
УДОСТОВЕРЯЮЩИЙ ЦЕНТР

# «IDC Управление ключами»

# Руководство пользователя

Версия 1.1

2026

Оглавление

# 1. Общие сведения

## 1.1. Основные функции

- Генерация ключевой пары посредством «CryptoAPI».
- Генерация запросов на выдачу сертификатов открытого ключа электронной подписи.
- Получение выданных сертификатов открытого ключа электронной подписи с последующей записью на ключевой носитель (токен).
- Просмотр содержимого выданных сертификатов открытого ключа электронной подписи.
- Проверка текущего статуса выданного сертификата открытого ключа электронной подписи.
- Отзыв, приостановка и возобновление действия выданных сертификатов открытого ключа электронной подписи.
- Установка корневого сертификата.
- Идентификация и аутентификация посредством учётных данных (логин/пароль) и второго фактора (email/sms).
- Идентификация и аутентификация посредством входа по сертификату.
- Идентификация и аутентификация посредством входа по QR-коду.

## 1.2. Регистрация в Удостоверяющем центре

Для получения первого сертификата открытого ключа электронной подписи с использованием программы «IDC Управление ключами», будущий владелец сертификата должен лично явиться к представителю Удостоверяющего центра для идентификации его личности и полномочий и пройти процедуру регистрации в строгом соответствии с Регламентом Удостоверяющего центра.

## 1.3. Системные требования

- Операционные системы: Windows 7, 10, 11
- Microsoft.NET Framework версии 4.7.2:
  - Веб-установщик
  - Автономный установщик

- Программное обеспечение для токена «EnterSafe PKI Manager - ePass2003».

  Установку и настройку программы необходимо произвести согласно п.1.3 документа «Руководство пользователя Токен ePass2003».

# 2. Установка программы

## 2.1. Загрузка автономного установщика программы и проверка его подлинности

Скачайте последнюю версию автономного установщика программы с официального сайта Удостоверяющего центра по ссылке.

После завершения загрузки установщика, откройте папку, в которую браузер сохраняет загруженные файлы, и убедитесь, что в ней присутствует файл “CAClientSetup-x.x.x.xx.exe” (x.x.x.xx – версия программы).

Пример:

*C:\CAClientSetup-1.0.0.50.exe*

Если файл отсутствует, выполните его повторную загрузку.

Для вычисления хэш-суммы SHA-1 в командной строке Windows (cmd) выполните команду:

*certutil -hashfile "<путь к файлу инсталлятора>" SHA1*

Пример:

*certutil -hashfile "C:\CAClientSetup-1.0.0.50.exe" SHA1*

Хэш-сумму SHA-1 также можно вычислить с использованием Windows PowerShell, выполнив команду:

*Get-FileHash "<путь к файлу инсталлятора>" -Algorithm SHA1*

Пример:

*Get-FileHash "C:\CAClientSetup-1.0.0.50.exe" -Algorithm SHA1*

Полученное значение хэш-суммы должно полностью совпадать со значением, опубликованным на официальном сайте Удостоверяющего центра. Совпадение значений подтверждает целостность и подлинность скачанного файла установщика.

2.2. Процесс установки программы

- Запустите «CAClientSetup.exe».
- После запуска автономного установщика программы появится окно приветствия мастера установки. Нажмите кнопку «Далее». (Рис.2.1).

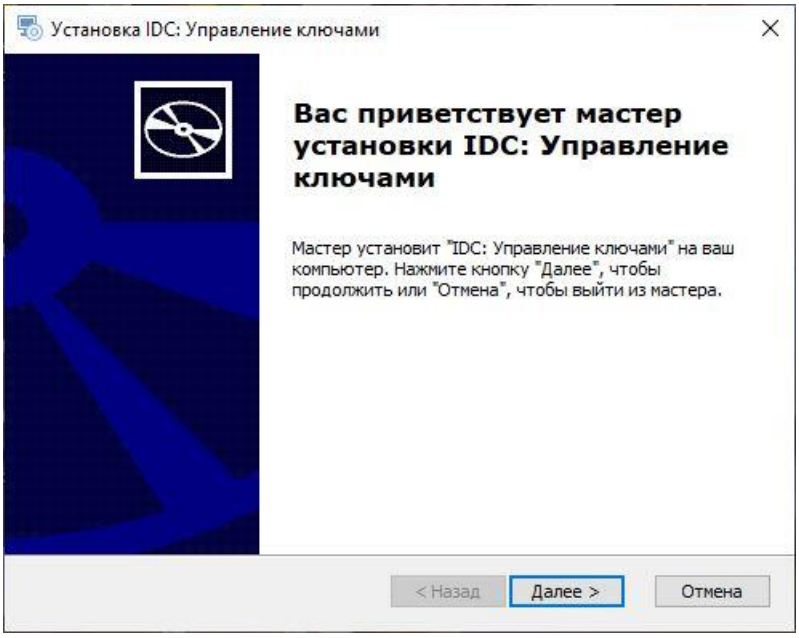



Рис.2.1

- Выберите папку для установки программы. Нажмите кнопку «Далее» (Рис.2.2).

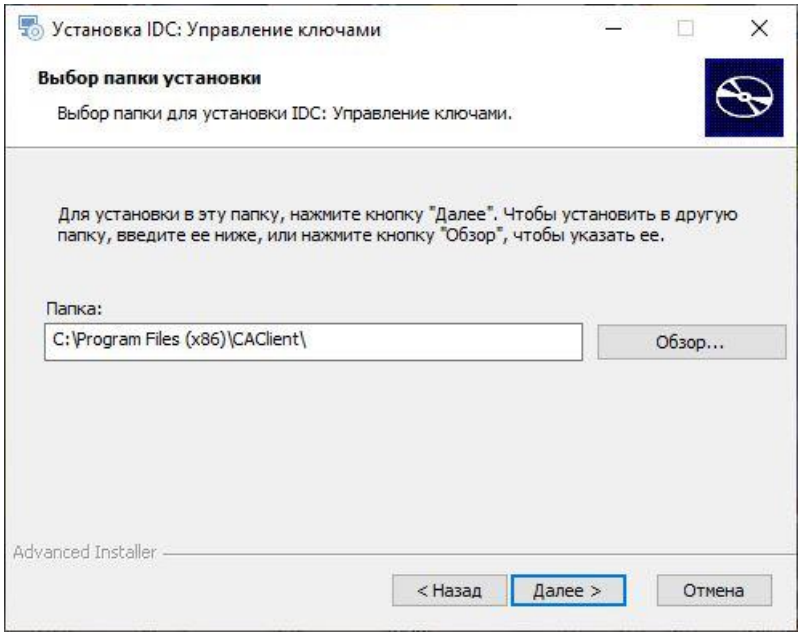



Рис.2.2

- Нажмите кнопку «Установить», чтобы начать установку программы (Рис.2.3).

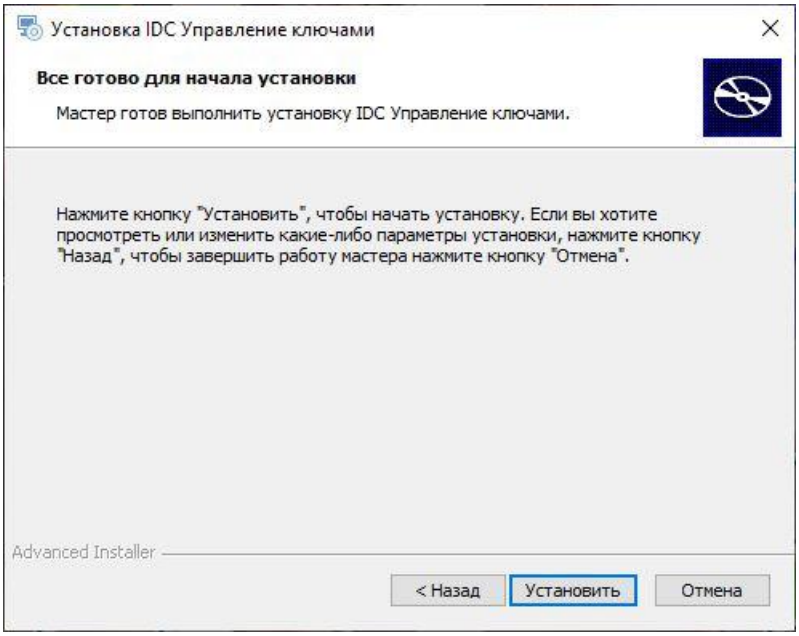



Рис.2.3

- Установка файлов программы в систему (Рис.2.4).

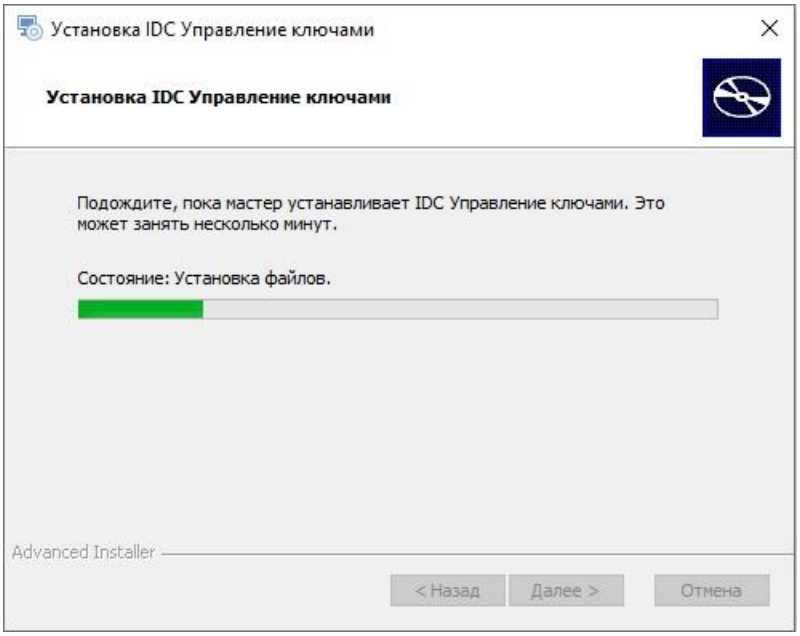



Рис.2.4

- Мастер установки проверяет наличие корневого сертификата «ROOT-PMR-CA» в оснастке «Certificates – Current User», в разделе «Доверенные корневые центры сертификации» вашей операционной системы. Если корневой сертификат не найден в оснастке, то мастер установки предложит Вам установить его. Нажмите кнопку «Да». (Рис.2.5).

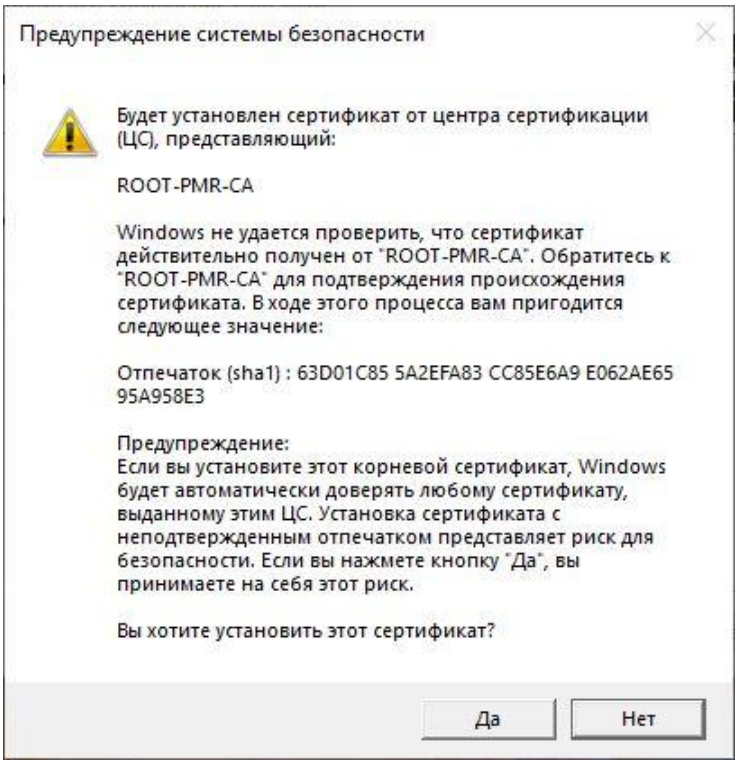



Рис.2.5

- Нажмите кнопку «Готово», чтобы запустить программу «IDC Управление ключами» (Рис.2.6).

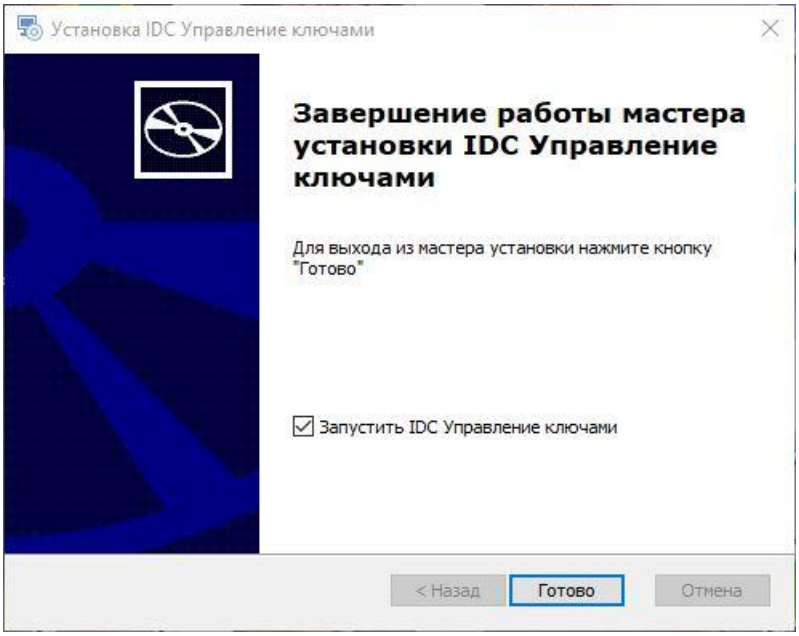



Рис.2.6

# 3. Удаление программы

## 3.1. Запуск мастера удаления программы

- Найдите в меню «Пуск» группу программ «IDC Удостоверяющий центр» и раскройте ее. Выберите пункт меню «Удалить IDC Управления ключами». Нажмите кнопку «Да». (Рис.3.1).

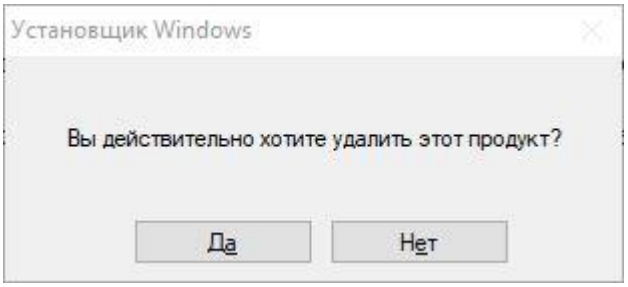



Рис.3.1

- Либо откройте «Панель управления», выберите категорию «Программы». В категории «Программы» выберите «Удаление программы». Найдите в списке программу «IDC Управления ключами» и дважды щёлкните по ней левой кнопкой мыши (Рис.3.2).

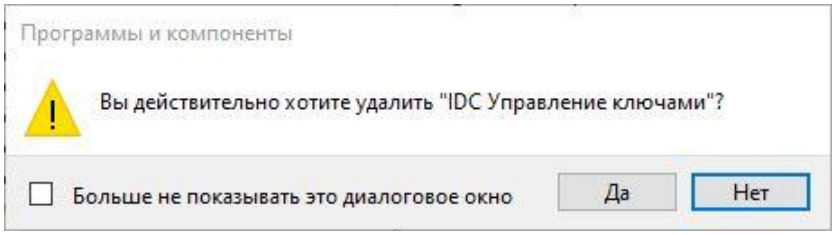



Рис.3.2

3.2. Процесс удаления программы

- Дождитесь окончания работы мастера удаления программы (Рис.3.3).

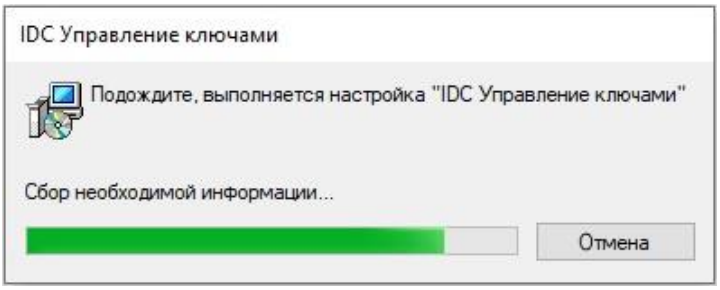



Рис.3.3

# 4. Запуск программы

## 4.1. Варианты запуска программы

- Найдите на рабочем столе ярлык «IDC Управление ключами» и дважды щёлкните по ярлыку левой кнопкой мыши. (Рис.4.1).

