

**СЧИТЫВАТЕЛИ БЕСКОНТАКТНЫЕ НАСТОЛЬНЫЕ
«Proxy-6-USB-G», «Proxy-6-USB-B», «Proxy-6-USB-W»**

Руководство по эксплуатации

АЦДР.425729.015 РЭП

Оглавление

1	Описание и работа	5
1.1	Назначение изделия	5
1.2	Технические характеристики	5
1.3	Состав изделия.....	6
1.4	Устройство и работа	6
1.5	Средства измерения, инструменты и принадлежности	11
1.6	Маркировка и пломбирование	11
1.7	Упаковка	11
2	Использование по назначению	12
2.1	Эксплуатационные ограничения.....	12
2.2	Подготовка изделия к использованию	12
2.2.1	Меры безопасности при подготовке изделия.....	12
2.2.2	Конструкция прибора.....	12
2.2.3	Монтаж прибора.....	12
2.2.4	Подключение прибора.....	12
2.2.5	Настройка прибора.....	15
2.2.6	Идентификация с помощью мобильного платежного приложения.....	39
2.2.7	Использование изделия	43
2.2.8	Обновление программного обеспечения считывателя	44
2.2.9	Проверка работоспособности	46
2.2.10	Действия в экстремальных ситуациях.....	46
2.2.11	Возможные неисправности и способ устранения	46
3	Техническое обслуживание изделия	47
3.1	Общие указания	47
3.2	Меры безопасности	47
3.3	Порядок технического обслуживания изделия	47
3.4	Проверка работоспособности изделия.....	47
3.5	Техническое освидетельствование	47
3.6	Консервация (расконсервация, переконсервация)	47
4	Текущий ремонт	48
5	Хранение.....	48
6	Транспортирование	48
7	Утилизация	48
8	Гарантии изготовителя.....	49
9	Сведения о сертификации.....	49
10	Сведения о ранее выпущенных версиях.....	49

Настоящее руководство по эксплуатации (в дальнейшем РЭ) предназначено для изучения принципов работы и эксплуатации «Proxy-6-USB-G», «Proxy-6-USB-B», «Proxy-6-USB-W» (в дальнейшем – «Proxy-6-USB» или считыватель).

Литера -G, -B, -W обозначают цвет корпуса: Grey (серый), Black (черный), White (белый).

К обслуживанию допускается персонал, изучивший настоящее руководство. Все работы по монтажу, пуску, регулированию и обкатке должны проводиться с соблюдением требований действующей на месте эксплуатации нормативной документации.

Список принятых сокращений:

- ОС – операционная система;
- ПК – персональный компьютер;
- ПО – программное обеспечение;
- РЭ – руководство по эксплуатации;
- СКУД – системы контроля и управления доступом;
- UID – (Unique Identifier) – это уникальный серийный номер (или идентификационный код), присваиваемый каждой бесконтактной карте на заводе-изготовителе;
- SL0 – (Security Level 0) уровень безопасности 0;
- SL1 – (Security Level 1) уровень безопасности 1;
- SL3 – (Security Level 3) уровень безопасности 3;
- PAN – (Primary Account Number) основной номер банковской карты;

1 Описание и работа

1.1 Назначение изделия

Считыватель бесконтактный настольный «Proxy-6-USB» предназначен для считывания уникального кода идентификационных карт и передачи его на персональный компьютер через USB порт.

Считыватель «Proxy-6-USB» считывает идентификационный код всех популярных карт стандарта MIFARE, например, MIFARE Ultralight, MIFARE Classic, MIFARE Plus, MIFARE DESFire EV1, банковских карт, а также карт HID ProxCard II и EM-Marin. В считывателе «Proxy-6-USB», реализован функционал работы с защищенными секторами карт MIFARE (используются алгоритмы шифрования Crypto-1, AES 128), позволяющий обеспечить защиту от копирования идентификационных карточек. Поддержка следующих карт: MIFARE Classic, MIFARE Plus (S, SE, X, EV1, EV2), банковские карты (со встроенным идентификатором MIFARE совместимым с Classic). Работа с защищенными секторами карт ограничена до 1 Кбайт. Также предусмотрена работа с платежными приложениями «Mir Pay», «SberPay», «Т-Pay», а именно осуществляется считывание токена банковской карты (токен - это замена PAN банковских карт для конкретного приложения).

Считыватель способен передать код карты в следующих форматах: 2, 3, 4, 5 и 7 байт + Enter в шестнадцатеричной (HEX), десятичной (DEC) системах счисления либо в формате Touch Memory (до 6 байт).

Считыватель предназначен для программирования мастер-карт и пользовательских карт, которые используются совместно со считывателями бесконтактными «Proxy-6ЕНМ-G», «Proxy 6ЕНМ-B» и «Proxy-6ЕНМ-W» в защищённых режимах работы.

Считыватель применяется в системах охраны и в системах контроля и управления доступом (СКУД).

Считыватель рассчитан на круглосуточный режим работы.

Считыватель предназначен для работы в жилых, коммерческих и производственных зонах.

Считыватель является восстанавливаемым, периодически обслуживаемым изделием.

1.2 Технические характеристики

Таблица 1.2.1

Наименование характеристики	Значение
Количество входов питания	1
Напряжение источника питания, В (USB-порт)	5
Ток потребления, не более, мА	180
Время технической готовности прибора к работе, с	3 с
Рабочая частота, МГц	0,125 13,56
Максимальная дистанция считывания, мм	
- EM-Marine, HID	100
- MIFARE	50
- Смартфон	20
Степень защиты оболочки по ГОСТ 14254-2015	IP40
Устойчивость к механическим воздействиям по ОСТ 25 1099-83	категория размещения 3

Наименование характеристики	Значение
Вибрационные нагрузки: - диапазон частот, Гц; - максимальное ускорение, g	1-35 0,5
Климатическое исполнение по ОСТ 25 1099-83	О3
Диапазон рабочих температур, °С	от 0 до + 65
Масса прибора, не более, кг	0,1
Габаритные размеры прибора, мм	85,3×85,3×24,2
Время непрерывной работы прибора	круглосуточно
Средняя наработка прибора на отказ в дежурном режиме работы, не менее, ч	80000
Вероятность безотказной работы за 1000 ч	0,98758
Средний срок службы прибора, лет	10

По устойчивости к электромагнитным помехам считыватель соответствует требованиям третьей степени жёсткости по ГОСТ Р 50009.

Считыватель удовлетворяет нормам промышленных помех, установленным для оборудования класса Б по ГОСТ 30805.22.

1.3 Состав изделия

Комплект поставки считывателя соответствует Таблице 1.3.1.

Таблица 1.3.1

Обозначения	Наименование	Количество
АЦДР.425729.015 АЦДР.425729.016-02 АЦДР.425729.017-02	Считыватель бесконтактный настольный «Proxy-6-USB-G» Считыватель бесконтактный настольный «Proxy-6-USB-B» Считыватель бесконтактный настольный «Proxy-6-USB-W»	1 шт.
Комплект запасных частей и принадлежностей (ЗИП):		
	USB-кабель (USB A – mini USB B)	1 шт.
Документация		
АЦДР.425729.015 РЭ	Считыватель бесконтактный настольный «Proxy-6-USB-G», «Proxy-6-USB-B», «Proxy-6-USB-W». Руководство по эксплуатации	1 шт.

1.4 Устройство и работа

Считыватель подключается к персональному компьютеру посредством USB-порта ПК. Электропитание считывателя осуществляется от этого же USB-порта.

На лицевой панели считывателя находятся (см. рис. 1):

- 1) светодиодный индикатор (цвет зависит от режима работы);
- 2) поле антенны считывателя.

Запуск устройства сопровождается следующей индикацией: светодиодный индикатор загорится три раза красным, зеленым и синим цветами в сопровождении звукового сигнала. При этом, в ОС, добавляются два устройства: клавиатура и COM-порт. Для работы считывателя требуется установить специальный драйвер, который входит в ПО «UProgProxy-6 v.x.x» и «UProgProxy-6-USB Security v.x.x» (как правило, драйвер требуется только для ОС Windows 7 (x86/x64)).

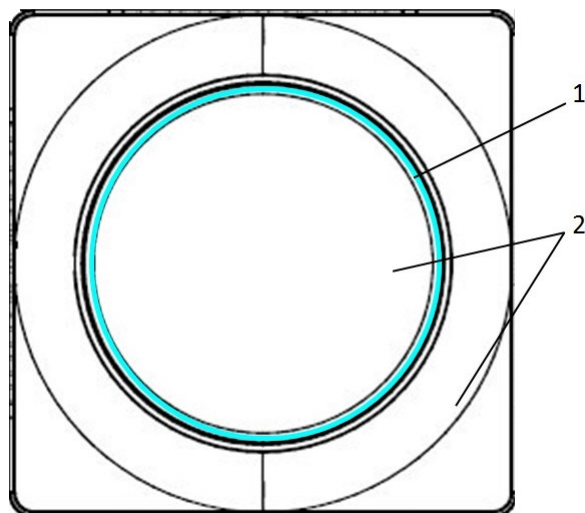


Рис.1 Лицевая панель Proxu-6-USB-G(-B/-W)

Постоянное свечение светового индикатора бирюзовым цветом означает, что считыватель находится в рабочем режиме «WINDOWS». Это такой режим, который работает только в операционной системе Windows и позволяет выводить UID карты на ПК вне зависимости от настройки языковой панели (раскладки клавиатуры).

Постоянное свечение светового индикатора фиолетовым цветом означает, что считыватель находится в рабочем режиме «Windows, Linux, MacOS». Этот режим зависит от настройки языковой панели, но не зависит от операционной системы. В этом режиме работы важно: прежде чем выводить UID карты на ПК, убедитесь, что языковая панель переключена на английский язык (EN) иначе выведенный номер карты будет не корректным.

Данные режимы задаются в ПО «UProgProxu-6 v.x.x».

Дальнейшая работа считывателя также сопровождается световой и звуковой индикацией.

После поднесения карты (смартфона), считыватель передаёт UID карты в одном из выбранных форматов данных, перечисленных в п.1.1 настоящего руководства.

Считывание карты подтверждается одним коротким звуковым сигналом и выключением светодиодного индикатора. При этом UID карты выводится в любой открытый и активный текстовый файл или в окно ввода открытого приложения.

Формат выходных данных задаётся с помощью ПО «UProgProxu-6 v.2.00» (программа находится на сайте компании <https://bolid.ru/> в разделе «Продукция» на странице считывателя бесконтактные настольные «Proxu-6-USB-G, Proxu-6-USB-B, Proxu-6-USB-W»).



ПО «UProgProxu-6 v.2.00» совместимо с ОС Windows 7 (x86/x64), 10, 11.

Также считыватель осуществляет программирование/считывание идентификационных карт и брелоков стандарта MIFARE для работы в защищённом режиме.

Виды поддерживаемых карт перечислены в п.1.1 настоящего руководства.

Для программирования мастер-карт и пользовательских карт предусмотрено ПО «UProgProxu-6-USB Security v.2.00» (программа находится на сайте компании <https://bolid.ru/> в разделе «Продукция» на странице считывателя бесконтактные настольные «Proxu-6-USB-G, Proxu-6-USB-B, Proxu-6-USB-W»).



Внимание! Для работы в ПО «UProgProxu-6-USB Security v.2.00» необходимо прошивку считывателя Proxu-6-USB обновить до версии 2.00 или выше.

ПО «UProgProxy-6-USB Security v.2.00» предназначено исключительно для программирования мастер и пользовательских карт стандарта MIFARE Classic и MIFARE Plus.

ПО «UProgProxy-6-USB Security v.2.00» совместимо с ОС Windows 7 (x86/x64), 10, 11.

Мигание светового индикатора возможно при работе в ПО «UProgProxy-6-USB Security v.2.00» с картами MIFARE: запись, считать, очистить, циклическая запись, циклическая очистка.

Помимо светодиодной индикации, внутри корпуса считывателя находится звуковой сигнализатор.

В считывателе предусмотрены три варианта защищённого режима работы.

Карта MIFARE содержит в себе несколько секторов. Каждый сектор состоит из трёх блоков, в которые можно записывать пользовательские данные. Доступ к каждому сектору карты защищён ключом, который состоит из шести байт (алгоритм шифрования Срупто-1 для карт MIFARE Classic и MIFARE Plus (SL1)) или из шестнадцати байт (алгоритм шифрования AES 128 для карт MIFARE Plus (SL3)).

В защищённых режимах работы считывателей «Proxy-6-USB», в независимости от типа карты, используются 15 секторов, в секторе можно выбрать один из трёх блоков.

АРМ «Орион Про»

Внимание! В ПО АРМ «Орион Про» считыватель Proxy-6-USB не нужно добавлять, как отдельное устройство.

При работе с АРМ «Орион Про», используя кнопку «Считывание с настольного считывателя» (тип кода: Proximity карта, Код: [поле]), считыватель необходимо настроить согласно рис.2. Обязательно нажать на кнопку «ЗАПИСАТЬ», чтобы изменения конфигурации применились и записались во внутреннюю память считывателя. Прежде чем считывать UID карты на ПК, убедитесь, что языковая панель переключена на английский язык (EN)!

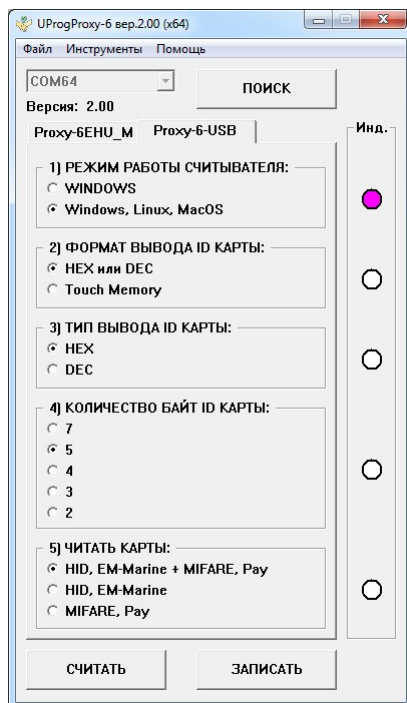


Рис.2 Вкладка Proxy-6-USB ПО «UProgProxy-6 v.2.00» с настройками для АРМ

В случае, если при считывании карты возникают проблемы в номере кода, попробуйте использовать другие форматы для считывания и количество байт ID карты.

Также код идентификатора «Proximity карта», в АРМ «Орион Про», может быть

добавлен вручную. Для этого считыватель необходимо настроить в соответствии с настройками периферийных считывателей СКУД. Стоит обратить внимание на «ИНТЕРФЕЙС» считывателей передачи UID карты (Touch Memory, Wiegand 26, Wiegand 44 или Wiegand 58). Как правило, UID карты хранится в формате Touch Memory, поэтому ниже приведем некоторые из возможных вариантов конфигурирования считывателя Proxu-6-USB в зависимости от «ИНТЕРФЕЙС-а» периферийных считывателей.

Touch Memory

Wiegand 26

Wiegand 44

Wiegand 58

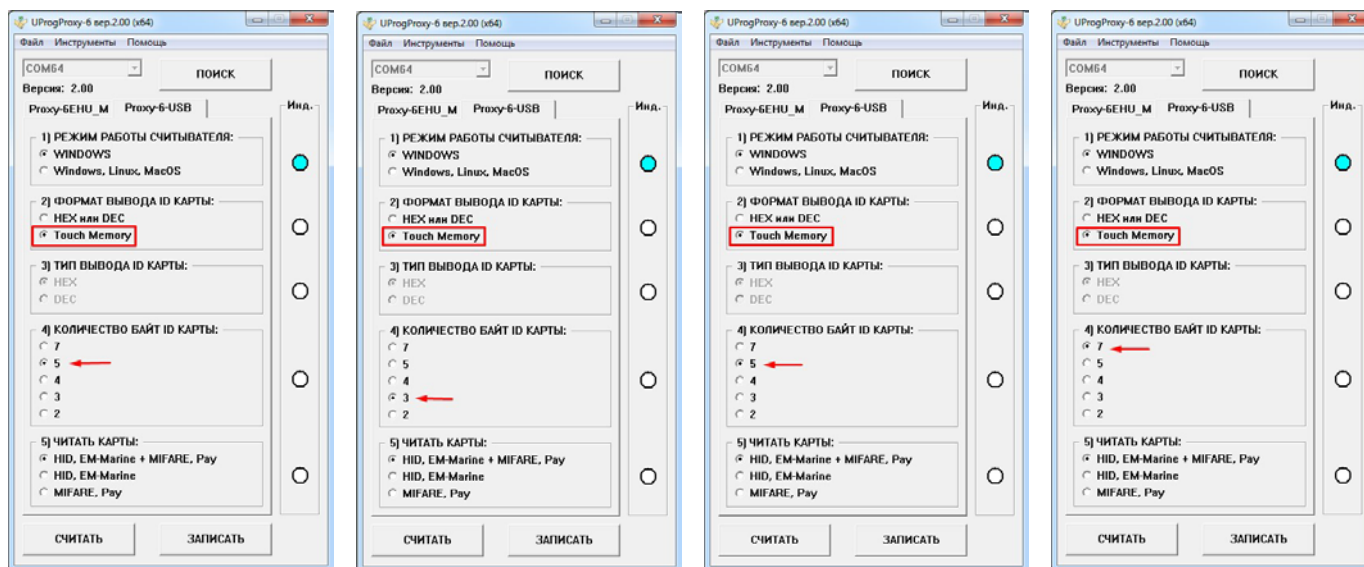


Рис.3 Вкладка Proxu-6-USB ПО «UProgProxu-6 v.2.00»

Обязательно нажать на кнопку «ЗАПИСАТЬ», чтобы изменения конфигурации применились и записались во внутреннюю память считывателя.

Далее, необходимо активировать окно ввода приложения (один клик левой клавишей мыши) или открыть любой текстовый файл и считать карту. UID карты отобразится согласно конфигурации. Если использовался текстовый файл, то необходимо скопировать считанный UID карты и вставить в окно ввода приложения.

Внимание! В некоторых текстовых файлах используется собственный форматированный вывод текста, поэтому UID карты может быть изменен. Рекомендуем использовать стандартное приложение «Блокнот» в ОС Windows.

В случае, если при считывании карты возникают проблемы в номере кода, попробуйте изменить «РЕЖИМ РАБОТЫ СЧИТЫВАТЕЛЯ» на «Windows, Linux, MacOS». Прежде чем считывать UID карты на ПК, убедитесь, что языковая панель переключена на английский язык (EN)!

Подробные инструкции по работе с идентификаторами в АРМ «Орион Про» приведены в руководстве пользователя на АРМ.

Обращаем ваше внимание, что таким способом настраивается вывод UID карт!

В том случае, если производится работа с защищенными секторами карт, то необходимо скопировать «Данные сектора» из «Конвертер пользовательской карты» в зависимости от «Интерфейс считывателя» в ПО «UProgProxu-6-USB Security v.x.x». Естественно, предварительно карта должна быть запрограммирована в ПО «UProgProxu-6-USB Security v.x.x».

Более подробная работа с ПО «UProgProxu-6-USB Security v.x.x» описана ниже.

