

Москва

Предисловие

1 Над программой работали

|  |  |
| --- | --- |
| Должность | ФИО |
| Разработчик | Осипович Р. |
| Тестировщик | Беляков Н.Д. |
| Разработка документов | Беляков Н.Д. |

2 Лист изменений

|  |  |
| --- | --- |
| Дата изменений | Содержание изменений |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

3 Системные требования

|  |  |
| --- | --- |
| Операционная система | Не менее Windows 10 Pro |
| Процессор | Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz 2.90 GHz |
| Оперативная память | 8,00 ГБ (доступно: 7,83 ГБ) |
| Тип системы | 64-разрядная операционная система, процессор x64 |

Приложение позволит выполнять следующие задачи:

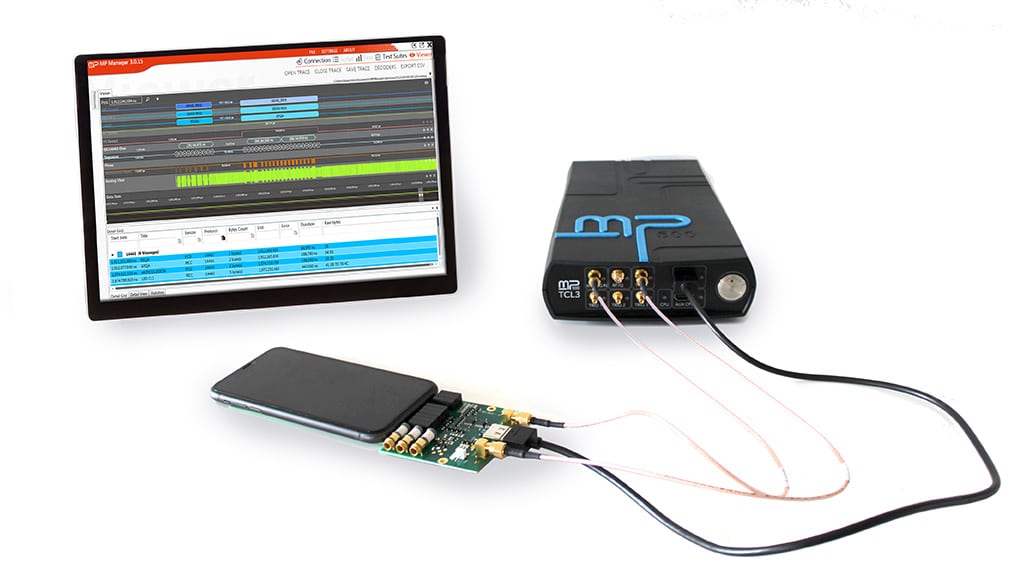
* Проверка карт на РЧ (реагирование чипа) и Добротность;
* Опознание чипа;
* Тестирование быстродействие по ПС ‘МИР’;
* Испытание для логических операций: - опрос (Тип А); - испытания переходов состояний PICC (Тип А).

4 Система считывания карт для ПО

|  |
| --- |
| Micropross MP 500 TCL3 |
| Micropross CTS II |
|  |
|  |

Структура работы программы.

Программа предназначена для проверки функционирования интеллектуальных бесконтактных карт.



Оглавление

[1. Бизнес-процессы. 6](#_Toc172643752)

[2. Общая информация о системе. 7](#_Toc172643753)

[3. Модули 12](#_Toc172643754)

[3.1. Базовый модуль 13](#_Toc172643755)

[3.2. Функциональный модуль «Быстродействие пластиковых карт. Требования ПС «МИР». 16](#_Toc172643756)

[3.3. Функциональный модуль «Соответствия требованиям ГОСТ Р 14443 для PICC. Протокольная часть. 32](#_Toc172643757)

# Бизнес-процессы.

Типовой производственный процесс разделен на 3 фазы, каждая из которых описана ниже.

* 1. Фаза 1. Настройка машины

В данной фазе производится подключение устройства к ПК.

* 1. Фаза 2. Передача данных.

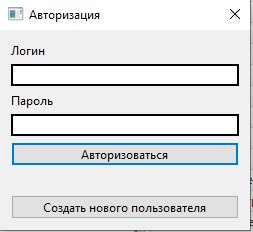
В данной фазе начинается взаимодействие устройства MP500 TCL3 или Micropross CTS II и ПК. Устройство передаёт данные на ПК со считанной карты.

* 1. Фаза 3. Вывод информации.

В данной фазе отображается информация о считанных картах от устройств на ПК. Данную информацию можно сохранить. Все считанные карты по быстродействию должны проходить согласно ГОСТ 10373-6 – 2015.

# Общая информация о системе.

* 1. Форма входа в систему



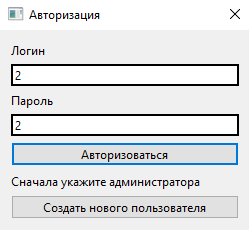
Данная форма должна содержать следующие элементы:

* Поле ввода Логина;
* Поле ввода Пароля;
* Кнопка «Авторизация» для подтверждения входа в систему.

Функционал кнопки – нажатие данной кнопки осуществляет поиск по реквизитам «Логин» и «Пароль» среди действующих пользователей системы, в случае успеха (совпадения реквизитов), закрывает данную форму и выводит основную форму пользователя в зависимости от того пользователь какого типа вошел в систему.

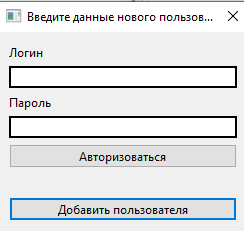
* Кнопка «Создать нового пользователя». Создаёт нового администратора системы, после авторизации под суперадминистратором.
  1. Управление пользователями в системе.
     1. Создание пользователя

Создать пользователя в системе можно в окне авторизации. Для этого заполняем поле логин и пароль и нажимаем на кнопку «Создать нового пользователя» (пользователь не может создавать других пользователей, только администратор, а администратора может создавать только суперпользователь).



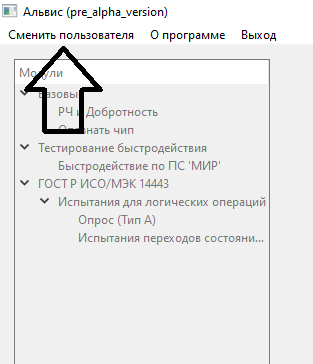
Вводим Логин и Пароль нового пользователя и нажимаем на кнопку «Добавить пользователя».

После этого откроется сново окно авторизации, где можно будет зайти под ранее созданным пользователем.



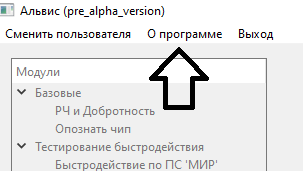
* + 1. Сменить пользователя.

После входа в систему можно сменить пользователя, нажав на кнопку «Сменить пользователя».

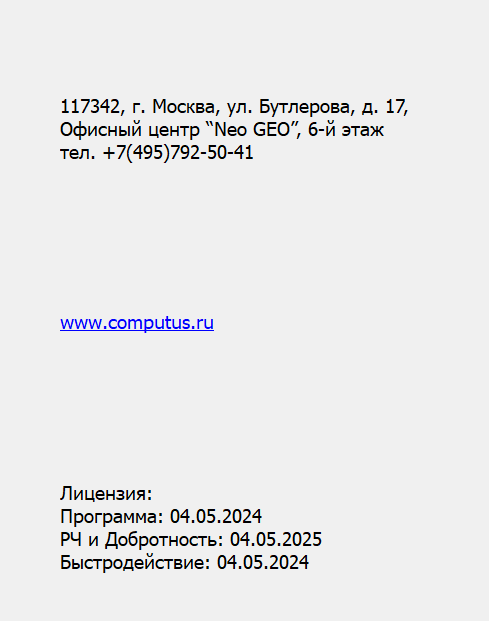


После нажатия на кнопку «Сменить пользователя», программа вернёт пользователя в окно авторизации.

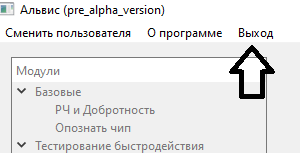
* 1. О программе.



Данная кнопка предназначенна для просмотра информации о программе. При нажатии кнопки, открывается информация о программе.



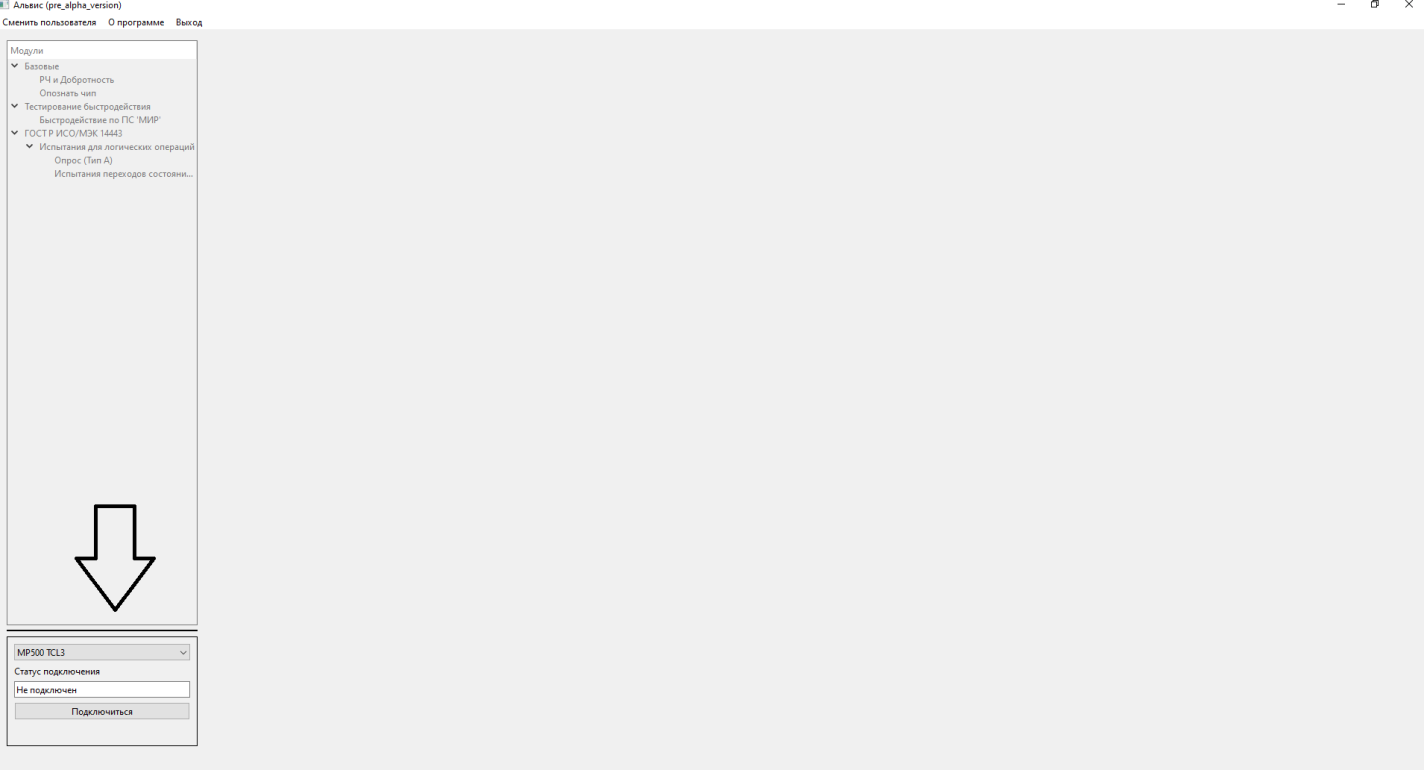
* 1. Выход.



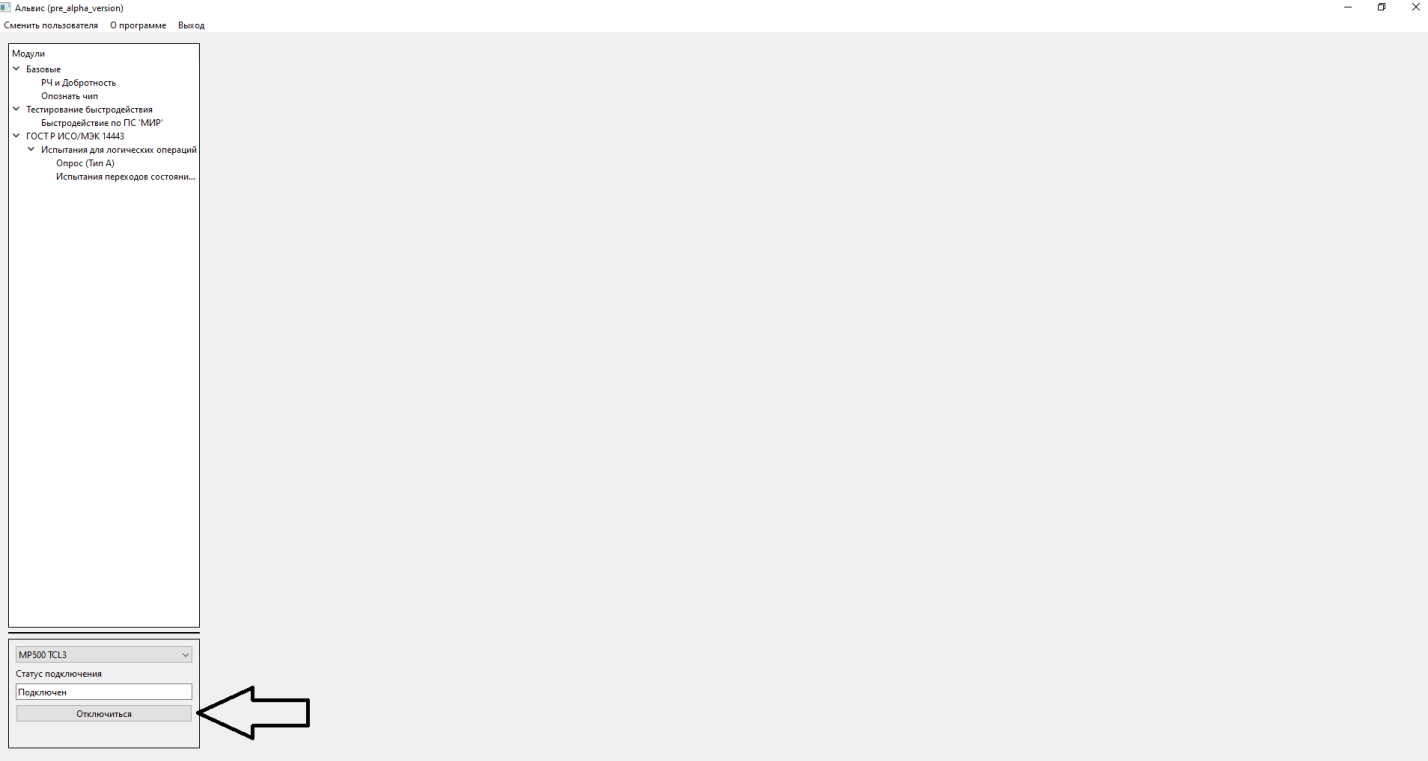
Данная кнопка предназначенна для выхода из программы. При нажатии кнопки – программа закрывается.

