Бастион 2 – Elsys Mobile. Руководство оператора мобильного клиента

Версия 1.3

(25.08.2022)

Самара, 2022

Оглавление

1 Общие сведения

1.1 Назначение и область применения

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

Ключевые возможности системы включают:

1. Считывание карт доступа на мобильных устройствах через NFC с регистрацией событий в АПК «Бастион-2».
2. Считывание QR-кодов, выдаваемых в АРМ «Бюро пропусков» АПК «Бастион-2» 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 оффлайн режима работы. В онлайн-режиме для полноценной работы системы требуется наличие связи с сервером АПК «Бастион-2». В оффлайн режиме вся БД пропусков скачивается на мобильное устройство. Оператор мобильного терминала имеет возможность видеть все сведения о пропуске, проверять его полномочия и регистрировать события даже при отсутствии связи с АПК «Бастион-2». При восстановлении связи все накопленные события передаются на сервер АПК «Бастион-2».
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 АПК «Бастион-2» 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 АПК «Бастион-2».
16. Возможность подключения к мобильной точке внешних считывателей ELSYS-SW-USB и ELSYS-PW-USB-NFC через USB-порт для возможности считывания не только карт доступа семейства Mifare.
17. Настройка форматов порядка байт кода карты для различных типов карт доступа

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.

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 *BastionMobileReader.apk*.

При первом запуске приложения будут запрошены следующие права:

1. Съемка фото и видео. Это право необходимо для съемки 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. Пиктограмма запуска приложения Elsys Mobile

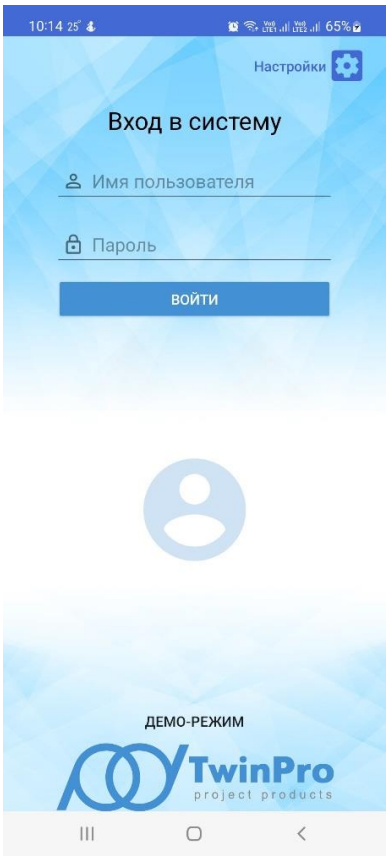

Рис. 2. Окно ввода учетных данных для подключения

Приложение использует общую с АПК «Бастион-2» систему авторизации, то есть логин и пароль для приложения – это имя и пароль операторов в АПК «Бастион-2». Для доступа к мобильному приложению у операторов АПК «Бастион-2» 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.

3.2 Настройка параметров приложения

3.2.1 Основные настройки

Для настройки подключения к серверу необходимо указать строку подключения (Рис. 3). При этом мобильный терминал должен быть зарегистрирован в модуле «Бастион 2 – Elsys Mobile». Адрес сервера состоит из трех частей: протокол соединения (HTTP или HTTPS в зависимости от выбранного на сервере режима), адрес сервера и порт. Пример правильной строки подключения к серверу изображен на Рис. 3.