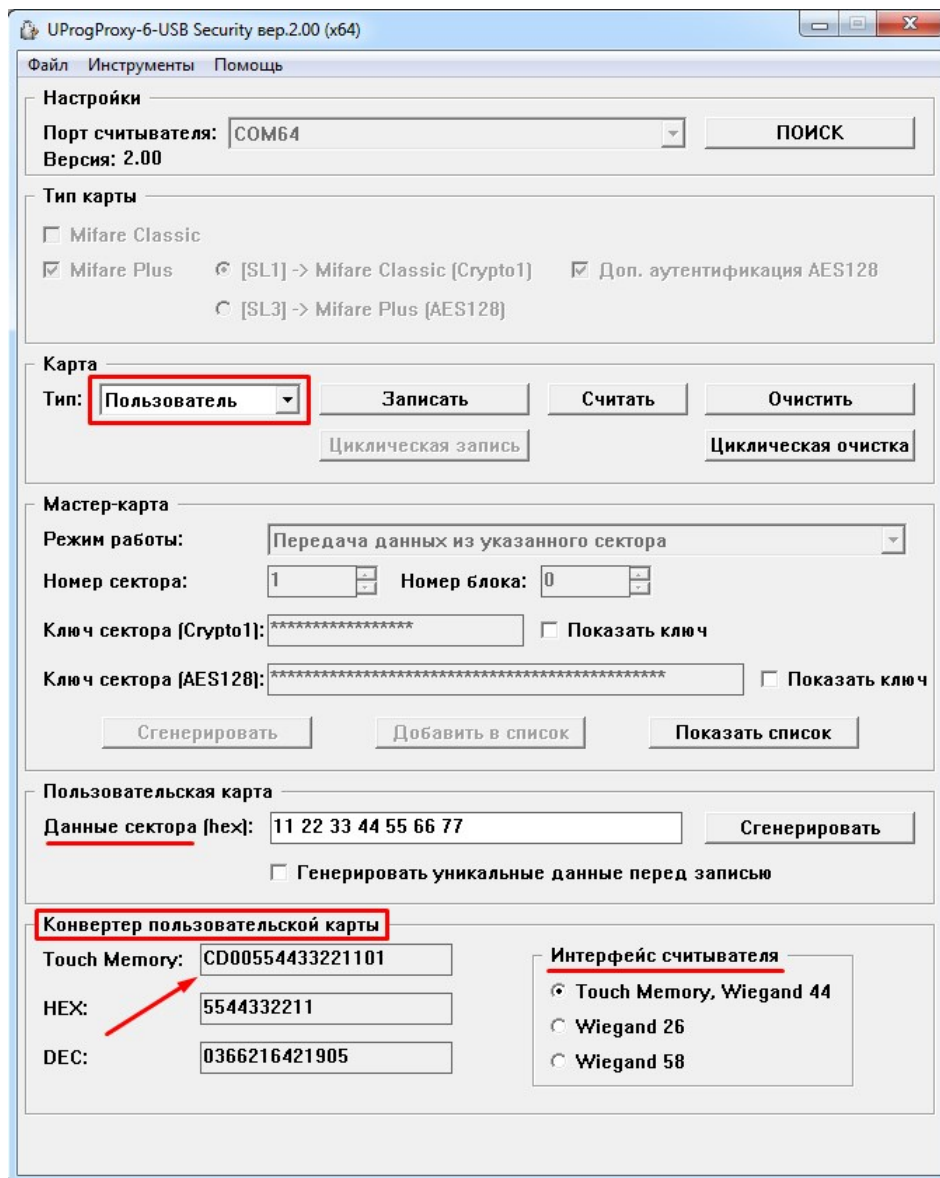


Рис.4 Карта «Пользователь» ПО «UProgProxy-6-USB Security v.2.00»

Режим передачи кода карты

В данном режиме в системе в качестве идентификатора используется UID карты присвоенный на заводе-изготовителе. С помощью мастер-карты, можно оперативно настроить считыватель(и) «Proxy-6ЕНМ-G (-B, -W)» (интерфейс, управление индикацией, индикация в дежурном режиме, опрос сенсорной кнопки) без эмиссии карт MIFARE.

Режим передачи данных из указанного сектора

В данном режиме в системе в качестве идентификатора используется код, записанный в один из блоков определённого сектора карты. Сектор защищается ключом. В блок может быть записан код длиной 7 байт.

Номер блока, номер сектора и ключ сектора задаётся настройщиком системы. Код, записываемый в блок карты можно вводить вручную, либо использовать генератор уникальных кодов, который встроен в ПО «UProgProxy-6-USB Security v.x.x».

Режим передачи кода карты при успешной авторизации к сектору

В данном режиме в системе в качестве идентификатора используется UID карты. Считыватель «Proxy-6ЕНМ-G (-B, -W)» передаст UID карты контроллеру СКУД только в том случае, если ему удастся авторизоваться к определённому сектору карты с определённым ключом.

Номер сектора и ключ сектора задаётся настройщиком системы.

Режим передачи данных из указанного сектора (с шифрованием)

Данный режим аналогичен режиму передачи данных из указанного сектора. Единственное отличие – код хранится в блоке в зашифрованном виде.

1.5 Средства измерения, инструменты и принадлежности

Средства измерения, инструменты и принадлежности при монтаже и обслуживании считывателя не требуются.

1.6 Маркировка и пломбирование

Каждый считыватель имеет маркировку, которая нанесена на тыльной стороне корпуса. Маркировка содержит: наименование прибора, его десятичный номер, заводской номер, год и квартал выпуска, знаки соответствия продукции.

1.7 Упаковка

Прибор совместно с ЗИП и руководством по эксплуатации упакованы в индивидуальную картонную коробку.

2 Использование по назначению

2.1 Эксплуатационные ограничения

Конструкция считывателя не предусматривает его использование в условиях воздействия агрессивных сред, пыли, а также во взрывопожароопасных помещениях.

Качество функционирования считывателя не гарантируется, если электромагнитная обстановка в месте его установки не соответствует условиям эксплуатации, указанным в разделе 1.2 настоящего руководства.

2.2 Подготовка изделия к использованию

2.2.1 Меры безопасности при подготовке изделия

- конструкция считывателя удовлетворяет требованиям пожарной и электробезопасности, в том числе в аварийном режиме по ГОСТ 12.2.007.0-75 и ГОСТ 12.1.004-91;
- считыватель не имеет цепей, находящихся под опасным напряжением;
- монтаж, установку, техническое обслуживание производить при отключенном напряжении питания считывателя;
- монтаж и техническое обслуживание считывателя должны производиться лицами, имеющими квалификационную группу по технике безопасности не ниже второй.

2.2.2 Конструкция прибора

Внешний вид и габаритные размеры считывателя приведены на рисунке 5.

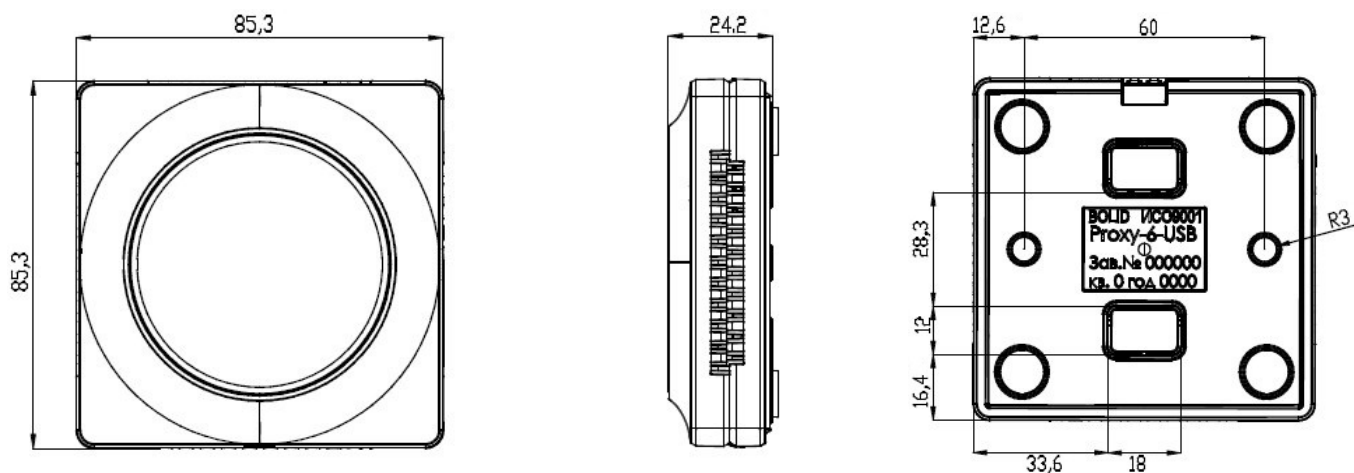


Рис.5 Внешний вид и габаритные размеры считывателя

2.2.3 Монтаж прибора

Считыватель имеет настольное исполнение, устанавливается на столе рядом с ПК.

2.2.4 Подключение прибора

Подключение считывателя к ПК осуществляется с помощью USB-кабеля тип А – mini USB B, входящего в комплект поставки.

После подключения считывателя к ПК в «Диспетчере устройств» он будет отображаться в разделе «Другие устройства» – «Proxy-6-USB», либо как «Неизвестное устройство».

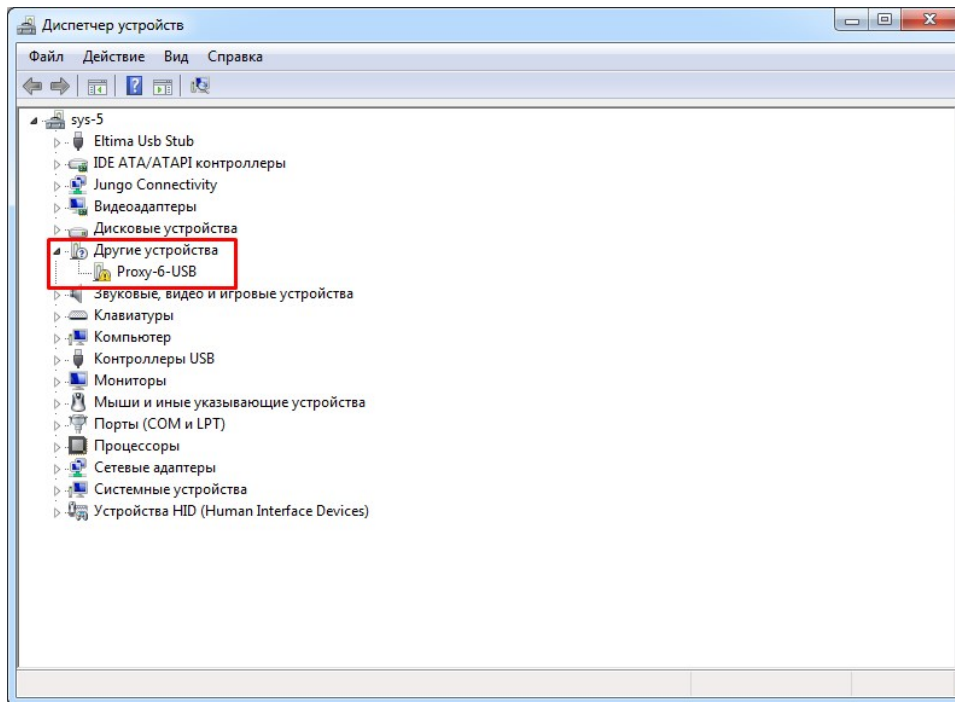


Рис.6 Диспетчер устройств ОС Windows 7

Для установки драйвера считывателя необходимо в «Диспетчере устройств» нажать правой кнопкой мыши на появившееся устройство и выбрать пункт «Обновить драйверы...».

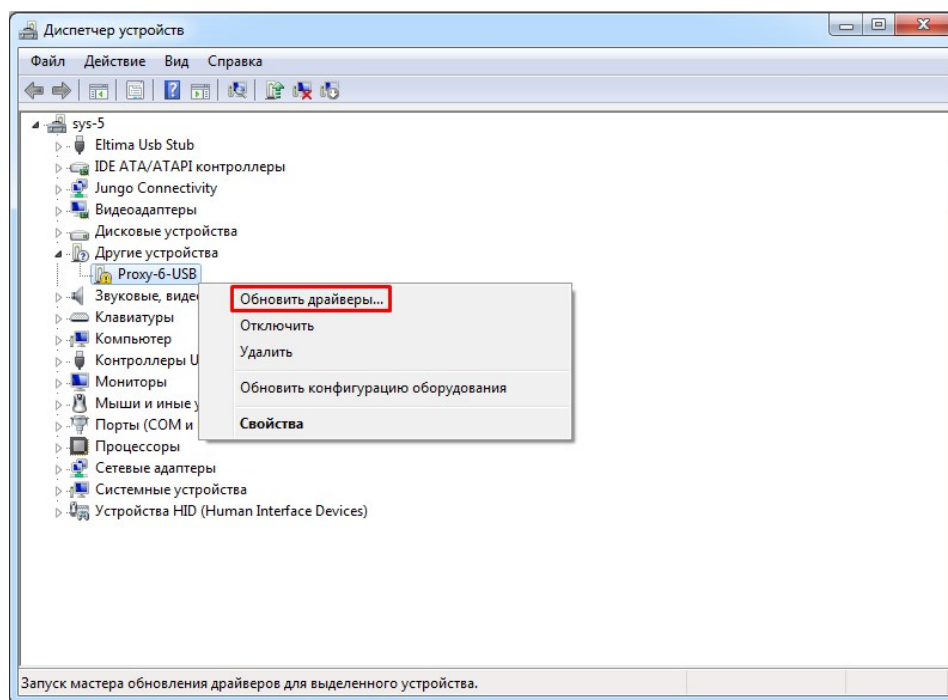


Рис.7 Обновление драйвера

В появившемся окне обновления драйверов устройства выбрать пункт «Выполнить поиск драйверов на этом компьютере».

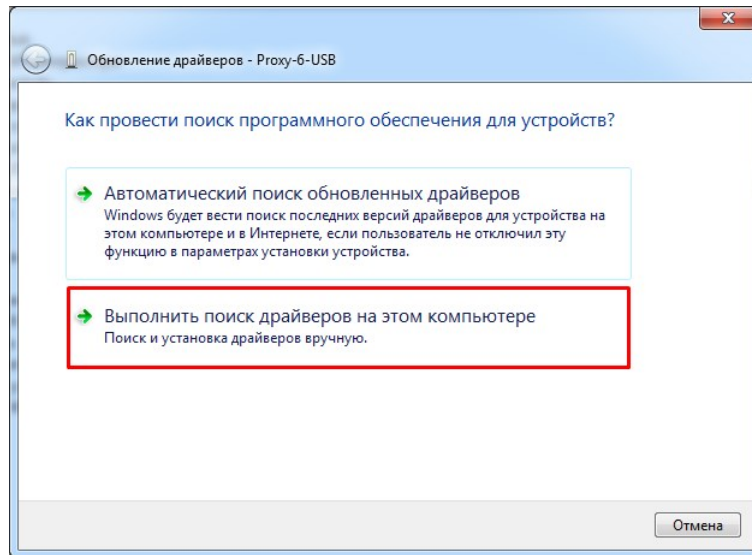


Рис.8 Поиск драйверов на ПК

В появившемся окне следует указать путь к папке с драйвером, а затем нажать кнопку «Далее» (Драйвер можно указать, как в папке с ПО «UProgProxy-6 v.x.x», так и в папке с ПО «UProgProxy-6-USB Security v.x.x»).

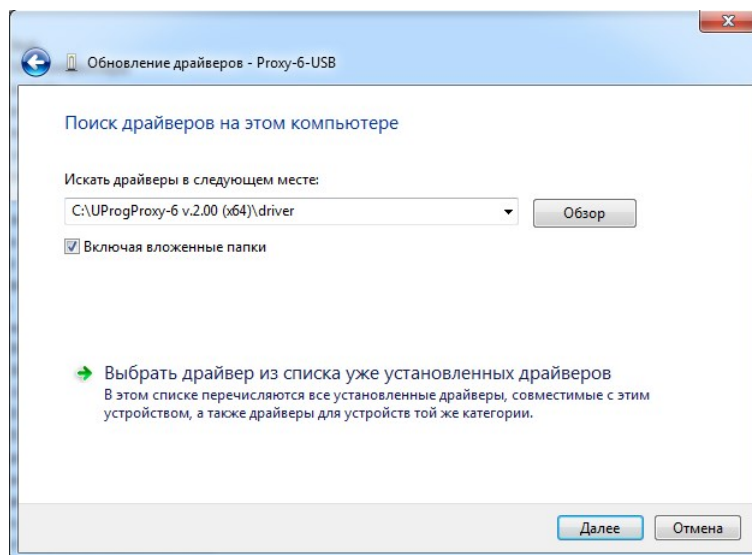


Рис.9 Выбор пути к папке с драйвером

По окончании установки драйверов появится соответствующее окно (см. рис.10).

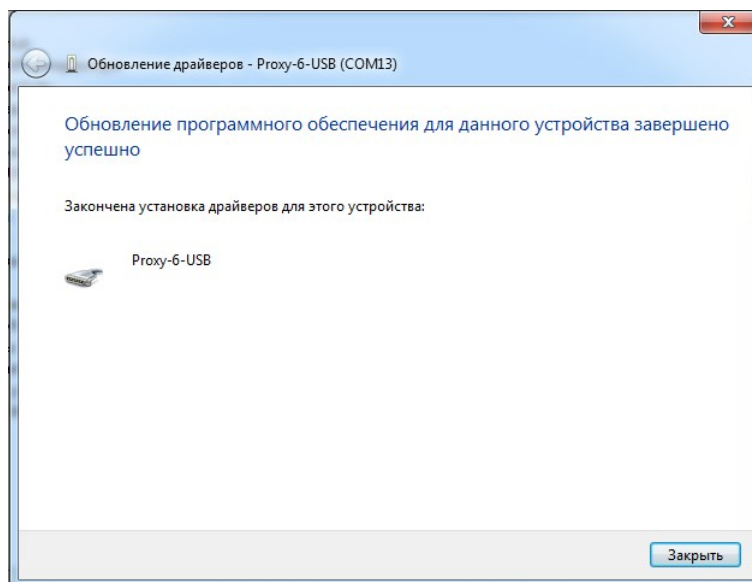


Рис.10 Завершение установки драйвера

Нажмите на кнопку «Закреть» и закройте «Диспетчер устройств».

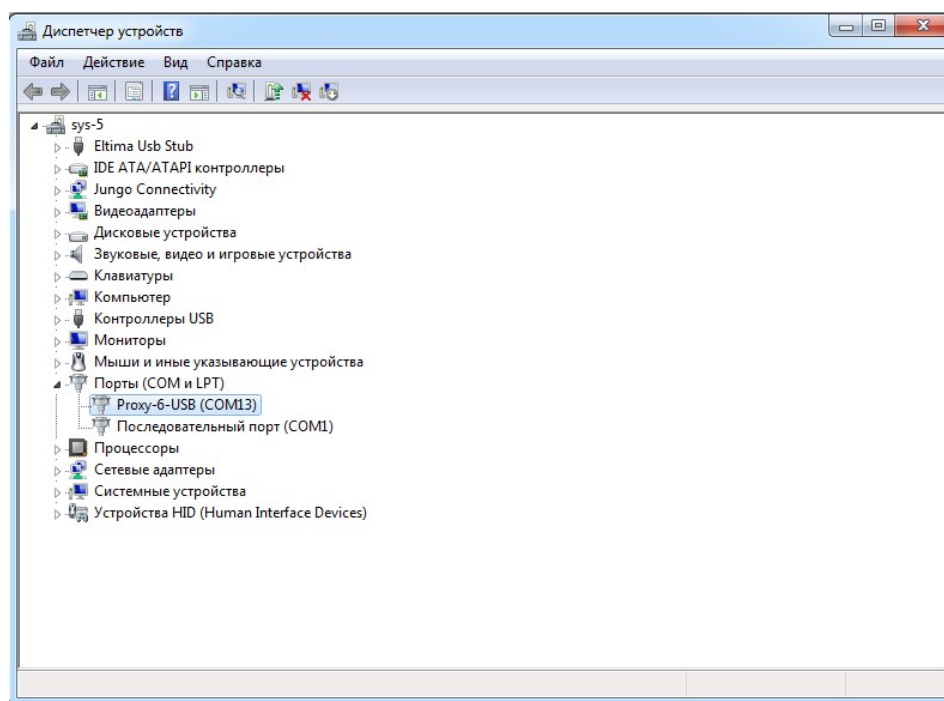


Рис.11 Диспетчер устройств ОС Windows 7

2.2.5 Настройка прибора

Основные сведения и настройка ПО «UProgProxy-6 v.2.00»

ПО «UProgProxy-6 v.2.00» (в дальнейшем – программа) предназначено и для настройки считывателя «Proxy-6-USB-G (-B, -W)».

Программу нужно установить, следуя инструкциям во время установки.

Для начала работы с программой следует запустить исполняемый файл «UProgProxy-6 v.2.00.exe» через меню «Пуск» либо через ярлык на рабочем столе.

После запуска программы нужно перейти на вкладку «Proxy-6-USB».

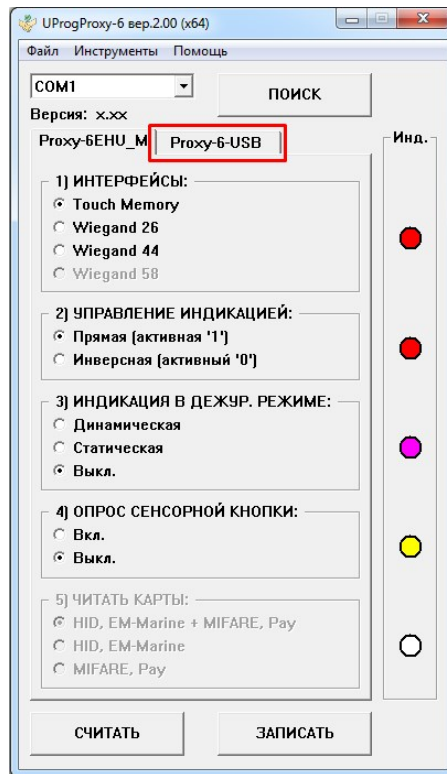


Рис.12 Выбор типа считывателя

Программа автоматически найдет считыватель с отображением номера СОМ-порта. Нужно подтвердить завершение поиска, нажав на кнопку «ОК».