* 1. Запуск программы.

Перед началом работы программы, нужно подключить устройство к системе, через USB и в программе выбрать подключенное устройство, после нажать кнопку «Подключиться».



После этого кнопка «Подключиться» поменяется на «Отключиться», а статус подключение поменяется с «Не подключён» на «Подключён». Также устройство можно отключить с помощью кнопки «Отключиться».



# Модули

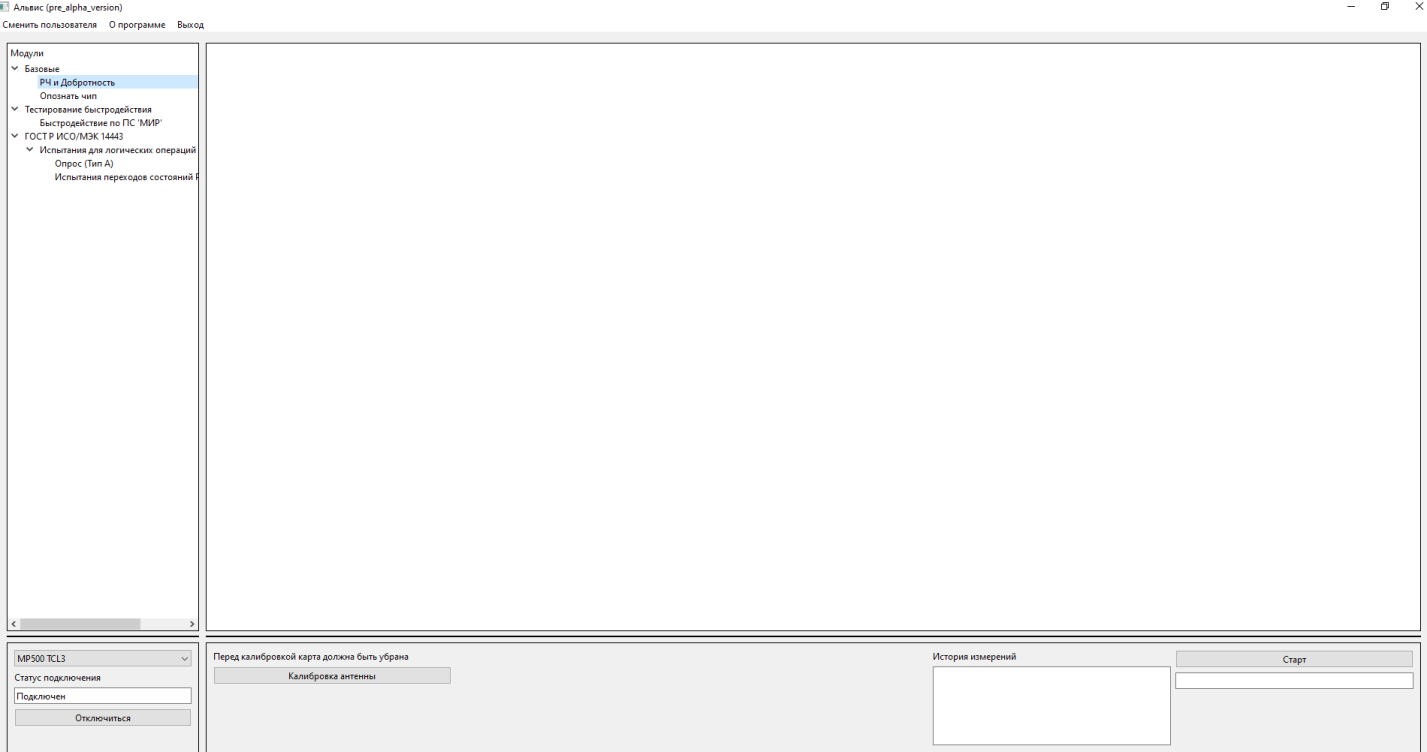


Данное окно состоит из:

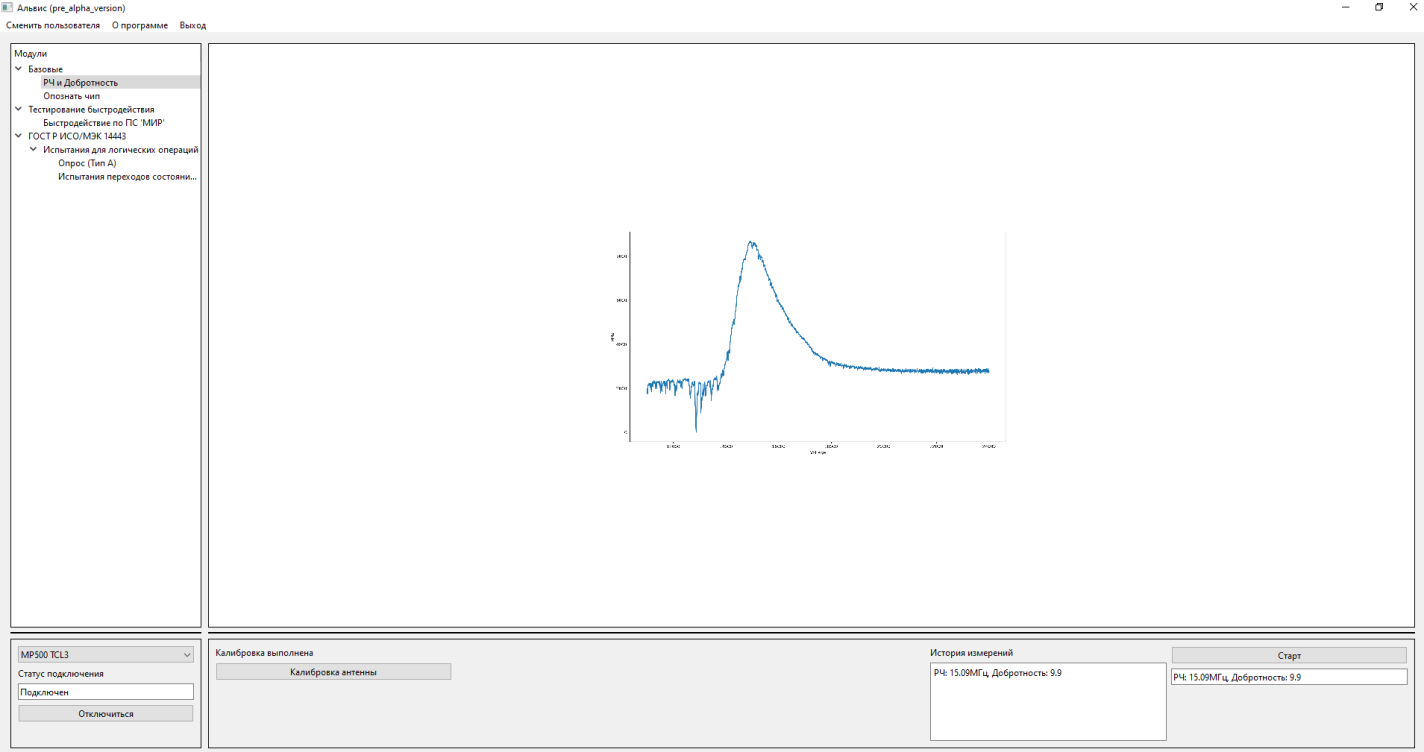
* Базовые:
* РЧ[[1]](#footnote-1) и Добротность;
* Опознать чип;
* Тестирование быстродействия:
* Быстродействие по ПС ‘МИР’
* ГОСТР ИСО/МЭК 14443:
* Испытания для логических операций
* Опрос (Тип А);
* Испытание переходов состояний PICC (Тип А)

