НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

МОБИЛЬНЫЙ КЛИЕНТ ANDROID

SAFEMOBILE

Москва

2025

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений 4

1 Введение 5

2 Установка приложения «Монитор» 6

2.1 Поддерживаемые устройства 7

2.2 Установка приложения «Монитор» на корпоративное устройство с Android версии 7.0 и выше для получения полномочий DO 8

2.3 Установка приложения «Монитор» на корпоративное устройство с Android версии 5.0 — 6 для получения полномочий DO 10

2.4 Установка приложения «Монитор» на корпоративное устройство производства Samsung с Android версии 5.0 — 9 для получения полномочий KNOX 11

2.5 Установка приложения «Монитор» на личное устройство с Android версии 7 и выше для получения полномочий ЛРП 14

2.6 Установка приложения «Монитор» на корпоративное устройство с Android версии 11 и выше для получения полномочий КРП 14

3 Применение приложения «Монитор» для подключения МСК к серверу 15

4 Особенности подключения личных устройств 24

5 Особенности работы с контейнером на устройствах Samsung 26

6 Проверка подключения МСК к системе «SafeMobile» 30

7 Сбор логов после установки 31

8 Установка ярлыков приложений 32

9 Просмотр информации о подключении и назначениях на устройство в приложении «Монитор». 35

9.1 Информация о конфигурации серверов 35

9.2 Информация о не корпоративных приложениях, назначенных на устройство 39

9.3 Информация о разрешениях приложения «Монитор» 40

9.4 Информация о назначениях на устройство 41

9.5 Информация об уведомлениях от администратора 43

9.6 Информация о ярлыках приложений 44

10 Допустимое время отклика 45

11 Корпоративные клиентские приложения 46
12 Получение файлов через приложение «Монитор» 50
13 Особенности работы МСК в режиме «киоск» 51
13.1 Настройки устройства в режиме «киоск» 55
13.2 Настройки Wi-Fi 57
13.3 Настройка разблокировки экрана в режиме киоск 61
14 Временная разблокировка устройства 63
14.1 Разблокировка при заблокированном экране 64
14.2 Разблокировка при наличии доступа к приложению «Монитор» 65
14.3 Разблокировка устройства в режиме работы «Киоск» 67
14.4 Разблокировка устройства через приложение набора номера телефона 68
Приложение 1: Установка приложения «Монитор» с использованием технологии NFC 69
Приложение 2: Установка приложения «Монитор» посредством ADB 71
Приложение 3: Возможные проблемы при установке и эксплуатации и способы их решения ... 74

Перечень используемых терминов и сокращений

Таблица 1 — Перечень терминов и сокращений

Сокращение	Полное наименование
AD	Active Directory (служба каталогов)
ADB	Android Debug Bridge (программное обеспечение для отладки, выявления ошибок в приложениях и разблокировки устройств на ОС Android)
DA	Device Administrator
DO	Device Owner
FCM	Служба отправки push-уведомлений (Firebase Cloud Messaging)
NFC	Near field communication (ближняя бесконтактная связь)
NFC метка	Устройство, используемое для передачи информации через NFC на смартфон, планшетный компьютер
QR-код	Quick Response Code (код быстрого отклика)
UEM	Unified Endpoint management (Унифицированное управление конечными устройствами)
АРМ	Автоматизированное рабочее место
ЛРП	Личный рабочий профиль
КРП	Корпоративный рабочий профиль
МСК	Мобильное средство коммуникации (смартфон, планшетный компьютер)
ОС	Операционная система
ПК	Персональный компьютер
Провизионирование	Первоначальная настройка устройства через QR или NFC
ПС	Пользовательское соглашение
РП	Рабочий профиль

1 Введение

Настоящее Руководство предназначено для пользователя, осуществляющего установку клиентского компонента комплексной цифровой мультиплатформы управления мобильными средствами коммуникаций «UEM SafeMobile» (далее по тексту — «UEM SafeMobile» или система), а именно: мобильного клиента МСК на платформе Android версии от 5.0 и выше.

Система «UEM SafeMobile» представляет из себя программный комплекс для управления мобильными устройствами.

Руководство содержит описание установки мобильного клиента SafeMobile и дальнейшее подключение МСК к системе «UEM SafeMobile».

2 Установка приложения «Монитор»

Перед началом работы пользователю необходимо проверить корректность значений даты, времени и часового пояса на МСК. В том случае если эти параметры установлены неверно, следует выключить на МСК автоматическое определение даты и времени, предоставляемое сетью, и осуществить настройку вручную.

Возможны несколько способов установки приложения «Монитор» на устройство. В зависимости от выбранного варианта установки приложение «Монитор» получит соответствующие полномочия для управления устройством. Для управления устройствами в системе SafeMobile приложению «Монитор» необходимо предоставить одно из следующих полномочий:

- DO — используется для корпоративных устройств, как производства Samsung, так и других производителей с Android версии 5.0 и выше.
- KNOX — используется для корпоративных устройств только производства Samsung с Android версии 5.0 — 9.
- ЛРП — используется для личных устройств, как производства Samsung, так и других производителей с Android версии 7 и выше.
- КРП — используется для корпоративных устройств как производства Samsung, так и других производителей с Android версии 11 и выше.

Для дальнейшего подключения устройства к системе «SafeMobile» с одним из вышеуказанных полномочий приложения «Монитор», Администратором системы «SafeMobile» должен предоставить либо QR-код, либо код приглашения, изготовленные с учетом указанных полномочий.

Примечание

Для полноценной работы приложения «Монитор» на устройствах Xiaomi, необходимо наличие FCM-пушсервера, а также указать в настройках Андроида:

- *раздел Параметры разработчика, выключить параметр MIUI Optimization;*
- *раздел Приложения, приложение Монитор, включить Автозапуск;*
- *раздел Приложения, приложение Монитор, выключить Контроль активности.*

ВАЖНО!

Для регистрации МСК в системе на устройстве должно было установлено приложение «Монитор» не ниже версии 11.0, в противно случае регистрация устройства в системе невозможна.

Если устройство подключено с правами DA (Device Administrator), то при попытке пользователя снять с приложения монитора права DA произойдет сброс устройства к заводским настройкам. Если необходимо отключить устройство от управления, то это необходимо делать из консоли администратора, командой отключения от управления с удалением только корпоративных данных.

2.1 Поддерживаемые устройства

Перед установкой приложения убедитесь, что устройство входит в список поддерживаемых устройств. В противном случае, часть функционала приложения может быть не доступна.

Список поддерживаемых устройств:

https://androidenterprisepartners.withgoogle.com/devices/#

Список устройств, протестированных разработчиком приложения:

https://safe-mobile.ru/product/devices-os/

Примечание

При подключении к системе устройств на Android 15 и выше возможно отсутствие разрешений, связанных с SMS — система может ограничивать их выдачу.
Если эти разрешения не предоставлены, функция автоматического определения номера МСК будет недоступна.

2.2 Установка приложения «Монитор» на корпоративное устройство с Android версии 7.0 и выше для получения полномочий DO

Для установки на МСК приложения **«Монитор»** необходимо выполнить следующие действия:

1. Произвести аппаратный сброс всех параметров и удаление всех данных до заводских настроек (Factory Reset).

> ***Примечание.***
>
> При установке на МСК Samsung приложения «Монитор» таким способом, мобильный клиент SafeMobile получает права Device Owner, поэтому создание KNOX-контейнера на таких устройствах невозможно.

2. После перезагрузки МСК в результате сброса к заводским настройкам шесть раз нажать на приветствие на первоначальном экране (рисунок 1), после чего будет запущен сканер QR-кодов, при помощи которого следует отсканировать QR-код, предоставленный Администратором системы «SafeMobile».

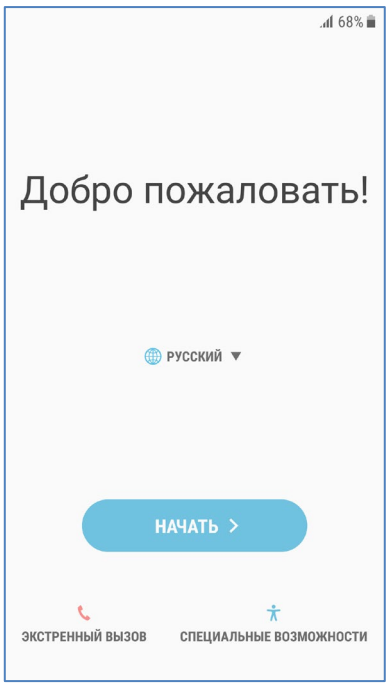


Рисунок 1 — Первоначальный экран МСК

После этого будет выполнена загрузка на МСК приложения **«Монитор».**

После прохождения несложного мастера первоначальной настройки и запроса основных разрешений появится уведомление «Система защищена».

Примечание.

- *Для данного способа подключения необходимо подключение либо Wi-Fi с выходом в интернет, либо выход в интернет через SIM;*
- *Если сканер QR-кода не появляется, необходимо воспользоваться способом подключения из п. 2.3.*

2.3 Установка приложения «Монитор» на корпоративное устройство с Android версии 5.0 — 6 для получения полномочий DO

На устройстве данного типа возможна установка приложения «Монитор» с использованием технологии NFC (при его наличии), которая приведена в приложении 1, или посредством ADB, которая приведена в приложении 2.

После чего, в приложении «Монитор» необходимо пройти процедуру подключения к серверу в соответствии с разделом 3.

Эти же способы могут быть использованы для установки приложения Монитор на устройства с урезанной прошивкой Android версии 7-11, в которых вендор вырезал возможность инициализации через QR-код после сброса на заводские настройки.

Примечание

Возможность подобного варианта установки приложения «Монитор» зависит от вендора устройства. Не во всех прошивках Android 5.0 — 6 вендором реализована поддержка данного варианта установки.

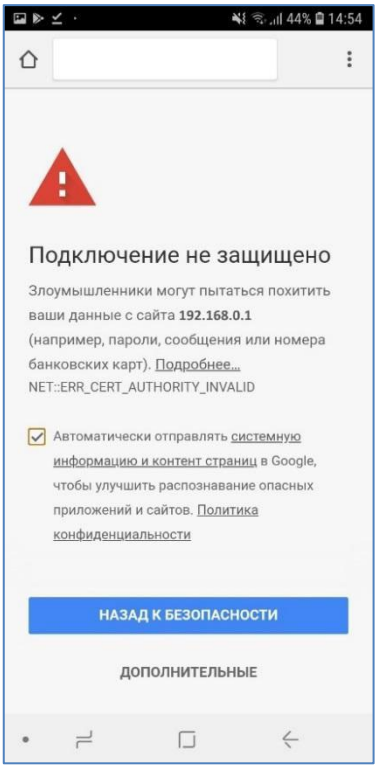
2.4 Установка приложения «Монитор» на корпоративное устройство производства Samsung с Android версии 5.0 — 9 для получения полномочий KNOX

Для установки на МСК приложения **«Монитор»** необходимо выполнить следующие действия:

1. Открыть браузер и ввести адрес портала регистрации, полученный от администратора системы. В том случае если портал недоступен, необходимо проверить наличие доступа в сеть Интернет.

Если доступ к порталу осуществляется с использованием сертификатов, выданных организацией, не входящей в состав доверенных, на МСК возможно появление сообщения **«Подключение не защищено»** (рисунок 2).

а)



б)

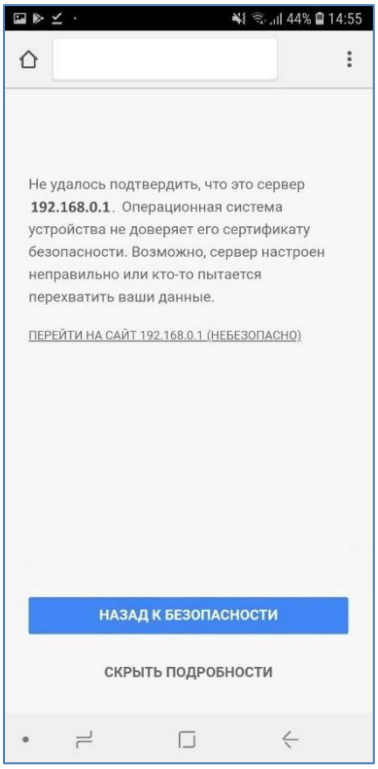


Рисунок 2а), 2б) — Сообщения о незащищенном соединении

При нажатии **«НАЗАД К БЕЗОПАСНОСТИ»** будет выполнен возврат к предыдущей странице интернет-браузера.

