ассоциация Электронные системы

Утилита MFCards.
Руководство пользователя

2014

Оглавление

1 Общие сведения

Утилита MFCards предназначена для программирования карт Mifare® Classic 1k / 4k (далее – карты Mifare) для обеспечения их работы в защищённом режиме совместно со считывателями Elsys-SW20-MF, используемыми в системах контроля и управления доступом.

Утилита обеспечивает:

- эмиссию карт, находящихся в транспортном состоянии;
- ведение базы данных эмитированных карт;
- ведение базы данных мастер-карт, содержащих заранее настроенные профили безопасности;
- формирование номеров карт в защищённой области размерностью до шести значащих байт;
- различные способы формирования номера карты в защищённой области (серийный номер, автоматически генерируемый номер из заданного диапазона, номер, вводимый пользователем вручную);
- проверку номеров карт на уникальность младшей части;
- перевод эмитированных карт в транспортное состояние;
- изменение профилей безопасности эмитированных карт.

Комплект поставки:

- исполняемый файл MFCards.exe;
- библиотека ZReader.dll;
- настоящее руководство.

При работе программы автоматически создаётся файл базы данных карт MFCards.db (файл создаётся в каталоге, где находится исполняемый файл MFCards.exe).

Для работы утилиты необходим подключенный к компьютеру по интерфейсу USB настольный считыватель Elsys-SW-USB-MF. Для обеспечения работы этого считывателя необходимо установить драйверы, поставляемые вместе с ним.

2 Защищённый режим работы карт Mifare. Основные понятия и термины

В обычном режиме считыватели карт Mifare Elsys-SW-20-MF в качестве номера карты передают заводской серийный номер карты. Этот номер является общедоступным и может быть прочитан любым считывателем карт Mifare.

Защищённый режим – особый режим работы считывателей карт Mifare Elsys-SW20-MF, в котором в качестве номера карты используются данные, хранящиеся в защищённой области памяти карты. Память карты Mifare 1k состоит из 16 секторов, доступ к каждому из которых защищён ключами, задаваемыми при программировании карты. Карты Mifare 4k в описываемой системе используются в режиме совместимости с картами Mifare 1k (используются сектора 0 – 15, структура которых идентична картам Mifare 1k).

Набор параметров защищённого режима (ключи защиты, номер используемого сектора) называется ***профилем безопасности***. Для обеспечения возможности чтения номера карты из защищённой области во все считыватели системы должны быть занесены параметры профиля безопасности. Считыватели Elsys-SW20-MF поставляются с профилем безопасности по умолчанию, отличным от транспортного профиля карт Mifare. Утилита MFCards также первоначально настроена для работы с профилем безопасности по умолчанию. **Настоятельно рекомендуется перед началом эксплуатации системы изменить во всех считывателях профиль безопасности!**

Изменение профиля безопасности в считывателях Elsys-SW20-MF осуществляется с помощью мастер-карты, для создания которой используется специальная утилита.

Мастер-карта – особым образом запрограммированная карта Mifare, предназначенная для занесения содержащихся в ней параметров защищённого режима в считыватели системы. Кроме профиля безопасности, каждая мастер-карта содержит уникальную информацию, обеспечивающую её работоспособность только на тех считывателях, где она впервые была использована. Это является дополнительным механизмом защиты, который предотвращает возможность перепрограммирования считывателей другой мастер-картой, созданной злоумышленником.

Внимание! Следует учитывать, что дальнейшая смена профилей безопасности в считывателях Elsys-SW20-MF возможна только с помощью мастер-карты (или её копии), которой была впервые выполнена смена заводского профиля безопасности.

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

Транспортное состояние карты Mifare – исходное состояние карты, в котором доступ ко всем секторам карты разрешён с помощью заводских ключей, которые являются общеизвестными. Карта, находящаяся в транспортном состоянии, в дальнейшем обозначается как «чистая карта».

Для выполнения эмиссии карт, а также для возможности изменения профиля безопасности и перевода эмитированных карт в транспортное состояние, в базе данных утилиты MFCards хранится история мастер-карт, соответствующая истории всех используемых профилей безопасности. Ввод нового профиля безопасности осуществляется предъявлением мастер-карты настольному считывателю Elsys-SW-USB-MF.

Текущий профиль безопасности – профиль, используемый в утилите MFCards для эмиссии карт. Текущий профиль безопасности вводится в базу данных автоматически, при предъявлении мастер-карты.

3 Описание работы программы

3.1 Пользовательский интерфейс главного окна программы

На рисунке (Рис. 1) изображено главное окно программы.

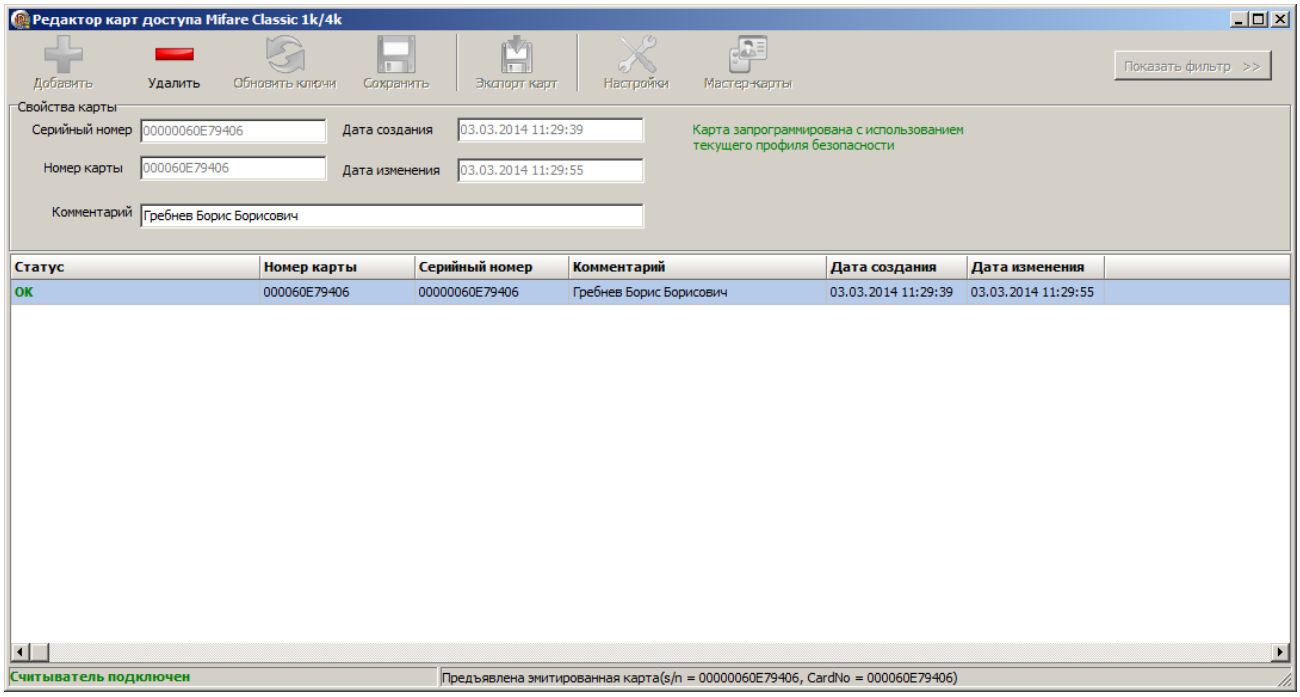

Рис. 1 – Главное окно программы MFcards.exe

В верхней части экрана находится панель инструментов, на которой находятся кнопки, с помощью которых можно выполнить различные действия («Добавить», «Удалить», «Обновить ключи», «Сохранить», «Экспорт карт», «Настройки», «Мастер-карты», «Показать/Скрыть фильтр»). Набор разрешённых действий зависит от состояния выбранной карты, от наличия подключенного считывателя и от наличия карты в поле считывателя.