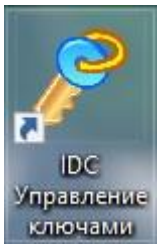



Рис.4.1

- Либо найдите в меню «Пуск» группу программ «IDC Удостоверяющий центр» и раскройте ее. Выберите пункт меню «IDC Управления ключами» (Рис.4.2).

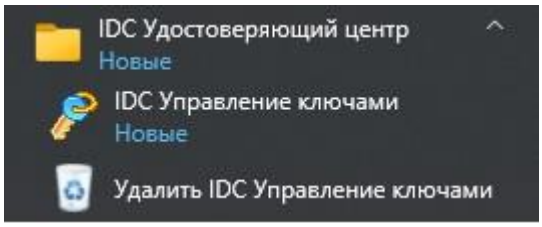



Рис.4.2

## 4.2. Двухфакторная аутентификация

Для входа в программу используйте учетные данные пользователя Удостоверяющего центра СЗАО «Интерднестрком».

- В качестве первого фактора аутентификации введите логин, пароль и нажмите кнопку «Вход» (Рис.4.3).

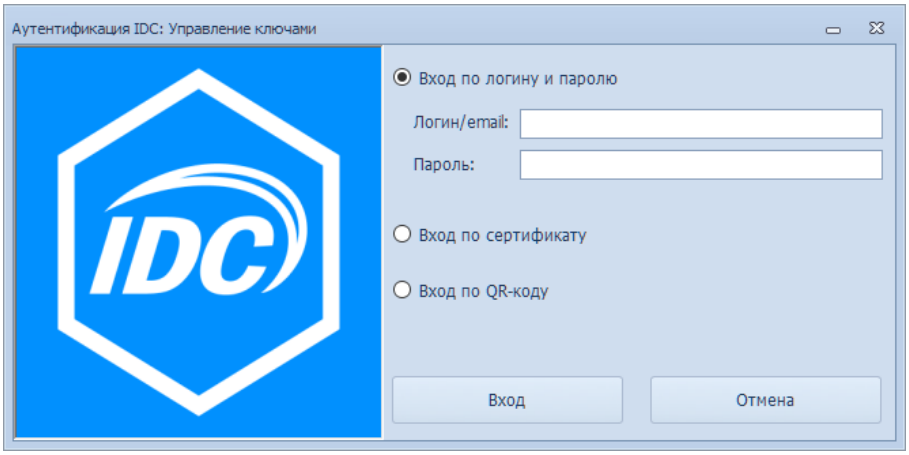



Рис.4.3

Удостоверяющим центром установлен лимит попыток ввода пароля – не более 5 неудачных попыток, после которых наступает временная блокировка возможности ввода пароля на 15 минут.

- Удостоверяющий центр отправит код подтверждения на Ваш контакт (электронная почта / SMS), указанный в строке «Двухфакторная аутентификация» ваших учетных данных для входа в программу (Рис.4.4).

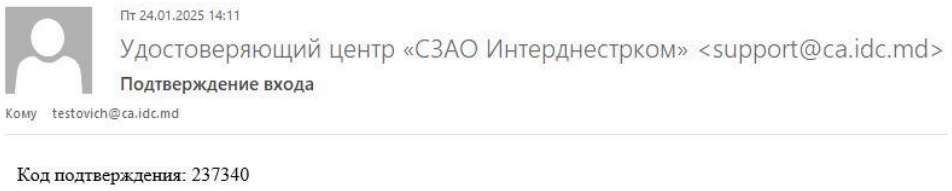



Рис.4.4

- В качестве второго фактора аутентификации введите код подтверждения в поле «код OTP» и нажмите кнопку «Вход». (Рис.4.5 и Рис.4.6).

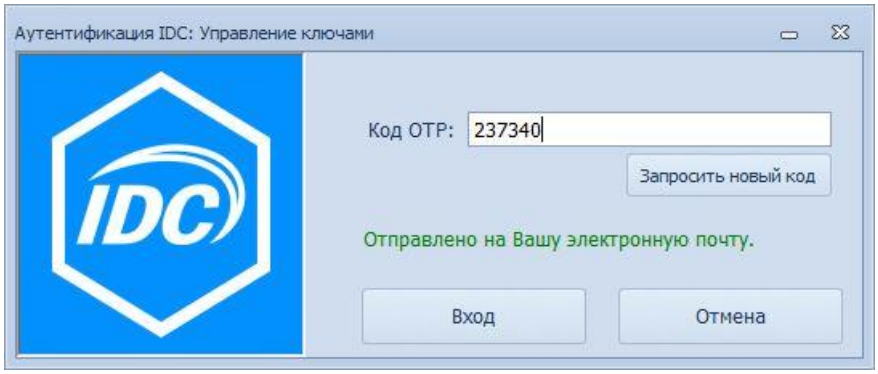



Рис.4.5

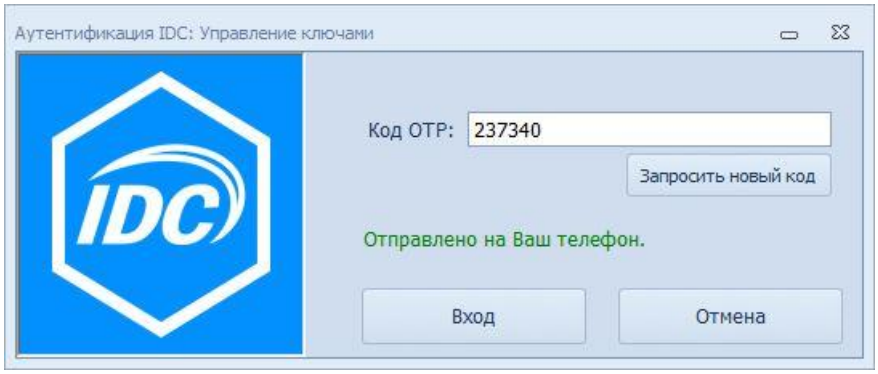



Рис.4.6

4.3. Идентификация и аутентификация посредством входа по сертификату

Выберите пункт «Вход по сертификату» (Рис.4.3) и нажмите кнопку «Вход». Откроется окно выбора сертификата, расположенного на токене пользователя. Отображаются только действительные сертификаты с актуальным сроком действия (рис 4.7).

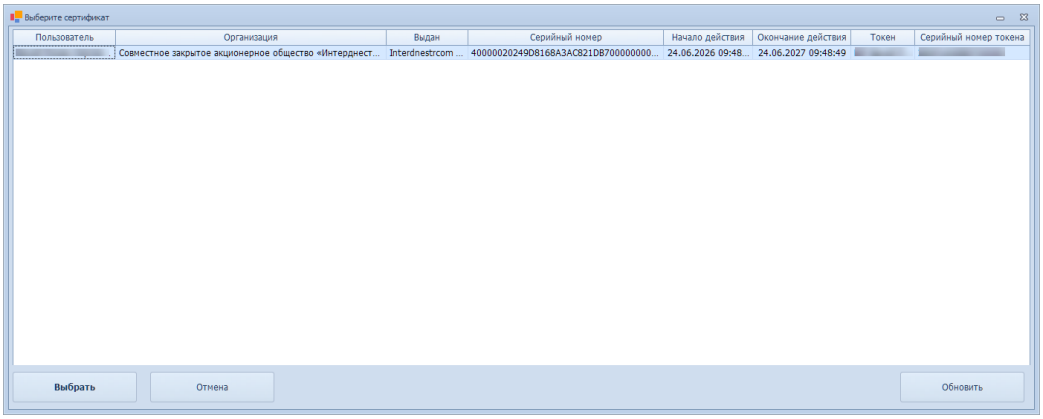



Рис. 4.7

Выберите сертификат из списка и нажмите кнопку «Выбрать». Окно выбора сертификата закроется, после чего будет запрошен ввод PIN-кода токена.

При корректном вводе PIN-кода и успешной аутентификации откроется главное окно программы (Рис.5.1).

4.4. Идентификация и аутентификация посредством входа по QR-коду

Выберите пункт «Вход по QR-коду» (Рис.4.3), и нажмите кнопку «Вход». Откроется окно с QR-кодом (рис. 4.8).


Рис. 4.8

Подтвердите вход путем сканирования QR-кода с использованием мобильного приложения «IDC Управление ключами: мобильная версия».

При успешной аутентификации откроется главное окно программы (Рис.5.1).

4.5. Замена пароля

- Ввод временного пароля приводит к процедуре замены пароля на постоянный.
- Пароль может содержать комбинацию строчных и прописных букв, цифр и специальных символов. Длина пароля должна составлять от 6 до 50 символов (включительно).
- Введите новый пароль, подтвердите его и нажмите «Ок». (Рис.4.9).

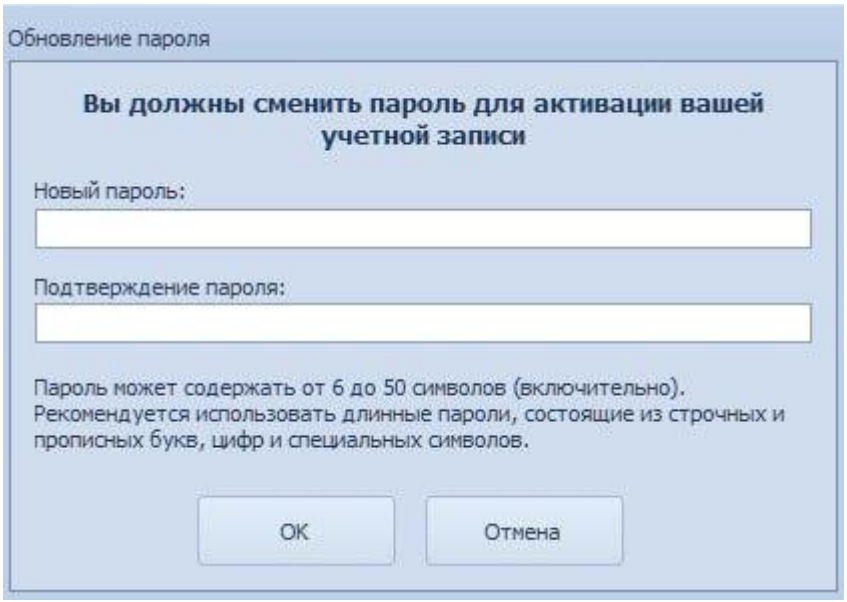



Рис.4.9

- Если Вы забыли или потеряли пароль (в том числе временный), то Вам необходимо обратиться в Удостоверяющий центр для получения нового временного пароля.

4.6. Обновление программы

- После успешной аутентификации программа проверяет наличие новой версии на сайте Удостоверяющего центра в разделе «Программы».
- При наличии более новой версии программы отображается уведомление о доступности обновления (рис. 4.10).

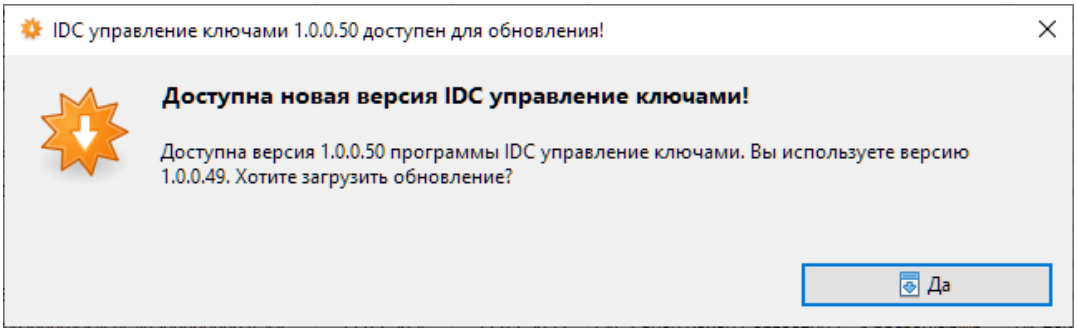



Рис.4.10

- Для загрузки и установки обновления необходимо нажать кнопку **«Да»**. После подтверждения программа выполняет загрузку обновлённых файлов, устанавливает обновление и автоматически перезапускается.
- Обновление программы является обязательным.
- Номер версии отображается в заголовке главного окна программы.

# 5. Описание интерфейса

Главное окно программы условно можно разбить на четыре основные части (Рис.5.1).

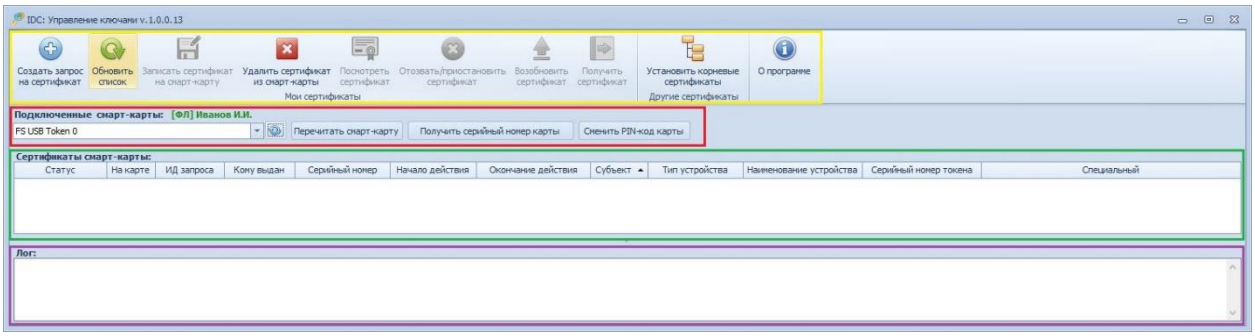



Рис.5.1 Главное окно программы «IDC: Управление ключами»

## 5.1. Лента меню

Лента меню (выделена желтым прямоугольником, Рис. 5.1) содержит кнопки для выполнения определённых действий с Вашими сертификатами. Перечисление слева направо:

- Кнопка «*Создать запрос на сертификат*» позволяет сгенерировать пару ключей (открытый и закрытый) на ключевом носителе, создать запрос на получение сертификата открытого ключа и отослать его в Удостоверяющий центр (Рис. 5.2).


Рис.5.2

см. п.6.3 «Создание запроса на сертификат».

- Кнопка «*Обновить список*» позволяет обновлять информацию в области отображения списка сертификатов. Если состояние того или иного сертификата или запроса на получение сертификата изменится информация в списке обновится (Рис. 5.3).


Рис.5.3

- Кнопка «*Записать сертификат на смарт–карту*» позволяет записать вновь полученный сертификат на ключевой носитель (Рис.5.4).

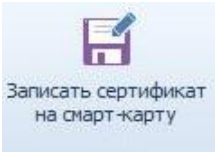



Рис.5.4

см. п.6.5 «Запись сертификата на ключевой носитель».

- Кнопка «*Удалить сертификат из смарт–карты*» позволяет удалить с ключевого носителя выбранный в списке сертификат (токена) (Рис.5.5).

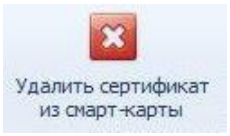



Рис.5.5

см. п.7.3 «Удаление ключей и сертификатов».

- Кнопка «*Посмотреть сертификат*» служит для просмотра детальной информации по выбранному сертификату из списка сертификатов. Аналогом действия данной кнопки служит двойной клик на требуемом сертификате в списке сертификатов (Рис.5.6).


Рис.5.6

см.п.7.4 «Просмотр детальной информации о сертификате»

- Кнопка «*Отозвать/приостановить сертификат*» позволяет сгенерировать для Удостоверяющего центра запрос на отзыв сертификата в случаях, когда пользователь считает, что дальнейшее использование сертификата небезопасно или есть необходимость временно приостановить действие сертификата (Рис.5.7).


Рис.5.7

см. п.6.6 «Приостановление действия сертификата».
см. п.6.8 «Аннулирование действия сертификата».

- Кнопка «*Возобновить сертификат*» позволяет возобновить действие временно приостановленного сертификата (Рис.5.8).


Рис.5.8

см. п.6.7 «Возобновление действия сертификата».

- Кнопка «*Получить сертификат*» позволяет возобновить процесс получения последующего сертификата. Аналогом действия данной кнопки служит клик правой кнопкой мыши на требуемом запросе на сертификат в списке сертификатов «*Ваши сертификаты*» (Рис.5.9).


Рис.5.9

см. п.6.4 «Контекстное меню запроса на сертификат».

- Кнопка «*Установить корневые сертификаты*» позволяет установить в хранилище сертификатов операционной системы сертификаты корневых центров сертификации. Данная процедура отрабатывается автоматически при установке программы (см. п.2.3). Но в процессе работы с сертификатами требуемые сертификаты корневых центров сертификации по различным причинам могут быть удалены, что приведет к неработоспособности системы управления сертификатами. Используя данный функционал, пользователь может самостоятельно скачать и установить в хранилище системы требуемые сертификаты (Рис.5.10).

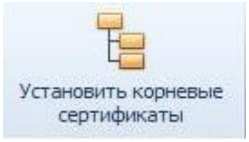



Рис.5.10

- Кнопка «*О программе*» позволяет ознакомиться с информацией о производителе программы (Рис.5.11).