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

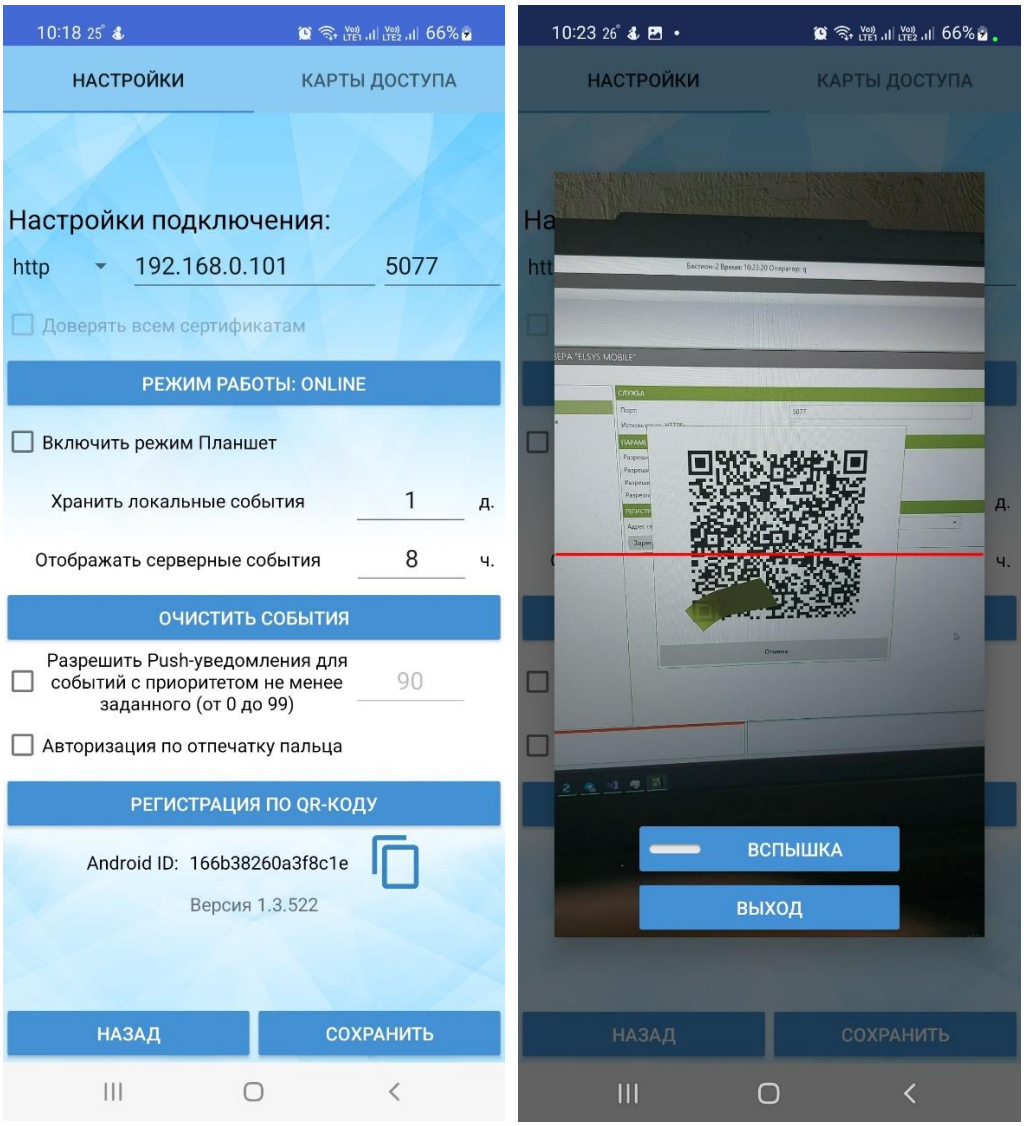

Рис. 3. Настройка строки подключения к серверу

Зарегистрировать устройство и получить параметры подключения к серверу проще всего через QR-код. Для этого на компьютере необходимо открыть конфигуратор «Бастион 2 – 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» (Рис. 3) и навести камеру телефона на QR-код, отображаемый на компьютере. Мобильный терминал будет зарегистрирован в системе, а «Настройки подключения» будут заполнены 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 АПК «Бастион-2» 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 АПК «Бастион-2». Регистрация событий возможна и без наличия подключения, но на терминале не будут отображаться параметры пропуска. При восстановлении связи возможна передача событий в АПК «Бастион-2» и уточнение их параметров.

В режиме *Offline* все сведения о пропусках сразу загружаются из АПК «Бастион-2» 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 АПК «Бастион-2» 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».

Включить режим «Планшет». Альтернативный вид пользовательского интерфейса для отображения всей информации о пропуске на одном экране.

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.

Разрешить push-уведомления о событиях с приоритетом не менее заданного. Позволяет отображать высокоприоритетные события, получаемые с сервера АПК «Бастион-2» 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 Бастион 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.

3.2.2 Настройки карт доступа

Дополнительно в приложении можно задать настройки для карт доступа (Рис. 4).

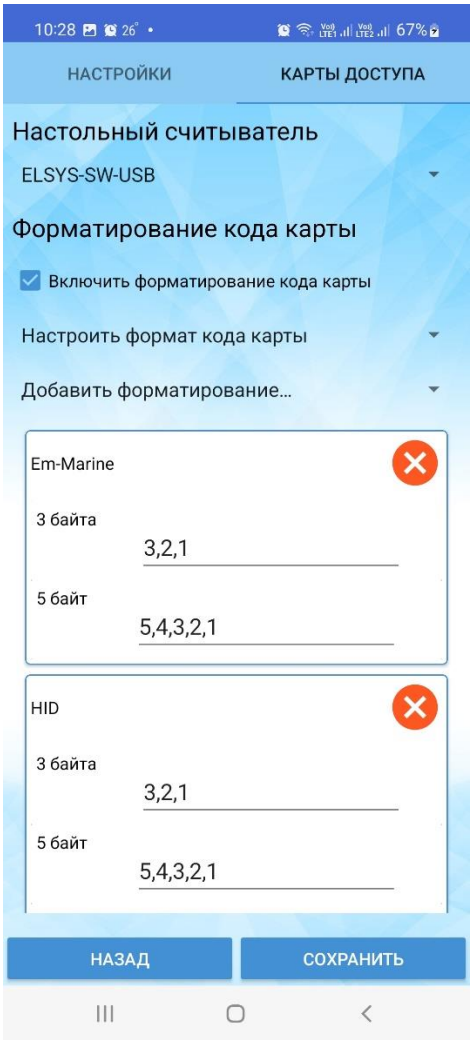

Рис. 4. Настройки карт доступа

В данном разделе можно выбрать какой внешний USB-считыватель будет подключаться к мобильному устройству. На выбор даются считыватели ELSYS-SW-USB и ELSYS-PW-USB-NFC. USB-

считыватели подключаются через OTG-кабель. Общение мобильного приложения со считывателями происходит по серийному порту.

Настройки форматирования кода карты представлены следующими параметрами:

1. *Включить форматирование кода карты* – при активной настройке будут браться форматы из заданных шаблонов, если шаблонов нет или параметр не активен, то используются шаблоны по умолчанию.
2. «Использовать формат по умолчанию» или «Настроить формат кода карты» - берутся заданные форматы порядков, если они есть, или берутся форматы по умолчанию.
3. Добавить форматирование – по нажатию на компонент открывается выпадающий список возможных типов карт доступа, по нажатию на которые в настройках появляется шаблон форматов для данной карты.

Шаблон форматов для карты доступа представляет из себя компонент с вложенным списком масок порядка кода карты для определенной длины кода карты. Маска состоит из набора цифр порядкового номера байта кода карты, разделенными между собой запятыми.

Для удобства настройки карт доступа на форме настроек можно проверить коды карт с учетом всех настроенных параметров форматирования. Для этого можно включить NFC-модуль мобильного устройства или подключить внешний USB-считыватель и считать карту доступа. После считывания откроется диалоговое окно с результатами кода карты, которые будут использоваться в дальнейшем в системе АПК «Бастион-2» (Рис. 5).