В нижней части главного окна находится панель, на которой отображается статус настольного считывателя («Считыватель подключен» или «Считыватель не найден») и информация о карте, находящейся в поле считывателя.

В нижней половине главного окна находится список карт, в котором в табличном виде отображены основные свойства карт (статус, номер карты, серийный номер, комментарий, дата создания, дата изменения). На панели «Свойства карты», отображаются элементы редактирования и отображения свойств выбранной карты.

Поле ***«Статус»*** - состояние карты, по отношению к текущему используемому профилю безопасности. В таблице информация о статусе карты отображена кратко, а на панели «Свойства карты» содержится более подробный комментарий. Статус ***«ОК»*** означает, что карта запрограммирована с использованием текущего профиля безопасности. Статус ***«Нужно обновить ключи»*** означает, что для карты необходимо установить текущий профиль безопасности. Кроме того, в поле «Статус» может содержаться информация об ошибках при работе с картой.

Поле ***«Комментарий»*** содержит произвольную текстовую информацию об эмитированной карте (например, это может быть имя владельца карты).

Все действия, выполняемые с картами Mifare (эмиссия, перевод в транспортное состояние, изменение профиля безопасности) и требующие обязательного наличия считывателя Elsys-SW-USB-MF, одновременно автоматически регистрируются в базе данных.

Внимание! При выполнении любых операций, связанных с программированием карт (эмиссия, смена профиля безопасности, возврат в транспортное состояние) недопустимо до завершения операции убирать карту из поля считывателя! В противном случае карта может быть повреждена!

Если считыватель не подключен, из операций редактирования данных доступно только изменение данных в поле «Комментарий».

При поднесении карты к считывателю выполняется поиск карты с данным серийным номером в базе данных, и, если такая карта найдена, выполняется позиционирование курсора в списке карт, с одновременным выводом подробной информации о карте на панели «Свойства карты».

Кнопка «Показать фильтр» выводит на экран дополнительную панель для фильтрации списка карт по заданным критериям.

3.2 Настройки

Для открытия окна настроек необходимо нажать кнопку «Настройки» на панели инструментов главного окна программы, после чего на экране появится окно настроек (Рис. 2).

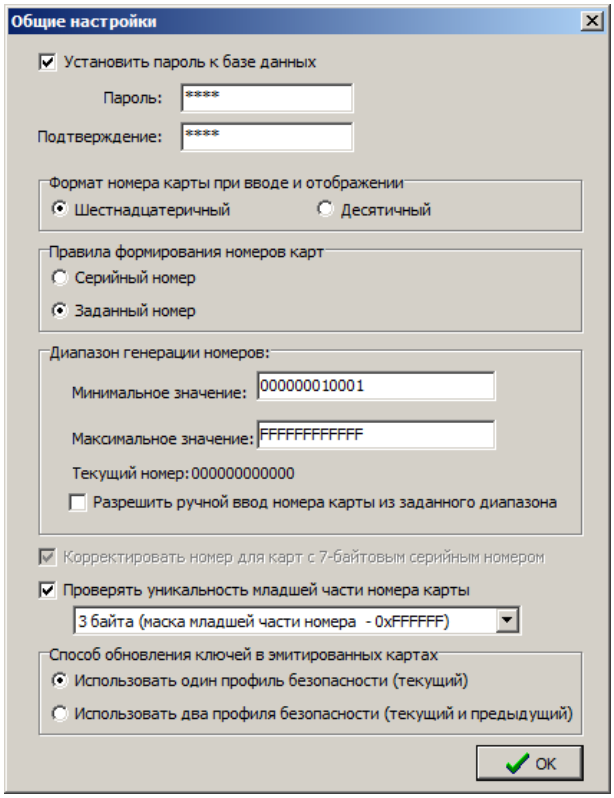

Рис. 2 – Общие настройки

Внимание! Настоятельно рекомендуется установить все основные настройки до начала эмиссии карт. В противном случае возможны конфликты при формировании номеров карт. О вероятности или наличии таких конфликтов будут сформированы предупреждающие сообщения. Кроме того, при наличии эмитированных карт в базе становится недоступным изменение настройки «Правила формирования номеров карт».

Базу данных, с которой работает утилита MFCards.exe, рекомендуется защитить паролем, для чего следует включить опцию ***«Установить пароль к базе данных»*** и ввести одинаковое значение пароля (в пароле должно быть не менее четырёх символов) в полях ***«Пароль»***, ***«Подтверждение»***. Если пароль задан, при старте программа MFCards.exe потребует ввести пароль.

Настройка ***«Формат номера карты при вводе и отображении»*** позволяет выбрать один из двух форматов для ввода и отображения числовых значений – шестнадцатеричный (по умолчанию) и десятичный.

Настройка ***«Правила формирования номеров карт»*** задаёт способ формирования номера карты. Если выбрано значение ***«Серийный номер»***, при эмиссии карты её серийный номер будет копироваться в защищённую область и в дальнейшем использоваться в качестве номера карты. Такой режим удобно использовать во многих случаях, в частности:

1) в случае, если для ввода карт в систему используется настольный считыватель, не поддерживающий защищённый режим (например, Elsys-SW-USB);

2) в случае, если в системе предусмотрен оперативный перевод считывателей из защищённого режима в обычный, и наоборот (например, в процессе смене профиля безопасности у всех выданных карт).

Дополнительная настройка ***«Корректировать номер для карт с 7-байтовым серийным номером»*** (актуальна, если для генерации номеров используется серийный номер) обеспечивает идентичность кодовых посылок для считывателей Elsys-SW20-MF при включенном и отключенном защищённом режиме, если серийный номер карты содержит семь байт. Если эта настройка включена, то при формировании номера карты используются байты 1 – 6 серийного номера, а если выключена – байты 0 – 5.

Если для настройки ***«Правила формирования номеров карт»*** выбрано значение ***«Заданный номер»***, то номер карты при её эмиссии будет автоматически формироваться из диапазона (***«Минимальное значение»*** … ***«Максимальное значение»***), заданного в группе настроек ***«Диапазон генерации номеров»***. Кроме того, если включена опция «Разрешить ручной ввод номера карты из заданного диапазона», номер может быть введён вручную, с учётом установленных ограничений.

Минимально возможное значение номера – 0x10001 (в десятичном формате – 65537). Максимально возможное значение – 0xFFFFFFFFFFFF (в десятичном формате – 281474976710655), что соответствует диапазону в шесть значащих байт.

Последний автоматически сгенерированный номер карты отображается в поле ***«Текущий номер»***.

