



Бастион 3 – Elsys Mobile. Руководство
оператора мобильного клиента

Версия 1.5

(17.09.2024)



Самара, 2024



Оглавление

1 Общие сведения.....	2
1.1 Назначение и область применения.....	2
1.2 Требования к совместимости.....	3
2 Установка.....	3
3 Работа в штатном режиме.....	4
3.1 Запуск приложения и вход в систему.....	4
3.2 Настройка параметров приложения.....	5
3.3 Работа в режиме считывания карт доступа.....	7
3.3.1 Основное окно приложения.....	7
3.3.2 Режим регистрации проходов.....	9
3.3.3 Работа в режимах «Всегда вход» и «Всегда выход».....	10
3.3.4 Работа в режиме «С подтверждением».....	11
3.3.5 Работа в режиме «Без регистрации».....	13
3.3.6 Использование QR-кодов в качестве идентификации.....	14
3.3.7 Обработка событий без связи с сервером.....	15
3.4 Мониторинг событий.....	16
3.4.1 Мониторинг собственных событий.....	16
3.4.2 Мониторинг событий других устройств СКУД.....	18
3.5 Режим «Точка сбора при эвакуации».....	18
3.5.1 Сценарий использования системы при эвакуации.....	18
3.5.2 Мобильное приложение в режиме «Точка сбора при эвакуации».....	19
3.6 Уведомления о проходе определенных лиц в заданную область контроля.....	21
3.7 Настройки карт доступа.....	23
3.8 Настройки USB считывателей.....	24
3.9 Защищенная область карт Mifare.....	26
3.10 Отчёт по находящимся на территории персон.....	28
3.11 Управление привязанными точками прохода.....	30
3.12 Цветовые профили событий сервера системы.....	31
3.13 Журнал событий мобильного клиента.....	32
3.14 Статистика используемых данных.....	32
3.15 Демонстрационный режим.....	33
3.16 Мобильная точка досмотра.....	34
Приложения.....	36
Приложение 1. История изменений.....	36



1 Общие сведения

1.1 Назначение и область применения

Система «Бастион-3 – Elsys Mobile» предназначена для использования мобильных устройств (терминалов) под управлением ОС Android в рамках единой системы СКУД ПК «Бастион-3» и АПК «Бастион-2».

Далее по тексту ПК «Бастион-3» и АПК «Бастион-2» именуется как ПК «Бастион-2/3».

Ключевые возможности системы включают:

1. Считывание карт доступа на мобильных устройствах через NFC с регистрацией событий в ПК «Бастион-2/3».
2. Считывание QR-кодов, выдаваемых в ПК «Бастион-2/3» в качестве пропусков.
3. Поддержка 3-х режимов работы каждого мобильного терминала:
 - a. Регистрация проходов в одном направлении (только входы или только выходы) без подтверждения оператора.
 - b. Регистрация входов и выходов на одном мобильном устройстве по одной точке прохода с подтверждением оператора (дополнительно оператор может ввести комментарий к событию).
 - c. Режим проверки пользователей СКУД без регистрации событий.
4. Полная поддержка онлайн и офлайн режима работы. В онлайн-режиме для полноценной работы системы требуется наличие связи с сервером ПК «Бастион-2/3». В офлайн режиме вся БД пропусков загружается на мобильное устройство. Оператор мобильного терминала имеет возможность видеть все сведения о пропуске, проверять его полномочия и регистрировать события даже при отсутствии связи с сервером. При восстановлении связи все накопленные события передаются на сервер.
5. Возможность автономной авторизации в системе при отсутствии связи с сервером системы.
6. Возможность передать в Бастион фотографию вместе с событием (в режиме с подтверждением оператора).
7. Управление преграждающими устройствами по событиям предъявления карт к мобильным считывателям.
8. Возможность мониторинга событий ПК «Бастион-2/3» на терминале (по настраиваемому фильтру).
9. Регистрация мобильных устройств в Бастионе через QR-коды.
10. Ограничение географической области работы каждого мобильного терминала (область работы можно задавать через Google Maps, Google Plus Codes и What3words).
11. Регистрация места (географической координаты) каждого события.
12. Отображение информации о транспортных и материальных пропусках на мобильных терминалах.



13. Режим «Точка сбора при эвакуации».
14. Уведомления о проходе определенных лиц в заданную область контроля.
15. Проверка данных QR-кода COVID-сертификата и внесение данных о сертификате в ПК «Бастион-3» или АПК «Бастион-2».
16. Демонстрационный режим.
17. Взаимодействие с настольными считывателями Elsys-SW-USB и Elsys-PW-USB-NFC.
18. Форматирование кодов карт доступа при помощи шаблонов порядка байт.

Область применения системы включает:

1. Строительные площадки, не оборудованные стационарным СКУД.
2. Удаленные объекты, где отсутствует постоянная связь.
3. Регистрация событий на входе / выходе из транспорта.
4. Дополнительная проверка прав сотрудников и посетителей, находящихся на территории.
5. Учет рабочего времени сотрудников, работающих удаленно или на выезде.
6. Контроль местоположения сотрудников и посетителей, в том числе контроль соблюдения режима карантина или самоизоляции.

1.2 Требования к совместимости

Приложение ELSYS Mobile работает на устройствах под управлением ОС Android версий 7.0 и выше.

Приложение Elsys Mobile совместимо с АПК «Бастион-2» версии 2.1.x, а также с ПК «Бастион-3» версии 2023.1 и выше.

Для считывания карт доступа мобильное устройство должно поддерживать технологию NFC. При отсутствии поддержки устройством NFC работа приложения возможна только в режиме отображения событий и считывания QR-кодов.

2 Установка

Установка приложения выполняется из Google Play Market, либо путём запуска установочного файла *ElsysMobile.apk*.

При первом запуске приложения будут запрошены следующие права:

1. Съёмка фото и видео. Это право необходимо для съёмки фотографий событий и работы с QR-кодами.
2. Доступ к данным о местоположении устройства. Это право необходимо для регистрации географических координат устройства в момент события.

3 Работа в штатном режиме

3.1 Запуск приложения и вход в систему

Запуск приложения выполняется по его пиктограмме (Рис. 1). После запуска приложения отображается окно входа, в котором требуется ввести логин и пароль для подключения. (Рис. 2).

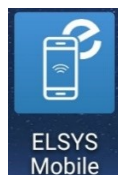


Рис. 1 Иконка запуска приложения Elsys Mobile

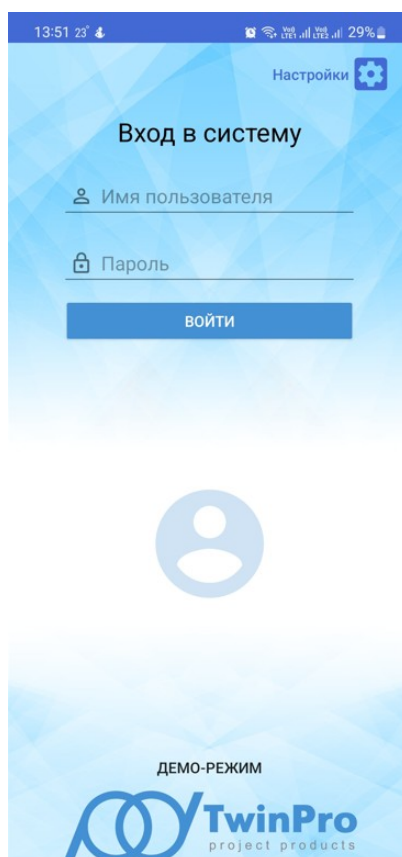


Рис. 2 Окно ввода учетных данных для подключения

Приложение использует общую с ПК «Бастион-2/3» систему авторизации, то есть логин и пароль для приложения – это имя и пароль операторов в ПК «Бастион-2/3». Для доступа к мобильному приложению у операторов ПК «Бастион-2/3» должно быть установлено полномочие «Право на доступ к системе Elsys Mobile».

Перед входом необходимо настроить строку подключения к серверу. Для настройки строки подключения нужно открыть окно настроек, переход на которое осуществляется путём нажатия кнопки «Настройки», расположенной в правом верхнем углу окна авторизации.

Внимание! Для успешного входа в приложение необходимо, чтобы на мобильном устройстве (а также на сервере оборудования) было настроено точное время.

Расхождение с сервером оборудования более, чем на несколько минут может привести к невозможности подключения.

3.2 Настройка параметров приложения

Для настройки подключения к серверу необходимо указать строку подключения (Рис. 3). При этом мобильный терминал должен быть зарегистрирован в модуле «Бастион-3 – Elsys Mobile». Адрес сервера состоит из трех частей: протокол соединения (HTTP или HTTPS в зависимости от выбранного на сервере режима), адрес сервера и порт.

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

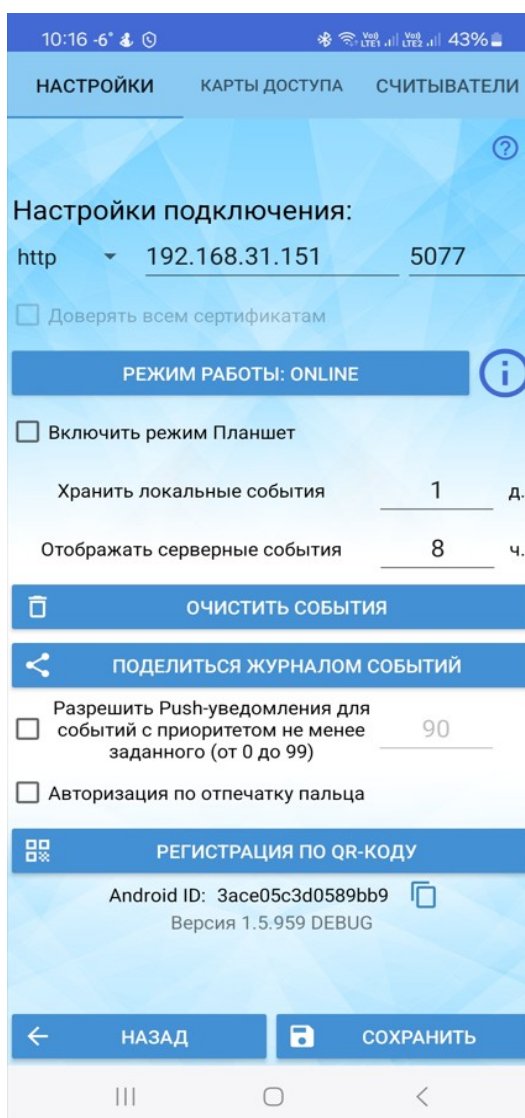


Рис. 3 Главные настройки

Зарегистрировать устройство и получить параметры подключения к серверу проще всего через QR-код. Для этого на компьютере необходимо открыть конфигуратор «Бастион-3 – Elsys Mobile». В поле «Адрес сервера» указать IP-адрес сервера и нажать кнопку «Зарегистрировать устройство по QR-коду». Затем в мобильном приложении нажать кнопку «Регистрация по QR-коду и привести камеру телефона на QR-код, отображаемый на компьютере. Мобильный терминал будет зарегистрирован в системе, а «Настройки подключения» будут заданы корректными значениями.



Зарегистрировать устройство можно и вручную, для этого под кнопкой «Регистрация по QR-коду» указывается уникальный идентификатор мобильного устройства, который необходимо указать в конфигураторе в поле Android ID. Идентификатор можно скопировать в буфер обмена, нажав на саму надпись идентификатора. Этот уникальный номер может обновляться в тех случаях, когда телефон сбрасывают до заводских настроек, в этом случае необходима повторная регистрация.

После указания строки подключения можно переходить обратно к окну входа для ввода логина и пароля оператора для выполнения входа в систему.

