УТВЕРЖДАЮ

Первый заместитель директора
республиканского унитарного
предприятия «Национальный центр
электронных услуг»

_____ С,А.Руднев

_____ 2021

КЛИЕНТСКАЯ ПРОГРАММА

Руководство оператора

Листов 43

Программное изделие «Клиентская программа» изготовлено РУП «Национальный центр электронных услуг»

Страна изготовитель: Республика Беларусь

2021

АННОТАЦИЯ

Настоящий документ предоставляет сведения для обеспечения процедуры общения оператора с графическим интерфейсом клиентской программы (КП) и содержит следующие разделы:

– назначение программы;
– условия выполнения программы;
– выполнение программы;
– входные и выходные данные;
– сообщения оператору;
– перечень сокращений.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. КП предназначена для организации взаимодействия между пользователем, его криптографическим токеном аутентификации (КТА) или средством электронной цифровой подписи (ЭЦП), комплексом программных средств прикладной системы BY.БФИД.10246-01 (далее – КПСИС) и Единой системой идентификации физических и юридических лиц BY.БФИД.10243-01 (далее – ЕС ИФЮЛ).

1.2. Основные функции, выполняемые КП:

- обеспечение взаимодействия между пользователем, его КТА или средством ЭЦП, КПСИС и сервером идентификации (СИ);
- установление защищенного соединения с TLS-сервером КПСИС;
- обеспечение взаимодействия со следующими программами криптопровайдера: NTCrypto БФИД.10186-01, Avest CSP BIGN/Avest CSP BEL РБ.ЮСКИ.12005-02 «AvPKISetup2.exe», Avest CSP Bel РБ.ЮСКИ.12004-02 34 01 «AvPKISetup2.exe»;
- обеспечение взаимодействия с любым веб-обозревателем для выработки и проверки ЭЦП с использованием средства ЭЦП;
- обеспечение взаимодействия с КТА для парольной аутентификации владельца КТА с помощью протокола формирования общего ключа BPACE;
- обеспечение взаимодействия с терминалами СИ и КПСИС, обеспечение взаимодействия КТА с терминалами СИ и КПСИС для установления протокола аутентификации BAUTH.

1.3. КП представляет собой локальный веб-сервис.

1.4. КП соответствует Техническому регламенту Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/BY).

1.5. Оператор должен изучить настоящий документ до начала работы с КП.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Минимальный состав технических и программных средств

2.1.1. КП функционирует на ПЭВМ со следующими характеристиками:

– объем свободного пространства – не менее 200 МБ;

– объем оперативной памяти – не менее 1 ГБ;

– тактовая частота процессора – не менее 2 ГГц.

2.1.2. КП функционирует на ПЭВМ со следующими программными средствами:

– ОС – Windows 8.1 x 32/64, Windows 10 x 32/64 [1];

– ОС – RedHat Linux Enterprise 7, Linux Enterprise Server 11, Linux Mint (17 и выше), CentOS (7.x.x и выше), Debian (8 и выше), Ubuntu (16 и выше), Xubuntu 16.04 LTS, Lubuntu 16.04 LTS, Kubuntu 17.04 (работа с устройствами AvBign и AvPass в операционных системах семейства Linux не поддерживается!);

– ОС – macOS 10.15 Catalina (работа с устройствами AvBign и AvPass в операционных системах семейства macOS не поддерживается!).

2.1.3. КП взаимодействует с идентификационной картой (КТА), соответствующей требованиям СТБ 34.101.79-2019, и считывателем.

2.1.4. КП взаимодействует с программой криптопровайдера (NTCrypto БФИД.10186-01 или Avest CSP BIGN/Avest CSP BEL РБ.ЮСКИ.12005-02 «AvPKISetup2.exe») и средством ЭЦП.

2.1.5. КП взаимодействует со средством ЭЦП (носителем ключевой информации, средством криптографической защиты информации), работающим по интерфейсу cryptoki согласно требованиям СТБ 34.101.21-2009. Перечень поддерживаемых сертифицированных носителей ключевой информации и средств криптографической защиты информации размещен по ссылке https://nces.by/pki/service/ (за исключением мобильной ЭЦП!).

2.1.6. Условия эксплуатации КП определяются условиями эксплуатации устройства, на котором предполагается его использовать, и требованиями эксплуатационных документов.

2.1.7. Запрещено эксплуатировать КП на ПЭВМ при невозможности задания политиками безопасности следующих требований к парольной аутентификации:

- пароли состоят не менее чем из 8 символов, обязательно содержат буквы в верхнем регистре, буквы в нижнем регистре, цифры;
- учетная запись пользователя блокируется после 30 попыток ввода неверного пароля.

2.2. Квалификация оператора

2.2.1. КП должен эксплуатироваться персоналом, имеющим навыки работы с ПЭВМ, функционирующей под управлением ОС семейств Windows, Linux, macOS.

[1] Применение нелицензионного ПО категорически запрещено.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Режимы работы программы

3.1.1. Работа с КП предусматривает два разделенных во времени процесса:
– установку (инсталляцию);
– штатную работу.
3.1.2. Корректность работы КП осуществляется внутренними средствами программы.

3.2. Установка программы

3.2.1. Установка программы на ПЭВМ, функционирующую под управлением ОС семейства Windows.

3.2.1.1. Скопировать на ПЭВМ файл «NTClientSoftware_версия системы_дата сборки.exe».

3.2.1.2. Запустить файл «NTClientSoftware_версия системы_дата сборки.exe». На экране появится окно мастера установки (рис. 1).

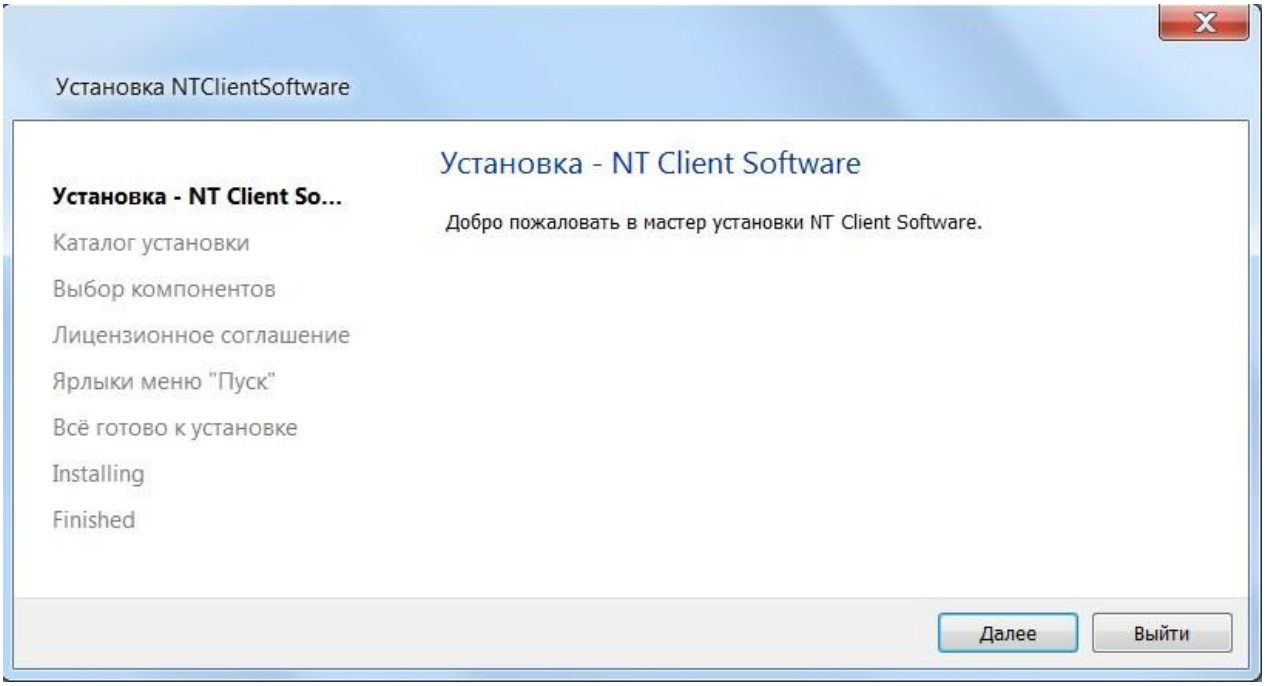

Рис. 1

3.2.1.3. Нажать кнопку «Далее» и выбрать каталог для установки программы (рис. 2), после чего следовать инструкциям мастера установки. Пример процесса установки приведен на рис. 3 – 6.

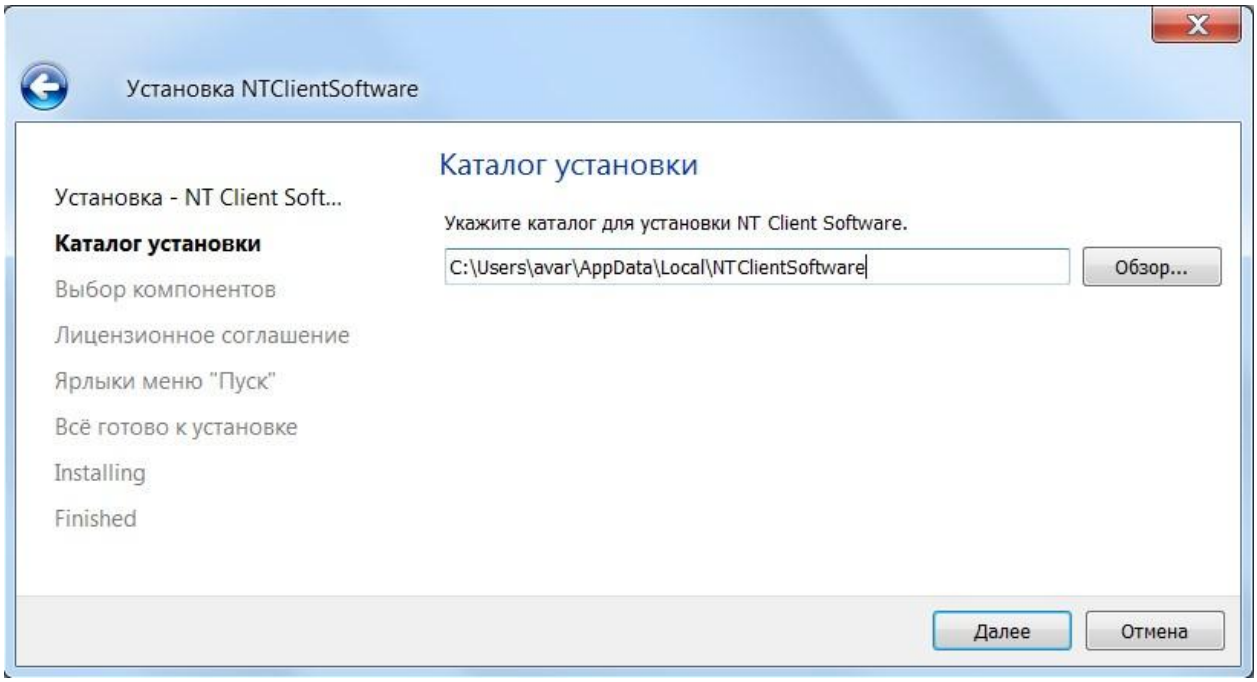
Установка NTClientSoftware
Каталог установки
Установка - NT Client Soft...
Каталог установки
Выбор компонентов
Лицензионное соглашение
Ярлыки меню "Пуск"
Всё готово к установке
Installing
Finished
Укажите каталог для установки NT Client Software.
C:\Users\avar\AppData\Local\NTClientSoftware
Обзор...
Далее
Отмена

Рис. 2

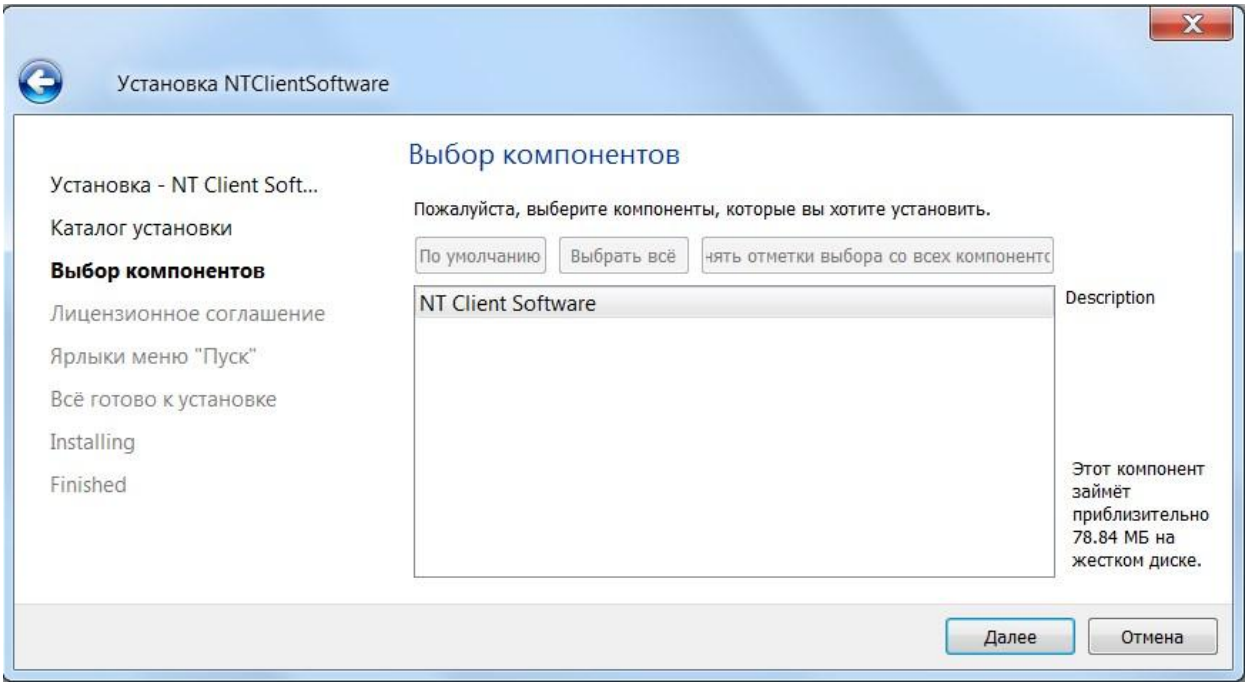
Установка NTClientSoftware
Выбор компонентов
Установка - NT Client Soft...
Каталог установки
Выбор компонентов
Лицензионное соглашение
Ярлыки меню "Пуск"
Всё готово к установке
Installing
Finished
Пожалуйста, выберите компоненты, которые вы хотите установить.
По умолчанию
Выбрать всё
нять отметки выбора со всех компонентс
NT Client Software
Description
Этот компонент займёт приблизительно 78.84 МБ на жестком диске.
Далее
Отмена