Настройка ***«Проверять уникальность младшей части номера карты»*** (в зависимости от выбранного варианта, на уникальность будут проверяться младшие 2, 3, 4, 5 или 6 байт) обеспечивает выполнение дополнительной проверки при формировании номера карты. Если при вводе номера карты в базе данных будет найдена карта с совпадающей младшей частью, будет сформировано сообщение об ошибке.

Если при включении этой настройки в базе будут обнаружены карты с совпадающей младшей частью, будет сформировано сообщение об ошибке (Рис. 3), а эти карты будут соответствующим образом отмечены в таблице (см. Рис. 4).

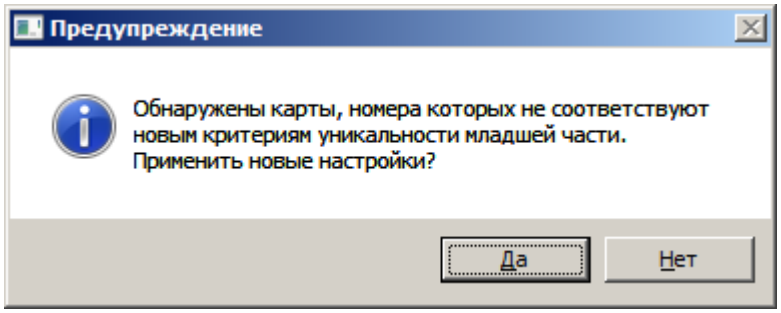

Рис. 3 – Сообщение о наличии в базе карт с совпадающей младшей частью

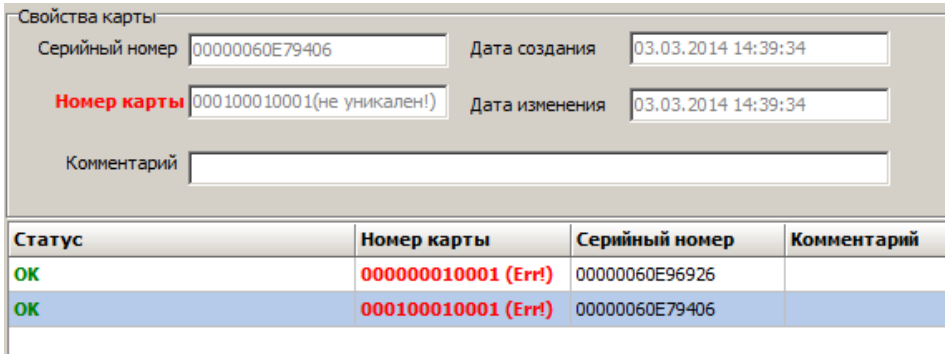

Рис. 4 – Отображение карт с совпадающей младшей частью

Настройка ***«Способ обновления ключей в эмитированных картах»*** задаёт, сколько профилей безопасности (один или два) будет использоваться в эмитированных картах при смене ключей. По умолчанию используется первый вариант (один профиль безопасности). Использование двух профилей безопасности при обновлении ключей в эмитированных картах описано ниже (п. 3.9).

3.3 Создание мастер-карт и ввод мастер-карт с новым профилем безопасности

Для создания мастер-карт используется отдельная утилита. При создании новой мастер-карты в этой утилите должны быть заданы ключ безопасности и рабочий сектор для эмиссии карт.

Следует помнить, что смена профилей безопасности в считывателях Elsys-SW20-MF и в утилите MFCards возможна только с помощью мастер-карты (или её копии), которой была впервые выполнена смена заводского профиля безопасности.

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). Считыватели Elsys-SW20-MF, для которых утеряна мастер-карта, могут быть возвращены в заводское состояние только на предприятии-изготовителе!

В утилите MFCards для эмиссии карт и смены ключей используется ***текущий профиль безопасности*** – профиль безопасности, прочитанный из последней предъявленной мастер-карты. Для установки нового текущего профиля безопасности следует, открыть окно «История мастер-карт», нажав в главном окне программы кнопку «Мастер-карты».

После предъявления мастер-карты с новым профилем безопасности на экране появится окно с запросом на изменение текущего профиля безопасности (Рис. 5). После подтверждения запроса профиль безопасности, считанный с мастер-карты, будет установлен текущим.

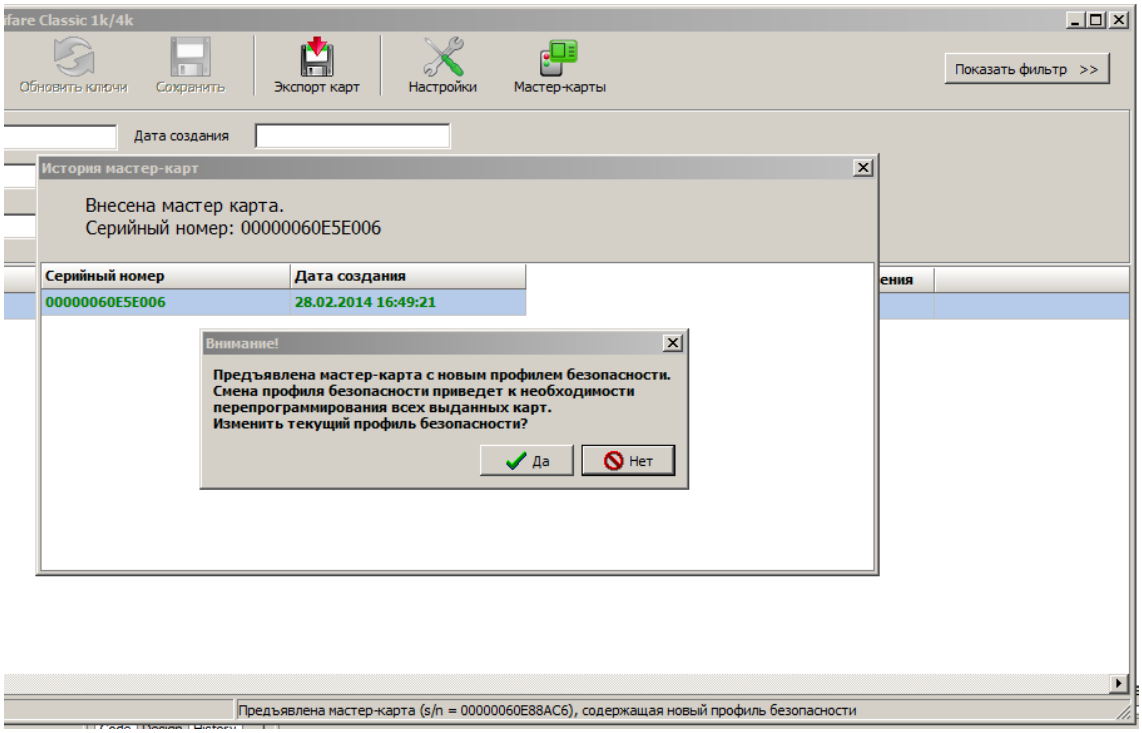

Рис. 5 – Окно «История мастер-карт»

Если будет предъявлена мастер-карта, имеющая профиль безопасности несовместимый с текущим, будет выведено предупреждающее сообщение (Рис. 6). Такую мастер-карту добавить в базу данных и использовать для смены профилей безопасности считывателей невозможно.