# Базовый модуль

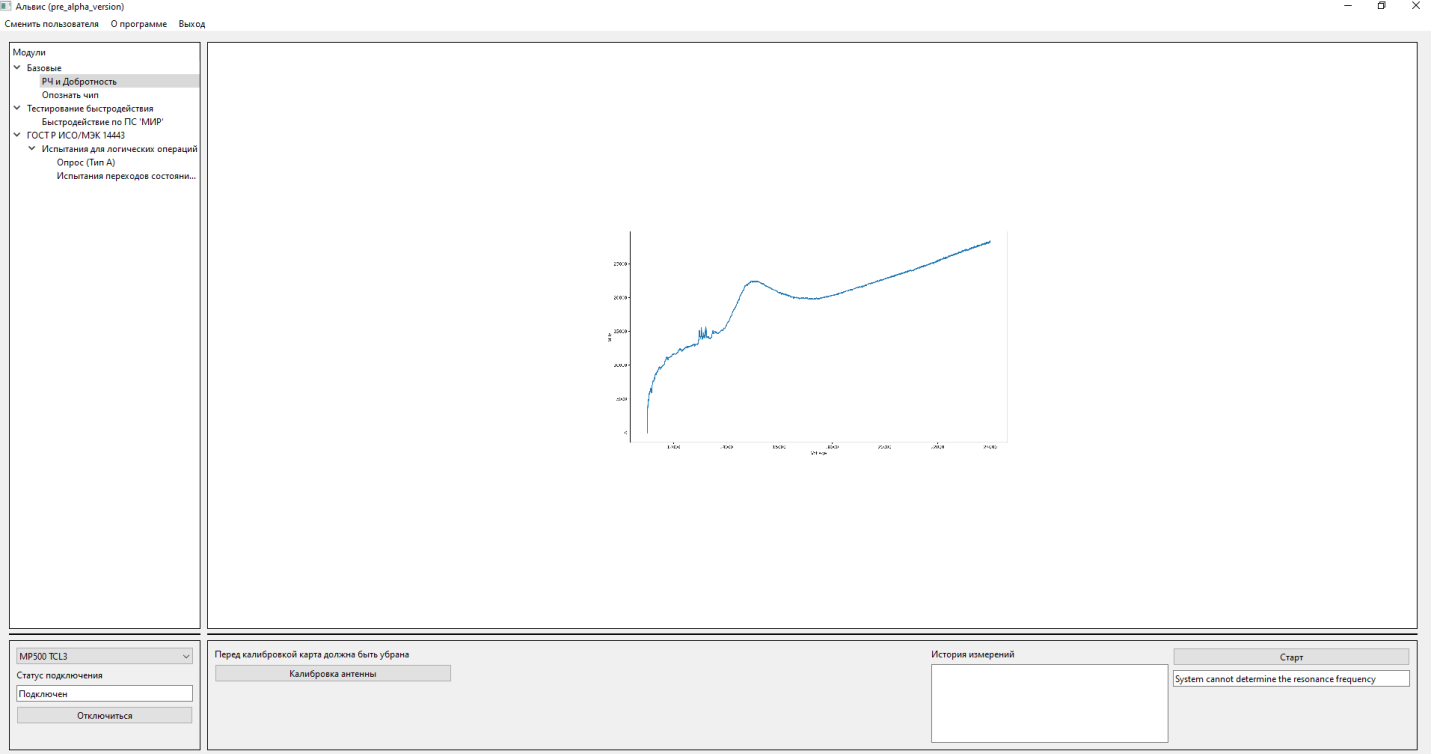
* + 1. РЧ и Добротность



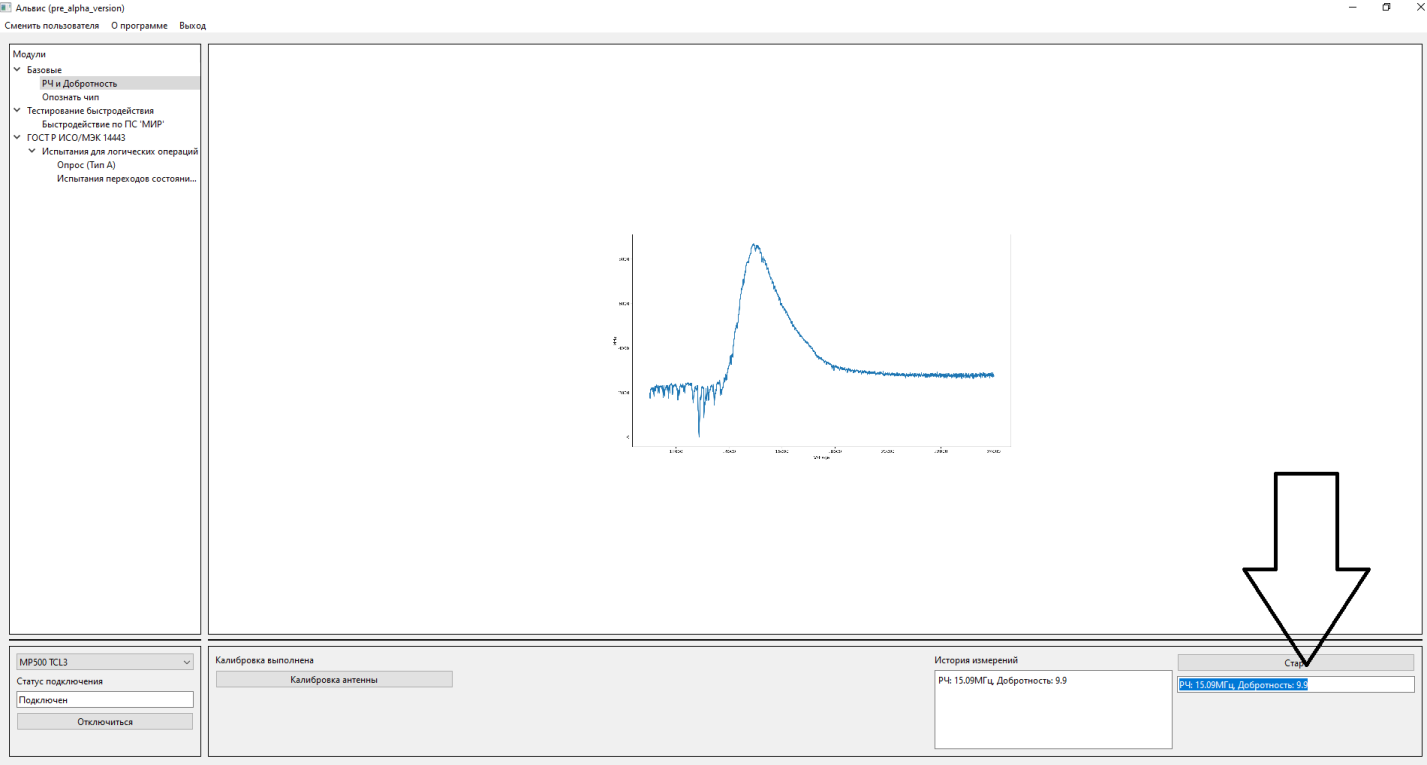
Перед началом работы нужно переключить на картридер который отвечает за РЧ и Добротность. Для этого нажимаем на кнопку «Калибровка антенны». Перед калибровкой карта должна быть убрана! – данная надпись будет написанна над кнопкой «Калибровка антенны». После успешной калибровки надпись меняется на «Калибровка выполнена». Далее нужно придложить карту к картридеру и нажать кнопку «Старт». После чего на экран выводится результат.



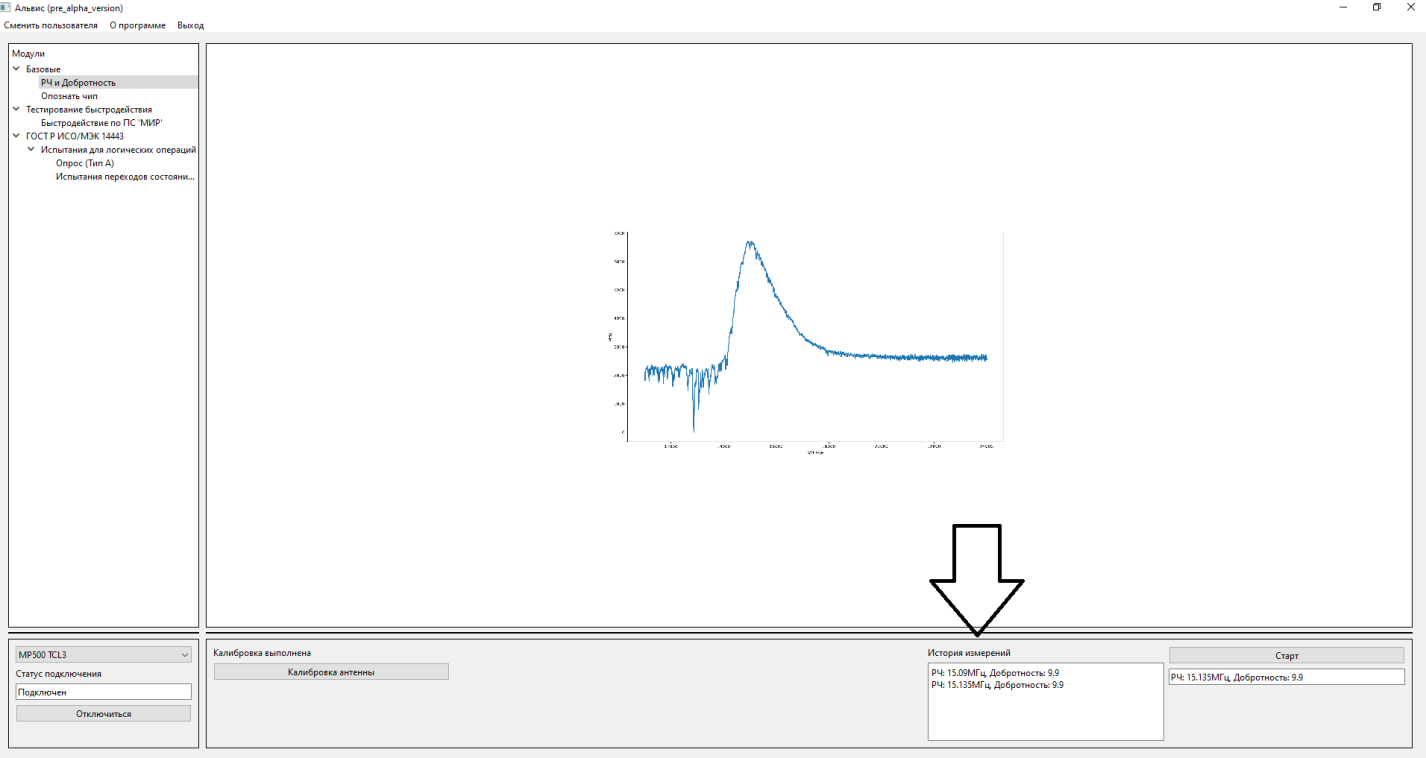
При не нажатии на кнопку «Калибровка антенны» и нажатии на кнопку «Старт» программа не выведет результат.



Под кнопкой «Старт» находится окно с информации о текущей карте.



Также есть окно «История измерений», которая отображает историю ранее отсканированных карт.



Требования к стандартам испытаний карты Мир.

* РЧ

При проведении испытания отклонения не должны превышать +/- 800КГц от среднего значения полученного при измерении всех ЗКДИ[[2]](#footnote-2) и ЗКБИ[[3]](#footnote-3) квалификационной выборки.

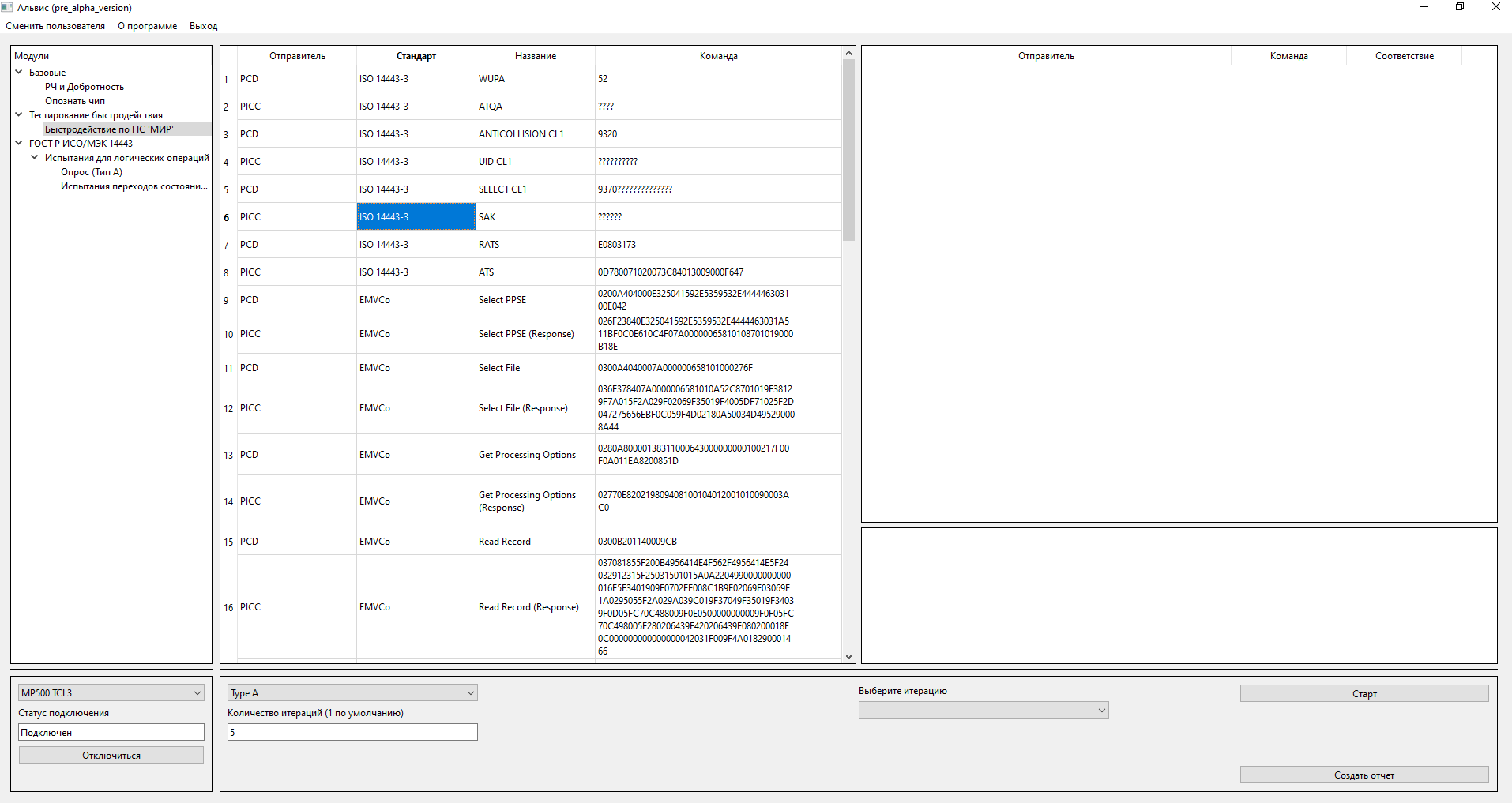
При этом, в случае, если среди квалификационных образцов, выбранных случайным образом, обнаружатся ЗКДИ и ЗКБИ не функционирующие по бесконтактному интерфейсу, квалификационное испытание должно считаться не пройденным.

* Добротность

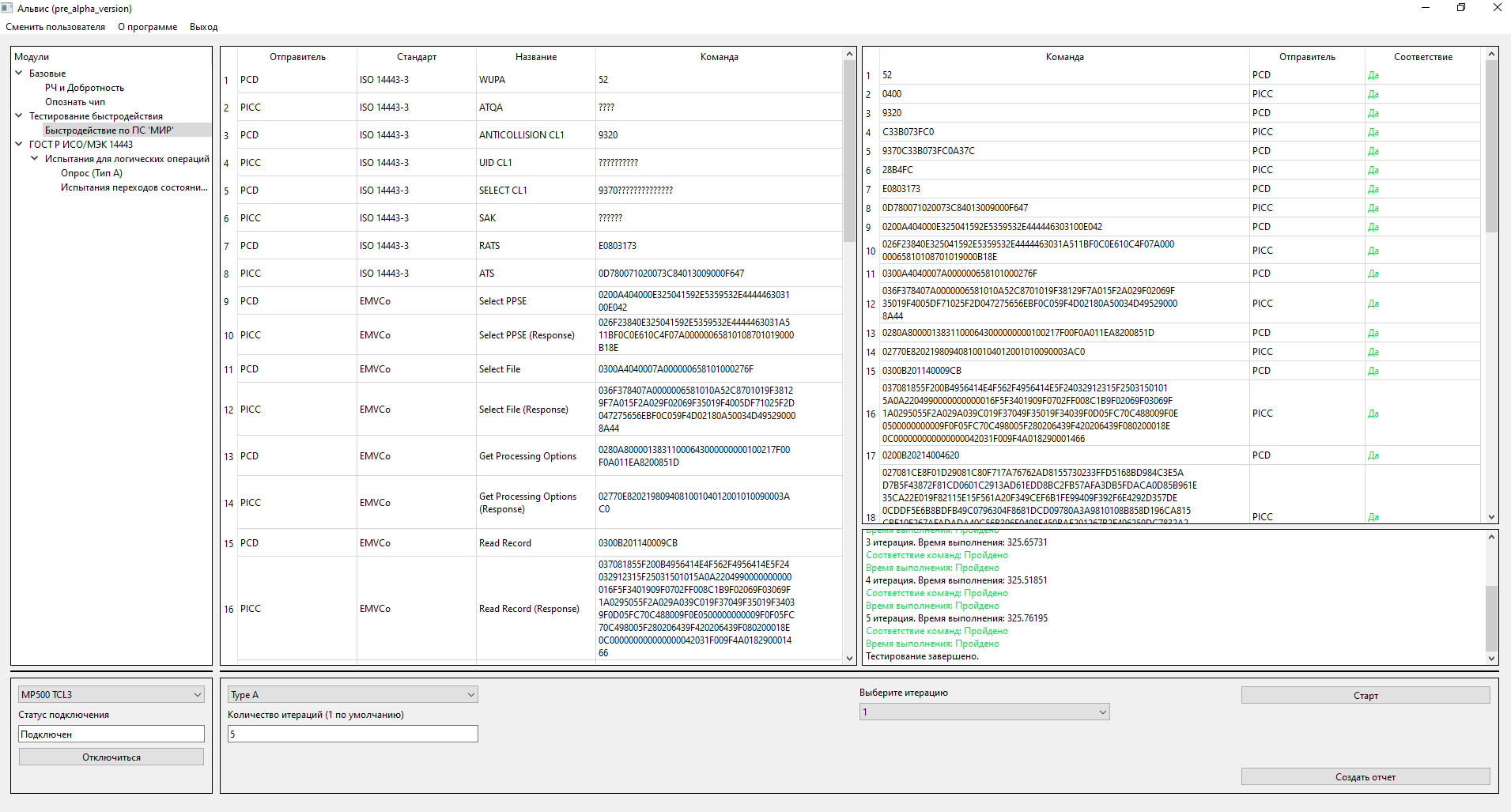
Измеренные значения в партии должны быть в диапазоне +/- 10% от среднего измеренного значения, полученного при измерении всех ЗКДИ и ЗКБИ квалификационной выборки.