При нажатии **«ДОПОЛНИТЕЛЬНЫЕ»** отобразится окно браузера с дополнительными сведениями о сертификате в соответствии с рисунком 2а).

Для продолжения работы необходимо нажать на ссылку **«ПЕРЕЙТИ НА САЙТ…(НЕБЕЗОПАСНО)»** (рисунок 2б), в результате чего отобразится окно портала регистрации (рисунок 3).

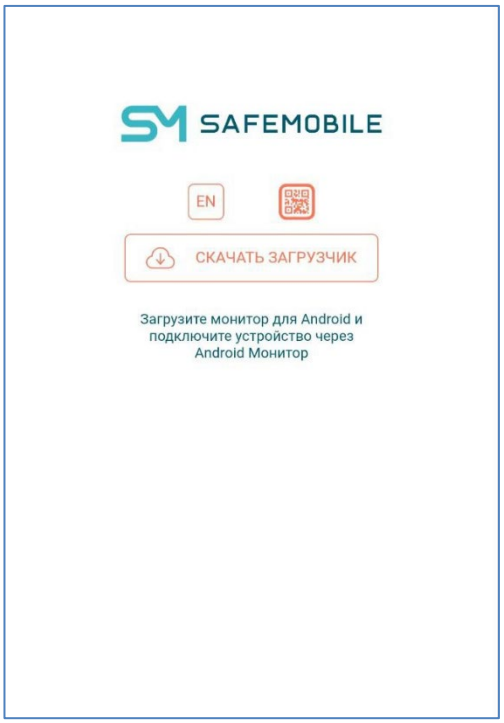


Рисунок 3 — Окно портала регистрации

При помощи кнопки RU осуществляется переключение языка интерфейса с русского на английский. Для обратного переключения предназначена кнопка EN.

2. Загрузить файл для установки приложения **«Монитор»**. Для этого следует нажать **«СКАЧАТЬ МОНИТОР»** (рисунок 3), дать согласие на загрузку файла **«monitor.apk»** и разрешение на доступ браузера к фото, мультимедиа и файлам на устройстве.

Примечание

- *Некоторые браузеры скачивают файл установки некорректно. Вместо файла «monitor.apk» скачивается файл «monitor.bin». В этом случает необходимо переименовать файл в «monitor.apk» и продолжить установку;*
- *Файл «monitor.apk», полученный от поставщика системы, возможно также поместить в корневой каталог МСК посредством USB-кабеля или сети Wi-Fi.*

3. Запустить файл **«monitor.apk»** и установить приложение **«Монитор»**.

По завершении установки в интерфейсе МСК отобразится значок приложения **«Монитор»** в соответствии с рисунком 4.

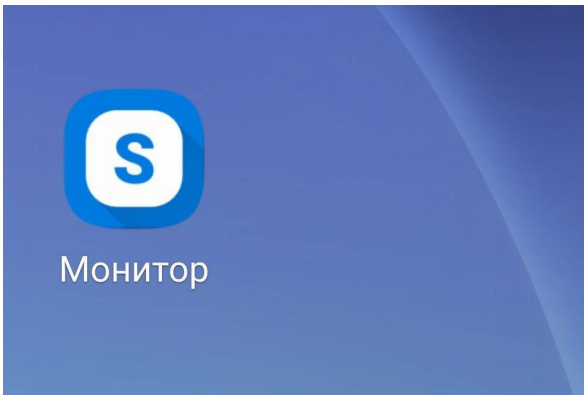


Рисунок 4 − Значок приложения «Монитор» в интерфейсе устройства

После чего, в приложении «Монитор» необходимо пройти процедуру подключения к серверу в соответствии с разделом 3.

2.5 Установка приложения «Монитор» на личное устройство с Android версии 7 и выше для получения полномочий ЛРП

Для установки приложения **«Монитор»** на личное МСК необходимо пройти процедуру как на устройствах производства Samsung с Android версии 5.0 — 9 в соответствии с подразделом 2.4 данной инструкции.

2.6 Установка приложения «Монитор» на корпоративное устройство с Android версии 11 и выше для получения полномочий КРП

Для установки приложения «Монитор» на корпоративное устройство с получением полномочий КРП необходимо пройти процедуру как на устройствах версии 7.0 и выше для получения полномочий DO в соответствии с подразделом 2.2 данной инструкции.

3 Применение приложения «Монитор» для подключения МСК к серверу

При использовании приложения «Монитор» для подключения МСК необходимо выполнить следующие действия:

1. Зарегистрировать МСК в системе «SafeMobile» посредством введения учетных данных в окне приложения «Монитор».

Пользователю предоставляется четыре варианта подключения, в зависимости от конфигурации сервера и данных, предоставленных Администратором. Вариант 4, Подключение по идентификаторам устройства становится доступен пользователю при наличии у Монитора достаточного уровня прав (Device Owner или KNOX).

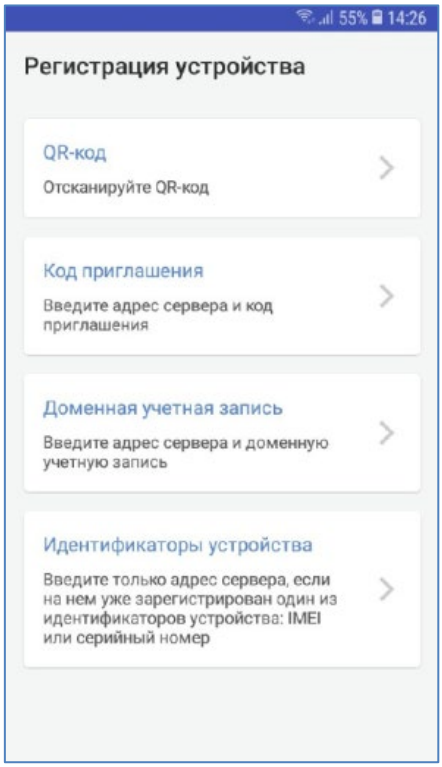


Рисунок 5 — Варианты подключения

- Вариант 1:

Авторизация через сканирование QR-кода, предоставленного Администратором (рисунок 6).

Рисунок 6 — Сообщение содержащие QR-код и код приглашения

- Вариант 2:

Авторизация путем введения кода приглашения и адреса сервера (рисунок 7), полученных у Администратора системы «SafeMobile».

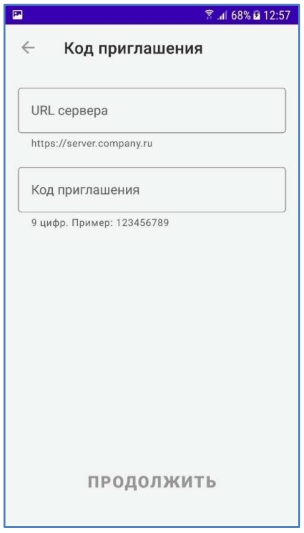


Рисунок 7 — Ввод учетных данных через код приглашения

- Вариант 3:

Авторизация путем введения данных пользователя в формате «username@domain», используя службу каталогов Microsoft Active Directory (рисунок 8).

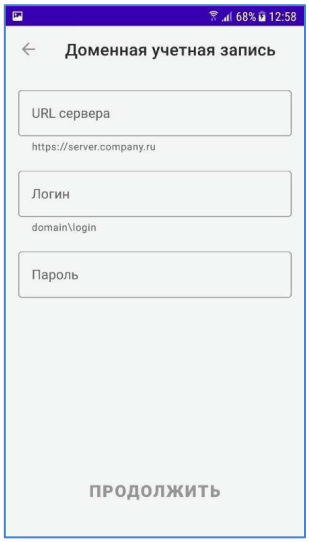


Рисунок 8 — Ввод учетных данных через AD

- Вариант 4:

Устройство, IMEI которого или серийный номер занесены в БД SafeMobile (ранее подключалось, или зарегистрировано Администратором) можно подключить к серверу, введя только его адрес (рисунок 9).

Рисунок 9 — Подключение через идентификаторы устройства устройства

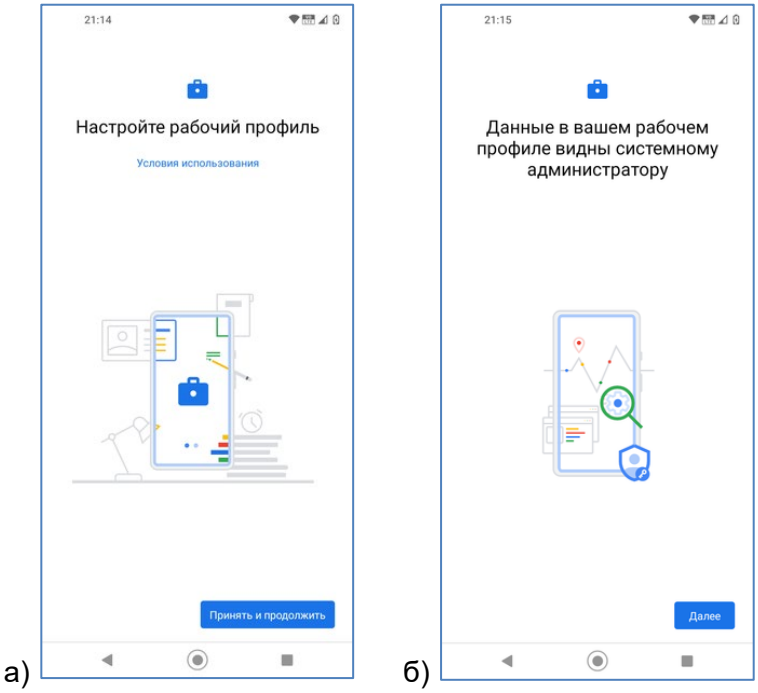
2. Если Администратором задано **«Пользовательское соглашение»**, то на МСК отобразится окно с текстом пользовательского соглашения.

Для продолжения процедуры подключения следует согласиться с условиями, нажав **«ПРИНЯТЬ»**. При нажатии **«ОТКЛОНИТЬ»** будет осуществлен возврат к окну ввода учетных данных, и процедура подключения будет прекращена.

3. Если подключается корпоративное устройство, необходимо дать приложению Монитор права администратора устройства, нажав **«ВКЛЮЧИТЬ»** (рисунок 10).

Рисунок 10 — Окно приложения «Монитор»

4. Если подключается личное устройство, произойдет создание рабочего профиля и копирование в него приложения Монитор, пользователю предлагается несложный мастер настройки, в котором достаточно нажать кнопки «Принять и продолжить», а затем «Далее» (рисунок 11).



а) б)

Рисунок 11 (а,б) — Мастер создания рабочего профиля

5. Если подключается корпоративное устройство Samsung, на экране МСК отобразится окно с политикой конфиденциальности (рисунок 12).

Рисунок 12 — Политика конфиденциальности

В данном окне пользователю следует ознакомиться и подтвердить согласие с предложенными условиями.

6. На последнем этапе подключения пользователю необходимо выдать приложению Монитор разрешение на работу в фоновом режиме (рисунок 13).

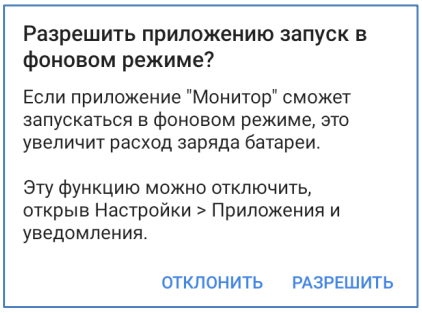


Рисунок 13 — Разрешение на работу в фоновом режиме

При успешном подключении в интерфейсе МСК отобразится уведомление **«Система защищена»** (рисунок 14) и значок в верхней части экрана (рисунок 15).

