

Инструкция по построению СКУД со считывателями Gate-Reader-MF и картами Mifare в защищенном режиме.

Общие принципы

Возможность клонирования идентификаторов в СКУД может приводить к случаям несанкционированного доступа, саботажа системы, искажению сведений учета рабочего времени. Кроме того, такая возможность не соответствует требованиям ряда законодательных актов по построению СКУД и обеспечению безопасности целого ряда государственных объектов.

Данная инструкция описывает один из способов решения задачи защиты идентификаторов СКУД от клонирования. Для реализации простого и доступного варианта защищенного режима SL1 используются считыватели Gate-Reader-MF, настольный считыватель Gate-USB-MF и карты (идентификаторы) Mifare следующих типов: Mifare Classic, Mifare ID.

В защищенном режиме в процессе взаимодействия и обмена данными между считывателем и картой используется специальный уникальный ключ защиты объекта. В такой СКУД могут использоваться только те карты, и только те считыватели, которые были запрограммированы для работы на данном объекте. Причем защищенные области данных карт не подвержены вскрытию и копированию, а также невозможно считывание ключа и иных служебных данных из рабочего считывателя. При успешном опознании (совпадении ключа защиты) поднесенной карты (идентификатора) считыватель выдает в контроллер СКУД wiegand-код заданной длины, содержащий идентификационный код соответствующего пользователя. Существует два основных варианта (два режима) работы системы:

а) в контроллер СКУД выдается уникальный идентификационный код пользователя, записанный в защищенный сектор карты при эмиссии;

б) в контроллер СКУД выдается UID данной карты.

Эти режимы имеют отличия и особенности, как при построении системы, так и при ее эксплуатации. Данная Инструкция отражает работу в первом режиме а) с выдачей уникального идентификационного кода пользователя из защищенной ячейки. Этот режим считается предпочтительным. Особенности настройки и построения системы во втором режиме б) описаны в дополнительной инструкции на сайте Gate.

Для хранения уникального ключа защиты и иных специальных параметров защищенной системы объекта, а также для эмиссии рабочих карт объекта (карт пользователей системы), используется специальная Мастер-карта объекта. Для программирования считывателей идентификаторов используется Мастер-карта объекта и специальные карты Инициализации двух типов:

- карта Инициализации для Нового считывателя — для активации и подготовке к записи технологических и объектовых параметров Нового считывателя. Под термином Новый понимается считыватель с заводскими настройками. После программирования Нового считывателя он становится Рабочим для данной системы. Под термином Рабочий понимается считыватель, запрограммированный для работы в СКУД данного объекта.

- карта Инициализации для Рабочего считывателя - для активации и подготовке к изменению технологических и объектовых параметров Рабочего считывателя данной системы.

Таким образом, минимальный комплект служебных карт системы содержит две карты Инициализации (для Новых и для Рабочих считывателей) и Мастер-карту объекта. При необходимости можно создать несколько подобных комплектов карт. Во избежание вскрытия и дискредитации защищенной системы доступа необходимо предпринимать особые организационно-технические меры по сохранению в тайне фактического значения ключа защиты, а также по защите от несанкционированного использования комплекта служебных карт объекта.

Процесс создания защищенной системы включает этапы:

1. Генерация уникального ключа объекта и создание комплекта служебных карт Инициализации и Мастер-карты объекта.
2. Программирование и перевод используемых считывателей в защищенный режим.
3. Эмиссия защищенных рабочих карт объекта (карт пользователей).

В процессе эксплуатации объекта для работы с картами пользователей используется настольный считыватель Gate-USB-MF и Мастер-карта объекта.

Для работы с настольным считывателем Gate-USB-MF используется бесплатная утилита «Gate-USB-MF Configurator», которая есть на общем CD дистрибутива ПО Gate, а также на сайте бренда http://skd-gate.ru/materiali/tehnicheskaya_gate/po/

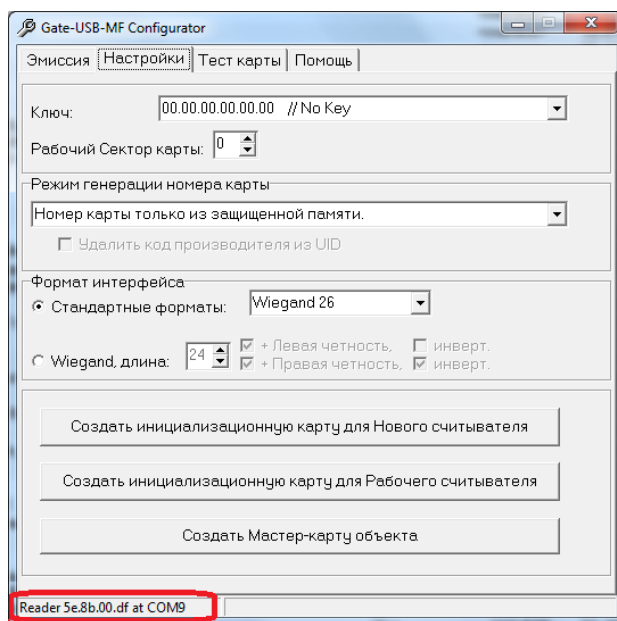
Порядок создания защищенной системы

1. Подготовить к работе настольный считыватель Gate-USB-MF:

- 1.1. Установить микропереключатели на задней стенке настольного считывателя следующим образом: 5 - ON, 6 - ON, остальные переключатели в нижнем положении (off).
- 1.2. Скачать с сайта бренда Gate (или с общего CD ПО Gate) и установить драйвер настольного считывателя Gate-USB-MF.
- 1.3. Подключить считыватель к ПК USB кабелем.

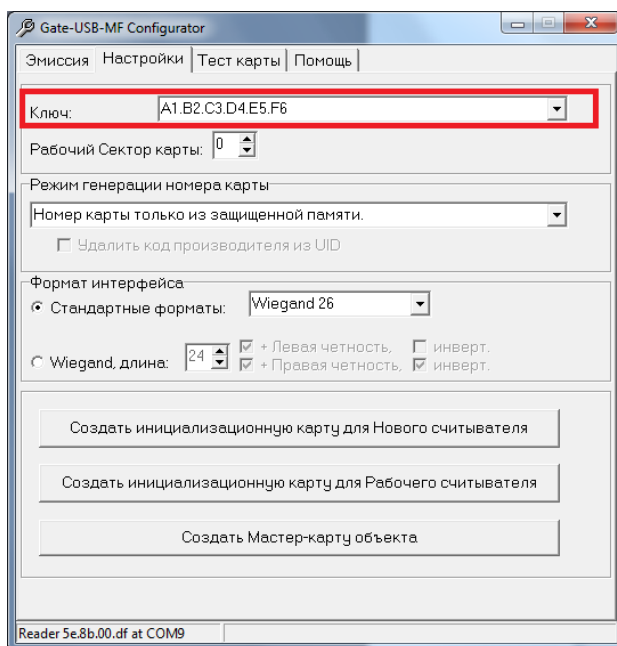
2. Настроить работу утилиты «Gate-USB-MF Configurator»

Скачать с сайта бренда Gate (или с общего CD ПО Gate) и запустить утилиту «Gate-USB-MF Configurator». Убедиться, что считыватель найден программой (см. информационное поле в левом нижнем углу интерфейса):



3. Задать необходимые параметры защищенной системы.

3.1. На вкладке «Настройки» ввести произвольный ключ защиты данной системы в шестнадцатеричном виде (6 байт). Для непредвиденных случаев утраты Мастер-карты объекта этот ключ надо запомнить и хранить в тайне от посторонних лиц.

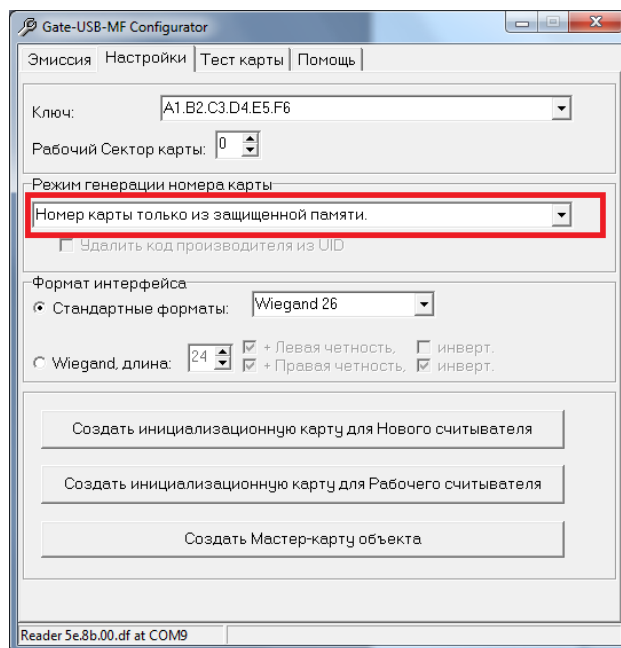


3.2. На этой же закладке указать «Рабочий сектор карты».

Внимание! Для работы с картами Mifare-ID допускается использовать только сектор 0.

Для карт Mifare Classic возможен выбор сектора в зависимости от особых требований и наличия свободных к использованию секторов в данных картах. При отсутствии особых требований также рекомендуется сектор 0.

3.3. Выбрать режим генерации номера карты «Номер карты только из защищенной памяти»



4. Создать комплект служебных карт объекта.