Рис. 3

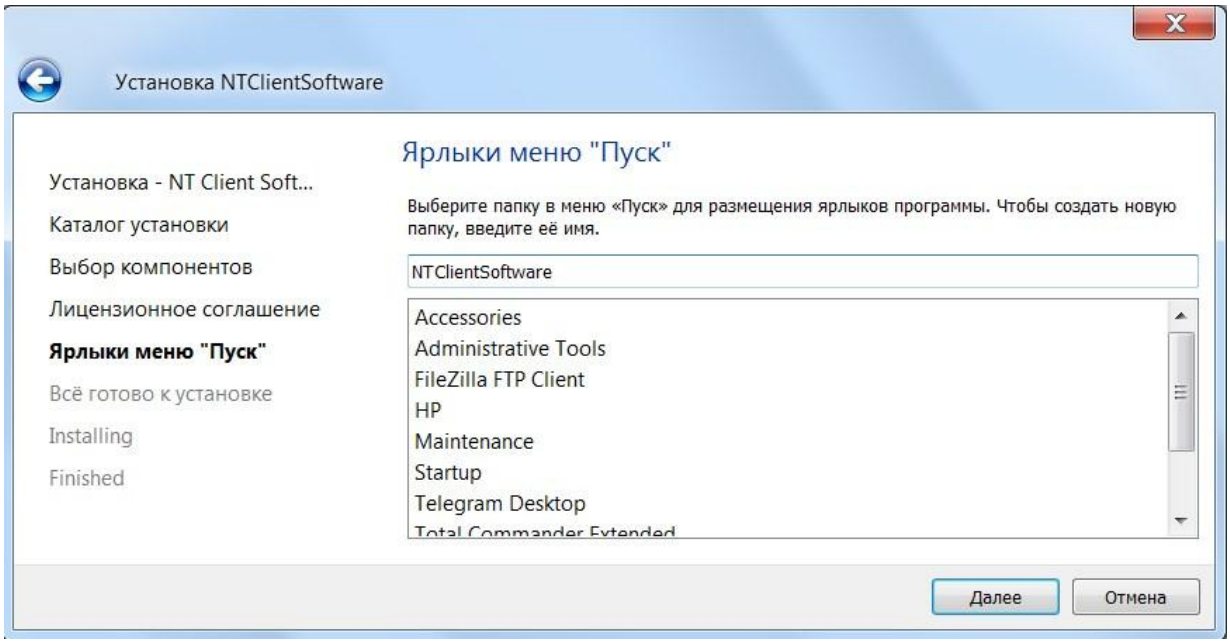
Установка NTClientSoftware
Установка - NT Client Soft...
Каталог установки
Выбор компонентов
Лицензионное соглашение
Ярлыки меню "Пуск"
Всё готово к установке
Installing
Finished
Ярлыки меню "Пуск"
Выберите папку в меню «Пуск» для размещения ярлыков программы. Чтобы создать новую папку, введите её имя.
NTClientSoftware
Accessories
Administrative Tools
FileZilla FTP Client
HP
Maintenance
Startup
Telegram Desktop
Далее
Отмена

Рис. 4

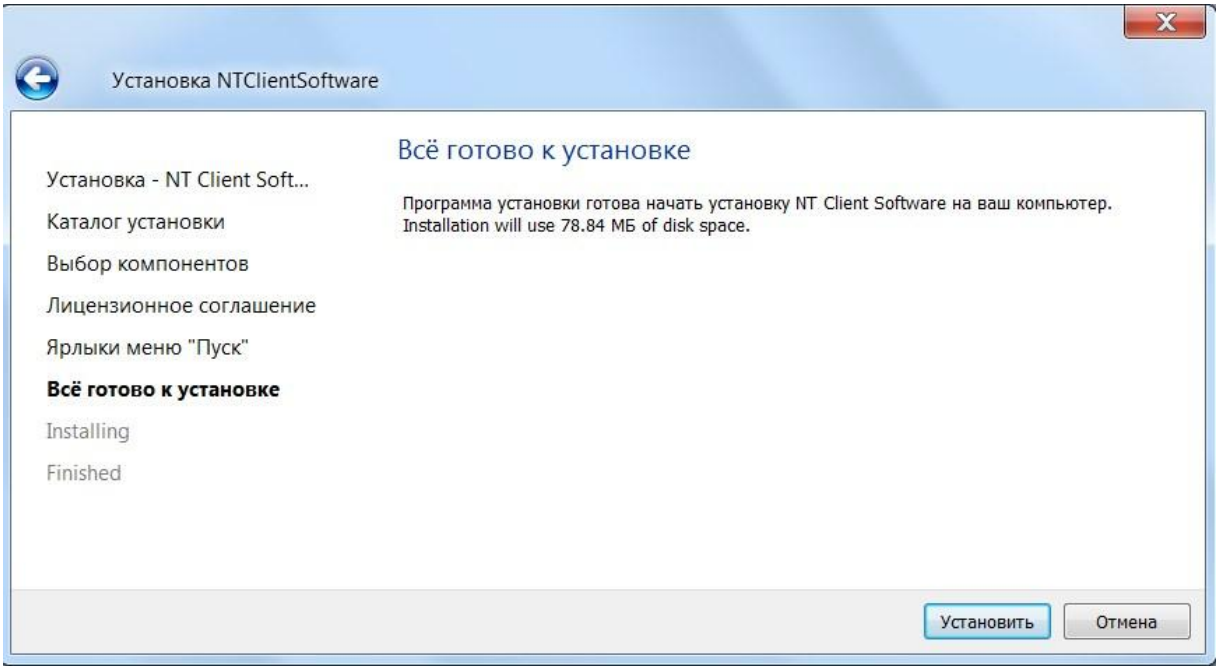
Установка NTClientSoftware
Установка - NT Client Soft...
Каталог установки
Выбор компонентов
Лицензионное соглашение
Ярлыки меню "Пуск"
Всё готово к установке
Installing
Finished
Всё готово к установке
Программа установки готова начать установку NT Client Software на ваш компьютер.
Installation will use 78.84 МБ of disk space.
Установить
Отмена

Рис. 5

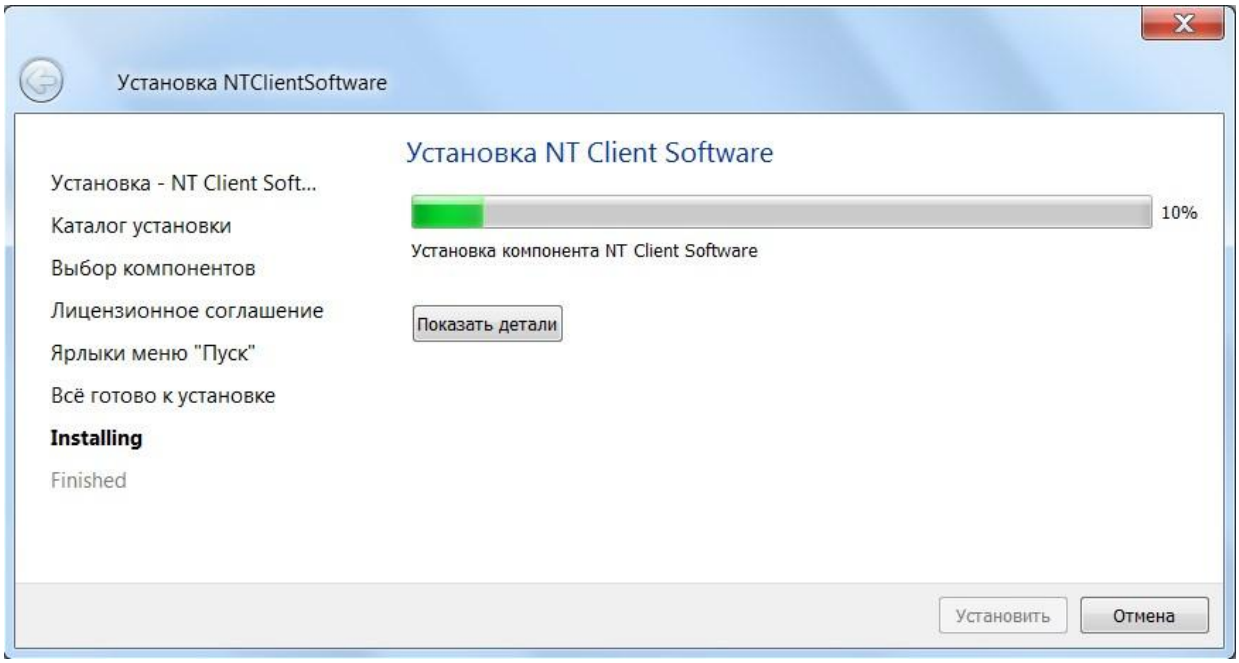

Рис. 6

3.2.1.4. В случае отсутствия сборки наборов библиотек и плагинов «Microsoft Visual C++ Redistributable» на экране появится предложение установить эту сборку (рис. 7).

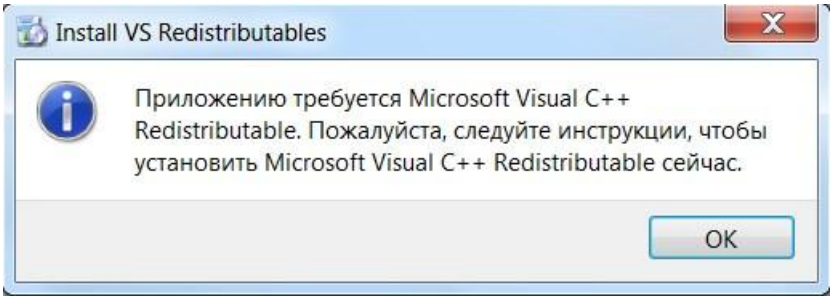

Рис. 7

3.2.1.5. Далее следовать инструкциям мастера установки (рис. 8).

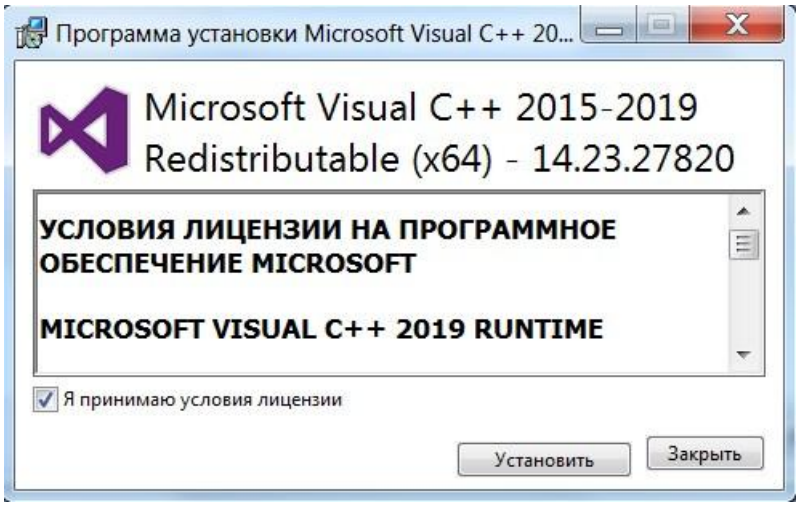

Рис. 8

3.2.1.6. При необходимости обновления будет предложено изменение установки (рис. 9). После чего нажать кнопку «Исправить» и следовать инструкциям мастера установки (рис. 10 – 12).