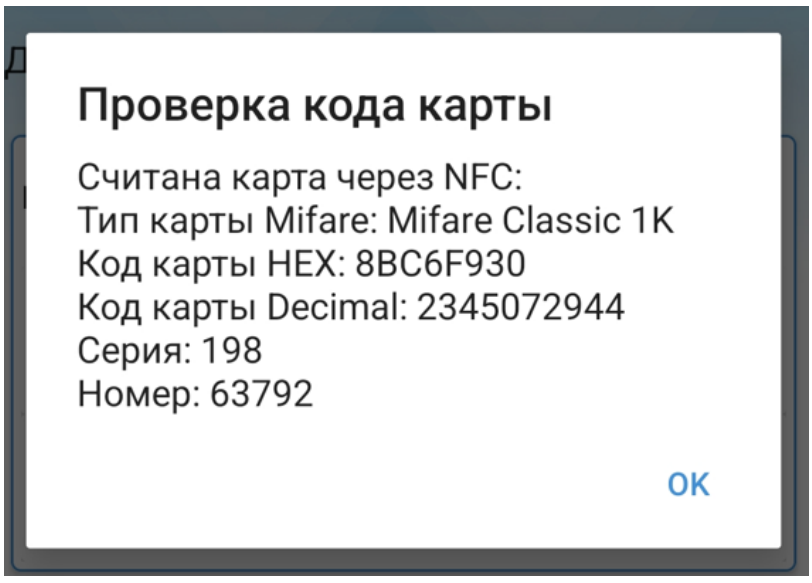

Рис. 5. Проверка кода считанной карты на форме настроек

3.3 Работа в режиме считывания карт доступа

3.3.1 Основное окно приложения

В основном окне приложения отображается ряд элементов, обозначенных на Рис. 6.

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 АПК «Бастион-2».

Область 4 – вызов меню.

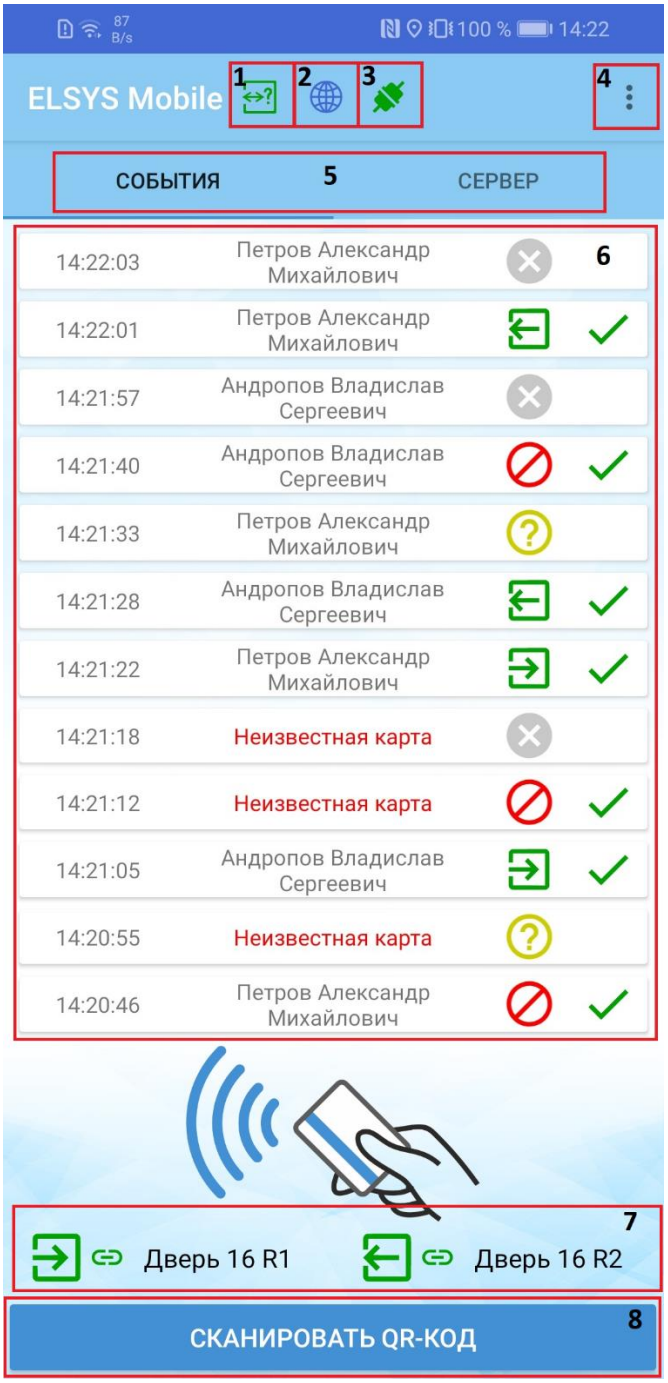

Рис. 6. Основное окно приложения

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 АПК «Бастион-2».

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. 6.

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

Если в верхней части экрана появится значок, обозначенный на Рис. 7, 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. 7. Предупреждающая иконка выхода из ограниченной зоны местоположения.

Статус активного подключения к внешнему USB-считывателю обозначается специальной иконкой (Рис. 8).

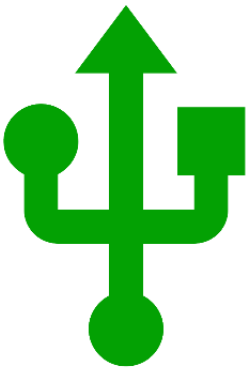

Рис. 8. Статус активного подключения с USB-считывателем

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 АПК «Бастион-2» 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 вход
	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 АПК «Бастион-2». Оператору отображается окно в форме карты доступа с загруженными параметрами пропуска, включая фотографию (Рис. 9). 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. 9 системой сформировано событие «Доступ запрещен», так как у владельца предъявленной карты нет прав на выход через данный мобильный терминал.