4.1. Создать Мастер-карту объекта, для чего поднести новую карту к настольному считывателю и нажать кнопку «Создать Мастер-карту объекта». Теперь все настройки вашей системы находятся на этой карте.

4.2. Создать карту Инициализации для Нового считывателя, для чего поднести новую карту к считывателю и нажать «Создать инициализационную карту для Нового считывателя». Эта карта понадобится при программировании Новых считывателей, находящихся в заводской конфигурации.

4.3. Создать карту Инициализации для Рабочего считывателя, для чего поднести новую карту к считывателю и нажать «Создать инициализационную карту для Рабочего считывателя». Эта карта понадобится когда потребуется сменить Ключи или другие параметры системы в Рабочем считывателе, находящемся в эксплуатации на объекте.

Примечания:

- при необходимости можно создать несколько комплектов служебных карт объекта;
- сброс Рабочего считывателя в исходную заводскую конфигурацию возможен **только в лаборатории производителя** (сервисный отдел бренда Gate).

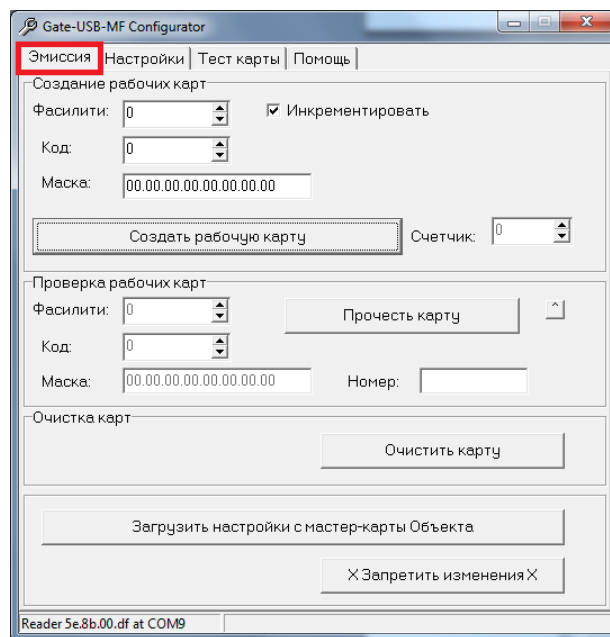
5. Произвести программирование считывателей Gate-Reader-MF, предназначенных для установки на объекте:

- включить питание считывателя и в течение следующих 30 секунд поднести к нему **карту Инициализации для Нового считывателя**. Считыватель перейдет в режим программирования – начнет издавать частые звуковые сигналы.
- поднести **Мастер-карту объекта**. Считыватель примет настройки из карты, прекратит звуковые сигналы, выйдет из режима программирования и перейдет в категорию Рабочего считывателя данного объекта.
- повторить эту операцию со всеми Новыми считывателями, предназначенными для данного объекта.

Примечание: В процессе эксплуатации системы может возникнуть необходимость изменения настроек Рабочих считывателей. Перепрограммирование Рабочих считывателей производится аналогичным способом, но при этом используется **карта Инициализации для Рабочего считывателя и новая Мастер-карта объекта** (с новыми параметрами системы).

6. Произвести эмиссию рабочих карт:

6.1. Запустить приложение «Gate-USB-MF Configurator». Убедиться, что считыватель найден программой (информационное поле в левом нижнем углу интерфейса). Перейти в закладку «Эмиссия», поднести к настольному считывателю Мастер-карту объекта и нажать кнопку «Загрузить настройки с Мастер-карты»



6.2. Задать значение кода идентификации пользователя (в разделе «Создание рабочих карт»). Для этого можно использовать два способа формирования значения кода идентификации пользователя: автоматический или ручной.

Автоматический: установить начальные фасилити и код карты; установить флаг «Инкрементировать», чтобы после каждого нажатия кнопки «Создать рабочую карту» значение поля «Код» увеличивалось на единицу (в противном случае все карты будут выпущены с одним и тем же кодом идентификации пользователя).

Ручной: вручную задать требуемый код рабочей карты (это бывает удобно при переходе от старой системы, в которой за пользователем уже был закреплен определенный идентификационный код).

Примечания:

- поле «Маска» при работе со считывателями с выходом Wiegand-26 рекомендуется оставить нулевым;
- после подготовки настроек Эмиссии можно нажать кнопку «X Запретить изменения X», что не позволит оператору, производящему работу по эмиссии карт, посмотреть настройки шифрования или случайными действиями сбить настройки;
- по окончании эмиссии карт есть возможность проконтролировать работу оператора по количеству выпущенных карт на основании значения поля Счетчик.

6.3. Поднести новую карту к настольному считывателю и нажать кнопку «Создать рабочую карту».