# Функциональный модуль «Быстродействие пластиковых карт. Требования ПС «МИР».

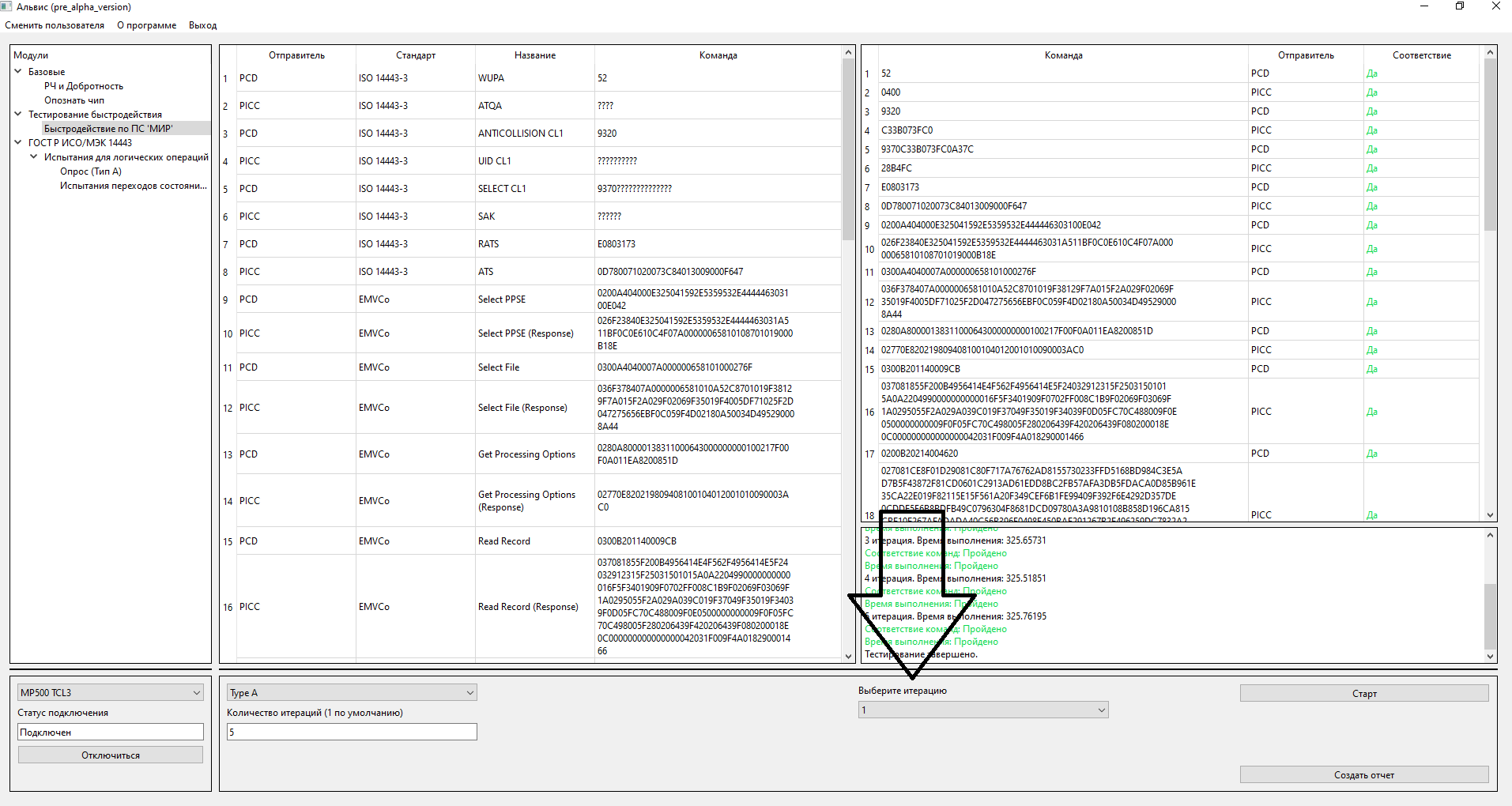
* + 1. Быстродействие по ПС ‘МИР’



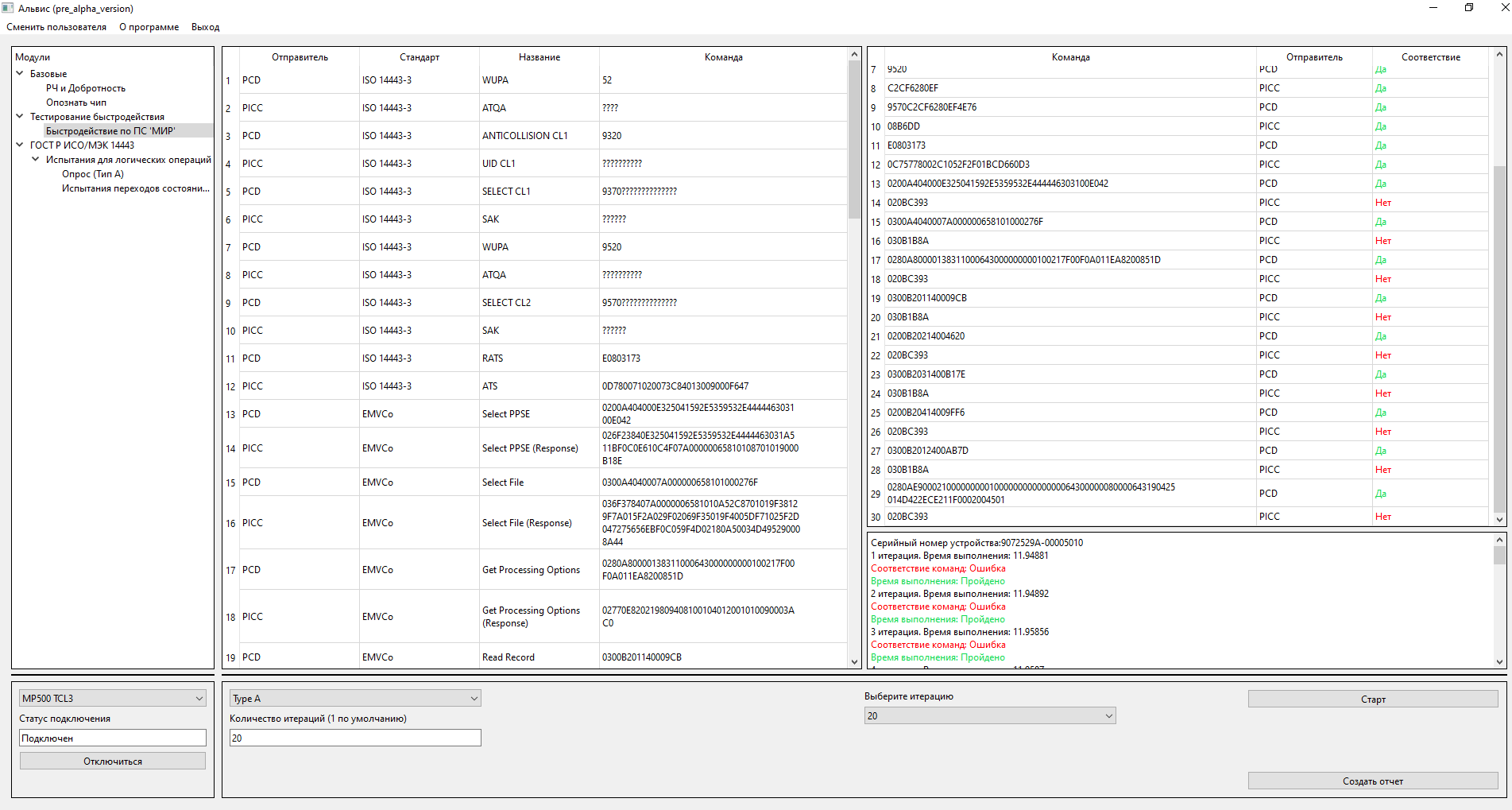
Перед началом работы нужно настроить тип карты (Type A или Type B). Вводим количество итераций, которые нужно выполнить. Прикладываем карту на картридер и нажимаем кнопку «Старт».



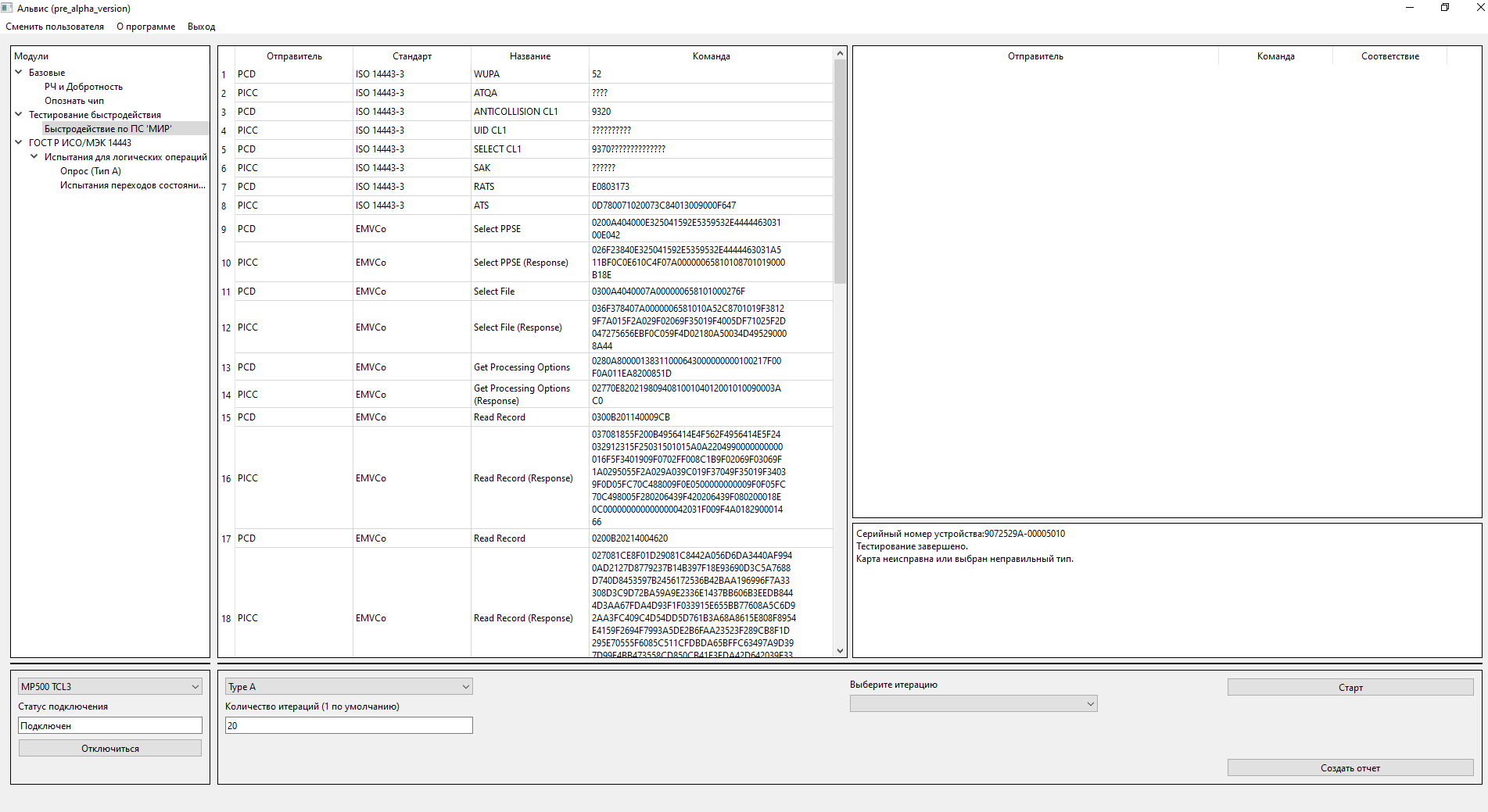
Переключение по итерации происходит в окне «Выберите итерацию». При нажатии на итерацию выводится информация о пройденной итерации.