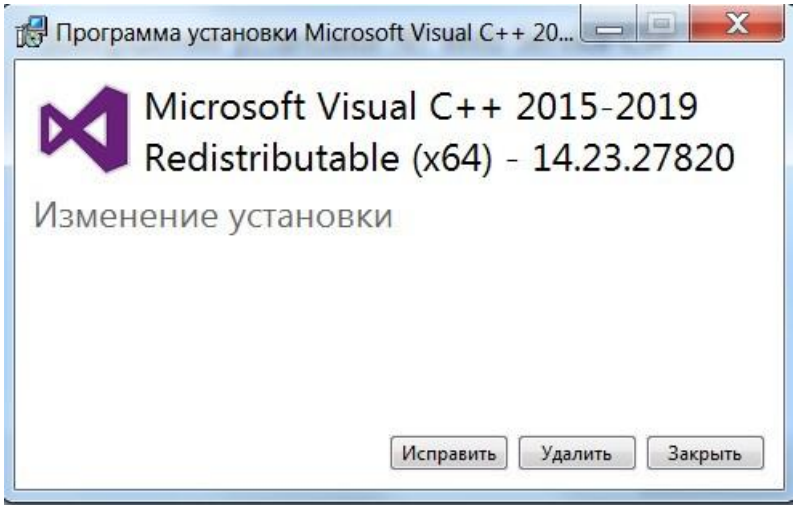

Рис. 9

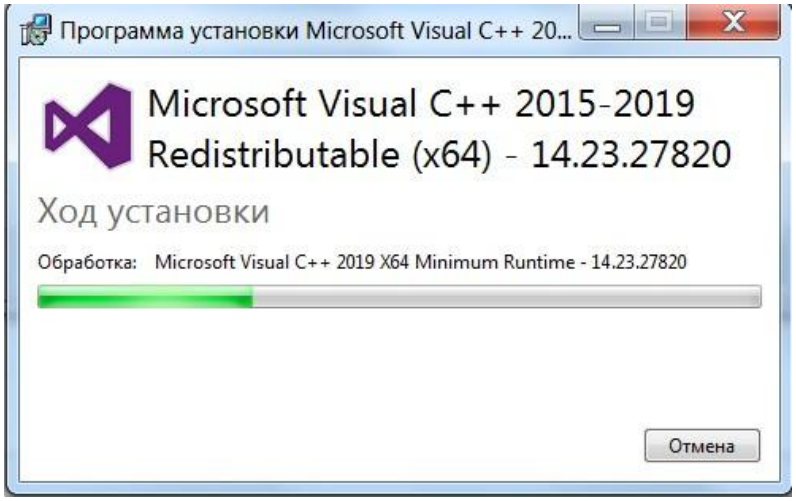

Рис. 10

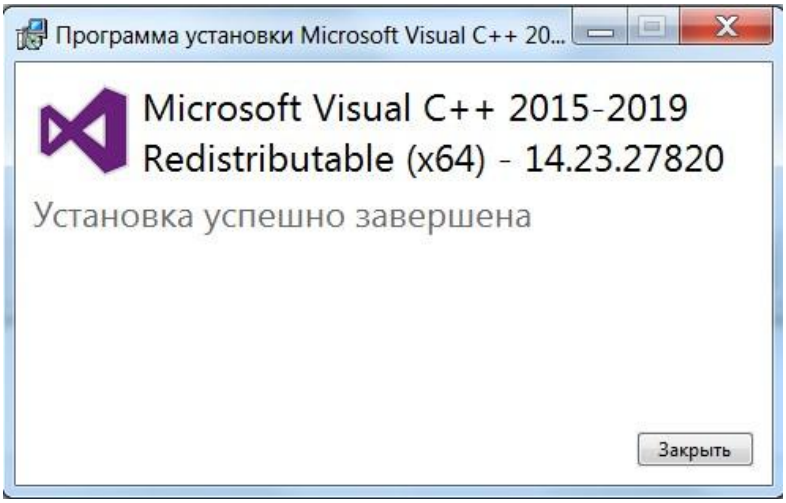

Рис. 11

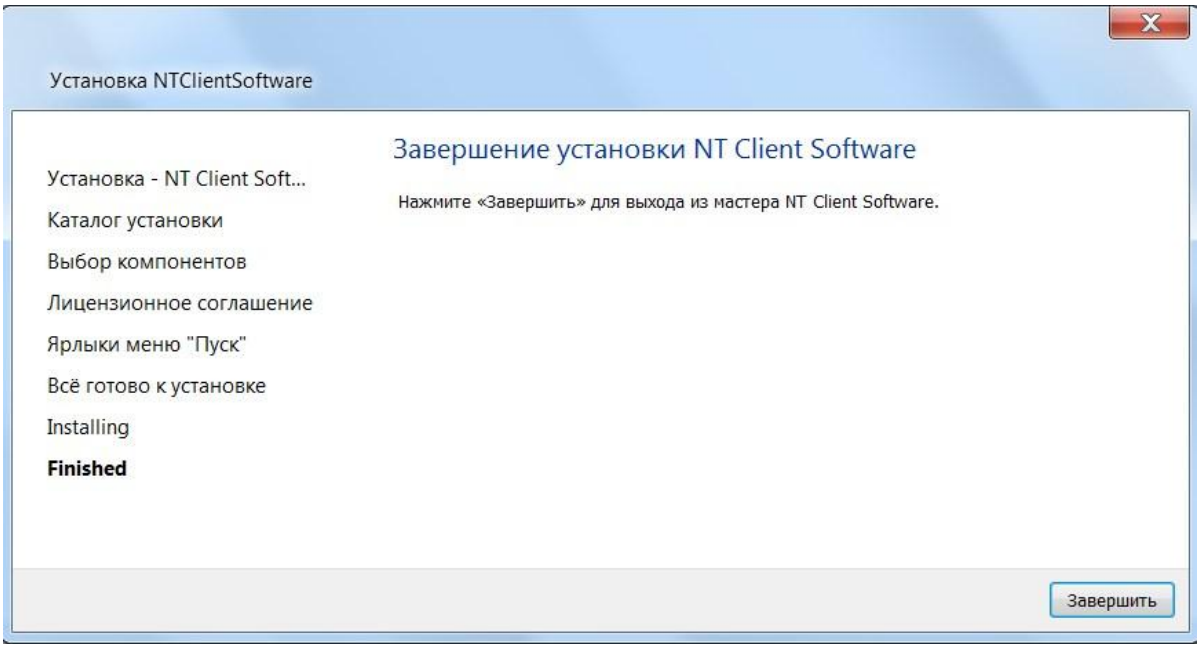

Рис. 12

3.2.2. Установка программы на ПЭВМ, функционирующей под управлением ОС семейства Linux, состоит из:

– копирования файла «NTClientSoftware_linux_дата сборки» на ПЭВМ;
– запуска файла «NTClientSoftware_linux_дата сборки» на ПЭВМ.

После запуска файла «NTClientSoftware_linux_дата сборки» на ПЭВМ, функционирующей под управлением ОС семейства Linux, процесс установки происходит аналогично описанной в 3.2.1.2, 3.2.1.3 последовательности действий.

При успешном завершении процесса установки отобразится окно, представленное на рис. 13.

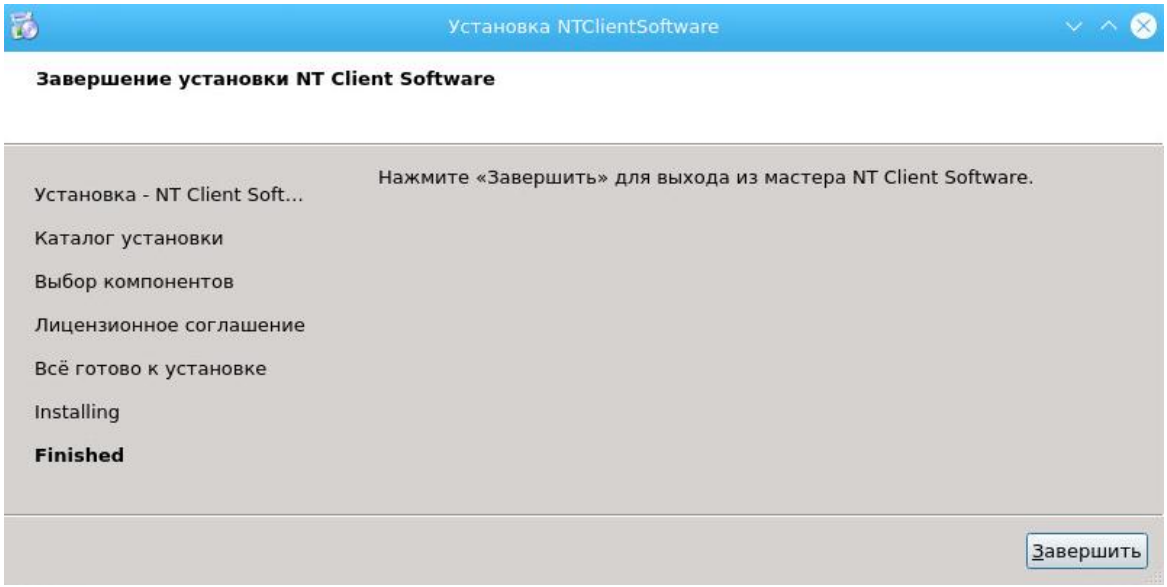

Рис. 13

3.2.3. Установка программы на ПЭВМ, функционирующей под управлением ОС семейства macOS, состоит из:

– копирования файла «NTClientSoftware_macos_дата сборки» на ПЭВМ;
– запуска файла «NTClientSoftware_macos_дата сборки» на ПЭВМ.

После запуска файла «NTClientSoftware_macos_дата сборки» на ПЭВМ, функционирующей под управлением ОС семейства macOS, процесс установки происходит аналогично описанной в 3.2.1.2, 3.2.1.3 последовательности действий.

При успешном завершении процесса установки отобразится окно, представленное на рис. 14.

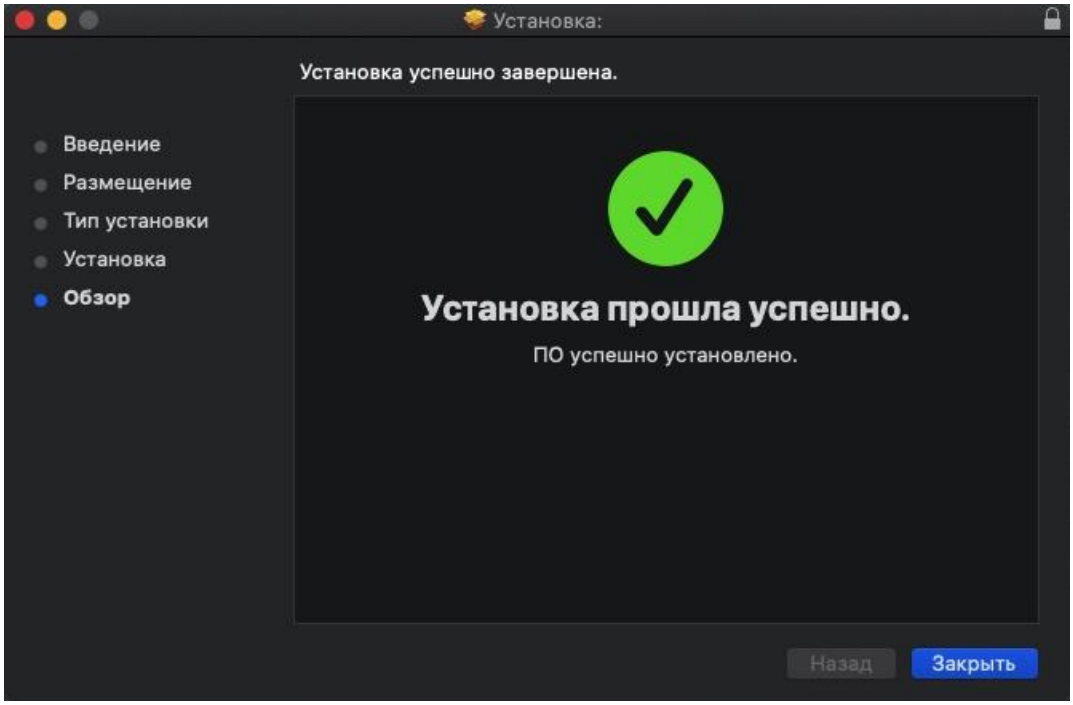

Рис. 14

3.3. Запуск программы

3.3.1. Для запуска программы на ПЭВМ, функционирующей под управлением ОС семейства Windows, необходимо дважды щелкнуть по ярлыку запуска программы на рабочем столе левой кнопкой «мыши». После автоматического запуска самотестирования (рис. 15) на экране появится окно с информационным сообщением об успешном запуске КП (рис. 16).

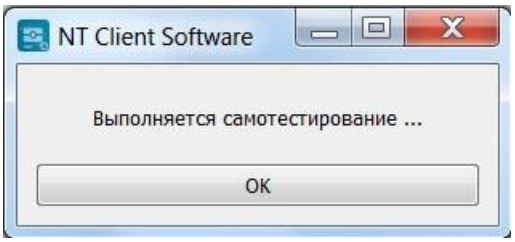

Рис. 15

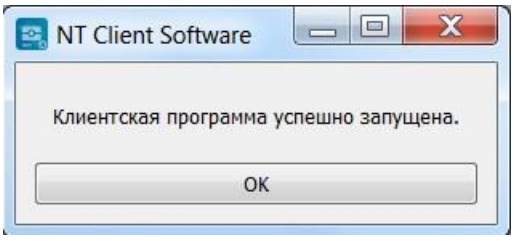

Рис. 16

3.3.2. При нажатии кнопки «ОК» появится информационное сообщение (рис. 17).

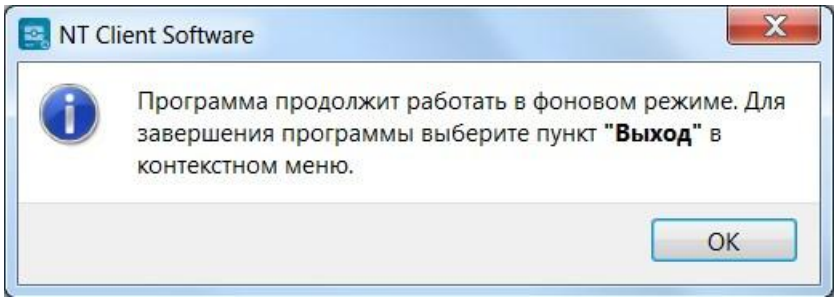

Рис. 17

3.3.3. При наведении курсора на значок программы в панели задач на экране появится сообщение, приведенное на рис. 18.

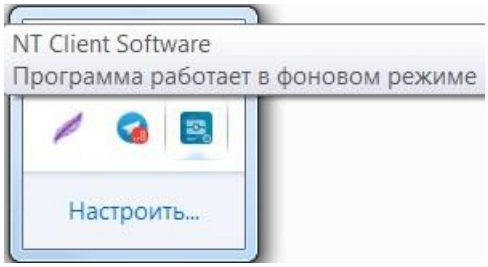

Рис. 18

3.3.4. Для запуска программы на ПЭВМ, функционирующей под управлением ОС семейства Linux, необходимо запустить скрипт «./NTClientSoftware.sh». После автоматического запуска самотестирования (рис. 19) на экране появится окно с информационным сообщением об успешном запуске КП (рис. 20).

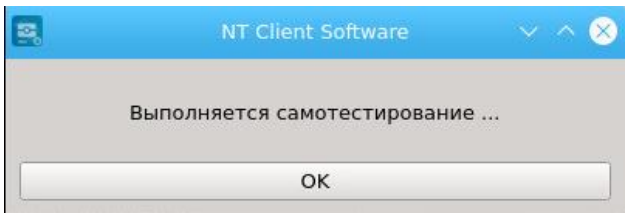

Рис. 19

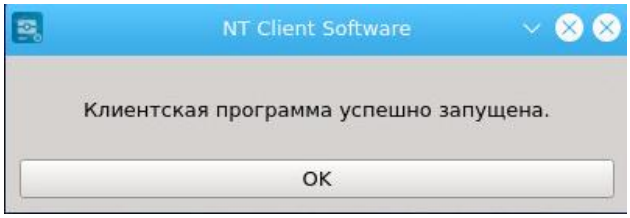

Рис. 20

3.3.5. При нажатии кнопки «OK» появится информационное сообщение (рис. 21).