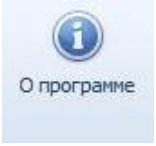



Рис.5.11

## 5.2. Блок управления ключевыми носителями (токенами)

Блок управления ключевыми носителями (красный прямоугольник, Рис.5.1) содержит функционал для работы с токенами:

- Поле с выпадающим списком отображает все ключевые носители, подключенные в текущий момент к компьютеру. Здесь пользователь может выбрать тот носитель, с которым ему необходимо работать. При выборе того или иного ключевого носителя содержимое области отображения списка сертификатов автоматически обновляется. Активным считается носитель, отображаемый непосредственно в поле на форме. Зеленым цветом отображается имя выбранного токена (Рис.5.12).

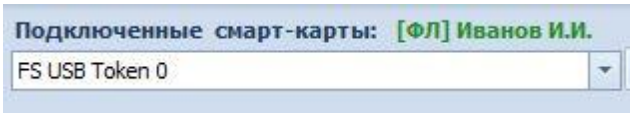



Рис.5.12

- Кнопка «*Обновить*» позволяет обновить список подключенных ключевых носителей. Необходимость в этом может возникнуть, когда пользователь вынимает какой–либо носитель из USB–разъема компьютера и вместо него подключает другой (Рис.5.13).

Рис.5.13

- Кнопка «*Перечитать смарт–карту*» обновляет список в области отображения сертификатов и запросов на получение сертификатов, т.е. отображает все сертификаты и запросы, ассоциированные с выбранным ключевым носителем.

- Кнопка «*Получить серийный номер карты*» позволяет узнать серийный номер ключевого носителя (токена) (Рис.5.14).

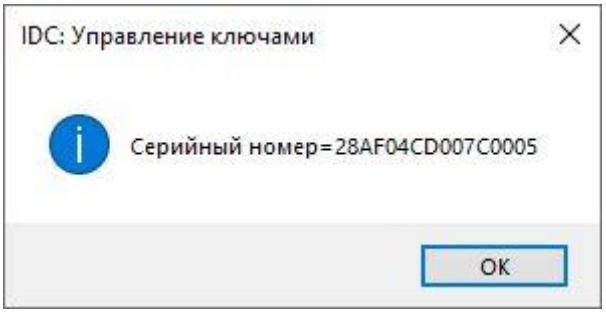



Рис.5.14

- Кнопка «*Сменить PIN-код карты*» позволяет установить новый PIN-код для доступа к ключевому носителю (токена).

  см. п.7.2 «Смена ПИН-кода».

## 5.3. Область отображения списка сертификатов

Область отображения списка сертификатов (зеленый прямоугольник, Рис.5.1), хранящихся на выбранном ключевом носителе, либо запросов на получение сертификатов в Удостоверяющем центре, ожидающих подтверждения, представляют собой таблицу. Данная таблица имеет следующие колонки:

- *Статус сертификата*. Отображает, в каком состоянии находится сертификат или запрос на его получение.

  Статус «*Запрос*» означает, что программой была сгенерирована пара открытого и закрытого ключей, записана на ключевой носитель, сгенерирован запрос для Удостоверяющего центра на получение сертификата открытого ключа и этот запрос был отправлен в Удостоверяющий центр. В текущий момент запрос находится в стадии ожидания ответа от Удостоверяющего центра (Рис.5.15).


Рис.5.15

Статус «*Сертификат выдан*» показывает, что для пары ключей Удостоверяющим центром выдан сертификат, и он в текущий момент действующий (Рис. 5.16).

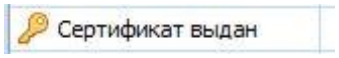



Рис.5.16

Статус «*Сертификат отозван*» говорит о том, что по какой–либо причине, возможно, самим пользователем, сертификат был отозван и включен в список отозванных сертификатов. Дальнейшее его использование невозможно (Рис. 5.17).

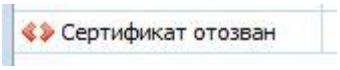



Рис.5.17

Статус «*Запрос отклонен*» говорит о том, что по какой–либо причине запрос на изготовление сертификата открытого ключа был отклонен Удостоверяющим центром (Рис. 5.18).

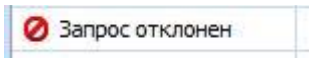



Рис.5.18

- *На карте*. Отображает пиктограмму в виде носителя информации, если копия сертификата содержится на ключевом носителе, выбранном для работы из списка подключенных смарт-карт (Рис. 5.19).

Рис.5.19

- *ИД запроса*. Отображает уникальный идентификатор запроса на получение сертификата открытого ключа в Удостоверяющем центре.

- *Кому выдан.* Отображает ФИО пользователя Удостоверяющего центра, на имя которого регистрируются запросы на выпуск сертификата и выпускаются сертификаты Удостоверяющим центром.

- *Серийный номер*. Отображает серийный номер сертификата, выпущенный Удостоверяющим центром.

- *Начало действия*. Отображает дату выдачи сертификата.

- *Окончание действия*. Отображает дату, до которой сертификат будет действителен, при условии, что он не будет отозван по какой-либо причине до окончания своего срока действия.

- *Субъект*. Отображает субъект, которому принадлежит сертификат: физическое лицо или организация, которую представляет сертификат:

  *E = testovich@ca.idc.md*
  *CN = Иванов Иван Иванович*
  *O = Совместное закрытое акционерное общество «Быстрая Пицца»*
  *L = Тирасполь*
  *C = MD*

- *Тип устройства.* Отображается тип и модель устройства, на которое осуществлялась запись ключей при генерации ключевой пары. Возможные значения:

  – ПК токен (<модель токена>);
  – Android устройство (<модель устройства>);
  – IOS устройство (<модель устройства>).

- *Наименование устройства.* Отображается наименование устройства (ПК или мобильного), на котором производилась генерация ключевой пары.

- *Серийный номер токена*. Отображается серийный номер ключевого носителя (токена) с помощью которого формировались открытый, закрытый ключи и запрос на сертификат открытого ключа в Удостоверяющий центр.

- *Специальный*. Отображается правовой статус владельца сертификата. Возможные значения:

  – Нотариус;

  – Частный нотариус;

  – Судебный исполнитель;

  – Следователь, дознаватель;

  – Налоговый инспектор.

### 5.4. Область отображения технической информации

В данной области отображается детальная информация о работе программы, по которой можно сделать вывод об успешности или не успешности выполнения той или иной запрошенной операции или действия (розовый прямоугольник, Рис.5.1).

## 6. Сертификат

Сертификат электронной подписи - это электронный документ, который подтверждает подлинность открытого ключа и связывает его с владельцем. Это официальное свидетельство, которое гарантирует, что подпись принадлежит конкретному человеку. Подлинность электронной подписи при ее использовании проверятся с помощью сертификата. Сертификат выдается Удостоверяющим центром и содержит информацию о владельце, сроке действия, статусе сертификата и другие данные (см. Регламент Удостоверяющего центра, Приложение №1 п.7, Приложение №2).

### 6.1. Выпуск первого сертификата

В соответствии с пунктом 4.8.6 Регламента Удостоверяющего центра, зарегистрированный пользователь может получить первый сертификат в течение двух месяцев после оплаты услуг по созданию и выдаче сертификата открытого ключа электронной подписи. За десять дней до истечения этого срока, Вы получите уведомление на Вашу электронную почту и телефон. По истечении указанного срока, выпуск первого сертификата возможен только после повторной оплаты услуг Удостоверяющего центра.

Для получения первого сертификата следуйте инструкциям п.6.3 «Создание запроса на сертификат».

### 6.2. Выпуск последующего сертификата

Рекомендуется использовать программу «IDC Управление ключами» для выпуска нового сертификата, если у Вас уже есть хотя бы один действующий сертификат.

За десять дней до завершения действия сертификата, Вы получите уведомление на Вашу электронную почту и телефон.

После истечения срока действия последнего действующего сертификата, новый сертификат можно будет выпустить только после посещения представителя Удостоверяющего центра.

Не следует выпускать новый сертификат, если Ваши данные в информационной системе Удостоверяющего центра требуют обновления. В этом случае Вам следует обратиться к представителю Удостоверяющего центра для внесения необходимых изменений.

Для получения нового сертификата следуйте инструкциям п.6.3 «Создание запроса на сертификат».

6.3. Создание запроса на сертификат

- Подключите токен (смарт-карту) к USB-разъему компьютера. Убедитесь, что в главном окне программы в поле «Подключенные смарт-карты» отображается модель токена и имя, которое Вы ему присвоили (см.п.5.2, Рис.5.12).

- Для создания запроса на получение сертификата открытого ключа необходимо нажать на кнопку меню «Создать запрос на сертификат» (см.п.5.1). Откроется форма «Создание запроса на сертификат» (Рис. 6.1).

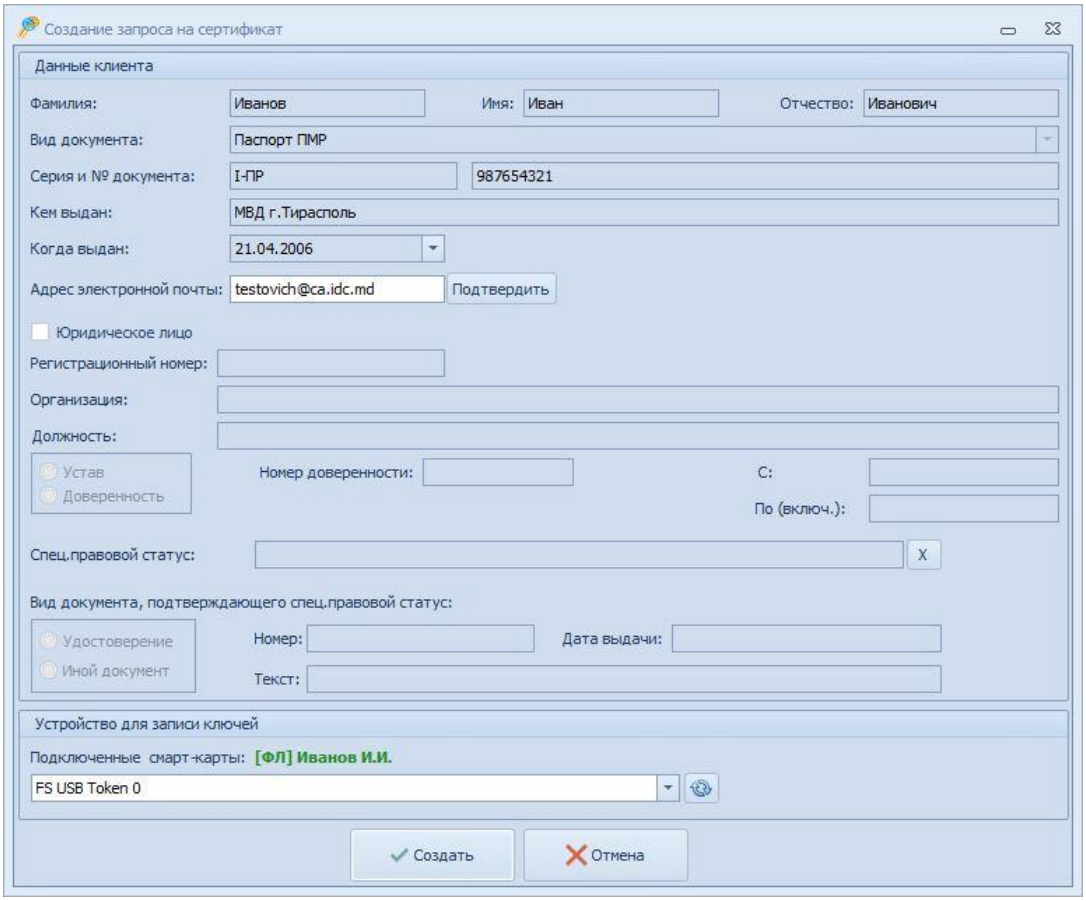



Рис. 6.1

По умолчанию, программа автоматически выбирает токен, который указан в поле «Подключенные смарт-карты» на главной форме программы (см.п.5.2). При необходимости Вы можете выбрать любой токен из списка доступных.

Поле «Адрес электронной почты» можно изменить. Этот адрес будет указан в вашем сертификате.

Все остальные поля доступны только для просмотра. В них отображаются Ваши регистрационные данные, внесенные в информационную систему Удостоверяющего центра. Если вы заметили неточности или ошибки в этих данных, нажмите кнопку «Отмена» и свяжитесь с Удостоверяющим центром для их актуализации.

- Введите Ваш адрес электронной почты в поле «Адрес электронной почты» на форме и нажмите кнопку «Подтвердить». Откроется окно «Подтверждение адреса электронной почты» (Рис. 6.2).

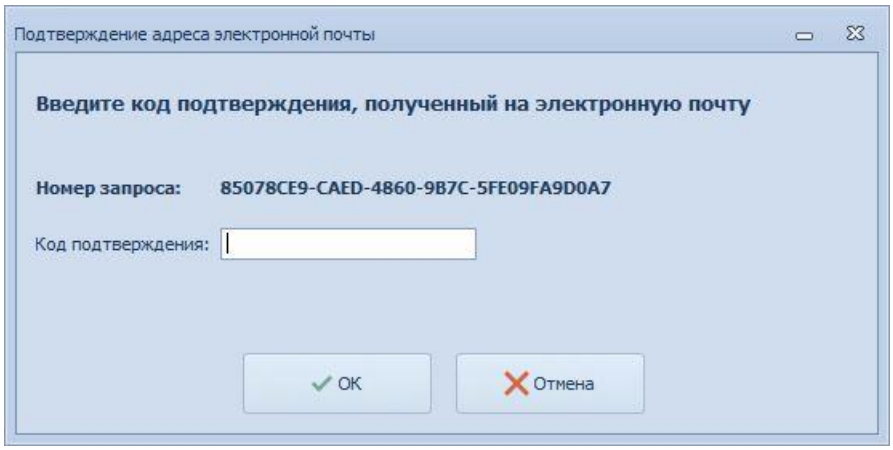



Рис. 6.2

На Ваш адрес электронной почты Удостоверяющий центр отправит письмо с проверочным кодом (см. Рис. 6.3).

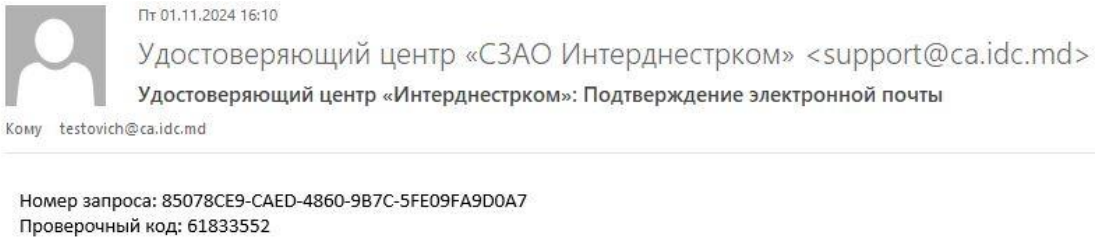



Рис. 6.3

Скопируйте значение проверочного кода из письма в поле «Код подтверждения» формы «Подтверждение адреса электронной почты» и нажмите кнопку «Ок». В окне «Создание запроса на сертификат» напротив кнопки «Подтвердить» появится запись «Адрес электронной почты подтвержден» (Рис. 6.4).

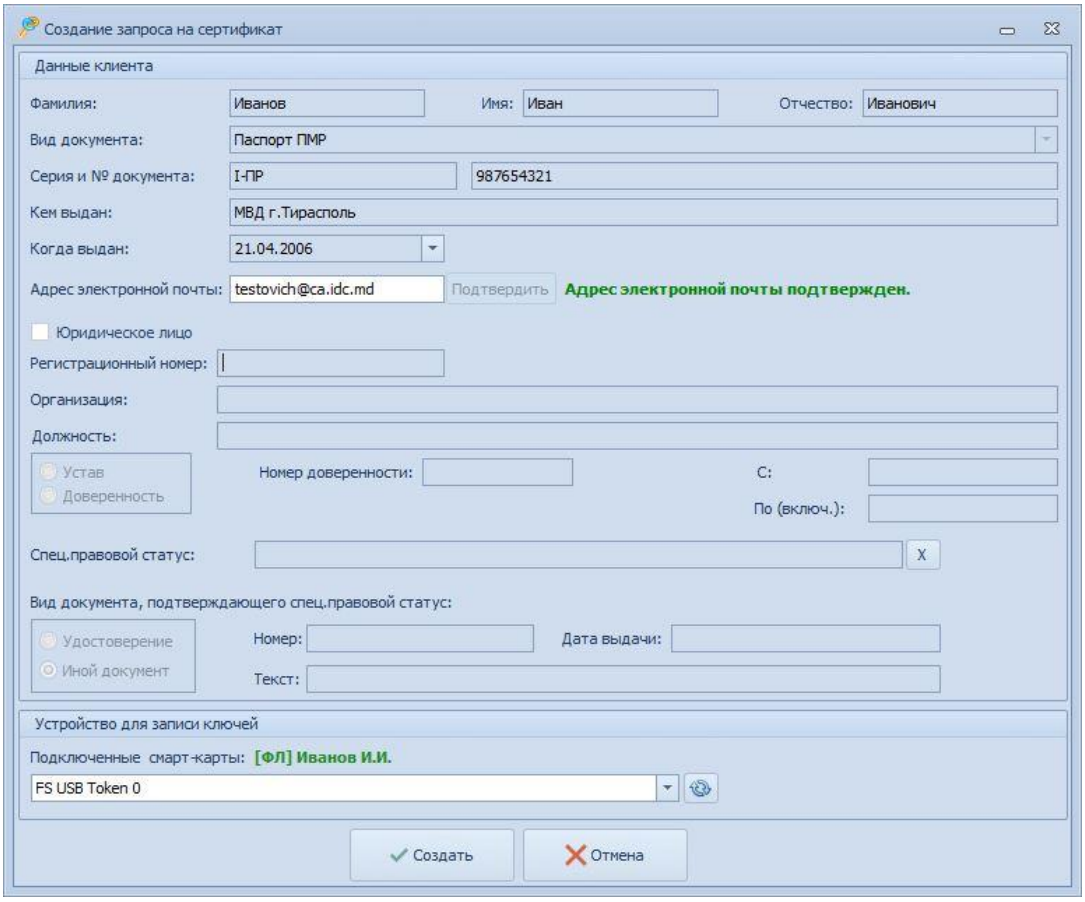



Рис. 6.4

- Нажмите кнопку «Создать». Откроется форма «Смарт-карта» (Рис. 6.5).