Также, в окне настроек можно задать несколько дополнительных параметров работы мобильного терминала:

Доверять всем сертификатам. Если для подключения используется HTTPS, то для установки соединения используется сертификат. Если в системе используется непроверенный (например, выданный самому себе) сертификат, то следует установить этот флаг. Установка этого флага снижает безопасность подключения. Данный флаг автоматически появляется, если указан протокол HTTPS.

Режим работы: Online или Offline.

В режиме *Online* все сведения о пропуске загружаются из ПК «Бастион-2/3» только при предъявлении карты доступа к мобильному терминалу. Таким образом, для отображения параметров пропусков на терминале необходимо наличие сети. В этом режиме не требуется синхронизация пропусков между мобильным терминалом и ПК «Бастион-3». Регистрация событий возможна и без наличия подключения, но на терминале не будут отображаться параметры пропуска. При восстановлении связи возможна передача событий в ПК «Бастион-2/3» и уточнение их параметров.

В режиме *Offline* все сведения о пропусках сразу загружаются из ПК «Бастион-2/3» и периодически синхронизируются. Таким образом, на мобильном терминале хранится своя копия БД пропусков и прав доступа. Для отображения параметров пропусков при регистрации событий не требуется наличие связи с сервером системы. События хранятся на мобильном терминале и передаются в ПК «Бастион-2/3» сразу при восстановлении связи с сервером.

При активном *Offline*-режиме мобильный клиент будет иметь возможность авторизоваться в системе при отсутствии связи с сервером системы. В этом случае авторизация будет производиться по сохраненным в кэше данным, полученным во время последней авторизации по установленной связи с сервером системы при активном *Online*-режиме или при активном и готовом к работе *Offline*-режиме.

Замечание: после изменений данных пропуска (номер карты, уровни доступа, временные блоки, праздничные дни, материально-транспортные пропуска) необходимо в контекстном меню пропуска выбрать команду «Обновить пропуск в контроллерах».

Хранить локальные события N д. Настраиваемый параметр времени хранения событий, которые были созданы на телефоне. Диапазон настроек от 1 дня до 30 дней.

Отображать серверные события N ч. Настраиваемый параметр времени отображения серверных событий. Диапазон настроек от 1 часа до 24 часов. При перезапуске мобильного приложения все серверные события удаляются.



Очистить события очищает все события чтения карт доступа и события, полученные от драйвера.

Разрешить push-уведомления о событиях с приоритетом не менее заданного. Позволяет отображать высокоприоритетные события, получаемые с сервера ПК «Бастиян-2/3» в виде push-уведомлений на заблокированном экране. Уведомления должны быть включены в Android для приложения Elsys Mobile.

Авторизация по отпечатку пальца. Позволяет оператору мобильного терминала авторизоваться в системе Бастиян по отпечатку пальца. При включении данной настройки необходимо будет для активации авторизации по отпечатку пальца приложить палец к сканеру и войти в систему по введенным логину и паролю.

3.3 Работа в режиме считывания карт доступа

3.3.1 Основное окно приложения

В основном окне приложения отображается ряд элементов, обозначенных на Рис. 4.

Область 1 – отображает выбранный режим регистрации событий (см. п. 3.3.2).

Область 2 – отображает режим работы приложения (онлайн / оффлайн).

Область 3 – отображает наличие связи с сервером ПК «Бастиян-2/3».

Область 4 – вызов меню.

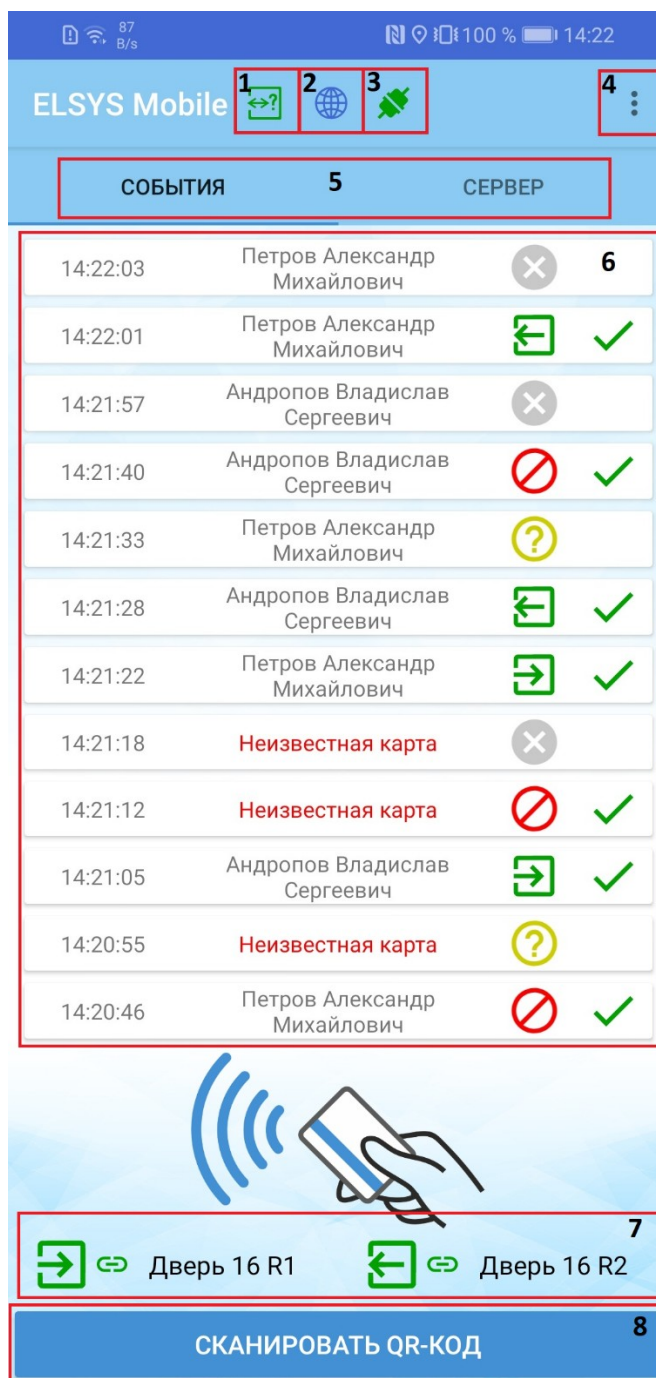


Рис. 4 Основное окно приложения

Область 5 – Переключение режима мониторинга событий. Если выбрать «События» - то в списке 6 будут отображаться только события, зарегистрированные на этом терминале. При выборе «Сервер» - будут отображаться события других устройств СКУД, принятые с сервера ПК «Бастион-2/3».

Область 6 – отображает список событий.

Область 7 – отображает считыватели СКУД, которые привязаны к направлениям данной мобильной точки доступа. Если регистрируется всегда вход или всегда выход, то будет отображен 1 считыватель (входной или выходной). Если же к терминалу привязано 2 считывателя, то они будут отображены, как показано на Рис. 4.

Область 8 – кнопка открытия окна для считывания карты доступа через QR-коды.

Если в верхней части экрана появится значок, обозначенный на Рис. 5, значит ваше мобильное устройство вышло за пределы ограниченной географической зоны, которая настраивается в конфигураторе драйвера. Либо на устройстве не включена геолокация, а в это время в конфигураторе драйвера было включено ограничение местоположения. В этом случае коды всех карт доступа не будут обрабатываться телефоном.



Рис. 5 Предупреждающая иконка выхода из ограниченной зоны местоположения.

3.3.2 Режим регистрации проходов

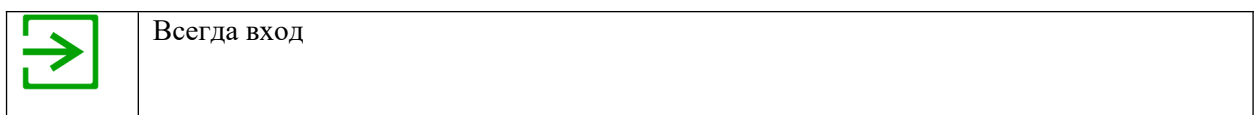
Для считывания информации о карте доступа необходимо приложить её к мобильному устройству (приложение «Elsys Mobile» должно быть активно) таким образом, чтобы карта попала в область считывания NFC.




В зависимости от настроенного режима регистрации проходов приложение будет выполнять разные действия:

1. *Режим с подтверждением.* Если мобильный терминал настроен на работу в этом режиме, то оператору при предъявлении карты будет выведено окно с выбором действий. Оператор может указать комментарий, сделать фотографию события и указать, регистрируется вход или выход.
2. *Вход* – при предъявлении карты всегда регистрируется вход, без подтверждения оператором (или отказ в доступе при отсутствии прав).
3. *Выход* – при предъявлении карты всегда регистрируется выход, без подтверждения оператором (или отказ в доступе при отсутствии прав).
4. *Без регистрации* – события в ПК «Бастион-2/3» не передаются, но при предъявлении карты в мобильном приложении выводятся данные пропуска.

Режим регистрации проходов настраивается в конфигураторе драйвера, отдельно для каждого мобильного устройства.

Выбранный режим регистрации проходов отображается в терминале в верхней части экрана в виде одной из пиктограмм:



	Всегда выход
	Режим с подтверждением
	Без регистрации

3.3.3 Работа в режимах «Всегда вход» и «Всегда выход»

При считывании карты доступа в этих режимах система автоматически формирует событие на основе данных, загруженных из ПК «Бастион-2/3». Оператору отображается окно в форме карты доступа с загруженными параметрами пропуска, включая фотографию (Рис. 6). Единственное доступное для оператора действие – закрыть это окно после ознакомления с информацией о событии.

Событие учитывает наличие полномочий у владельца карты доступа. Например, на Рис. 6 системой сформировано событие «Доступ запрещен», так как у владельца предъявленной карты нет прав на выход через данный мобильный терминал.

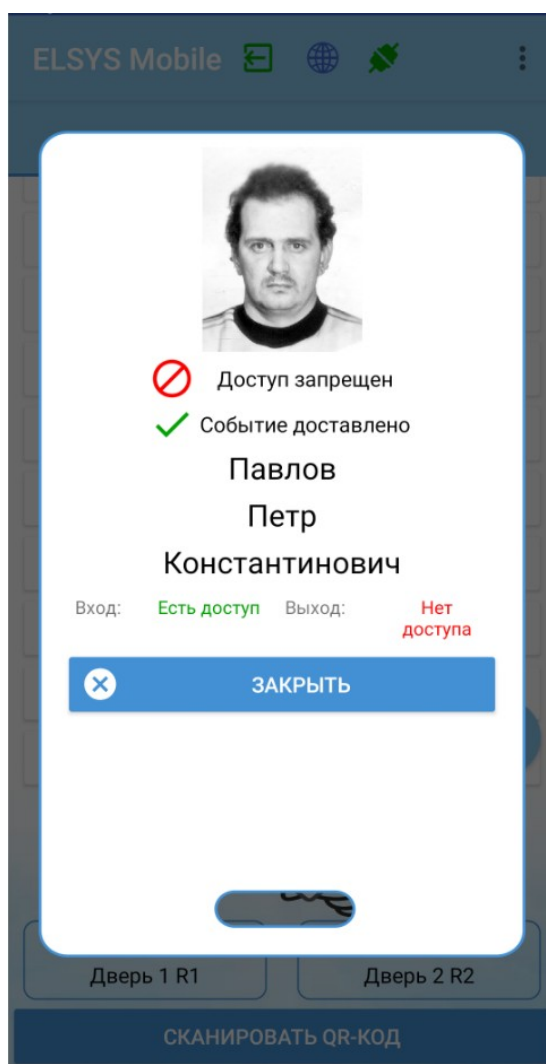


Рис. 6 Считывание карты в режиме «Всегда выход»

3.3.4 Работа в режиме «С подтверждением»

При считывании карты доступа в режиме с подтверждением перед формированием события оператору будет выведено окно в форме карты доступа с загруженными параметрами пропуска, включая фотографию (Рис. 7).