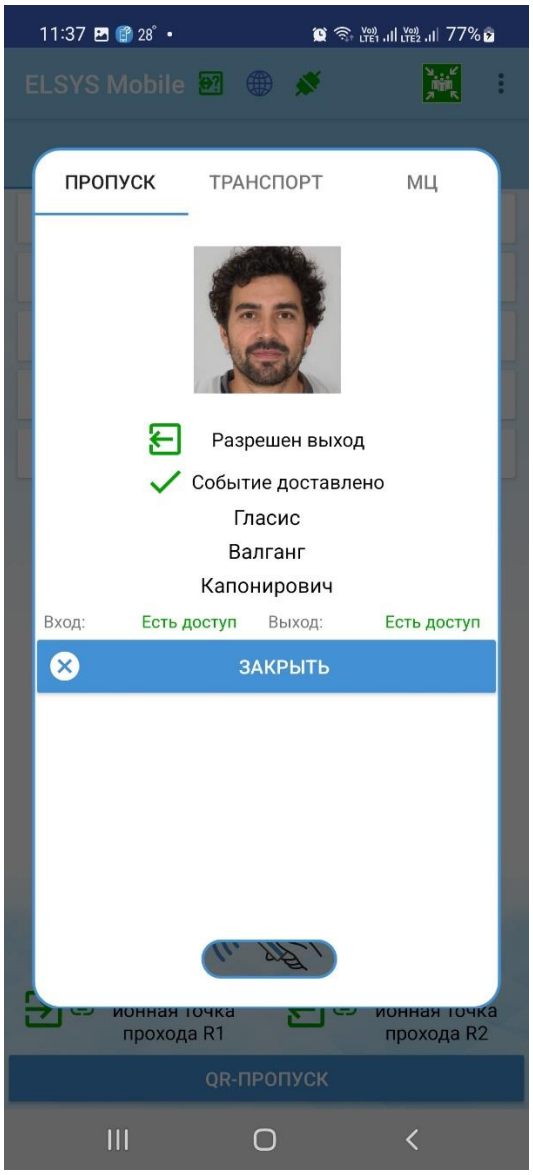

Рис. 9. Считывание карты в режиме «Всегда выход»

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. 10).

Оператор может выполнить следующие действия до отправки события:

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

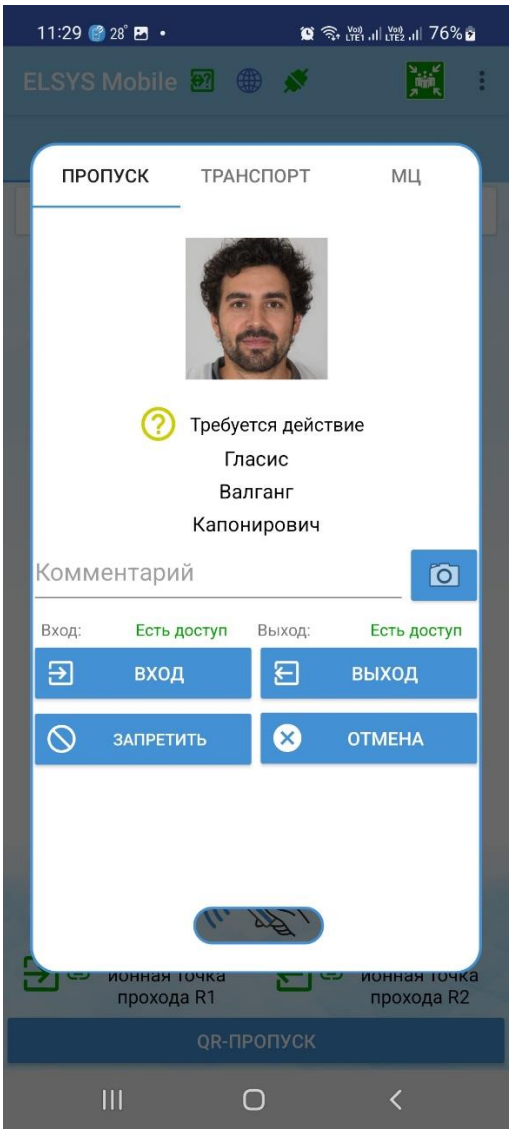

Рис. 10. Считывание карты в режиме «С подтверждением»

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. 10).
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.

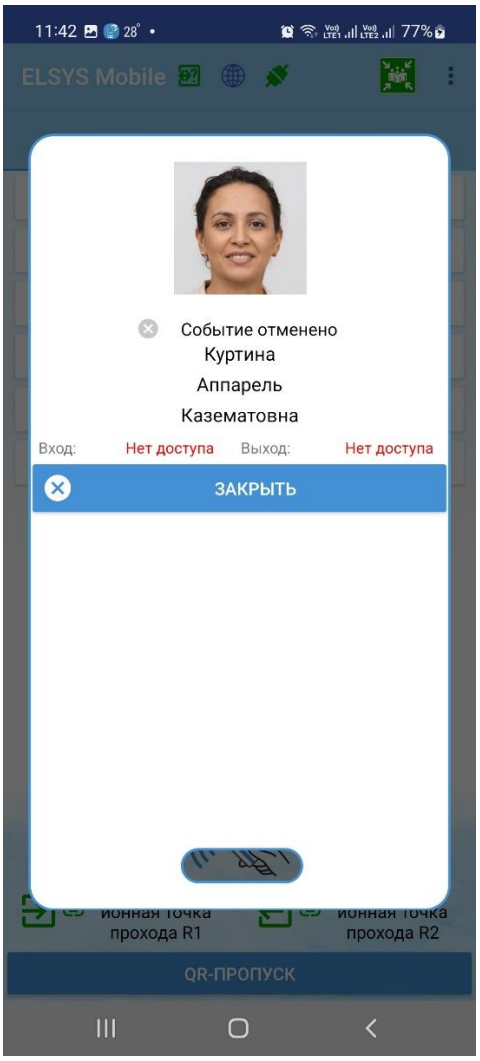

Рис. 11. Окно с результатом обработки предъявленной карты

После нажатия на одну из кнопок, описанных выше, окно регистрации события примет вид, представленный на Рис. 11 или Рис. 12.