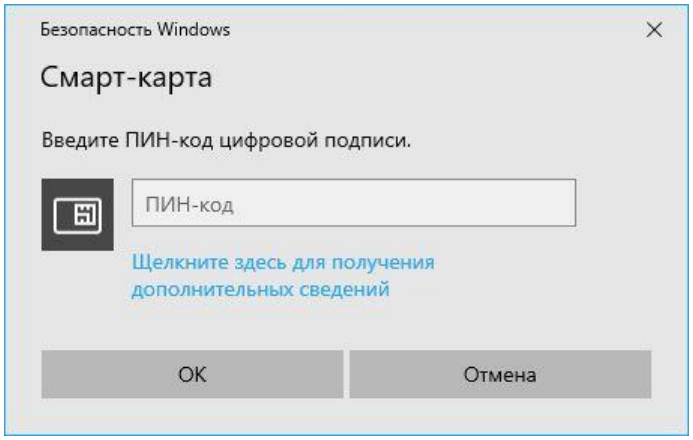



Рис. 6.5

Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос на создание ключевой пары в токене.

Во время генерации и сохранения ключевой пары программное обеспечение токена показывает в правом нижнем углу экрана всплывающие окна с уведомлениями о ходе выполнения операции (Рис.6.6).

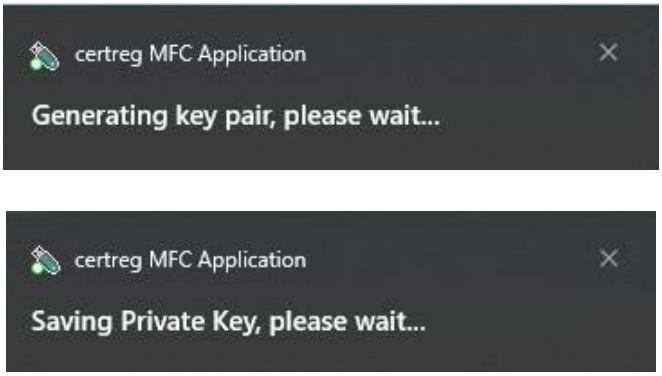



Рис. 6.6

Программа использует ключевую пару для формирования запроса на сертификат электронной подписи и отправляет этот запрос в информационную систему Удостоверяющего центра. В главном окне программы, в области списка сертификатов «Ваши сертификаты» появится новая строка со статусом «Запрос» (Рис.6.7).

Все действия программы, связанные с формированием запроса на сертификат, фиксируются в журнале и отображаются в соответствующей области главного окна программы (Рис.6.7).

- *Первый сертификат* выдается немедленно и статус «Запрос» меняется на статус «Сертификат выдан» (Рис.6.7).

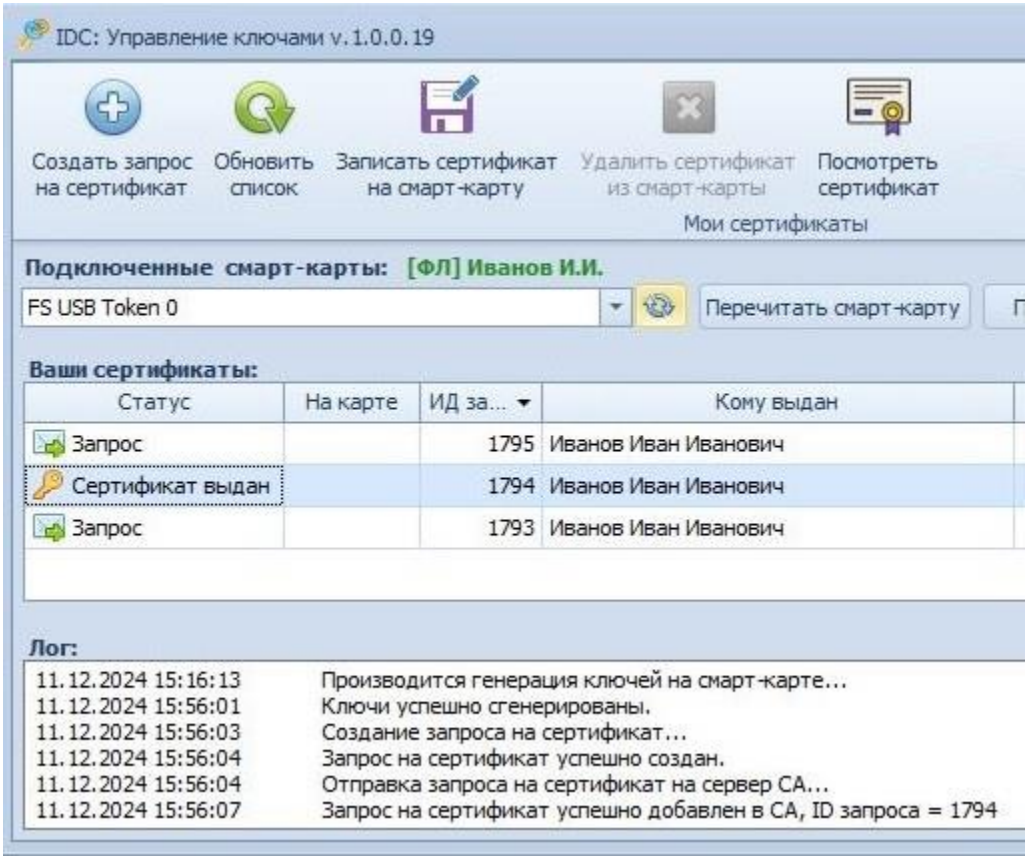
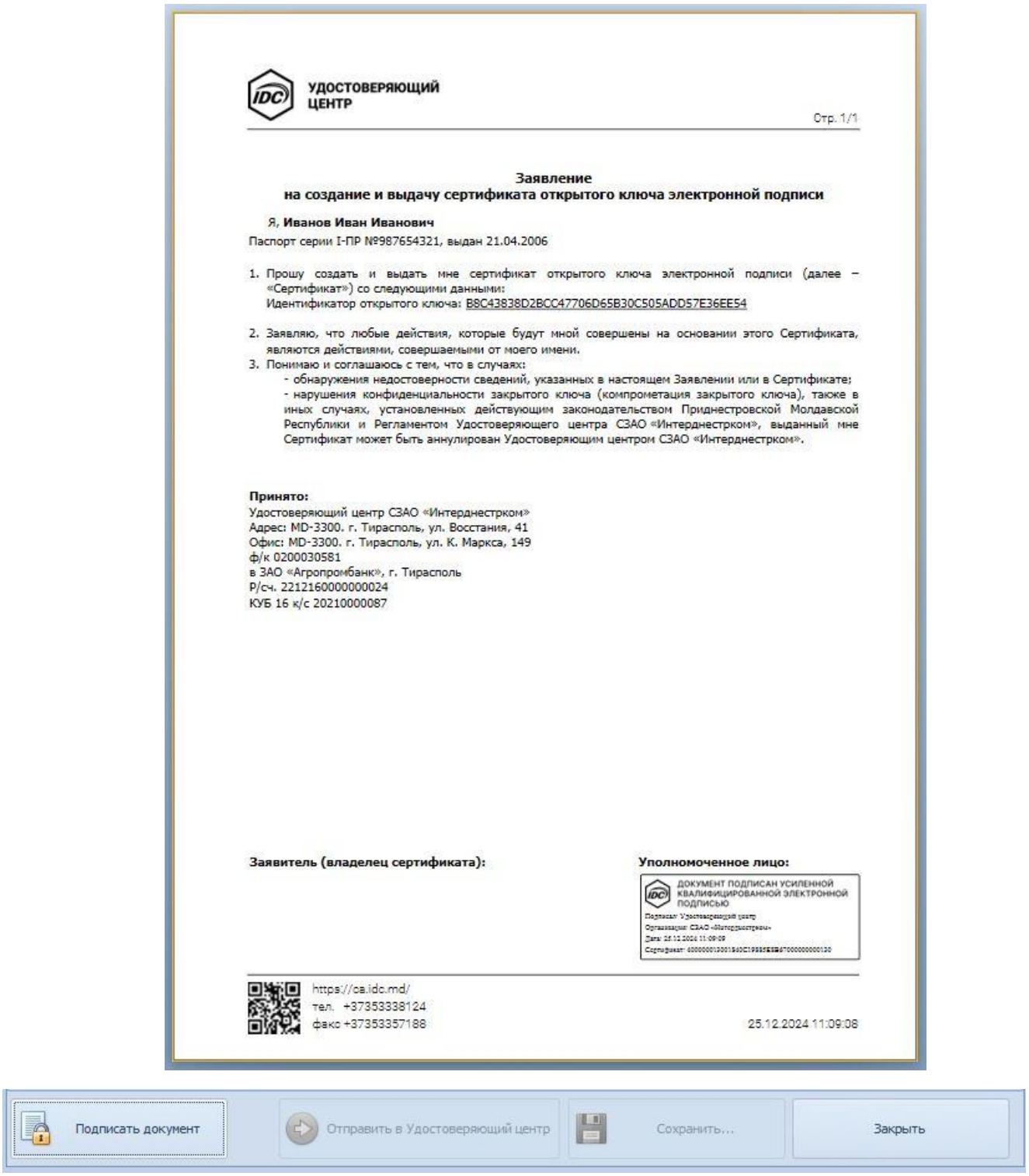



Рис. 6.7

Сохраните сертификат на ключевой носитель (токен). Для этого выполните шаги, описанные в пункте 6.5 «Запись сертификата на ключевой носитель».

- *Последующий сертификат* выдается после выполнения следующих шагов:

  В ответ на Ваш запрос на сертификат, информационная система Удостоверяющего центра формирует и отображает на экране отдельную форму с заявлением на создание и выдачу сертификата открытого ключа электронной подписи, подписанным уполномоченным лицом Удостоверяющего центра электронной цифровой подписью. (Рис.6.8).



УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Отр. 1/1

**Заявление**
**на создание и выдачу сертификата открытого ключа электронной подписи**

Я, **Иванов Иван Иванович**
Паспорт серии I-ПР №987654321, выдан 21.04.2006

1. Прошу создать и выдать мне сертификат открытого ключа электронной подписи (далее – «Сертификат») со следующими данными:
   Идентификатор открытого ключа: B8C43838D2BCC47706D65B30C505ADD57E36EE54
2. Заявляю, что любые действия, которые будут мной совершены на основании этого Сертификата, являются действиями, совершаемыми от моего имени.
3. Понимаю и соглашаюсь с тем, что в случаях:
   - обнаружения недостоверности сведений, указанных в настоящем Заявлении или в Сертификате;
   - нарушения конфиденциальности закрытого ключа (компрометация закрытого ключа), также в иных случаях, установленных действующим законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра СЗАО «Интерднестром», выданный мне Сертификат может быть аннулирован Удостоверяющим центром СЗАО «Интерднестром».

**Принято:**
Удостоверяющий центр СЗАО «Интерднестром»
Адрес: MD-3300. г. Тирасполь, ул. Восстания, 41
Офис: MD-3300. г. Тирасполь, ул. К. Маркса, 149
ф/к 0200030581
в ЗАО «Агропромбанк», г. Тирасполь
Р/сч. 2212160000000024
КУБ 16 к/с 20210000087

**Заявитель (владелец сертификата):**

**Уполномоченное лицо:**

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

https://ca.idc.md/
тел. +37353338124
факс +37353357188

25.12.2024 11:09:08



Рис. 6.8

Бланк заявления на создание и выдачу сертификата открытого ключа электронной подписи представлен в приложении №3м к Регламенту Удостоверяющего центра.

Заявление связано с запросом на сертификат и доступно из контекстного меню области списка сертификатов «Ваши сертификаты» до момента его подписания и отправки в информационную систему Удостоверяющего центра (см. п.6.4 «Контекстное меню запроса на сертификат»).

Нажмите кнопку «Подписать документ». Откроется окно со списком сертификатов, доступных для подписания заявления. Выберите сертификат из списка, если их несколько, и нажмите кнопку «Ок». Если у Вас есть только один доступный сертификат, просто нажмите кнопку «Ок». (Рис.6.9).

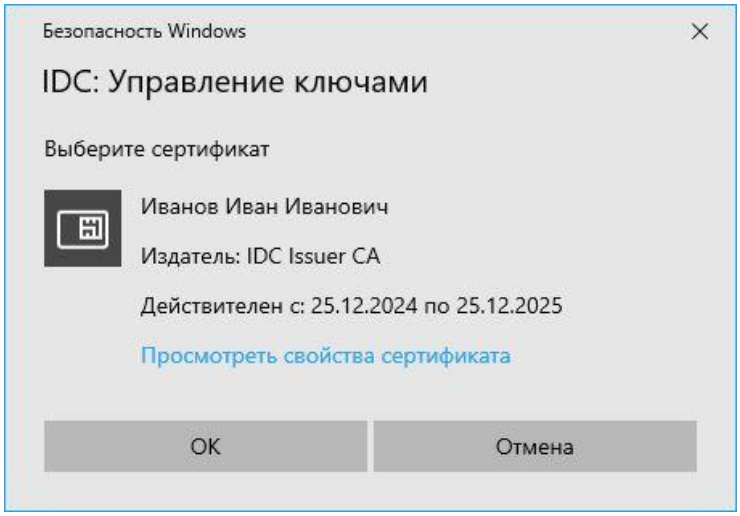



Рис. 6.9

Откроется форма «Смарт-карта» (Рис.6.10). Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос в токен на выполнение операции подписания заявления Вашей электронной цифровой подписью.

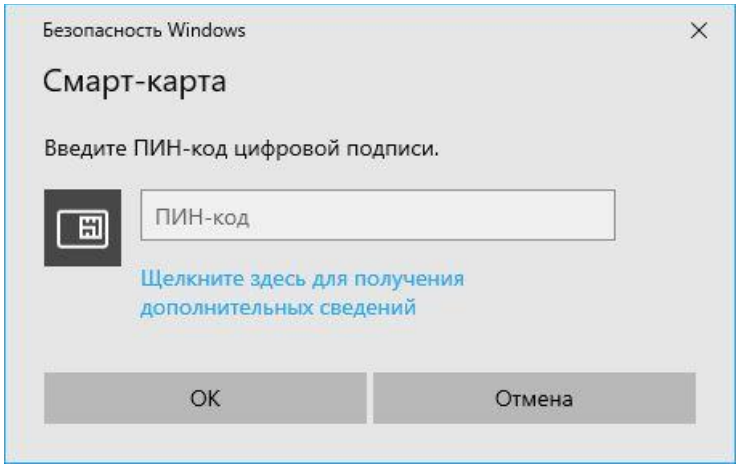



Рис. 6.10

В области «Заявитель (владелец сертификата)» на заявлении будет проставлен штамп с данными вашей электронной цифровой подписи.

В нижней части формы, справа от кнопки «Подписать документ», появится надпись: «Документ подписан» (Рис.6.11).

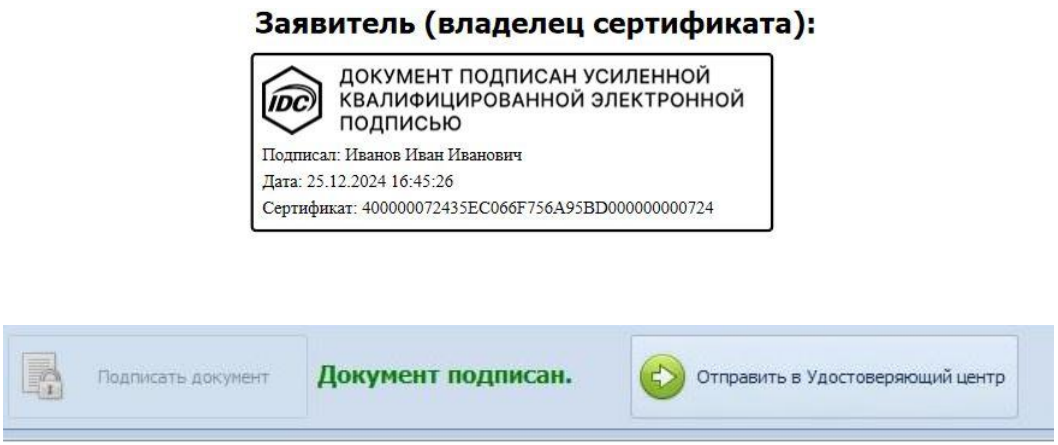



Рис. 6.11

Нажмите кнопку «Отправить в Удостоверяющий центр», чтобы отправить подписанное заявление в информационную систему Удостоверяющего центра.