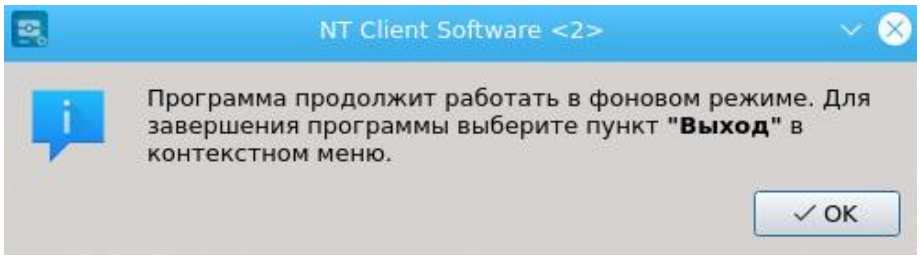

Рис. 21

3.3.6. Для запуска программы на ПЭВМ, функционирующей под управлением ОС семейства macOS, необходимо запустить файл «NTClientSoftware» (рис. 22), находящийся в каталоге «Программы» («Applications»). После автоматического запуска самотестирования

(рис. 23) на экране появится окно с информационным сообщением об успешном запуске КП (рис. 24).

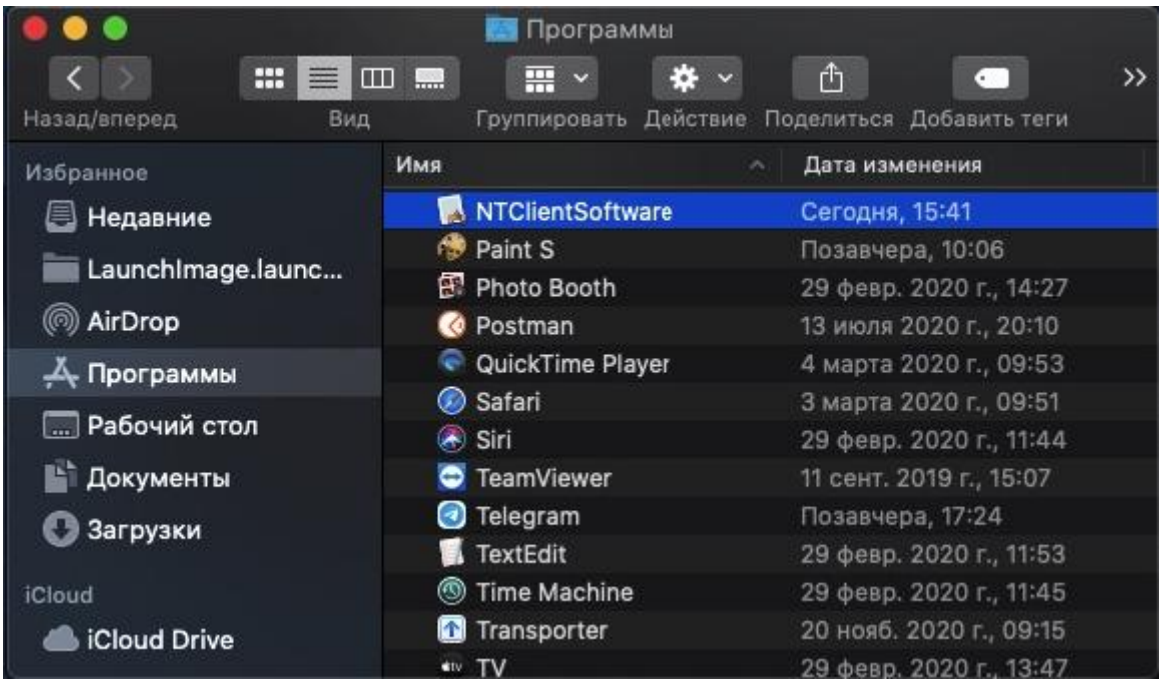

Рис. 22

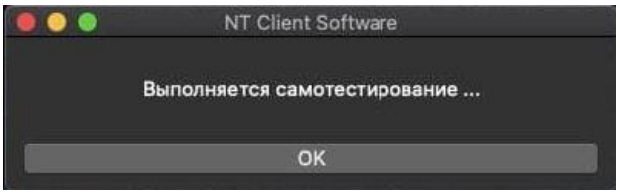

Рис. 23

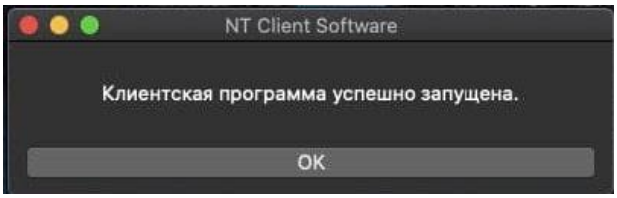

Рис. 24

3.4. Работа с программой

3.4.1. В меню программы доступны следующие действия: «Развернуть окно», «Информация», «Получить группы данных», «Разблокировать пароль PIN1», «Сменить пароль PIN1», «Разблокировать пароль PIN2», «Сменить пароль PIN2», «Автозапуск», «Самотестирование», «Настройки», «Выход» (рис. 25).

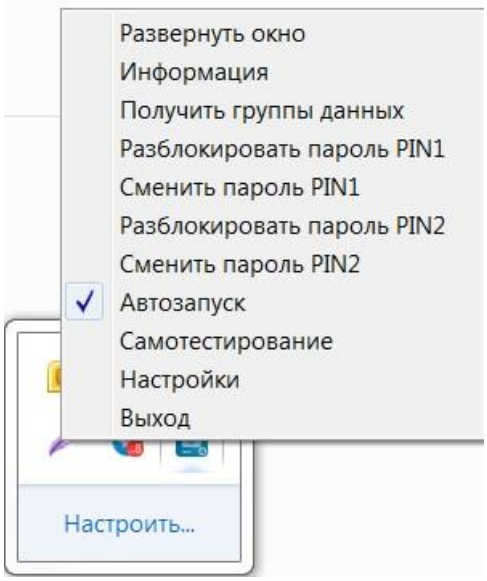

Рис. 25

Пароли: PIN1, PIN2 и PUK – выдаются вместе с идентификационной картой (КТА).

Примечания:

1. Для разблокировки PIN1 необходимо ввести PUK.

2. После десяти неудачных попыток ввода PUK происходит необратимая блокировка идентификационной карты (КТА).

3. При неверном вводе PIN2 в количестве трех раз необходимо ввести PUK.

4. После десяти неудачных попыток ввода PUK происходит блокировка идентификационной карты (КТА).

3.4.2. При выборе пункта «Развернуть окно» появится окно программы.

3.4.3. При выборе пункта «Информация» появится окно, отображающее номер текущей версии программы, дату и время последней сборки (рис. 26).

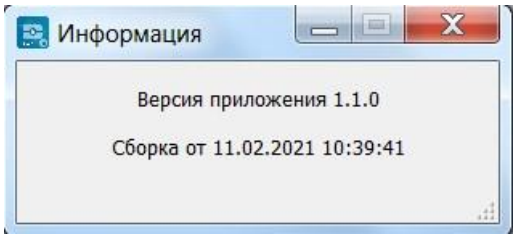

Рис. 26

3.4.4. При выборе пункта «Получить группы данных» необходимо ввести CAN (содержится непосредственно на id-карте) и нажать «ОК» (рис. 27, 28).

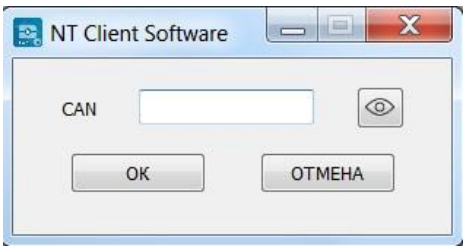

Рис. 27

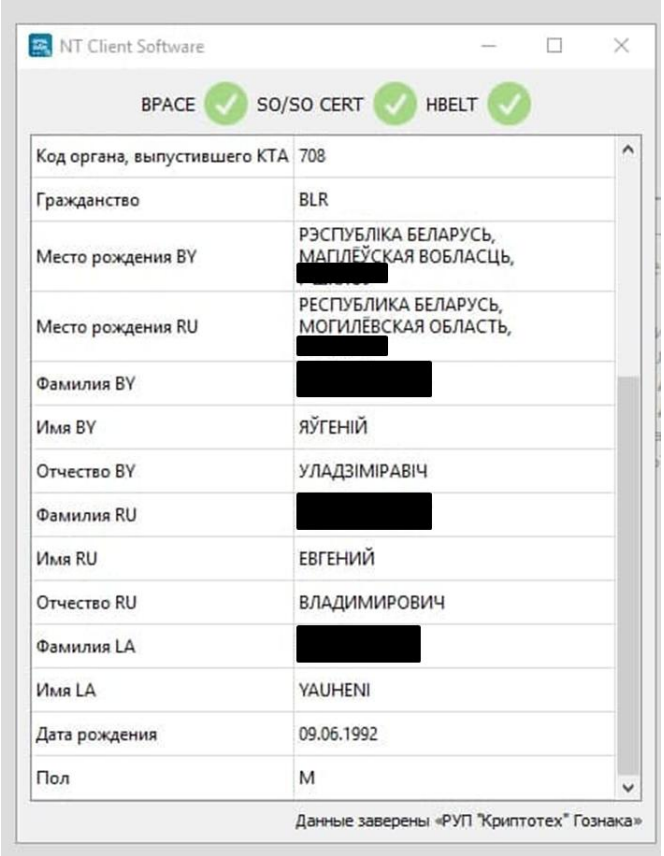

Рис. 28

3.4.5. При выборе пункта «Разблокировать пароль PIN1» необходимо ввести PUK (рис. 29). При вводе корректного PUK и нажатия кнопки «ОК» появится окно, представленное на рис. 30. При вводе некорректного PUK появится окно, представленное на рис. 31. Если некорректный PUK введен десять раз, произойдет блокировка идентификационной карты (КТА), в этом случае необходимо обратиться к поставщику идентификационной карты (КТА) с целью ее замены.

Рис. 29

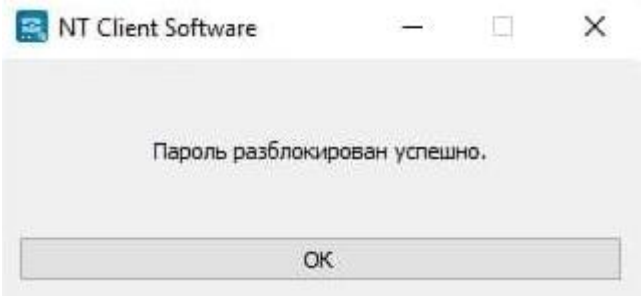

Рис. 30

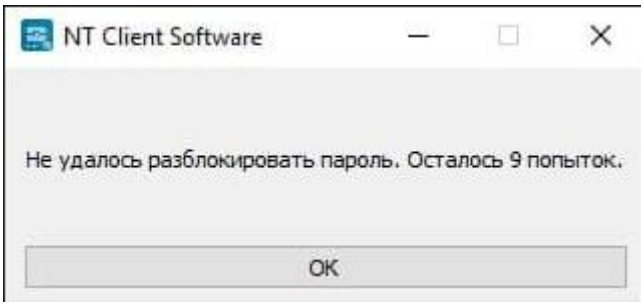

Рис. 31

Если оператор нажал кнопку «Разблокировать PIN1», когда PIN1 не заблокирован, то появится информационное окно, представленное на рис. 32.

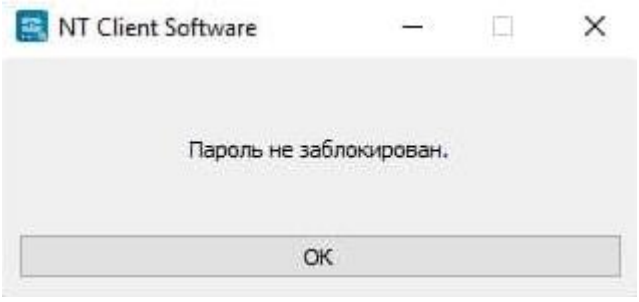

Рис. 32

3.4.6. При выборе пункта «Сменить пароль PIN1» необходимо ввести текущий PIN1 и заменить на новый PIN1 согласно РБ.ЮСКИ.19003-01 91 01 «Профиль КТА» (рис. 33).

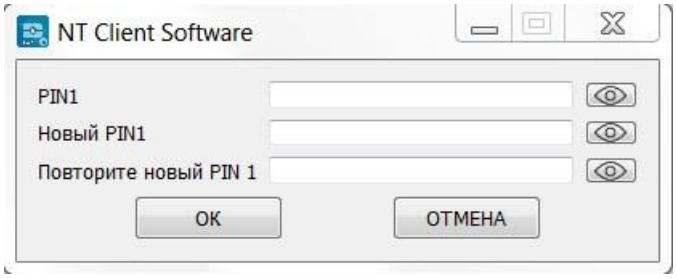

Рис. 33

3.4.7. При выборе пункта «Разблокировать пароль PIN2» появится окно (см. рис. 29). Также необходимо ввести PUK.

3.4.8. При выборе пункта «Сменить пароль PIN2» необходимо ввести PIN1, текущий PIN2 и заменить на новый PIN2 согласно РБ.ЮСКИ.19003-01 91 01 «Профиль КТА» (рис. 34).

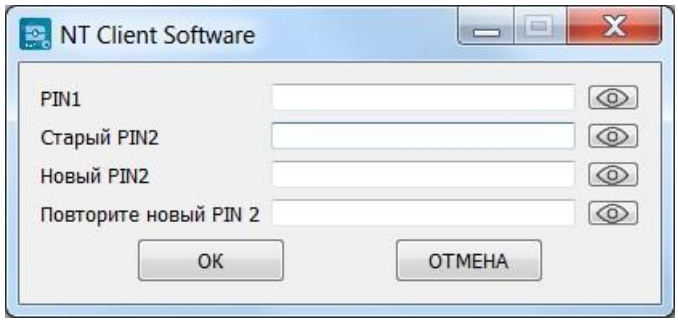

Рис. 34

3.4.9. При выборе пункта «Автозапуск» нажатие по нему левой кнопкой «мыши» приведет к отключению автозапуска, т.к. автозапуск включен по умолчанию.