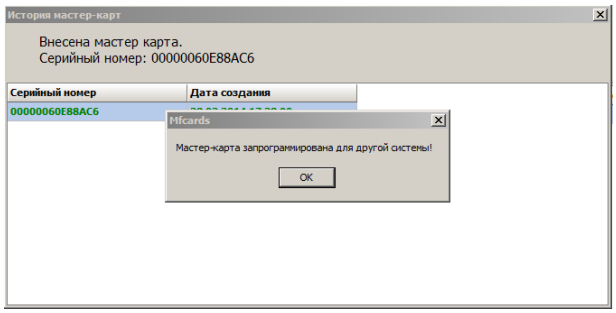

Рис. 6 – Предупреждение о несовместимости мастер-карты

3.4 Эмиссия карт и добавление их в базу

Для выполнения эмиссии карт следует в главном окне нажать кнопку «Добавить», после чего на экране появится окно, изображённое на Рис. 7.

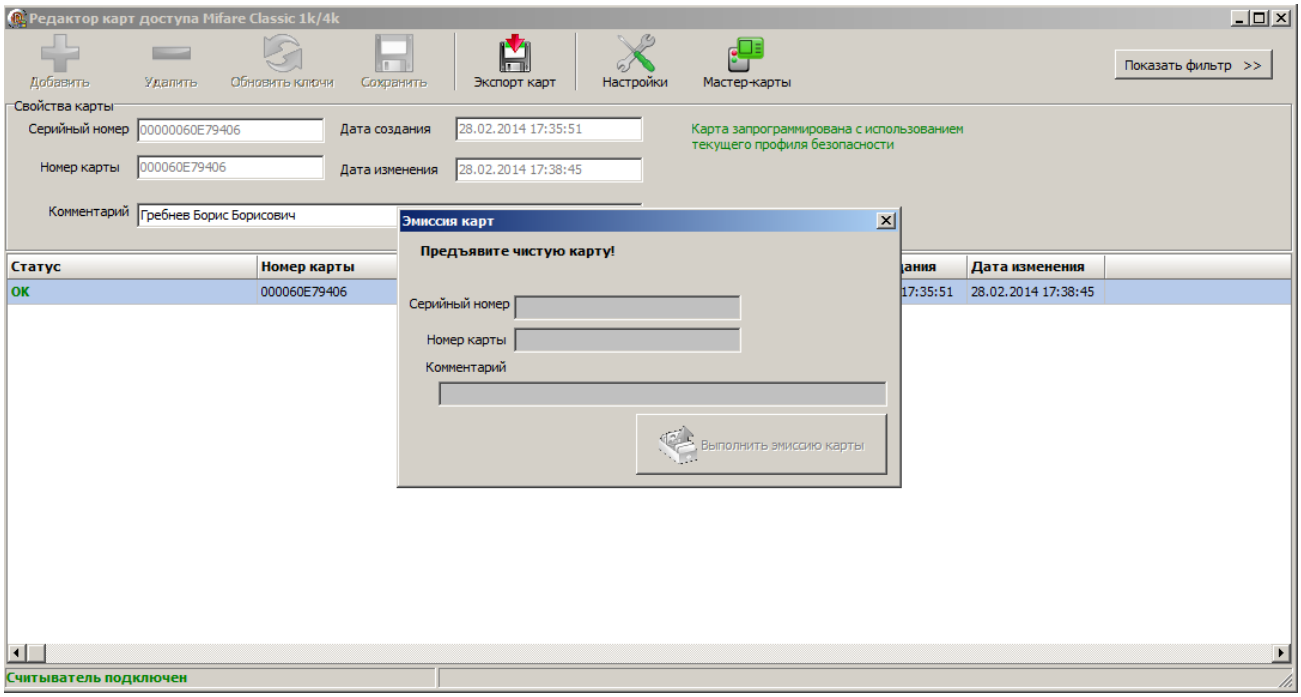

Рис. 7 – Эмиссия карт

После предъявления чистой карты в этом окне становится активной кнопка «Выполнить эмиссию карты» (Рис. 8).

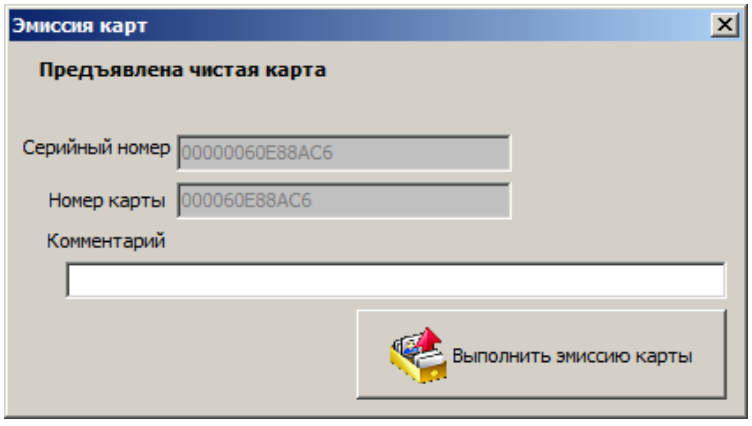

Рис. 8 – Выполнение эмиссии карт

Окно, изображённое на Рис. 8, автоматически появится на экране также в случае, если сразу предъявить чистую карту, не нажимая кнопку «Добавить».

В этом окне может быть введён текстовый комментарий, а также, если включена настройка «Разрешить ручной ввод номера карты», может быть изменён автоматически сформированный номер карты.

После нажатия кнопки «Выполнить эмисию карты» появится окно с предупреждением (Рис. 9).

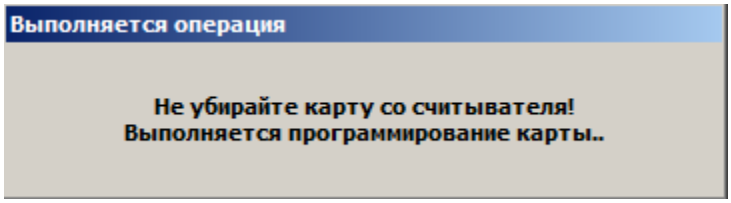

Рис. 9 – Окно предупреждения при выполнении эмиссии карт

После завершения эмисии в окне «Эмиссия карт» появится сообщение о том, что карта запрограммирована (Рис. 10), а карта добавится в базу данных.

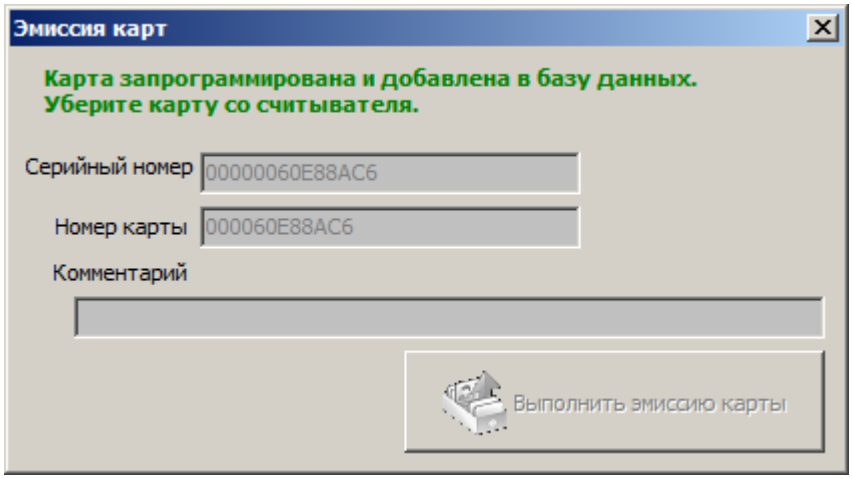

Рис. 10 – Успешное завершение эмиссии карт

Если операция эмиссии, несмотря на предупреждение, была прервана, карта может быть повреждена. Однако, возможны другие варианты: карта может остаться чистой (в этом случае её можно попытаться запрограммировать ещё раз), либо оказаться в эмитированном состоянии (последнее возможно, если карту убрали в момент проверки записи).

