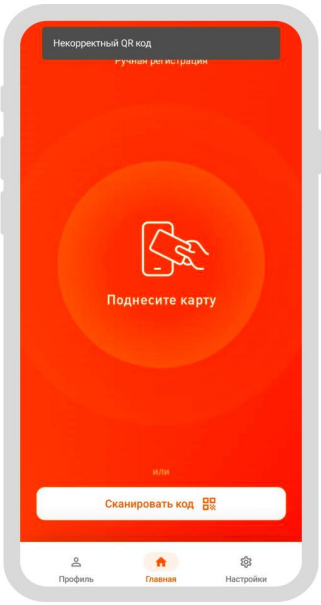
После распознавания QR-кода/штрихкода приложение выполняет проверку пропуска. В случае успешного распознавания отображаются данные сотрудника и выполняется автоматическая или ручная регистрация.

Если считанный QR-код/штрихкод не соответствует ни одному зарегистрированному пропуску, на экране отображается предупреждение «Неизвестный пропуск» с номером пропуска.



Пример предупреждения «Неизвестный пропуск».

При сканировании QR-кода или штрихкода неподдерживаемого формата отображается предупреждение «Некорректный QR-код/штрихкод».



Пример предупреждения «Некорректный QR-код».

SEC.RU | Короткий путь к информации Скачано с sec.ru

9. TLS/mTLS шифрование трафика

По умолчанию между сервером и приложением «Мобильный терминал Sigur» используется незащищённое соединение. Однако поддерживаются протоколы соединения TLS и mTLS.

Выбор предпочтительного метода взаимодействия остаётся за пользователем системы. Приложение «Мобильный терминал Sigur» поддерживает TLSv1.2 и выше.

Для обеспечения защищённого соединения необходимо настроить сервер и приложение.

Процесс установки зашифрованного соединения между клиентом и сервером Sigur описан в следующих разделах «Руководства администратора ПО Sigur»:

- «Установка зашифрованного соединения между клиентом и сервером» — для соединения по TLS.
- «Взаимная аутентификация» — для соединения по mTLS.

Поскольку приложение также является клиентом, процесс настройки сервера для взаимодействия с ним аналогичен. Ниже описана настройка зашифрованного соединения в приложении.

9.1. Настройка TLS/mTLS на мобильном устройстве

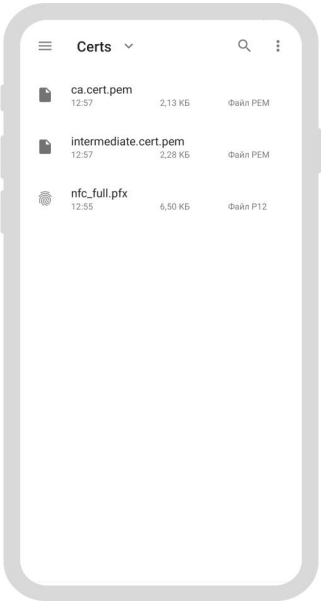
Установка пользовательских сертификатов на Android.

1. Для обеспечения соединения по защищенному протоколу TLS/mTLS необходимо загрузить сертификаты в смартфон с ОС Android, на котором установлено приложение «Мобильный терминал»:

- корневой сертификат;
- промежуточный сертификат;
- пользовательский сертификат — только для соединения по mTLS.

Корневой и промежуточный сертификат допускается загружать в виде файла .pem, пользовательский сертификат — в виде файла .pfx или .p12.

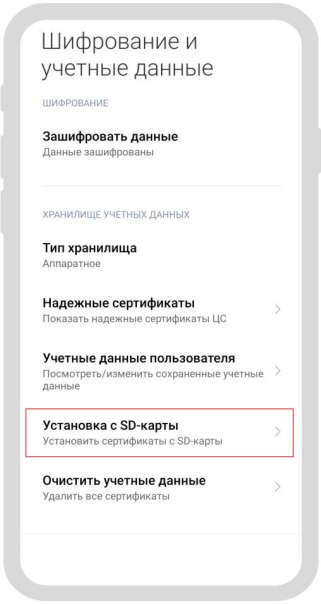
SEC.RU | Короткий путь к информации Скачано с sec.ru



Пример каталога с файлами сертификатов.