Откроется форма с счетом на оплату услуги по созданию и выдаче сертификата открытого ключа электронной подписи (Рис.6.12).

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Отр. 1/1

СЗАО "ИНТЕРДНЕСТРКОМ"
MD-3300, г. Тирасполь, ул. Восстания 41
Тел.: 1198, факс: +(373533) 57711
Р/сч 2212160000000024
ЗАО «Агропромбанк» г. Тирасполь, КУБ 16
ф/к 0200030581, Кор.сч. 20210000087

**Счет № 8877760**

Выставлен: 26.12.2024 16:23:25
**Оплатить до: 29.12.2024**
Плательщик: Иванов Иван Иванович

| Наименование | Цена | Скидка в % | Цена со скидкой | Кол-во | Сумма |
|---|---|---|---|---|---|
| Выдача сертификата открытого ключа электронной подписи сроком действия 1 год для физических лиц | 49.00 | | | 1 | 49.00 |

**Итого к оплате:** **49.00**

Сумма прописью: сорок девять рублей 00 копеек

**Начальник УБУиО - главный бухгалтер** /Здановский А.Л./

https://ca.idc.md/
тел. +37353338124
факс +37353357188

26.12.2024 16:23:25


Рис. 6.12

Сформированный счет связан с запросом на сертификат и доступен из контекстного меню области списка сертификатов «Ваши сертификаты» до момента оплаты счета (см. п.6.4 «Контекстное меню запроса на сертификат»).

Чтобы сохранить копию заявления и/или счета на Вашем устройстве для дальнейшего использования (например, для печати), нажмите кнопку «Сохранить…», которая находится в нижней части формы с документом (Рис.6.12). Заявление можно сохранить только после того как Вы подпишете его цифровой электронной подписью и отправите в Удостоверяющий центр.

После оплаты счета, сертификат будет выдан в течении одной минуты. В главном окне программы, в области списка сертификатов «Ваши сертификаты» строка со статусом «Запрос» изменит свое значение на «Сертификат выдан». (Рис.6.13).

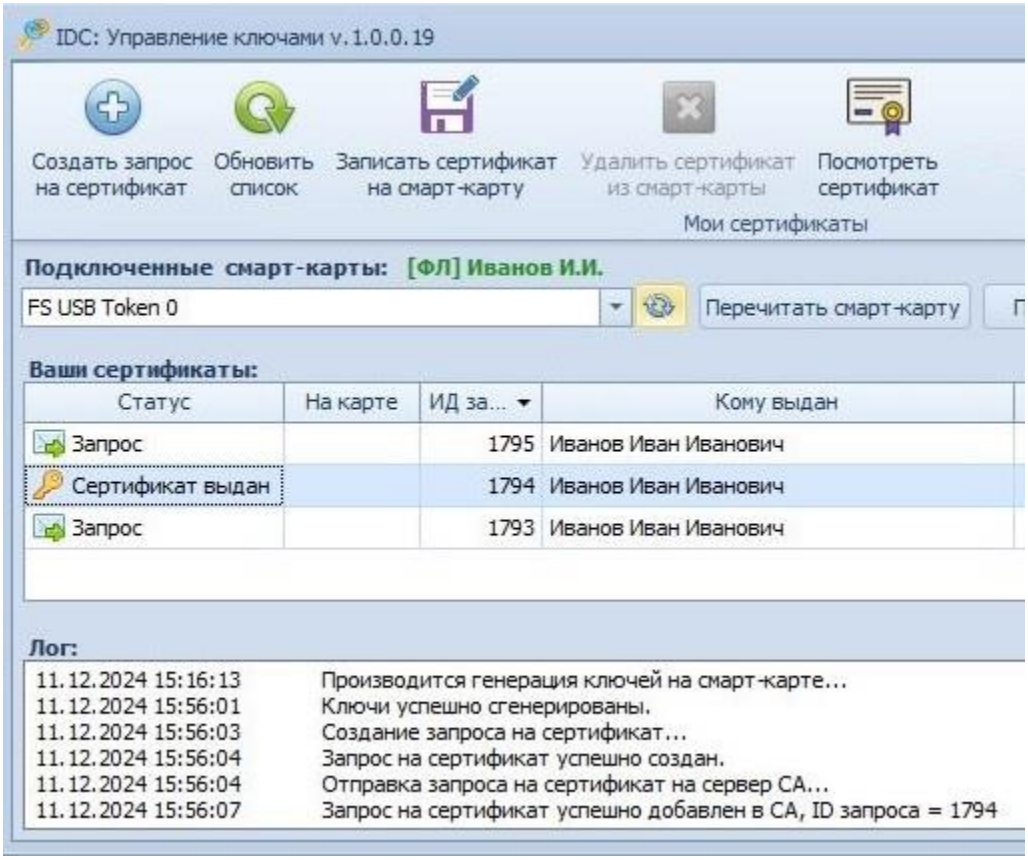



Рис.6.13

Сохраните сертификат на ключевой носитель (токен). Для этого выполните шаги, описанные в пункте 6.5 «Запись сертификата на ключевой носитель».

## 6.4. Контекстное меню запроса на сертификат

В главном окне программы, в области списка сертификатов «Ваши сертификаты» для выбранного запроса на сертификат доступно контекстное меню с пунктом меню - «Получить сертификат» (Рис.6.14).

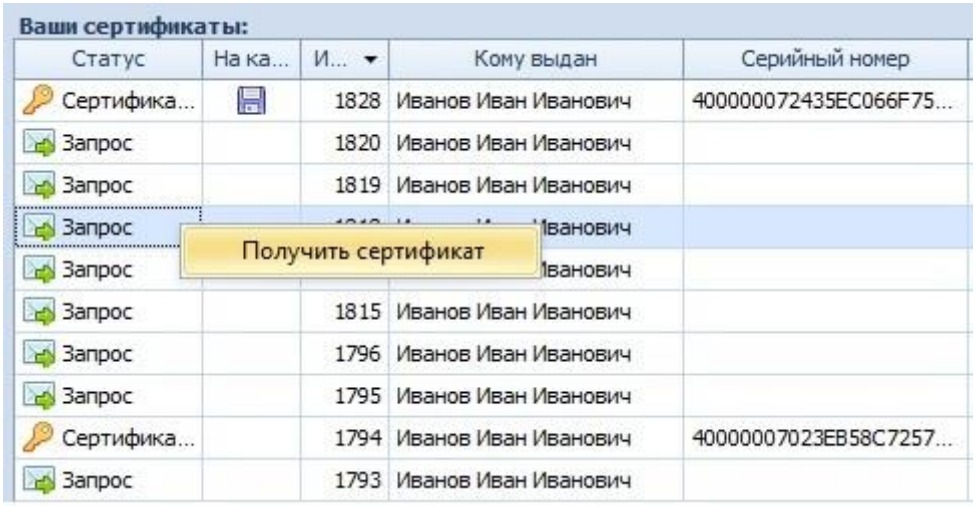



Рис. 6.14

Контекстное меню позволяет Вам возобновить выпуск последующего сертификата.

В процессе выпуска сертификата, Вам необходимо подписать заявление на создание и выдачу сертификата действующим сертификатом и отправить его в Удостоверяющий центр. Контекстное меню позволяет получить доступ к заявлению до момента его отправки в Удостоверяющий центр. Вы можете сохранить подписанную копию заявления на Ваше устройство (Рис.6.8).

Контекстное меню позволяет получить доступ к счету на оплату услуги по созданию и выдаче сертификата, только после отправки заявления на создание и выдачу сертификата в Удостоверяющий центр и до момента оплаты счета. Вы можете сохранить подписанную копию счета на Ваше устройство (Рис.6.12).

Нажмите кнопку «Получить сертификат» чтобы возобновить выпуск последующего сертификата. В зависимости от того, на каком шаге была прервана процедура получения последующего сертификата, информационная система Удостоверяющего центра откроет форму с заявлением на создание и выдачу сертификата либо форму со счетом на оплату услуги по созданию и выдаче сертификата.

Следуйте инструкциям, представленным в п.6.3 «Создание запроса на сертификат» - получение последующего сертификата.

## 6.5. Запись сертификата на ключевой носитель

Чтобы использовать токен для работы с электронной подписью на любом устройстве, необходимо, чтобы сертификат открытого ключа электронной подписи находился в том же контейнере на токене, что и ключевая пара (открытый и закрытый ключи).

Для записи сертификата на носитель (токен):

- Выберите токен из выпадающего списка «Подключенные смарт-карты» (Рис.6.15).

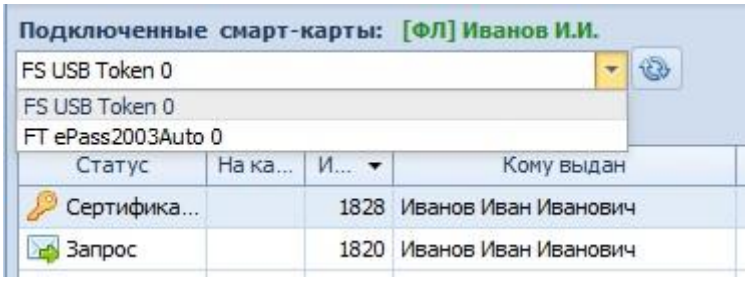



Рис. 6.15

*Внимание! При записи сертификата в качестве активного ключевого носителя должен быть выбран тот носитель, который был активен при подаче запроса на получение сертификата. В противном случае запись сертификата на носитель не будет произведена. При этом будет выдано соответствующее сообщение (Рис.6.16).*

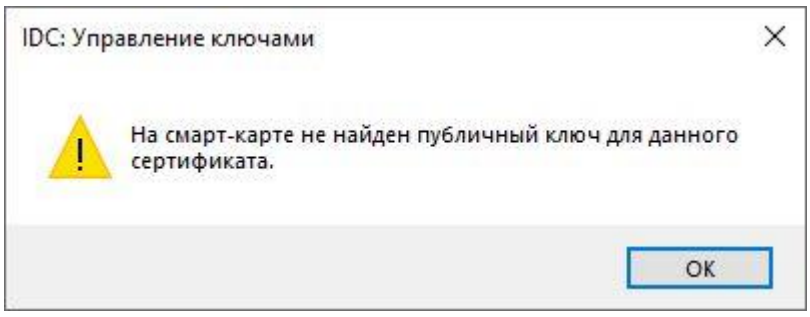



Рис. 6.16

- Выберите интересующий Вас сертификат в списке сертификатов «Ваши сертификаты» (Рис. 6.17).

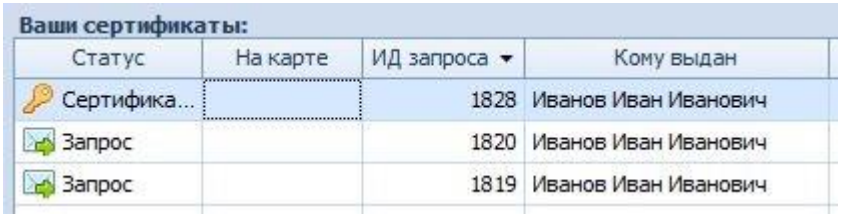



Рис. 6.17

- Нажмите кнопку меню «Записать сертификат на смарт–карту» (Рис.6.18).

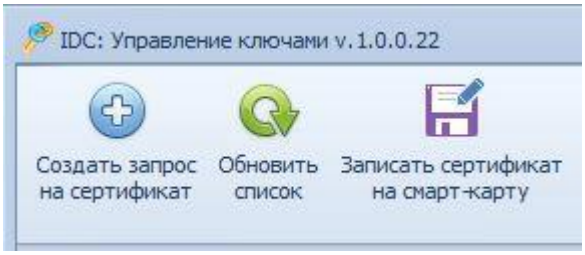



Рис. 6.18

- Нажмите кнопку «Да» чтобы подтвердить операцию записи сертификата на токен (Рис.6.19).

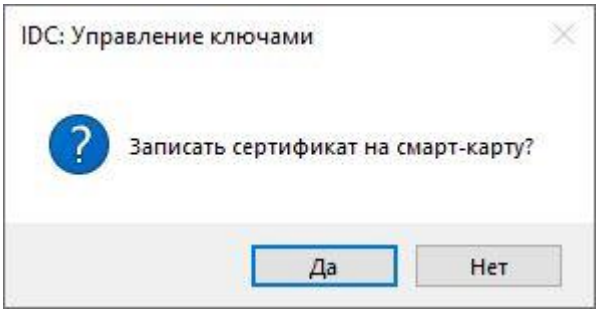



Рис. 6.19

- Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос в токен на выполнение операции записи сертификата в хранилище токена (Рис.6.20).

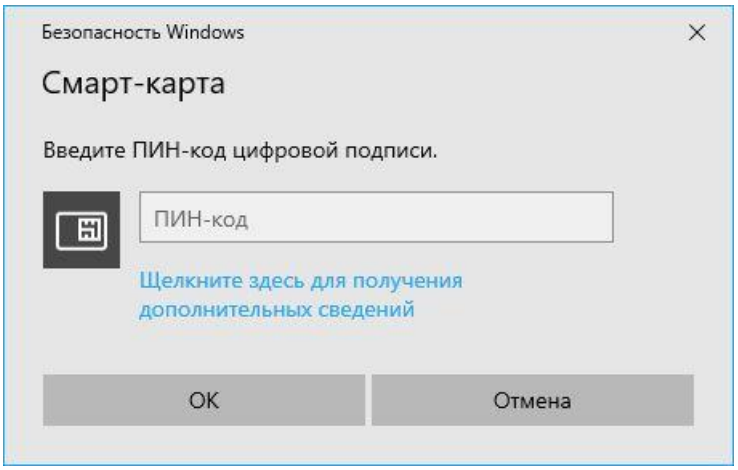



Рис. 6.20

- Программное обеспечение токена покажет в правом нижнем углу экрана всплывающее окно с уведомлением о том, что сертификат успешно сохранен в хранилище токена (Рис.6.21).

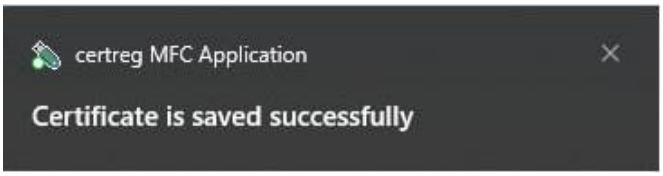



Рис. 6.21

- Нажмите кнопку «Ок» чтобы закрыть окно с сообщением (Рис.6.22).

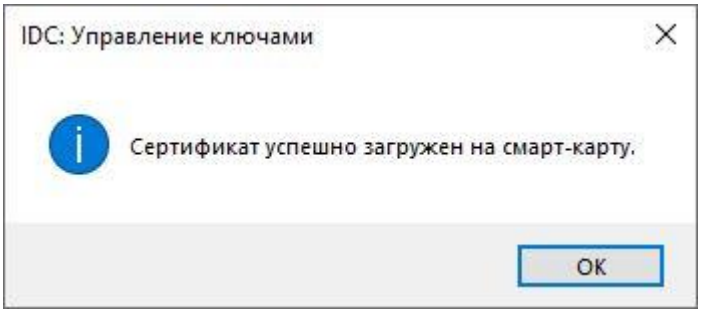



Рис. 6.22

- В списке сертификатов «Ваши сертификаты» в колонке «На карте» будет отображена пиктограмма (Рис.6.23).

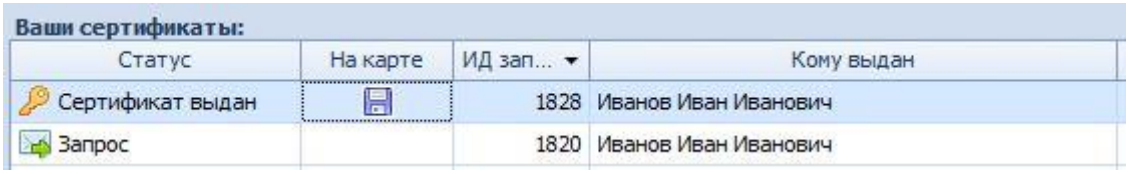



Рис. 6.23

## 6.6. Приостановление действия сертификата

Приостановление сертификата рекомендуется в случае возникновения угрозы компрометации закрытого ключа, возможного длительного неисполнения обязанностей.

Для приостановления действия сертификата:

- Выберите интересующий Вас сертификат из списка «Ваши сертификаты». Убедитесь в том, что в колонке «На карте» отображается пиктограмма (см. Рис.6.24).