Если карта эмитирована, но по каким-то причинам отсутствует в базе, её можно добавить в базу, предъявив считывателю, после чего появится окно, изображённое на Рис. 11.

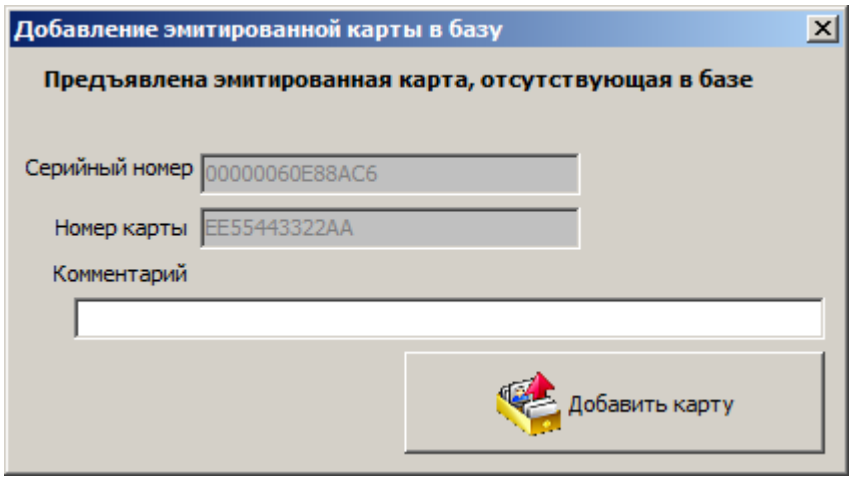

Рис. 11 – Добавление эмитированной карты в базу

3.5 Очистка карт (перевод в транспортное состояние)

Для выполнения очистки карты следует предъявить её считывателю, после чего в таблице будет автоматически выбрана нужная запись и станет активной кнопка «Удалить» на панели инструментов. После нажатия кнопки «Удалить» на экран будет выведено предупреждение (Рис. 12), и после подтверждения будет начата процедура очистки карты.

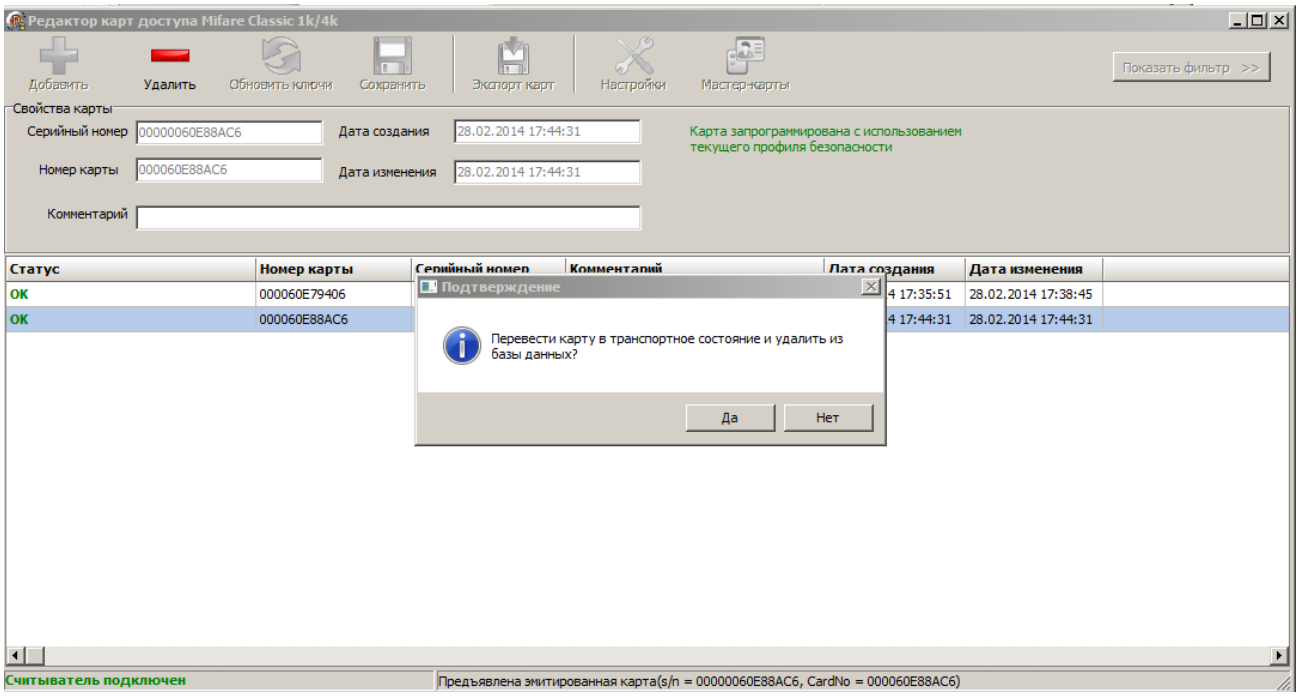

Рис. 12 – Перевод эмитированной карты в транспортное состояние

При успешном завершении операции очистки карта будет удалена из базы данных. Если операция завершилась неудачей (например, если, несмотря на предупреждение, карту преждевременно убрали со считывателя), в базе данных будет отмечен факт ошибки. Для такой карты можно попытаться выполнить операцию очистки повторно.

3.6 Изменение профиля безопасности эмитированных карт

Для изменения профиля безопасности у карты, имеющей статус «Нужно обновить ключи!», следует предъявить карту считывателю, после чего в таблице будет автоматически выбрана нужная запись и станет активной кнопка «Обновить ключи» на панели инструментов (Рис. 13). После нажатия этой кнопки будет начата процедура обновления ключей безопасности. Во время этой процедуры нельзя убирать карту со считывателя, о чём будет выведено предупреждение (Рис. 14).