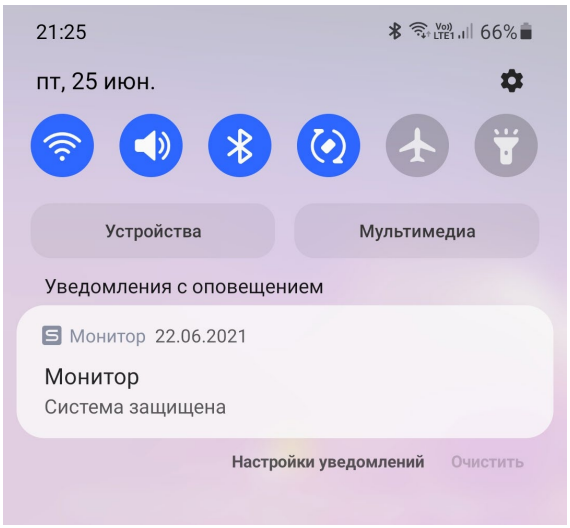


Рисунок 14 – Сообщение на МСК

Рисунок 15 – Интерфейс МСК со значком приложения «Монитор»

7. После подключения к МСК будут применены профили, настроенные Администратором системы «SafeMobile».

После применения профилей, если Администратором задан сбор местоположений корпоративного МСК, в интерфейсе отобразится уведомление (рисунок 16) и запрос о предоставлении приложению «Монитор» доступа к геопозиции устройства посредством службы геолокации Google (рисунок 17), в котором следует нажать «ОК».

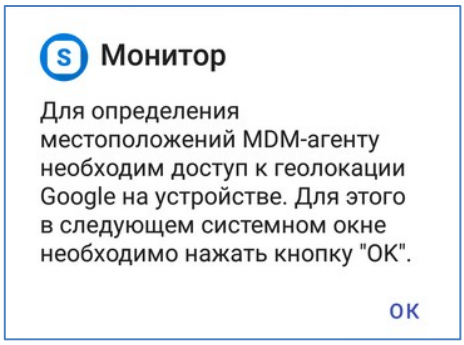


Рисунок 16 — Уведомление о предоставлении доступа к геолокации

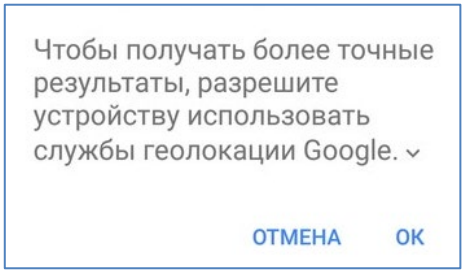


Рисунок 17 — Запрос на предоставление доступа к геолокации

4 Особенности подключения личных устройств

При подключении к SafeMobile личного МСК на устройстве создается рабочий профиль. Это условная выделенная область на устройстве, в которой работают корпоративные приложения, хранятся корпоративные данные и к которой могут быть применены политики ограничений. Таким образом, само устройство остается личным и установленное на нем приложение Монитор скрыто и не может выполнять никаких функций. А в рабочем профиле работает копия приложения Монитор (рисунок 18), которая взаимодействует с сервером и выполняет функции управления.

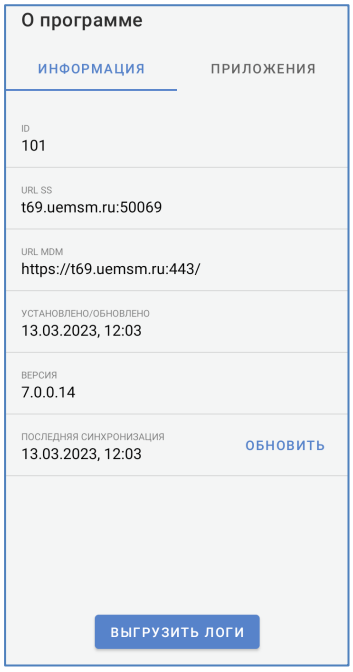
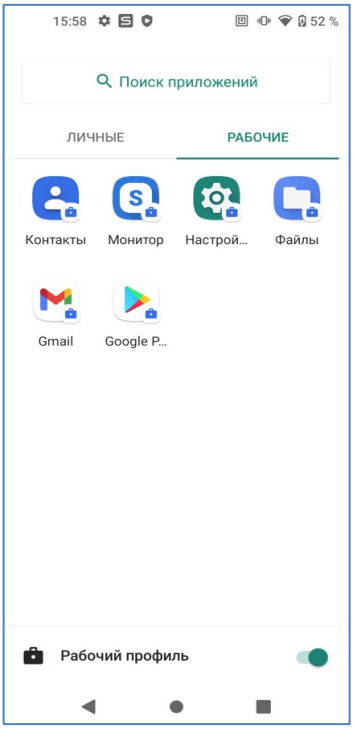


Рисунок 18 –Копия приложения Монитор на устройстве в рабочем профиле

В зависимости от производителя устройства возможны два варианта размещения иконок приложений в рабочем профиле. В лаунчере могут быть выделены отдельные закладки «Личные»/»Рабочие» (рисунок 19а), либо все приложения отображаются единым блоком, а приложения из профиля выделяются только небольшим значком портфеля в нижнем правом углу иконки (рисунок 19б).

а) 

б)

Рисунок 19 (а,б) — Два варианта размещения приложений рабочего профиля

На устройствах требуется подтверждение пользователя при установке и удалении корпоративных и некорпоративных приложений, поэтому в Мониторе есть вкладка со списком приложений.

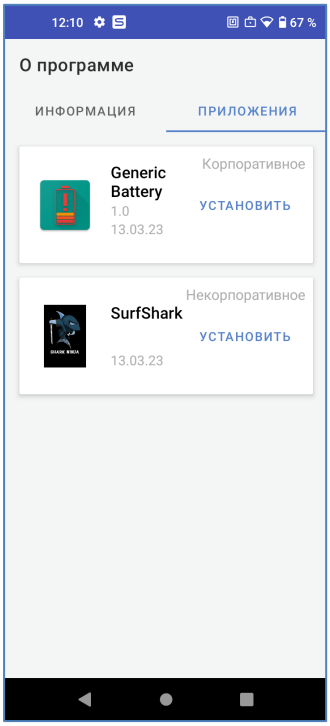


Рисунок 20 — Вкладка в Мониторе со списком приложений

5 Особенности работы с контейнером на устройствах Samsung

Если в АРМ Администратора задан профиль с созданием Knox-контейнера на устройстве производства компании Samsung, то в интерфейсе МСК отобразится уведомление об активации Knox (рисунок 21) либо, при возникновении ошибки в процессе активации, соответствующее сообщение.

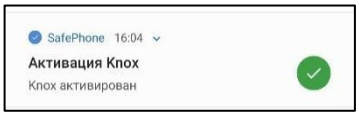


Рисунок 21 — Уведомление об активации Knox

В случае возникновения ошибки следует проверить наличие сети Интернет для доступа к серверам Samsung с целью активации сервиса.

После успешной активации ключа Knox отобразится запрос на создание контейнера Knox (рисунок 22) и окно создания рабочей области с условиями от производителя устройства (рисунок 23).

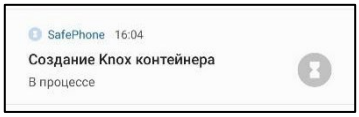


Рисунок 22 — Запрос на создание контейнера

Рисунок 23 — Условия использования Knox

Функция управления контейнером на МСК позволяет изолировать друг от друга персональные и корпоративные приложения и их данные на устройстве, управление контейнером осуществляется с использованием Samsung Knox. Для создания на МСК контейнера Knox следует согласиться с предложенными условиями, нажав на кнопку **«ПРИНЯТЬ»**. После этого запустится процесс создания контейнера с рабочей областью Workspace. Затем требуется задать тип блокировки Knox: пароль / PIN / узор.

Если контейнер Knox на МСК не требуется, в окне создания контейнера следует нажать **«ОТМЕНА»**.

Примечание

Если на МСК был установлен Knox warranty bit в результате проведения незаводской прошивки, то создание контейнера на устройстве невозможно.
При установке на МСК мобильного клиента SafeMobile в качестве Device Owner (с использованием технологии NFC или посредством ADB) создание контейнера на устройстве невозможно.

По завершении процедуры создания контейнера в интерфейсе МСК отобразится иконка приложения **«Workspace»** (рисунок 24) при ОС версий 8 − 9 и сообщение SafeMobile об успешном создании контейнера (рисунок 25). При ОС версии 7 отобразится иконка приложения **»Knox»** .

В случае возникновения ошибки при создании контейнера Knox в интерфейсе МСК отобразится значок и сообщение с информацией о причинах, по которым не удалось создать контейнер.

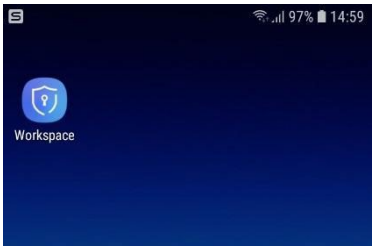


Рисунок 24 — Значок приложения «Workspace» в интерфейсе МСК

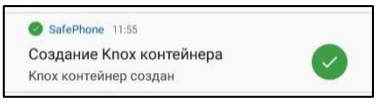


Рисунок 25 — Сообщение о создании контейнера

В интерфейсе МСК приложения, установленные в контейнер и вне его, будут отличаться. На иконках приложений, установленных в контейнер, отображаются специальные индикаторы в соответствии с рисунком 26.

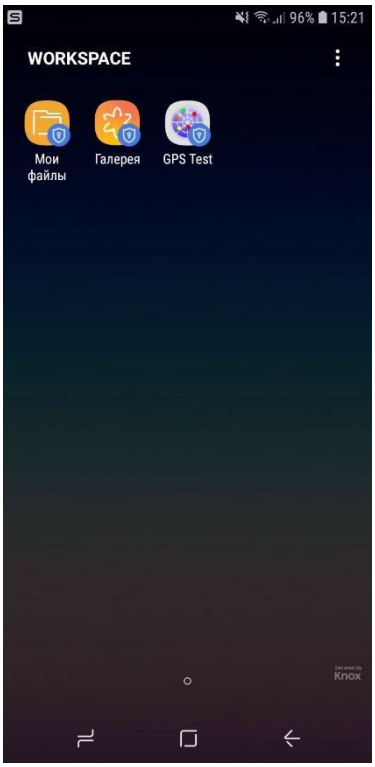
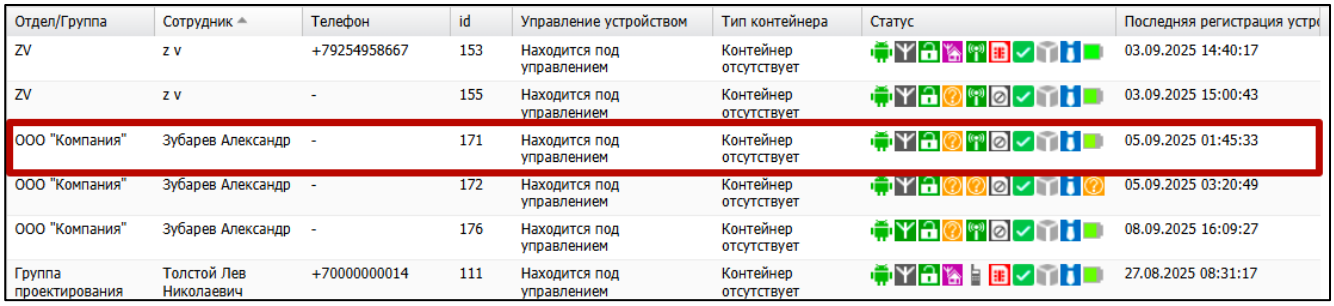


Рисунок 26 — Окно приложения «Workspace»

Специальные индикаторы будут также воспроизводиться на уведомлениях и рабочих окнах приложений в контейнере. Для того, чтобы запустить приложение или просмотреть уведомление необходимо ввести пароль Knox, заданный при создании контейнера.

6 Проверка подключения МСК к системе «SafeMobile»

При успешном подключении МСК в АРМе Администратора в столбце **«Статус»** главной таблицы для абонента МСК отобразятся значки **«В сети»** и **«Находится под управлением»** в соответствии с рисунком 27.



Отдел/Группа	Сотрудник	Телефон	id	Управление устройством	Тип контейнера	Статус	Последняя регистрация устр
ZV	z v	+79254958667	153	Находится под управлением	Контейнер отсутствует		03.09.2025 14:40:17
ZV	z v	-	155	Находится под управлением	Контейнер отсутствует		03.09.2025 15:00:43
ООО "Компания"	Зубарев Александр	-	171	Находится под управлением	Контейнер отсутствует		05.09.2025 01:45:33
ООО "Компания"	Зубарев Александр	-	172	Находится под управлением	Контейнер отсутствует		05.09.2025 03:20:49
ООО "Компания"	Зубарев Александр	-	176	Находится под управлением	Контейнер отсутствует		08.09.2025 16:09:27
Группа проектирования	Толстой Лев Николаевич	+70000000014	111	Находится под управлением	Контейнер отсутствует		27.08.2025 08:31:17

Рисунок 27 – Запись о МСК сотрудника в главной таблице АРМ Администратора

В главной таблице АРМ Администратора в столбце **«Статус»**:

- для личных устройств отобразится значок (рисунок 27), а для корпоративных – значок ;
- при наличии контейнера на МСК отобразится значок «Samsung Knox» (рисунок 27), а при отсутствии контейнера – значок «Контейнер отсутствует»;
- при наличии профиля на МСК отобразиться значок »Рабочий профиль Android».