Оператор может выполнить следующие действия до отправки события:

1. Ввести комментарий к событию.
2. Сделать фотографию события, нажав на пиктограмму камеры.

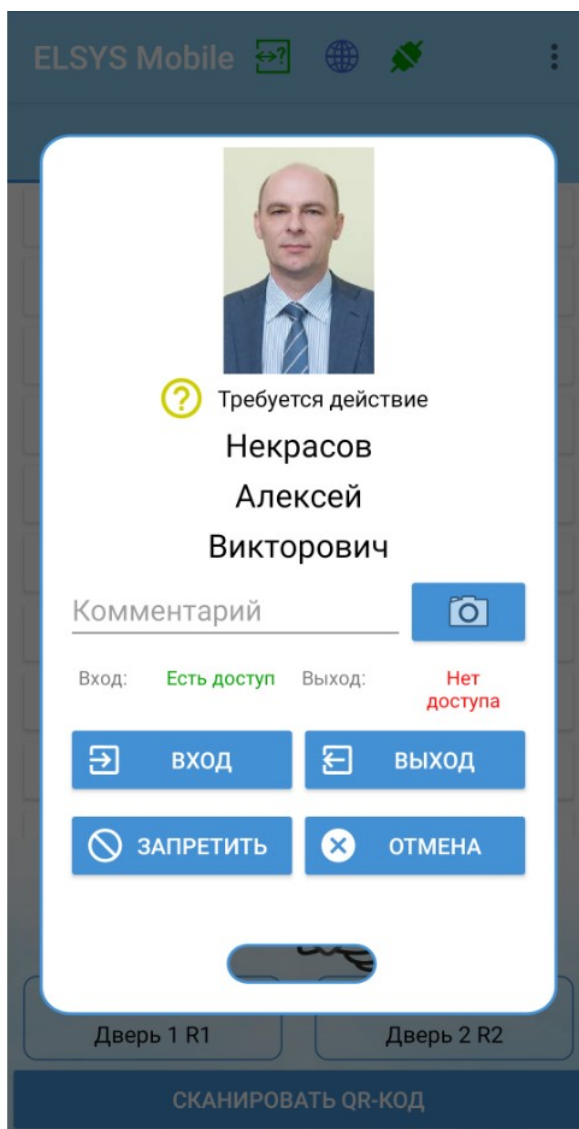


Рис. 7 Считывание карты в режиме «С подтверждением»

После этого оператор может нажать кнопки в нижней части окна, что приведет к следующим результатам:

1. *Вход*. При нажатии на эту кнопку будет сформировано событие «Штатный вход», независимо от наличия прав доступа у владельца пропуска. То есть, в режиме с подтверждением решение о предоставлении доступа принимает оператор мобильного терминала. Система только выводит подсказки, есть ли доступ на вход и выход (Рис. 7).

2. *Выход*. При нажатии на эту кнопку будет сформировано событие «Штатный выход», независимо от наличия прав доступа у владельца пропуска.
3. *Запретить*. При нажатии на эту кнопку будет сформировано событие «Доступ запрещён», независимо от наличия прав доступа у владельца пропуска.
4. *Отмена*. Никаких событий сформировано не будет.

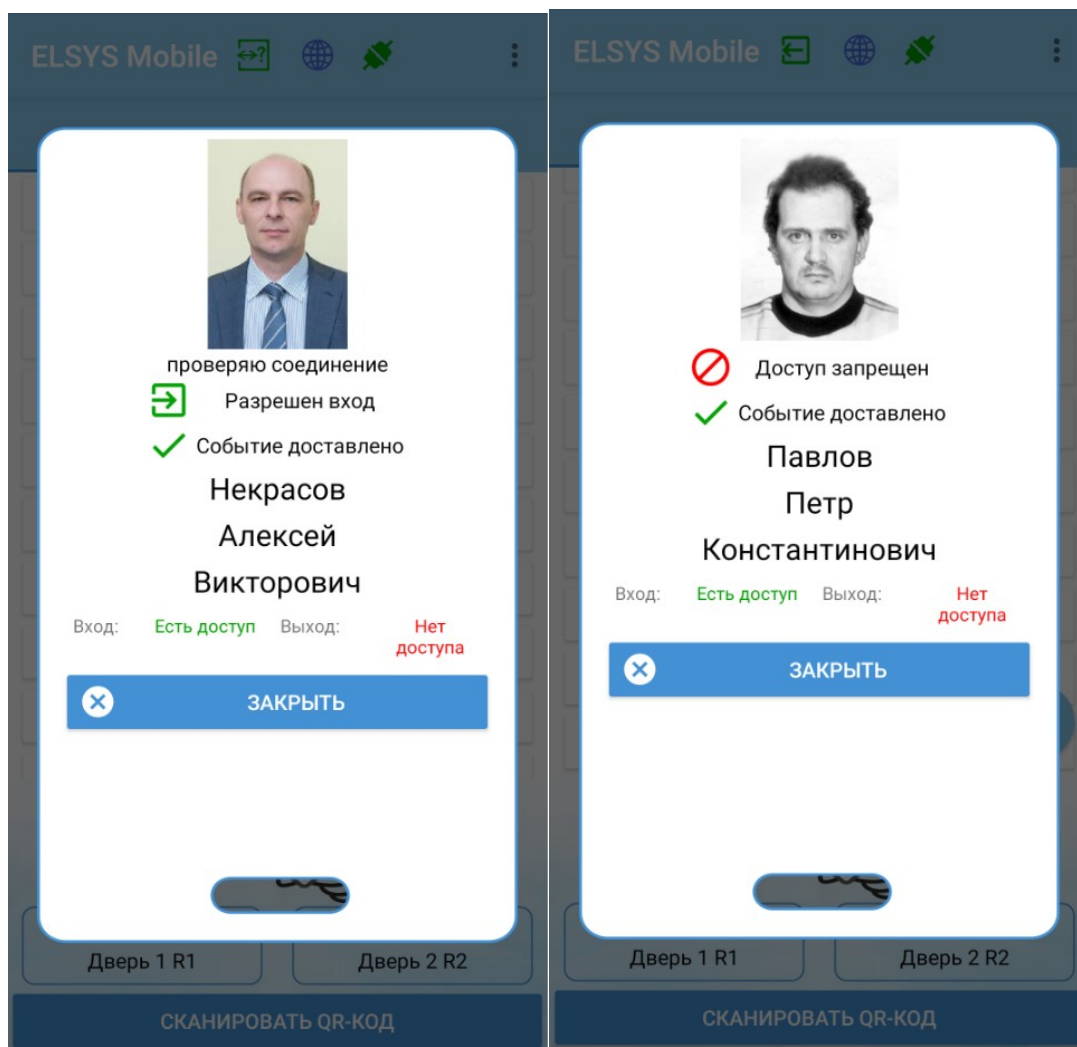


Рис. 8 Окно с результатом обработки предъявленной карты

После нажатия на одну из кнопок, описанных выше, окно регистрации события примет вид, представленный на Рис. 8 или Рис. 9.

Под фотографией владельца будет размещаться комментарий, который оставил оператор мобильного терминала.

Надпись «Событие доставлено» говорит о том, что событие успешно передано на сервер ПК «Бастион-2/3».

На Рис. 9 рядом с фотографией владельца пропуска из ПК «Бастион-2/3» отображается фотография события, сделанная оператором мобильного терминала.

Для завершения работы с событием следует нажать кнопку «Заккрыть».

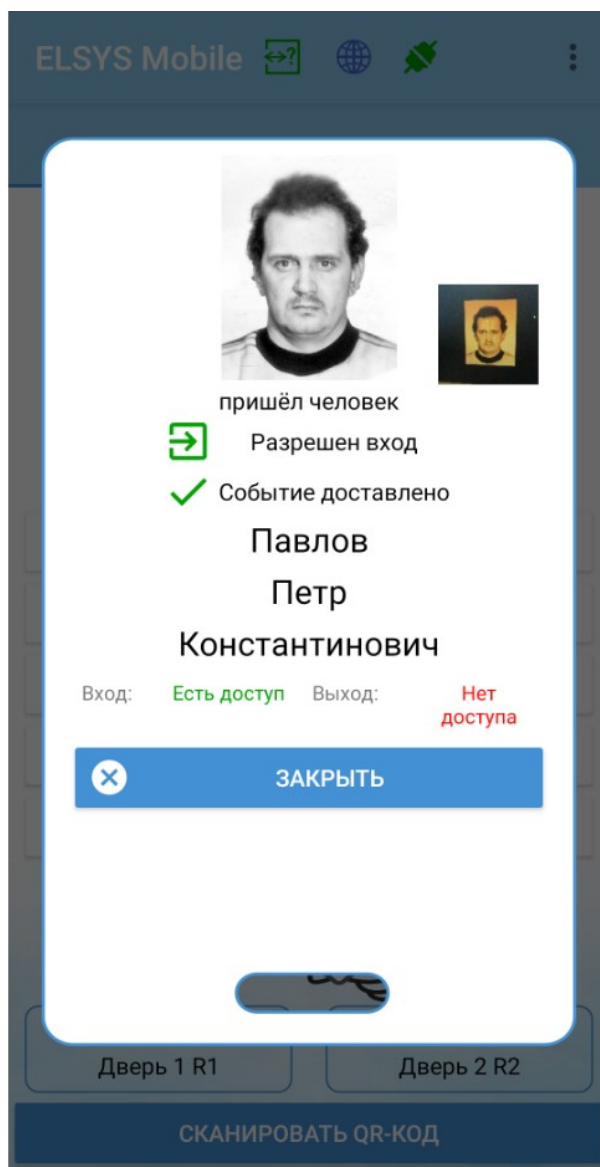


Рис. 9 Окно с результатом обработки предъявленной карты с фотографией события

3.3.5 Работа в режиме «Без регистрации»

В режиме без регистрации событий (Рис. 10) никакие события не передаются в ПК «Бастион-2/3». Мобильный терминал используется только для проверки прав доступа.

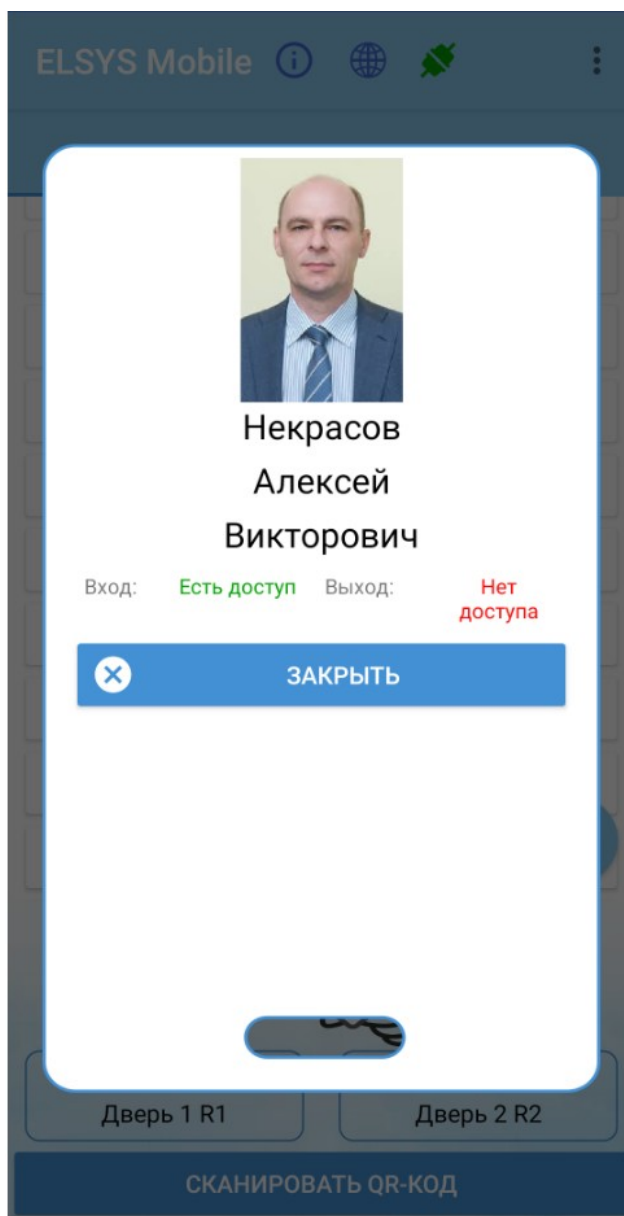


Рис. 10 Считывание карты в режиме «Без регистрации»

3.3.6 Использование QR-кодов в качестве идентификации

Мобильный терминал может считывать номера карт, закодированные в QR-кодах. Эти QR-коды должны быть предварительно сформированы в АРМ «Бюро пропусков» ПК «Бастион-2/3». Работа с QR-кодами должна быть разрешена в настройках мобильного терминала.