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

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

На Рис. 12 рядом с фотографией владельца пропуска из АПК «Бастион-2» отображается фотография события, сделанная оператором мобильного терминала.

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

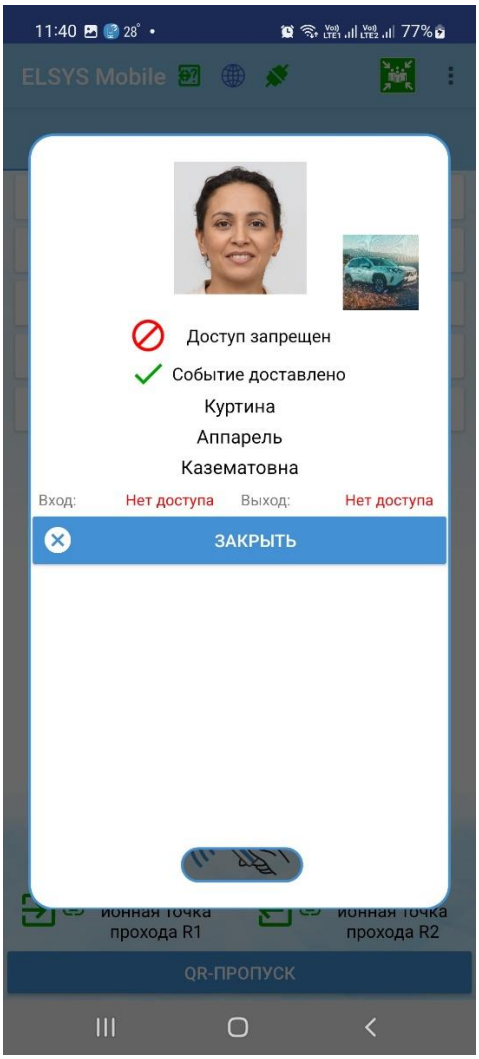

Рис. 12. Окно с результатом обработки предъявленной карты с фотографией события

3.3.5 Работа в режиме «Без регистрации»

В режиме без регистрации событий (Рис. 13) никакие события не передаются в АПК «Бастион-2». Мобильный терминал используется только для проверки прав доступа.

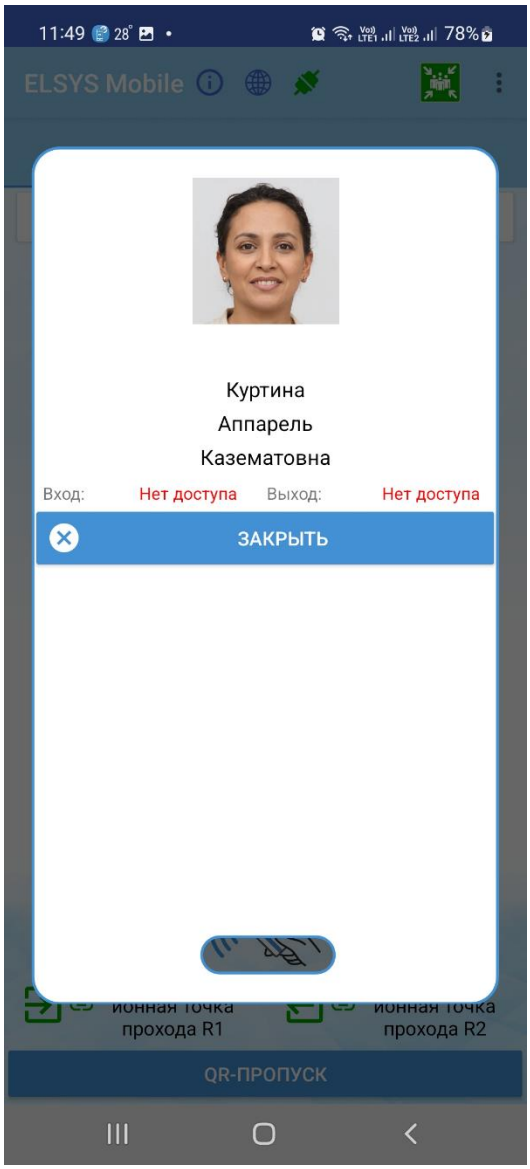

Рис. 13. Считывание карты в режиме «Без регистрации»

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» АПК «Бастион-2». 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. 13). 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 АПК «Бастион-2» нет, то поведение терминала зависит от режима его работы – онлайн или оффлайн.

Отсутствие связи с сервером АПК «Бастион-2» индицируется красной пиктограммой разорванного соединения в верхней части основного экрана приложения (Рис. 14).