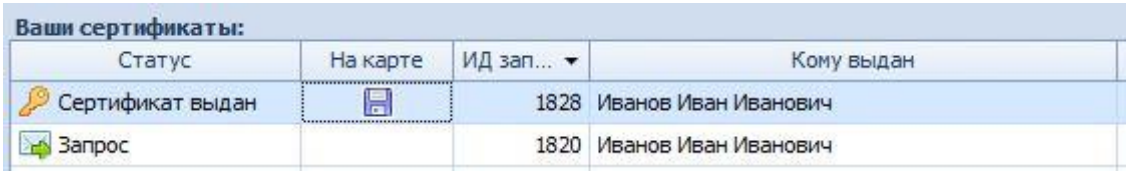



Рис. 6.24

*Внимание! Возможность приостановки действия сертификата доступна только для сертификатов, записанных на токен. Для сертификатов, не записанных на токен, будет выдано соответствующее уведомление (Рис.6.25).*

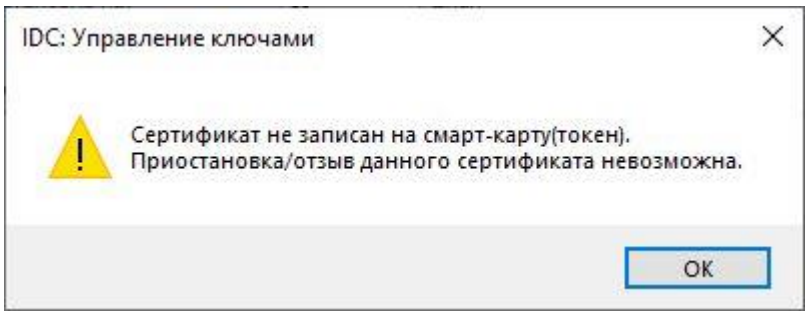



Рис. 6.25

*см. п.6.5 «Запись сертификата на ключевой носитель».*

- Нажмите кнопку меню «Отозвать/приостановить сертификат» (Рис.6.26).


Рис. 6.26

- Откроется форма «Отозвать/приостановить сертификат» (см. Рис. 6.27).

  Выберите опцию «Приостановка действия сертификата» из выпадающего списка «Причина отзыва/приостановки».

  Введите в поле «Приостановка на» количество дней, на которые Вы хотите приостановить действие сертификата. Минимальный срок приостановления составляет 10 дней (п.4.5.5 Регламента Удостоверяющего центра).

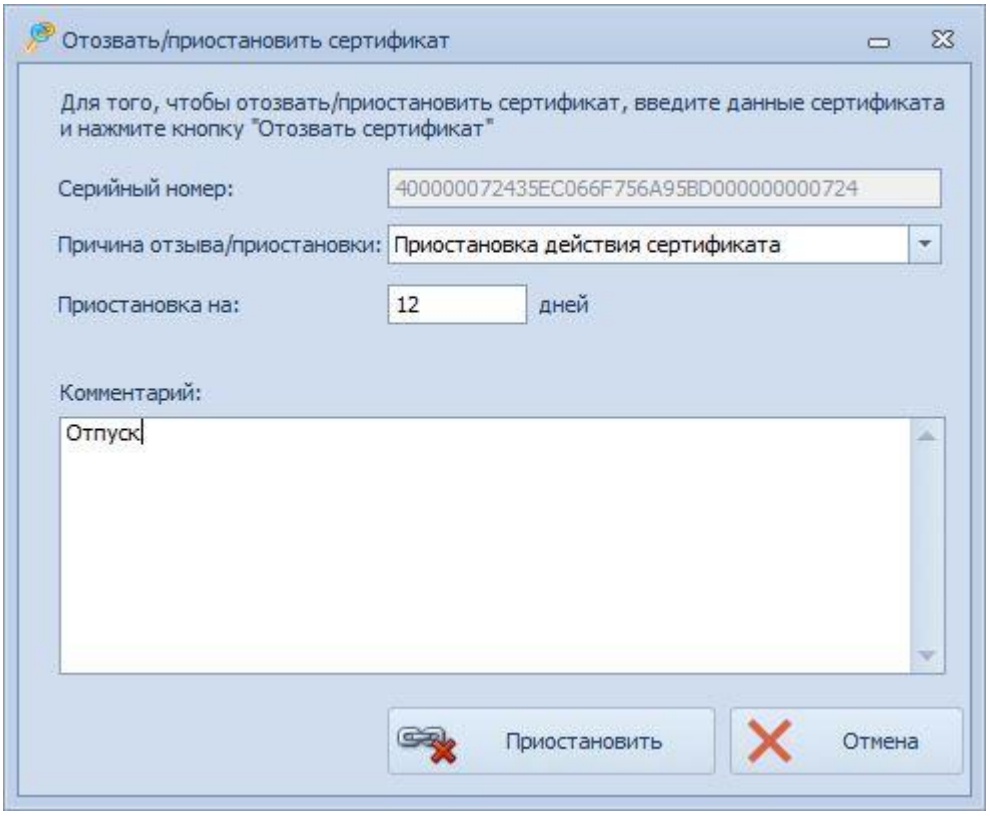
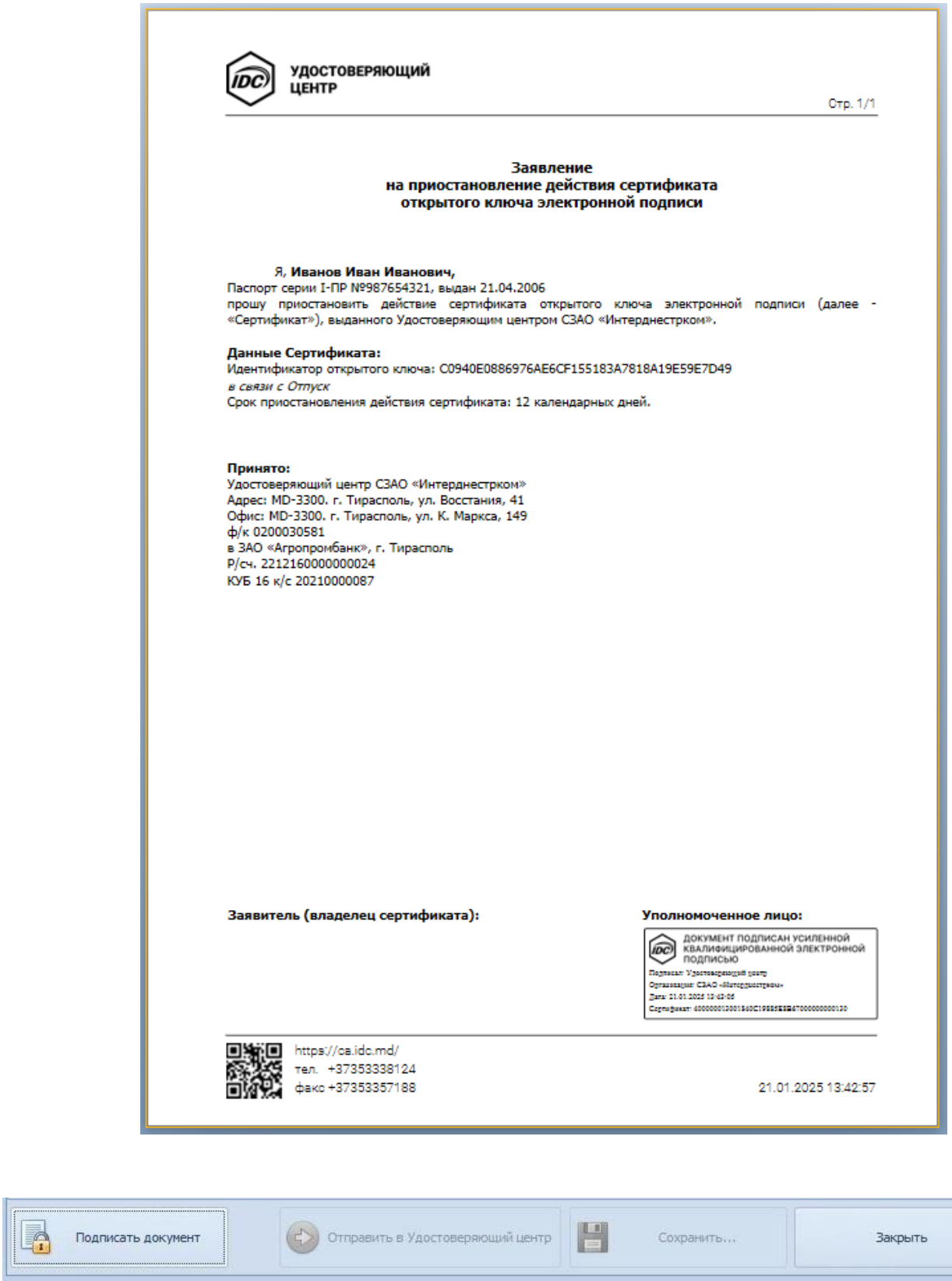



Рис. 6.27

Поле «Комментарий» не обязательно к заполнению. Вы можете оставить его пустым или, если необходимо, добавить дополнительную информацию, связанную с приостановкой действия сертификата.

Нажмите кнопку «Приостановить».

- Информационная система Удостоверяющего центра формирует и отображает на экране отдельную форму с заявлением на приостановление действия сертификата открытого ключа электронной подписи, подписанным уполномоченным лицом Удостоверяющего центра электронной цифровой подписью. (Рис.6.28).



УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Отр. 1/1

**Заявление**
**на приостановление действия сертификата**
**открытого ключа электронной подписи**

Я, **Иванов Иван Иванович,**
Паспорт серии I-ПР №987654321, выдан 21.04.2006
прошу приостановить действие сертификата открытого ключа электронной подписи (далее - «Сертификат»), выданного Удостоверяющим центром СЗАО «Интерднестрком».

**Данные Сертификата:**
Идентификатор открытого ключа: C0940E0886976AE6CF155183A7818A19E59E7D49
*в связи с Отпуск*
Срок приостановления действия сертификата: 12 календарных дней.

**Принято:**
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. г. Тирасполь, ул. Восстания, 41
Офис: MD-3300. г. Тирасполь, ул. К. Маркса, 149
ф/к 0200030581
в ЗАО «Агропромбанк», г. Тирасполь
Р/сч. 2212160000000024
КУБ 16 к/с 20210000087

**Заявитель (владелец сертификата):**

**Уполномоченное лицо:**

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

https://ca.idc.md/
тел. +37353338124
факс +37353357188

21.01.2025 13:42:57

Подписать документ | Отправить в Удостоверяющий центр | Сохранить... | Закрыть

Рис.6.28

Бланк заявления на приостановление действия сертификата открытого ключа электронной подписи представлен в приложении №3е, №3ж к Регламенту Удостоверяющего центра.

Нажмите кнопку «Подписать документ».

- Откроется окно со списком сертификатов, доступных для подписания заявления. Выберите сертификат из списка, если их несколько, и нажмите кнопку «Ок». Если у Вас есть только один доступный сертификат, просто нажмите кнопку «Ок». (Рис.6.29).

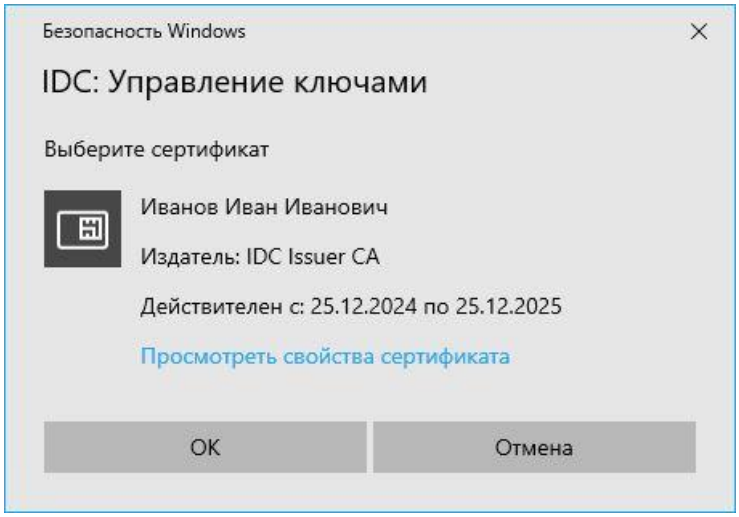



Рис.6.29

- Откроется форма «Смарт-карта» (Рис.6.30). Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос в токен на выполнение операции подписания заявления Вашей электронной цифровой подписью.

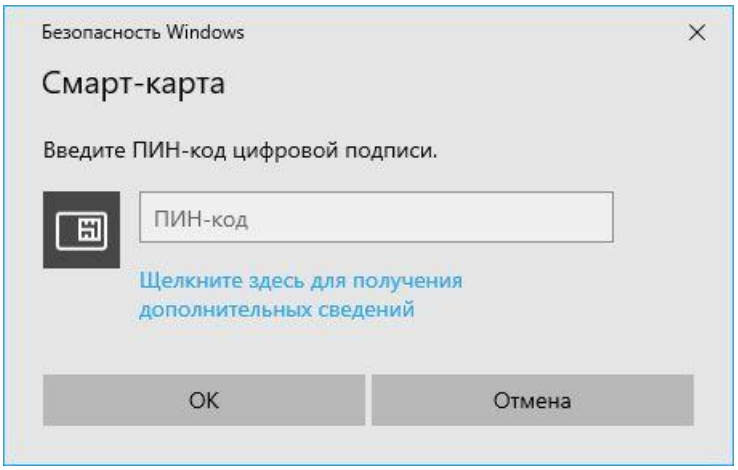



Рис.6.30

- В области «Заявитель (владелец сертификата)» на заявлении будет проставлен штамп с данными вашей электронной цифровой подписи. В нижней части формы, справа от кнопки «Подписать документ», появится надпись: «Документ подписан» (Рис.6.31).

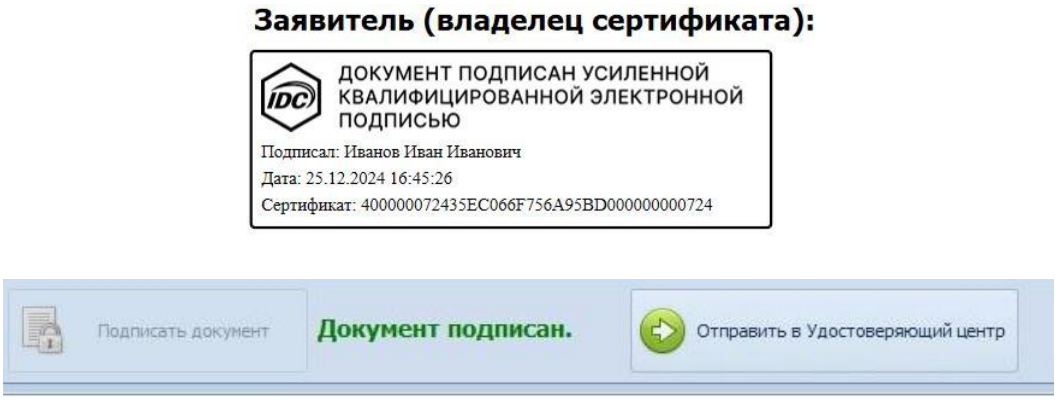



Рис. 6.31

- Нажмите кнопку «Отправить в Удостоверяющий центр», чтобы отправить подписанное заявление в информационную систему Удостоверяющего центра.
- Нажмите кнопку «Ок» чтобы закрыть окно с сообщением (Рис.6.32).

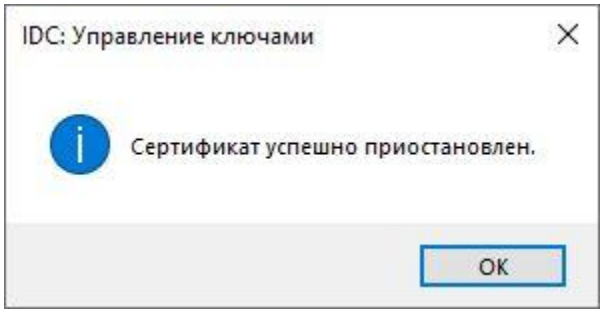



Рис. 6.32

- Чтобы сохранить копию заявления на Вашем устройстве для дальнейшего использования (например, для печати), нажмите кнопку «Сохранить…», которая находится в нижней части формы с документом (Рис.6.31). Заявление можно сохранить только после того как Вы подпишете его цифровой электронной подписью и отправите в Удостоверяющий центр.

- Статус «Сертификат выдан» меняется на статус «Сертификат приостановлен» (Рис.6.33).

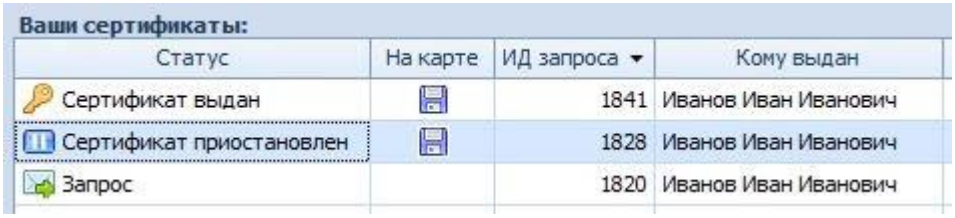



Рис. 6.33

- Возобновить действие сертификата можно в течение срока приостановления действия сертификата (см. п.6.7 «Возобновление действия сертификата»).

