



Бастион-2 — АРМ Бюро пропусков
Работа с картами Mifare в защищенном режиме
Быстрый старт



Самара, 2020

1 Общие сведения

В данной инструкции кратко рассмотрена настройка системы контроля и управления доступом и модуля «Бастион-2 - АРМ Бюро пропусков» для работы с картами Mifare в защищенном режиме.

2 Последовательность действий при настройке

- 2.1 Для работы с картами Mifare подключите к ПК настольный считыватель Elsys-SW-USB-MF, установите драйвер для считывателя. Драйвер можно скачать со страницы www.trevog.net/support/software.
- 2.2 Скачайте со страницы www.trevog.net/support/software утилиту MFMasterCard для создания мастер-карт. Распакуйте архив, запустите файл MFMasterCard.exe (рис. 1).

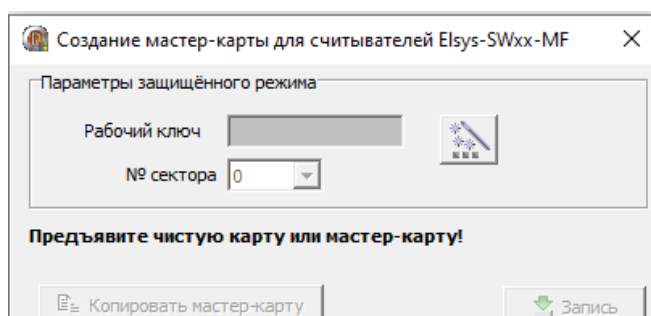



Рис. 1. Окно утилиты MFMasterCard

- 2.3 Поднесите к настольному считывателю чистую карту Mifare. Затем задайте параметры защищённого режима – номер сектора (диапазон значений 0...15), который будет использоваться для эмиссии карт и рабочий ключ, который будет использоваться для чтения и записи защищённой области памяти. Рабочий ключ – это шестнадцатеричное число длиной 6 байт. Чтобы его задать, введите в поле «Рабочий ключ» 12 символов из диапазона «0»...«9», «А»...«F» либо сгенерируйте ключ автоматически нажатием на кнопку  (рис 2).

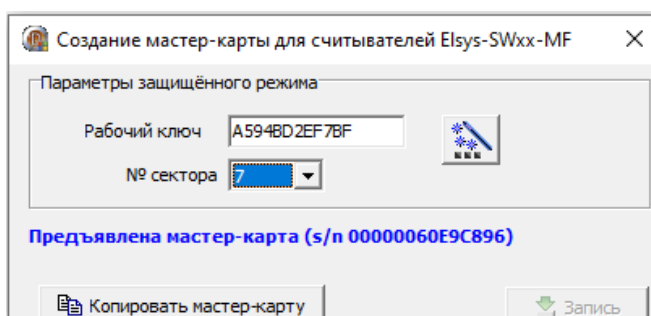


Рис. 2. Создание мастер-карты



Внимание! Мастер-карта является физическим носителем профиля безопасности. Настоятельно рекомендуется создать резервные копии мастер-карты!

При создании и хранении мастер-карты и её копий следует обеспечить необходимые меры безопасности. При утере мастер-карты дальнейшая эксплуатация системы может оказаться невозможной (в частности, будет

невозможна модернизация системы – эмиссия новых карт, программирование новых считывателей и смена ключей в имеющихся считывателях).

- 2.4 Переведите настенные считыватели Elsys-SW20-MF в защищенный режим работы, соединив синий провод (Secure) с общим проводом (GND).
- 2.5 Предъявите мастер-карту к настенным считывателям для записи в них параметров защищенного режима.
- 2.6 Добавьте настольный считыватель в «Бастион-2 – АРМ Бюро пропусков» через меню «Инструменты – Настольный считыватель...» (рис. 3). Утилита MFMasterCard должна быть при этом закрыта.