QR-коды могут выдаваться для любых пропусков.

Срок действия QR-кода равняется сроку действия пропуска.

Если в системе разрешено использовать QR-коды, то в главном окне внизу отображается кнопка «Сканировать QR-код» (Рис. 10). При нажатии на нее откроется окно сканирования QR-кода. После распознавания кода карты из QR-кода все действия аналогичны действиям при предъявлении карты доступа.

3.3.7 Обработка событий без связи с сервером

Если связи с сервером ПК «Бастион-2/3» нет, то поведение терминала зависит от режима его работы – онлайн или офлайн.

Отсутствие связи с сервером ПК «Бастион-2/3» индицируется красной пиктограммой разорванного соединения в верхней части основного экрана приложения (Рис. 11).

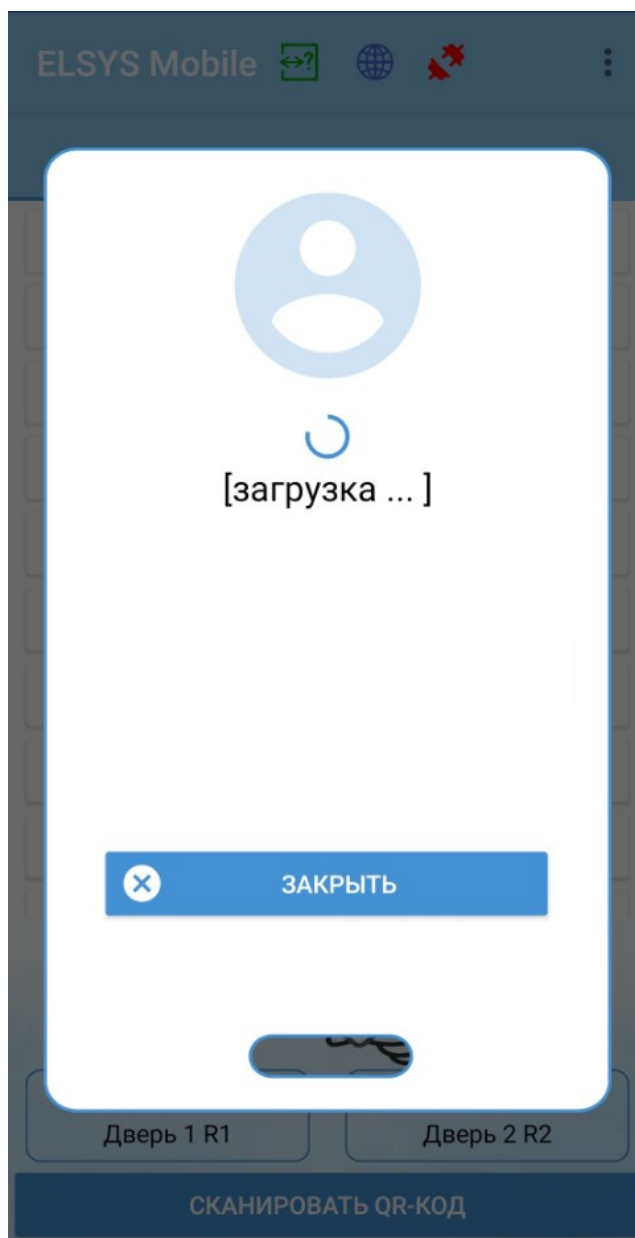


Рис. 11 Попытка загрузки данных без связи с сервером в онлайн режиме

В режиме «Онлайн» терминал не хранит БД пропусков, поэтому сведения о пропуске не будут отображены при предъявлении карты доступа (Рис. 11). Тем не менее, в этом режиме терминал все равно сохраняет события предъявления карт доступа локально. При восстановлении связи с сервером ПК «Бастион-2/3» оператор может уточнить параметры каждого события, нажав на это событие в списке событий (Рис. 12). События, возникшие без связи с сервером, в этом случае будут отображаться в виде строки с надписью «[загрузка...]».

В режиме «Оффлайн» копия БД пропусков ПК «Бастион-2/3» хранится на каждом мобильном терминале. Поэтому обработка событий на мобильном терминале не зависит от наличия связи с сервером ПК «Бастион-2/3». Накопленные события передаются на сервер при восстановлении связи.

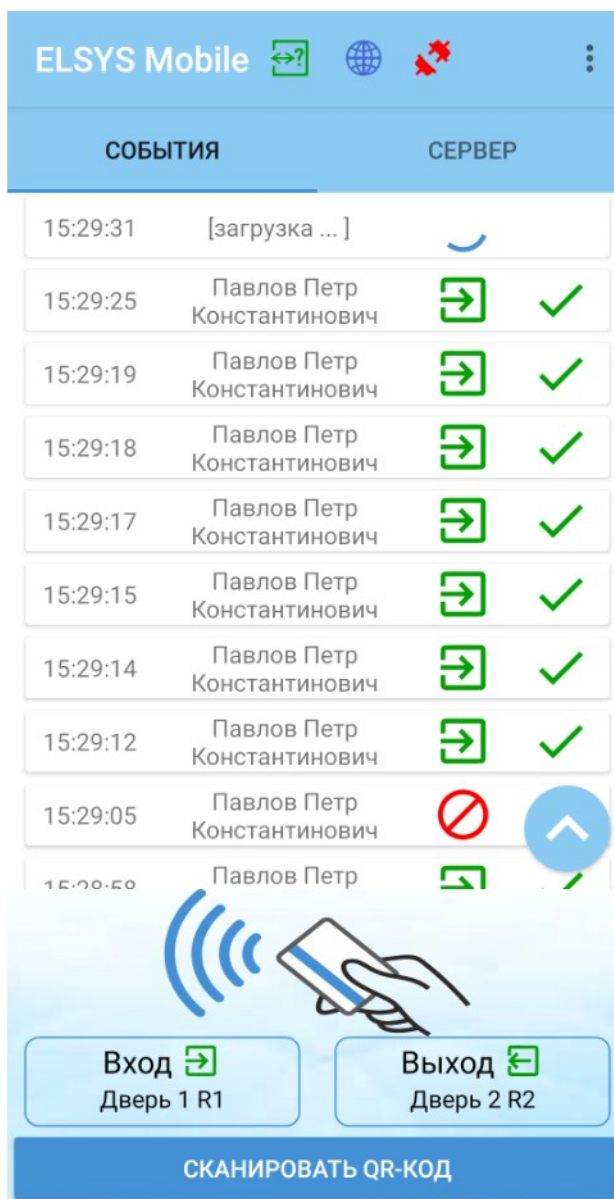


Рис. 12 Отображение событий в онлайн режиме без связи с сервером

3.4 Мониторинг событий

3.4.1 Мониторинг собственных событий

Мобильный терминал обеспечивает сохранение и мониторинг собственных событий. По умолчанию, в основном окне выбран как раз этот режим (Рис. 13).

В окне отображаются только события за последние сутки. Этот параметр можно поменять в настройках терминала (можно указать количество дней хранения локальных событий, см. п. 3.2).

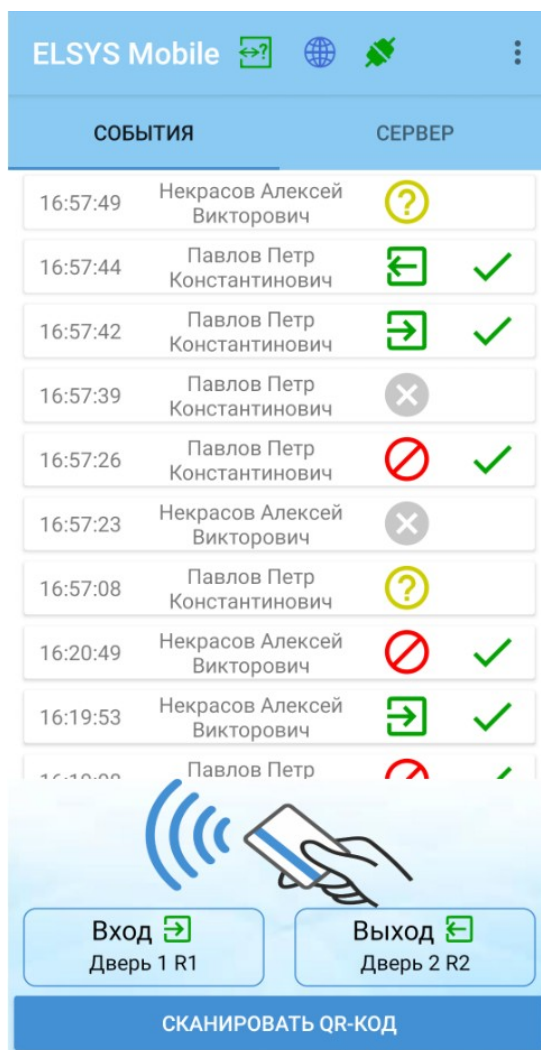








Рис. 13 Основное окно приложения в режиме мониторинга собственных событий

Значение пиктограмм, отображаемых справа от события, приведены в таблице ниже:

	Зарегистрировано событие «Штатный вход».
	Зарегистрировано событие «Штатный выход».
	Зарегистрировано событие «Доступ запрещен».
	Событие не зарегистрировано, не будет передано в ПК «Бастион-2/3».
	Требуется действие со стороны оператора мобильного терминала.
	Событие успешно передано на сервер ПК «Бастион-2/3».

3.4.2 Мониторинг событий других устройств СКУД

Мобильный терминал обеспечивает отображение событий, загруженных с сервера ПК «Бастион-2/3». В конфигураторе драйвера «Elsys Mobile» есть возможность настройки, события от каких устройств СКУД будут передаваться на мобильные терминалы.

События, принятые с сервера, отображаются на отдельной вкладке «Сервер» (Рис. 14). По умолчанию отображаются события за последние 8 часов (задается в настройках мобильного терминала).



Рис. 14 Основное окно приложения в режиме мониторинга событий других устройств СКУД
Для каждого события отображается время его возникновения, устройство и текст события.

3.5 Режим «Точка сбора при эвакуации»

3.5.1 Сценарий использования системы при эвакуации

При эвакуации персонал должен собраться в точке сбора, определенной режимом. Точек сбора может быть несколько, в зависимости от размера и конфигурации объекта. Точка, куда человек

эвакуируется, определяется его текущим местоположением (областью контроля) на момент объявления эвакуации (но программно это никак не учитывается, следует ориентироваться на указатели и планы эвакуации). Предполагается, что при объявлении эвакуации все точки прохода разблокируются.