3.4.10. При выборе пункта «Самотестирование» осуществляется тестирование целостности файлов, тестирование криптоалгоритмов и тестирование генератора случайных чисел (рис. 35-38).

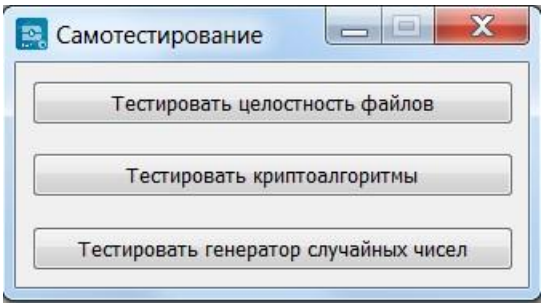

Рис. 35

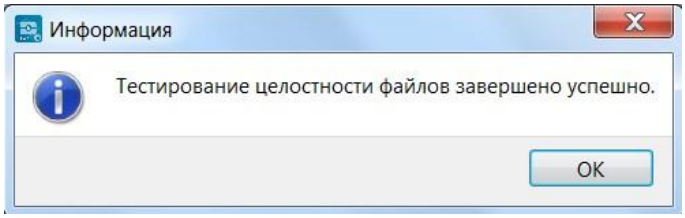

Рис. 36

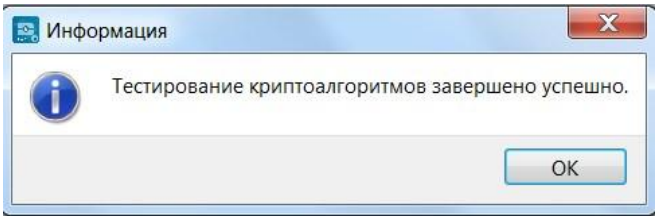

Рис. 37

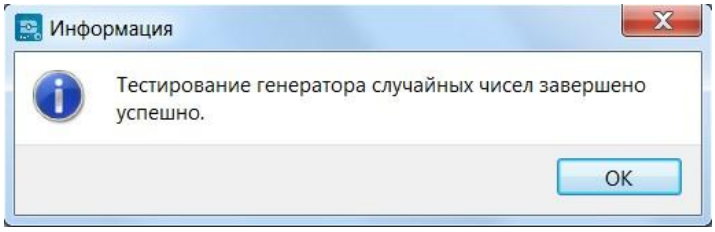

Рис. 38

Действия, описанные в 3.4.1 – 3.4.10, идентичны для КП на ПЭВМ, функционирующей под управлением ОС семейств Windows, Linux, macOS.

3.4.11. При выборе пункта «Настройки» необходимо убедиться, что идентификационная карта (КТА) подключена к ПЭВМ.

Окно пункта «Настройки» для КП на ПЭВМ, функционирующей под управлением ОС семейства Windows, имеет вид, представленный на рис. 39 – 41.

При отсутствии подключения окно пункта «Настройки» будет иметь вид, представленный на рис. 39. При наличии подключения окно пункта «Настройки» будет иметь вид, представленный на рис. 40, 41 (для AvBign нужно предварительно указать путь к библиотекам JSE-провайдера как на рис. 41). Для обновления информации обо всех подключенных идентификационных картах (КТА) необходимо выбрать пункт «ID-карта» и нажать значок обновления  .

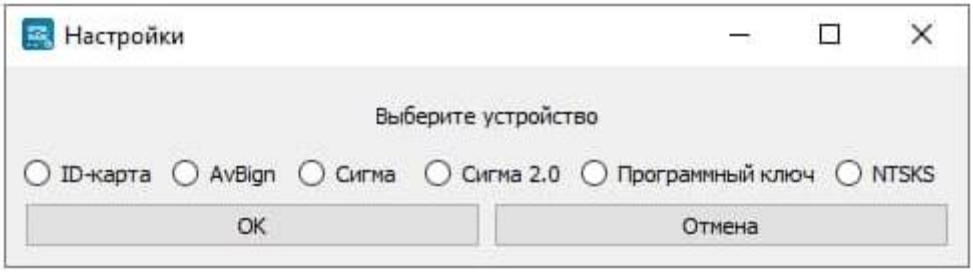

Рис. 39

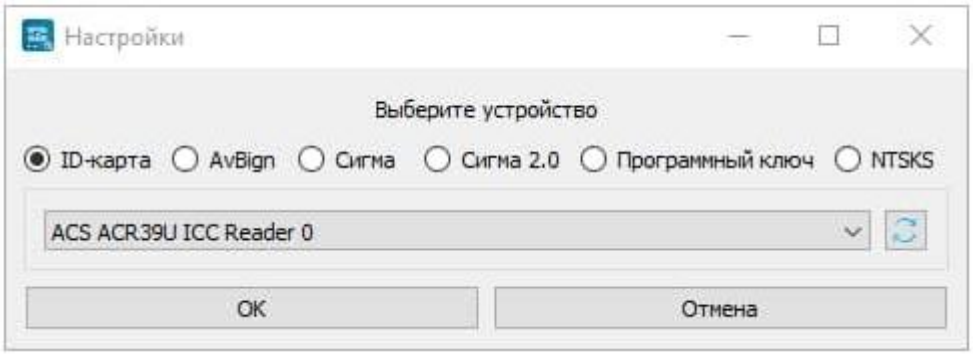

Рис. 40

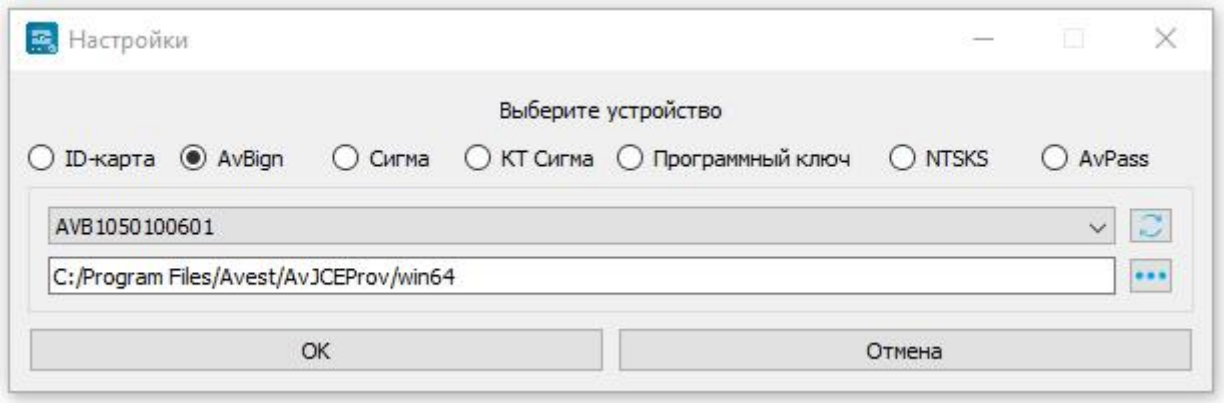

Рис. 41

Окно пункта «Настройки» для КП на ПЭВМ, функционирующей под управлением ОС семейств Linux, macOS, имеет вид, представленный на рис. 42.

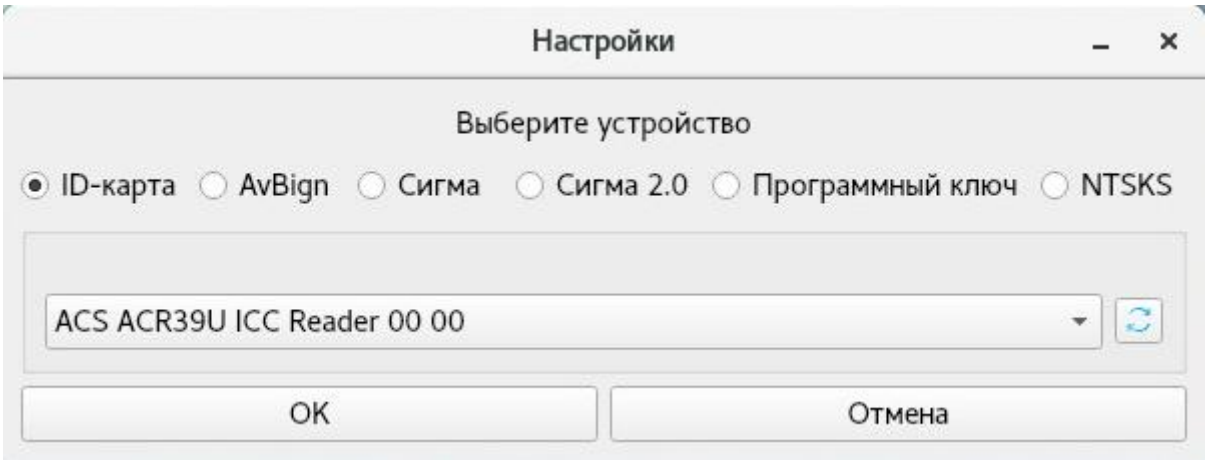

Рис. 42

3.4.12. Для прохождения процедуры аутентификации с помощью средства ЭЦП для КП на ПЭВМ, функционирующей под управлением ОС семейства Windows, необходимо нажать кнопку «Войти с помощью ID-карты или ключа ЭЦП»[2] в прикладной системе и подтвердить предоставление доступа к указанным на рис. 43 данным путем нажатия кнопки «ОК».

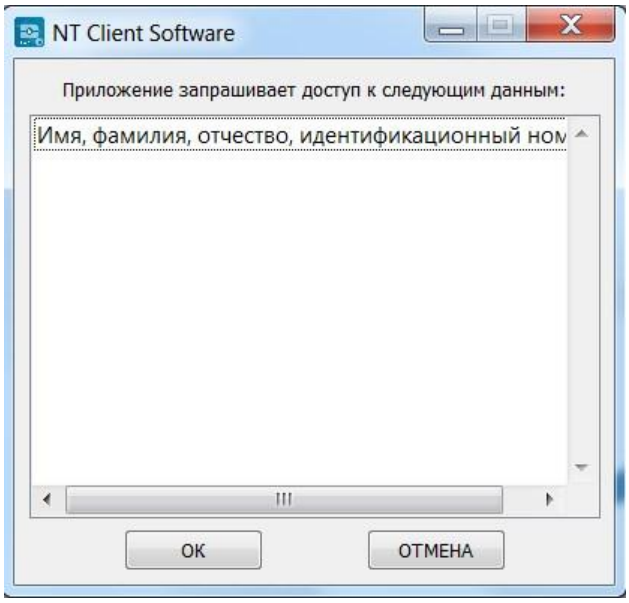

Рис. 43

В открывшемся окне нажать кнопку «Электронная цифровая подпись» (рис. 44), после чего выбрать сертификат открытого ключа (СОК) и ввести пароль средства ЭЦП (рис. 45, рис. 46).

При необходимости, для выбора иного сертификата (кроме отображаемого), необходимо нажать в окне выбора кнопку «Больше вариантов» (подробнее рис. 45).