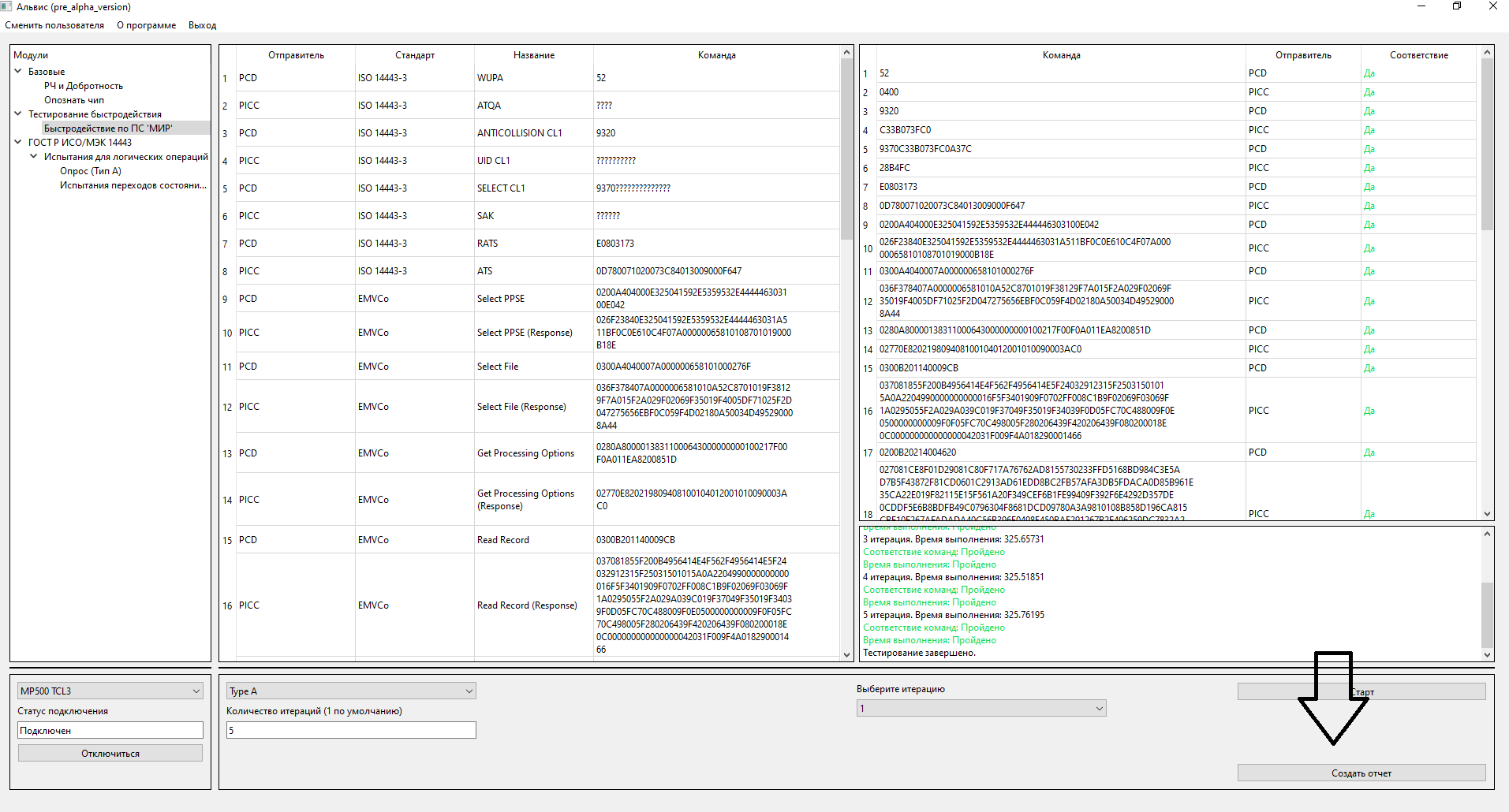
При отрицательном результате выводится ошибка.

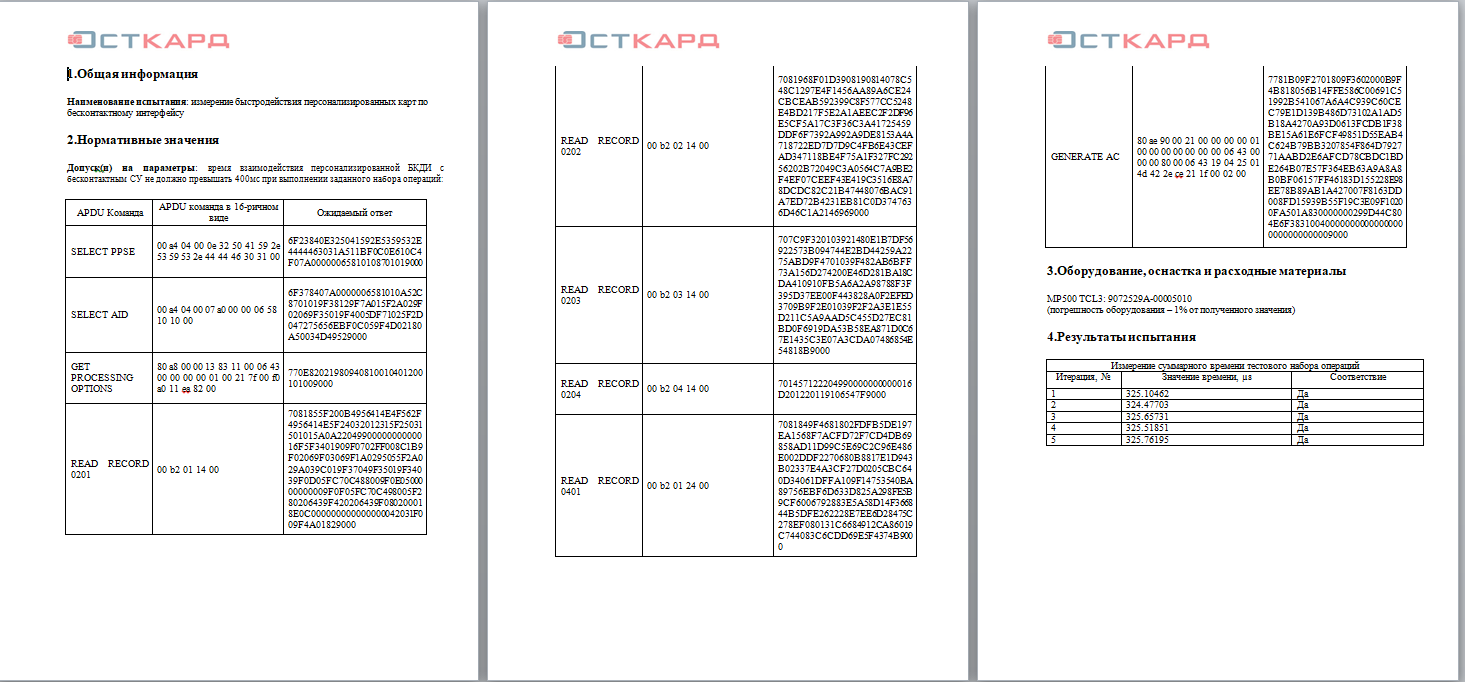


Если выбран неправильный тип карты выводится информация: «Карта неисправна или выбран неправильный тип».



Также можно сохранить отчёт, нажав на клавишу «Создать отчёт». Выбираем путь для сохранения и сохраняем.





**Требования к стандартам испытаний карты Мир.**

Приложение № 1. DUAL, длина RSA ключа 1024.

1. SELECT FILE 2PAY.SYS.DDF01 to get the PPSE directory

Подаваемая команда:

00a404000e325041592e5359532e444446303100

Ожидаемый ответ на команду:

6f23840e325041592e5359532e4444463031a511bf0c0e610c4f07a0000006581010870101

SW1SW2 : 90 00 (Success)

2. Select application by AID

Подаваемая команда:

00a4040007a000000658101000

Ожидаемый ответ на команду:

6f378407a0000006581010a52c8701019f38129f7a015f2a029f02069f35019f4005df71025f2d047275656ebf0c059f4d02180a50034d4952

SW1SW2 : 90 00 (Success)

3. Send GET PROCESSING OPTIONS command

Подаваемая команда:

80a80000138311000643000000000001227f00f0a011020200

Ожидаемый ответ на команду:

770e8202198094081001040120010100

SW1SW2 : 90 00 (Success)

4. Send READ RECORD to read SFI 2 record 1

Подаваемая команда:

00b2011400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081855f200b4956414e4f562f4956414e5f24032012315f25031501015a0a2204990000000000016f5f3401909f0702ff008c1b9f02069f03069f1a0295055f2a029a039c019f37049f35019f34039f0d05fc70c488009f0e0500000000009f0f05fc70c498005f280206439f420206439f080200018e0c000000000000000042031f009f4a0182

SW1SW2 : 90 00 (Success)

5. Send READ RECORD to read SFI 2 record 2

Подаваемая команда:

00b2021400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081968f01d390819007e32e659f13a72cf1f56e57aef9ad2258ce1171355f03a1952fc4d2bbf4bbd986c90d7dd8f76fbf7f4a2a31bd31039a3c9bcd1c100b092fd89ac90e7379437b6e57a78d9185ca59624e892d75a3da4d98fdce3fb4d7c567605594c01a574dccfee54e7de393cb1490431aa37b956a3dd301606f02358ebca012a6e952241986d81166b179ff79f7afc7966a69228c28

SW1SW2 : 90 00 (Success)

6. Send READ RECORD to read SFI 2 record 3

Подаваемая команда:

00b2031400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

707c9f3201039214022313ad0c8e615cd6e2b4a8f1402c8eafbaf7739f4701039f482ac4b2c0c7c76538f86b654f5cd1dd516b62e76764ced5fa936ba397d0470d55c06606d6a360ee3a08f87b9f2e01039f2f2a8e79fd38921b3bb7f4dc720c7f64bba2947d42457fe817de5d3e36655fb320d41674706ca813e5e61ccb

SW1SW2 : 90 00 (Success)

7. Send READ RECORD to read SFI 2 record 4

Подаваемая команда:

00b2041400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

701457122204990000000000016d201220119106547f

SW1SW2 : 90 00 (Success)

8. Send READ RECORD to read SFI 4 record 1

Подаваемая команда:

00b2012400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081849f46818011b56286a39d8bdcce52a94f6e0db275913a556273f92d0ea9dbaa9173cef99e85a77eb9e92bc1857b1cd1a760fc94ced6f161348457a7fd62b197505098ffcfc892418370b4702d0571e9aeeced370d58140e6c185ec1661018afa05c26cb9d1c8805f59a41f9d5d82c6200accf02295ec35b9ea3215dd3e3367e15d4410385

SW1SW2 : 90 00 (Success)

9. Send GENERATE first APPLICATION CRYPTOGRAM command

Подаваемая команда: 80ae90002100000000000100000000000006430000008000064319061101ad1c3a7e221f000200

Пример ответа на команду (требуемые проверки описаны п.5-п.6 “Методика испытаний набора карт”):

7781b09f2701809f360200039f4b81805145858e413b4a8863cf4b6edad27ce711d6ee752c4add8c0ca7e8487dde070c94afae91c717c3097dd683e6a44f37bf992b4caeed2b883566ceedaca7ef471bcb857158014f541ede46c20097cd56e67ab115265b793c9e446812850af7a77cf30accd45562f18f8662f08c74489c372647bd4941de002323363098187d4cc49f10200fa501a8300000007ed08b215fb5882310040000000000000000000000000000

SW1SW2 : 90 00 (Success)

Приложение № 2. DUAL, длина RSA ключа 1440.

1. SELECT FILE 2PAY.SYS.DDF01 to get the PPSE directory

Подаваемая команда:

00a404000e325041592e5359532e444446303100

Ожидаемый ответ на команду:

6f23840e325041592e5359532e4444463031a511bf0c0e610c4f07a0000006581010870101

SW1SW2 : 90 00 (Success)

2. Select application by AID

Подаваемая команда:

00a4040007a000000658101000

Ожидаемый ответ на команду:

6f378407a0000006581010a52c8701019f38129f7a015f2a029f02069f35019f4005df71025f2d047275656ebf0c059f4d02180a50034d4952

SW1SW2 : 90 00 (Success)

3. Send GET PROCESSING OPTIONS command

Подаваемая команда:

80a80000138311000643000000000001227f00f0a011020200

Ожидаемый ответ на команду:

770e8202198094081001040120010100

SW1SW2 : 90 00 (Success)

4. Send READ RECORD to read SFI 2 record 1

Подаваемая команда:

00b2011400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081855f200b4956414e4f562f4956414e5f24032012315f25031501015a0a2204990000000000016f5f3401909f0702ff008c1b9f02069f03069f1a0295055f2a029a039c019f37049f35019f34039f0d05fc70c488009f0e0500000000009f0f05fc70c498005f280206439f420206439f080200018e0c000000000000000042031f009f4a0182

SW1SW2 : 90 00 (Success)

5. Send READ RECORD to read SFI 2 record 2

Подаваемая команда:

00b2021400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081ce8f01d29081c83751fe88e9c52265bb332b34a088130551a99123ddbd016e982e0f39b058b290e9abdc500976c3bdac105039c93fe5b7a1be82c234f484148b0fcfaa125c06faf13e90da3fbc3cbdafc1d497e17416f8af2191cfdc4224ac10b99d72f6174ed460738c1a6e14935bcaebfb4802396d60ca189c8794f18520cdbbaf1f51fd5b647923e47e70ba3a69cf6a461dd139799ff418699b7597c4edce139493e58eb7e73b952e378bbb233fa97cacdf95193758f28fe9ad812b7b4079572a8392f971d3c9096099c650b4eb

SW1SW2 : 90 00 (Success)

6. Send READ RECORD to read SFI 2 record 3

Подаваемая команда:

00b2031400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

70789f32010392109ccb5695aa683b6732d8bf72b693b4c79f4701039f482a8531ac3752787287bcfe1359ff72241f02bee2b55546b227c16edf58f4a5368cd0bbd6bb663ca1d6dbab9f2e01039f2f2a832a2246a93677150d1ceba9d2c27ee1093630810c68499567b1b3a9199dd932cb35e829382b5d9b351d