Ответственное лицо с мобильным устройством с установленным Elsys Mobile прибывает в точку сбора и нажимает в приложении кнопку "Эвакуация".

При этом на экране отобразятся следующие сведения:

- Сколько человек должно быть эвакуировано всего.
- Сколько человек уже отмечилось в точках эвакуации.
- Сколько человек еще не отметились.
- Список тех, кто не отметился в точках сбора с указанием их последнего места предъявления карты доступа и времени этого предъявления. Эту информацию надо обновлять периодически, чтобы видеть, если люди вдруг пришли на другую точку сбора.

Все люди, прибывающие на точку сбора, отмечаются, прикладывая карту к мобильному терминалу. При этом оператору кратковременно отображается – кто прибыл. Прибывший пропадает из списка ожидаемых людей. В ПК «Бастион-2/3» отправляется специальное событие – «Прибыл в место сбора при эвакуации ФИО».

Если пытается отметить человек, не из списка эвакуируемых - он учитывается отдельно (В ПК «Бастион-2/3» отправляется специальное событие – "Прибыл в место сбора при эвакуации ФИО", но он не вычитается из числа ожидаемых людей).

Когда число ожидаемых людей стало равно 0 (все эвакуированы), в ПК «Бастион-2/3» отправляется событие «Эвакуация завершена успешно».

Если кто-то не отметился в точках сбора, но ждать дольше нет смысла, оператор должен иметь возможность нажать кнопку «Завершить эвакуацию» (с подтверждением). В ПК «Бастион-2/3» будет отправлено событие «Эвакуация завершена вручную», с указанием сколько человек не были отмечены.

В генераторе отчетов ПК «Бастион-2/3» есть возможность сформировать отчет, который будет содержать события эвакуации.

3.5.2 Мобильное приложение в режиме «Точка сбора при эвакуации»

При включении в конфигураторе драйвера настроек «Разрешить режим эвакуации» и «Является точкой сбора эвакуации» в мобильном приложении в верхней части экрана загорится иконка (Рис. 15).



Рис. 15 Кнопка запуска режима «Точка сбора при эвакуации»

При нажатии на эту иконку оператор должен подтвердить своё решение о начале эвакуации. После подтверждения на драйвер придет сообщение, что данная мобильная точка

инициализировала начало эвакуации, а само событие будет называться «<Имя мобильной точки> Эвакуация (начало)».

В момент работы режима эвакуации на мобильном приложении будет открыта форма, изображенная на Рис. 16.



Рис. 16 Интерфейс режима «Точка сбора при эвакуации»

Сверху будет отображаться статус соединения с сервером. Ниже – информация о количестве людей, находящихся на территории, количество сотрудников, отмеченных в точках сбора и количество неотмеченных сотрудников. Далее располагается сам список людей, ожидаемых в точке сбора при эвакуации.

Каждый пришедший сотрудник должен идентифицировать себя при помощи приложенной карты доступа или при помощи сканирования QR-кода пропуска.

При считывании карты доступа, которая не зарегистрирована в ПК «Бастион-2/3», будет отправлено сообщение «Прибыл в место сбора при эвакуации человек с неизвестной картой».

В случае, если пришел сотрудник, которого не было в списке ожидаемого персонала, считанная карта доступа посчитается как ожидаемая и будет отправлено стандартное сообщение о приходе сотрудника к месту сбора при эвакуации. При этом, число сотрудников, находящихся в области контроля, и число отмеченных сотрудников увеличится.

После регистрации последнего сотрудника на экране мобильного телефона появится диалоговое сообщение о том, что персонала на территории не обнаружено с предложением завершить эвакуацию или продолжить (Рис. 17).

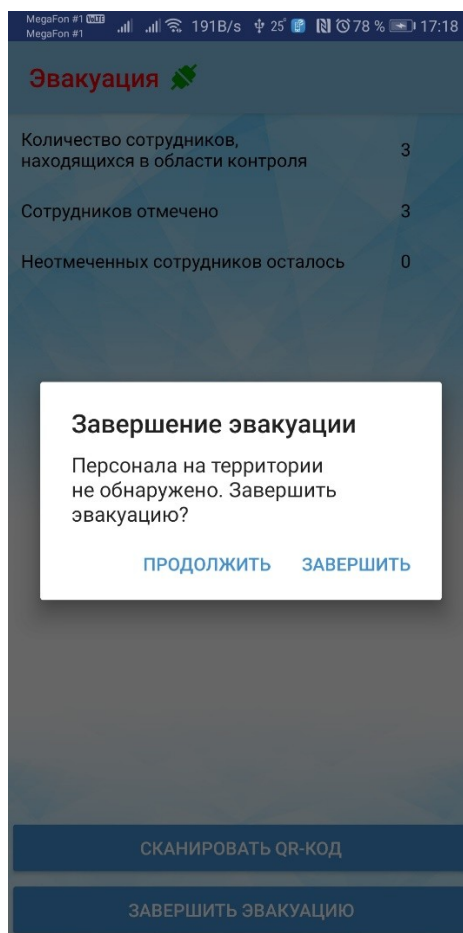


Рис. 17 Завершение эвакуации

При завершении эвакуации драйвер выведет соответствующее сообщение в ПК «Бастион-2/3».

Оператор так же может завершить эвакуацию вручную, если нет возможности ждать оставшихся сотрудников, в таком случае в ПК «Бастион-2/3» будет сформировано сообщение «Эвакуация завершена вручную. Прибыло n из m человек».

3.6 Уведомления о проходе определенных лиц в заданную область контроля

Начиная с версии драйвера 1.2 в мобильном клиенте появилась возможность уведомлять оператора мобильного клиента о проходе определенных лиц в заданную область контроля.

Внимание! Эта функция активируется на мобильном приложении только при подключении к драйверу «Бастион-3 – Elsys Mobile» версии 1.2 с ПК «Бастион-2/3» версии 2.1.12.

Уведомления приходят на мобильном клиенте в виде push-уведомлений. Уведомления настраиваются в виде создания подписок на проход выбранной персоны в выбранную область контроля. Настройка уведомлений на мобильном клиенте осуществляется при открытии пункта меню «Уведомления о проходе» справа вверху на главном экране мобильного приложения (Рис. 18).

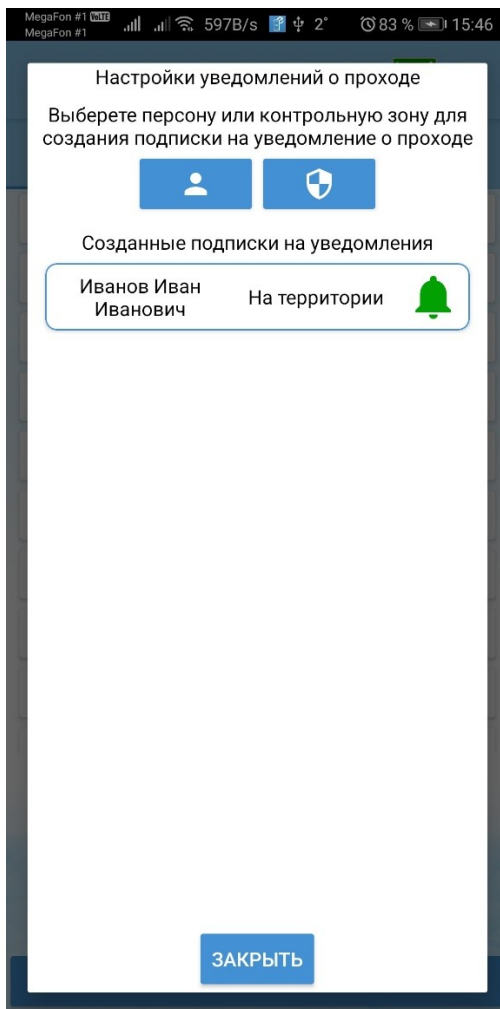







Рис. 18 Настройка уведомлений о проходе лиц

Предоставляется возможность создавать 2 типа подписок на уведомления о проходе:

- Уведомление о проходе одной персоны в одну или несколько областей контроля;
- Уведомление о проходе в одну область контроля одной или нескольких персон.

Элементы управления для настроек уведомлений о проходе представлены в таблице:

	<p>Создается подписка на уведомление типа «одна персона в одну или несколько областей». Для этого выбирается сначала одна персона, а потом несколько областей контроля.</p>
	<p>Создается подписка на уведомления типа «одна область контроля на одну или несколько персон». Для этого выбирается сначала одна область контроля, а потом несколько персон.</p>
	<p>Сброс несохраненных настроек подписки и возврат на начальный экран настроек.</p>

	Подписка будет уведомлять о проходе определенных лиц в заданные области контроля.
	Подписка не будет уведомлять о проходе определенных лиц в заданную область.

Все созданные подписки отображаются в главном списке (Рис. 19).

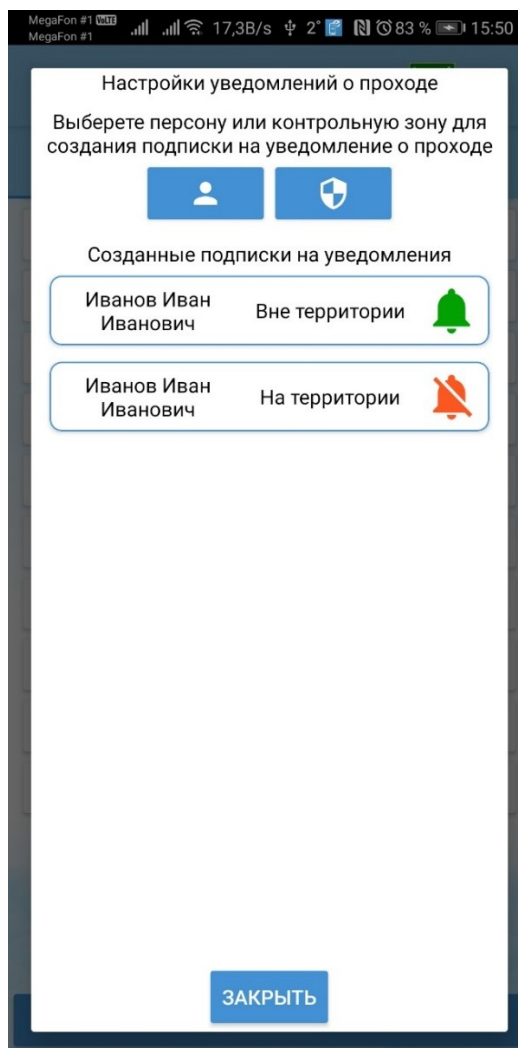


Рис. 19 Созданные подписки на уведомления

При проходе определенного лица в область контроля мобильное приложение создаст push-уведомление с заголовком «Уведомление о проходе» и текстом «<ФИО> Зарегистрирован в <Имя_контрольной_области>»

3.7 Настройки карт доступа

Форматирование кодов карт доступа осуществляется в разделе настроек «Карты доступа». Данная настройка позволяет задать порядок принимаемых байт кода карты. Для этого необходимо включить галочку «Включить форматирование кода карты». Предлагается 2 варианта форматирования: форматирование по умолчанию или форматирование редактируемыми шаблонами (Рис. 20).