Для того чтобы на МСК, после подключения к системе «SafeMobile», имелась возможность установки публичных приложений, сотруднику необходимо аутентифицироваться в магазине публичных приложений Google Play.

7 Сбор логов после установки

Приложение «Монитор» позволяет выгрузить логи разработчика для анализа и исправления ошибок. Чтобы выгрузить логи при первичной настройке необходимо выполнить следующие действия:

1. На логотипе нажать 5 раз, после чего устройство откроет рабочий экран;

Рисунок 28 — логотип приложения

2. Зайти в «Монитор» и нажать кнопку «⋮»;

3. Выбрать опцию меню «Выгрузить архив логов», после чего в папку «download» будет выгружен архив с логами;

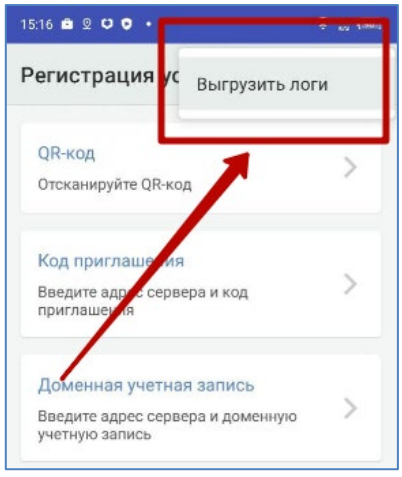


Рисунок 29 — кнопка выгрузки логов

8 Установка ярлыков приложений

Если в АРМ Администратора задан профиль “Ярлык рабочего стола Android”, то в интерфейсе МСК отобразиться уведомление “Добавление ярлыка” (рисунок 30).

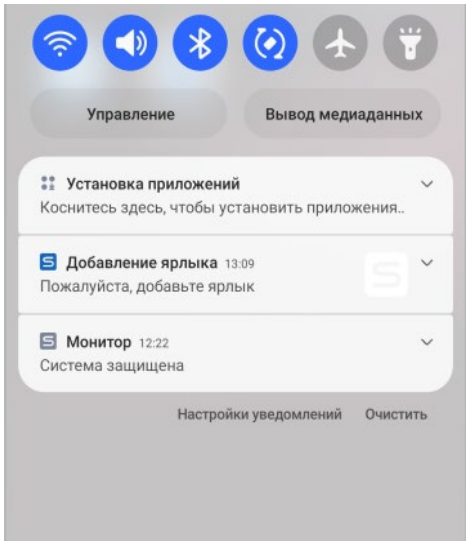


Рисунок 30 — Уведомление о добавлении ярлыка

Для добавления ярлыка на рабочий стол необходимо нажать на уведомление, далее на МСК появится окно подтверждения размещения ярлыка на рабочем столе (рисунок 29). После подтверждения появится уведомление об успешном добавлении ярлыка, сам ярлык будет расположен на главном экране (рисунок 31). Все ярлыки будут выделяться логотипом SafeMobile .

Рисунок 31 — Окно подтверждения добавления ярлыка

Рисунок 32 — Уведомление и ярлык рабочего стола

Если в АРМ Администратора снят ранее назначенный профиль “Ярлык рабочего стола Android”, то в интерфейсе МСК ярлык потускнеет, став черно-белым, при попытке нажатия по нему будет выдаваться уведомление (рисунок 33).

Рисунок 33 — Выключенный ярлык рабочего стола

Отключенный от управления ярлык можно удалить с МСК посредством выделения ярлыка (зажатием) и удалением его с рабочего стола (рисунок 34).

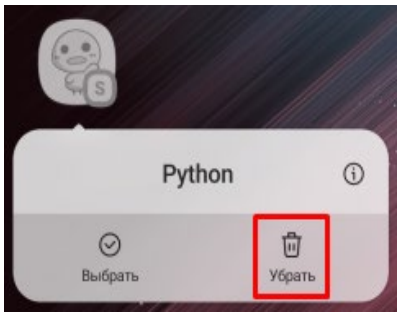


Рисунок 34 — Удаление ярлыка с МСК

9 Просмотр информации о подключении и назначениях на устройство в приложении «Монитор».

9.1 Информация о конфигурации серверов

Информацию о конфигурации серверов можно получить в разделе «Настройки — О программе», в котором отображаются следующие данные (рисунок 35):

- ID (номер комплекта)
- Список серверов, раздающих сертификаты и файлы (FDS). Каждая строка списка состоит из:
  - Название сервера, раздающего сертификат или файлы;
  - URL сервера;
  - Индикатор качества подключения:
    - Зеленый — есть соединение, данные передаются;
    - Желтый — сервер доступен, но нельзя передать данные из-за проблем с сертификатами (SslHandshake);
    - Красный — сервер недоступен: нет сети, роута и т.д.
- Сервер выдающий MTLS сертификат — (актуален/не актуален);
- Дата установки и обновления приложения;
- Версия приложения;
- Информация о последней принудительной синхронизации сертификатов;
  - Кнопка принудительной синхронизации — при нажатии запускается процесс обновления сертификатов;
- Кнопка «выгрузить логи» (см. раздел 7)

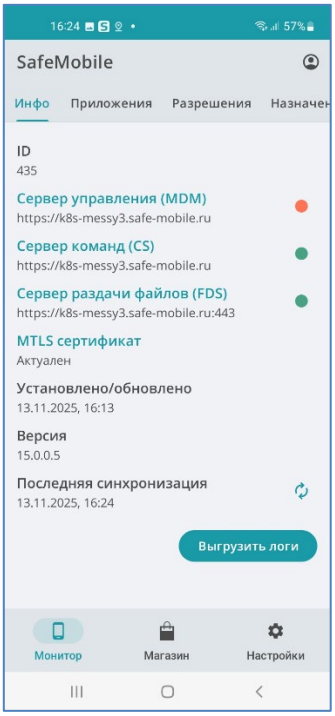


Рисунок 35 — Список подключений к серверам сертификатов и раздачи файлов

Для просмотра подробной информации о каждом подключении следует нажать на название интересующего сервера, после чего откроется экран с подробной информацией (рисунок 36). Экран описания информации о подключении к серверу содержит:

- URL сервера;
- Флаг Certificate pinning;
- Список сертификатов, в котором каждая строка списка содержит:
  - Серверный сертификат;
  - Субъект.

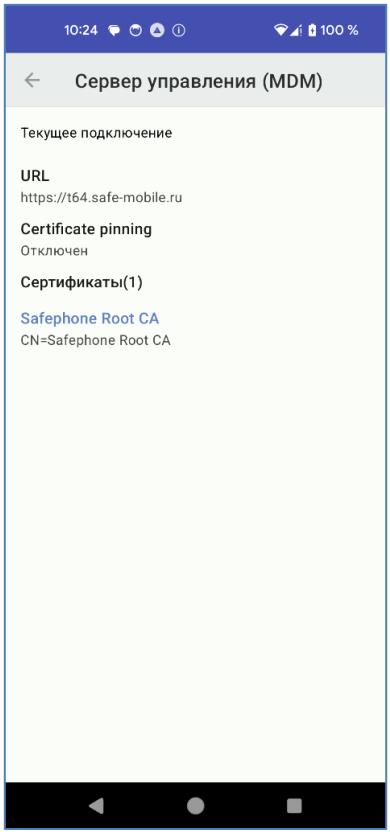


Рисунок 36 — Информация о подключении к серверу сертификатов

Для просмотра подробной информации о сертификате следует нажать на название сертификата, после чего откроется экран с соответствующей информацией (рисунок 37), который состоит из:

- Отпечаток сертификата.
- Субъект.
- Версия.
- Серийный номер.
- Период действия, не ранее.
- Период действия, не позднее.
- Издатель.

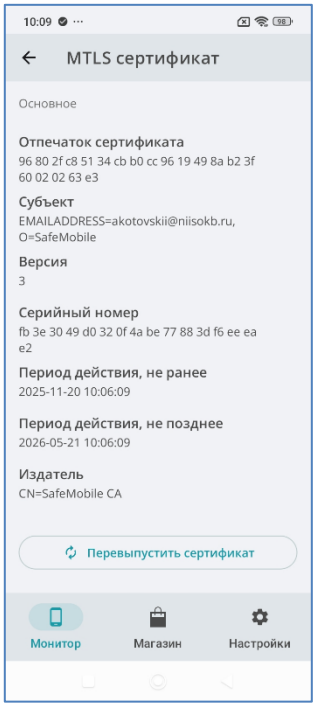


Рисунок 37 — Информация о полученном сертификате

При просмотре данных MTLS сертификата пользователь может запросить перевыпуск сертификата. Для этого следует нажать кнопку «Перевыпустить сертификат» (рисунок 38) , после чего сертификат будет обновлен.

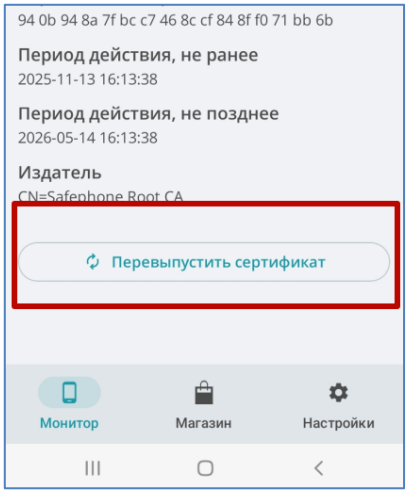


Рисунок 38 — Кнопка перевыпуска сертификата

9.2 Информация о не корпоративных приложениях, назначенных на устройство

Информацию о некорпоративных приложений требующих установки можно получить в разделе «Настройки — Приложения», в котором отображаются следующие данные по каждому приложению (рисунок 39):

- Наименование приложения,
- Дата назначения на устройство,
- Кнопка «Установить» — при нажатии открывается страница загрузки приложения из публичного магазина.

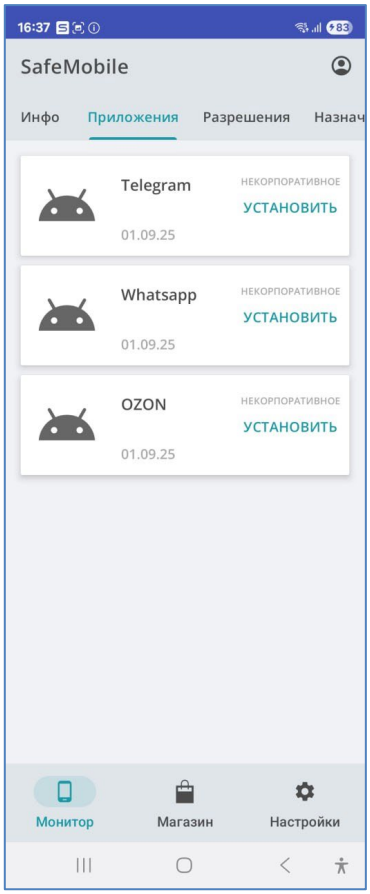


Рисунок 39 — Приложения, установленные на устройство системой

9.3 Информация о разрешениях приложения «Монитор»

Информацию о **не выданных** разрешениях приложения «Монитор» можно получить в разделе «Настройки — Разрешения» (рисунок 40). При клике на запись о разрешении происходит переход к настройкам выдачи разрешения.