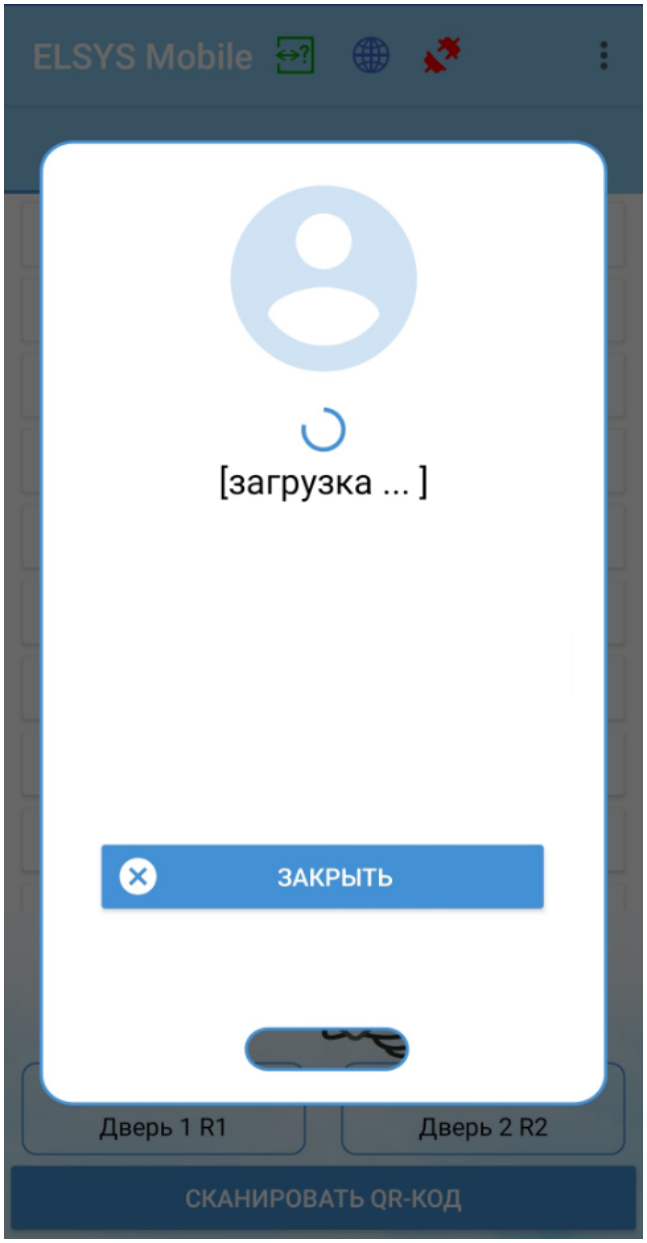

Рис. 14. Попытка загрузки данных без связи с сервером в онлайн режиме

В режиме «Онлайн» терминал не хранит БД пропусков, поэтому сведения о пропуске не будут отображены при предъявлении карты доступа (Рис. 14). Тем не менее, в этом режиме терминал все равно сохраняет события предъявления карт доступа локально. При восстановлении связи с сервером АПК «Бастион-2» оператор может уточнить параметры каждого события, нажав на это событие в списке событий (Рис. 15). События, возникшие без связи с сервером, в этом случае будут отображаться в виде строки с надписью «[загрузка…]».

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

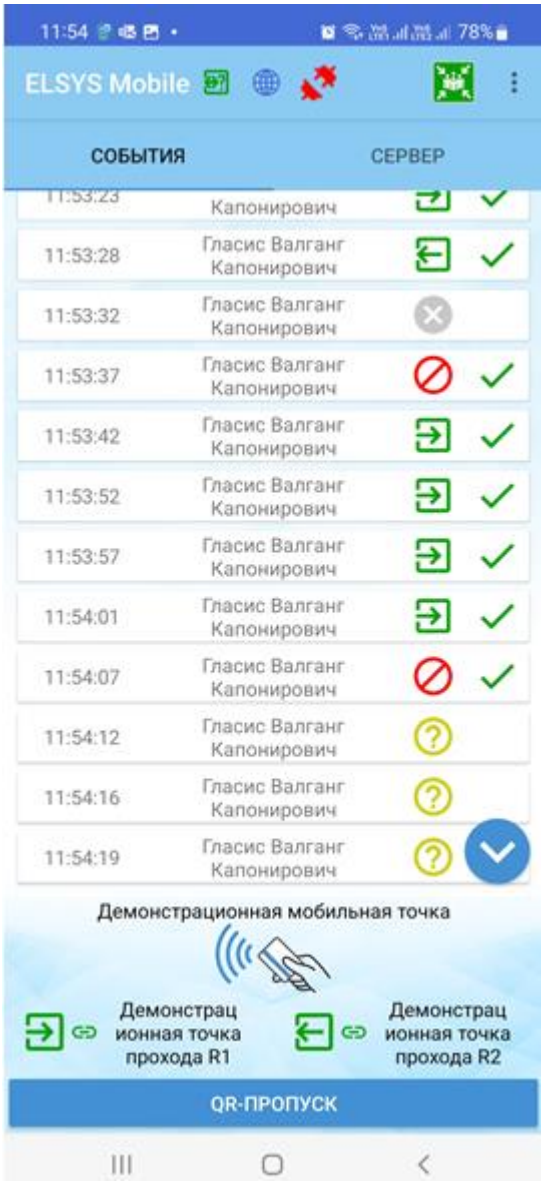

Рис. 15. Отображение событий в онлайн режиме без связи с сервером

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. 16).

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).