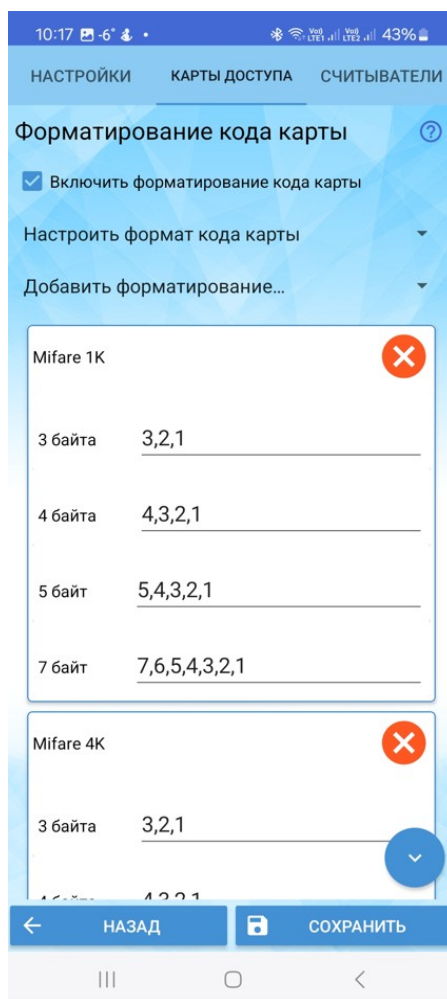


Рис. 20 Настройки форматирования кода карты

Если включено форматирование, но редактируемые шаблоны не были созданы, то будет использоваться шаблон по умолчанию. Тип карты доступа определяется при помощи настольного считывателя. Если карта читается мобильным NFC-модулем, то тип карты определяется по известным байтам ATQA и SAK, которые предоставляет производитель карт NXP. Данные байты работают по интерфейсу NfcA. Некоторые карты, на пример банковские, могут иметь свой набор ATQA и SAK байт производителя или не иметь интерфейс NfcA. Некоторые банковские карты МИР не используют данный интерфейс. Если не удастся определить интерфейс NfcA и тип карты, то номер карты берется по-старому методу из серийного номера карты.

3.8 Настройки USB считывателей

Мобильное приложение поддерживает работу с внешними считывателями Elsys-SW-USB, Elsys-PW-USB-NFC и другими OTG-устройствами, которые будут присылать мобильному клиенту через COM порт код карты в текстовом HEX-формате.

В рамках работы с OTG-устройствами реализована поддержка преобразователей интерфейсов Elsys-CU-USB/232-485. К данному USB-преобразователю можно подключить преобразователь Elsys-IC-WG/RS/TM в режиме WG→RS, который принимает с интерфейса Wiegand код карты и передает его в RS-232 асинхронно в посимвольном HEX-формате. Таким образом к преобразователю можно подключить любой настенный Wiegand-считыватель.

Для возможности чтения считываемых карт через указанные настольные считыватели, необходимо в настройках приложения в разделе «Считыватели» выбрать нужный считыватель (Рис. 21).

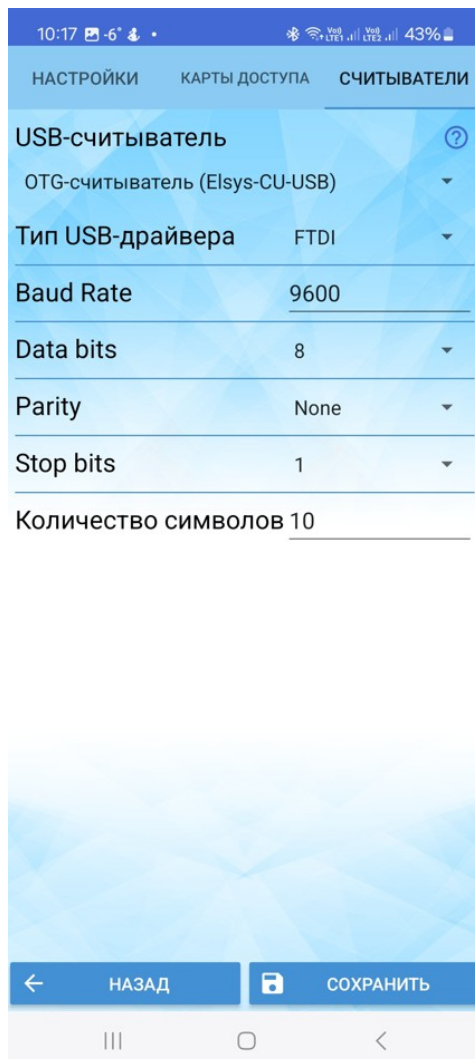


Рис. 21: Настройки OTG-считывателей

Преобразователь Elsys-IC-WG/RS/TM в посылке передает 5 байт кода карты и байт контрольной суммы в следующем виде:

D5H D5L D4H D4L D3H D3L D2H D2L D1H D1L CSH CSL

где DxH – старшие полубайты, DxL – младшие полубайты шестнадцатиричного кода карты, CSH, CSL – полубайты контрольной суммы, вычисляемой поразрядным исключающим ИЛИ двоичного пятибайтового кода карты. Пример получаемой текстовой посылки: «688FAA292C48». Мобильному клиенту необходим только код карты, поэтому в настройках указываем значение «Количество символов», равное 10.

Для работы с OTG-устройством Elsys-CU-USB/232-485 необходимо задать следующие настройки:

- 1) Тип USB-драйвера — FTDI;
- 2) Boud Rate – 9600;

- 3) Data bits – 8;
- 4) Parity – None;
- 5) Stop bits – 1.

При выборе USB-считывателя «OTG-считыватель (Elsys-CU-USB)» все необходимые настройки будут выставлены по умолчанию.

После выбора необходимого считывателя и авторизации оператора в системе Бастион считыватели подключаются к мобильному устройству при помощи OTG-кабеля. При успешном подключении считывателя в верхней части интерфейса приложения появится соответствующая иконка статуса подключения (Рис. 22).



Рис. 22 Иконка статуса подключения внешнего USB-считывателя

3.9 Защищенная область карт Mifare

На мобильном приложении появилась возможность чтения кода карты из защищенной области карт Mifare типа SL1 (Mifare Classic) и SL3 (Mifare Plus). Профиль безопасности настраивается в отдельном диалоговом окне (Рис. 23).

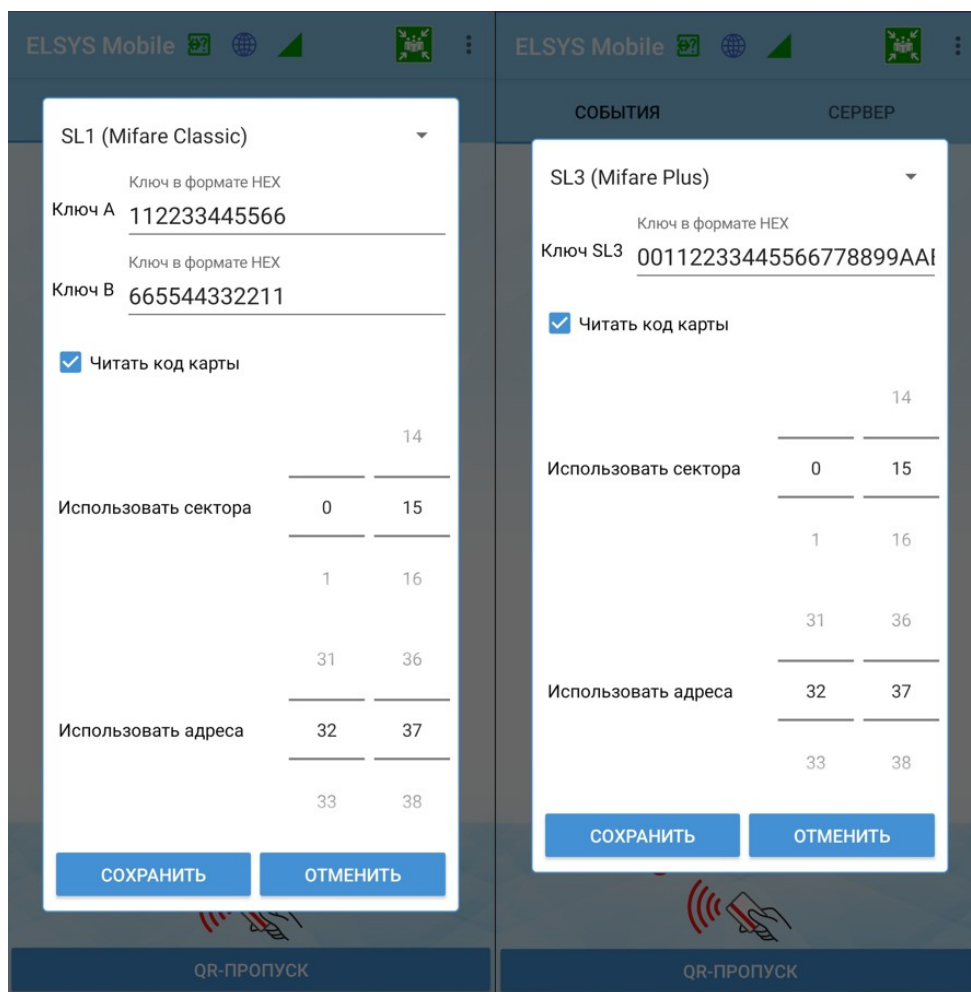


Рис. 23. Настройки профиля безопасности Mifare

По умолчанию используется профиль «Стандартный номер карты».

- Ключ А — HEX-ключ А для профиля безопасности SL1;
- Ключ В — HEX-ключ В для профиля безопасности SL1;
- Ключ SL3 – HEX-ключ для профиля безопасности SL3;
- Читать код карты — если настройка включена в случае успешной авторизации в секторе мобильный клиент будет читать UID карты, при выключенной настройке код карты берётся из диапазона адресов;
- Использовать сектора — диапазон секторов, в которые будет производиться авторизация;
- Использовать адреса — диапазон адресов байт, которые будут читаться из сектора.

Защищенная область карт доступа Mifare поделена на сектора. Нумерация начинается с 0. Каждый сектор состоит из 4 блоков. Последний блок каждого сектора содержит в себе сам ключ безопасности, поэтому пользовательские данные хранятся только в первых 3 блоках.

Ключи безопасности профиля SL1 имеют длину 6 байт, ключ безопасности SL3 имеет длину 16 байт. Для работы с SL1 имеется возможность авторизации в секторах по ключам «А» и «В». Если

карта доступа запрограммирована по одному ключу, то ключ «В» в настройках профиля не указывается. Ключи указываются в формате HEX.

Когда настройка «Читать код карты» включена указывается диапазон секторов, к которым мобильный клиент будет пытаться авторизоваться. После первой успешной авторизации в секторе из диапазона мобильный клиент читает UID считанной карты.

Когда настройка «Читать код карты» выключена мобильный клиент будет читать код карты по адресу. Для этого необходимо указать единственный сектор (левая и правая граница диапазона секторов совпадают) и диапазон адресов байт защищенной области. При успешной авторизации в указанном секторе производится чтение его байт и возвращение байт из диапазона в виде кода карты. Например, нужный код карты «2» находится в секторе 8 на месте 16-ого байта, в профиле безопасности мобильного клиента необходимо указать диапазон секторов 8-8. Диапазон адресов 16-21 вернет код карты в обратном порядке байт «000000000002». Если диапазон адресов сдвинуть в пределы 13-18, то код карты будет «000002000000» (Рис. 24).

```

Sector 8 (0x08)
[20] 00 00 00 00 00 00 00 00 | \\\\\\\\\\\ |
    rwi 00 00 00 00 00 00 00 00 | \\\\\\\\\\\ |
[21] 02 00 00 00 00 00 00 00 | \\\\\\\\\\\ |
    rwi 00 00 00 00 00 00 00 00 | \\\\\\\\\\\ |
[22] 00 00 00 00 00 00 00 00 | \\\\\\\\\\\ |
    rwi 00 00 00 00 00 00 00 00 | \\\\\\\\\\\ |
[23] 28:DA:CC:CF:A8:49 Мохито-Коломбо А
    wxx FF:07:80 69
    (r) 29:F0:56:D4:9A:4C Мохито-Коломбо В
    
```

Рис. 24 Пример содержимого сектора защищенной области

Профиль безопасности сохраняется при нажатии на кнопку «Сохранить». Кнопка «Отмена» откатывает профиль безопасности до старых значений.