[2] Название кнопки может меняться в зависимости от прикладной системы

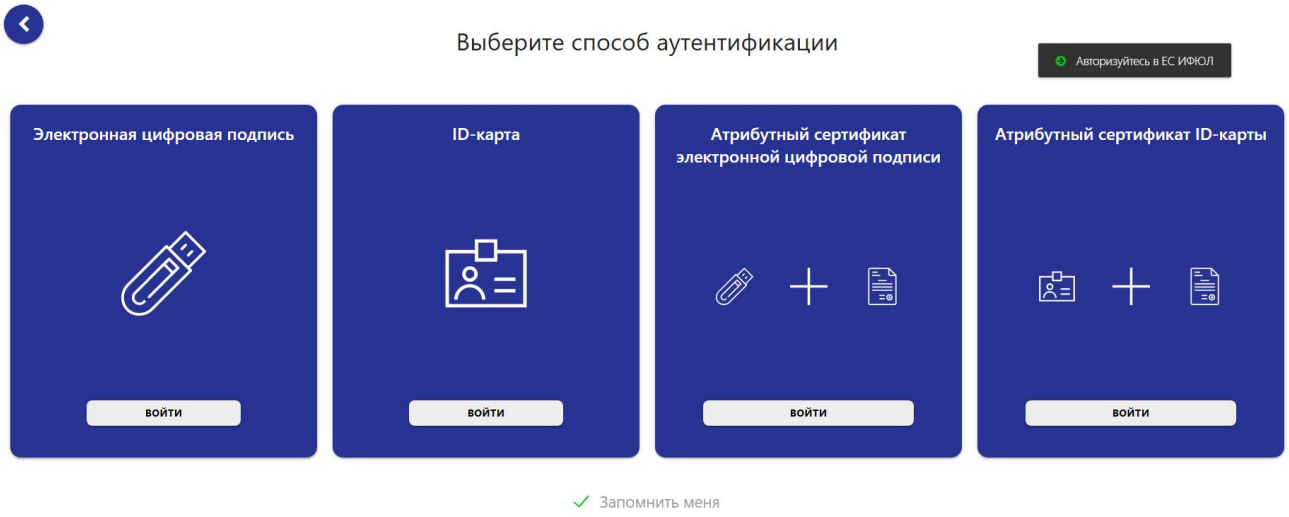

Рис. 44

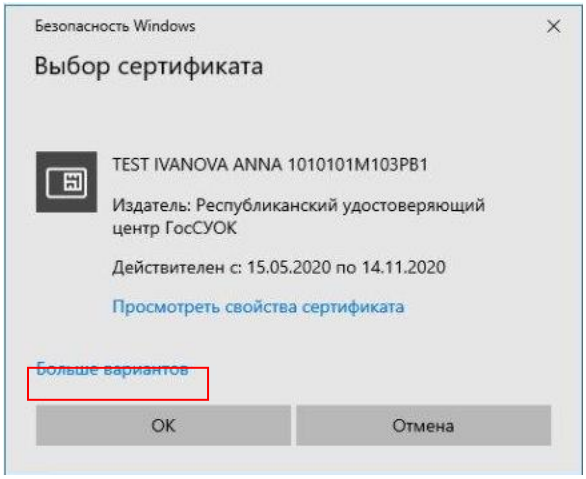

Рис. 45

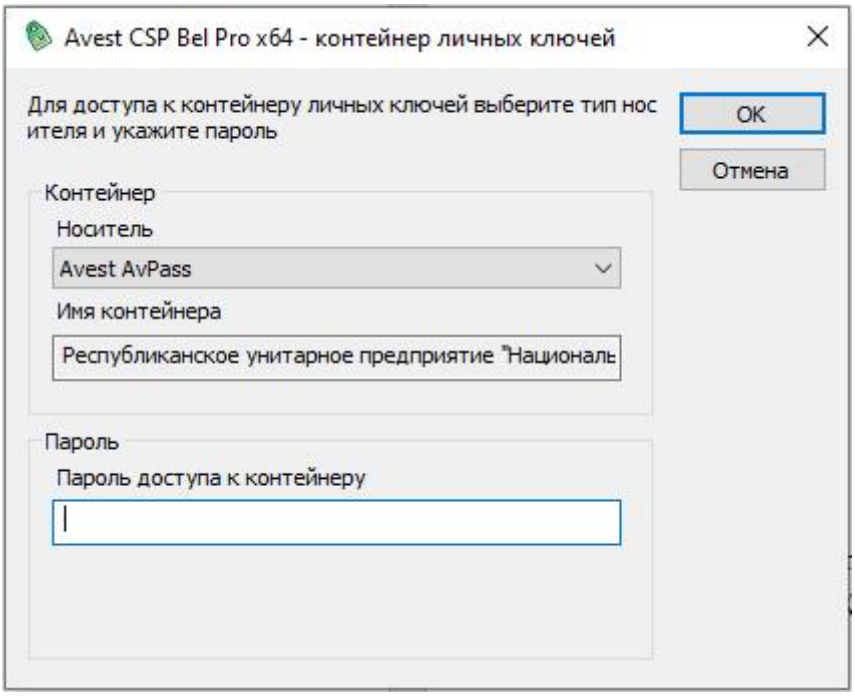

Рис. 46

3.4.13. Для прохождения процедуры аутентификации с помощью идентификационной карты (КТА) для КП на ПЭВМ, функционирующей под управлением ОС семейства Windows, необходимо нажать кнопку «Войти с помощью ID-карты или ключа ЭЦП»[3] в прикладной системе и подтвердить предоставление доступа к указанным на рис. 43 данным путем нажатия кнопки «ОК».

В открывшемся окне нажать кнопку «ID-карта» (см. рис. 44), после чего необходимо ввести PIN1 и нажать «ОК» (рис. 49).

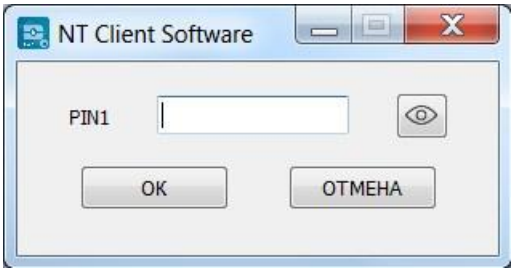

Рис. 49

При вводе корректного PIN1 произойдет успешное завершение авторизации (рис. 50).

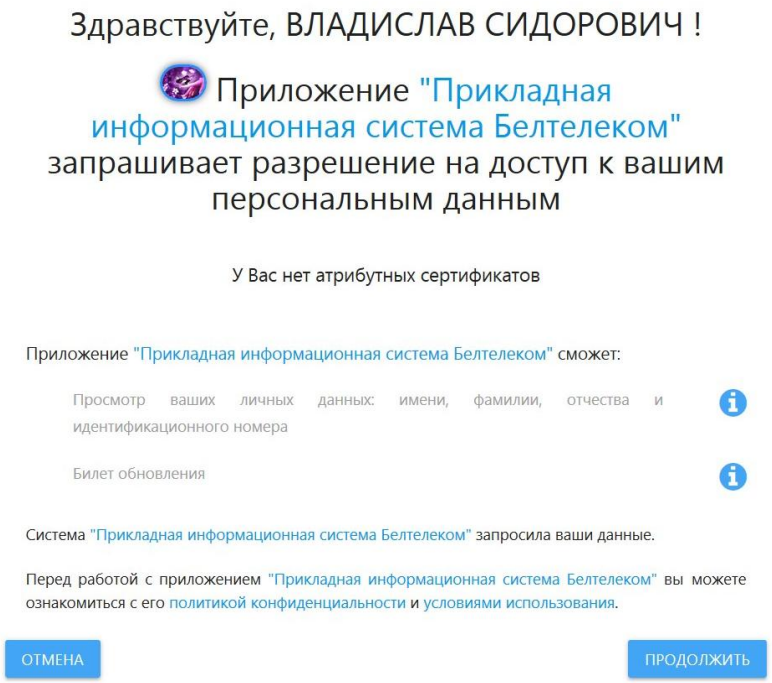

Рис. 50

3.4.14. Для прохождения процедуры аутентификации с помощью идентификационной карты (КТА) для КП на ПЭВМ, функционирующей под управлением ОС семейств Linux, macOS, необходимо нажать кнопку «Войти с помощью ID-карты или ключа ЭЦП»[3] в прикладной системе и подтвердить предоставление доступа к указанным на рис. 43 данным путем нажатия кнопки «ОК».

В открывшемся окне нажать кнопку «Авторизация через ID-карту» (см. рис. 44), после чего выбрать СОК и ввести пароль средства ЭЦП (см. рис. 47, рис. 48).

[3] Название кнопки может меняться в зависимости от прикладной системы

3.5. Завершение работы программы

3.5.1. Для завершения работы программы необходимо щелкнуть правой кнопкой «мыши» по значку программы в панели задач и выбрать в открывшемся меню пункт «Выход» (рис. 51). После чего значок программы исчезнет из панели задач (рис. 52).

Важно! Указанные в 3.5.1 действия обязательны к выполнению для завершения работы программы на ПЭВМ, функционирующей под управлением ОС семейства Linux.

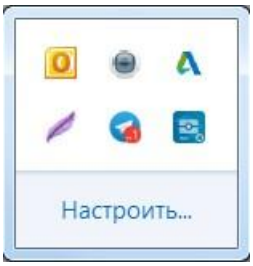

Рис. 51

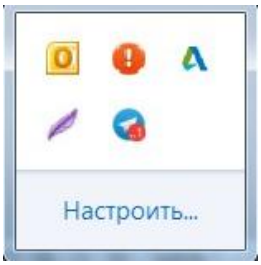

Рис. 52

3.6. Порядок действий в случае сбоев, отказа ПЭВМ, при уничтожении или модификации программы

3.6.1. При аппаратных сбоях ПЭВМ необходимо выполнить следующие действия:

– перегрузить ПЭВМ;

– перезапустить КП;

– переподключить считыватель КТА.

3.6.2. При аппаратном отказе ПЭВМ необходимо выполнить следующие действия:

– заменить ПЭВМ;

– установить минимальный состав программных средств, необходимых для функционирования КП;

– установить КП;

– подключить считыватель КТА.

3.6.3. Порядок действий при уничтожении или модификации программы: установить программу на ПЭВМ из инсталляционного пакета или самораспаковывающегося архива.

3.7 Добавление второй цепочки сертификатов

3.7.1. Скачать скрипт для добавления второй цепочки корневых сертификатов из облачного хранилища НЦЭУ (https://store.nces.by/) – downloadCA.ps1 :

3.7.1.1. В вашем кабинете Облачного хранилища перейти в каталог KP_ESIFUL, выделить файл downloadCA.ps1:

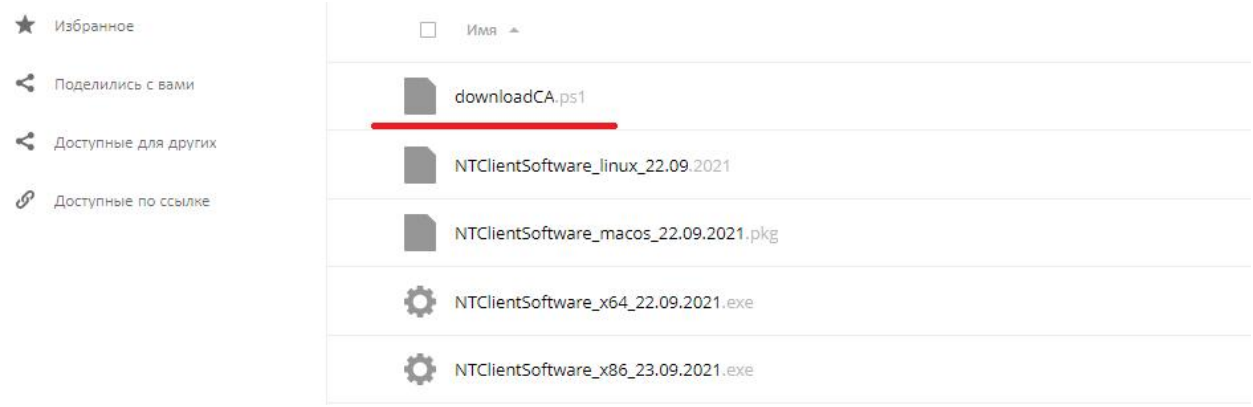

Рис. 53

3.7.1.2. Нажать кнопку «Скачать» :

Рис. 54

3.7.2. Разместить скачанный в файл в корневом каталоге КП (по умолчанию C:\NTClientSoftware)

3.7.3. Запустить выполнения скрипта, для чего: Кликнуть правой кнопкой по скрипту – «Выполнить с помощью PowerShell» (см. рис 3)

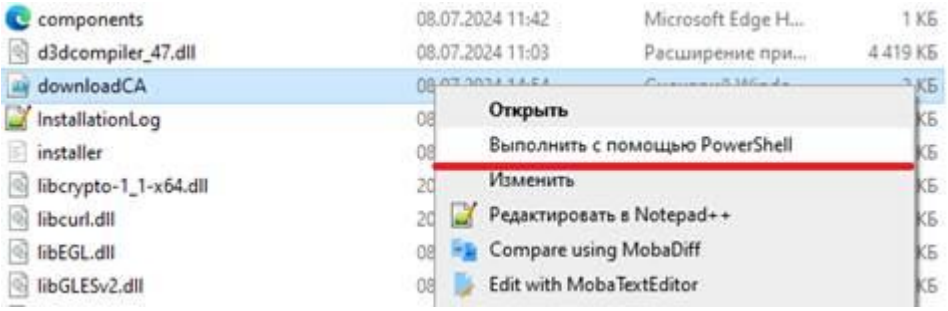

Рис. 55

Примечание: скрипт скачает вторую цепочку корневых сертификатов (kuc2.cer, ruc3.cer , cas_ruc3.cer) а также COCы для них и поместит в каталоги ./CA и ./CRL .

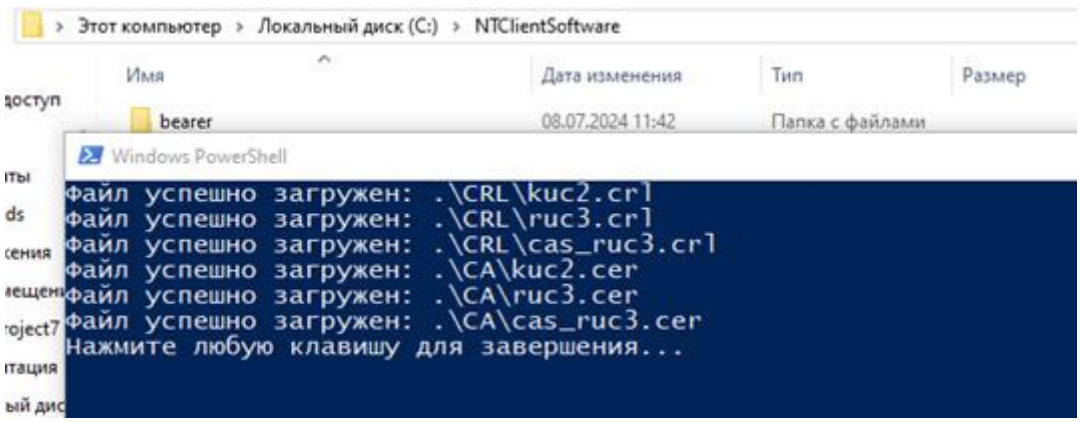

Рис. 56

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Выработка ЭЦП, сохранение Scope_ПС, выделение и сохранение базовой ЭЦП (URL): http://127.0.0.1:8084/select_auth.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате BASE64>»
}
```

Выходные данные:

```
{
    «step 0»: «<проверка ЭЦП, сохранение Scope_Пс, выделение и сохранение базовой ЭЦП прошло успешно>»
}
```

4.2. Выработка ЭЦП через средство ЭЦП (URL): http://127.0.0.1:8084/sauth.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате BASE64>»
}
```

Выходные данные:

```
{
    «cms»: «<данные для ЭЦП в формате Base64>»
}
```

4.3. Взаимодействие с идентификационной картой (КТА) (URL): http://127.0.0.1:8084/bauth.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате BASE64>»,
    «init»: «<параметр инициализации>»,
    «cmd»: «<команда на идентификационную карту (КТА)>»,
    «cert»: «<сертификат терминала>»

}
```

Выходные данные:

```
{
    «So»: «<объект безопасности>»,
    «SO Cert»: «<сертификат объекта безопасности>»,
    «rdf»: «<ответ от идентификационной карты (КТА)>»,
    «penult»: «<индикатор последнего шага на КП>»
}
```

4.4. Выработка ЭЦП и создание CMS-структуры (URL): http://127.0.0.1:8084/sign.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате BASE64>»,
    «isDetached»: «<параметр, который определяет, будет ли ЭЦП отсоединенная>»
}
```

Выходные данные:

```
{
    «cms»: «<значение CMS в формате BASE64>»
}
```

4.5. Выработка ЭЦП через идентификационную карту (КТА) (URL): http://127.0.0.1:8084/sign_kta.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате BASE64>»
}
```

Выходные данные:

```
{
    «cok»: «<значение СОК>»,
    «data»: «<подписываемые данные в формате Base64>»,
    «sig»: «<значение ЭЦП>»,
    «error»: «<код ошибки>»
}
```

4.6. Выработка ЭЦП через идентификационную карту (КТА) и создание CMS-структуры с добавлением атрибутного сертификата (URL): http://127.0.0.1:8084/sign_kta_cms_ac.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате BASE64>»,
    «AC»: «<значение атрибутного сертификата>»,
    «isDetached»: «<параметр, который определяет, будет ли ЭЦП отсоединенная>»
}
```

Выходные данные:

```
{
    «sig»: «<значение ЭЦП>»,
    «error»: «<код ошибки>»
}
```

4.7. Проверка базовой ЭЦП (URL): http://127.0.0.1:8084/verify_base.