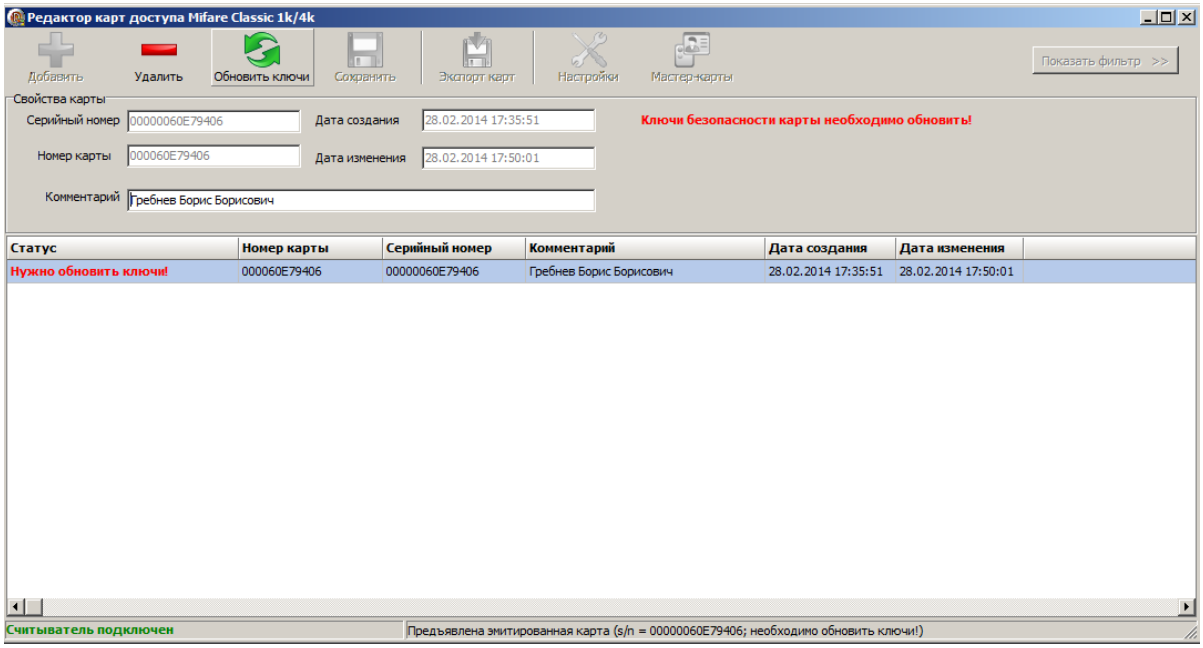

Рис. 13 – Изменение профиля безопасности карты

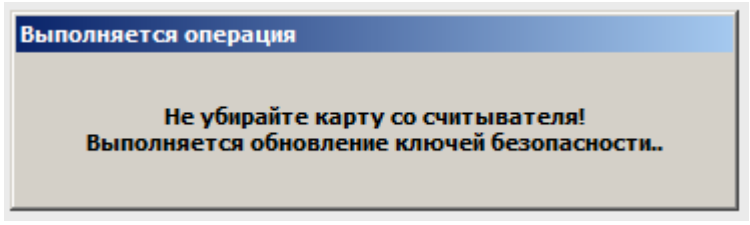

Рис. 14 – Предупреждение при изменении профиля безопасности карты

В случае, если карта была преждевременно убрана со считывателя, несмотря на предупреждение, есть вероятность её повреждения. Ошибка будет зарегистрирована в базе данных со статусом «Ошибка обновления ключей». Для такой карты (Рис. 15) можно попытаться завершить операцию обновления ключей, снова предъявив её считывателю.

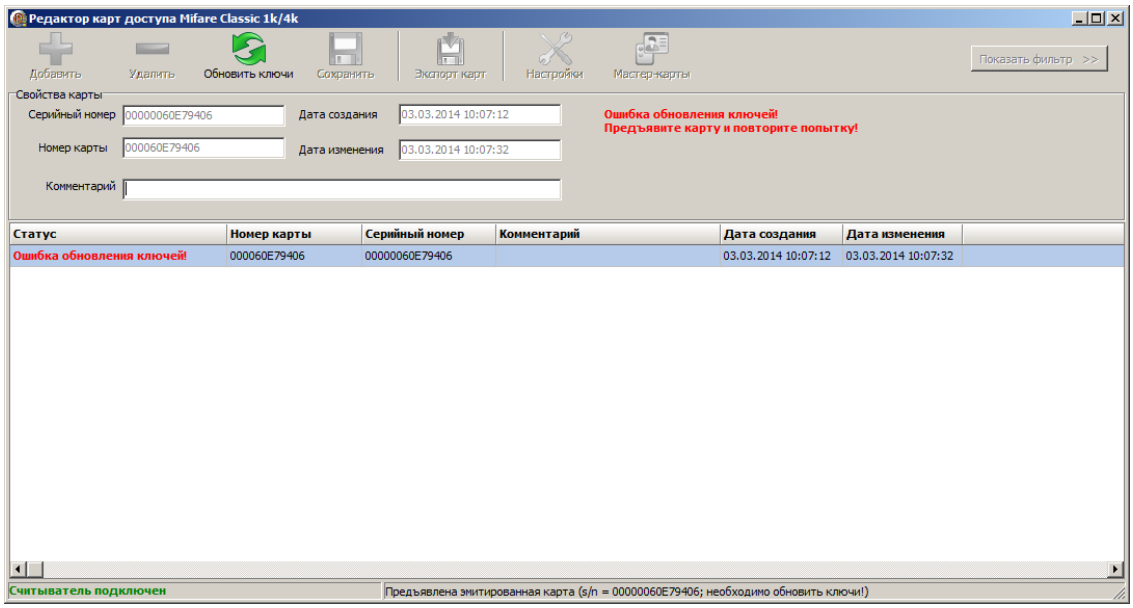

Рис. 15 – Повторное выполнение операций, завершившихся ошибкой

3.7 Редактирование данных об эмитированных картах

Для эмитированных карт, занесённых в базу данных, может быть введён произвольный текст в поле «Комментарий» (до 80 символов). После внесения изменений становится активной кнопка «Сохранить», выполняющая сохранение внесённых изменений (Рис. 16).