  По истечению срока приостановления действия сертификата, сертификат аннулируется (см. п.4.5.10 Регламента Удостоверяющего центра).

## 6.7. Возобновление действия сертификата

Возобновление действия сертификата открытого ключа электронной подписи возможно только в случае, если его действие было приостановлено.

Для возобновления действия приостановленного сертификата требуется наличие хотя бы одного действующего сертификата. Это необходимо для подтверждения подлинности и обеспечения безопасности процесса возобновления.

Для возобновления действия сертификата:

- Выберите интересующий Вас сертификат из списка «Ваши сертификаты». Убедитесь в том, что в колонке «На карте» отображается пиктограмма (см. Рис.6.34).

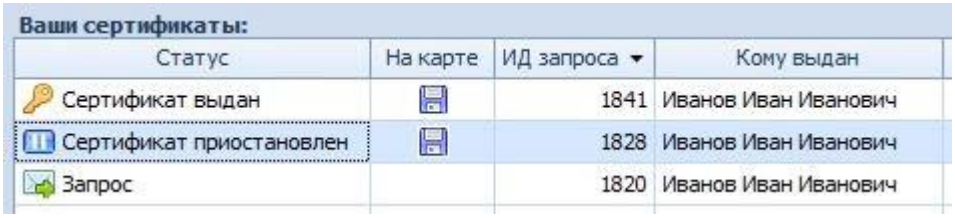



Рис. 6.34

*Внимание! Возможность возобновления действия сертификата доступна только для сертификатов, записанных на токен.*

*см. п.6.5 «Запись сертификата на ключевой носитель».*

- Нажмите кнопку меню «Возобновить сертификат» (Рис.6.35).

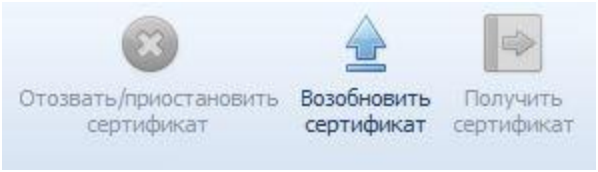
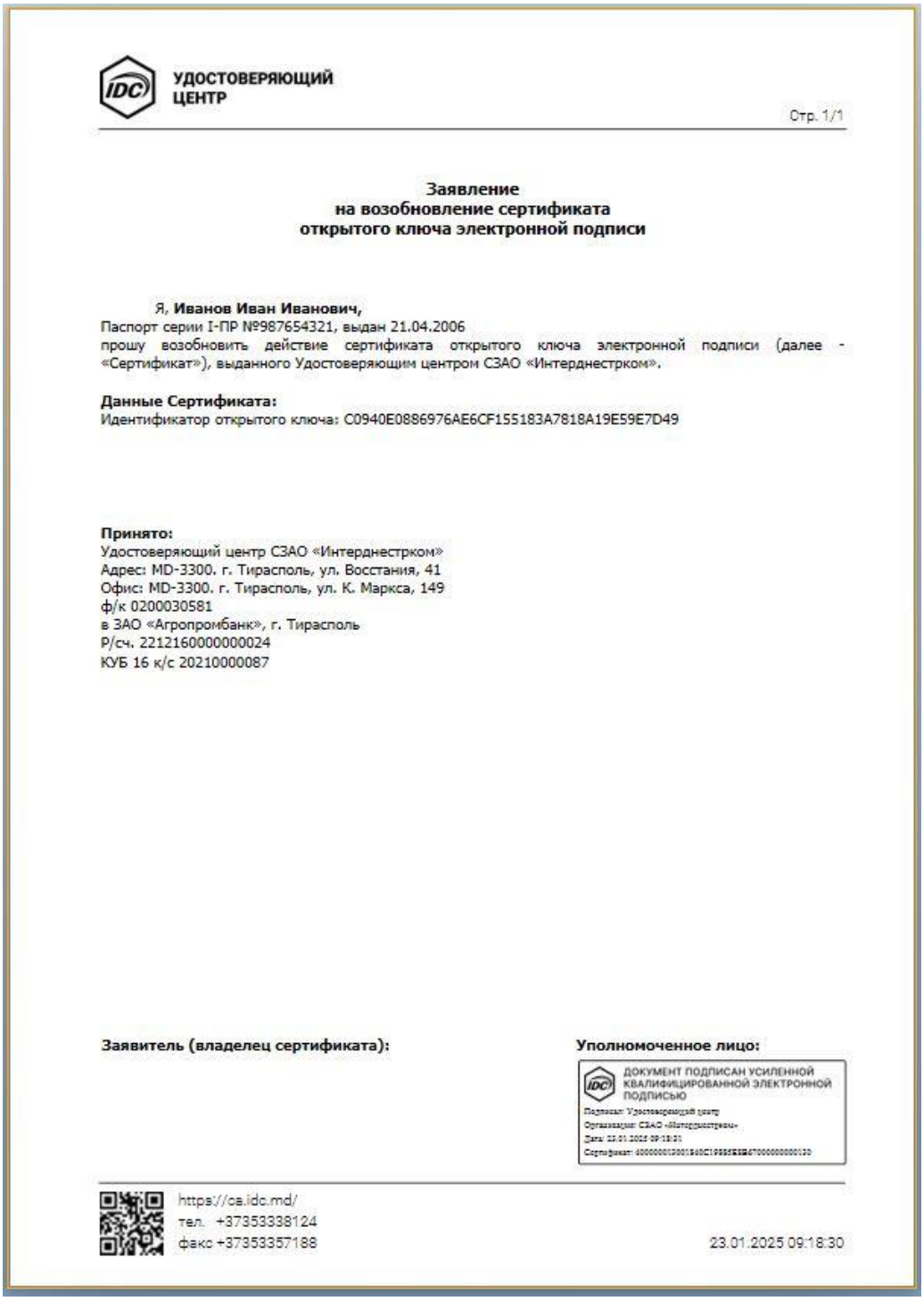



Рис. 6.35

- Информационная система Удостоверяющего центра формирует и отображает на экране отдельную форму с заявлением на возобновление действия сертификата открытого ключа электронной подписи, подписанным уполномоченным лицом Удостоверяющего центра электронной цифровой подписью. (Рис.6.36).



УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Отр. 1/1

**Заявление**
**на возобновление сертификата**
**открытого ключа электронной подписи**

Я, **Иванов Иван Иванович,**
Паспорт серии I-ПР №987654321, выдан 21.04.2006
прошу возобновить действие сертификата открытого ключа электронной подписи (далее - «Сертификат»), выданного Удостоверяющим центром СЗАО «Интерднестрком».

**Данные Сертификата:**
Идентификатор открытого ключа: C0940E0886976AE6CF155183A7818A19E59E7D49

**Принято:**
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. г. Тирасполь, ул. Восстания, 41
Офис: MD-3300. г. Тирасполь, ул. К. Маркса, 149
ф/к 0200030581
в ЗАО «Агропромбанк», г. Тирасполь
Р/сч. 2212160000000024
КУБ 16 к/с 20210000087

**Заявитель (владелец сертификата):**

**Уполномоченное лицо:**

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

https://ca.idc.md/
тел. +37353338124
факс +37353357188

23.01.2025 09:18:30


Рис. 6.36

Бланк заявления на возобновление действия сертификата открытого ключа электронной подписи представлен в приложении №3з, №3и к Регламенту Удостоверяющего центра.

Нажмите кнопку «Подписать документ».

- Откроется окно со списком сертификатов, доступных для подписания заявления. Выберите сертификат из списка, если их несколько, и нажмите кнопку «Ок». Если у Вас есть только один доступный сертификат, просто нажмите кнопку «Ок». (Рис.6.37).

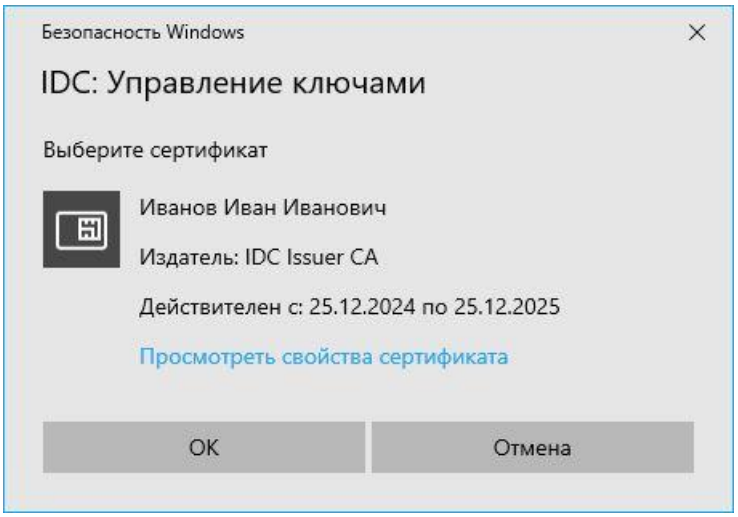



Рис. 6.37

- Откроется форма «Смарт-карта» (Рис.6.38). Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос в токен на выполнение операции подписания заявления Вашей электронной цифровой подписью.

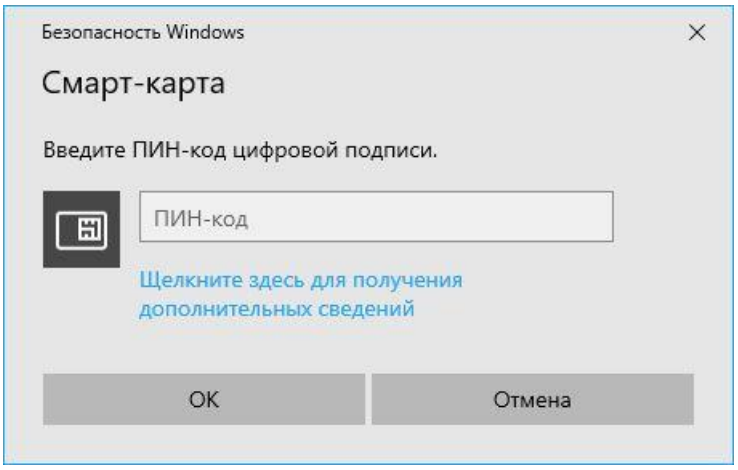



Рис. 6.38

- В области «Заявитель (владелец сертификата)» на заявлении будет проставлен штамп с данными вашей электронной цифровой подписи. В нижней части формы, справа от кнопки «Подписать документ», появится надпись: «Документ подписан» (Рис.6.39).

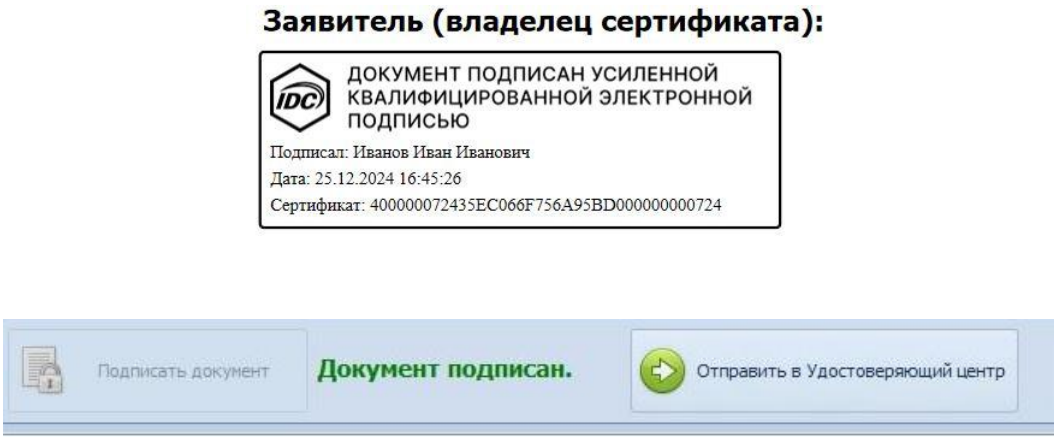



Рис. 6.39

- Нажмите кнопку «Отправить в Удостоверяющий центр», чтобы отправить подписанное заявление в информационную систему Удостоверяющего центра.
- Нажмите кнопку «Ок» чтобы закрыть окно с сообщением (Рис.6.40).

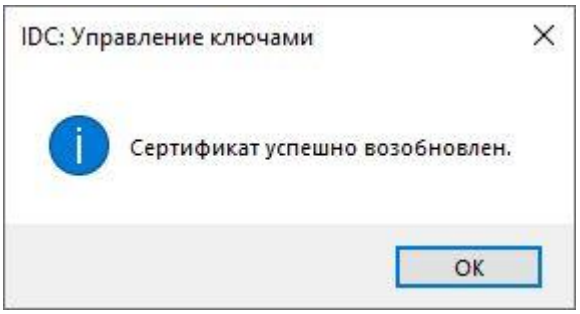



Рис. 6.40

- Чтобы сохранить копию заявления на Вашем устройстве для дальнейшего использования (например, для печати), нажмите кнопку «Сохранить…», которая находится в нижней части формы с документом (Рис.6.36). Заявление можно сохранить только после того как Вы подпишете его цифровой электронной подписью и отправите в Удостоверяющий центр.

- Статус «Сертификат приостановлен» меняется на статус «Сертификат выдан» (Рис.6.37).

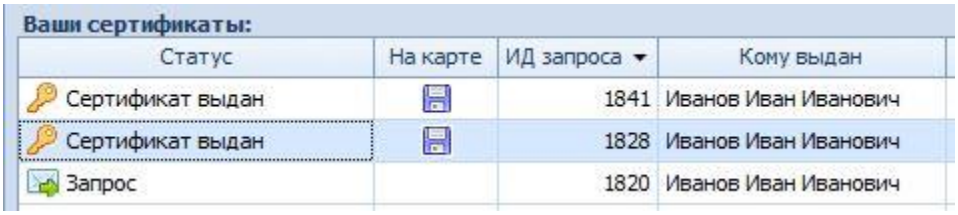



Рис. 6.37

## 6.8. Аннулирование действия сертификата

Действие сертификата открытого ключа электронной подписи полностью приостанавливается и возобновлению не подлежит. Для использования сертификата открытого ключа электронной подписи необходимо выпустить новый сертификат (см. п.6.3 «Создание запроса на сертификат»).

Аннулирование сертификата рекомендуется при компрометации закрытого ключа.

Для аннулирования сертификата:

- Выберите интересующий Вас сертификат из списка «Ваши сертификаты». Убедитесь в том, что в колонке «На карте» отображается пиктограмма (см. Рис.6.38).

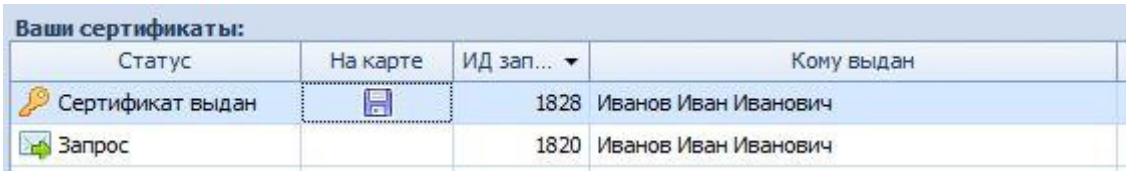



Рис. 6.38

*Внимание! Возможность аннулирования сертификата доступна только для сертификатов, записанных на токен. Для сертификатов, не записанных на токен, будет выдано соответствующее уведомление (Рис.6.39).*

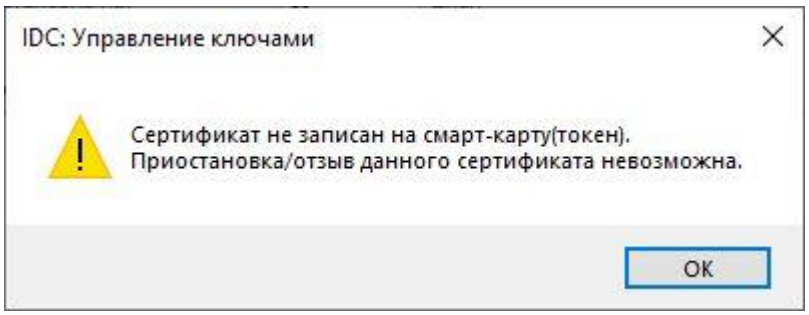



Рис. 6.39

*см. п.6.5 «Запись сертификата на ключевой носитель».*

- Нажмите кнопку меню «Отозвать/приостановить сертификат» (Рис.6.40).


Рис. 6.40

- Откроется форма «Отозвать/приостановить сертификат» (см. Рис. 6.41).

  Выберите причину отзыва сертификата из выпадающего списка «Причина отзыва/приостановки».

  Выбор причины «Приостановка действия сертификата» приводит к приостановке действия сертификата с возможностью последующего возобновления действия сертификата (см. п.6.6 «Приостановление действия сертификата»).