После этого программа считывает настройки со считывателя и также сообщит, что «Настройки считаны!». Нужно подтвердить считывание настроек, нажав на кнопку «ОК».

Интерфейс программы обновится в соответствии с настройками считывателя.

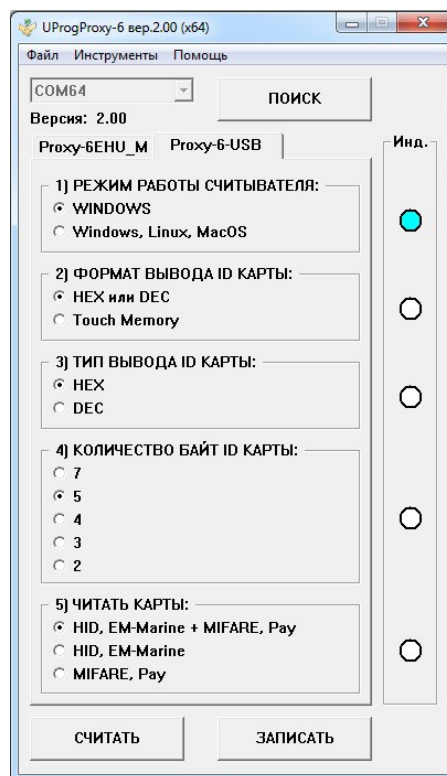


Рис.13 Интерфейс вкладки «Proxy-6-USB»

Вкладка «Proxy-6-USB» разделена на пять областей:

- 1 – «РЕЖИМ РАБОТЫ СЧИТЫВАТЕЛЯ» (разница между разными режимами описана в п.1.4 настоящего руководства).
- 2 – «ФОРМАТ ВЫВОДА ID КАРТЫ» (HEX или DEC – шестнадцатеричная или десятичная система счислений; Touch Memory – формат по типу электронных идентификаторов iButton).
- 3 – «ТИП ВЫВОДА ID КАРТЫ» (задаём тип при выборе в пункте 2 настройки «HEX» или «DEC»).
- 4 – «КОЛИЧЕСТВО БАЙТ UID КАРТЫ» (размер кода карты в байтах: 7,5,4,3,2).
- 5 – «ЧИТАТЬ КАРТЫ» (задаём тип карт с которыми будем работать).

После того, как все настройки заданы, нужно нажать на кнопку «ЗАПИСАТЬ». Программа сообщит, что «Настройки записаны!». Нужно подтвердить завершение записи настроек, нажав на кнопку «ОК». Теперь считыватель работает в соответствии заданных настроек.

Основные сведения и настройка ПО «UProgProxy-6-USB Security v.2.00»

ПО «UProgProxy-6-USB Security v.2.00» (в дальнейшем – программа) предназначено для программирования мастер-карт и пользовательских карт, которые впоследствии будут использоваться совместно со считывателями «Proxy-6ЕНМ-G (-B, -W)».

Программу нужно установить, следуя инструкциям во время установки.

Для начала работы с программой следует запустить исполняемый файл «UProgProxy-6-USB Security v.2.00.exe» через меню «Пуск» либо через ярлык на рабочем столе.

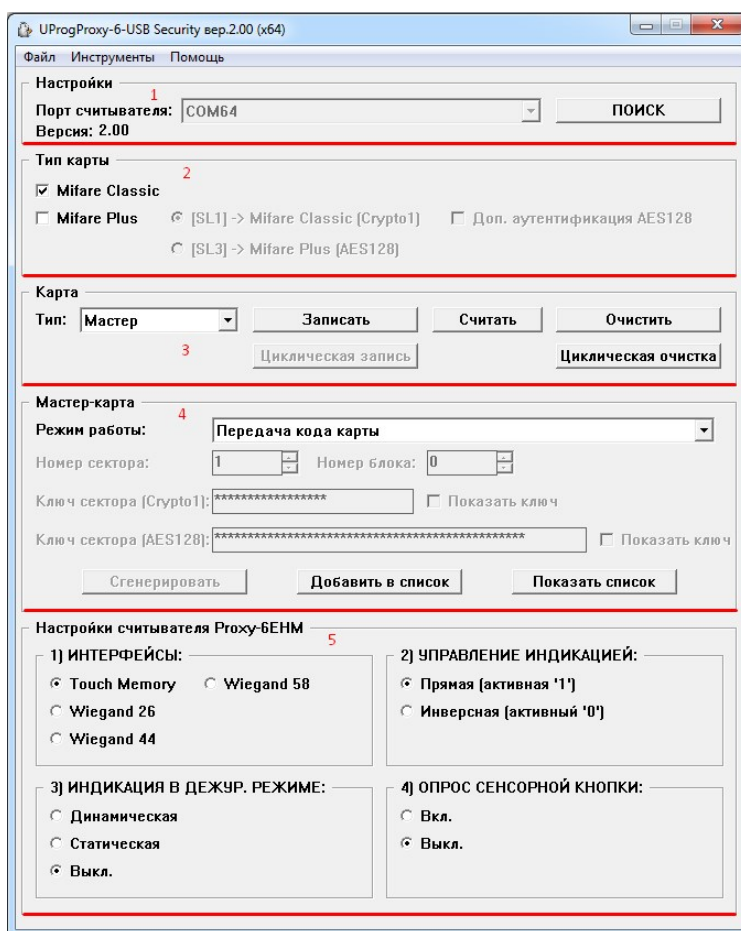


Рис.14 Интерфейс ПО «UProgProxy-6-USB Security v.2.00»

Программа автоматически найдёт считыватель с отображением номера СОМ-порта. В противном случае следует в области «Настройки» нажать кнопку «ПОИСК», после чего программа повторно произведёт поиск считывателя и обновит список СОМ-портов. В том случае, если программе не удалось найти считыватель, а в «Диспетчере устройств» -> «Порты СОМ и LPT» считыватель отображается, то необходимо в программе из списка «Порт считывателя» выбрать тот СОМ-порт, который отображается в «Диспетчере устройств». Программа попытается подключиться к считывателю непосредственно через данный СОМ-порт.

Основное окно программы разделено на пять областей:

- 1 – «Настройки» - область, в которой расположена кнопка для «ручного» поиска считывателя, а также отображается номер СОМ-порта и версия считывателя;
- 2 – «Тип карты» - область, в которой реализован выбор карт: «MIFARE Classic» или «MIFARE Plus» с дополнительными настройками;
- 3 – «Карта» - область, в которой реализован выбор карт: «Мастер» или «Пользователь»;
- 4 – «Мастер-карта» - область, в которой задаются настройки пользовательской карты, а именно выбираем режим работы, область памяти и определяем ключ(и) секторов карты.
- 5 – «Настройки считывателя Proху-бЕНМ» - область, в которой задаем настройки считывателя «Proху-бЕНМ-G (-B, -W)».

Если выбрать карту «Пользователь», то интерфейс программы изменится: область 5 сменится на область «Пользовательская карта» и добавится область 6 «Конвертер пользовательской карты».

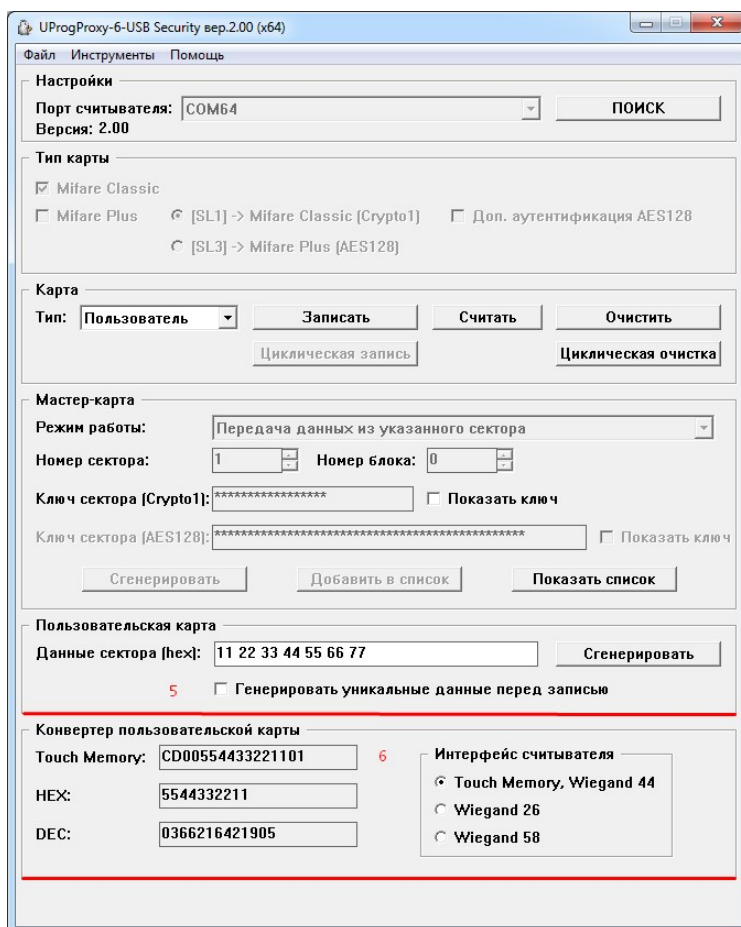


Рис.15 Интерфейс ПО «UProgProxy-6-USB Security v.2.00»

5 – «Пользовательская карта» - область, в которой задаем собственный UID карты.

6 – «Конвертер пользовательской карты» - область, в которой отображается заданный UID карты в различных форматах. Формат зависит от выбора в области «Интерфейс считывателя» (выбираем тот интерфейс считывателя, который используется в СКУД считывателем Proxu-6ЕНМ).

Работа со списком ключей секторов

При программировании карт для защищённых режимов работы предусмотрен список ключей секторов, которыми будет оперировать программа. Данный список нужен для хранения ключей секторов, которые когда-либо использовались в программе. Также в списке находятся стандартные транспортные ключи «FF FF FF FF FF FF» (Crypto-1) и «FF FF» (AES 128).

Работа со списком ключей секторов доступна во всех режимах.

Карта MIFARE Classic, MIFARE Plus (SL1)

Запись в сектора карт осуществляется только на новые карты либо в очищенные сектора. Чтение или очистка мастер-карт не требует кого-либо дополнительного ввода в поле «Ключ сектора [Crypto1]». При чтении или очистки секторов пользовательских карт программа обращается к сектору карты ключом, введённым в поле «Ключ сектора [Crypto1]».

Обязательно сформируйте ключ сектора AES 128 для карт *MIFARE Plus (SL1)*.



Ключи сектора AES 128 нельзя стереть, перезаписать или изменить после программирования карт!

Даже, если карту, в будущем, необходимо будет перевести на уровень безопасности (SL3), то ключ сектора не изменится!

Карта MIFARE Plus (SL3)

Запись в сектора карт осуществляется на новые карты (уровень безопасности SL0) и не требуется предварительно очищать сектора, если карты уже были персонализированы. Чтение или очистка мастер-карт не требует кого-либо дополнительного ввода в поле «Ключ сектора [AES128]». При чтении или очистки секторов пользовательских карт программа обращается к сектору карты ключом, введённым в поле «Ключ сектора [AES128]».

Карты MIFARE

Для обеспечения возможности последующего перепрограммирования секторов пользовательских карт, нужно хранить все когда-либо использовавшиеся ключи секторов в списке ключей программы.



Ключи сектора AES 128 нельзя стереть, перезаписать или изменить после программирования карт!

Храните ключ сектора AES 128 в строжайшем секрете, иначе теряется весь смысл в криптостойком алгоритме AES 128!

Список ключей вместе с настройками считывателя «Proxu-6ЕНМ-G (-B, -W)» хранится в зашифрованном виде в файле «crkeys.data», который находится в папке с программой. Для открытия списка ключей следует нажать кнопку «Показать список» в основном окне программы. Рекомендуем, время от времени, копировать файл «crkeys.data» и хранить отдельно.

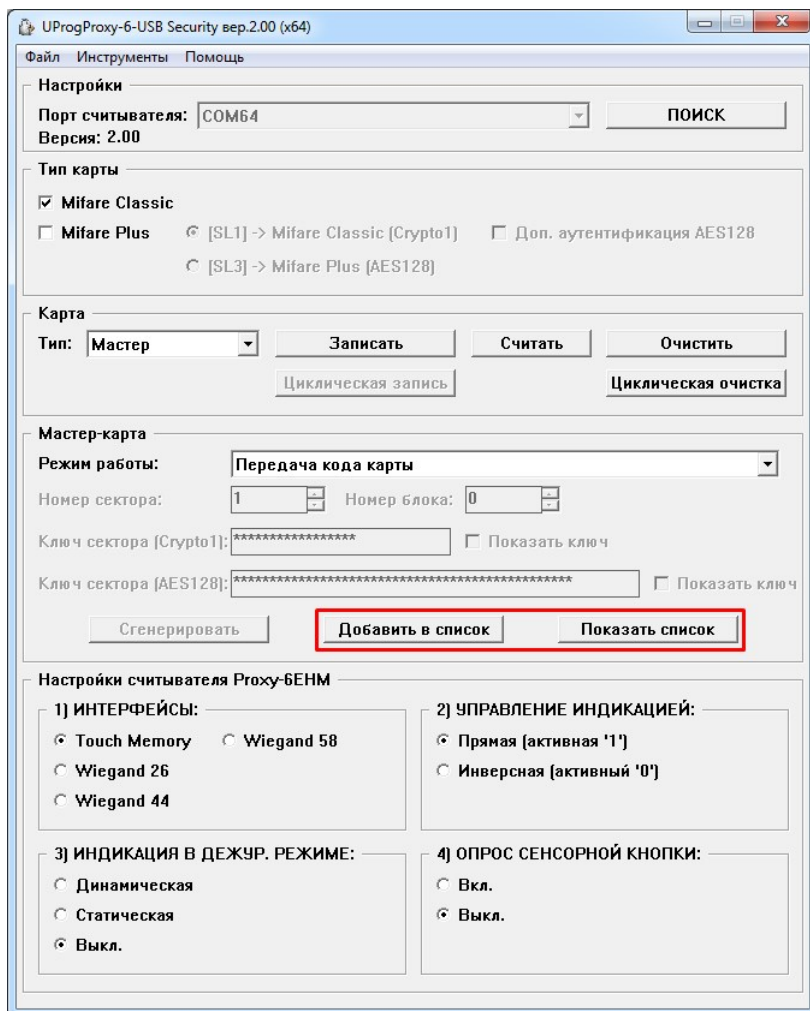


Рис.16 Основное окно программы с активными кнопками списка ключей

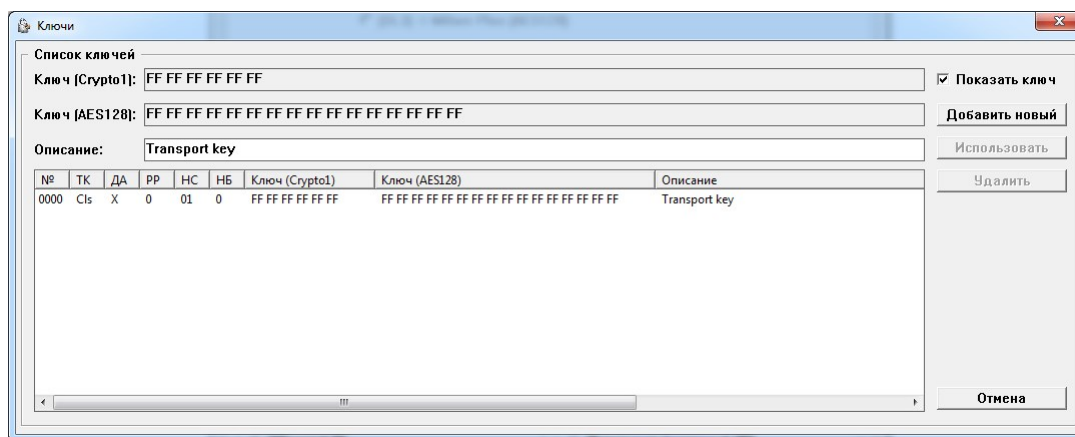


Рис.17 Список ключей

По умолчанию все ключи в окне списка ключей закрыты «звёздочками». Для отображения ключей следует установить галочку «Показать ключ».

Добавить ключи в список можно только из основного окна программы, нажав кнопку «Добавить в список». При этом в список добавятся ключи, который введены (или не введены) в поле «Ключ сектора [Crypto1]» и в поле «Ключ сектора [AES128]» основного окна программы. В поле «Описание» ввести описание ключа/ключей, а затем нажать кнопку «Добавить новый».

Для удаления ключа/ключей из списка следует выбрать ту строку, которую необходимо удалить и нажать кнопку «Удалить». Далее подтвердить выбор.

Чтобы выбрать ключ/ключи, которые предполагается использовать при программировании карт, следует отметить ключ/ключи в списке одним кликом левой клавишей мыши и нажать кнопку «Использовать». Окно с ключами при этом закрывается, а в поля ввода «Ключ сектора [Crypto1]» и «Ключ сектора [AES128]» основного окна программы запишутся выбранные ключи. Также отобразится вся информация мастер-карты, начиная с «Тип карты» и заканчивая «Настройки считывателя Proху-БЕНМ».

Выбрать ключ/ключи можно и двойным кликом левой клавишей мыши, при этом, ключи вместе с описанием отобразятся в соответствующих полях ввода окна «Ключи».

Ключи сектора можно ввести с клавиатуры либо сгенерировать случайным образом кнопкой «Сгенерировать» в основном окне программы.

В списке ключей, кроме самих ключей и описания, отображается дополнительная информация:

- 1) *№* – Номер ключа/ключей в списке.
- 2) *ТК* – Тип карты (*СIs* – MIFARE Classic; *SL1* - MIFARE Plus (SL1); *SL3* - MIFARE Plus (SL3)).
- 3) *ДА* – Дополнительная аутентификация (*X* - не используется; *V* - используется).
- 4) *РР* – Режим работы (по списку в основном окне: *0* – «Передача кода карты», *1* – «Передача данных из указанного сектора», *2* – «Передача кода карты после успешной авторизации к сектору», *3* – «Передача данных из указанного сектора (с шифрованием)»).
- 5) *НС* – номер сектора (*01* – *15*).
- 6) *НБ* – номер блока (*0-2*).

Настройки считывателя «Proху-БЕНМ-G (-B, -W)» не отображаются. Их можно просмотреть в основном окне при выборе ключа/ключей.

Особенности персонализации карт MIFARE Plus (SL1, SL3)

SLx – (Security Level x) уровень безопасности x. Для карт MIFARE Plus доступны четыре уровня безопасности: *SL0*, *SL1*, *SL2*, *SL3*.

- SL0* – начальная конфигурация поставки, используется для персонализации карт. (Доступен только UID карты завода-изготовителя!)
- SL1* – функциональный режим обратной совместимости с MIFARE Classic (Crypto-1) с опциональной аутентификацией AES 128.
- SL2* – обязательная аутентификация AES 128 с шифрованием данных Crypto-1. (Редко используется данный уровень и не все карты поддерживают, поэтому и не реализована поддержка в считывателе!)
- SL3* – наивысший уровень, используется криптостойкий алгоритм шифрования AES 128 для защиты от несанкционированного доступа и клонирования.

Персонализация и повышение уровня безопасности карт MIFARE Plus происходит в следующем порядке:



SL0 → *SL1* → *SL3* (или) *SL0* → *SL1* (или) *SL1* → *SL3*

Понизить уровень безопасности карты невозможно!

SL0 ✘ *SL1* ✘ *SL3*

Программирование ключа сектора AES 128, карт MIFARE Plus, происходит уже на уровне персонализации *SL0* -> *SL1*.



Очень важно сохранить ключи сектора, иначе вы не сможете воспользоваться дополнительной аутентификацией на уровне безопасности SL1, не сможете в будущем перевести карту с уровня SL1 -> SL3 и не сможете получить доступ к сектору, если карта уже переведена на уровень SL3.

Ключи сектора AES 128 нельзя стереть, перезаписать или изменить после программирования карт!

Дополнительная аутентификация AES 128 на уровне безопасности SL1

Карты *MIFARE Plus (SL1)* можно использовать в СКУД, как карты MIFARE Classic без каких либо изменений, но и без каких-либо улучшений в плане безопасности. Для повышения безопасности возможно применить дополнительную аутентификацию AES 128.

Плюсы дополнительной аутентификации: наименьшее количество усилий по обновлению инфраструктуры считывателей.

Недостатки: ограниченное улучшение безопасности.

Пример: Представим себе, что есть объекты «А» и «Б». На этих объектах используют считыватели с картами MIFARE Classic. Тогда модернизацию СКУД можно провести следующим образом:

Объект «А» - не требует дополнительной защиты (и/или обновление считывателей невозможно).