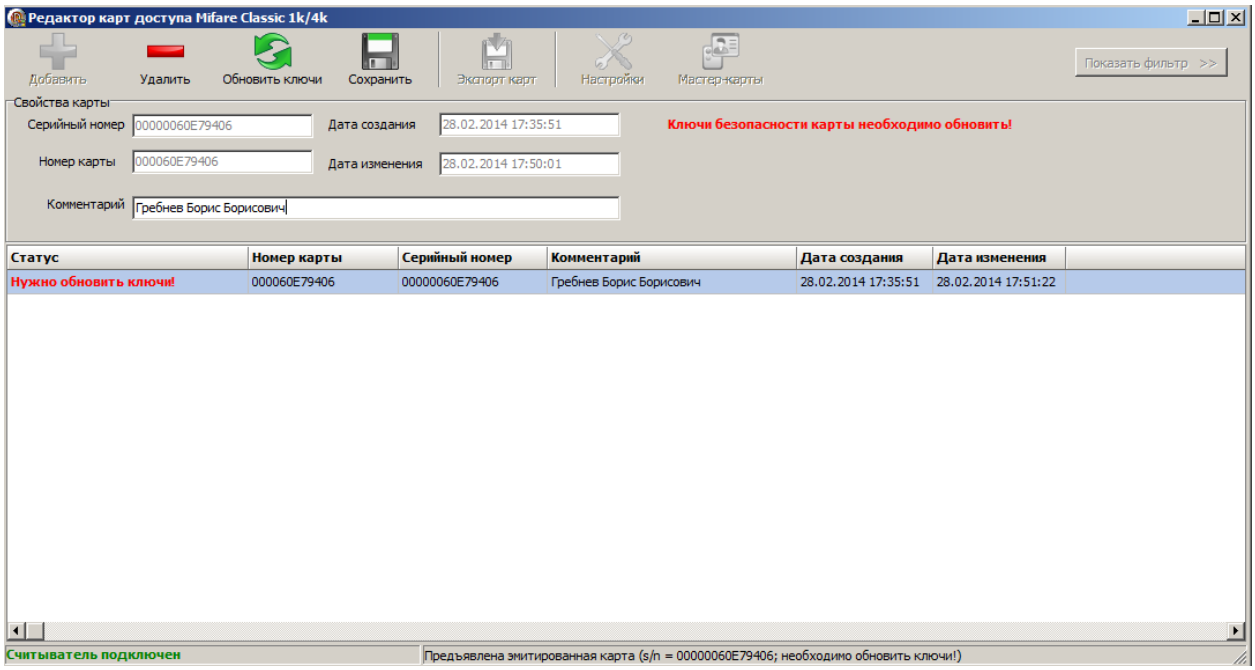

Рис. 16 – Редактирование данных об эмитированных картах

3.8 Экспорт списка карт

Для выполнения экспорта данных следует нажать кнопку «Экспорт» в главном окне программы, после чего появится стандартный диалог сохранения файла (Рис. 17). Возможен экспорт данных в одном из двух форматов:

- файл с разделителями csv;

- XML-файл в формате, совместимом с форматом импортируемых данных для ПО Бастион 1.7.

В первом случае все данные, находящиеся в таблице, с учётом фильтра (Рис. 18) сохраняются в текстовом файле с разделителями.

Во втором случае в XML-файле сохраняются данные из всех строк таблицы, с учётом фильтра, из полей «Номер карты» и «Комментарий».

Числовое значение номера карты преобразуется в поля SITECODE и CARDNO (в соответствии с правилами формирования номера в формате «сайт-код + номер»), а поле «Комментарий» преобразуется в поля NAME, FIRSTNAME, SECONDNAME (тест делится на три части, разделённые пробелами; если одна из частей отсутствует, значение соответствующего поля будет равно пустой строке). Так, для комментария, показанного на Рис. 16, данные будут извлечены следующим образом:

NAME = “Гребнев”, FIRSTNAME = “Борис”, SECONDNAME = “Борисович”.

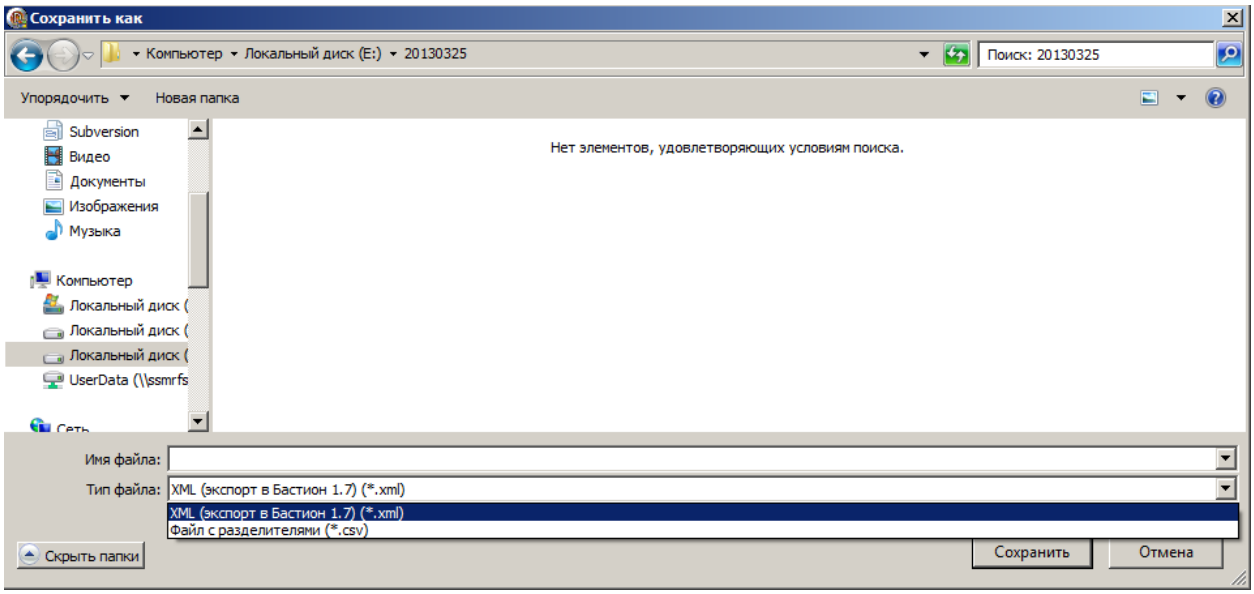

Рис. 17 – Экспорт данных

При необходимости фильтрации списка карт по заданным критериям может быть использован фильтр (Рис. 18). Панель фильтра может быть выведена на экран кнопкой «Показать фильтр».

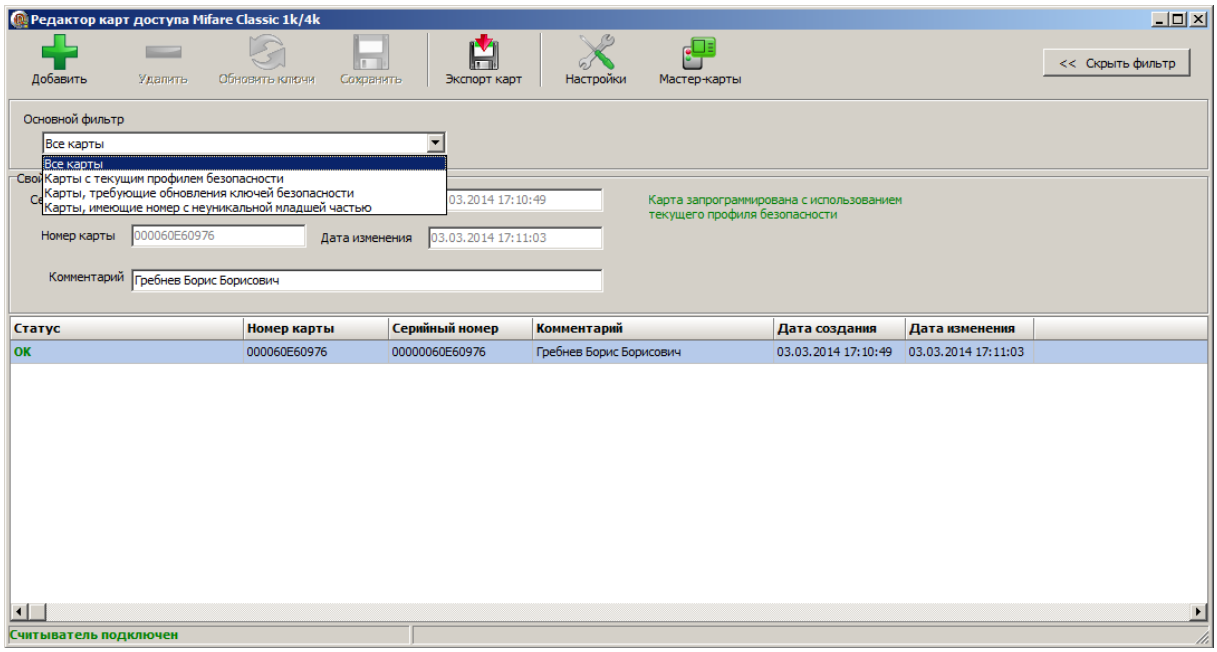

Рис. 18 – Установка фильтра списка карт

3.9 Особенности обновления параметров защиты карт при использовании двух профилей безопасности

Использование двух профилей безопасности – один из способов обеспечения на объекте постепенной замены профилей безопасности карт. Основное достоинство этого способа заключается в том, что при смене профиля безопасности не требуется приостанавливать работу системы или отключать защищённый режим.