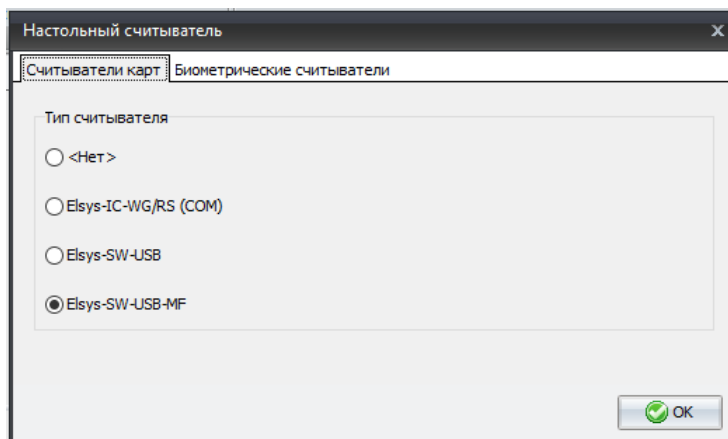


Рис. 3. Добавление настольного считывателя

- 2.7 Перейдите в меню «Общие настройки–Карты доступа». Выберите тип карты «Программируемый номер карты в защищенной области памяти (карты Mifare)» (рис. 4).

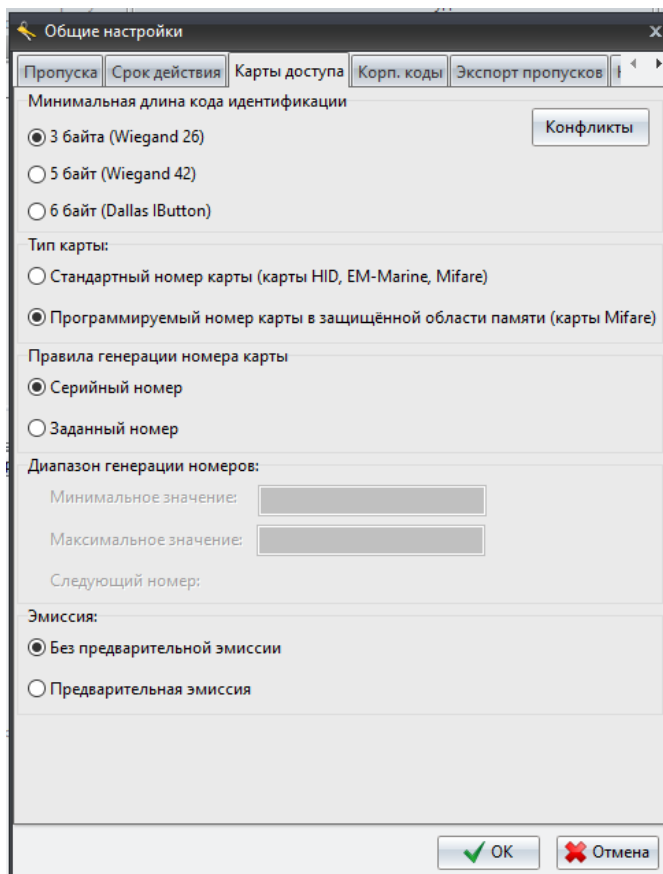


Рис. 4. Настройка правил работы с картами Mifare

Установите правило генерации номера карты в зависимости от требований заказчика.

Правило «Серийный номер» удобно использовать в случае, когда для ввода карт в систему используется настольный считыватель Elsys-SW-USB, не поддерживающий защищённый режим. Пример: эмиссия (выпуск) карт выполняется централизованно с помощью настольного считывателя Elsys-SW-USB-MF, далее эти карты передаются в филиалы, где установлены считыватели Elsys-SW-USB, не поддерживающие программирование карт Mifare, но способные выдавать карты по серийному номеру.