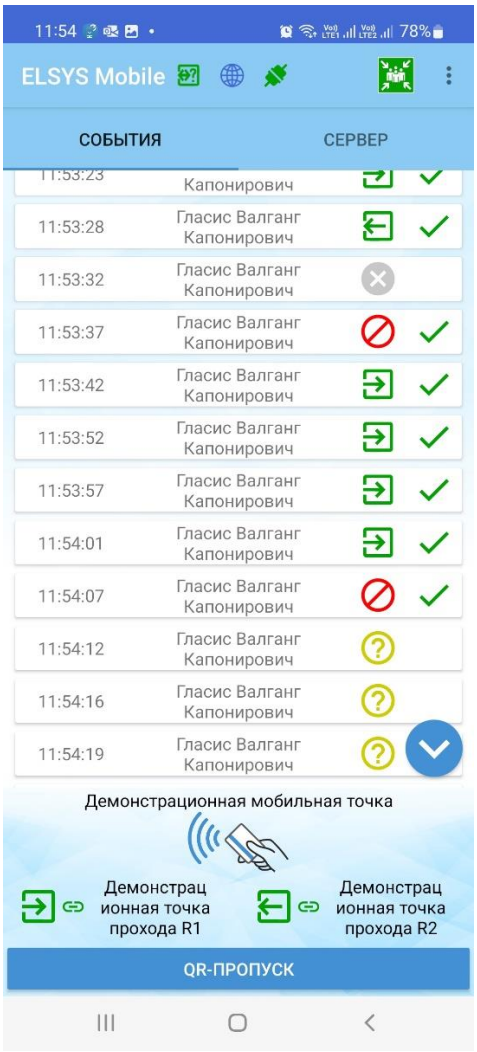

Рис. 16. Основное окно приложения в режиме мониторинга собственных событий

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 АПК «Бастион-2».
	Требуется действие со стороны оператора мобильного терминала.
	Событие успешно передано на сервер АПК «Бастион-2».

3.4.2 Мониторинг событий других устройств СКУД

Мобильный терминал обеспечивает отображение событий, загруженных с сервера АПК «Бастион-2». 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. 17). По умолчанию отображаются события за последние 8 часов (задается в настройках мобильного терминала).

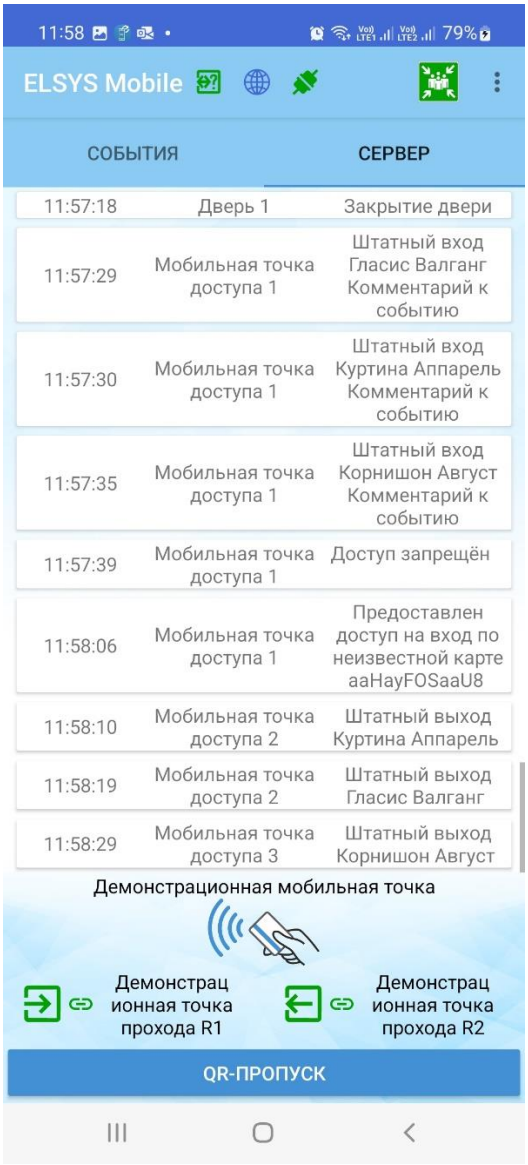

Рис. 17. Основное окно приложения в режиме мониторинга событий других устройств СКУД

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 отметилось 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 АПК «Бастион-2» отправляется специальное событие – «Прибыл в место сбора при эвакуации ФИО».

Если пытается отметиться человек, не из списка эвакуируемых - он учитывается отдельно (В АПК «Бастион-2» 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 АПК «Бастион-2» 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 АПК «Бастион-2» будет отправлено событие «Эвакуация завершена вручную», с указанием сколько человек не были отмечены.

В генераторе отчетов АПК «Бастион-2» 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 эвакуаций» в мобильном приложении в верхней части экрана загорится иконка (Рис. 18).

Рис. 18. 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. 19.

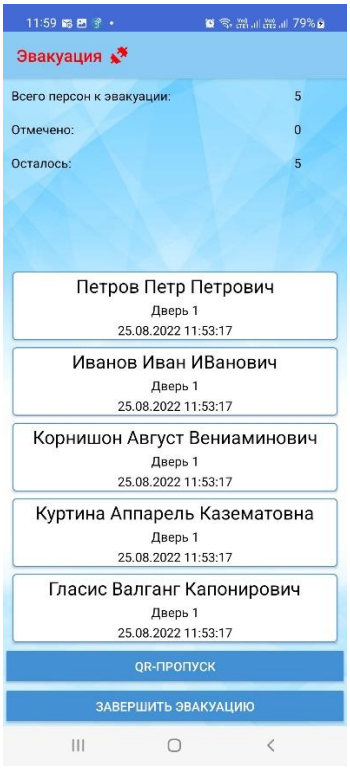

Рис. 19. Интерфейс режима «Точка сбора при эвакуации»

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 АПК «Бастион-2», 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. 20).