SW1SW2 : 90 00 (Success)

7. Send READ RECORD to read SFI 2 record 4

Подаваемая команда:

00b2041400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

701457122204990000000000016d201220119106547f

SW1SW2 : 90 00 (Success)

8. Send READ RECORD to read SFI 4 record 1

Подаваемая команда:

00b2012400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081b89f4681b434962aa0cb7c81eaa571caafc60224d787b05a705613175a39d546d62eb502b8e210c6d5e6dfed68cfce858fb8d27ca9d8ee8f56284532a9e8fc555562493dfd1eb3e824ce588d80702d519a492c034137da0500b56e83ee5f206d81c74df0f26d067fa4e698279c84bf7043dd6c371fed2102c53c719e433f1ddde3d32dc01b10417a23edcc9f0763d3149dae6279d86f411fd69bd6fe4c4fe398abd752e7a14eeb6efcbcb704d18eea666ce0832a06d46e2e9e

SW1SW2 : 90 00 (Success)

9. Send GENERATE first APPLICATION CRYPTOGRAM command

Подаваемая команда:

80ae900021000000000001000000000000064300000080000643190611018426970b221f000200

Пример ответа на команду (требуемые проверки описаны п.5-п.6 “Методика испытаний набора карт”):

7781e49f2701809f360200019f4b81b41da867d123e3de68ebeb38c26a6415324b7c66ff48d046b9bba05838e0d54ca469a64bc7abc54be261f22abb728ae1e259d81960d5a29757e4393426f74b097f1c4f0d6cbfdcbbc5df861b851994c3c2d19b2c1cd93e9fbade5781d3e17e011ab4a852b47d1054d0739ed225e1412ca45f8544b57bba4ee5d026edb944eb5c977e11bbbbe0962f3756164a2a5f05881f061be475784bc026f451e3b58d0155dd139cdca7809c5d14259be2acaba28531f179c24c9f10200fa501a830000000de4f0145adcc4c1f10040000000000000000000000000000

SW1SW2 : 90 00 (Success)

Приложение № 3. DUAL, длина RSA ключа 1600.

1. SELECT FILE 2PAY.SYS.DDF01 to get the PPSE directory

Подаваемая команда:

00a404000e325041592e5359532e444446303100

Ожидаемый ответ на команду:

6f23840e325041592e5359532e4444463031a511bf0c0e610c4f07a0000006581010870101

SW1SW2 : 90 00 (Success)

2. Select application by AID

Подаваемая команда:

00a4040007a000000658101000

Ожидаемый ответ на команду:

6f378407a0000006581010a52c8701019f38129f7a015f2a029f02069f35019f4005df71025f2d047275656ebf0c059f4d02180a50034d4952

SW1SW2 : 90 00 (Success)

3. Send GET PROCESSING OPTIONS command

Подаваемая команда:

80a80000138311000643000000000001227f00f0a011020200

Ожидаемый ответ на команду:

770e8202198094081001040120010100

SW1SW2 : 90 00 (Success)

4. Send READ RECORD to read SFI 2 record 1

Подаваемая команда:

00b2011400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081855f200b4956414e4f562f4956414e5f24032012315f25031501015a0a2204990000000000016f5f3401909f0702ff008c1b9f02069f03069f1a0295055f2a029a039c019f37049f35019f34039f0d05fc70c488009f0e0500000000009f0f05fc70c498005f280206439f420206439f080200018e0c000000000000000042031f009f4a0182

SW1SW2 : 90 00 (Success)

5. Send READ RECORD to read SFI 2 record 2

Подаваемая команда:

00b2021400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081ce8f01d29081c84f74d2bda0c2589c76d09fac081cb05302f3ee8ad2bb35bd1d06ff8e5ed5365efc38f67936d86da58f09fda5a4f8a71634470334ddf2248f0fd820c0eda1d3a108b144b28711702f71832f56349c0f86a78f2c9954daf600a0837a221f70c7e9d2af149afd38a58974ba746bb7ac4d45e016610c7f6654da48401f2b9470a0ea89367762c5d422afb1536fcb789f885b10d94199369a197fe0b8e5c4eb16d7c6bbe08a7ecbd542b041940750bb5d7f3c4d29ac0495c7056f0a29de17873e060ce0da002b7f5c8c4a

SW1SW2 : 90 00 (Success)

6. Send READ RECORD to read SFI 2 record 3

Подаваемая команда:

00b2031400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

70818c9f320103922469382ba9301efe74b08a86b6b50db509d9165d6514d152d36d2de9a2631c48bdf3512c839f4701039f482a1b600ac6e32111e8575a6e539aa0d4a3bc25ca798add42f7ef9a17bd3f4b96fe3fb93571b663054a72059f2e01039f2f2a2c2bd1a95caec72a2724966d7ab3ca4a3765698c0eea4794cb16a907131af93be273fbda6933924d918f

SW1SW2 : 90 00 (Success)

7. Send READ RECORD to read SFI 2 record 4

Подаваемая команда:

00b2041400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

701457122204990000000000016d201220119106547f

SW1SW2 : 90 00 (Success)

8. Send READ RECORD to read SFI 4 record 1

Подаваемая команда:

00b2012400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081cc9f4681c81b7757769def0969f67a34758f7c64391e2d03d45e21f6ec1231c20259555d71bf75f8244c28a76186a6a596e125e3c15683a5686e71e179579e5a0da26c10196c29fbca642c7116b1b29284f62d7d08e6e9933f50c97883889edc90ff9e48f52a6e5d4eb7fc7e644168bca72f9fa837d0b7a9310348d187f1e6598f4c414e80ddd5334ddc1952cd4827150e20430d74dc5b8c

647fca9789236e576beb9ea7c1fba2848267b661cf2f2db0b6ad216f58da6ba09b5f2a7a3b4f8131f2609caf0bd23b03a5d5756c23

SW1SW2 : 90 00 (Success)

9. Send GENERATE first APPLICATION CRYPTOGRAM command

Подаваемая команда:

80ae9000210000000000010000000000000643000000800006431906110128f8d90a221f000200

Пример ответа на команду (требуемые проверки описаны п.5-п.6 “Методика испытаний набора карт”):



SW1SW2 : 90 00 (Success)

Приложение № 4. CONTACTLESS, длина RSA ключа 1024.

1. SELECT FILE 2PAY.SYS.DDF01 to get the PPSE directory

Подаваемая команда:

00a404000e325041592e5359532e444446303100

Ожидаемый ответ на команду:

6f23840e325041592e5359532e4444463031a511bf0c0e610c4f07a0000006581010870101

SW1SW2 : 90 00 (Success)

2. Select application by AID

Подаваемая команда:

00a4040007a000000658101000

Ожидаемый ответ на команду:

6f378407a0000006581010a52c8701019f38129f7a015f2a029f02069f35019f4005df71025f2d047275656ebf0c059f4d02180a50034d4952

SW1SW2 : 90 00 (Success)

3. Send GET PROCESSING OPTIONS command

Подаваемая команда:

80a80000138311000643000000000001227f00f0a011020200

Ожидаемый ответ на команду:

770e8202198094081001040120010100

SW1SW2 : 90 00 (Success)

4. Send READ RECORD to read SFI 2 record 1

Подаваемая команда:

00b2011400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081855f200b4956414e4f562f4956414e5f24032012315f25031501015a0a2204990000000000016f5f3401909f0702ff008c1b9f02069f03069f1a0295055f2a029a039c019f37049f35019f34039f0d05f270c480009f0e0500000000009f0f05f270c480005f280206439f420206439f080200018e0c000000000000000042031f009f4a0182

SW1SW2 : 90 00 (Success)

5. Send READ RECORD to read SFI 2 record 2

Подаваемая команда:

00b2021400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081968f01d39081901e0d0b0ae89530385d997697eb912b632183278da0ac55f30ae66af7f4060ba7f37b6e8a5f1f004c70db99aab72564dda2d391582aa343e8be30d4552af85f47a90275fb7f279dd415b8d47908a2d9db32da104b9a75113eb210dad8f51a09d1ef8af5b12fc93047ca5d6b6e1337387171a943c0915844c8e1e77e5a8f61f63079ac762db9e4b153b6e1dd79f5356fc8

SW1SW2 : 90 00 (Success)

6. Send READ RECORD to read SFI 2 record 3

Подаваемая команда:

00b2031400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

704b9f3201039214ba0479ff44e1e78f9367ebe2d4f42f216ce9b6f39f4701039f482aba8e335a69378f8d3547402a550ae71bd5118a004a0469a0f7ad0c25485802f40d17bcdea8f9a1af68a7

SW1SW2 : 90 00 (Success)

7. Send READ RECORD to read SFI 2 record 4

Подаваемая команда:

00b2041400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

701457122204990000000000016d201220619106547f

SW1SW2 : 90 00 (Success)

8. Send READ RECORD to read SFI 4 record 1

Подаваемая команда:

00b2012400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081849f4681804025e5f8f6f7cd5fdc76a6d06db89f1e9e622111e3102d9dbdc74cfc49e6ebca3af2f6820b2aeb9ce437dcff427dcb3caf6a0d35e5f4aa02e430ef86b5333e92ed66adee4b3c5380de0a5e8c8744421e8e7ff5377be56a14ae6597604fab4203f618ba6006bd6109bdb2b0b59a72efb348043a3b45c079c44f694698a7428839

SW1SW2 : 90 00 (Success)

9. Send GENERATE first APPLICATION CRYPTOGRAM command

Подаваемая команда:

80ae900021000000000001000000000000064300000080000643190611011ce914b5221f000200

Пример ответа на команду (требуемые проверки описаны п.5-п.6 “Методика испытаний набора карт”):

7781b09f2701809f3602000b9f4b81806108eb0f9dfe0f675e880ea0e022e829e500a67824c3cc0ae10467d235cfce6c819cf4cec27f318ceb57c4719f0b2aab9fbdcb71a0d1d1245766e548d65af3fba8c4a18dfd4ed96913d0d4bc79fe6a4c714c5e23a719c13c0009183e2cef764c8fd2c7776077e4cf295f38ccfa74d5a26eb15b0a080b8df6d3b89052223ec76b9f10200fa501a800000000f26e07616c1addc610040000000000000000000000000000

SW1SW2 : 90 00 (Success)

Приложение № 5. CONTACTLESS, длина RSA ключа 1440.

1. SELECT FILE 2PAY.SYS.DDF01 to get the PPSE directory

Подаваемая команда:

00a404000e325041592e5359532e444446303100

Ожидаемый ответ на команду:

6f23840e325041592e5359532e4444463031a511bf0c0e610c4f07a0000006581010870101

SW1SW2 : 90 00 (Success)

2. Select application by AID

Подаваемая команда:

00a4040007a000000658101000

Ожидаемый ответ на команду:

6f378407a0000006581010a52c8701019f38129f7a015f2a029f02069f35019f4005df71025f2d047275656ebf0c059f4d02180a50034d4952

SW1SW2 : 90 00 (Success)

3. Send GET PROCESSING OPTIONS command

Подаваемая команда:

80a80000138311000643000000000001227f00f0a011020200

Ожидаемый ответ на команду:

770e8202198094081001040120010100

SW1SW2 : 90 00 (Success)

4. Send READ RECORD to read SFI 2 record 1

Подаваемая команда:

00b2011400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081855f200b4956414e4f562f4956414e5f24032012315f25031501015a0a2204990000000000016f5f3401909f0702ff008c1b9f02069f03069f1a0295055f2a029a039c019f37049f35019f34039f0d05f270c480009f0e0500000000009f0f05f270c480005f280206439f420206439f080200018e0c000000000000000042031f009f4a0182

SW1SW2 : 90 00 (Success)

5. Send READ RECORD to read SFI 2 record 2

Подаваемая команда:

00b2021400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081ce8f01d29081c837add47d9ff722bf57b8038344b112b5bbcc4e43046a780ddb807c47b0b975d15369369517ae88e2446511f21b60e7e2abeb0bf233626ef8a14daec6db6073b9ee003ed5f5a6d9ba8bb2c2b82b00593cc94aa3481e64dc96fa95c4b13d1156dd228dcc76d089ef8246050ff38d31b81ab048d1cdf75d9820bbb2d7e78bc44562ef0ebffd7832451dec15da6dbe92d34007b93e4c251f1ba30c8f5caef1baa6533c9ee76f7836116ac5a1b9b8d1bf98e84418048c966917062419235ff310106531d9e3eecb8fbb84

SW1SW2 : 90 00 (Success)

6. Send READ RECORD to read SFI 2 record 3

Подаваемая команда:

00b2031400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

70479f3201039210dbe119117fc705c51e026d017e471f2d9f4701039f482aa0780d51f24ae1461f4f3334c17fe59e9176c2c29b7b199b4b95970c102d79fa9c190f73008357e98dbd

SW1SW2 : 90 00 (Success)

7. Send READ RECORD to read SFI 2 record 4

Подаваемая команда:

00b2041400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

701457122204990000000000016d201220619106547f

SW1SW2 : 90 00 (Success)

8. Send READ RECORD to read SFI 4 record 1

Подаваемая команда:

00b2012400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081b89f4681b43d4bb68b8dcc0c92d62a8b3c333cb177412ad99ae7b255aa15c652b6b781911b9258eeaea2bec118442e81b87e7728f908d3e282539ef2f9ec0ec6fce4fe282e3b62de4b689efa4d10d2fd9c9c5844de20b81f2e6f866e29eafb1662f31271aeb7aa2f3e81b5d4b46c083fed00da3aa7dc71f7fd72b14540a2b8541aba579500630281a4f63fe0ed40c16e84fe0c6ad673d7d50ae0a1f546b140e0c14e77300eb0309ccb87fb5d5c7767fa8f19f9fa114fc972e0

SW1SW2 : 90 00 (Success)

9. Send GENERATE first APPLICATION CRYPTOGRAM command

Подаваемая команда:

80ae9000210000000000010000000000000643000000800006431906110141a87ed1221f000200

Пример ответа на команду (требуемые проверки описаны п.5-п.6 “Методика испытаний набора карт”):

7781e49f2701809f360200059f4b81b48ff56177236e875f995bac8b09464635c31400e065b62d994117b4962d816a4c42b1a2b4e1f3f8745e6a474004b97239cf603e5e53104dacd6c466a525ede0ff392d4463d16217525a44b7c3e8e5e0cdf95eba82bd59662ef3867ee5d53de40095506b79a4ef016c297579c1dbaeeaf5c6ccb5f571d4eeb84f7004e81e1eea689e5f864614bdb90feefef1e0609ac54b9e6cdb2d2f70df9d48def440cea08d68ddc32695bb1763fb66623b6e6c6e49383aaa19d79f10200fa501a800000000e5219abc8292650910040000000000000000000000000000

SW1SW2 : 90 00 (Success)

Приложение № 6. CONTACTLESS, длина RSA ключа 1600.