2. Загруженные файлы необходимо установить на смартфон. Для этого перейдите в «Настройки» — «Конфиденциальность» — «Шифрование и учетные данные» — «Хранилище учетных данных» — «Установить сертификаты».

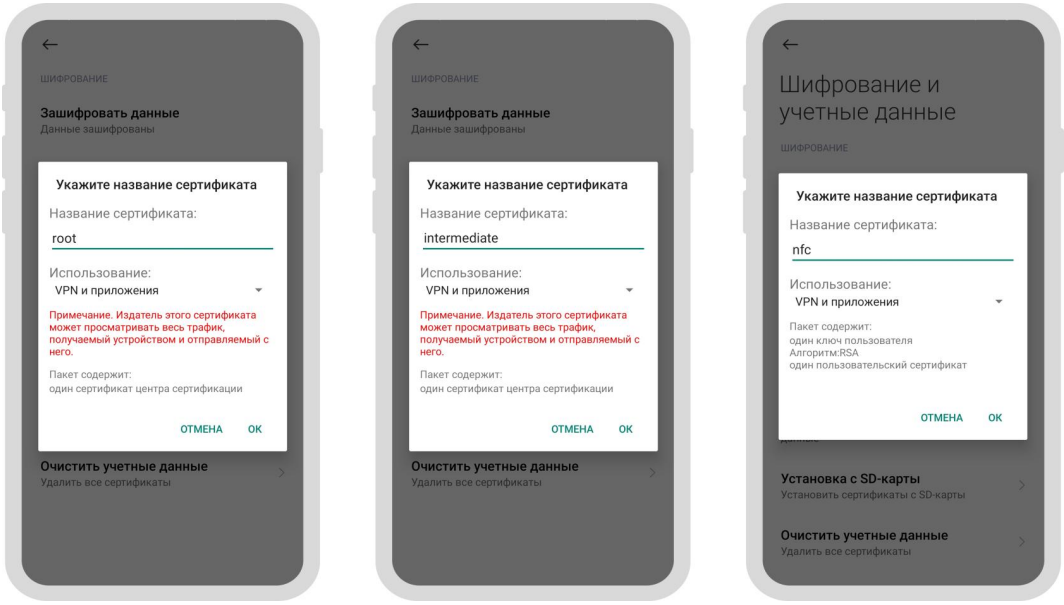
В зависимости от версии ОС Android и графической оболочки путь к настройкам может отличаться.



Хранилище сертификатов.

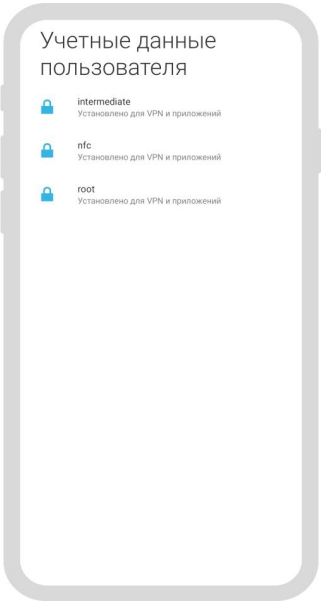
SEC.RU | Короткий путь к информации Скачано с sec.ru

3. При установке сертификатов будет предложено выбрать файлы из памяти смартфона и указать название сертификата (например root — для корневого, intermidiate — для промежуточного, nfc — для пользовательского). При загрузке пользовательского сертификата необходимо ввести пароль. Пароль устанавливается администратором или пользователем в процессе генерации хранилища пользовательского сертификата.



Установка сертификатов.

4. После успешной установки сертификаты будут отображаться в учетных данных пользователя.



Установленные сертификаты.