Объект «Б» - необходимо обеспечить безопасность (и/или считыватели могут быть модернизированы).

Внимание! Не все карты MIFARE Plus поддерживают дополнительную аутентификацию AES 128. Лучший способ убедиться в том, что карта поддерживает дополнительную аутентификацию – это запрограммировать пользовательскую карту (см. описание ниже).

Также можно ориентироваться на следующий список: MIFARE Plus (S, SE, X) – **НЕ** поддерживают дополнительную аутентификацию AES 128; MIFARE Plus (EVx) – поддерживают.

Программирование карт в режиме «Передача кода карты»

MIFARE Classic

В данном режиме программируется только мастер-карта. Задаётся режим работы чтение UID любой карты и настройки считывателя «Proxu-6EHM-G (-B, -W)».

Для программирования карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Classic».
3. В выпадающем списке «Режим работы» выбрать «Передача кода карты».
4. Задать настройки считывателя в области «Настройки считывателя Proxu-6EHM».
5. Нажать кнопку «Записать».

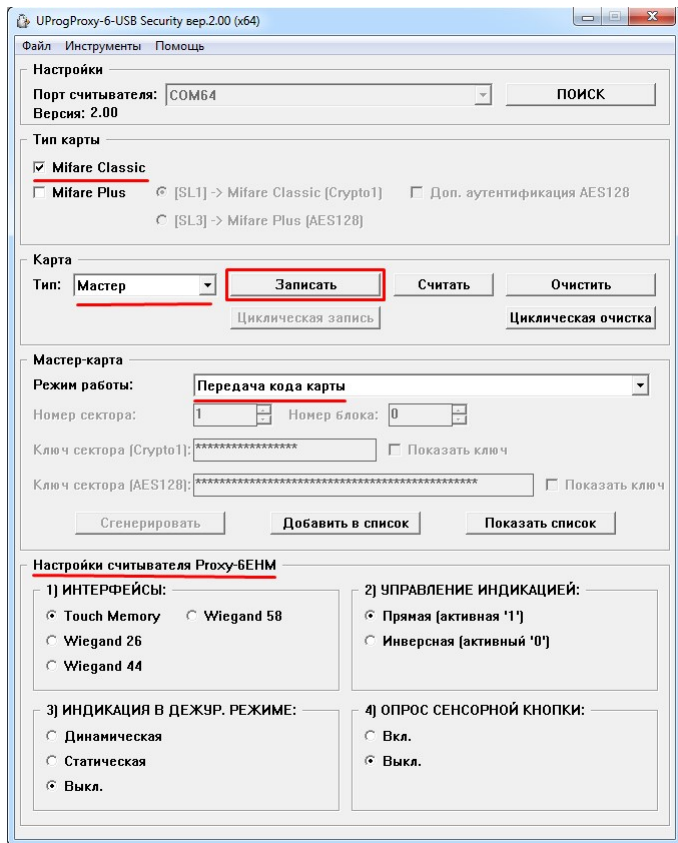
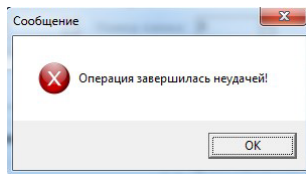


Рис.18 Программирование мастер-карты

Если в процессе программирования возникли ошибки, то программа выдаст следующее сообщение:



или

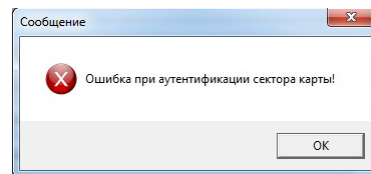


Рис.21 Ошибка при записи карты

В этом случае следует повторить процедуру программирования карты. Если ошибка повторилась, следует обратиться к пункту «Решение проблем при программировании карт» настоящего руководства.

MIFARE Plus

В данном режиме программируется мастер-карта. Задаётся режим работы чтение UID любой карты и настройки считывателя «Proxu-6ЕНМ-G (-B, -W)».

Для программирования карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Plus». (Выбор SL1, SL3 или доп. аутентификация, здесь, не имеет значение.)
3. В выпадающем списке «Режим работы» выбрать «Передача кода карты».
4. Задать настройки считывателя в области «Настройки считывателя Proxu-6ЕНМ».
5. Нажать кнопку «Записать».

Появится окно ожидания «Поднесите карту»:

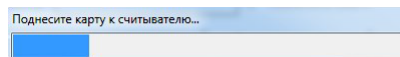


Рис.19 Ожидание карты

Если перед нажатием кнопки «Записать» карта была приложена к считывателю, то удалите её и поднесите заново. Удерживайте карту пока не закончится программирование карты. Если карта запрограммирована успешно, то программа выдаст следующее сообщение:

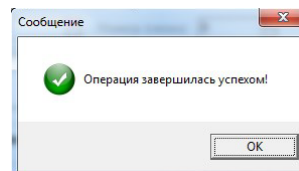
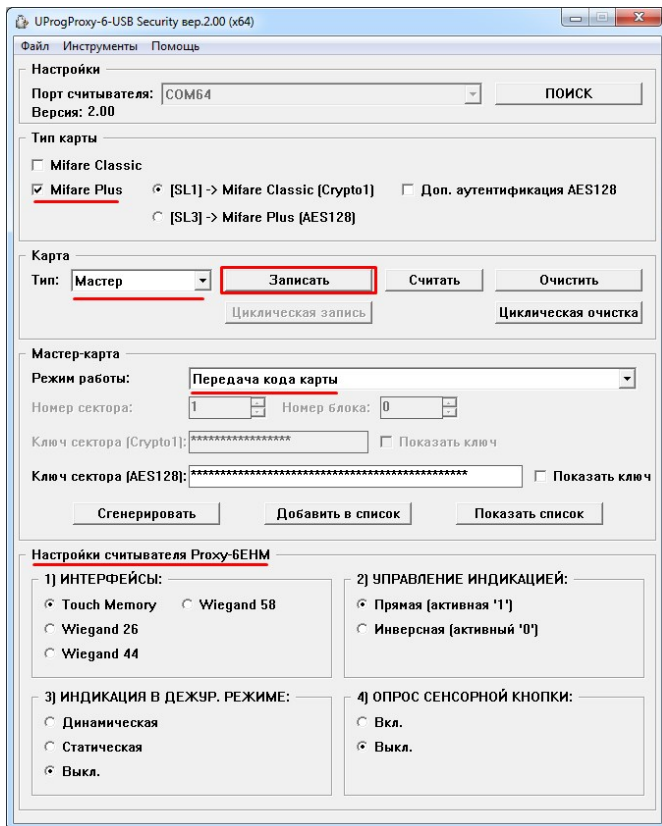


Рис.20 Успешная запись карты



Мастер-карта **MIFARE Plus** программируется единожды и навсегда остается мастер-картой. Кнопка «Очистить» приведет только к тому, что сотрутся заданные настройки считывателя. На мастер-карту MIFARE Plus можно записывать различную конфигурацию считывателя, но перевести мастер-карту в пользовательскую уже невозможно!



Программирование пользовательских карт MIFARE Classic, в режиме «Передача кода карты», невозможно. Для карт MIFARE Plus возможно персонализировать карту (перевести с SL0 на SL1 или SL3), на будущее, но в этом особого смысла нет. «Собственный UID» в карту не прописывается, можно сказать, что карта «пустая», поэтому лучше производить персонализацию карт в других оставшихся режимах.

(Не забываем сохранить ключ сектора AES 128!).

Дальнейшие окна/сообщения аналогичны, как в **MIFARE Classic** описанные выше.

Рис.22 Программирование мастер-карты

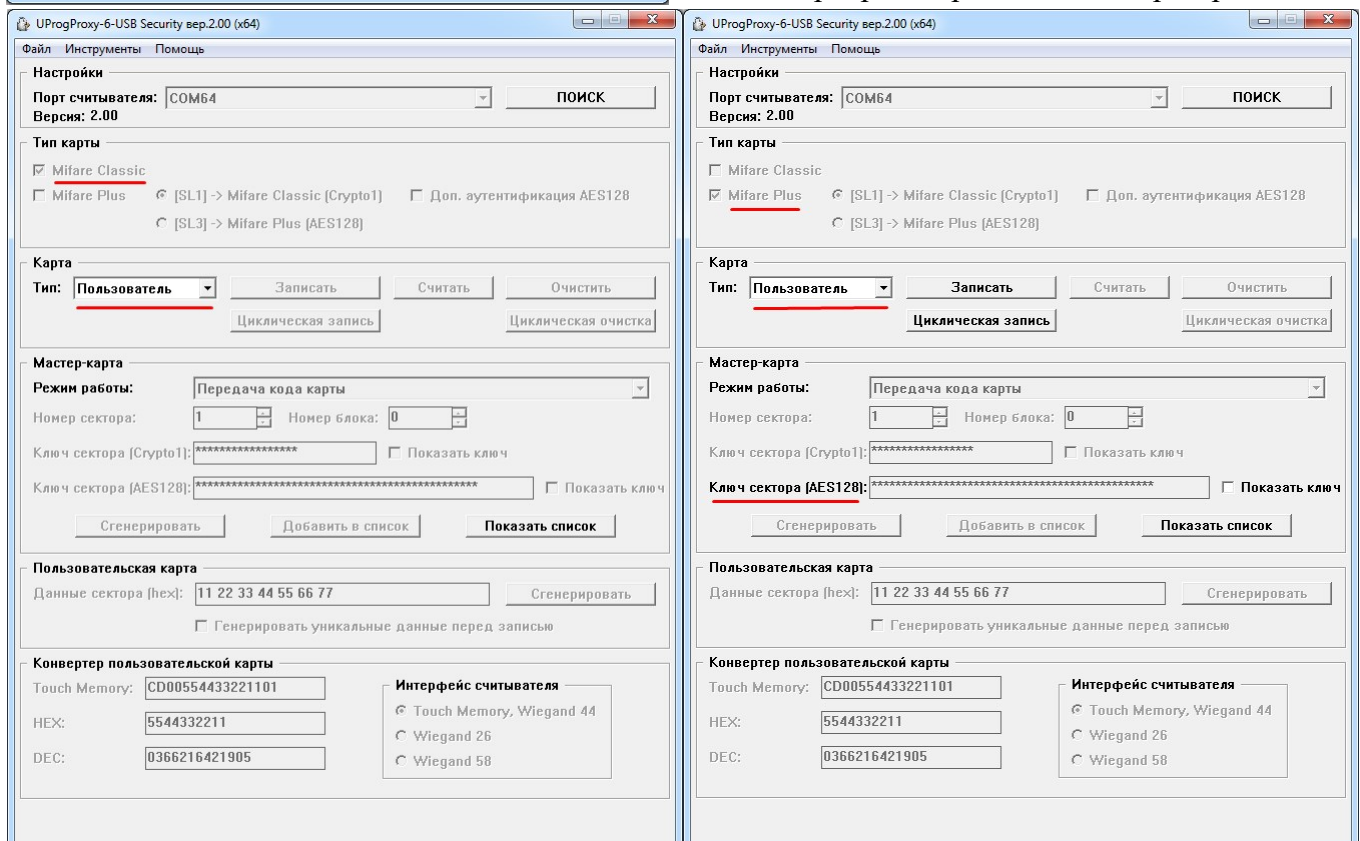


Рис.23 Программирование пользовательской карты



Пользовательская карта **MIFARE Plus** программируется единожды и навсегда остается пользовательской с заданным ключом сектора. Кнопка «Очистить» приведет только к тому, что сотрется заданный UID («Данные сектора») карты. На пользовательскую карту MIFARE Plus можно записывать различные данные сектора, но перевести пользовательскую карту в мастер-карту уже невозможно!

Программирование карт в режиме «Передача данных из указанного сектора» / «Передача данных из указанного сектора (с шифрованием)»

С точки зрения программирования карт, защищенные режимы работы «Передача данных из указанного сектора» и «Передача данных из указанного сектора (с шифрованием)» ничем не отличаются.

MIFARE Classic

Для программирования мастер-карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Classic».
3. В выпадающем списке «Режим работы» выбрать «Передача данных из указанного сектора» или «Передача данных из указанного сектора (с шифрованием)».
4. В поле «Номер сектора» ввести номер сектора (от 1 до 15), к которому будет проводиться авторизация.
5. В поле «Номер блока» ввести номер блока (от 0 до 2), в котором будет храниться код карты.

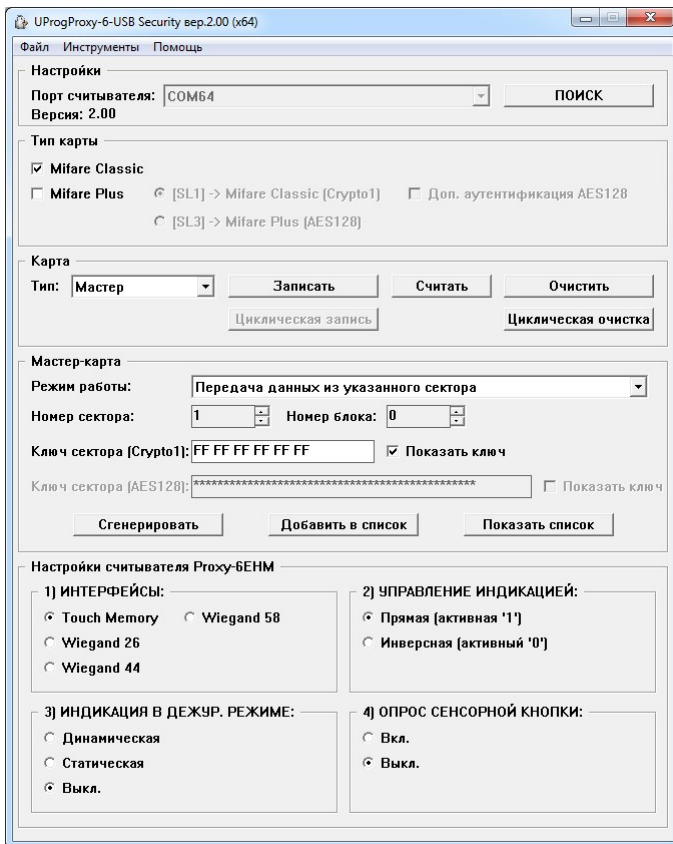


Рис.24 Программирование мастер-карты

6. В поле «Ключ сектора [Crypto1]» ввести ключ сектора (6 байт в шестнадцатеричном формате) или сгенерировать, либо выбрать ключ из списка.
7. Задать настройки считывателя в области «Настройки считывателя Proxу-6ЕНМ».
8. Нажать кнопку «Записать».

Появится окно ожидания «Поднесите карту»:

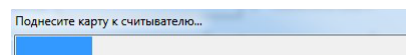


Рис.25 Ожидание карты

Если перед нажатием кнопки «Записать» карта была приложена к считывателю, то удалите её и поднесите заново. Удерживайте карту, пока не закончится программирование карты. Если карта запрограммирована успешно, то программа выдаст следующее сообщение:

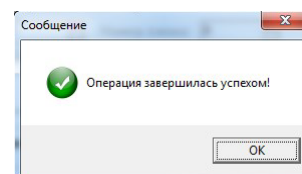
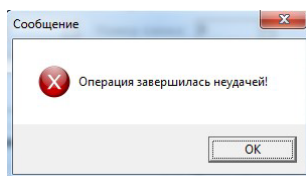


Рис.26 Успешная запись карты

Если в процессе программирования возникли ошибки, то программа выдаст следующее сообщение:



или

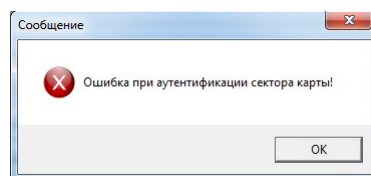


Рис.27 Ошибка при записи карты

В этом случае следует повторить процедуру программирования карты. Если ошибка повторилась, следует обратиться к пункту «Решение проблем при программировании карт» настоящего руководства.

MIFARE Plus

Для программирования мастер-карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Plus».
3. Задать определение пользовательской карты: [SL1] Mifare Classic (с или без доп. аутентификацией AES128) или [SL3] Mifare Plus.
4. В выпадающем списке «Режим работы» выбрать «Передача данных из указанного сектора» или «Передача данных из указанного сектора (с шифрованием)».
5. В поле «Номер сектора» ввести номер сектора (от 1 до 15), к которому будет проводиться авторизация.
6. В поле «Номер блока» ввести номер блока (от 0 до 2), в котором будет храниться код карты.
7. В [SL1], в поле «Ключ сектора [Crypto1]» и в поле «Ключ сектора [AES128]» ввести

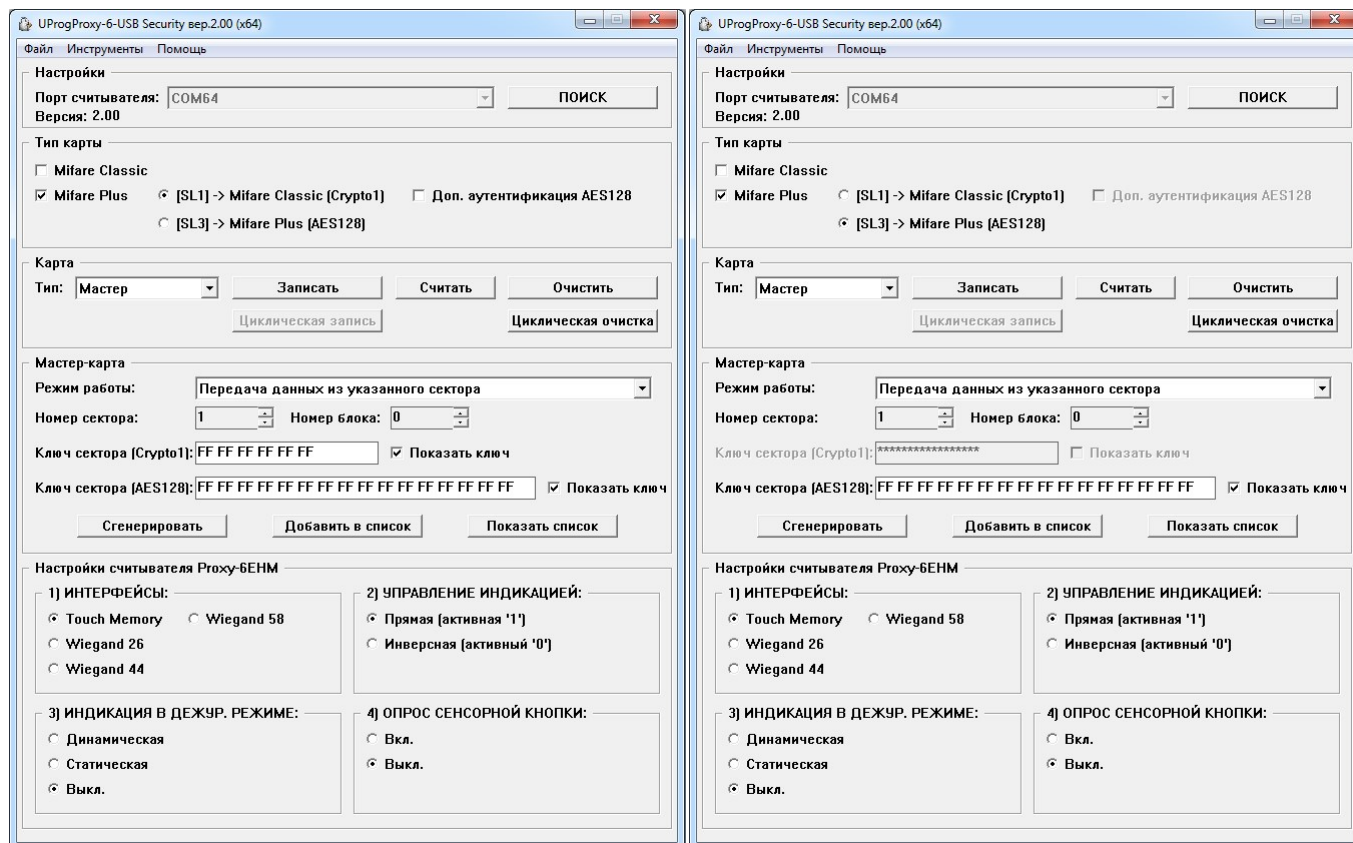


Рис.28 Программирование мастер-карты

ключ сектора (6 байт и 16 байт соответственно в шестнадцатеричном формате) или сгенерировать, либо выбрать ключ/ключи из списка.

В [SL3] работаем только с полем «Ключ сектора [AES128]».

8. Задать настройки считывателя в области «Настройки считывателя Proxu-6ЕНМ».

9. Нажать кнопку «Записать».

Дальнейшие окна/сообщения аналогичны, как в *MIFARE Classic* описанные выше.