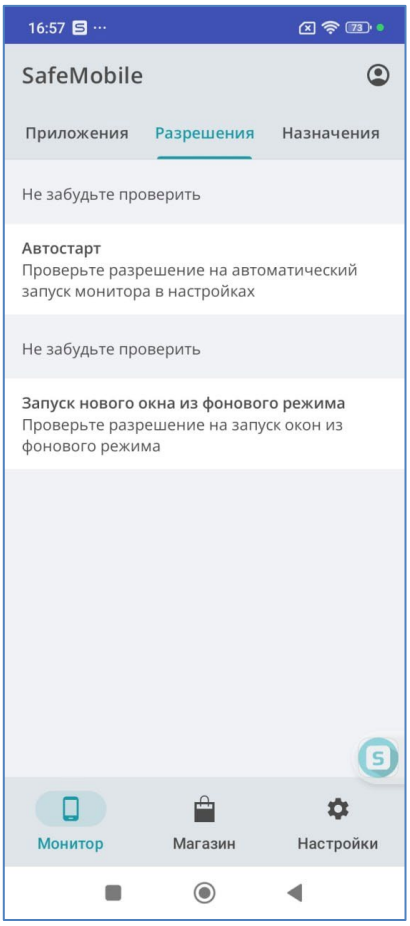


Рисунок 40 — Не выданные разрешения для «Монитора»

9.4 Информация о назначениях на устройство

Информацию о сущностях, назначенных на устройство можно получить в разделе «Настройки — Назначения» (рисунок 41), а именно:

- приложения,
- конфигурации,
- профили:
  - информация о профиле,
  - клиентские и серверные сертификаты для профилей имеющих политики с сертификатами (опционально).

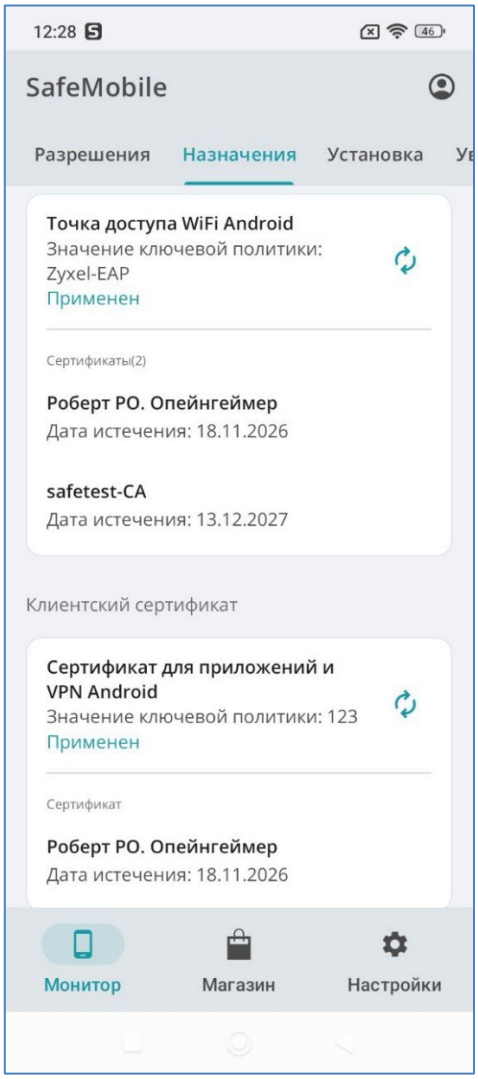


Рисунок 41 — Раздел «Назначения»

Раздел содержит данные о сущностях:

- Приложения:
  - Содержит список приложений с информацией:
    - Корпоративное/Некорпоративное.
    - Наименование приложения.
    - Наименование правила.
    - Применено/Неприменено.
- Конфигурации.
  - Наименование приложения.
  - Наименование конфигурации.
  - Применено/Неприменено.
- Профили.
  - Тип профиля.
  - Название ключевой политики.
  - Значение ключевой политики.
  - Наименование профиля — для раздельных профилей или список наименований профилей — для совместных профилей;
  - Применено/Неприменено;
  - Информация о сертификатах — при клике открывается экран с данными сертификата (аналогичный экрану информации о сертификате во вкладке «Инфо»);
  - Кнопка «Переустановить профиль».

Примечание
Отображение кнопки «Переустановить профиль» управляется политиками профиля «Монитора».
При нажатии кнопки выполняются действия аналогичные команде «Переустановка профиля»:

1. *Снимается профиль с устройства.*
2. *Запускается синхронизация.*

9.5 Информация об уведомлениях от администратора

Список уведомлений от администратора содержится в разделе «Настройки — Уведомления» (рисунок 42).

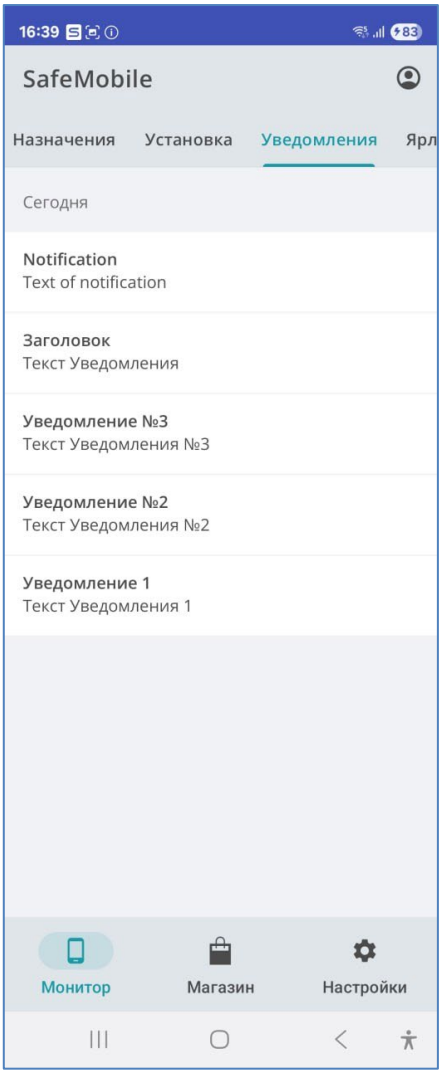


Рисунок 42 — Раздел «Уведомления»

9.6 Информация о ярлыках приложений

Список ярлыков приложений, требующих от сотрудника подтверждения (для размещения на «рабочем столе» устройства) располагается в разделе «Настройки — Ярлыки» (рисунок 43). При клике на кнопку «Добавить» ярлык приложения будет добавлен на «рабочий стол» устройства.

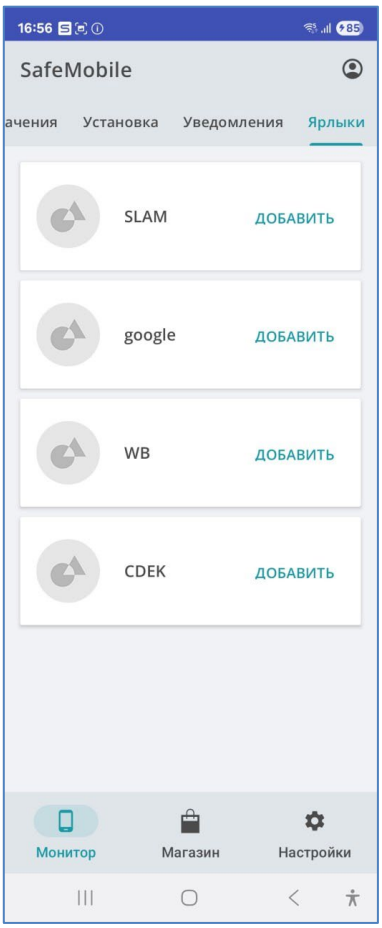


Рисунок 43 — Раздел «Ярлыки»

10 Допустимое время отклика

При наличии связи с сервером мобильный клиент SafeMobile передаст информацию о событии из очереди на сервер в течение одной секунды.

11 Корпоративные клиентские приложения

После установки на МСК клиентской части Администратор при помощи АРМ Администратора может назначить на устройства приложения которые могут быть установлены на устройство как корпоративные т.е. из магазина SafeStore приложения «Монитор».

Информацию о корпоративных приложениях, назначенных на устройство можно получить в разделе «Настройки — Магазин». Раздел магазин «SafeStore» отображает список установленных и доступных для установки корпоративных приложений, совместимых с платформой МСК (рисунок 44).

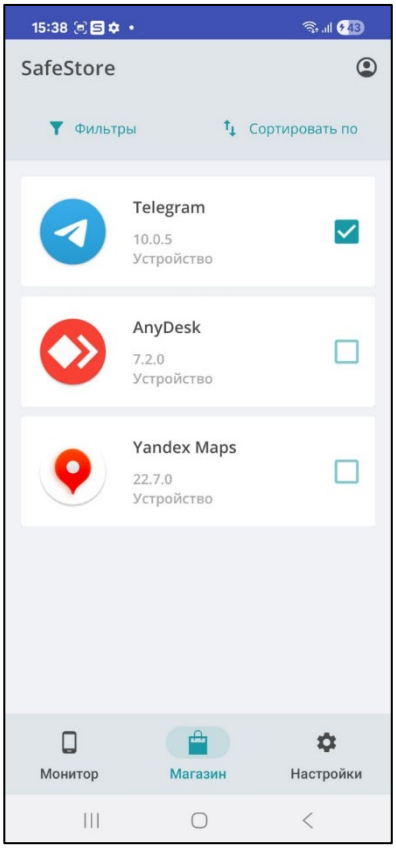


Рисунок 44 — Главное окно приложения «SafeStore»

В строке списка отображается:

- иконка приложения,
- название (если не доступно, то отображается UID),
- версия,
- чекбокс «установлено/неустановлено»,
- статус «недоступности установки» (опционально) — для приложений выбранных ранее пользователем, но не доступных для установки на текущий момент. Если приложение имеет статус «недоступно для установки», то при

отключении чекбокса «установлено» приложение будет удалено из списка.

Список приложений может быть упорядочен следующими способами:

- Сортировка:
  - По алфавиту (A-Z, Z-A),
  - По UID (A-Z, Z-A),
- Фильтрация:
  - Место установки:
    - Любое,
    - Устройство,
    - Контейнер.
  - Состояние:
    - Любое,
    - Назначено,
    - Не назначено,
  - Показать недоступные приложения.

По клику в строке списка доступен просмотр подробных данных по приложению:

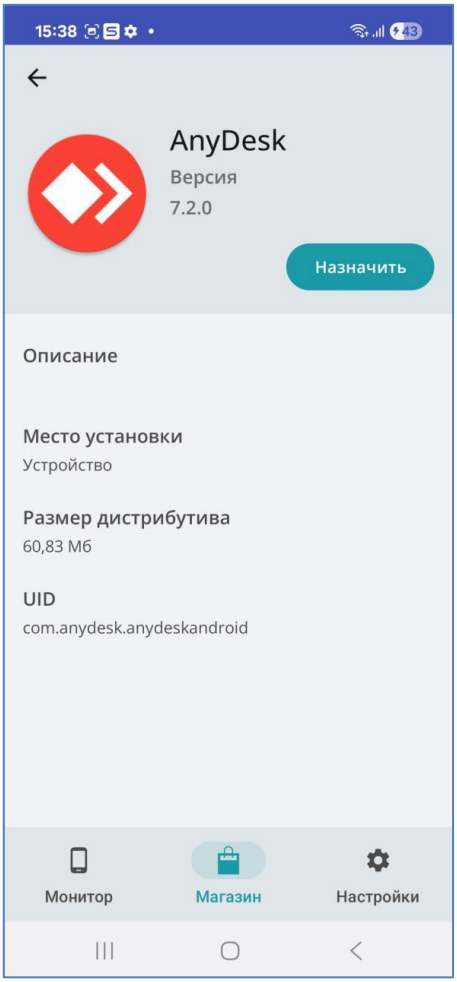


Рисунок 45 — Данные о приложении из SafeStrore

Для установки приложения на МСК следует установить галочку в строке с выбранным приложением. В этом случае приложение установиться на устройстве и на рабочем столе отобразится его иконка.

При снятии галочки приложение будет удалено с МСК, после подтверждения правильности действия в присланном уведомлении.

Обновление версий в списке приложений осуществляется автоматически.

Примечание

Если на устройстве уже установлена публичная версия приложения, а затем на это устройство применяется стратегия ЛРП/КРП, то при установке в контейнер более

старой версии «Монитор» выдаст ошибку (также эта ошибка будет отправлена администратору в список «событий»).
Эту проблему можно решить назначением установленного ранее, публичного приложения в контейнер с помощью ПУП.

12 Получение файлов через приложение «Монитор»

Пользователь МСК имеет возможность получать файлы от администратора «SafeMobile». При выполнении администратором команды по отправке файла пользователь МСК получает уведомление о получении файла (рисунок 46).