SEC.RU | Короткий путь к информации Скачано с sec.ru

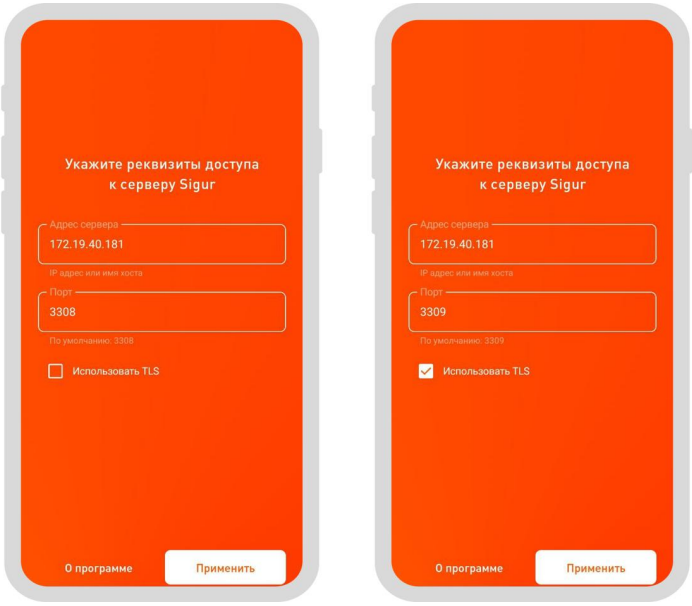
Далее откройте приложение «Мобильный терминал Sigur».

Настройка подключения в приложении.

1. При подключении к серверу пользователю будет предложено ввести реквизиты: IP-адрес и TCP-порт.

Для использования соединения по TLS пользователю необходимо активировать соответствующий чекбокс. При этом TCP-порт по умолчанию в пользовательском интерфейсе будет изменен на 3309.

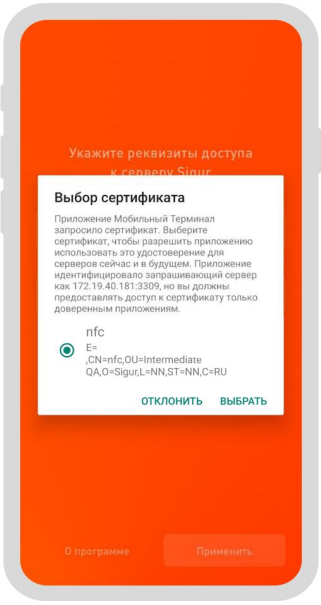
После ввода параметров необходимо нажать кнопку «Применить». В случае сбоя подключения к серверу на экране будет отображаться сообщение об ошибке.



Подключение приложения к серверу с использованием TLS.

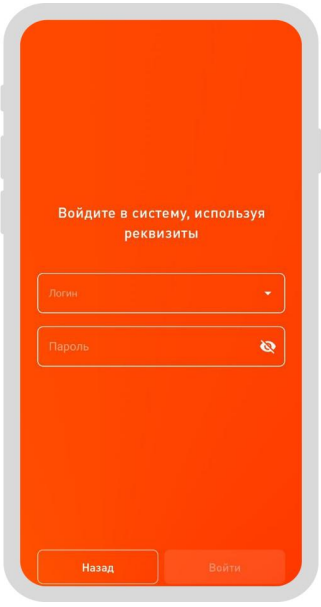
2. При подключении с mTLS приложение «Мобильный терминал» предложит выбрать пользовательский сертификат из доступных на устройстве.

SEC.RU | Короткий путь к информации Скачано с sec.ru



Выбор пользовательского сертификата.

3. Нажмите кнопку «Выбрать». После этого приложение готово к работе.



Вход в систему.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10. Контакты

ООО «Промышленная автоматика – контроль доступа»
Адрес: 603001, Нижний Новгород, ул. Керченская, д. 13, 4 этаж.

Система контроля и управления доступом «Sigur»
Сайт: www.sigur.com
По общим вопросам: info@sigur.com
Техническая поддержка: support@sigur.com
Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93

SEC.RU | Короткий путь к информации
Скачано с sec.ru