Правило «Серийный номер» можно использовать и в случае, когда в системе предусмотрен оперативный перевод считывателей из защищённого режима в обычный и наоборот (например, в процессе смене профиля безопасности у всех выданных карт).

- 2.8 Установите правила выдачи карт Mifare - без предварительной эмиссии или с предварительной эмиссией.

Эмиссия карты – это запись сформированного по установленным правилам числового идентификатора (номера) в защищённую область памяти карты, с одновременной установкой ключей защиты для доступа к сектору данных.

Режим «Предварительная эмиссия» удобен в случае, когда для ввода карт в систему используется настольный считыватель, не поддерживающий защищённый режим (пример в п. 2.7).

- 2.9 Перейдите в меню «Инструменты - История мастер-карт». Предъявите к настольному считывателю мастер-карту (рис. 5).

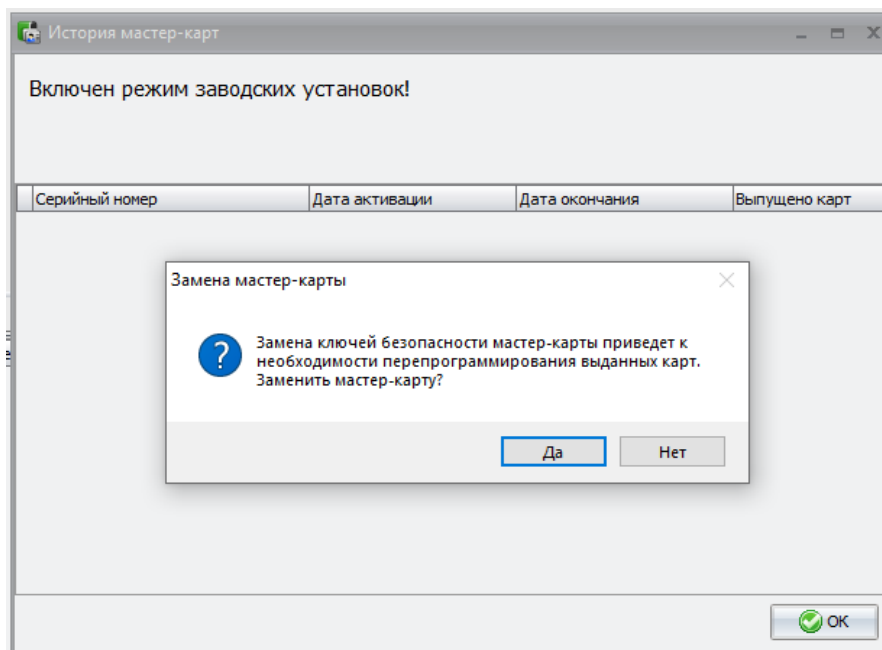


Рис. 5. Добавление мастер-карты

На запрос «Заменить мастер-карту?» выберите ответ «Да», затем введите пароль оператора для подтверждения действия.

Мастер-карта будет добавлена в список (рис. 6). Закройте окно нажатием кнопки «ОК».