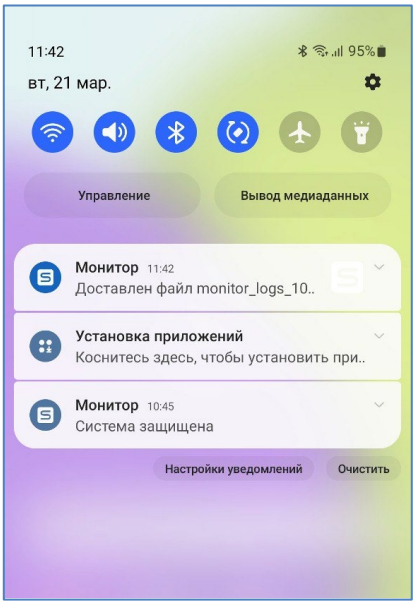


Рисунок 46 — Уведомление о получении файла

Файл будет сохранен в папке «Внутреннее хранилище\Download» (рисунок 47)

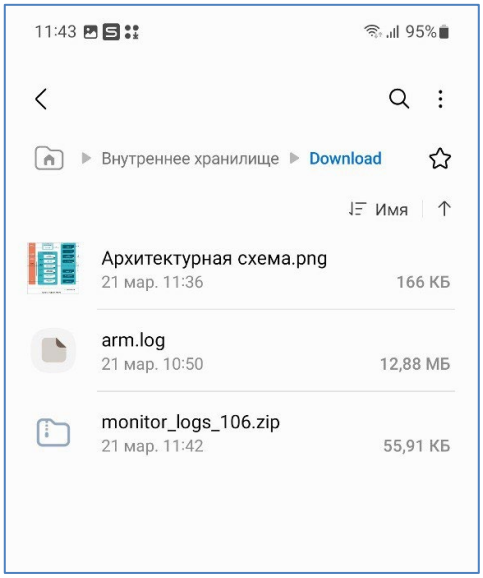


Рисунок 47 — Отображение файла во «Внутреннем хранилище»

13 Особенности работы МСК в режиме «киоск»

Пользователю МСК доступен вход и выход из режима «киоска» (при соответствующих настройках «SafeMobile»).

Примечание для администратора.
Для включения возможности входа и выхода из режима «киоск» необходимо: 1. *Назначить устройству профиль «Режим киоска Android»;* 2. *В настройках профиля «Режим киоска Android» разрешить «Выход из режима киоска по паролю»;* 3. *Установить пароль для выхода из режима «киоск».*

Для корректной работы ярлыков в режиме киоска, добавленных профилем «Ярлык рабочего стола Android» необходимо учитывать следующее:

1. *Если в профиле ярлыка **задан** «UID веб браузера, в котором необходимо открывать URL...», то этот же UID должен быть добавлен в политику «Список UID'ов отображаемых приложений» профиля «Режим киоска Android», примененного к данному устройству.*

2. *Если в профиле ярлыка **не задан** «UID веб-браузера, в котором необходимо открывать URL...», то ярлык будет открываться браузером «по умолчанию». Соответственно UID «браузера по умолчанию» должен быть добавлен в политику «Список UID'ов отображаемых приложений» профиля «Режим киоска Android», примененного к данному устройству.*

В режиме работы «киоск», на управление WiFi и яркостью экрана действуют не только политики «киоска», но и политики профиля ограничений Android, а именно:

- *«Запретить добавлять новые точки доступа WiFi»;*
- *«Запретить изменять состояние WiFi»;*
- *«Запретить изменение настроек точек доступа Wi-Fi»;*
- *«Минимальный уровень безопасности WiFi»;*
- *«Запретить регулировку яркости».*

*На некоторых слабопроизводительных устройствах настройки режима киоска в режиме одного приложения могут отображаться некорректно. Чтобы это исправить, необходимо предоставить разрешение **AlwaysOnDisplay**.*
Выполните следующую команду через ADB:

```
adb shell pm grant ru.niisokb.mcc android.permission.SYSTEM_ALERT_WINDOW
```

Без этого разрешения в киоске с одним приложением будут недоступны:

- *Выход по паролю,*
- *Настройки сети,*
- *Bluetooth,*
- *Настройки дисплея.*

Режим «киоск» автоматически применяется к устройству, после назначения администратором профиля киоска.

Для выхода из режима «киоск» необходимо выполнить следующие действия:

1. Нажать кнопку «Настройки».

2. Нажать кнопку «Выход».
3. Ввести пароль для выхода из киоска, нажать кнопку «Выйти» (рисунок 48), после чего устройство выходит из режима «киоск».
   После 15-ти подряд неудачных попыток ввода пароля выход из режима «Киоск» будет заблокирован.

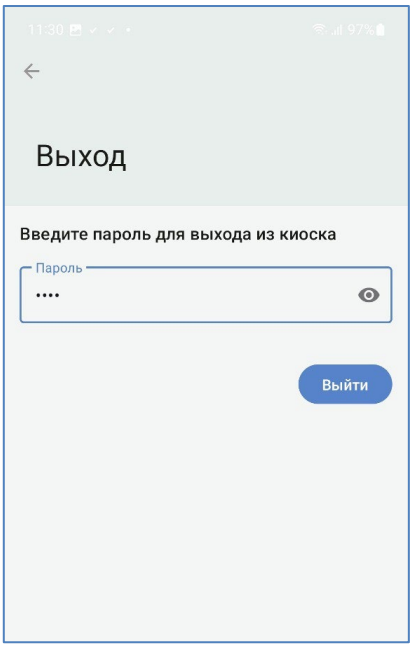


Рисунок 48 — Выход из режима «киоск»

Для возврата в режим «киоск» необходимо выполнить следующие действия:

1. Открыть на МСК приложение «Монитор».
2. На главном экране приложения нажать кнопку «Режим киоска» (рисунок 49). После чего МСК будет работать в режиме «киоск», а на рабочем экране устройства будут отображены доступные для использования приложения.

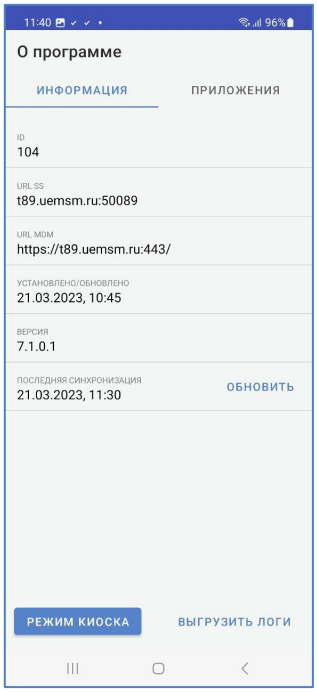


Рисунок 49 — Кнопка входа в режим «киоск»

13.1 Настройки устройства в режиме «киоск»

Для доступа к настройкам устройства в режиме «киоск» необходимо нажать кнопку «Настройки» (рисунок 50), после чего откроется экран управления настройками устройства.

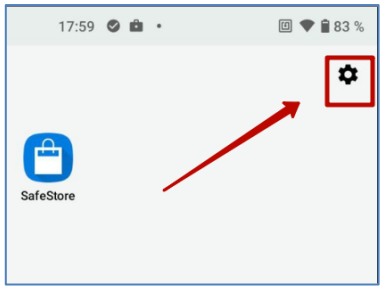


Рисунок 50 — Кнопка «Настройки»

Экран настроек устройства в режиме «киоск» содержит следующие опции (рисунок 51):

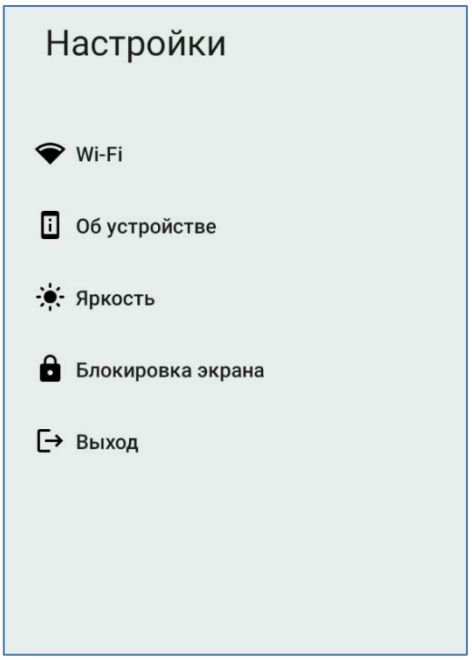


Рисунок 51 — Настройки устройства, в режиме работы «киоск»

- **Wi-Fi —** при нажатии открывается экран настроек Wi-Fi (см.раздел 13.2);
- **Об устройстве —** при нажатии открывается экран с информацией об устройстве (рисунок 52). Экран содержит следующую информацию об устройстве:
  - Модель — название модели устройства;
  - Версия Android — версия ОС Android;
  - IMEI — International Mobile Equipment Identity представляет собой

международный идентификатор мобильного оборудования;

- Серийный номер — заводской, серийный номер устройства;

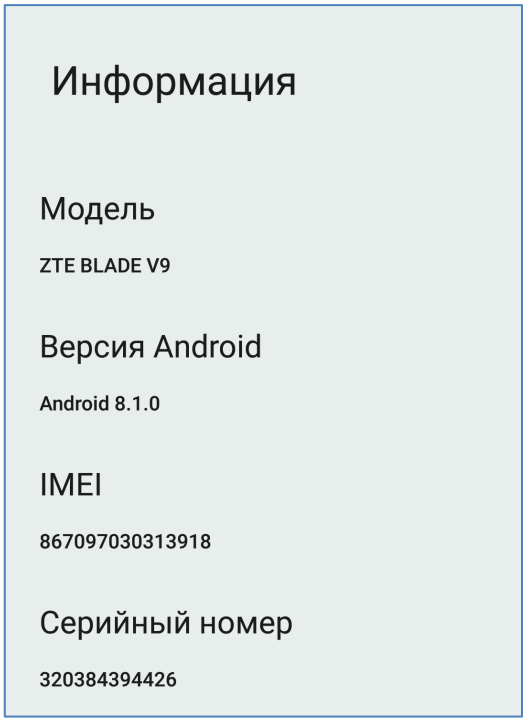
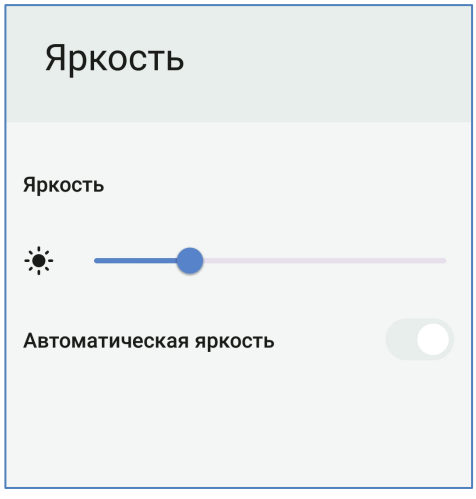


Рисунок 52 — Информация об устройстве

- **Яркость** — при нажатии открывается экран регулировки яркости экрана (рисунок 53а). Данный экран содержит функционал настроек, позволяющих установить яркость вручную или включить режим автоматической настройки яркости (рисунок 53б);

а)



б)

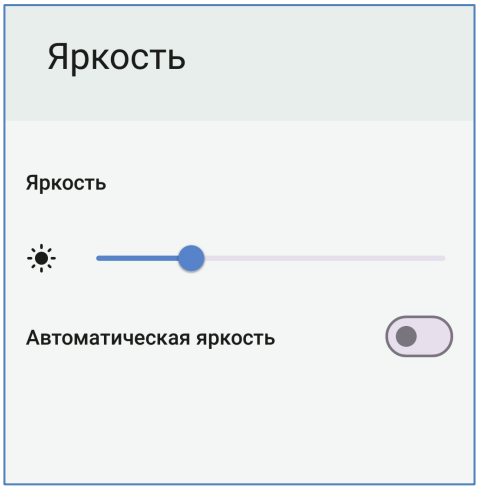


Рисунок 53 (а,б) — А — экран настройки яркости экрана. Б — Режим автоматической настройки яркости включен

- **Кнопка «Выход»** — пари нажатии устройство выходит из режима «киоск».