Особенности мастер-карт MIFARE Plus, описаны выше в разделе «Программирование карт в режиме «Передача кода карты»».

Для программирования пользовательской карты необходимо выполнить следующие действия:

1. Сформировать мастер-карту, как описано выше (или выбрать мастер-карту из списка, если ранее уже была создана).
2. В выпадающем списке «Тип» следует выбрать «Пользователь».
3. В поле «Данные сектора [hex]» ввести код карты (7 байт в шестнадцатеричном формате), либо нажать кнопку «Сгенерировать».
4. Нажать кнопку «Записать».

Примечание. В область «Конвертер пользовательской карты» ничего не нужно вводить. Данная область – это вспомогательная область, которая отображает пользовательский ключ в различных форматах и в зависимости от выбранного интерфейса считывателя «Proxu-6ЕНМ-G (-B, -W)». Имейте ввиду, что версия считывателя «Proxu-6ЕНМ-G (-B, -W) v.1.00» использует максимум 5 младших байт кода карты из 7 введенных (сгенерированных), а версия считывателя «Proxu-6ЕНМ-G (-B, -W) v.1.10» и выше выдаст уже все 7 байт только при интерфейсе Wiegand 58.

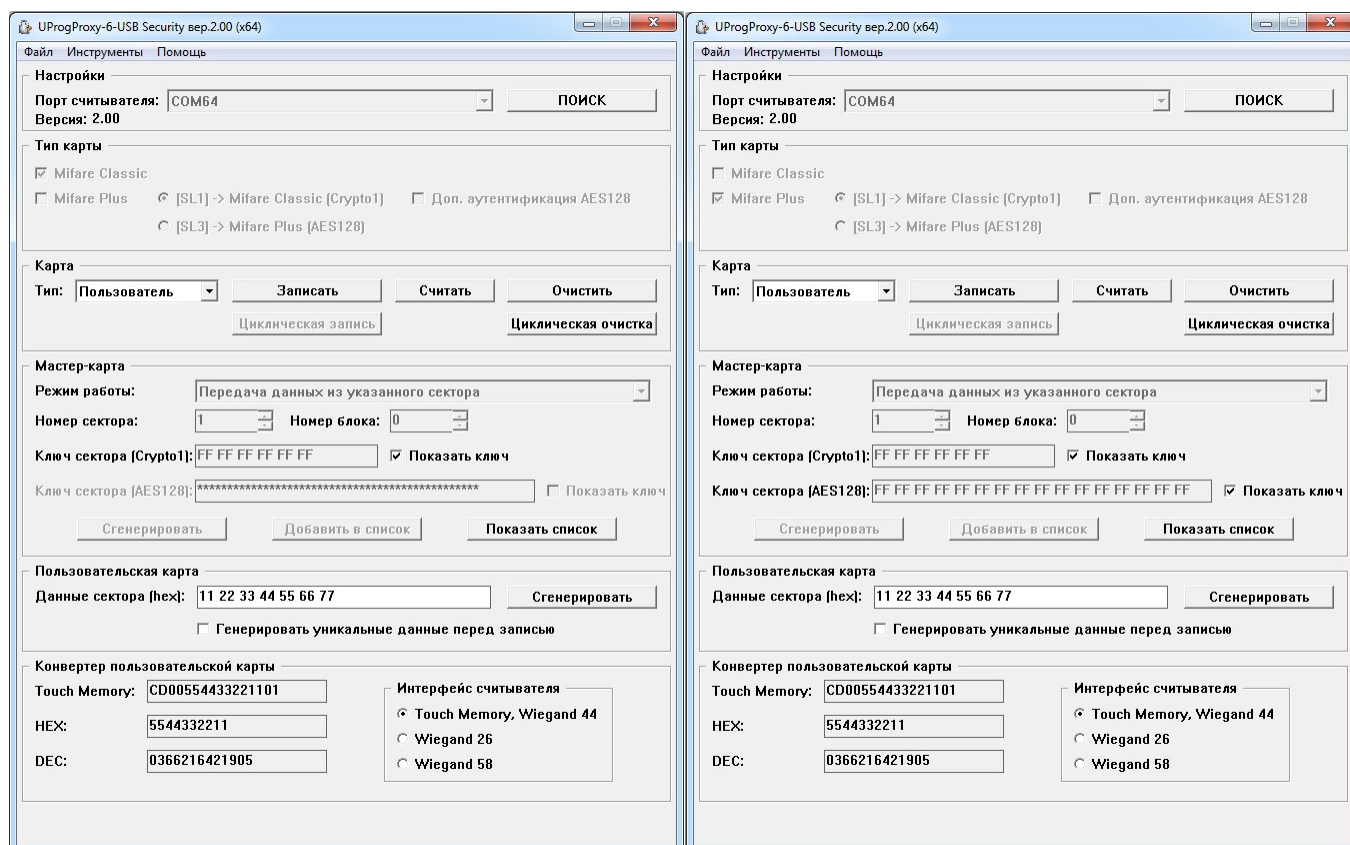
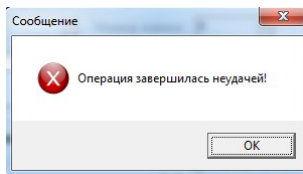




Рис.29 Программирование пользовательской карты

Если в процессе программирования возникли ошибки, то программа выдаст следующее сообщение:



или

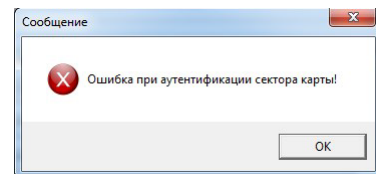


Рис.32 Ошибка при записи карты

В этом случае следует повторить процедуру программирования карты. Если ошибка повторилась, следует обратиться к пункту «Решение проблем при программировании карт» настоящего руководства.



Особенности пользовательских карт MIFARE Plus, описаны выше в разделе «Программирование карт в режиме «Передача кода карты»».

В программе предусмотрен генератор уникальных данных, который позволяет перед записью карты генерировать неповторяющиеся 7 ми байтные коды. Все когда-либо сгенерированные программой коды хранятся в файле «usersData.data» в папке с программой в открытом виде. После генерации очередного кода программа сверяется с этим списком, чтобы код не совпадал со сгенерированными ранее кодами.

Для использования функции генерации уникальных кодов необходимо в области «Пользовательская карта» основного окна программы установить галочку «Генерировать уникальные данные перед записью». При этом поле «Данные сектора [hex]» и кнопка «Сгенерировать» станут неактивными.

Появится окно ожидания «Поднесите карту»:

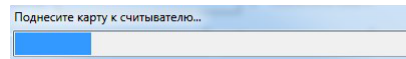


Рис.30 Ожидание карты

Если перед нажатием кнопки «Записать» карта была приложена к считывателю, то удалите её и поднесите заново. Удерживайте карту, пока не закончится программирование карты. Если карта запрограммирована успешно, то программа выдаст следующее сообщение:

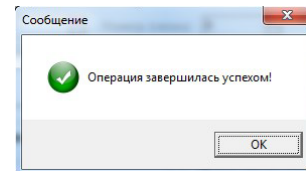


Рис.31 Успешная запись карты

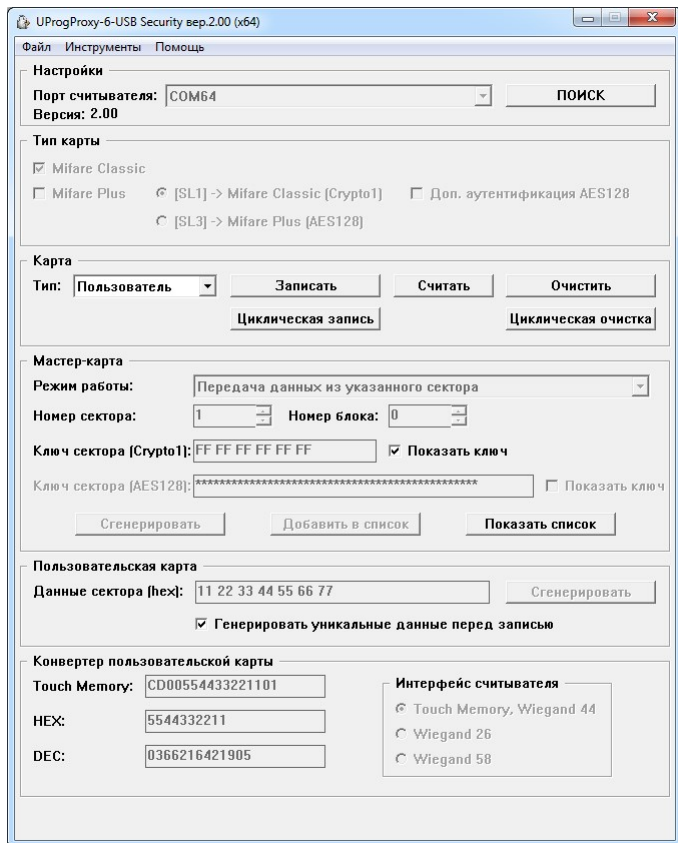


Рис.33 Генерация уникальных кодов

При каждом нажатии кнопки «Записать» программа будет генерировать уникальный код и записывать его в карту. Сгенерированный код будет отображаться в неактивном поле «Данные сектора [hex]». Если требуется запрограммировать большое количество карт, то нужно нажать кнопку «Циклическая запись». При этом программа отобразит следующее окно:

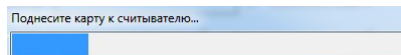


Рис.34 Ожидание карты

Затем следует подносить карты к считывателю по одной. После завершения программирования карты полоса прогресса вернется в исходное состояние «Ожидание новой карты». После этого можно подносить следующую карту. По окончании программирования партии карт ничего не нужно делать, полоса прогресса дойдет до конца, и процесс завершится отобразив следующее окно:

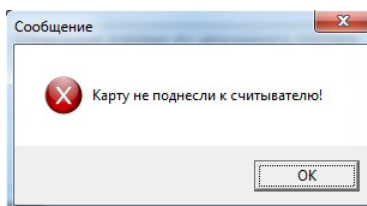


Рис.35 Окно окончания массового программирования карт

Программирование карт в режиме «Передача кода карты после успешной авторизации к сектору»

MIFARE Classic

Для программирования мастер-карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Classic».
3. В выпадающем списке «Режим работы» выбрать «Передача кода карты после успешной авторизации к сектору».
4. В поле «Номер сектора» ввести номер сектора (от 1 до 15), к которому будет проводиться авторизация.
5. В поле «Ключ сектора [Crypto1]» ввести ключ сектора (6 байт в шестнадцатеричном формате) или сгенерировать, либо выбрать ключ из списка.
6. Задать настройки считывателя в области «Настройки считывателя Проху-6ЕНМ».
7. Нажать кнопку «Записать».

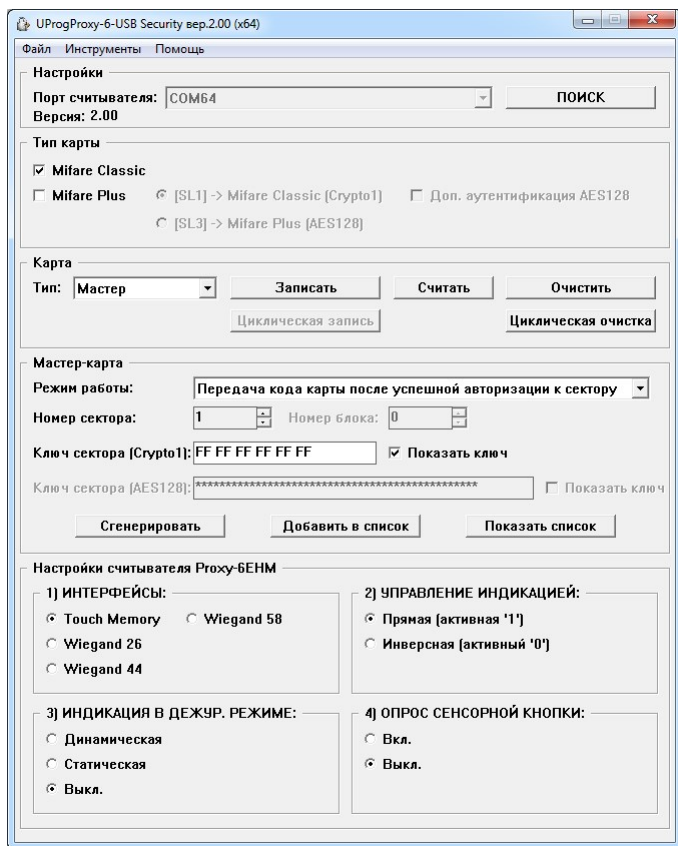
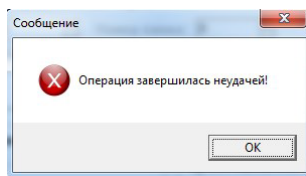


Рис.36 Программирование мастер-карты

Если в процессе программирования возникли ошибки, то программа выдаст следующее сообщение:



или

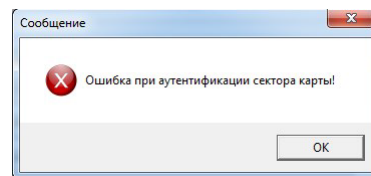


Рис.39 Ошибка при записи карты

В этом случае следует повторить процедуру программирования карты. Если ошибка повторилась, следует обратиться к пункту «Решение проблем при программировании карт» настоящего руководства.

MIFARE Plus

Для программирования мастер-карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Plus».
3. Задать определение пользовательской карты: [SL1] Mifare Classic (с или без доп. аутентификацией AES128) или [SL3] Mifare Plus.
4. В выпадающем списке «Режим работы» выбрать «Передача кода карты после успешной авторизации к сектору».
5. В поле «Номер сектора» ввести номер сектора (от 1 до 15), к которому будет проводиться авторизация.
6. В [SL1], в поле «Ключ сектора [Crypto1]» и в поле «Ключ сектора [AES128]» ввести ключ сектора (6 байт и 16 байт соответственно в шестнадцатеричном формате) или сгенерировать, либо выбрать ключ/ключи из списка.

Появится окно ожидания карты:

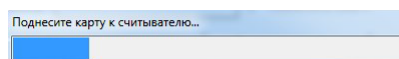


Рис.37 Ожидание карты

Если перед нажатием кнопки «Записать» карта была приложена к считывателю, то удалите её и поднесите заново. Удерживайте карту, пока не закончится программирование карты. Если карта запрограммирована успешно, то программа выдаст следующее сообщение:

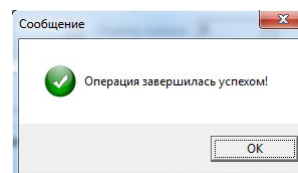


Рис.38 Успешная запись карты

В [SL3] работаем только с полем «Ключ сектора [AES128]».

7. Задать настройки считывателя в области «Настройки считывателя Proxu-6ЕНМ».

8. Нажать кнопку «Записать».

Дальнейшие окна/сообщения аналогичны, как в *MIFARE Classic* описанные выше.

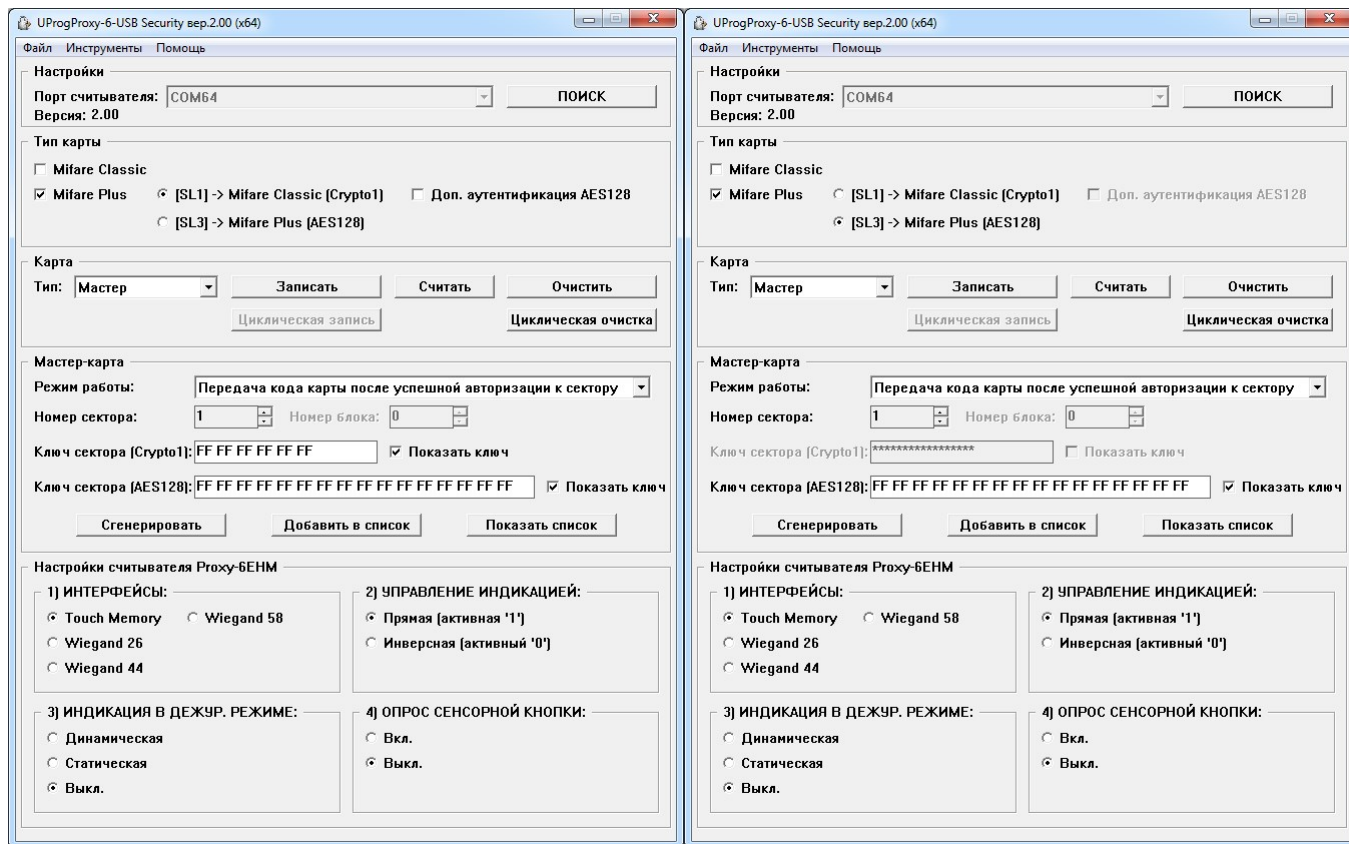


Рис.40 Программирование мастер-карты



Особенности мастер-карт MIFARE Plus, описаны выше в разделе «Программирование карт в режиме «Передача кода карты»».

Для программирования пользовательской карты необходимо выполнить следующие действия:

1. Сформировать мастер-карту, как описано выше (или выбрать мастер-карту из списка, если ранее уже была создана).
2. В выпадающем списке «Тип» следует выбрать «Пользователь».
3. Нажать кнопку «Записать».