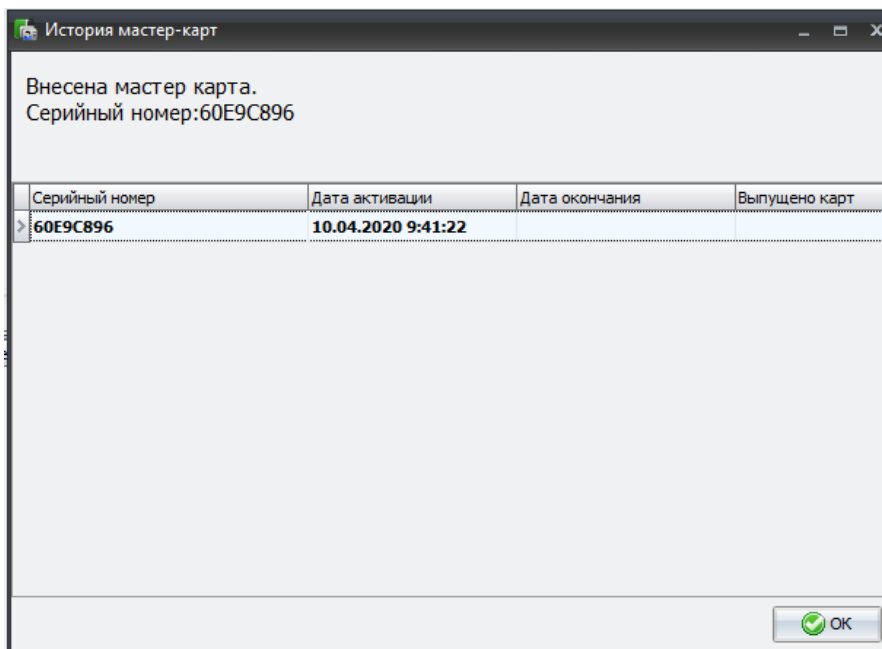


Рис. 6. Мастер-карта добавлена

3 Выдача пропусков

После добавления в систему параметров безопасности мастер карты можно переходить к выдаче пропусков и присвоения им карт доступа Mifare.

- 3.1 Выдача пропусков без предварительной эмиссии карт производится в следующем порядке:
- создать заявку на пропуск;
 - нажать кнопку «Выдать», при этом появится окно «Выдача пропуска» (рис. 7).

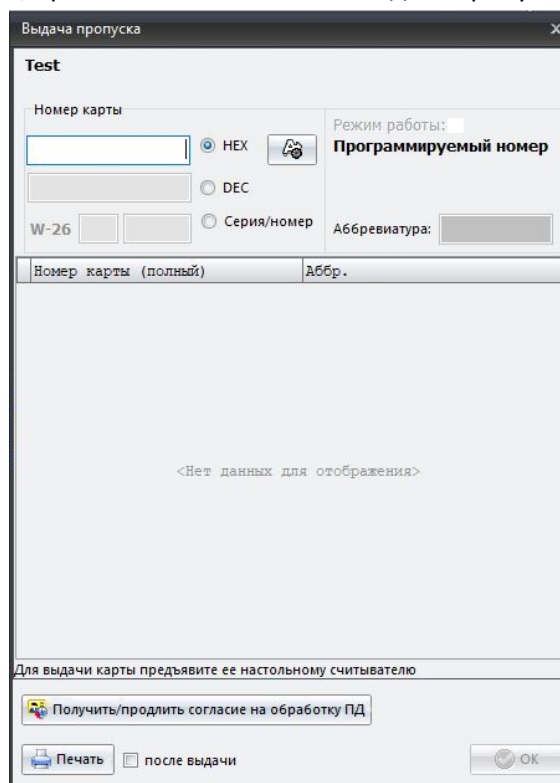


Рис. 7. Окно выдачи пропуска

- приложить к настольному считывателю карту Mifare, находящуюся в транспортном состоянии, после чего произойдет автоматическая эмиссия и выдача карты, номер карты отобразится в списке.

Транспортное состояние карты Mifare – исходное состояние, в котором доступ ко всем секторам карты разрешён с помощью заводских ключей, являющихся общеизвестными.

- 3.2 Предварительная эмиссия карт производится в следующем порядке:

- выбрать режим «Предварительная эмиссия» (см. п. 2.8);
- перейти в меню «Основное – Карты доступа»;

- в панели инструментов окна нажать кнопку



- «Предварительная эмиссия», после чего будет выведено окно с запросом (рис. 8);