13.2 Настройки Wi-Fi

Раздел настроек Wi-Fi состоит из:

- Списка беспроводных сетей, найденных устройством (рисунок 54). Каждая строка списка отображает:
  - Качество сигнала беспроводной сети, в виде пиктограммы;
  - Название сети;
  - Индикация подключенной на текущий момент сети;

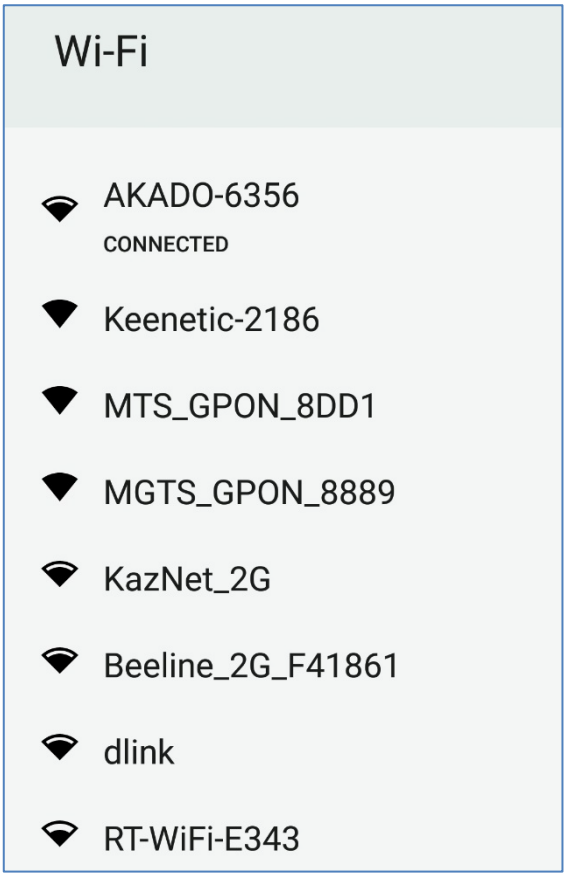


Рисунок 54 — Список беспроводных сетей, обнаруженных устройством

- Списка сохраненных сетей (открывается кнопкой «Сохраненные сети») (рисунок 55). Отображает список сетей, добавленных пользователем;

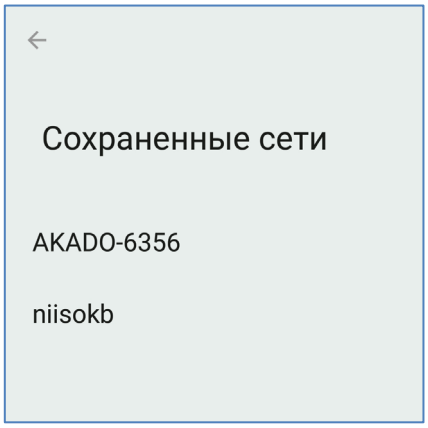
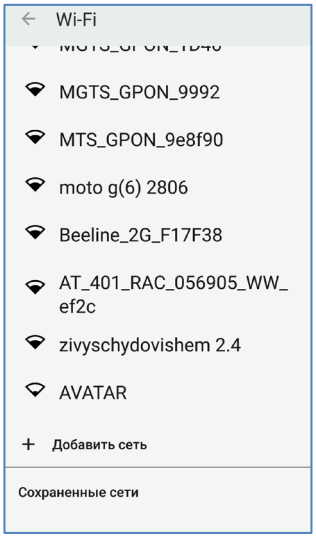


Рисунок 55 — Список беспроводных сетей, добавленных пользователем

- Функционала добавления пользователем новой сети в список сетей.

Чтобы добавить новую сеть необходимо выполнить следующие действия:

1. Нажать кнопку «+ Добавить сеть» в нижней части раздела настроек Wi-Fi (рисунок 56а), после чего откроется экран функционала добавления новой, беспроводной сети (рисунок 56б);

а) 

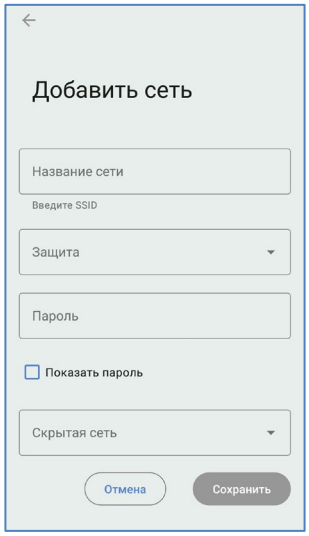
б) 

Рисунок 56 (а,б) А — расположение кнопки «+Добавить сеть». Б — экран функционала «Добавить сеть»

2. Заполнить следующие поля данными:

- **Название сети (SSID)** — название сети, отображаемое при ее обнаружении устройством;
- **Защита** — выбор типа защиты новой сети из выпадающего списка;
    - **Нет (не указывать тип защиты);**
    - **Enhanced open;**
    - **WEP;**
    - **WPA/WPA2-Personal;**
    - **WPA3-Personal;**
- **Пароль** (для просмотра введенного пароля следует включить чек-бокс «Показать пароль»);
- **Скрытая сеть** — выбор типа отображения сети;
    - **Да** — сеть не будет отображаться в списке обнаруженных сетей для устройств;
    - **Нет** — сеть будет отображаться в списке обнаруженных сетей для устройств;

3. Нажать кнопку «Сохранить», после чего новая сеть будет отображаться в списке «Сохраненные сети».

Примечание для администратора

Для того чтобы настройки стали доступны пользователю, необходимо в профиле «Режим киоска Android» политики:

- *Настройка подключения к WiFi;*
- *Информация об устройстве;*
- *Разрешить настройки дисплея.*

13.3 Настройка разблокировки экрана в режиме киоск

В режиме киоск доступно несколько режимов работы разблокировки экрана. Полный список вариантов соответствует системным возможностям модели телефона.

Пример вариантов блокировки экрана:

- Без блокировки,
- Разблокировка экрана через свайп,
- Разблокировка через графический ключ,
- PIN-код,
- Пароль.

Также, в зависимости от модели могут присутствовать варианты разблокировки с помощью отпечатка пальцев и фейсконтроль.

Для выбора режима разблокировки экрана необходимо открыть меню «Настройки» и выбрать «Блокировка экрана» (рисунок 57), после чего будет открыт экран с системными настройками телефона блокировки экрана. Ввести пароль разблокировки экрана (если уже задан), после чего откроется экран выбора способа блокировки экрана (пример на рисунке 58).

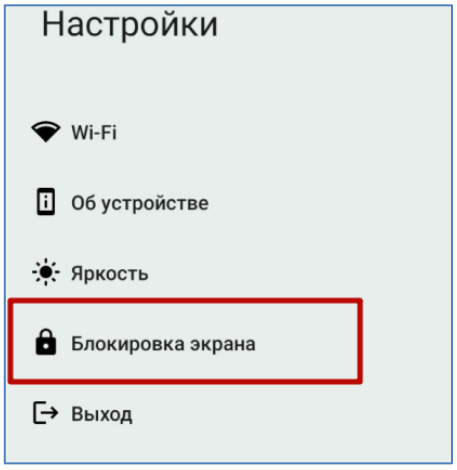


Рисунок 57 — Расположение опции «Блокировка экрана»

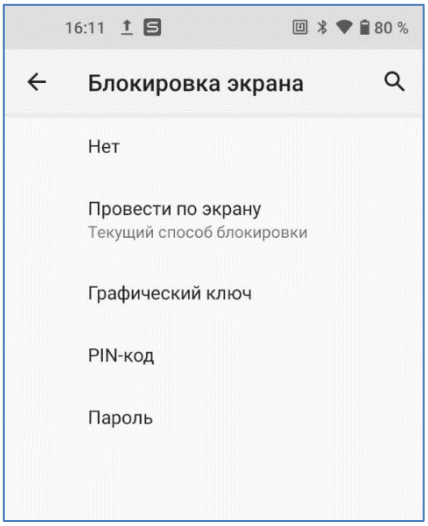


Рисунок 58 — Настройки блокировки экрана

Выбрать один из вариантов блокировки-разблокировки экрана, задать параметры в соответствии с моделью телефона:

- Для использования PIN-кода сделает задать последовательность **цифр** длинной от 4 до 17 знаков;
- Для использования пароля следует задать последовательность **символов** длинной от 4 до 17 знаков;
- Для использования опций «отпечаток пальца» или «фейсконтроль» должен быть задан один из вариантов: пароль, PIN-код или графический ключ (в зависимости от модели телефона).

Примечание

Для смены способа или пароля блокировки экрана (в том числе при блокировке устройства или смене пароля администратором) необходимо:

- *Зайти в «настройки».*
- *Ввести действующий пароль.*
- *Задать необходимый пароль или способ блокировки согласно данной инструкции.*

Если действующий пароль не известен, то необходимо обратиться к администратору за назначением нового пароля на устройство.

14 Временная разблокировка устройства

В результате работы политик и профилей устройство может быть автоматически заблокировано (например, в результате работы команды «Заблокировать устройство») (рисунок 59). Текст на экране блокировки задается администратором и может отличаться от указанного в примере.

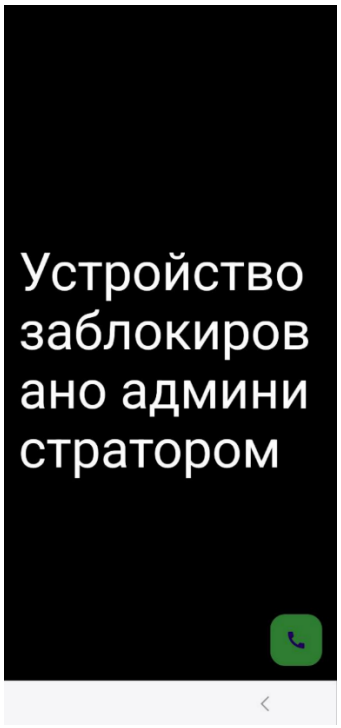


Рисунок 59 — Экран заблокированного системой устройства

14.1 Разблокировка при заблокированном экране

Для временного снятия блокировки устройства необходимо выполнить следующие действия:

1. Получить пароль разблокировки устройства от администратора. Пароль действует в течении 60 минут от времени, заданного Администратором при создании пароля. За это время его необходимо применить на устройстве для разблокировки. Если за это время не пароль не был успешно применен к устройству, то следует запросить новый пароль у администратора.

2. Разблокировать экран устройства.
3. 6 раз нажать на экране (tap), после чего откроется экран ввода пароля разблокировки (рисунок 60).

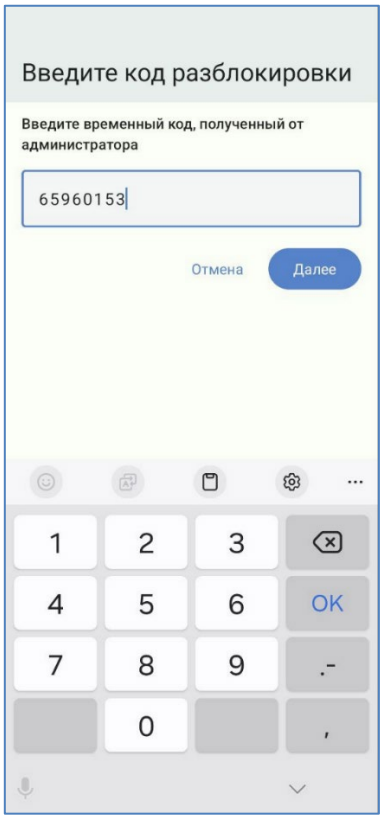


Рисунок 60 — Экран ввода пароля

4. Ввести пароль, полученный от администратора. Для ввода пароля дается 5 попыток (по умолчанию). Если, после 5 попыток пароль не был принят устройством, следует

запросить новый пароль у администратора.

5. Нажать кнопку «Далее», после чего устройство будет разблокировано в течении 30 минут (по умолчанию).
6. Для возврата устройства под управление системой следует перезагрузить устройство или дождаться окончания времени разблокировки.

14.2 Разблокировка при наличии доступа к приложению «Монитор»

Для снятия ограничений (все виды связи, вайп устройства, hard reset и т.п.) наложенных на устройство в результате применения политик необходимо выполнить следующие действия:

1. Получить пароль разблокировки устройства от администратора. Пароль действует в течении 60 минут от времени, заданного Администратором при создании пароля. За это время его необходимо применить на устройстве для разблокировки. Если за это время не пароль не был успешно применен к устройству, то следует запросить новый пароль у администратора.