1. SELECT FILE 2PAY.SYS.DDF01 to get the PPSE directory

Подаваемая команда:

00a404000e325041592e5359532e444446303100

Ожидаемый ответ на команду:

6f23840e325041592e5359532e4444463031a511bf0c0e610c4f07a0000006581010870101

SW1SW2 : 90 00 (Success)

2. Select application by AID

Подаваемая команда:

00a4040007a000000658101000

Ожидаемый ответ на команду:

6f378407a0000006581010a52c8701019f38129f7a015f2a029f02069f35019f4005df71025f2d047275656ebf0c059f4d02180a50034d4952

SW1SW2 : 90 00 (Success)

3. Send GET PROCESSING OPTIONS command

Подаваемая команда:

80a80000138311000643000000000001227f00f0a011020200

Ожидаемый ответ на команду:

770e8202198094081001040120010100

SW1SW2 : 90 00 (Success)

4. Send READ RECORD to read SFI 2 record 1

Подаваемая команда:

00b2011400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081855f200b4956414e4f562f4956414e5f24032012315f25031501015a0a2204990000000000016f5f3401909f0702ff008c1b9f02069f03069f1a0295055f2a029a039c019f37049f35019f34039f0d05f270c480009f0e0500000000009f0f05f270c480005f280206439f420206439f080200018e0c000000000000000042031f009f4a0182

SW1SW2 : 90 00 (Success)

5. Send READ RECORD to read SFI 2 record 2

Подаваемая команда:

00b2021400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081ce8f01d29081c85f38baa060fbaeb6333fa9db06878944d860b25721d8a96db6bdb991e4f510ead66d794da87d2b5bbe4098e9bd286729711bc08f8841e5987f67fa97fa06decaf7fea77942a0d30bc527fe80f36f200d483655dc6ec17aee2828d08390b06973160a9fd10e5da4ed523847c750d8b4369bc5d438f2f45be3f63a86e53e7cd42991c9cb2c7142697ffc99b108401a468b7e3c22a7e403a5425d35903fb583f0d8eb791efb608f7666bca68bcceba76b471b2b88ace8e21f15ad4baf0444e137a8cb93d8de848cc089

SW1SW2 : 90 00 (Success)

6. Send READ RECORD to read SFI 2 record 3

Подаваемая команда:

00b2031400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

705b9f32010392248ae417cd25a7e032ab2a09c8b49073935316cf981aa18e53c929298b52c6730839cee9479f4701039f482a2167d6e7db699c4f353f5c17bb326d34b1bb6203185901d1dcaf782a59ee8d65b9b3fc5c82459a331873

SW1SW2 : 90 00 (Success)

7. Send READ RECORD to read SFI 2 record 4

Подаваемая команда:

00b2041400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):701457122204990000000000016d201220619106547f

SW1SW2 : 90 00 (Success)

8. Send READ RECORD to read SFI 4 record 1

Подаваемая команда:

00b2012400

Пример ответа на команду (требуемые проверки описаны в п.4 “Методика испытаний набора карт”):

7081cc9f4681c81e7f5da69cae66ea3eefee8a80e690ef97b0b024804af0b0f2f5584b0e3b2728d745859a4f48fecaea8e488422a1917fdcb153c2ebc0136cbbaac2c85109de311d519692bc12b23bf6229b14570d42fb6ea67bd00946a6ac52e0cde9b5720a3e8c26136f3397a268bd9e488d5ee7f7952191e081e65356b299f1bfb7782ad7c8bf4ad9ae9ac9c7c14f83a2c9cdf99dc422b0df5b3d6f1a4258c42a136847b3b7ec7001a8321ecca7b5eb46137a6ab65698d93c649a6390fa21c75d4d058b9a1227e1c3ddce3ab707

SW1SW2 : 90 00 (Success)

9. Send GENERATE first APPLICATION CRYPTOGRAM command

Подаваемая команда:

80ae90002100000000000100000000000006430000008000064319061101250355c7221f000200

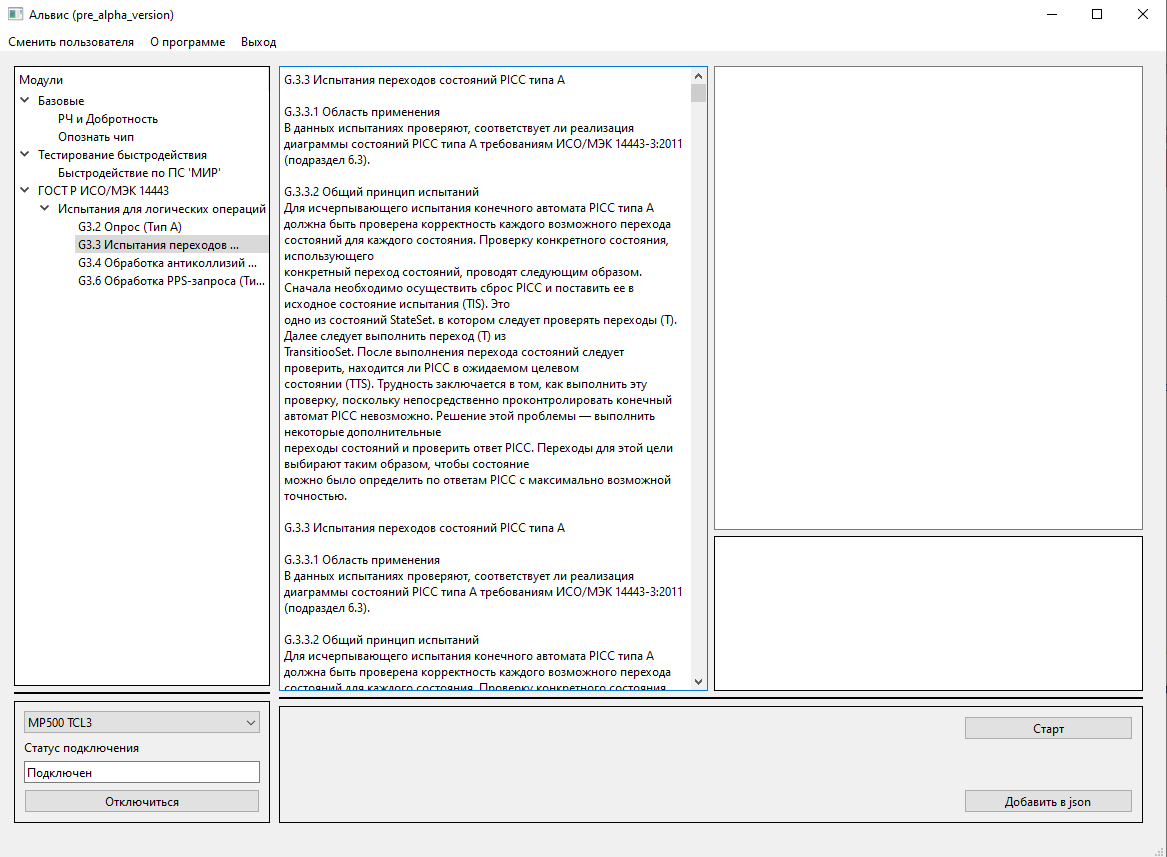
Пример ответа на команду (требуемые проверки описаны п5-п.6 “Методика испытаний набора карт”):



SW1SW2 : 90 00 (Success)

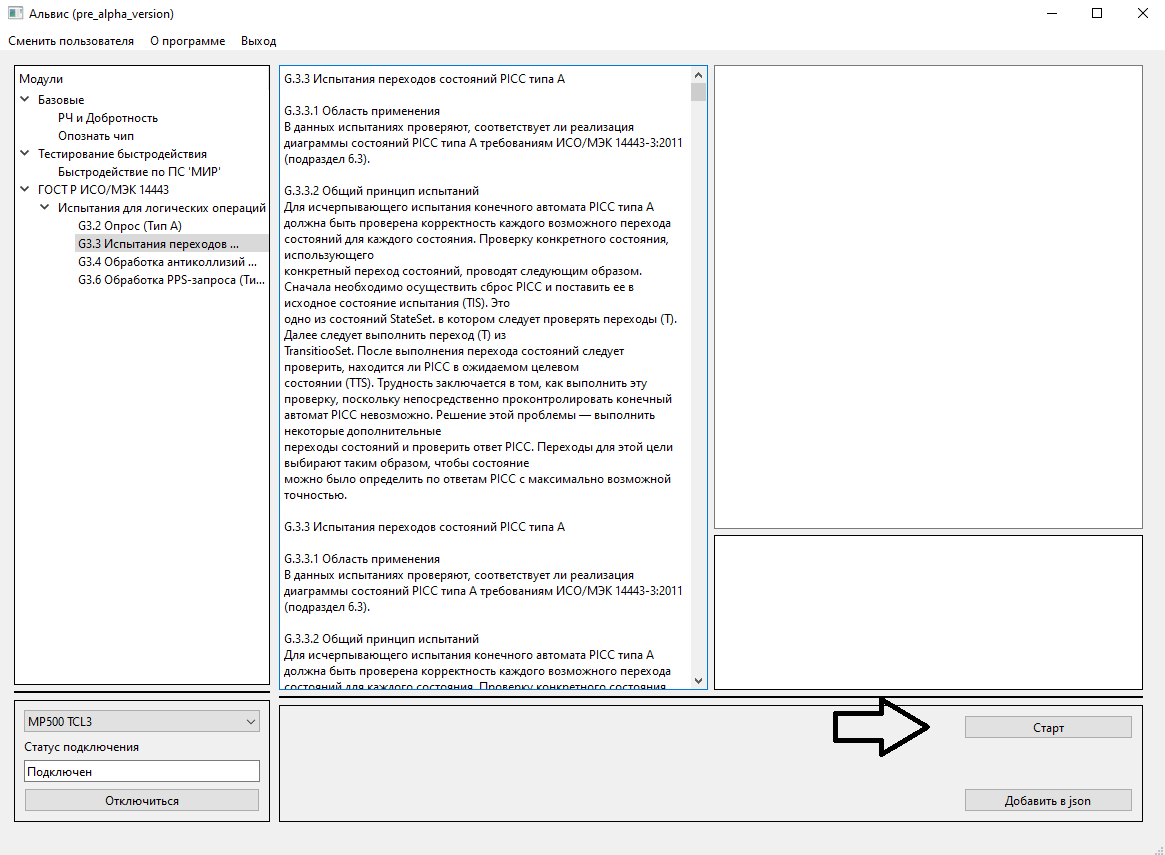
# Функциональный модуль «Соответствия требованиям ГОСТ Р 14443 для PICC. Протокольная часть.

* + 1. Испытания переходов состояний PICC типа А.

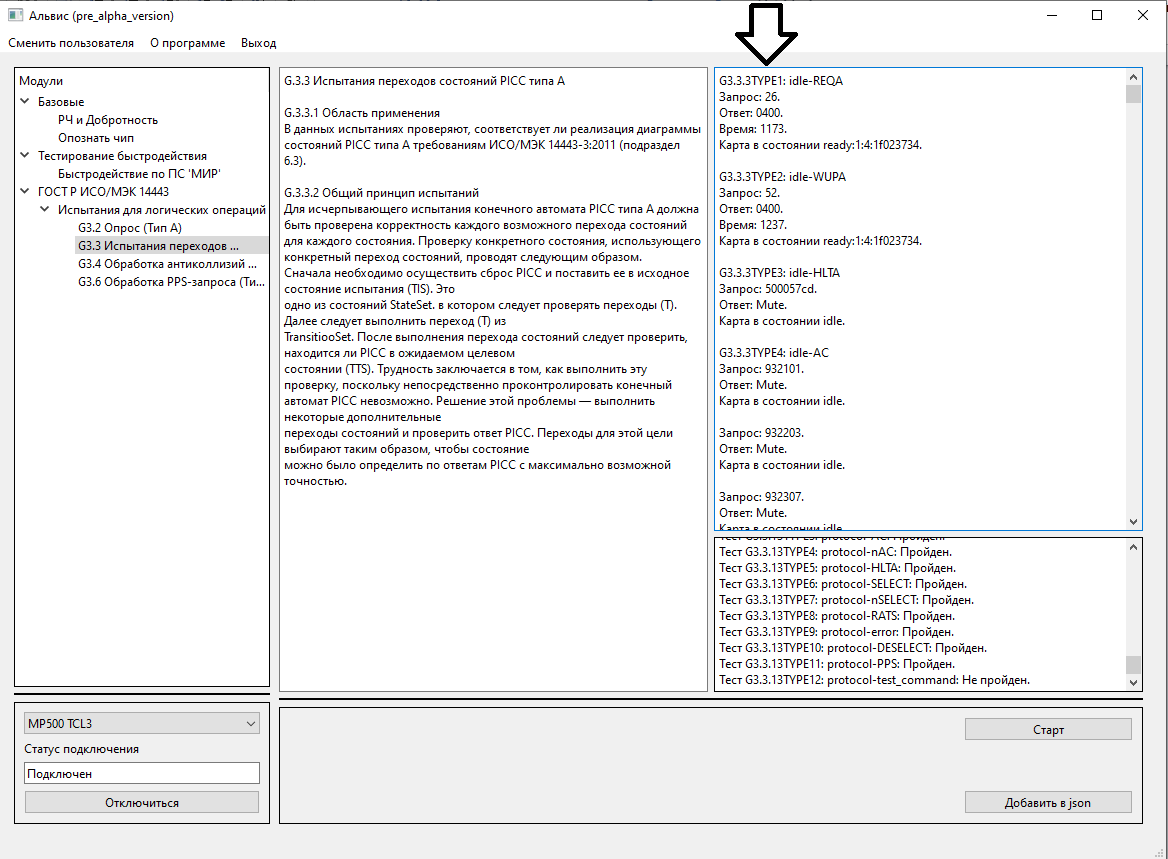


В данных испытаниях проверяют, соответствует ли реализация диаграммы состояний PICC типа А требованиям ИСО/МЭК 14443-3:2011. Для исчерпывающего испытания конечного автомата PICC типа А должна быть проверена корректность каждого возможного перехода состояний для каждого состояния.