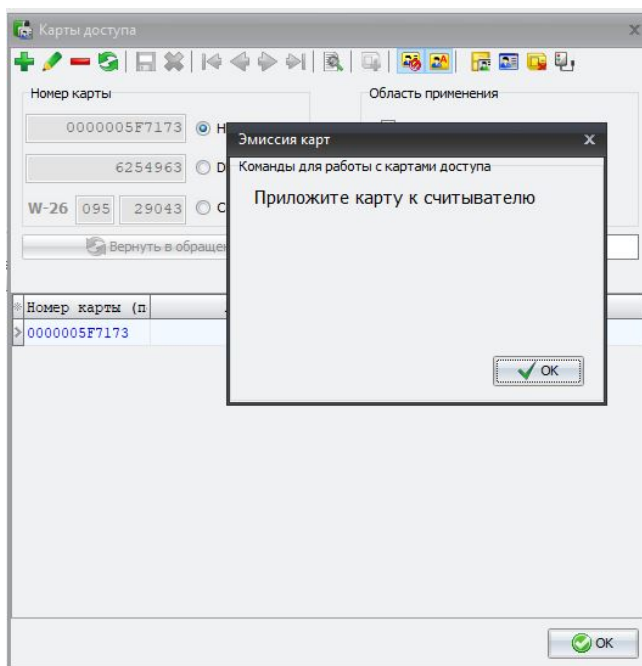


Рис. 8. Окно запроса при эмиссии карты

- приложите к настольному считывателю карту в транспортном состоянии;
- после завершения программирования карты будет выведено информационное сообщение (рис. 9) и можно будет приложить следующую карту.

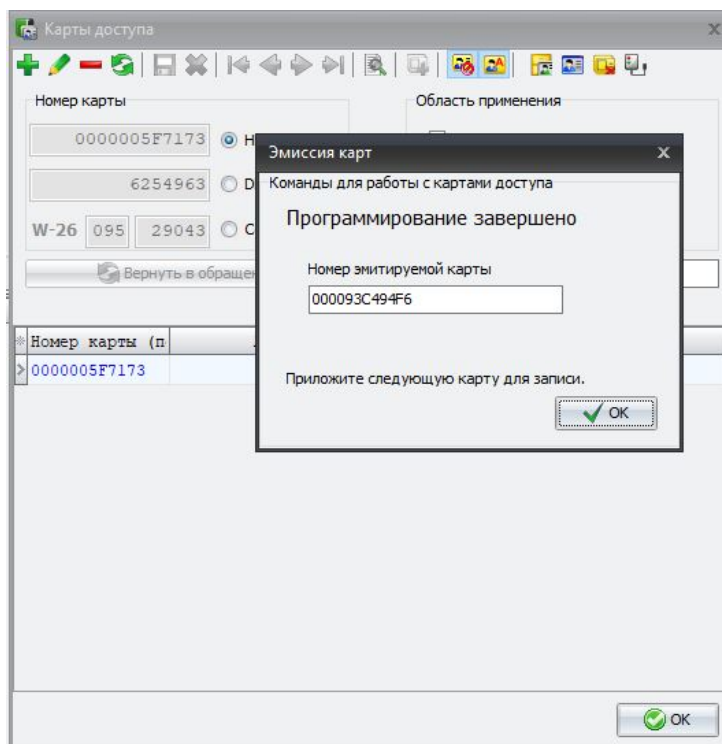


Рис. 9. Эмиссия карты завершена

Эмитированная карта будет отображаться в списке карт со статусом «неактивна». Такую карту в дальнейшем можно будет присвоить пропуску, выбрав ее вручную из списка либо предъявив настольному считывателю.

4 Дополнительные операции при работе с картами Mifare

4.1 Возврат карты в транспортное состояние.

Выберите в списке пропусков нужный пропуск, нажмите кнопку «Вернуть». Отобразится окно «Возврат пропуска» (рис. 10).