Примечание: для создания очередной рабочей карты в режиме автоматического формирования кода достаточно поднести очередную новую карту к считывателю и нажать кнопку «Создать рабочую карту». В режиме ручного формирования кода перед нажатием данной кнопки необходимо вручную задать новое значение кода.

7. Чтение запрограммированных рабочих карт.

В процессе эксплуатации системы, в частности в процессе занесения карты в СКУД и выдачи ее пользователю, требуется чтение рабочей карты. Для этого:

7.1. Запустить приложение «Gate-USB-MF Configurator». Убедиться, что считыватель найден программой (информационное поле в левом нижнем углу интерфейса). Перейти в закладку «Эмиссия», поднести к настольному считывателю Мастер-карту объекта и нажать кнопку «Загрузить настройки с Мастер-карты»

7.2. Поднести рабочую карту к настольному считывателю и нажать кнопку «Прочитать карту». В поле «Номер» отобразится полный номер карты в формате, требуемом для программы Gate-Terminal. Его можно скопировать и использовать в учетной карточке пользователя в ПО СКУД.

Методика поэтапного перевода СКУД с незащищенных карт формата Em-Marine на защищенный режим с картами Mifare.

1. Приобрести необходимое для замены количество считывателей Gate-Reader-MF, настольных считывателей Gate-USB-MF и карт Mifare (Mifare Classic, Mifare ID)
2. Изготовить комплект служебных карт защищенной системы данного объекта в соответствии с п. 4 данной инструкции.
3. Произвести программирование комплекта считывателей Gate-Reader-MF, предназначенных для установки на объекте в соответствии с п.5 данной инструкции.
4. Произвести полную единовременную или постепенную эмиссию защищенных рабочих карт Mifare для каждого пользователя системы в соответствии с п.6 данной инструкции. При этом использовать режим ручного ввода кода карты, в качестве которого указывать wiegand код действующей в СКУД карты Em-Marine данного пользователя. Код действующей карты Em-Marine каждого пользователя можно скопировать из БД СКУД или считать с помощью настольного считывателя Z2-USB.
5. Произвести полную единовременную или постепенную выдачу новых рабочих карт пользователям системы, с рекомендацией хранить и использовать обе карты вместе. После полного завершения процесса выдачи новых карт всем пользователям можно перейти к следующему этапу.
6. Произвести полную единовременную или постепенную замену старых считывателей на новые рабочие считыватели Gate-Reader-MF. В случае постепенной замены считывателей доступ пользователей во всех точках прохода обеспечивается наличием у них двух карт разного стандарта (старых Em-Marine и новых защищенных Mifare).
7. По окончании процесса замены считывателей можно организовать сбор старых карт или оповестить пользователей об окончании их функционирования.

Важными удобствами данной методики перехода на защищенные идентификаторы с наследованием кодов старых карт являются отсутствие необходимости каких либо изменений в БД СКУД и возможность постепенного выполнения основных этапов.

Последствия утраты или компрометации ключа защиты системы.

1. Физическая утрата Мастер-карты при отсутствии знания фактического кода защиты автоматически приводит к невозможности наращивания системы (добавления точек доступа), изменения настроек системы, эмиссии карт и чтения карт настольным считывателем. В этом случае неизбежно встает вопрос о необходимости создания новой системы. С использованием настольного считывателя Gate-USB-MF и чистых новых карт Mifare можно создать новый комплект служебных карт для новой системы. Рабочие считыватели Gate-Reader-MF невозможно перепрограммировать на месте и их придется снимать и отсылать производителю для сброса к заводским установкам. Рабочие карты стандарта Mifare-ID в данной ситуации не подлежат повторному использованию. Рабочие карты стандарта Mifare Classic можно будет использовать в новой системе при условии наличия у них другого свободного сектора.
 2. Компрометация ключа защиты или Мастер-карты объекта не блокирует возможность работы системы или ее наращивания, но обеспечивает возможность и вызывает реальную угрозу создания действующих дубликатов карт или реализации диверсионного перепрограммирования рабочих считывателей объекта. Поэтому в подобной ситуации требуется обновление системы:
 - создать новый комплект служебных карт с новым ключом защиты в соответствии с п.4 данной инструкции;
 - перепрограммировать Рабочие считыватели в соответствии с п.5 данной инструкции, но с использованием старой карты Инициализации для Рабочего считывателя и новой Мастер-карты объекта (с новыми параметрами системы);
 - произвести эмиссию и выдачу новых карт в соответствии с п. 6 данной инструкции, или перевыпустить старые рабочие карты. При этом каждую карту предварительно нужно очистить (очистить рабочую карту) и создать заново с новыми параметрами.
- В период проведения данных работ СКУД находится в нерабочем состоянии и это надо учитывать при планировании и организации работ по обновлению системы.