Главное требование для реализации этого режима – обеспечить при создании мастер-карты, чтобы текущий и предыдущий профили безопасности имели разные рабочие сектора.

В случае использования рассматриваемого режима, при изменении профиля безопасности карта будет приобретать новый профиль безопасности, но останется работоспособной и при использовании старого профиля безопасности. Это позволит постепенно, не приостанавливая эксплуатацию системы, выполнить смену профиля безопасности во всех картах, после чего выполнить смену профиля безопасности во всех считывателях системы.

Если включен режим использования двух профилей безопасности, то главное окно программы и окно истории мастер-карт приобретают иной вид (Рис. 19, Рис. 20).

В таблице карт выводится дополнительное поле «Предыдущий профиль», отображающее совместимость карты с ранее использовавшимся профилем.

В таблице «Мастер-карты» выводится дополнительное поле «№ сектора для эмиссии карт».

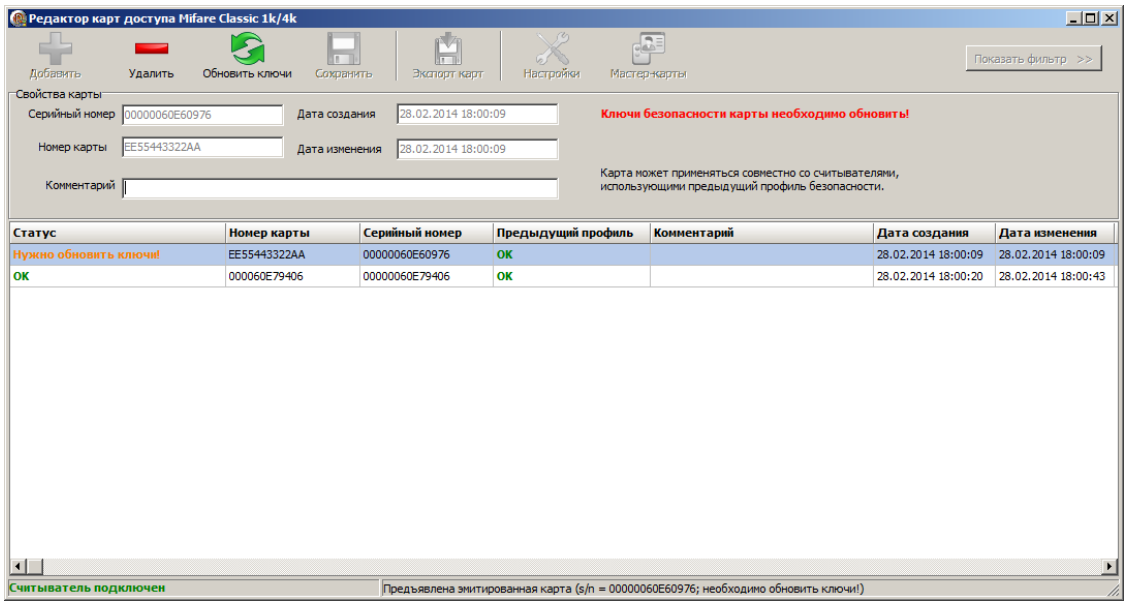

Рис. 19 – Вид главного окна программы при использовании двух профилей безопасности

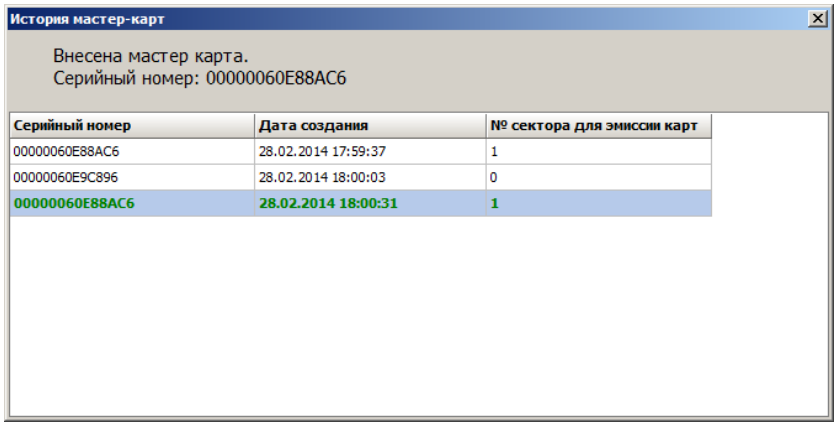

Рис. 20 – Вид окна «История мастер-карт» при использовании двух профилей безопасности

4 Настройка и эксплуатации системы, использующей карты Mifare в защищённом режиме

Перед началом эксплуатации системы необходимо создать мастер-карту и выполнить эмиссию карт, которые будут использоваться в системе.

4.1 Настройка считывателей Elsys-SW20-MF для работы в защищённом режиме

Для включения защищённого режима в считывателях Elsys-SW20-MF необходимо соединить линию Secure (синий провод считывателя) с общим проводом (цепью GND).

Во все считыватели системы необходимо мастер-картой занести текущий профиль безопасности, который используется при эмиссии карт. Для установки нового профиля безопасности следует предъявить мастер-карту считывателю, находящемуся в защищённом режиме, и дождаться продолжительного звукового сигнала (длительностью около 1 с), сопровождаемого свечением зелёного светодиода.

4.2 Обновление профилей безопасности в системе

В процессе эксплуатации системы может возникнуть необходимость смены профиля безопасности в системе. Следует учитывать, что это трудоёмкий и организационно сложный процесс, поскольку предусматривает перепрограммирование всех считывателей системы и всех карт доступа, находящихся в обращении.

Для смены профиля безопасности сначала следует записать новый профиль безопасности в мастер-карту.

Далее, необходимо установить новый профиль безопасности как текущий для утилиты MFCards и записать новый профиль безопасности во все карты доступа (для этого каждый владелец карты должен посетить бюро пропусков).

Затем, по завершении обновления профиля безопасности в картах доступа, следует занести мастер-картой новый профиль безопасности во все считыватели системы.

Однако, 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 только 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. Этот вариант предусматривает физическую коммутацию линий управления защищённым режимом для всех считывателей системы, что может оказаться трудоёмким.

3. Выдать всем сотрудникам новые пропуска, 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.

4. Использовать специальный режим обновления параметров защиты с использованием двух профилей безопасности (описан в п. 3.9).

Последний вариант в большинстве случаев является оптимальным для обновления параметров защищённого режима.