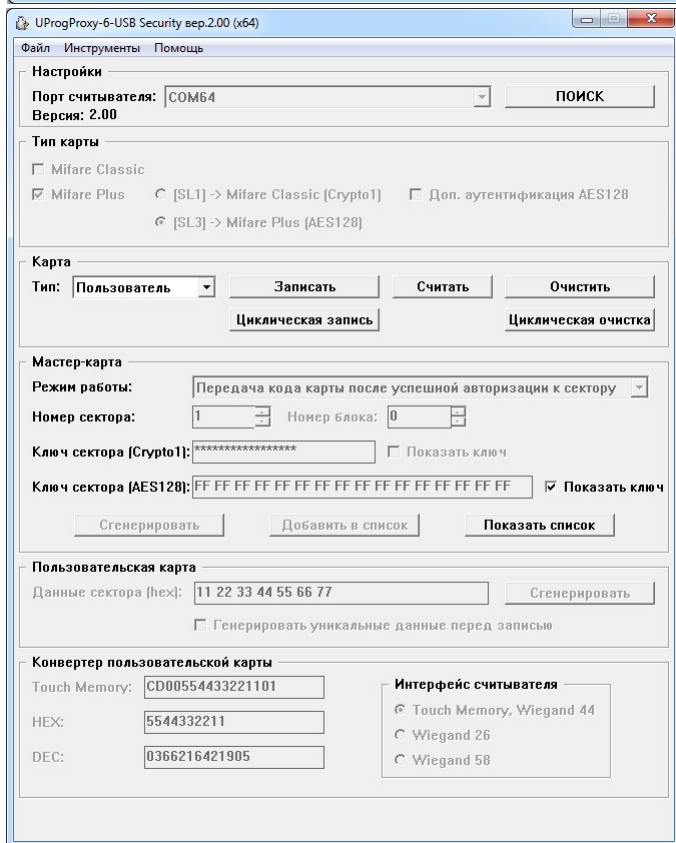
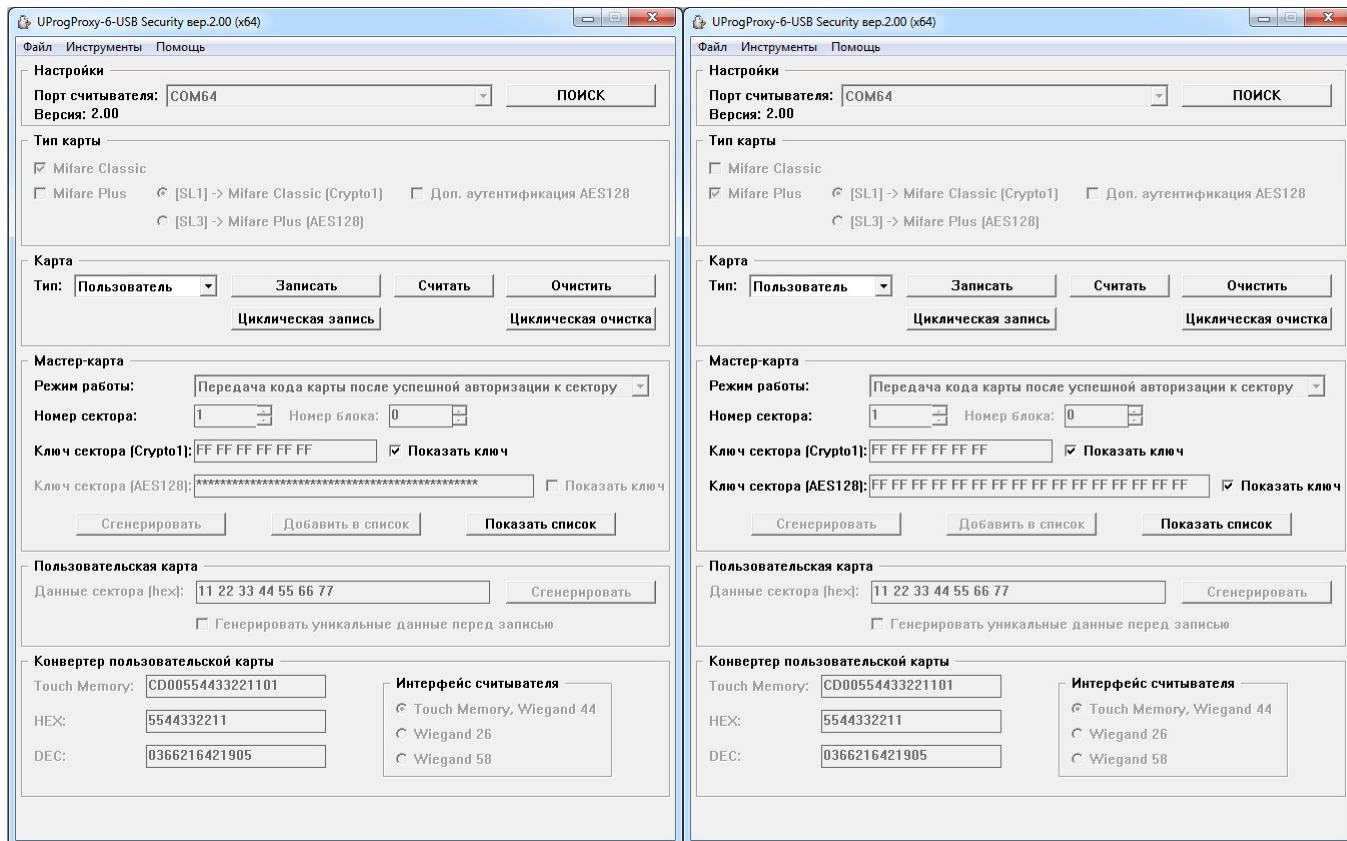


Рис.41 Программирование пользовательской карты

Появится окно ожидания карты:

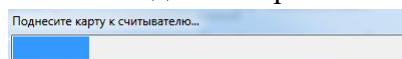


Рис.42 Ожидание карты

Если перед нажатием кнопки «Записать» карта была приложена к считывателю, то удалите её и поднесите заново. Удерживайте карту, пока не закончится программирование карты. Если карта запрограммирована успешно, то программа выдаст следующее сообщение:

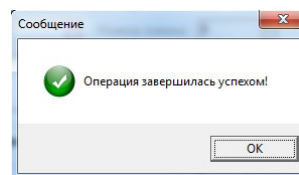


Рис.43 Успешная запись карты

Если в процессе программирования возникли ошибки, то программа выдаст следующее сообщение:



или

Рис.44 Ошибка при записи карты

В этом случае следует повторить процедуру программирования карты. Если ошибка повторилась, следует обратиться к пункту «Решение проблем при программировании карт» настоящего руководства.



Особенности пользовательских карт MIFARE Plus, описаны выше в разделе «Программирование карт в режиме «Передача кода карты»».

Если требуется запрограммировать большое количество карт, то нужно нажать кнопку «Циклическая запись». При этом программа отобразит следующее окно:

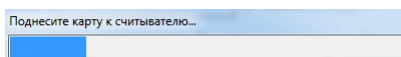


Рис.45 Ожидание карты

Затем следует подносить карты к считывателю по одной. После завершения программирования карты полоса прогресса вернется в исходное состояние «Ожидание новой карты». После этого можно подносить следующую карту. По окончании программирования партии карт ничего не нужно делать, полоса прогресса дойдет до конца, и процесс завершится отобразив следующее окно:

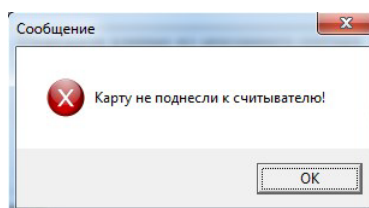


Рис.46 Окно окончания массового программирования карт

Чтение данных из карт

Функция чтения карт позволяет считывать ранее записанные в карты данные. В частности функция полезна для восстановления параметров системы, поскольку можно прочитать настройки из мастер-карт.

Для чтения мастер-карты необходимо выполнить следующие действия:

1. В выпадающем списке «Тип» следует выбрать «Мастер».
2. В области «Тип карты» следует выбрать «Mifare Classic» или «Mifare Plus».
3. Нажать кнопку «Считать».

Появится окно ожидания карты:

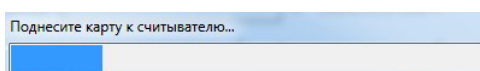


Рис.47 Ожидание карты

Если перед нажатием кнопки «Считать» карта была приложена к считывателю, то удалите её и поднесите заново. Удерживайте карту, пока не закончится чтение карты. Если карта считана успешно, то программа выдаст следующее сообщение:

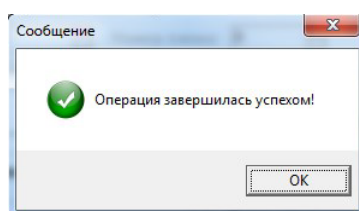
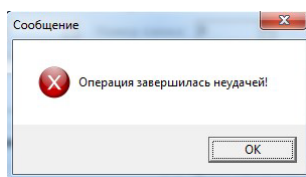


Рис.48 Успешное чтение карты

В основном окне программы, в соответствующих полях, отобразятся параметры, запрограммированные в данной мастер-карте.

Если в процессе чтения возникли ошибки, то программа выдаст следующее сообщение:



или

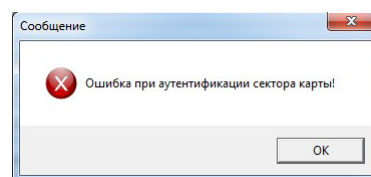


Рис.49 Ошибка при чтении карты

В этом случае следует повторить процедуру чтения карты. Если ошибка повторилась, следует обратиться к пункту «Решение проблем при программировании карт» настоящего руководства.

В режиме чтения пользовательских карт программа позволяет считать код из указанного сектора карты.

Для чтения пользовательской карты необходимо выполнить следующие действия:

1. В меню «Тип» следует выбрать «Пользователь».
2. Нажать кнопку «Показать список» и выбрать нужный ключ. Следует использовать тот ключ, которым был защищён сектор при программировании карт.

(Ручной ввод настроек карт «Тип карты», «Режим работы», «Номер сектора», «Номер блока», «Ключ сектора...» и т.д., задаётся при формировании мастер-карт).

3. Нажать кнопку «Считать».

Дальнейшие окна/сообщения аналогичны, как при чтении мастер-карт описанные выше.

Очистка карт

Функция очистки карт позволяет стирать мастер-карты, а также удалять данные из секторов пользовательских карт.

Процедура «Очистка карт» аналогична, как и процедура «Чтение данных из карт» (Описана выше).

MIFARE Classic, MIFARE Plus (SL1)

В результате ключ сектора Crypto-1 будет изменен на транспортный – «FF FF FF FF FF FF» (hex). Ключ сектора AES 128, для карт MIFARE plus, не изменится!

Данные в указанном блоке указанного сектора будут изменены на «FF FF FF FF FF...».

В дальнейшем, карту, можно использовать либо как мастер-карту, либо как пользовательскую.

«Записать» данные на карты возможно только на новые карты, либо на карты прошедшие процедуру «Очистка карт».

MIFARE Plus (SL3)

В результате ключ сектора AES 128 не изменится!

Данные в указанном блоке указанного сектора будут изменены на «FF FF FF FF FF...».

Т.к. ключ сектора AES 128 программируется один раз, то сменить тип карты «Мастер» на «Пользователь» или наоборот невозможно! Смена уровня безопасности с SL1 на SL3, также не приведет к изменению (удалению) ключа сектора. В результате смены уровня безопасности с SL1 на SL3, вы получите карту «Пользователь» SL3 с низким ключом сектора и без возможности перевести карту обратно на уровень безопасности SL1.

«Записать» данные возможно поверх существующих данных (любого типа карт), поэтому процедура «Очистка карт» не обязательна. Процедура «Очистка карт» полезна для удаления данных с карт.

Решение проблем при программировании карт

Основной причиной ошибок при записи/чтении/очистке карт является ввод неправильного ключа сектора.

MIFARE Classic

Если ошибки возникают с новыми картами, то следует уточнить у поставщика/изготовителя карт, какие транспортные ключи установлены в карте. В большинстве случаев ключ по умолчанию «FF FF FF FF FF FF» (hex), но у отдельных производителей он может быть свой.

MIFARE Plus

Настоятельно рекомендуем закупать новые карты с уровнем безопасности SL0!

(Как правило, карты распространяются с данным уровнем безопасности.)

Ни в коем случае не заказывайте персонализацию карт у поставщика/изготовителя карт или у других сторонних лиц.

Используйте ключи сектора AES 128 из ранее сформированного списка и для определенных карт, разделов, объектов.

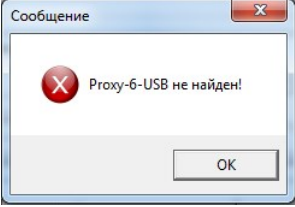
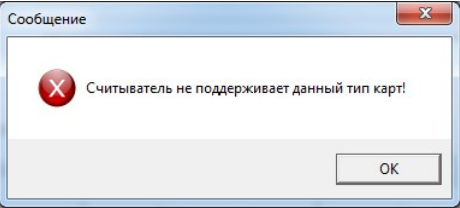
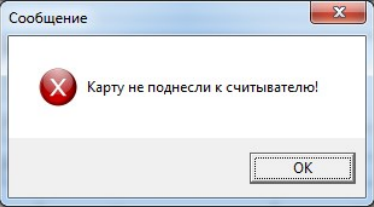
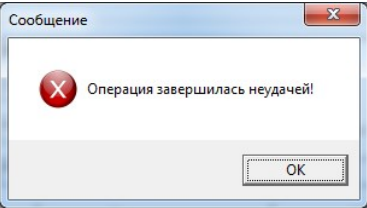
Для обеспечения возможности последующего перепрограммирования секторов пользовательских карт, нужно хранить все когда-либо использовавшиеся ключи секторов в списке ключей программы.

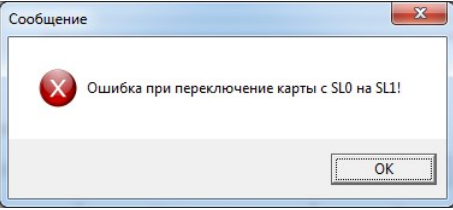
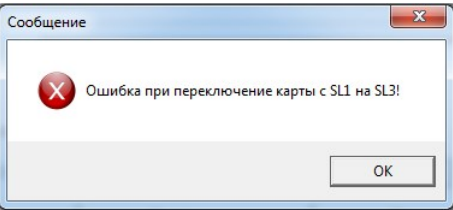
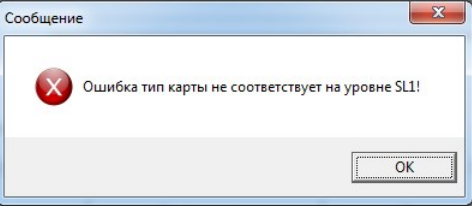
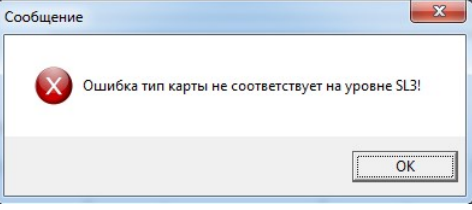
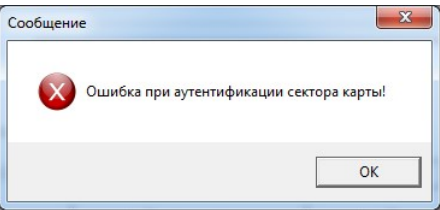


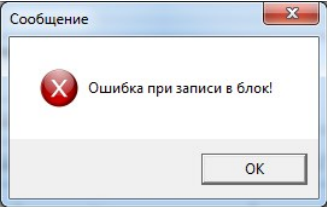
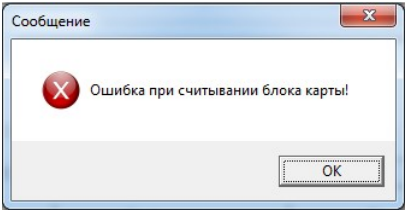
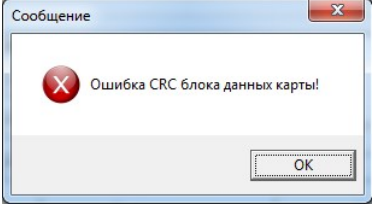
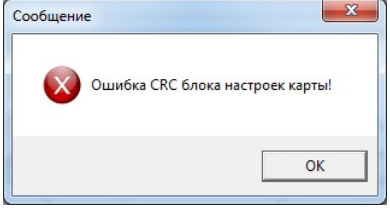
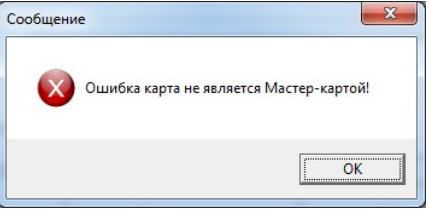
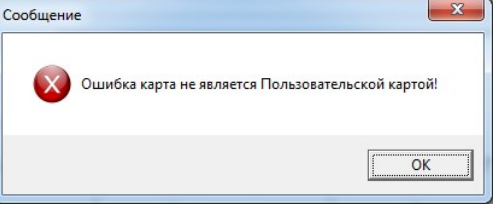
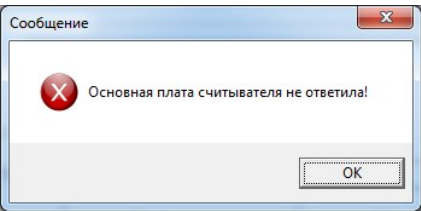
Ключи сектора AES 128 нельзя стереть, перезаписать или изменить после программирования карт!

Храните ключ сектора AES 128 в строжайшем секрете, иначе теряется весь смысл в криптостойком алгоритме AES 128!

Дополнительно приведем таблицу с сообщениями об ошибках, которые возможны в ПО «UProgProxy-6-USB Security v.2.00.exe».

Сообщения	Причины/Решение
	<p>Считыватель не подключен к USB разъёму ПК. Не установлен драйвер.</p> <p>Решение: Проверить подключение считывателя к USB разъёму ПК. Переподключить считыватель. Проверить, отображается ли считыватель в «Диспетчере устройств», при необходимости установить драйвер, как описано в данном руководстве.</p>
	<p>Карта не принадлежит ни к одному из стандартов бесконтактных смарт-карт поддерживаемых считывателем. Стандарты бесконтактных смарт-карт перечислены в п.1.1 данного руководства.</p> <p>Карта принадлежит к одному из стандартов бесконтактных смарт-карт, но является неким развитием серии, которое не учтено в текущей прошивки считывателя.</p> <p>Решение: Обновить прошивку считывателя (актуальные обновления размещены на сайте). Воспользоваться другими картами.</p>
	<p>Карта находится вне зоны считывания карт. Считыватель не смог считать карту. Карта не принадлежит ни к одному из стандартов MIFARE Classic или MIFARE Plus.</p> <p>Решение: Поднести карту вплотную к считывателю. Воспользоваться другой картой.</p>
	<p>Решение: Повторить попытку.</p>

	<p>Персонализация карты прошла неудачно.</p> <p>Решение: Повторить попытку. Воспользоваться другой картой.</p>
	<p>Персонализация карты прошла неудачно.</p> <p>Решение: Повторить попытку. Воспользоваться другой картой.</p>
	<p>Персонализация карты прошла неудачно. Карта имеет другой уровень безопасности, отличный от ожидаемого уровня.</p> <p>Решение: Повторить попытку. Проверить настройки в основном окне программы: «Тип карты», «Карта» -> «Тип». Воспользоваться другой картой.</p>
	<p>Персонализация карты прошла неудачно. Карта имеет другой уровень безопасности, отличный от ожидаемого уровня.</p> <p>Решение: Повторить попытку. Проверить настройки в основном окне программы: «Тип карты», «Карта» -> «Тип». Воспользоваться другой картой.</p>
	<p>Неверно заданы настройки в основном окне программы:</p> <ul style="list-style-type: none"> - «Тип карты»; - «Карта» -> «Тип»; - MIFARE Classic карта не новая, либо не очищен сектор; - «Мастер-карта» -> «Номер сектора» и/или «Номер блока» указан(ы) неверно. - Ключи сектора Crypto-1 и/или AES 128 задан(ы) неверно. - Карта не поддерживает доп. аутентификацию. <p>Решение: Повторить попытку. Нажать кнопку «Показать список» и выбрать нужный ключ. Очистить сектор карты MIFARE Classic.</p>

	<p>Решение: Повторить попытку.</p>
	<p>Решение: Повторить попытку.</p>
	<p>Повреждены данные на карте, либо карта была запрограммирована сторонним считывателем.</p> <p>Решение: Повторить попытку. Воспользоваться другой картой. Очистить карту. Записать новые данные.</p>
	<p>Повреждены данные на карте, либо карта была запрограммирована сторонним считывателем.</p> <p>Решение: Повторить попытку. Воспользоваться другой картой. Очистить карту. Записать новые данные.</p>
	<p>Мастер-карта MIFARE Plus очищена.</p> <p>Решение: Записать новые данные. Воспользоваться другой мастер-картой.</p>
	<p>Пользовательская карта MIFARE Plus очищена.</p> <p>Решение: Записать данные. Воспользоваться другой пользовательской картой.</p>
	<p>Внутренний сбой коммуникации двух плат считывателя.</p> <p>Решение: Переподключить считыватель и повторить попытку. Передать в ремонт.</p>

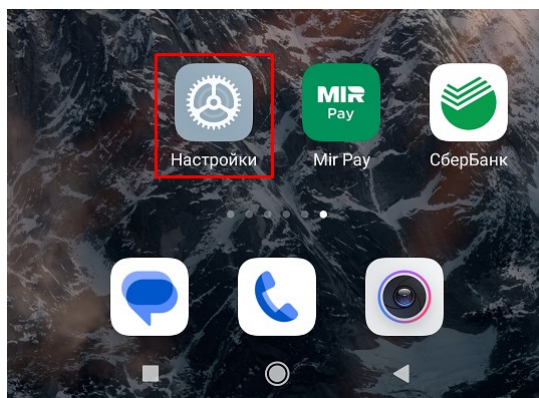
2.2.6 Идентификация с помощью мобильного платежного приложения

В считывателе «Proхy-6-USB» предусмотрена работа с платежными приложениями «Mir Pay», «SberPay», «Т-Pay», а именно осуществляется считывание токена банковской карты. Токен – это замена PAN банковских карт для конкретного приложения. Даже если произойдет «перехват» токена, то им нельзя воспользоваться для оплаты покупок или списания средств в интернете или магазине.