3.10 Отчёт по находящимся на территории персон

Начиная с версии драйвера 2.1 в мобильном клиенте появилась возможность просмотра отчёта по находящимся на территории персон. Просмотреть отчет можно по нажатию в меню пункта «Персоны на территории» (Рис. 25).

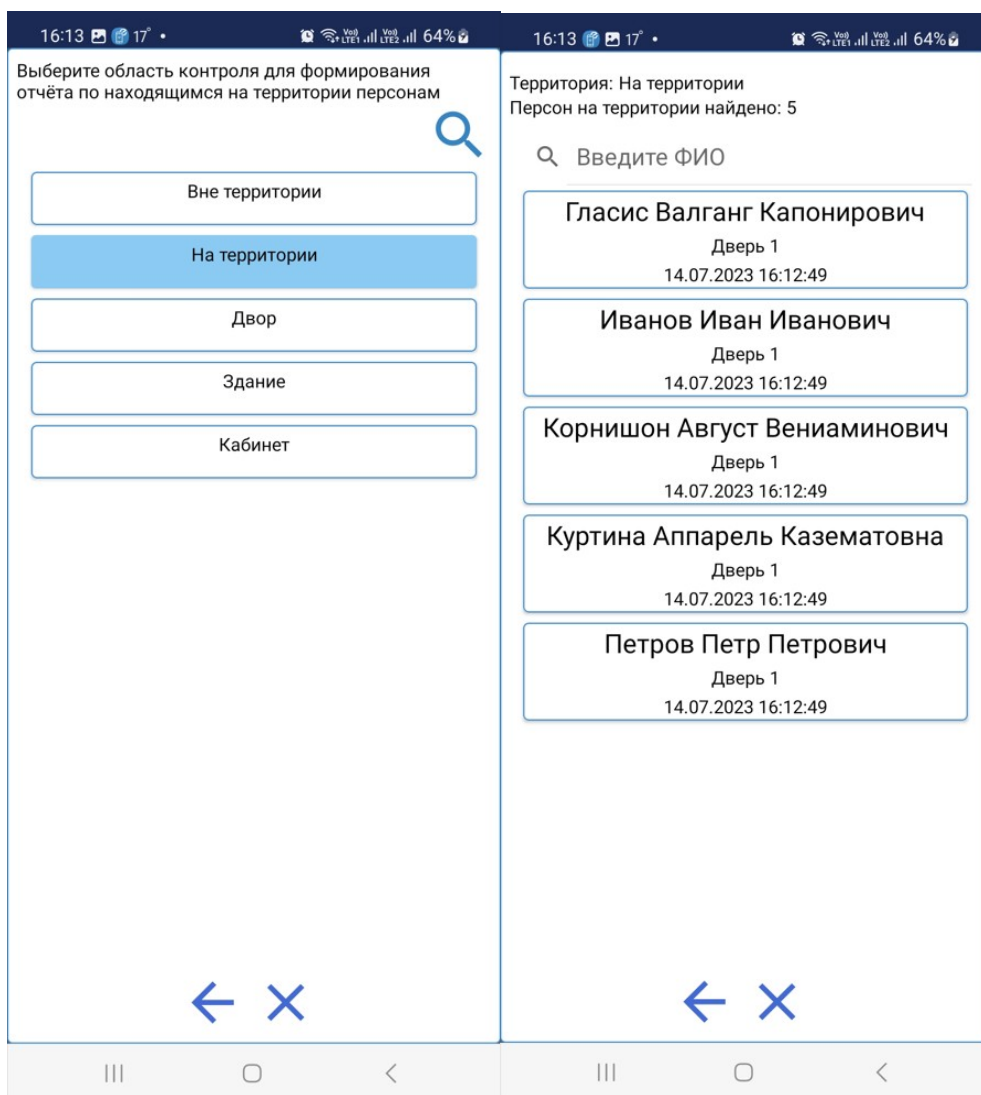


Рис. 25. Поиск персон на территории

Для поиска персон необходимо выбрать территорию и начать поиск персон. По результату поиска в списке отобразятся найденные персоны на выбранной территории. После выбора интересующей персоны откроется фрагмент с краткой информацией о персоне и её фотография ().

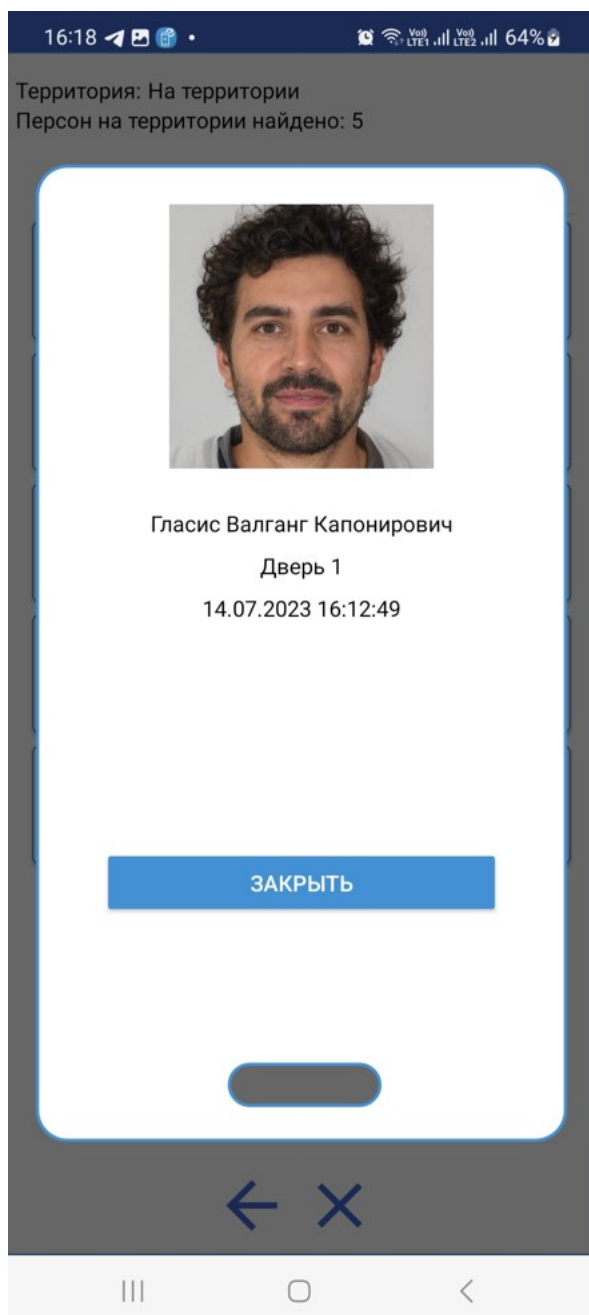


Рис. 26. Информация о персоне на выбранной территории

3.11 Управление привязанными точками прохода

Начиная с версии драйвера 2.1 в мобильном клиенте появилась возможность отправления с мобильного клиента команд управления точками прохода, которые привязаны к мобильной точке доступа, на драйвер (Рис. 27).

Внимание! Эта функция активируется на мобильном приложении только при подключении к драйверу «Бастион-3 – Elsys Mobile» версии 2.1 с ПК «Бастион-2/3».

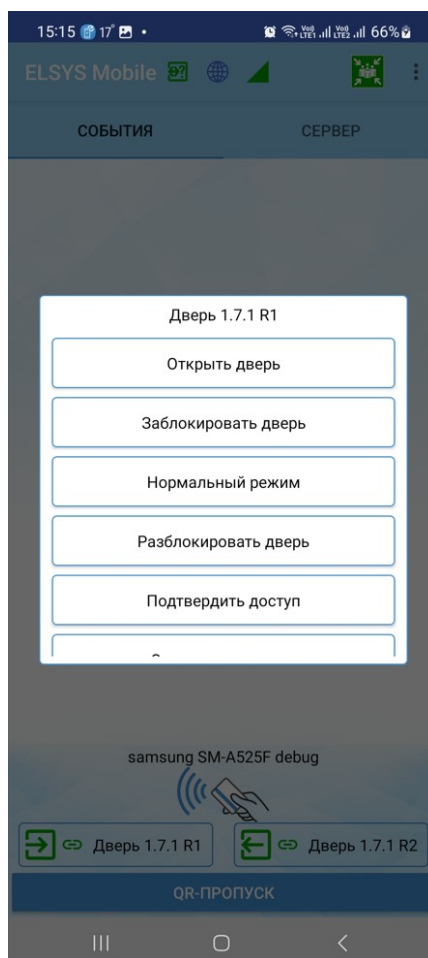


Рис. 27. Окно выбора команды управления

Окно выбора команд управления открывается по нажатию на кнопки с названием соответствующей точки проход в нижней части экрана. В открывшемся окне будет предоставлен полный список команд, которые поддерживает привязанная к мобильной точки доступа точка прохода. По нажатию на необходимую команду управления мобильный клиент отправит команду управления на драйвер, а драйвер отправит команду на сервер оборудования. В случае успеха мобильный клиент сообщит об этом сообщением «Команда управления отправлена». В противном случае отобразится диалоговое окно с текстом ошибки.

3.12 Цветовые профили событий сервера системы

Начиная с версии драйвера 2.1 в мобильный клиент использует цветовые профили событий сервера системы, которые настраиваются в Панели управления ПК «Бастион 3».

Внимание! Эта функция активируется на мобильном приложении только при подключении к драйверу «Бастион-3 – Elsys Mobile» версии 2.1 с ПК «Бастион-2/3».

При каждой авторизации оператора мобильный клиент запрашивает профили событий сервера системы. Так же после каждого изменения профилей событий в Панели управления ПК «Бастион-2/3» драйвер мобильного клиента синхронизирует изменения с активными мобильными клиентами. Палитра цветов используется в соответствии с настроенной на Андроиде темой оформления (Рис. 28)