Входные данные:

```
{
    «cok»: «<значение СОК>»,
    «data»: «<подписываемые данные в формате Base64>»,
    «sig»: «<значение ЭЦП>»
}
```

Выходные данные:

```
{
    «verify»: «<значение, равное OK, если проверка успешна>»,
    «error»: «<код ошибки, если проверка неуспешна>»
}
```

4.8. Проверка CMS-структуры (URL): http://127.0.0.1:8084/verify_cms.

Входные данные:

```
{
    «cms»: «<значение ЭЦП в формате Base64>»,
    «data»: «<подписываемые данные в формате Base64>»
}
```

Выходные данные:

```
{
    «verify»: «<значение, равное OK, если проверка успешна>»,
    «error»: «<код ошибки, если проверка неуспешна>»
}
```

4.9. Выработка ЭЦП через терминал (URL): http://127.0.0.1:8084/auth_sign.

Входные данные:

```
{
    «init»: «<параметр инициализации>»,
    «data»: «<подписываемые данные в формате Base64>»,
    «cmd»: «<команда на идентификационную карту (КТА)>»,
    «cert»: «<сертификат терминала>»
```

```
}
```

Выходные данные:

```
{
    «So»: «<объект безопасности>»,
    «SO Cert»: «<сертификат объекта безопасности>»,
    «rdf»: «<ответ от идентификационной карты (КТА)>»,
    «penult»: «<индикатор последнего шага на КП>»
}
```

4.10. Формирование конфигурационного файла для TLS-соединения (URL): http://127.0.0.1:8084/tls_init.

Входные данные:

```
{
     «tls_server_ip_port»: «<IP-порт и порт TLS-сервера>»,
    «tls_client_port»: «<порт TLS-клиента>»

}
```

Выходные данные:

```
{
    «error»: «<0>»
}
```

4.11. Выработка ЭЦП через идентификационную карту (КТА) и создание CMS-структуры (URL): http://127.0.0.1:8084/sign_kta_cms.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате Base64>»,
    «isDetached»: «<параметр, который определяет, будет ли ЭЦП отсоединенная>»
}
```

Выходные данные:

```
{
    «cok»: «<значение СОК>»,
    «data»: «<подписываемые данные в формате Base64>»,
    «sig»: «<значение ЭЦП>»,
    «error»: «<код ошибки>»
}
```

4.12. Считывание групп данных с идентификационной карты (КТА) (URL): http://127.0.0.1:8084/data_groups.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате Base64>»,
    «init»: «<параметр инициализации>»,
    «cmd»: «<команда на идентификационную карту (КТА)>»,
    «cert»: «<сертификат терминала>»
}
```

Выходные данные:

```
{
    «So»: «<объект безопасности>»,
    «SO Cert»: «<сертификат объекта безопасности>»,
    «rdf»: «<ответ от идентификационной карты (КТА)>»,
    «penult»: «<индикатор последнего шага на КП>»
}
```

4.13. Выработка ЭЦП размером 48 байт через программу криптопровайдера (URL): http://127.0.0.1:8084/sign_base.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате Base64>»
}
```

Выходные данные:

```
{
    «cok»: «<значение СОК>»,
    «data»: «<подписываемые данные в формате Base64>»,
    «sig»: «<значение ЭЦП>»,
    «error»: «<код ошибки>»
}
```

4.14. Выработка ЭЦП через программу криптопровайдера с добавлением атрибутного сертификата (URL): http://127.0.0.1:8084/sign_cms_ac .

Входные данные:

```
{
    «data»: «<подписываемые данные в формате Base64>»,
    «AC»: «<значение атрибутного сертификата>»,
    «isDetached»: «<параметр, который определяет, будет ли ЭЦП отсоединенная>»
}
```

Выходные данные:

```
{
    «sig»: «<значение ЭЦП>»,
    «error»: «<код ошибки>»
}
```

4.15. Генерация ключа для usb-токенов (URL): http://127.0.0.1:8084/keygen.

Входные данные:

```
{
    «init»: «<начало генерации ключа>»
}
```

Выходные данные:

```
{
    «NKI_serial_number»: «<серийный номер USB-токена>»,
    «status»: «<статус>»,
    «name»: «<наименование ключевой пары>»,
    «public_key»: «<значение открытого ключа>»
}
```

4.16. Выработка ЭЦП от хеш-значения через программу криптопровайдера (URL): http://127.0.0.1:8084/sign_base_hash.

Входные данные:

```
{
    «hash»: «<подписываемое хеш-значение в формате Base64>»
}
```

Выходные данные:

```
{
    «sig»: «<значение ЭЦП>»
}
```

4.17. Выработка ЭЦП от хеш-значения через идентификационную карту (КТА) (URL): http://127.0.0.1:8084/sign_base_hash_kta.

Входные данные:

```
{
    «hash»: «<подписываемое хеш-значение в формате Base64>»
}
```

Выходные данные:

```
{
```

```
    «sig»: «<значение ЭЦП>»
}
```

4.18. Шифрование данных (URL): http://127.0.0.1:8084/env_base.

Входные данные:

```
{
    «data»: «<данные для конвертования>»,
    «COK_Reg»: «<значение СОК регистратора РЦ>»
}
```

Выходные данные:

```
{
    «Env_req_fl»: «<конвертованные данные>»
}
```

4.19. Дешифрование данных через программу криптопровайдера (URL): http://127.0.0.1:8084/remove_env_base.

Входные данные:

```
{
    «env_data»: «<данные для конвертования>»
}
```

Выходные данные:

```
{
    «data»: «<расшифрованные данные>»
}
```

4.20. Дешифрование данных через идентификационную карту (КТА) (URL): http://127.0.0.1:8084/remove_env_base_kta.

Входные данные:

```
{
    «env_data»: «<данные для конвертования>»
}
```

Выходные данные:

```
{
    «data»: «<расшифрованные данные>»
}
```

4.21. Выработка ЭЦП через средство ЭЦП с помощью открытого ключа (URL): http://127.0.0.1:8084/sign_public_key_sigma.

Входные данные:

```
{
    «data»: «<подписываемые данные в формате Base64>»,
    «name»: «<наименование открытого ключа>»,
    «public_key»: «<значение открытого ключа>»
}
```

Выходные данные:

```
{
    «data»: «<подписываемые данные в формате Base64>»,
    «sig»: «<значение ЭЦП>»,
    «error»: «<код ошибки>»
}
```

4.22. Подготовительная команда для работы с терминалом, идентификационной картой (КТА) или sigma2 при авторизации (URL): /api/v1/terminal_proxy_bauth_prefetch.

Входные данные:

```
{
    «cms»: «<CMS, которая приходит от СИ>»,
    «stb»: «<если значение true, то работа идет с sigma2; если значение false, то работа идет с идентификационной картой (КТА)>»
```

```
}
```

Выходные данные:

```
{
    «err»: «<текст ошибки>»,
    «so_certificate»: «<сертификат объекта безопасности>»,
    «cert_id»: «<серийный номер терминального сертификата КТА>»
}
```

4.23. Инициализация протокола BAUTH (URL): /api/v1/terminal_proxy_bauth_init.

Входные данные:

```
{
    «terminal_certificate»: «<сертификат терминала>»,
    «cmd_to_card»: «<команда на идентификационную карту (КТА)>»,
    «is_bilateral»: true
}
```

Выходные данные:

```
{
    «err»: «<текст ошибки>»,
    «card_response»: «<ответ от идентификационной карты (КТА)>»
}
```

4.24. Шаги протокола BAUTH (URL): /api/v1/terminal_proxy_bauth.

Входные данные:

```
{
    «header_cmd_to_card»: «<заголовок команды на идентификационную карту (КТА)>»,
    « cmd_to_card»: «<команда на идентификационную карту (КТА)>»
}
```

Выходные данные:

```
{
    «err»: «<текст ошибки>»,
    «card_response»: «<ответ от идентификационной карты (КТА)>»
}
```

4.25. Обмен сообщениями с терминалом (URL): /api/v1/terminal_proxy_command.

Входные данные:

```
{
    «header_cmd_to_card»: «<заголовок команды на идентификационную карту (КТА)>»,
    « cmd_to_card»: «<команда на идентификационную карту (КТА)>»
}
```

Выходные данные:

```
{
    «err»: «<текст ошибки>»,
    «card_response»: «<ответ от идентификационной карты (КТА)>»
}
```

4.26. Инициализация ЭЦП (URL): /api/v1/terminal_proxy_sign_init.

Входные данные:

```
{
    «header_cmd_to_card»: «<заголовок команды на идентификационную карту (КТА)>»,
    « cmd_to_card»: «<команда на идентификационную карту (КТА)>»
}
```

Выходные данные:

```
{
    «err»: «<текст ошибки>»,
    «card_response»: «<ответ от идентификационной карты (КТА)>»
}
```

4.27. Подготовительная команда для работы с терминалом, с идентификационной картой (КТА) или sigma2 (URL): terminal_proxy_bauth_app_prefetch.

Входные данные:

```
{
    «cms»: «<CMS, которая приходит от СИ>»,
    «stb»: «<если значение true, то работа идет с sigma2; если значение false, то работа идет с идентификационной картой (КТА)>»
}
```

Выходные данные:

```
{
    «err»: «<текст ошибки>»,
    «so_certificate»: «<сертификат объекта безопасности>»,
    «cert_id»: «<серийный номер терминального сертификата КТА>»
}
```

4.28. Описание полей конфигурационного файла *ini.

[listener]

cleanupInterval=60000 - время, после которого неиспользуемые потоки удаляются;

maxMultiPartSize=10000000 – размер запроса, который принимается частями;

maxRequestSize=160000000 – максимальная длина запроса;

maxThreads=100 – максимальное количество одновременных рабочих потоков;

minThreads=4 – минимальное количество потоков, которое будет поддерживаться даже после отключения всех остальных потоков в течение времени cleanupInterval;

port=8084 – порт, на котором работает КП;

readTimeout=60000 – время, в течение которого операция чтения блокирует ожидание данных;

[logging]

bufferSize=100 – размера буфера, куда записывается лог-файл (вначале в буфер, потом в файл);

fileName=../logs/NTClientSoftware.log – путь для записи лог-файлов;

maxBackups=2 – сколько старых файлов журнала должно храниться на диске;

maxSize=1000000 – ограничения размера журнала в байтах;

minLevel=0 – уровень, при котором записываются все сообщения;

msgFormat={timestamp} {typeNr} {type} {thread} {msg} – формат сообщения;

timestampFormat=dd.MM.yyyy hh:mm:ss.zzz – формат времени;

[stunnel]

accept=127.0.0.1:8085 – на каком порту принимать трафик;

ciphers=DHT-BIGN-BELT-DWP-HBELT:DHE-BIGN-BELT-DWP-HBELT:DHT-BIGN-BELT-CTR-MAC-HBELT:DHE-BIGN-BELT-CTR-MAC-HBELT – шифронаборы TLS-соединения;

connect=192.168.155.41:8443 – адрес TLS-сервера;

create=true – создание конфигурационного файла при запуске, при «false» будет использоваться существующий;

debug=7 – уровень логирования;

verify=0 – не проверять сертификат сервера;

[verify_cms]

ca_path=./CA – путь к ca-файлам;

crl_path=./CRL – путь к crl-файлам;

root_ca_crl_link=https://nces.by/wp-content/uploads/certificates/pki/kuc.crl - ссылка на скачивание;

sub_ca_crl_link=https://nces.by/wp-content/uploads/certificates/pki/ruc.crl - ссылка на скачивание;

[avbign]

lib_path=C:/Users/aaleks/Documents/CP/avbign_lib/x64 - путь к библиотеке для работы с носителем ключевой информации AvBign ИЯТА.467532.003 из состава

AvJCEProv;

name="AVB1050041731 " - серийный номер носителя ключевой информации AvBign ИЯТА.467532.003;

[sigma]

cert= - путь к файлу СОК пользователя;

lib=../lib/libnki3.0.so - путь к библиотеке для работы со средством криптографической защиты информации «Сигма» БФИД.467379.001-01;

serial_num=1086 - серийный номер средства криптографической защиты информации «Сигма» БФИД.467379.001-01;

[sigma2]

name=NII TZI Sigma 2 0 – наименование средства криптографической защиты информации «Сигма» БФИД.467379.001-01;

[idcard]

reader=ACS ACR39U ICC Reader 0 - название считывателя;

[ntsks]

name=89375027010016832260 - серийный номер СИМ-карты;

[current_token]

name=ntsks - тип текущего используемого носителя;

[name]

ntsks=89375027010016832260 - серийный номер текущего токена;

[software_key]

path_to_key=C:/Users/aaleks/Desktop/shards/key.pem - путь к файловому контейнеру личного ключа пользователя;

shard0=C:/Users/aaleks/Desktop/shards/shard0.pem - путь к частичным секретам пользователя;

shard1=C:/Users/aaleks/Desktop/shards/shard1.pem - путь к частичным секретам пользователя;

shard2=C:/Users/aaleks/Desktop/shards/shard2.pem - путь к частичным секретам пользователя;

shard3=C:/Users/aaleks/Desktop/shards/shard3.pem - путь к частичным секретам пользователя;

shard4=C:/Users/aaleks/Desktop/shards/shard4.pem - путь к частичным секретам пользователя;

shard5=C:/Users/aaleks/Desktop/shards/shard5.pem - путь к частичным секретам пользователя;

shard6=C:/Users/aaleks/Desktop/shards/shard6.pem - путь к частичным секретам пользователя;

[eye_button_section] – кнопка отображения/скрытия пароля;

is_hidden=true – пароль отображается, если «is_hidden=false», пароль скрыт и в окне ввода пароля появится кнопка «Показать пароль»

5. СООБЩЕНИЯ ОПЕРАТОРУ

5.1. Тексты сообщений, выдаваемых в ходе выполнения КП, описание их содержания и соответствующие действия оператора приведены в таблице 1.

Таблица 1

Текст сообщения	Причина сообщения	Действие оператора
Bad request = 400	Структура пакета неверна	Обратиться к поставщику программного обеспечения (ПО)
Internal error = 500	Непредвиденная ошибка сервера	Обратиться к поставщику ПО
Коды ошибок, возвращаемые веб-сервисом – тег «error»		
STUNNEL_FAILED_TO_INIT = 100	Не удалось инициализировать TLS-соединение	Обратиться к поставщику ПО
CO_FAILED_TO_GET_DIGEST = 201	Ошибка получения структуры EVP_MD	Обратиться к поставщику ПО
CO_DIGEST_INIT_FAILED = 202	Ошибка инициализации ctx контекста дайджеста	Обратиться к поставщику ПО
CO_DIGEST_UPDATE_FAILED = 203	Ошибка хеширования cnt байтов данных в контекст дайджеста ctx 203	Обратиться к поставщику ПО
CO_DIGEST_FINAL_FAILED = 204	Ошибка получения значения дайджеста из ctx и помещения его в md	Обратиться к поставщику ПО
CO_DIGEST_VERIFY_INIT_FAILED = 205	Ошибка установки ctx контекста проверки для использования дайджеста с именем «mdname» и открытым ключом «pkey»	Обратиться к поставщику ПО
CO_DIGEST_VERIFY_UPDATE_FAILED = 206	Ошибка хеширования cnt байт данных в контекст проверки ctx 206	Обратиться к поставщику ПО
CO_PARSE_CERT_FAILED = 207	Не удалось собрать сведения о СОК	Обратиться к поставщику ПО
CO_PARSE_CMS_FAILED = 208	Не удалось собрать сведения о CMS-структуре	Обратиться к поставщику ПО
CO_CREATE_X509_STORE_FAILED = 209	Не удалось создать структуру X509_STORE	Обратиться к поставщику ПО
CO_ADD_CERT_TO_STORE_FAILED = 210	Не удалось добавить СОК в структуру X509_STORE	Обратиться к поставщику ПО
CO_ADD_CRL_TO_STORE_FAILED = 211	Не удалось добавить CRL в структуру X509_STORE	Обратиться к поставщику ПО

Продолжение таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
CO_STORE_SET_PURPOSE_FAILED = 212	Не удалось установить значение по умолчанию для соответствующих значений, используемых при проверке цепочки СОК	Обратиться к поставщику ПО
CO_STORE_SET_FLAG_FAILED = 213	Не удалось установить значение по умолчанию для соответствующих значений, используемых при проверке цепочки СОК	Обратиться к поставщику ПО
CO_GET_CMS_CONTENT_FAILED = 214	Не удалось вернуть указатель на указатель ASN1_OCTET_STRING, содержащий встроенный контент	Обратиться к поставщику ПО
CMS_VERIFICATION_FAILURE = 215	Не удалось проверить CMS-структуру	Обратиться к поставщику ПО
CMS_CERTIFICATE_VERIFY_ERROR = 216	Не удалось проверить СОК	Обратиться к поставщику ПО
CMS_get0_SignerInfos_ERROR = 217	Не удалось вернуть все структуры CMS_SignerInfo, связанные со структурой signedData CMS	Обратиться к поставщику ПО
sk_CMS_SignerInfo_value_ERROR = 218	Не удалось получить структуру CMS_SignerInfo	Обратиться к поставщику ПО
CMS_SignerInfo_get0_signature_ERROR = 219	Не удалось извлечь ЭЦП, связанную с si, в указателе на структуру ASN1_OCTET_STRING	Обратиться к поставщику ПО
NEED_INIT = 801	Не получена команда на инициализацию	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
PASSWORD_LOCKED_FOREVER = 802	Пароль заблокирован навсегда	Обратиться к поставщику идентификационной карты (КТА)
FAILED_TO_GET_PROTECTED_COMMAND = 803	Не удалось отправить защищенную команду на терминал	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
PASSWORD_ENTRY_CANCELED = 804	Отменен ввод пароля	Ввести пароль
PASSWORD_LOCKED = 805	Пароль заблокирован	Разблокировать пароль

Продолжение таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
SELECTION_OF_CERTIFICATE_CANCELED = 806	Отменен выбор СОК	Выбрать СОК
CryptEncodeObjectEx_len_FAILED = 807	Ошибка получения длины закодированной структуры szOID_RSA_signingTime	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CryptEncodeObjectEx_FAILED = 808	Ошибка получения закодированной структуры szOID_RSA_signingTime	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
ERROR_GETTING_OID_HASH_ALGORITHM = 809	Ошибка получения OID алгоритма хеширования	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
SPS_SCOPE_DO_NOT_MATCH = 900	Не совпали данные ЭЦП и Scope_ПС	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
NO_S_ = 901	Нет базовой ЭЦП в CMS-структуре	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
FAILED_TO_VERIFY_SIGNATURE = 902	Не удалось проверить ЭЦП	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
TIME_DIDNT_CONCIDE = 903	ЭЦП вычислена позже, чем 300 с	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
NO_CONTENT = 904	Нет подписанных данных	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
CMS_UNSUPPORTED_TYPE = 905	Формат ЭЦП некорректен	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
CMS_VERIFY_FAILED = 906	Не удалось проверить ЭЦП	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
BASE_VERIFY_FAILED = 907	Не удалось проверить базовую ЭЦП	Обратиться к поставщику ПО

Продолжение таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
READ_KTA_2c02_FILE = 908	Не удалось прочитать данные с идентификационной карты (КТА)	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
READ_KTA_2c03_FILE = 909	Не удалось прочитать данные с идентификационной карты (КТА)	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
FAILED_INIT_BAUTH = 910	Не удалось инициализировать протокол Bauth	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
FAILED_CHECK_CERT_BAUTH = 911	Не удалось проверить СОК терминала	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
FAILED_SEND_M0_BAUTH = 912	Не удалось отправить первое сообщение протокола Bauth	Пройти авторизацию повторно. В случае неудачи обратиться к поставщику ПО
FAILED_SEND_M2_BAUTH = 913	Не удалось отправить третье сообщение протокола Bauth	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_TERMINAL_STEP = 914	Ошибка одного из шагов терминала	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_PROXY_TERMINAL_COMMAND = 915	Не удалось отправить защищенную команду на идентификационную карту (КТА)	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_TO_SWITCH_CONTEXT = 916	Не удалось инициализировать engine	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_TO_READ_KTA_FILE = 917	Не удалось прочитать данные с идентификационной карты (КТА)	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CLAIMS_CANCELED = 918	Отменено подтверждение списка запрашиваемых разрешений	Подтвердить действие
CONF_FAILED_TO_READ_ROOT_CA_LINK_PARAM = 919	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО

Продолжение таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
CONF_FAILED_TO_READ_SUB_CA_LINK_PARAM = 920	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DL_FAILED_TO_CREATE_FOLDER = 921	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CONF_FAILED_TO_READ_SUB_CA_CRL_LINK_PARAM = 922	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DL_FAILED_TO_OPEN_FILE = 923	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DL_FAILED_TO_READ_SERVER_REPLY = 924	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DL_FAILED_TO_WRITE_TO_FILE = 925	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DL_FAILED_TO_DOWNLOAD_FILE = 926	Не удалось загрузить CRL	Включить интернет или обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CERT_LIST_CANCELED = 927	Отменено подтверждение отсутствия роли в СОК	Подтвердить действие
THE_OPERATION_ISNT_SUPPORTED = 928	Не удалось загрузить открытый ключ	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_TO_LOAD_PRIVATE_KEY = 929	Не удалось загрузить открытый ключ	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_TO_GENERATION_CMS_SIGNED_DATA = 930	Не удалось создать CMS-структуру	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
PASSWORD_FAIL = 931	Некорректный пароль	Ввести верный пароль
FAILED_ENUM_KEYS = 932	Не удалось загрузить ключи с usb-токена	Обратиться к поставщику USB-токена или поставщику ПО
DNT_GET_CMS_CERT = 933	Не удалось получить сертификат из CMS-структуры	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО

Продолжение таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
SIGN_ERROR = 934	Не удалось выработать ЭЦП	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
FAILED_TO_LOAD_CERTIFICATE = 935	Не удалось загрузить СОК	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
SIGN_BASE_HASH = 936	Не удалось подписать хеш-значение	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
SWITCH_CONNECTION_ERROR = 937	Не удалось инициализировать engine	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
READ_KTA_FILE5120 = 938	Не удалось прочитать сертификат терминала eSign с идентификационной карты (КТА)	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
PARSE_CMS_ERROR = 939	Не удалось собрать сведения о CMS-структуре	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
NO_V_ASN1_SEQUENCE = 940	Не удалось найти роль в СОК	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
NO_V_ASN1_OBJECT =941	Не удалось найти роль в СОК	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
NO_GET_BY_NID = 942	Не удалось найти роль в СОК	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DO_NOT_MATCH_BPKI_ROLE_IDC = 943	Не удалось найти роль в СОК	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CERTIFICATE_FAILED = 944	Не удалось получить СОК при шифровании	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
ENV_ERROR = 945	Не удалось расшифровать данные	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
NO_HSTORE = 946	Не удалось расшифровать данные через программу криптопровайдера	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CRYPT_DECRYPT_MESS_ERR = 947	Не удалось расшифровать данные через программу криптопровайдера	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
DECRYPT_ERR = 948	Не удалось расшифровать данные через идентификационную карту	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО

Продолжение таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
	(КТА)	

READ_KTA_FILE5110 = 949	Не удалось получить СОК с идентификационной карты (КТА)	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
TOKEN_CMS_ENCRYPT_ERROR = 950	Не удалось законвертировать данные	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
getSlotIdList_ERROR = 951	Не удалось получить список подключенных считыватель КТА	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
getSlotNameByteId_ERROR = 952	Не удалось найти подключенный считыватель КТА из списка	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CARD_NOT_CONNECTED = 953	Идентификационная карта (КТА) не подключена	Подключить идентификационную карту (КТА)
READER_NOT_CONNECTED = 954	считыватель КТА не подключен	Подключить считыватель КТА
EVP_PKEY_verify_init_ERROR = 955	Ошибка проверки открытого ключа	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
EVP_PKEY_CTX_set_signature_md_ERROR = 956	Не удалось установить тип профиля сообщения, используемый в ЭЦП	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
EVP_PKEY_sign_ERROR = 957	Не удалось подписать открытый ключ	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
CTX_ERROR = 958	Не удалось получить CTX	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
EVP_PKEY_sign_init_ERROR = 959	Не удалось инициализировать CTX контекста алгоритма открытого ключа для ЭЦП	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
MD_ERROR = 960	Не удалось получить MD	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
EVP_DigestSignInit_ERROR = 961	Не удалось установить контекст	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
EVP_DigestSignFinal_ERROR = 962	Не удалось подписать данные CTX и поместить ЭЦП в sig	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО

Окончание таблицы 1

Текст сообщения	Причина сообщения	Действие оператора
EVP_DigestSignUpdate_ERROR = 963	Не удалось хешировать байт данных в контекст ЭЦП	Обратиться к поставщику идентификационной карты (КТА) или поставщику ПО
COULD_NOT_DECRYPT_REQUEST = 964	Не удалось расшифровать сообщение	Обратиться к поставщику поставщику ПО
EVP_PKEY_CTX_NEW_FAILED = 965	Не удалось выделить контекст алгоритма открытого ключа, используя алгоритм, указанный в pkey и ENGINE	Обратиться к поставщику поставщику ПО

EVP_PKEY_DECRYPT_INIT_FAILED = 966	Не удалось инициализировать контекст алгоритма открытого ключа, используя ключ pkey для операции дешифрования	Обратиться к поставщику поставщику ПО
EVP_PKEY_CTX_CTRL_FAILED = 967	Не удалось отправить управляющую операцию в контекст	Обратиться к поставщику поставщику ПО
EVP_PKEY_DECRYPT_FAILED= 968	Не удалось выполнить операцию дешифрования открытого ключа с помощью ctx	Обратиться к поставщику поставщику ПО
MAC_FAILED = 969	Не удалось вычислить mac	Обратиться к поставщику поставщику ПО
LOGIN_ERROR = 970	Не удалось авторизоваться	Проверить пароль или обратиться к поставщику поставщику ПО
GENERATE_KEY_PAIR_ERROR = 971	Не удалось сгенерировать ключевую пару	Обратиться к поставщику поставщику ПО
FAILED_TO_SAVE_KEY_TO_BUFFER = 972	Не удалось сохранить key.pem и shard	Обратиться к поставщику поставщику ПО
NO_ENV_DATA = 973	Некорректные входные параметры, отсутствует env_data	Обратиться к поставщику поставщику ПО
MAC_DO_NOT_MATCH = 974	Не удалось сравнить mac	Обратиться к поставщику поставщику ПО
cipherDecrypt_ERROR = 975	Не удалось расшифровать сообщение	Обратиться к поставщику поставщику ПО
COULD_NOT_PARSE_SO_CONTENT = 978	Не удалось собрать сведения об объекте безопасности	Обратиться к поставщику поставщику ПО
DG_HASH_ARE_NOT_EQUAL = 979	Хеш-значения групп данных не совпадают	Обратиться к поставщику поставщику ПО
Запуск программы невозможен, так как на компьютере отсутствует api-ms-win-crt-runtime-l1-1-0.dll	Отсутствует обновление UpdatePack7R2-20.7.15 для ОС Windows 7	Установить обновление UpdatePack7R2-20.7.15 для ОС Windows 7
Ошибка при запуске приложения (0x000007b). Для выхода из приложения нажмите кнопку «ОК».	Отсутствует обновление UpdatePack7R2-20.7.15 для ОС Windows 7	Установить обновление UpdatePack7R2-20.7.15 для ОС Windows 7

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

ЕС ИФЮЛ	– Единая система идентификации физических и юридических лиц;
КП	– клиентская программа;
КПСИС	– комплекс программных средств прикладной системы;
КТА	– криптографический токен аутентификации;
ОС	– операционная система;
ПО	– программное обеспечение;
ПЭВМ	– персональная электронная вычислительная машина;
СИ	– сервер идентификации;
СОК	– сертификат открытого ключа;
ЭЦП	– электронная цифровая подпись.