2. Запустить приложение «Монитор».

3. Открыть раздел «Инфо».

4. 6 раз нажать (tap) на заголовке окна «О программе» (рисунок 61), после чего откроется экран ввода пароля разблокировки (рисунок 62).

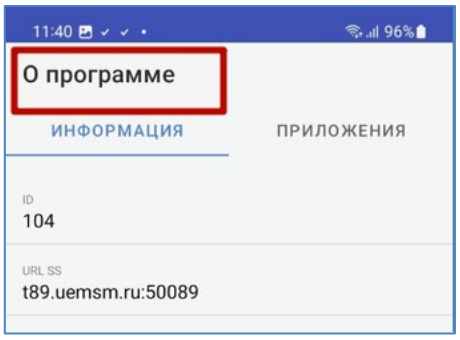


Рисунок 61 — Область вызова экрана разблокировки

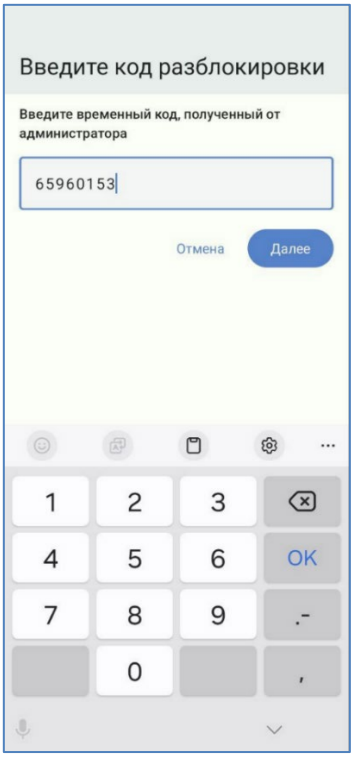


Рисунок 62 — Экран ввода пароля

5. Ввести пароль, полученный от администратора. Для ввода пароля дается 5 попыток (по умолчанию). Если, после 5 попыток пароль не был принят устройством, следует запросить новый пароль у администратора.
6. Нажать кнопку «Далее», после чего устройство будет разблокировано в течении 30 минут (по умолчанию).
7. Для возврата устройства под управление системой следует перезагрузить устройство или дождаться окончания времени разблокировки.

14.3 Разблокировка устройства в режиме работы «Киоск»

Для снятия ограничений (все виды связи, вайп устройства, hard reset и т.п.) наложенных на устройство в результате применения политик необходимо выполнить следующие действия:

1. Получить пароль разблокировки устройства от администратора. Пароль действует в течение 60 минут от времени, заданного Администратором при создании пароля. За это время его необходимо применить на устройстве для разблокировки. Если за это время пароль не был успешно применен к устройству, то следует запросить новый пароль у администратора.

2. Разблокировать экран устройства;

3. В любом свободном месте экрана 6 раз нажать (tap), после чего откроется экран ввода пароля разблокировки;

4. Далее шаги аналогичны действиям, описанным в разделе 14.2, начиная с пункта 5.

14.4 Разблокировка устройства через приложение набора номера телефона

При доступном приложении ввода номера телефона возможен вызов окна разблокировки через ввод secret кода *#*#240506#*#*. Для разблокировки этим способом необходимо выполнить следующие действия:

1. Получить пароль разблокировки устройства от администратора. Пароль действует в течение 60 минут от времени, заданного Администратором при создании пароля. За это время его необходимо применить на устройстве для разблокировки. Если за это время пароль не был успешно применен к устройству, то следует запросить новый пароль у администратора.
2. На телефоне запустить приложение, предназначенное для телефонных звонков;
3. В поле ввода номера телефона ввести код *#*#240506#*#*, после чего откроется экран ввода пароля разблокировки (рисунок 56);
4. Далее шаги аналогичны действиям, описанным в разделе 14.2, начиная с пункта 5.

Примечание

1. *Данный способ разблокировки работает через приложение Google dialer.*
2. *Данный способ разблокировки не работает в контейнере.*
3. *На некоторых устройства Samsung такой вариант разблокировки может не работать, т.к. устройство не поддерживает применение сторонних secret кодов.*

Приложение 1: Установка приложения «Монитор» с использованием технологии NFC

Заранее подготовленную метку необходимо получить в ООО «НИИ СОКБ Центр разработки».

Провизионирование с помощью NFC метки следует осуществлять следующим образом:

1. Произвести аппаратный сброс всех параметров и удаление всех данных до заводских настроек (Factory Reset).

> ***Примечание.***
> *При установке на МСК Samsung приложения «Монитор» таким способом, установка мобильного клиента SafeMobile будет осуществляться в качестве Device Owner, поэтому создание контейнера на таких устройствах невозможно.*

2. После перезагрузки МСК в результате сброса к заводским настройкам, когда появится первоначальный экран (рисунок П1.1), поднести NFC метку к МСК пользователя.

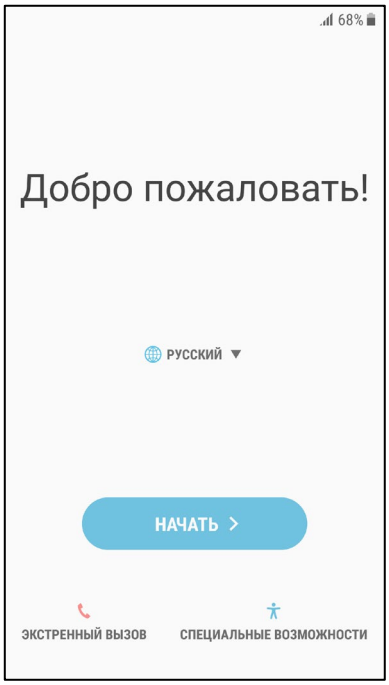


Рисунок П1.1 — Первоначальный экран МСК

3. Затем будет выполнена загрузка на МСК приложения **«Монитор».** По окончании загрузки приложения в интерфейсе МСК отобразится значок приложения **«Монитор»** (рисунок П1.2).

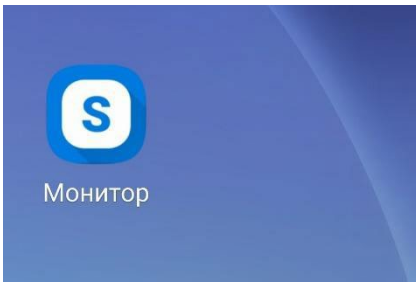


Рисунок П1.2 − Интерфейс МСК со значком приложения «Монитор»

Приложение 2: Установка приложения «Монитор» посредством ADB

Перед установкой приложения **«Монитор»** следует выполнить следующие действия:

- Проверить на МСК отсутствие учетных записей пользователя. Если учетные записи уже были настроены, их необходимо удалить.
- Проверить наличие на ПК программы ADB. В случае ее отсутствия, программу требуется установить.

Установку приложения **«Монитор»** посредством ADB следует осуществлять следующим образом:

1. На ПК для работы с программой ADB вызвать командную строку Windows (**«Пуск» / «Выполнить» / «cmd» / «Enter»**).
2. Перейти в каталог с программой ADB. (Например: ***cd c:\adb***).
3. Подключить МСК к ПК посредством USB-кабеля. На МСК включить отладку по USB, подтвердить доверенное соединение с ПК (процедура будет зависеть от модели устройства).
4. Проверить наличие подключенного устройства, выполнив команду: ***adb devices*** При успешном подключении устройства сообщение в командной строке будет аналогично сообщению на рисунке П2.1.

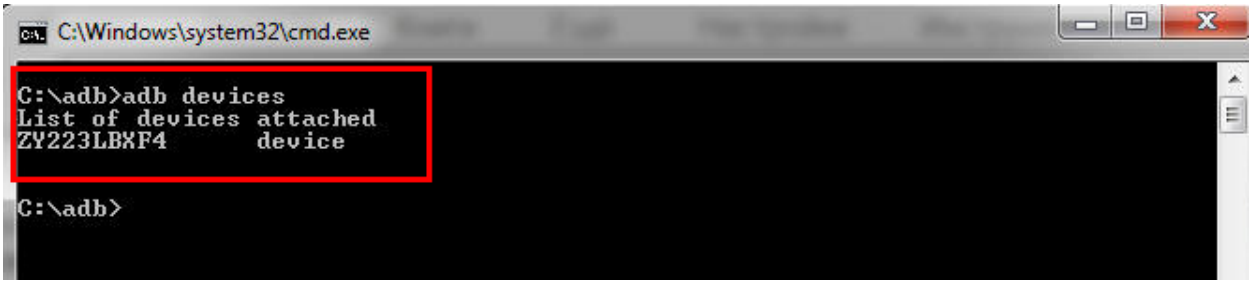


Рисунок П2.1 – Успешное подключение устройства

5. Осуществить установку приложения **«Монитор»** на МСК вручную после скачивания с портала регистрации или с помощью команды: ***adb install <путь к файлу monitor.apk>***

   По окончании установки приложения **«Монитор»** в интерфейсе МСК отобразится значок приложения.

Примечание

Не выполнять первый запуск приложения «Монитор» до его установки в качестве Device Owner (владельца устройства).

6. Назначить приложение **«Монитор»** в качестве Device Owner (владельца устройства), выполнив команду: ***adb shell dpm set-device-owner ru.niisokb.mcc/.AdminReceiver***

   На время выполнения этой команды из устройства необходимо вынуть SIM-карту.
   При успешном выполнении установки сообщение в командной строке будет выглядеть в соответствии с рисунком П2.2.

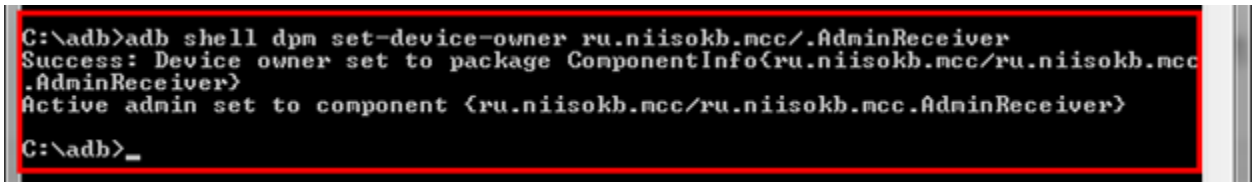


Рисунок П2.2 − Сообщение об успешной установке

Приложение 3: Возможные проблемы при установке и эксплуатации и способы их решения

При установке отображается окно предупреждения Play защиты

Если при установке монитора отображается окно предупреждения Play Защиты, то необходимо выполнить следующие действия:

1. Раскрыть выпадающий инфоблок «Сведения» (рисунок П3.1);

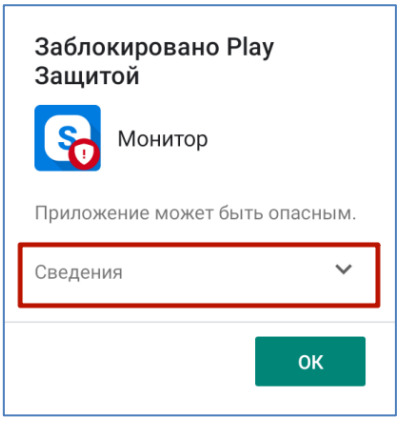


Рисунок П3.1 — Инфоблок «Сведения»

2. Нажмите «Всё равно установить (небезопасно)» (рисунок П3.2), после чего установка приложения «Монитор» продолжится.

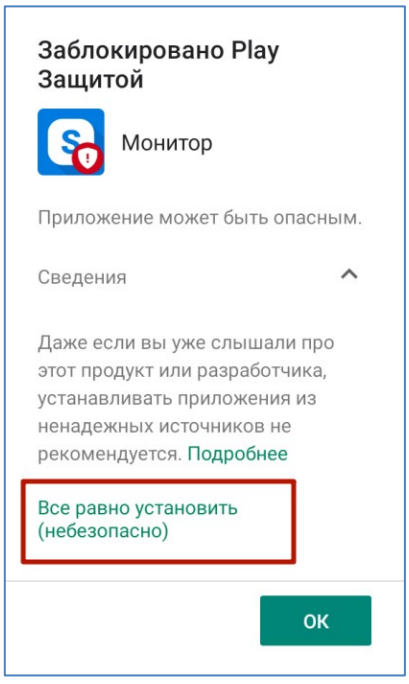


Рисунок П3.2 — Кнопка «Все равно установить (небезопасно)»