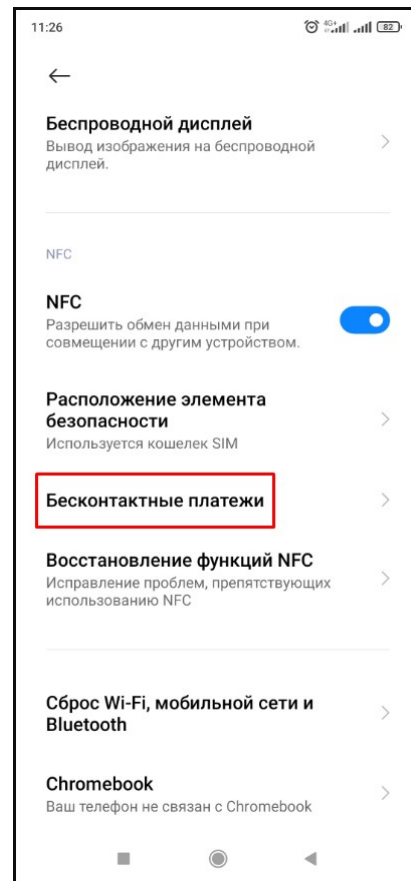
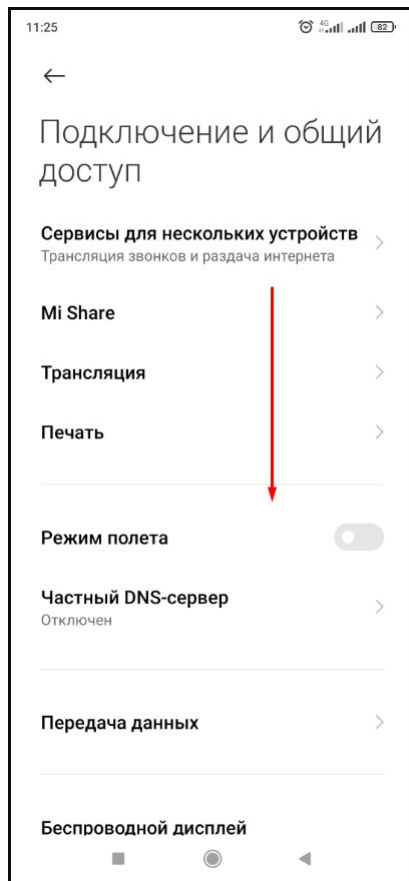
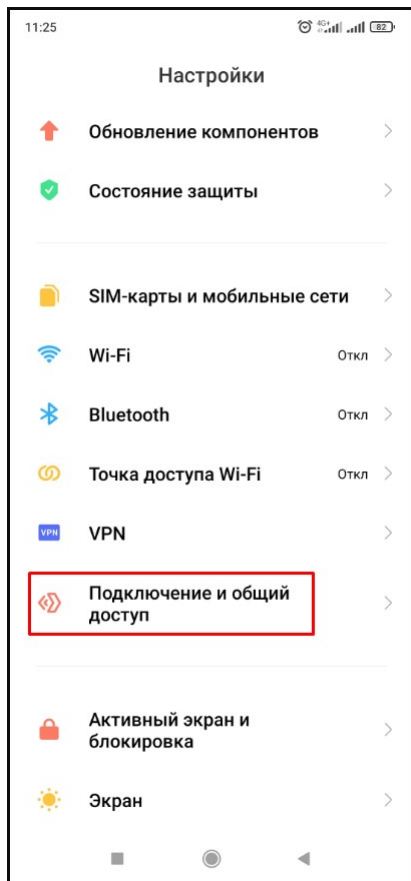
Добавления токена в СКУД происходит с помощью считывателей «Proхy-6-USB» или «Proхy-6EHM-G, -B, -W». Считыватели должны быть настроены на формат/интерфейс (Touch Memor, Wiegand xx, количество байт и т.д.) соответствующий вашей СКУД. Также предполагается, что платежное приложение «Mir Pay» и/или «SberPay» (входит в приложение «СберБанк Онлайн»), и/или «Т-Pay» уже установлен(ы) на ваш телефон. Установка, настройка приложений и привязка карт(ы) описано на соответствующих ресурсах.

Далее, необходимо определиться какое приложение и какая карта будет использоваться для идентификации/прохода в СКУД. Идентификация в СКУД будет происходить по тому приложению, которое выбрано как «Оплата по умолчанию» и соответственно по той карте (в этом приложении), которая обозначена как «Для оплаты по умолчанию» или «Основная». Изменить настройки телефона и приложения можно следующим образом (какие-то разделы/вкладки могут отличаться, но алгоритм общий для всех и данные шаги не являются единственно возможными):

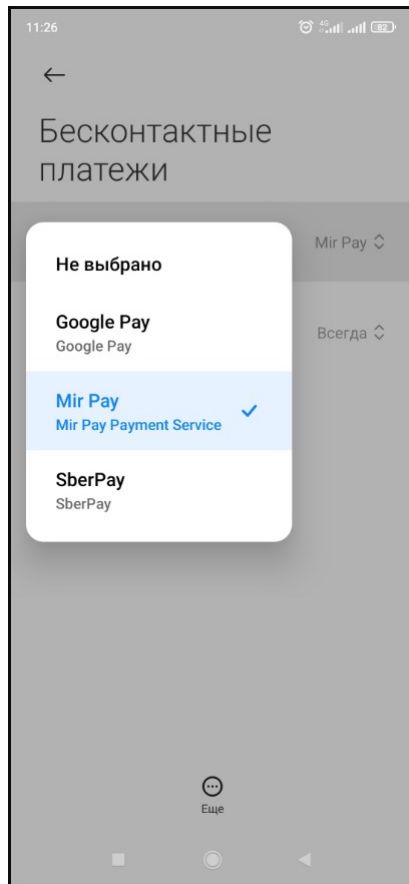
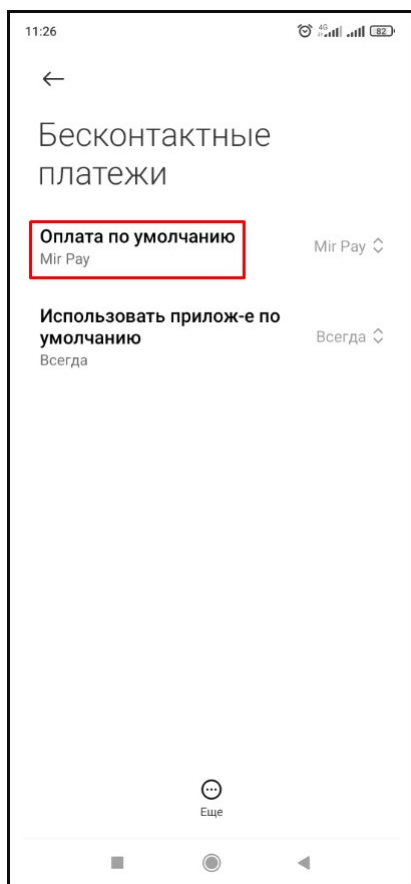
- 1) Откройте «Настройки» вашего телефона.



- 2) Нажмите на раздел «Подключение и общий доступ».
- 3) Найдите раздел «Бесконтактные платежи» и нажмите.



4) Нажмите на раздел «Оплата по умолчанию» и выберите платежное приложение.



5) Настройте приложение, т.е. назначьте карту.

Для приложения «Mir Pay»:

5.1 Открываем приложение.

5.2 Выбираем карту и нажимаем по надписи «Для оплаты по умолчанию».

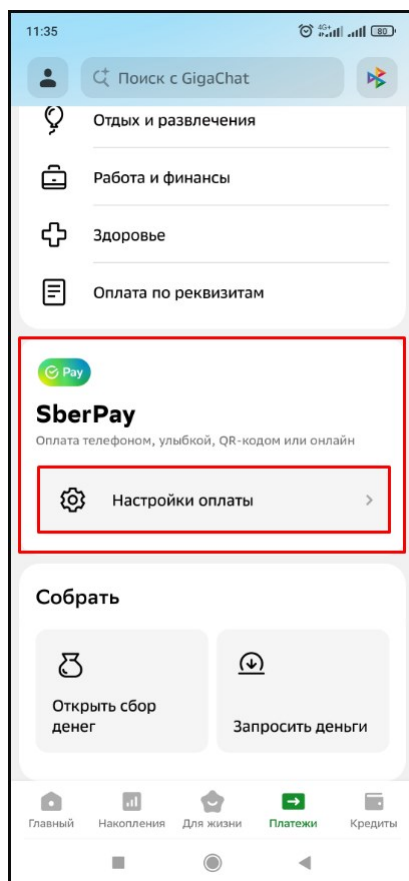
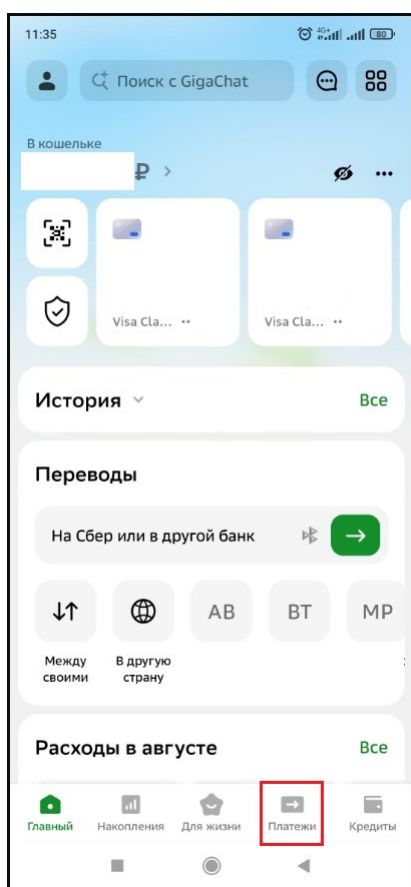
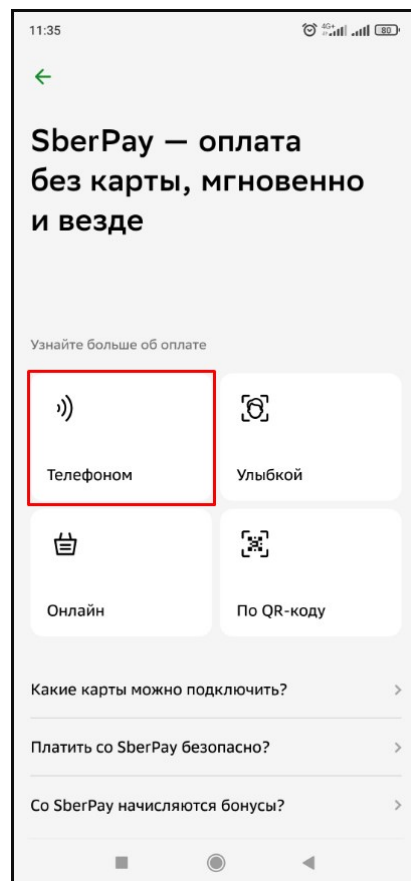
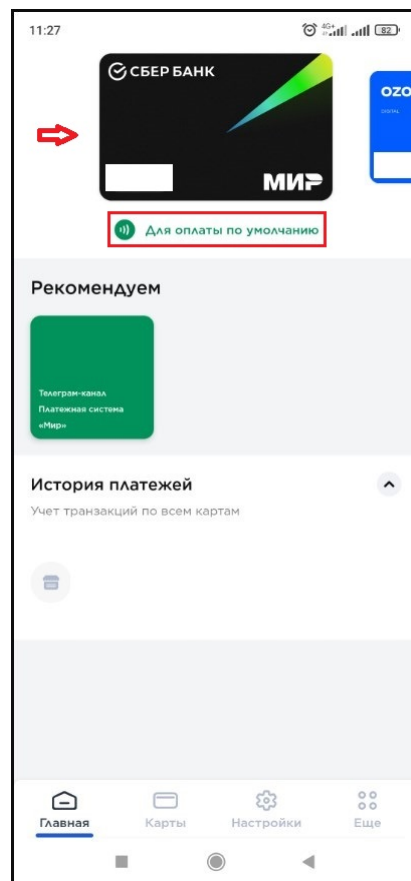
Для приложения «SberPay»:

5.1 Открываем приложение.

5.2 Нажимаем на раздел «Платежи».

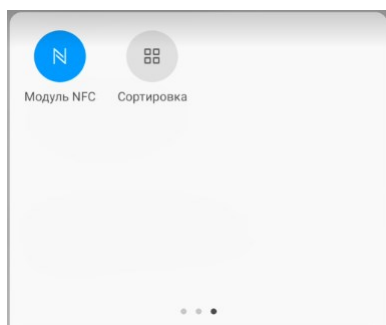
5.3 Находим раздел «SberPay» и нажимаем «Настройки оплаты».

5.4 Нажимаем раздел «Телефоном».



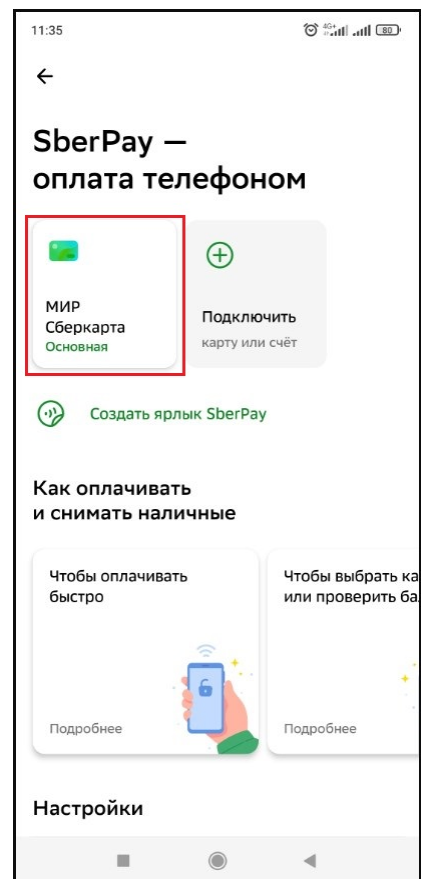
5.5 Выбираем карту и назначаем её как «Основная».

- б) Проверяем, активирован ли «Модуль NFC» телефона. Для этого нужно зайти в настройки телефона, либо сдвинуть вниз верхнюю «шторку» и отыскать значок «Модуль NFC».



Если модуль не активирован, то нажатием по значку активируйте его. Также, активация, возможна и в платежных приложениях нажав на соответствующую кнопку/значок.

Внимание! При идентификации в СКУД «Модуль NFC» должен быть активирован. И, как правило, экран телефона должен быть разблокирован. В некоторых случаях, для стабильного считывания токена, необходимо запустить приложение. У приложения «SberPay» есть раздел «Создать ярлык SberPay» (см. выше), нажимаем на него и на вашем «рабочем столе»/экране установится соответствующий ярлык, и уже через этот ярлык, запускаем приложение.



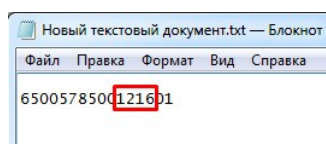
Подносим телефон к считывателю, как можно ближе, и той стороной/областью, где расположена антенна модуля NFC. Как правило, это задняя сторона телефона, наверху, возле видекамеры. Процедура такая же, как при оплате покупок в магазине, либо при оплате проезда в общественном транспорте.

Далее, происходит считывание токена банковской карты мобильного приложения. В случае считывателя «Proxy-6-USB», результат можно, к примеру, посмотреть в любом текстовом файле, предварительно открыв его, а в случае «Proxy-6-ЕНМ-G, -B, -W» в программе «UProg» в разделе «Ключи», предварительно подключив его к прибору СКУД.

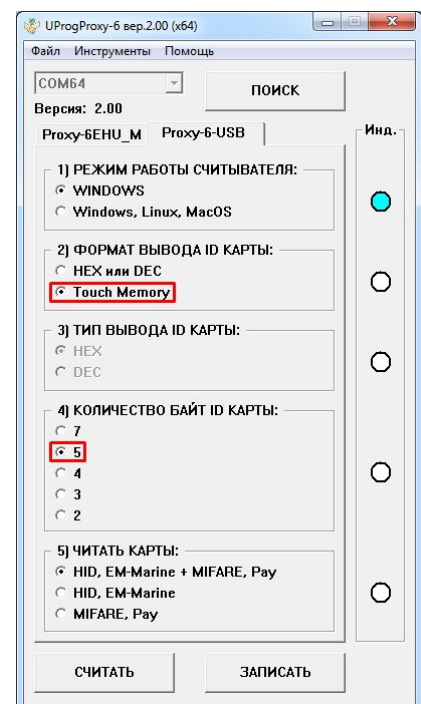
Пример и проверка результата считывания токена банковской карты для считывателя «Proxy-6-USB».

Считыватель «Proxy-6-USB» настроен следующим образом: «Touch Memory»; 5 байт.

В файле программы «Блокнот», при считывании токена, отобразится следующий ключ:

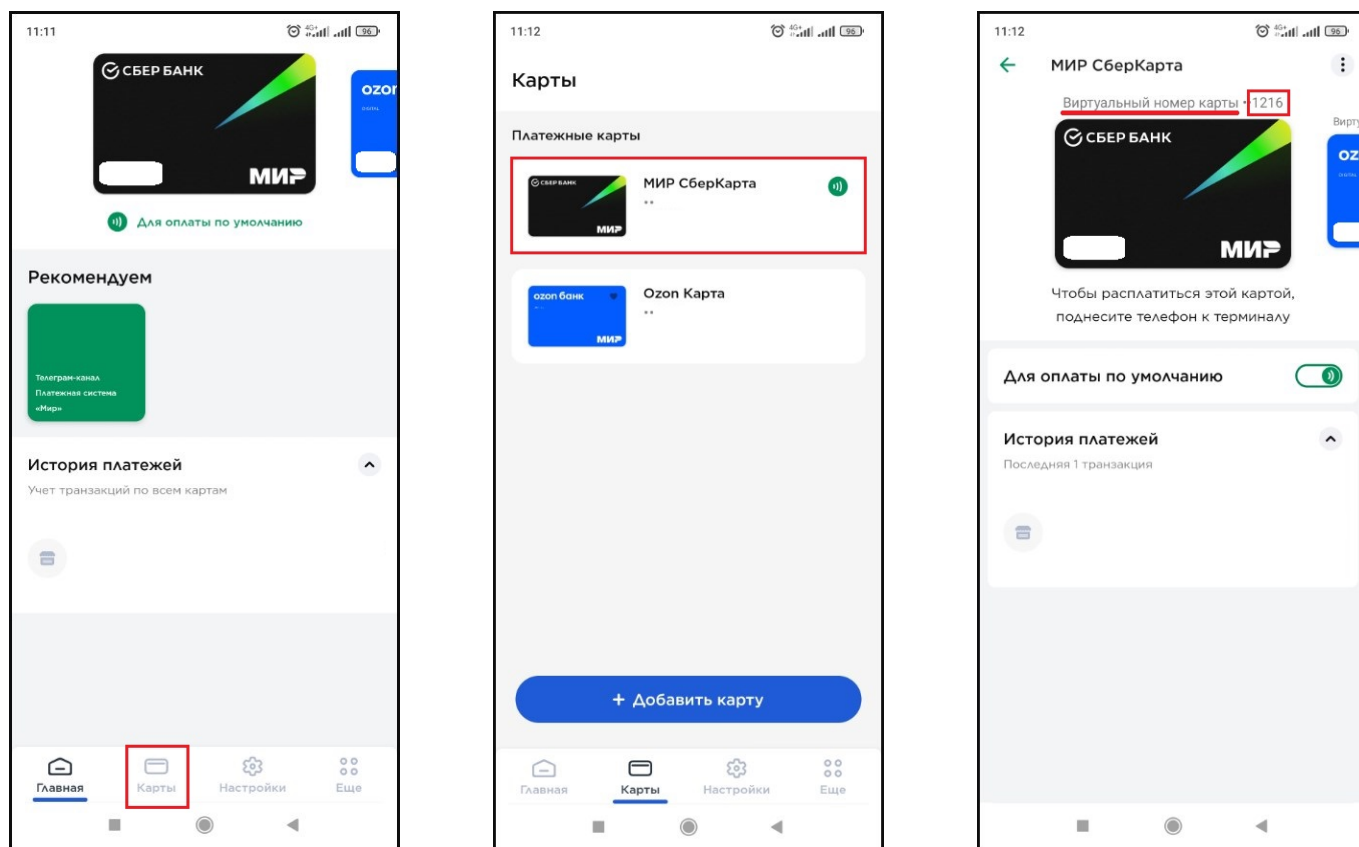


Важно, чтобы в ключе содержалась часть токена, которая отображается в платежном приложении.