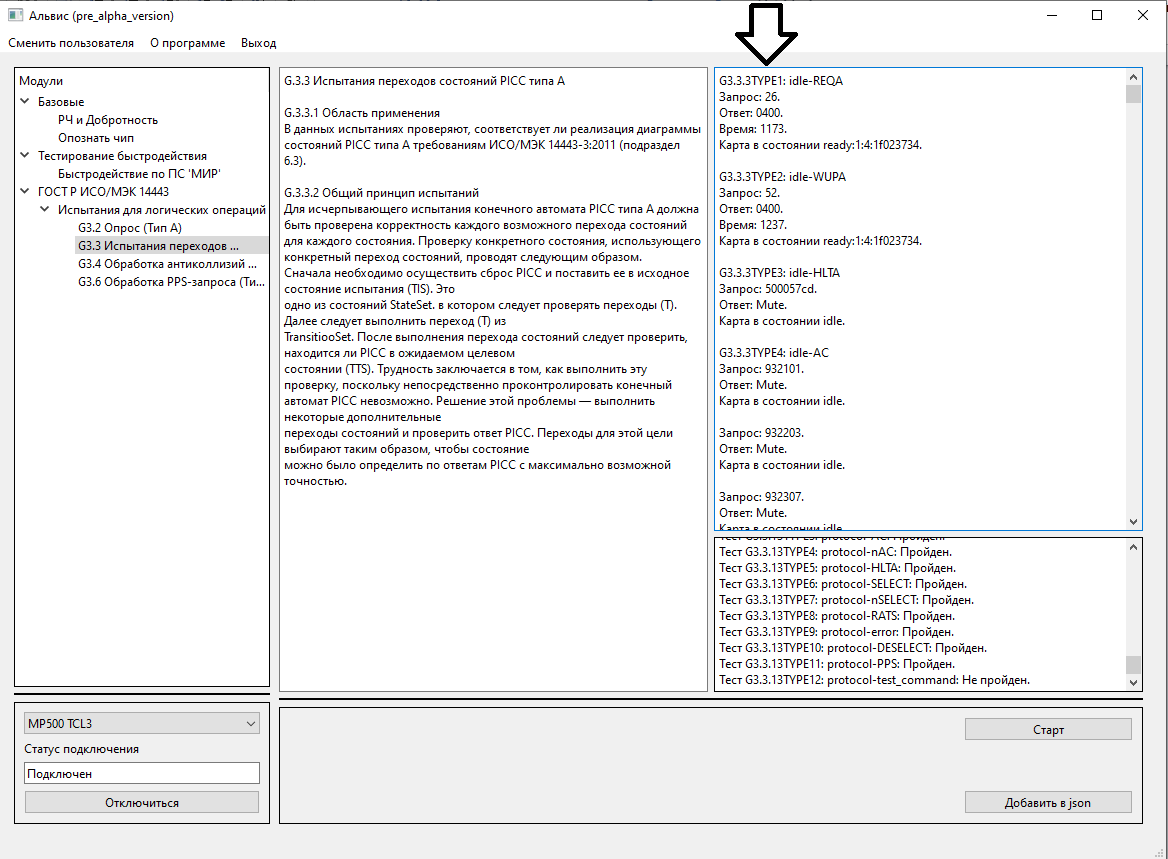
Для запуска проверки испытания нажимаем на кнопку «Старт».



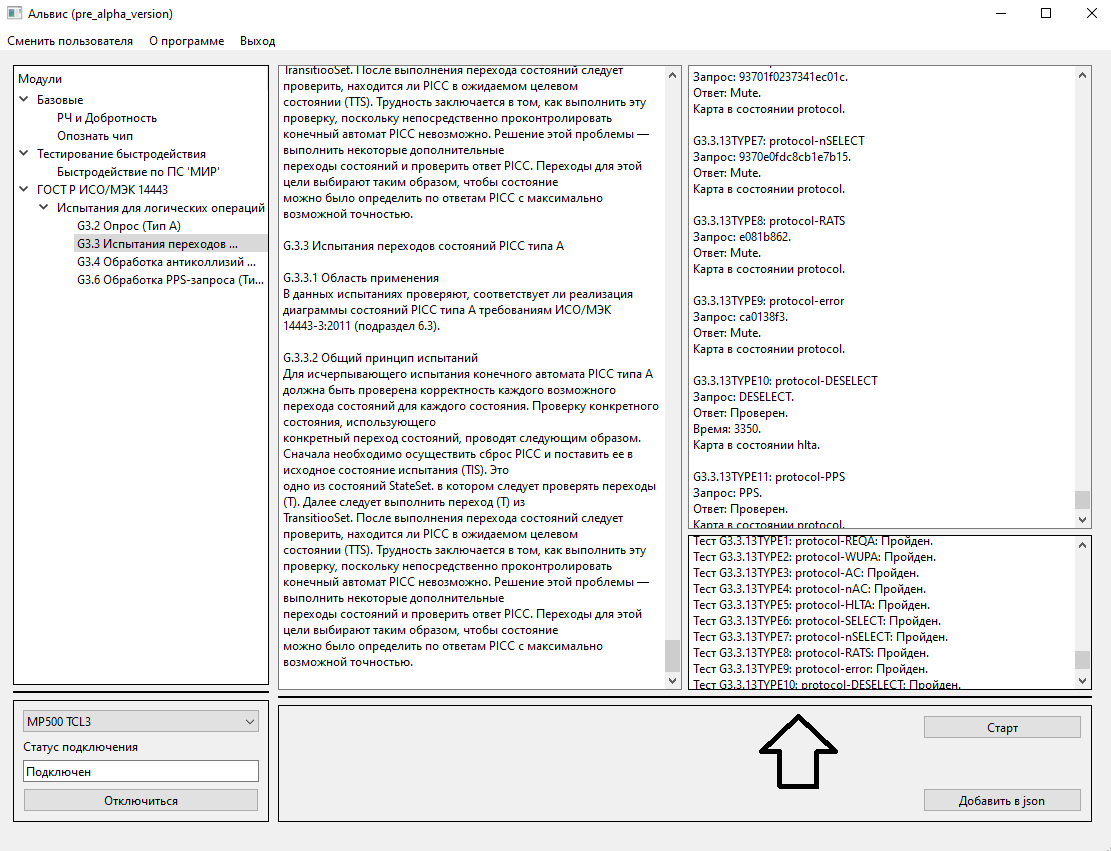
После нажатия кнопки, запускается процесс проверки карты.



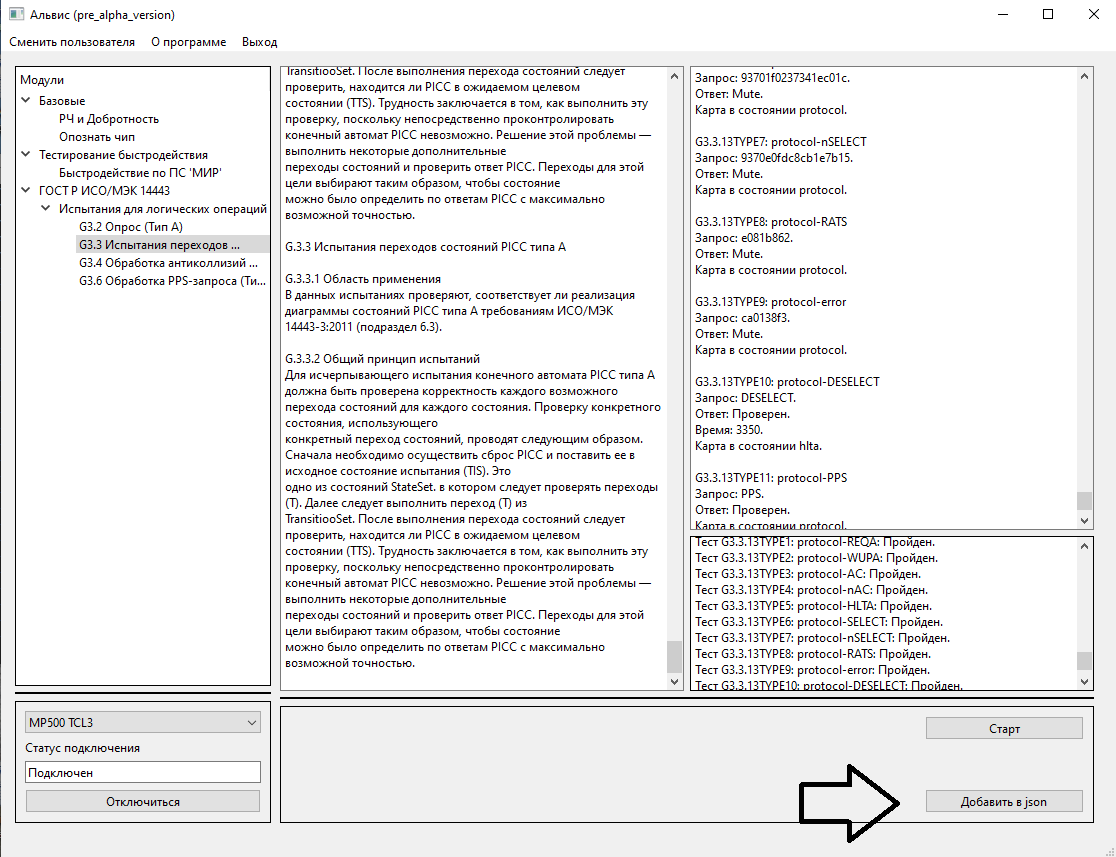
В верхней части окна отображается более подробная информация проверки по каждому состоянию.

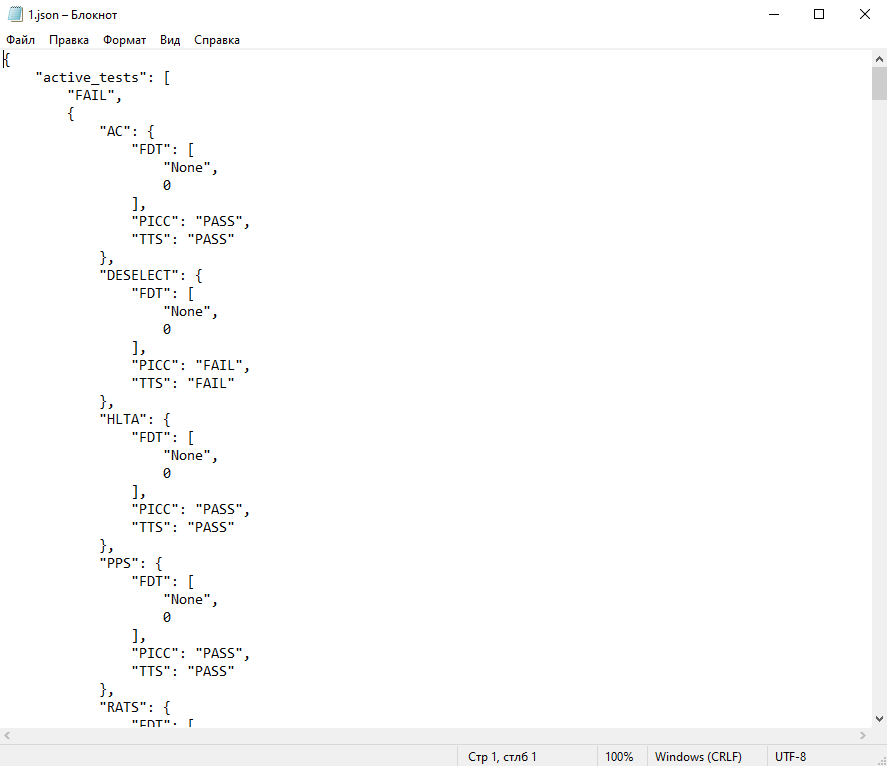


В нижней части окна отображается результаты проверки.



Отчёт проверки можно сохранить в текстовом файле (.json) с помощью кнопки «Добавить в json». Выбираем путь для сохранения и сохраняем файл.





1. Резонансная частота [↑](#footnote-ref-1)
2. Заготовка Карты с дуальным интерфейсом, эквивалентно DICC [↑](#footnote-ref-2)
3. Заготовка Карты с единственным Бесконтактным интерфейсом (БИ), эквивалентно PICC [↑](#footnote-ref-3)