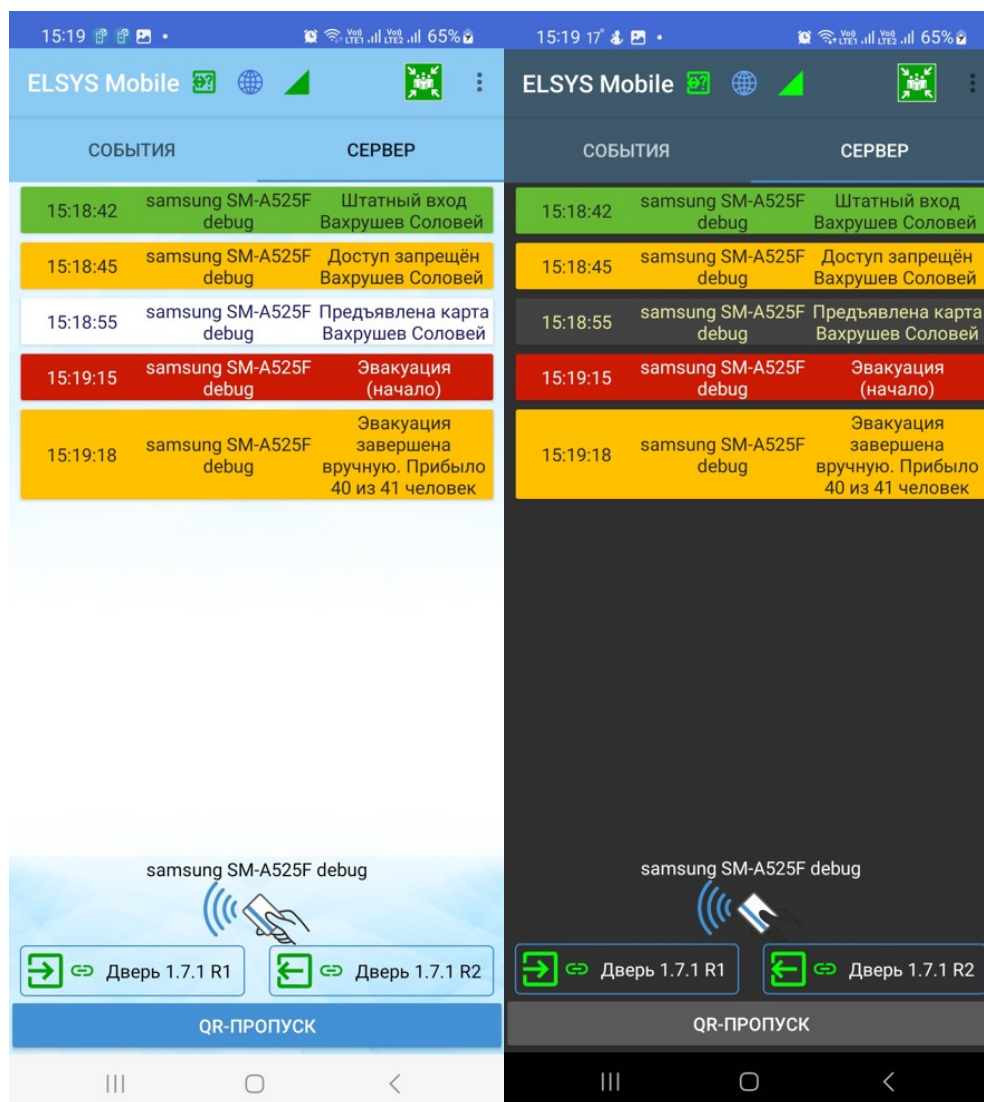


Рис. 28. Цветовые профили событий

3.13 Журнал событий мобильного клиента

Мобильный клиент во время своей работы ведёт журнал событий в виде текстового документа. Текстовый документ записывается в файл log.txt в директории: «\Внутреннее хранилище\Android\data\ru.twinpro.mobilerreader\cache». ОС Android может запретить доступ к директории кеша с самого смартфона, поэтому доступ к файлу можно получить при помощи подключения к компьютеру по USB. Дополнительно, лог-файлом можно поделиться непосредственно из настроек, отправив файл в любое место, предоставляемое ОС Android: почта, мессенджеры и др.

3.14 Статистика используемых данных

В главных настройках мобильного приложения можно посмотреть подробную информацию о занимаемом месте в памяти смартфона. Предоставляется информация о размере схем локальной базы данных приложения, о количестве записей в каждой таблице и о размере медиа-файлов (Рис. 29).

Информация о локальных данных	
settings_database	72,2 KiB
access_levels_database	68,2 KiB
cards_database	48,1 KiB
events_database	422,3 KiB
control_pass	3,1 MiB
car_passes_database	64,2 KiB
mat_values_database	522,9 KiB
person_notifications	60,2 KiB
card_code_formats_data base	52,1 KiB
mifare_profile_table	80,3 KiB
message_profile_table	281,5 KiB
Персональные карты	0
Уровни доступа	0
Временные блоки	0
Праздничные дни	0
События	5
Персоны на эвакуацию	41
Транспортные пропуска	0

Рис. 29. Информация о локальных данных

3.15 Демонстрационный режим

Демонстрационный режим предназначен для предоставления функционала мобильного приложения без необходимости подключения к драйверу Elsys Mobile. Данный режим запускается из экрана авторизации по нажатию на кнопку «Демо-режим» (Рис. 2). В данном режиме все события получают из заранее сгенерированного сценария демонстрации. В базе хранятся данные о трех персонах с номерами карт «000000000001», «000000000002» и «000000000003». QR-пропуска для них представлены на Рис. 30.



Рис. 30 Демонстрационные QR-пропуска

3.16 Мобильная точка досмотра

Начиная с версии Бастиона и драйвера 2024.1 появился функционал для взаимодействия с установленным модулем «Бастион 3 — Досмотр».

Мобильный клиент способен считать QR-код материально-транспортных пропусков. Так же для удобства есть возможность найти материальный или транспортный пропуск вручную, введя номер пропуска. Для поиска транспортных пропусков поиск производится дополнительно по номеру ТС.

После считывания или поиска номера материального или транспортного пропуска мобильный клиент выводит информацию о текущей персоне-владельце пропуска. Порядок отображения вкладок с информацией зависит от типа считанного пропуска, если был предоставлен материальный пропуск, то на первом месте отображаются все материальные пропуска с выделением того пропуска, на втором месте транспортные пропуска и на последнем месте информация о персоне владельце, аналогично для считывания транспортных пропусков (Рис. 31).

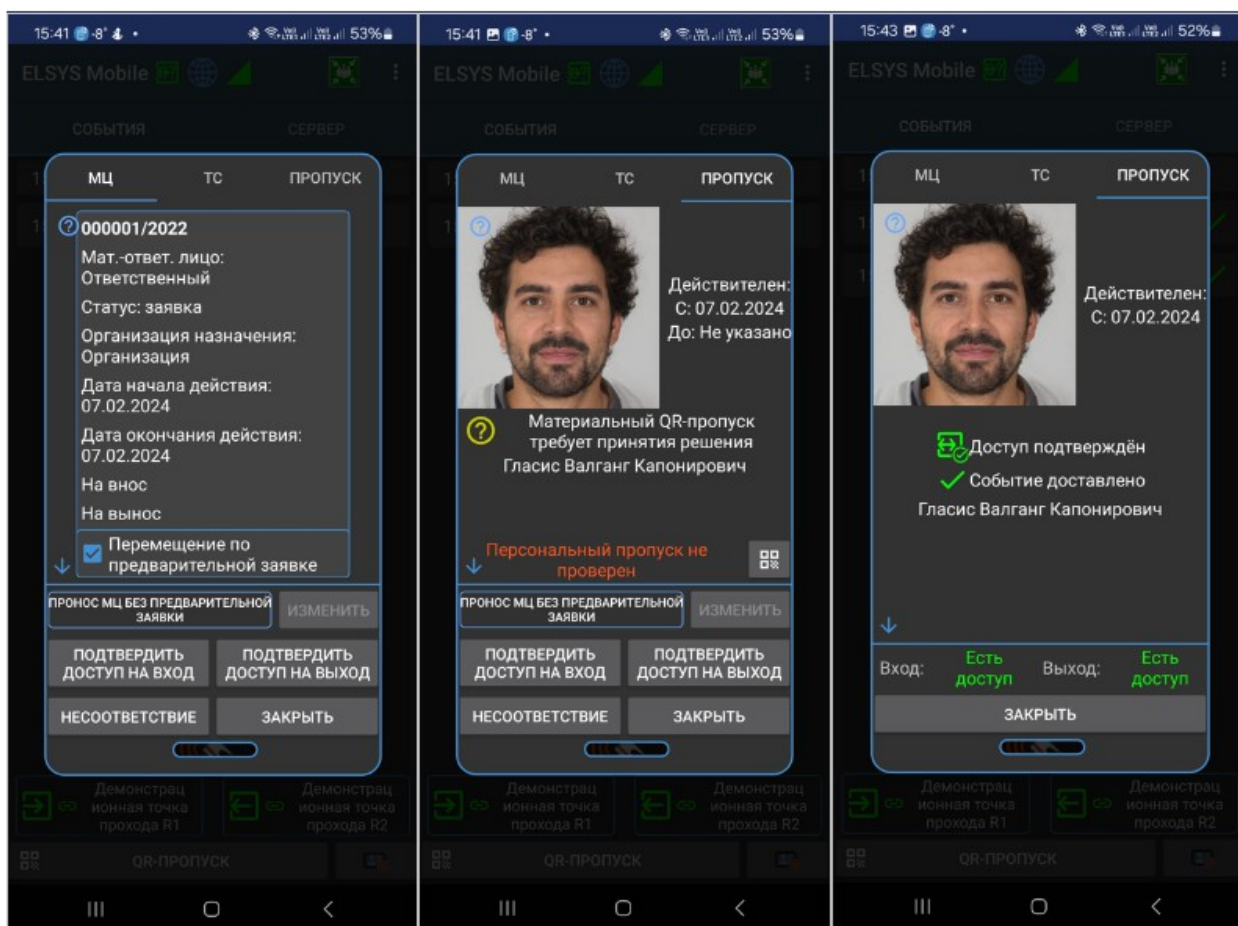


Рис. 31 Информация о считанном материальном пропуске



После считывания материального пропуска оператор может заполнить форму перемещения материальных ценностей без предварительной заявки. Для этого необходимо активировать «Пронос МЦ без предварительной заявки» и нажать на кнопку «Изменить». Откроется форма, на которой можно произвести фиксирование накладной на материальные ценности через фотографирование и заполнение полей ввода необходимой информацией.

Для подтверждения персонального пропуска владельца необходимо считать номер персонального пропуска имеющимися способами: считав карту доступа или сканировать QR персонального пропуска. При совпадении пропуска владельца МТП и персонального пропуска у события на мобильном клиенте появится статус подтверждения пропуска. Дополнительно оператор может вручную указать несоответствие персонального, транспортного или материального пропуска.

Если мобильная точка привязана к точкам прохода, то оператор может предоставить доступ МТП на вход и/или выход.

Мобильный клиент подтверждает только те проходы МТП, которые имеются в модуле «Бастион-3 — Досмотр». При подтверждении или отклонении мобильным оператором прохода МТП драйвер Elsys Mobile выполняет поиск актуальных нерешенных проходов в модуле Досмотр и выполняет операцию подтверждения или отклонения найденного прохода. В приложении «Бастион-3 — Пост охраны» в открытых окнах согласования доступа МТП подтверждение или отклонение будет невозможным, так как решение было принято на другом устройстве мобильного клиента. В этом случае в Посте охраны будет выведено соответствующее сообщение и окно согласования будет закрыто.

После принятия решения о предоставлении доступа материально-транспортному пропуску локальные события мобильного клиента будут иметь следующие статусы:

	Доступ материально-транспортного пропуска подтвержден
	Зафиксировано нарушение перемещения материальных ценностей.

В случае отсутствия соответствующего нерешенного прохода в модуле Досмотра мобильный клиент выведет сообщение, что такого прохода МТП не было найдено и событие подтверждения не будет сохранено.



Приложения

Приложение 1. История изменений

1.5 (07.02.2024)

- [+] Добавлена совместимость с версией ПК «Бастион-3» 2024.1.
- [+] Добавлен функционал для взаимодействия с установленным модулем «Бастион 3 — Досмотр».
- [+] Добавлен ручной поиск МТП пропусков (при наличии установленного модуля «Бастион 3 — Досмотр»).
- [+] Добавлена поддержка 7 и 8 байтовых кодов карт.
- [+] В приложении добавлена справочная информация о возможностях клиента Elsys Mobile.
- [*] Адаптация вывода длинных ФИО персон (по 100 символов).
- [*] Проведена адаптация графического интерфейса под различные размеры экранов устройств и другие визуальные доработки.

1.4 (25.01.2024)

- [+] Добавлена совместимость с версией ПК «Бастион-3» 2023.3.

1.4 (19.09.2023)

- [+] Добавлена возможность работы с картами Mifare в защищённом режиме.
- [+] Добавлена возможность управления привязанными точками прохода стационарной СКУД.
- [+] При отображении событий используются цвета из цветовой схемы Бастиона.
- [+] Добавлена возможность просмотра отчёта о находящихся на территории.
- [+] Добавлена индикация скорости загрузки данных.
- [*] Проведена оптимизация работы системы в различных режимах.