Покажем на примере приложения «MirPay».

- 1) Открываем платежное приложение.
- 2) Переходим в раздел карты.
- 3) Выбираем карту.
- 4) Сравниваем последние цифры «Виртуальный номер карты» с частью выведенного ключа (см. выше).



Пример и проверка результата считывания токена банковской карты для считывателя «Proxu-6ENM-G, -B, -W» приведен в РЭ на соответствующий считыватель.

Внимание!



Бывают редкие случаи, когда считанный токен не совпадает с токеном в платежном приложении! Тогда, на телефоне закройте все платежные приложения, при этом, модуль NFC оставьте активированным. Поднесите телефон к считывателю несколько раз и посмотрите в файл программы "Блокнот" на считанные ключи.

В том случае, если считанный ключ не меняется, от считывания к считыванию, то тогда телефон можно использовать в СКУД, как карту доступа без использования платежных приложений.

2.2.7 Использование изделия

К работе с изделием допускается персонал, изучивший настоящее руководство и получивший удостоверение о проверке знаний правил по техники безопасности.

Для считывания кода карты необходимо поднести карту к считывателю на расстояние не более, чем указано в п.1.2.5 настоящего РЭ. Считыватель издаст один короткий звуковой сигнал и световой индикатор погаснет на время пока карта находится в поле считывателя.

2.2.8 Обновление программного обеспечения считывателя

Для обновления ПО считывателя необходимо убедиться, что считыватель подключен к ПК и работает в штатном режиме. Считыватель «Proху-6-USB», как правило, имеет два файла для обновления ПО. На ПК, двойным кликом мыши, запустите exe-файл с обновлением ПО (не имеет значения с какого файла начинать). Считыватель перейдет в режим загрузчика, а программа обновления ПО, в автоматическом режиме, подключится к считывателю. Файлы обновления ПО представлены на Рис.50.

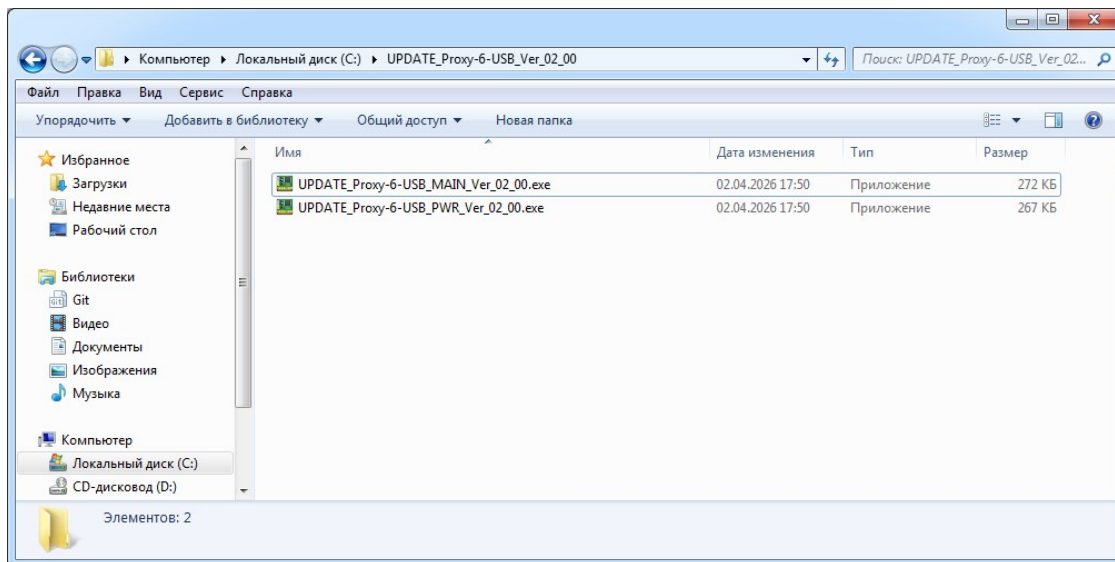
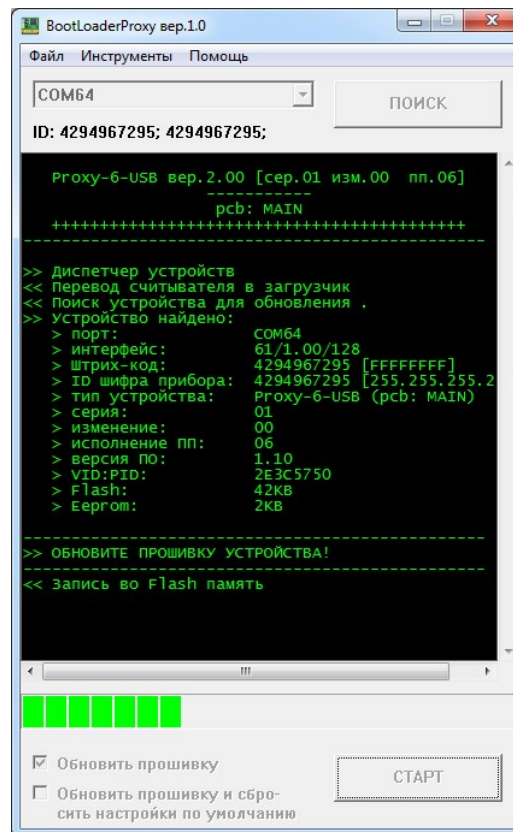
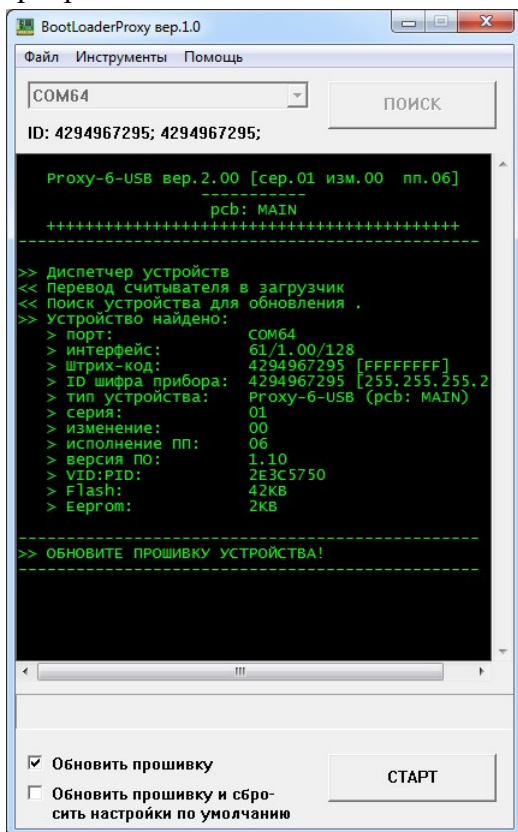
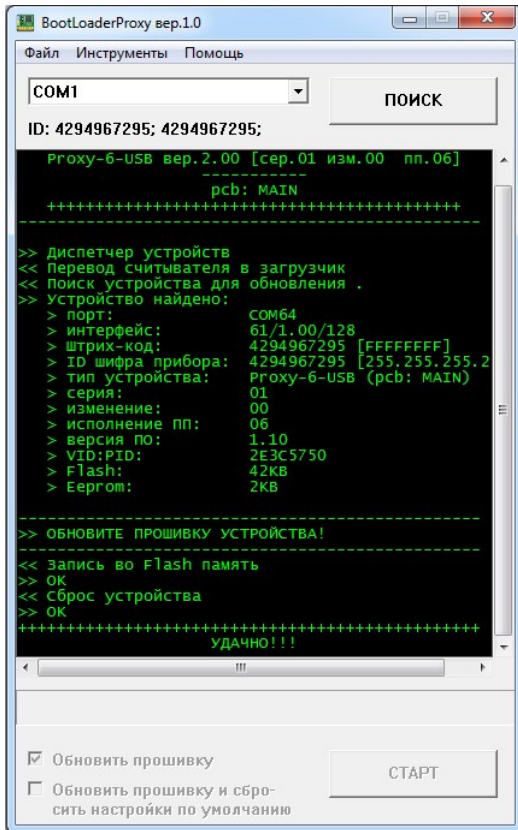


Рис.50 Файлы обновления ПО считывателя «Proху-6-USB»

Необходимо выбрать каким образом будет происходить обновление: **«Обновить прошивку»** или **«Обновить прошивку и сбросить настройки по умолчанию»**. (В исключительных случаях такой выбор заблокирован!)

Затем нажать на кнопку **«СТАРТ»**. На экране ПО будет выведен лог-файл и запустится строка прогресса обновления считывателя.

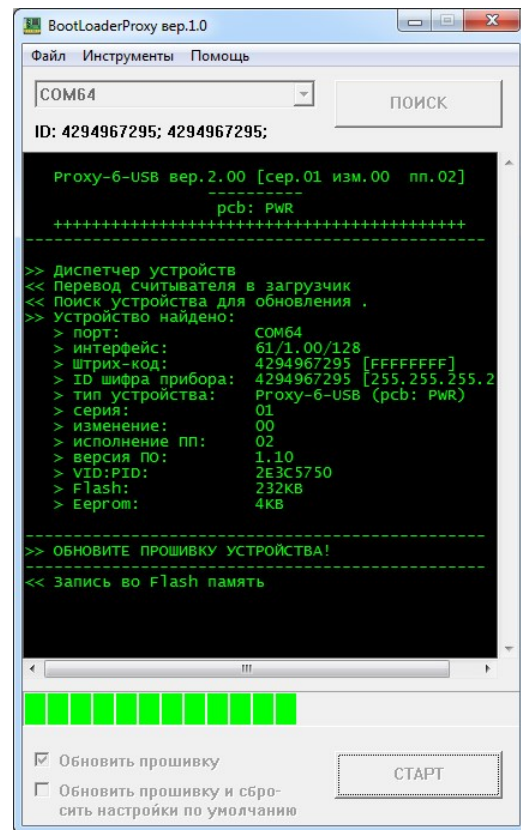
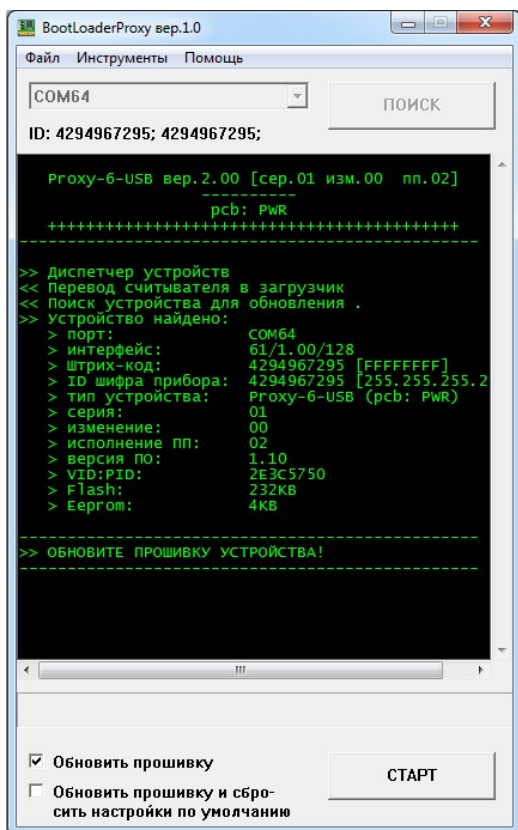


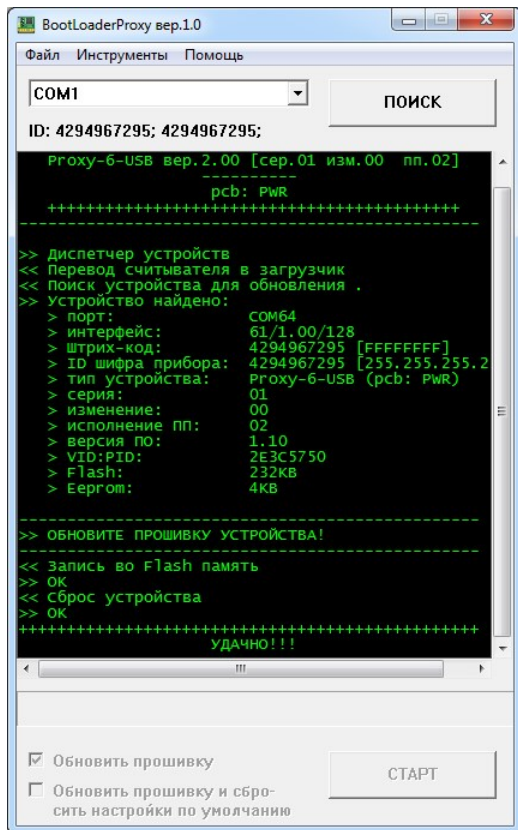


По окончании обновления программа выдаст сообщение об успешном обновлении, а считыватель перезагрузится и запустится в штатном режиме.

В случае сбоя процедуры обновления считыватель останется в режиме загрузчика. В таком случае необходимо повторить процедуру обновления ПО, нажав кнопку «СТАРТ», либо нажать на кнопку «ПОИСК», а затем на кнопку «СТАРТ». В случае отрицательного результата, повторите все шаги п.2.2.8 настоящего РЭ.

Если же программа обновления ПО сообщила об успешном обновлении, а считыватель после перезагрузки не запустился в штатном режиме, то переходите ко второму файлу обновления. Повторите процедуру обновления ПО, как описано выше.





По окончании обновления программа выдаст сообщение об успешном обновлении, а считыватель перезагрузится и запустится в штатном режиме.

В случае сбоя процедуры обновления считыватель останется в режиме загрузчика. В таком случае необходимо повторить процедуру обновления ПО, нажав кнопку «СТАРТ», либо нажать на кнопку «ПОИСК», а затем на кнопку «СТАРТ». В случае отрицательного результата, повторите все шаги п.2.2.8 настоящего РЭ.

2.2.9 Проверка работоспособности

Проверку работоспособности произвести согласно п. 3.4 настоящего руководства

2.2.10 Действия в экстремальных ситуациях



Внимание!

В случае обнаружения в месте установки изделия искрения, возгорания, задымленности, запаха горения изделие должно быть обесточено и передано в ремонт.

2.2.11 Возможные неисправности и способ устранения

Таблица 2.2.11.1

Неисправность	Возможная проблема	Пути решения
Считыватель не определяется в ПО «UProgProxy-6 v.2.00» или в ПО «UProgProxy-6-USB Security v.2.00»	Считыватель не подключен к ПК Не установлен драйвер	Проверить подключение считывателя, при необходимости переподключить Проверить установку драйвера, при необходимости переустановить
Не удастся произвести операции с сектором карты в ПО «UProgProxy-6-USB Security v.2.00»	Неверный ключ сектора, либо карта в отличном от транспортного состоянии	Проверить список ключей, использовать другую карту

3 Техническое обслуживание изделия

3.1 Общие указания

Техническое обслуживание считывателя производится по планово-предупредительной системе, которая предусматривает ежегодное плановое техническое обслуживание.

3.2 Меры безопасности

Техническое обслуживание считывателя должно производиться лицами, имеющими квалификационную группу по электробезопасности не ниже второй.

3.3 Порядок технического обслуживания изделия

Работы по плановому техническому обслуживанию включают в себя:

- проверку внешнего состояния считывателя;
- проверку подключаемого USB кабеля, разъемов, контактных соединений;
- проверку работоспособности согласно п. 3.4 настоящего руководства.

3.4 Проверка работоспособности изделия

При подключении питания световой индикатор в сопровождении звукового сигнализатора выдаст следующую индикацию: красный, зеленый, синий. Откройте на ПК любой текстовый файл и поднесите идентификационную карточку к считывателю. После считывания кода карточки считыватель издаст короткий звуковой сигнал, а номер карты отобразится в текстовом файле.

3.5 Техническое освидетельствование

Технического освидетельствования изделия не предусмотрено.

3.6 Консервация (расконсервация, переконсервация)

Консервация изделия не предусмотрена.

4 Текущий ремонт

Текущий ремонт неисправного изделия производится на предприятии-изготовителе или в авторизированных ремонтных центрах. Отправка изделия для проведения текущего ремонта оформляется в соответствии с СТО СМК 8.5.3-2015, размещённом на нашем сайте <https://bolid.ru/support/remont/>.



Внимание!

Оборудование должно передаваться для ремонта в собранном и чистом виде, в комплектации, предусмотренной технической документацией.

Претензии принимаются только при наличии приложенного рекламационного акта с описанием возникшей неисправности.

Выход изделия из строя в результате несоблюдения потребителем правил монтажа или эксплуатации не является основанием для рекламации и гарантийного ремонта.

Рекламации направлять по адресу:

АО НВП «Болид», Россия, 141070, Московская область, г. Королёв, ул. Пионерская, 4.

Адрес места осуществления деятельности по изготовлению продукции:

141006, Московская обл., г. Мытищи, Ярославское ш., 120Б, стр. 3.

Тел.: +7 (495) 775-71-55, электронная почта: info@bolid.ru

При затруднениях, возникших при эксплуатации изделия, рекомендуется обращаться в техническую поддержку по телефону +7 (495) 775-71-55 или по электронной почте support@bolid.ru.

5 Хранение

В транспортной таре допускается хранение при температуре окружающего воздуха от минус 50 до плюс 50 °С и относительной влажности до 95 % при температуре плюс 35 °С.

В потребительской таре допускается хранение только в отапливаемых помещениях при температуре от плюс 5 до плюс 40 °С и относительной влажности до 80 % при температуре плюс 20 °С.

6 Транспортирование

Транспортировка приборов допускается в транспортной таре при температуре окружающего воздуха от минус 50 до плюс 50 °С и относительной влажности до 95 % при температуре плюс 35 °С.

7 Утилизация

Утилизация прибора производится с учётом отсутствия в нём токсичных компонентов.

Содержание драгоценных материалов: не требует учёта при хранении, списании и утилизации (п. 1.2 ГОСТ 2.608-78).

Содержание цветных металлов: не требует учёта при списании и дальнейшей утилизации изделия.

8 Гарантии изготовителя

Изготовитель гарантирует соответствие прибора требованиям настоящего РЭ при соблюдении потребителем правил транспортирования, хранения, монтажа и эксплуатации.

Гарантийный срок эксплуатации – 18 месяцев со дня ввода в эксплуатацию, но не более 24 месяцев со дня выпуска изготовителем.

9 Сведения о сертификации

Считыватели бесконтактные настольные «Proху-6-USB-G», «Proху-6-USB-B», «Proху-6-USB-W» соответствуют требованиям технического регламента Таможенного союза ТР ТС 020/2011 «Электромагнитная совместимость технических средств», имеют декларацию о соответствии ЕАЭС N RU Д-РУ.РА10.В.89250/24.

Считыватели бесконтактные настольные «Proху-6-USB-G», «Proху-6-USB-B», «Proху-6-USB-W» соответствуют требованиям Технического регламента ТР ЕАЭС 037/2016 «Об ограничении применения опасных веществ в изделиях электротехники и радиоэлектроники» и имеют декларацию о соответствии ЕАЭС N RU Д-РУ.РА10.В.89253/24.

Считыватели бесконтактные настольные «Proху-6-USB-G», «Proху-6-USB-B», «Proху-6-USB-W» входят в состав Системы контроля и управления доступом, которая имеет сертификат соответствия технических средств обеспечения транспортной безопасности требованиям к их функциональным свойствам № МВД.03.001730, выданный ФКУ НПО «СТиС» МВД России.

Производство считывателей бесконтактных настольных «Proху-6-USB-G», «Proху-6-USB-B», «Proху-6-USB-W» имеет сертификат соответствия ГОСТ Р ИСО 9001. Сертификат соответствия размещен на сайте <https://bolid.ru> в разделе «О компании».

10 Сведения о ранее выпущенных версиях

Версия	Начало выпуска	Содержание отличий	Совместимость
2.00	04.2026	Добавлено: - поддержка карт MIFARE Plus (S, SE, X, EV1, EV2); - работа с защищенными секторами карт используя алгоритм шифрования Сгруто-1 и/или AES 128.	«UProgProху-6 v.2.00» «UProgProху-6-USB Security v.2.00»
1.10	09.2025	Добавлено: - поддержка обновления ПО; - увеличен вывод количества байт ID карты (7 мь байт); - поддержка платежных приложений «Mir Pay», «SberPay» и «Т-Рау»; - поддержка запроса штрих-кода и идентификатора шифра прибора (отображается в ПО считывателей).	«UProgProху-6 v.1.10» «UProgProху-6-USB Security v.1.10»
1.00	05.2024	Первая серийно выпускаемая версия.	«UProgProху-6 v.1.0» «UProgProху-6-USB Security v.1.0»