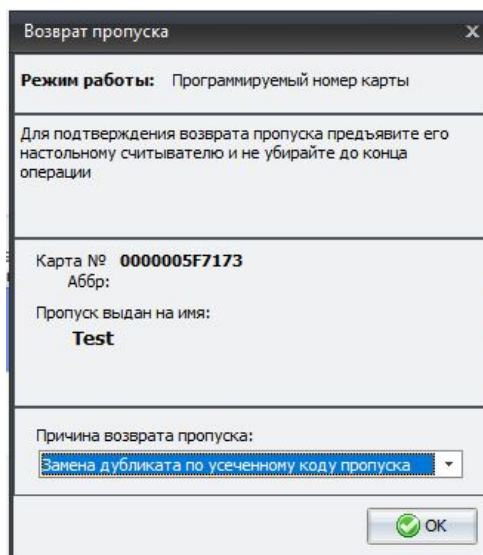


Рис. 10. Возврат пропуска

Приложите к настольному считывателю соответствующую пропуску карту доступа, после чего карта перейдет в транспортное состояние. Для проверки того, что карта теперь находится в транспортном состоянии, можно повторно приложить карту к настольному считывателю, при этом будет выведено информационное сообщение (рис. 11):

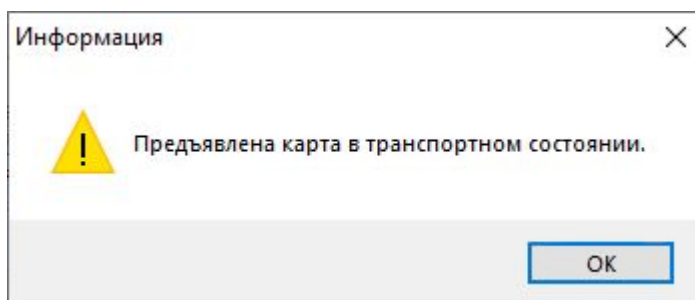


Рис. 11. Сообщение о предъявлении карты в транспортном состоянии



Внимание! Возврат в транспортное состояние мастер-карт не предусмотрен.

4.2 Замена ключей безопасности.

Замена ключей безопасности в выданных картах требуется при изменении профиля безопасности мастер-карты. Процедура изменения профиля безопасности мастер-карты описана в инструкции к утилите MFMasterCard. После изменения профиля безопасности необходимо перепрограммировать настенные считыватели, добавить новую мастер-карту в бюро пропусков.

Для обновления ключей безопасности в уже выданных картах доступа перейдите в меню «Инструменты - Замена ключей безопасности (автоматический режим)». Появится информационное окно (рис. 12).

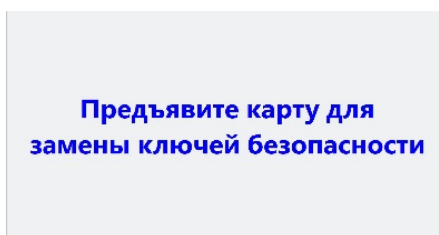


Рис. 12. Запрос при замене ключей безопасности

Приложите к настольному считывателю по очереди каждую карту, выданную с предыдущим профилем безопасности.

После завершения замены ключей безопасности потребуется ввести пароль оператора для подтверждения операции.

Штатная работа системы во время выполнения мероприятий по обновлению профиля безопасности может оказаться невозможной, если не принять специальных мер. Есть несколько вариантов организации обновления профиля безопасности в системе:

1) Кратковременно приостановить эксплуатацию системы на время, пока выполняется обновление параметров безопасности в картах и считывателях. Такой вариант можно рекомендовать для небольших объектов.

2) На время обновления параметров безопасности выключить защищённый режим. Этот вариант возможен только в случае, если для формирования номера в защищённой области используется серийный номер карты. Предполагается изменение физического подключения линий управления защищённым режимом для всех считывателей системы, что может оказаться трудоёмким.

3) Выдать всем сотрудникам новые карты доступа, а старые оставить в обращении до смены параметров безопасности в считывателях. Этот вариант сопряжён с дополнительными затратами (приобретение новых карт), и, кроме того, требует специальной поддержки в программном обеспечении бюро пропусков.