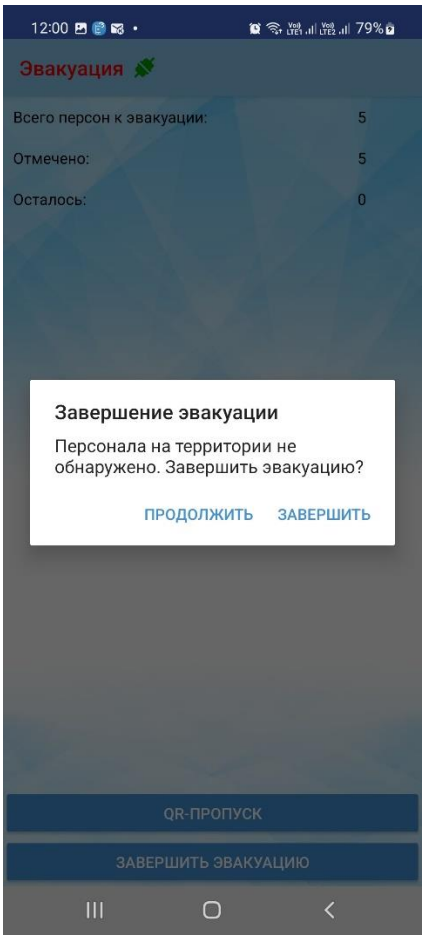

Рис. 20. Завершение эвакуации

При завершении эвакуации драйвер выведет соответствующее сообщение в АПК «Бастион-2».

Оператор так же может завершить эвакуацию вручную, если нет возможности ждать оставшихся сотрудников, в таком случае в АПК «Бастион-2» 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-2 – Elsys Mobile» версии 1.2 с АПК «Бастион-2» 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. 21).

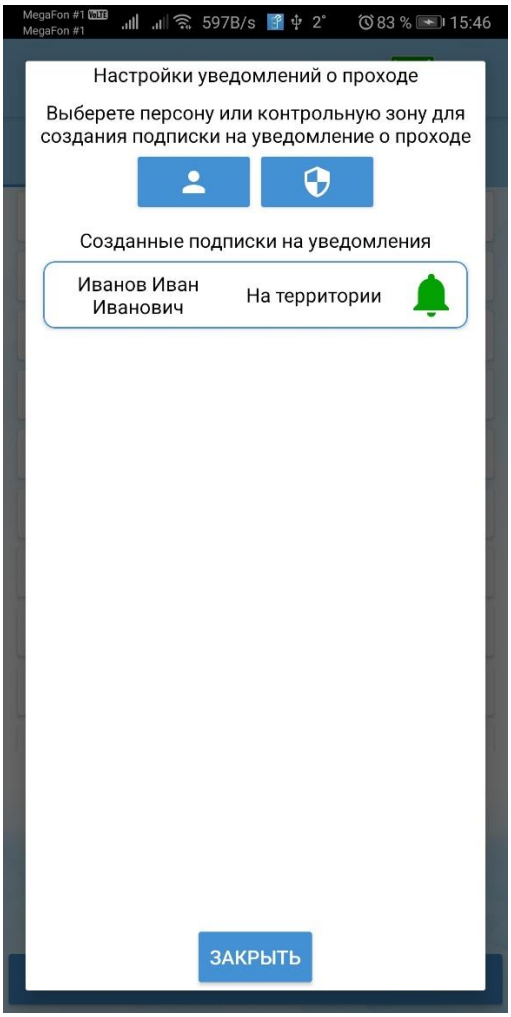

Рис. 21. Настройка уведомлений о проходе лиц

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:

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

	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. 22).

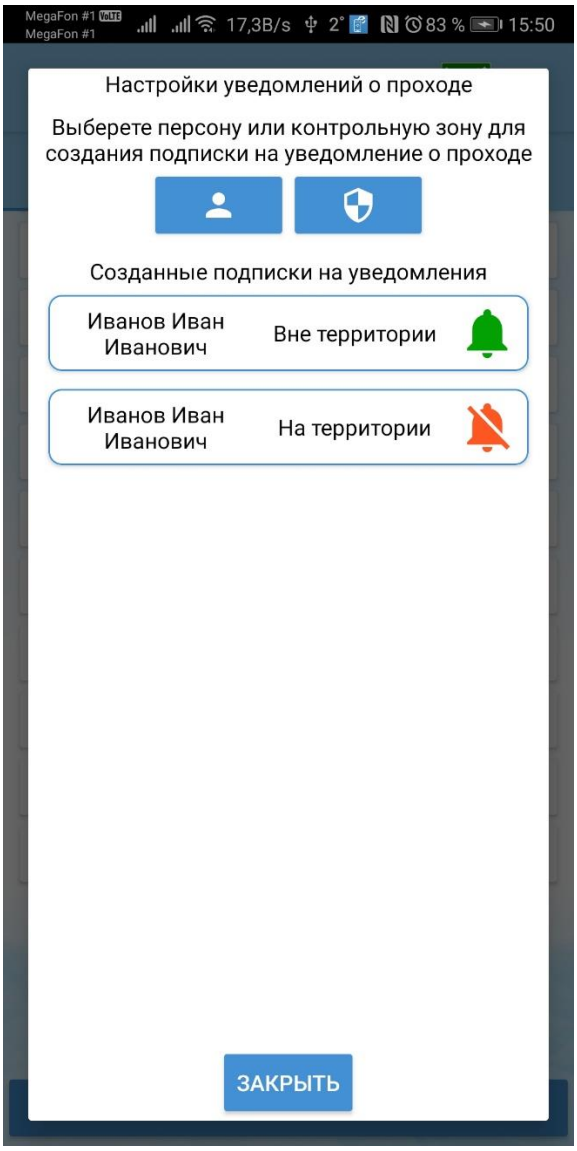

Рис. 22. Созданные подписки на уведомления

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 Интеграция с производственным планшетом

Приложение поддерживает работу со специальным встроенным модулем STLF Low Frequency Moddel C 125 kHz. Данный модуль позволяет читать мобильным устройством карты семейства Em-

Marine. За подробной информацией о данном планшете необходимо обращаться у производителей мобильного приложения Elsys Mobile.

3.8 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» (**Ошибка! Источник ссылки не найден.**). В данном режиме все события получаются 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. 23**Ошибка! Источник ссылки не найден.**.

Рис. 23 Демонстрационные QR-пропуска