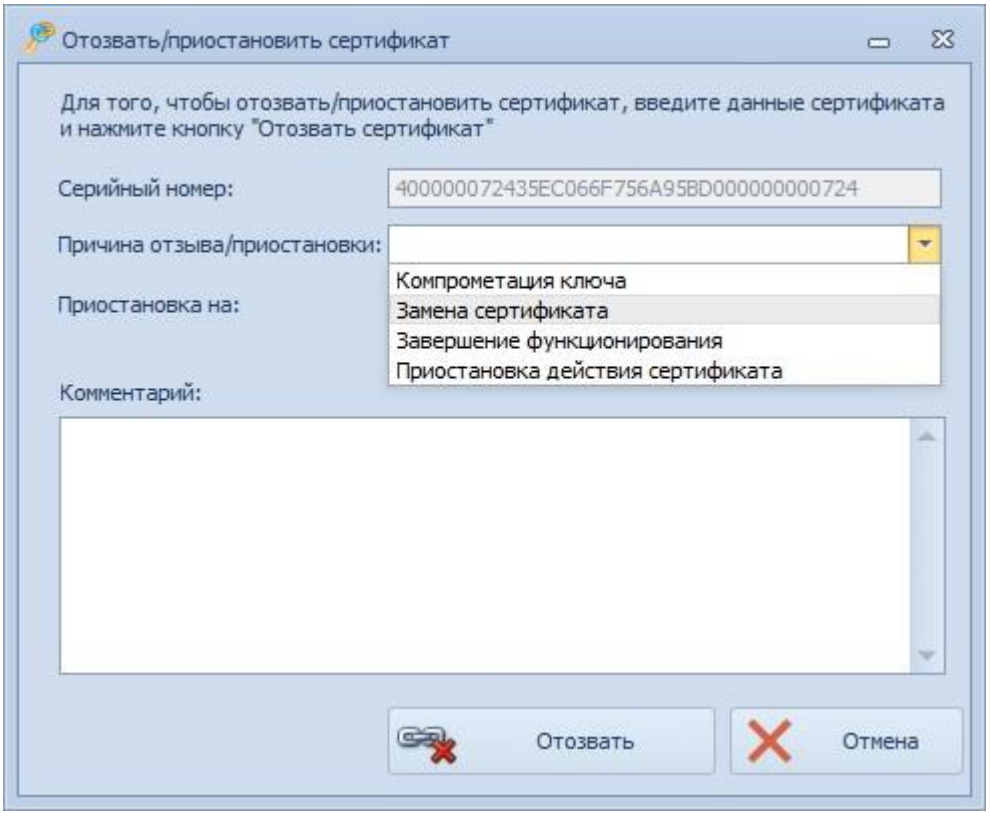



Рис. 6.41

Поле «Комментарий» не обязательно к заполнению. Вы можете оставить его пустым или, если необходимо, добавить дополнительную информацию, связанную с аннулированием действия сертификата.

Нажмите кнопку «Отозвать».

- Нажмите кнопку «Да», чтобы подтвердить аннулирование сертификата (Рис.6.42).

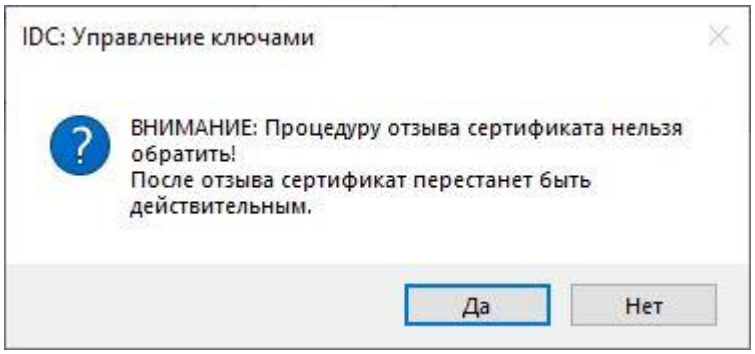
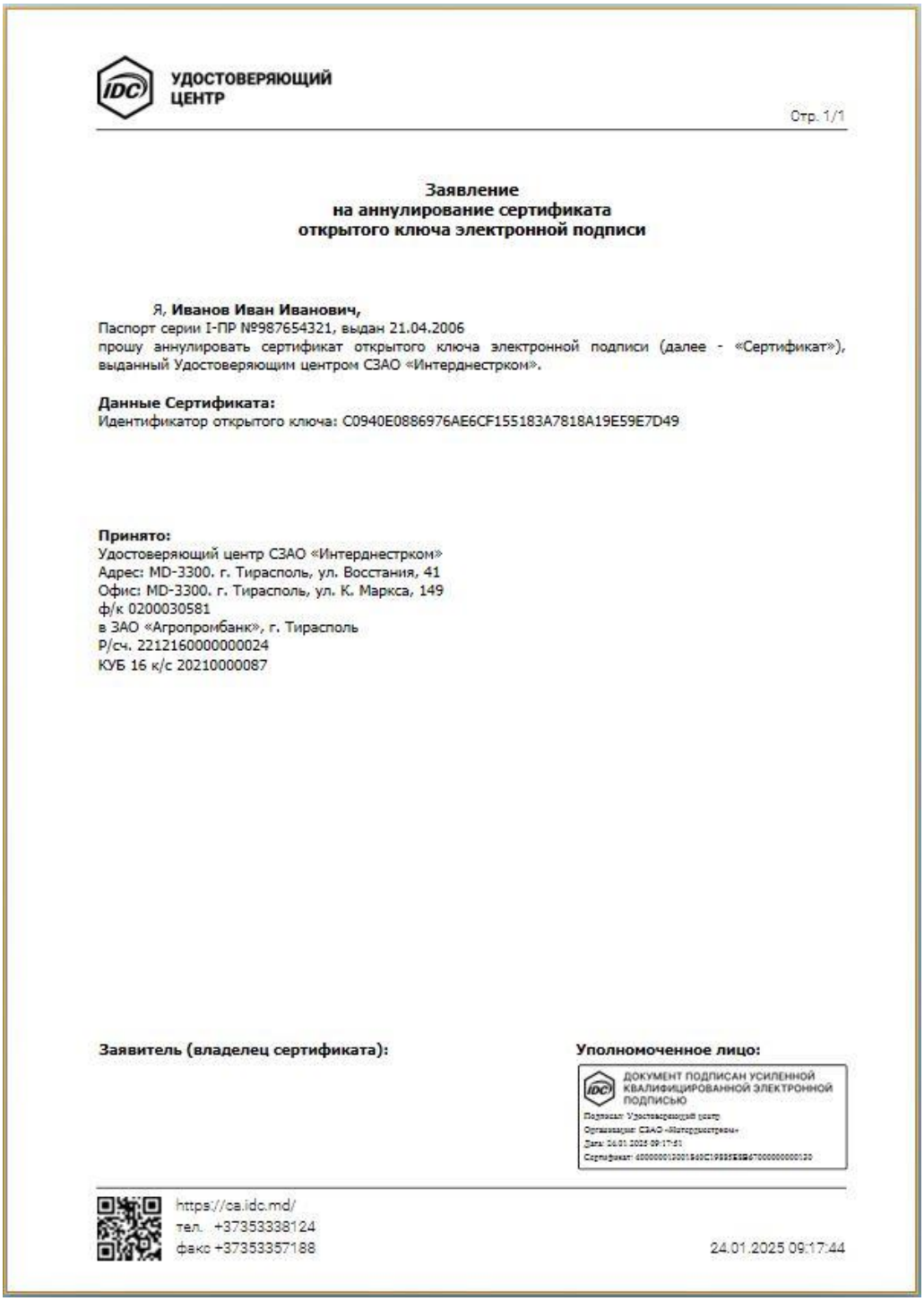



Рис. 6.42

- Информационная система Удостоверяющего центра формирует и отображает на экране отдельную форму с заявлением на аннулирование сертификата открытого ключа электронной подписи, подписанным уполномоченным лицом Удостоверяющего центра электронной цифровой подписью. (Рис.6.43).



УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Отр. 1/1

**Заявление**
**на аннулирование сертификата**
**открытого ключа электронной подписи**

Я, **Иванов Иван Иванович,**
Паспорт серии I-ПР №987654321, выдан 21.04.2006
прошу аннулировать сертификат открытого ключа электронной подписи (далее - «Сертификат»), выданный Удостоверяющим центром СЗАО «Интерднестрком».

**Данные Сертификата:**
Идентификатор открытого ключа: C0940E0886976AE6CF155183A7818A19E59E7D49

**Принято:**
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. г. Тирасполь, ул. Восстания, 41
Офис: MD-3300. г. Тирасполь, ул. К. Маркса, 149
ф/к 0200030581
в ЗАО «Агропромбанк», г. Тирасполь
Р/сч. 2212160000000024
КУБ 16 к/с 20210000087

**Заявитель (владелец сертификата):**

**Уполномоченное лицо:**

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

https://ca.idc.md/
тел. +37353338124
факс +37353357188

24.01.2025 09:17:44



Рис.6.43

Бланк заявления на аннулирование сертификата открытого ключа электронной подписи представлен в приложении №3г, №3д к Регламенту Удостоверяющего центра.

Нажмите кнопку «Подписать документ».

- Откроется окно со списком сертификатов, доступных для подписания заявления. Выберите сертификат из списка, если их несколько, и нажмите кнопку «Ок». Если у Вас есть только один доступный сертификат, просто нажмите кнопку «Ок». (Рис.6.44).

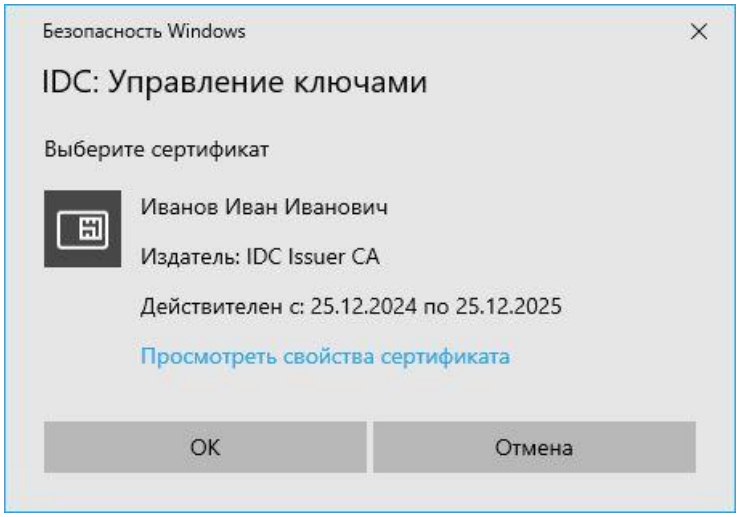



Рис.6.44

- Откроется форма «Смарт-карта» (Рис.6.45). Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос в токен на выполнение операции подписания заявления Вашей электронной цифровой подписью.

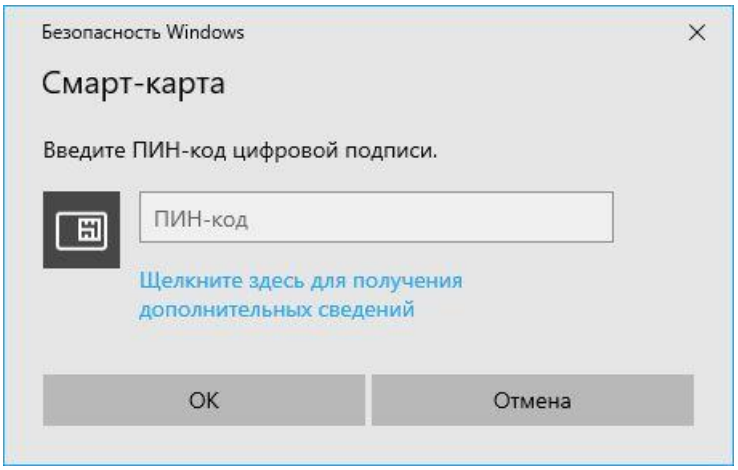



Рис.6.45

- В области «Заявитель (владелец сертификата)» на заявлении будет проставлен штамп с данными вашей электронной цифровой подписи. В нижней части формы, справа от кнопки «Подписать документ», появится надпись: «Документ подписан» (Рис.6.46).

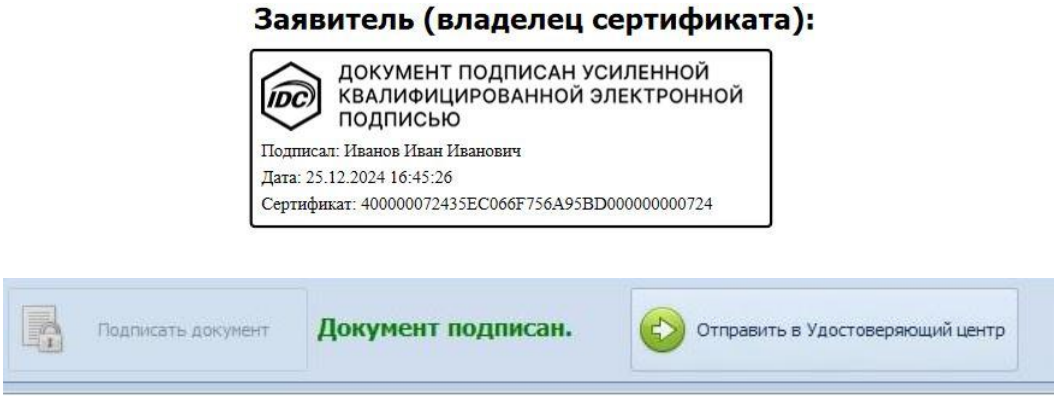



Рис. 6.46

- Нажмите кнопку «Отправить в Удостоверяющий центр», чтобы отправить подписанное заявление в информационную систему Удостоверяющего центра.

- Нажмите кнопку «Ок» чтобы закрыть окно с сообщением (Рис.6.47).

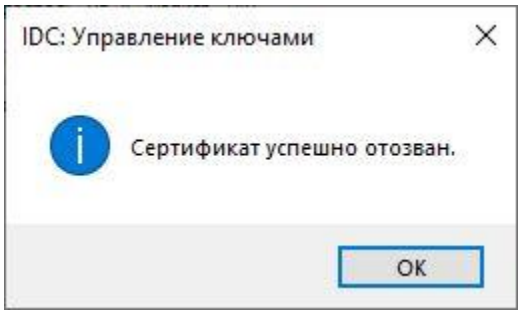



Рис. 6.47

- Чтобы сохранить копию заявления на Вашем устройстве для дальнейшего использования (например, для печати), нажмите кнопку «Сохранить…», которая находится в нижней части формы с документом (Рис.83). Заявление можно сохранить только после того как Вы подпишете его цифровой электронной подписью и отправите в Удостоверяющий центр.

- Статус «Сертификат выдан» меняется на статус «Сертификат отозван» (Рис.6.48).

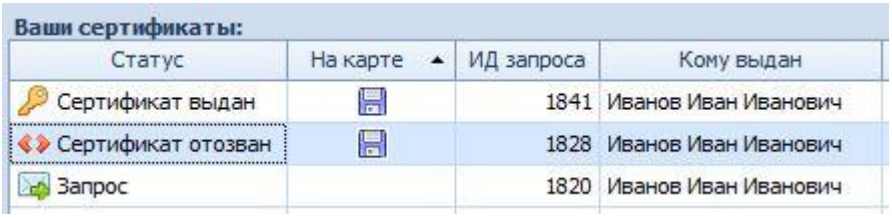



Рис. 6.48

6.9. Просмотр детальной информации о сертификате.

Программа позволяет просматривать детальную информацию о сертификате независимо от его статуса и независимо от того, записан ли он на токен.

Детальная информация о сертификате включает:

1. Имя владельца сертификата
2. Даты начала и окончания действия сертификата
3. Издатель сертификата
4. Ключи шифрования
5. Другие технические данные

В Регламенте Удостоверяющего центра приводится список базовых полей сертификата открытого ключа электронной подписи. В Приложении №1 п.7 и Приложении №2 Вы найдете все необходимые детали и описание каждого поля.

Для просмотра детальной информации о сертификате:

- В списке сертификатов «Ваши сертификаты» выберите нужный сертификат (см. Рис.6.49).

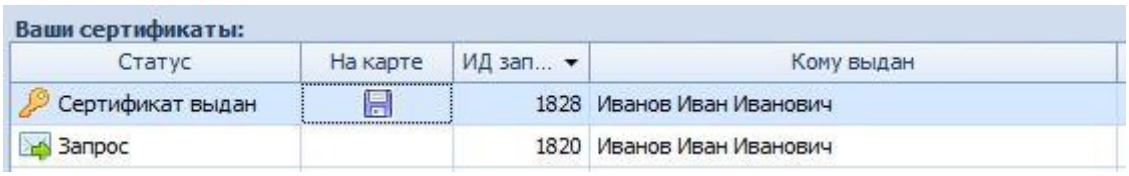



Рис.6.49

- Дважды кликните левой кнопкой мыши по записи выбранного сертификата либо нажмите кнопку меню «Посмотреть сертификат» (Рис.6.50).


Рис.6.50

- На экран будет выведено информационное окно с детальной информацией о сертификате (Рис.6.51).

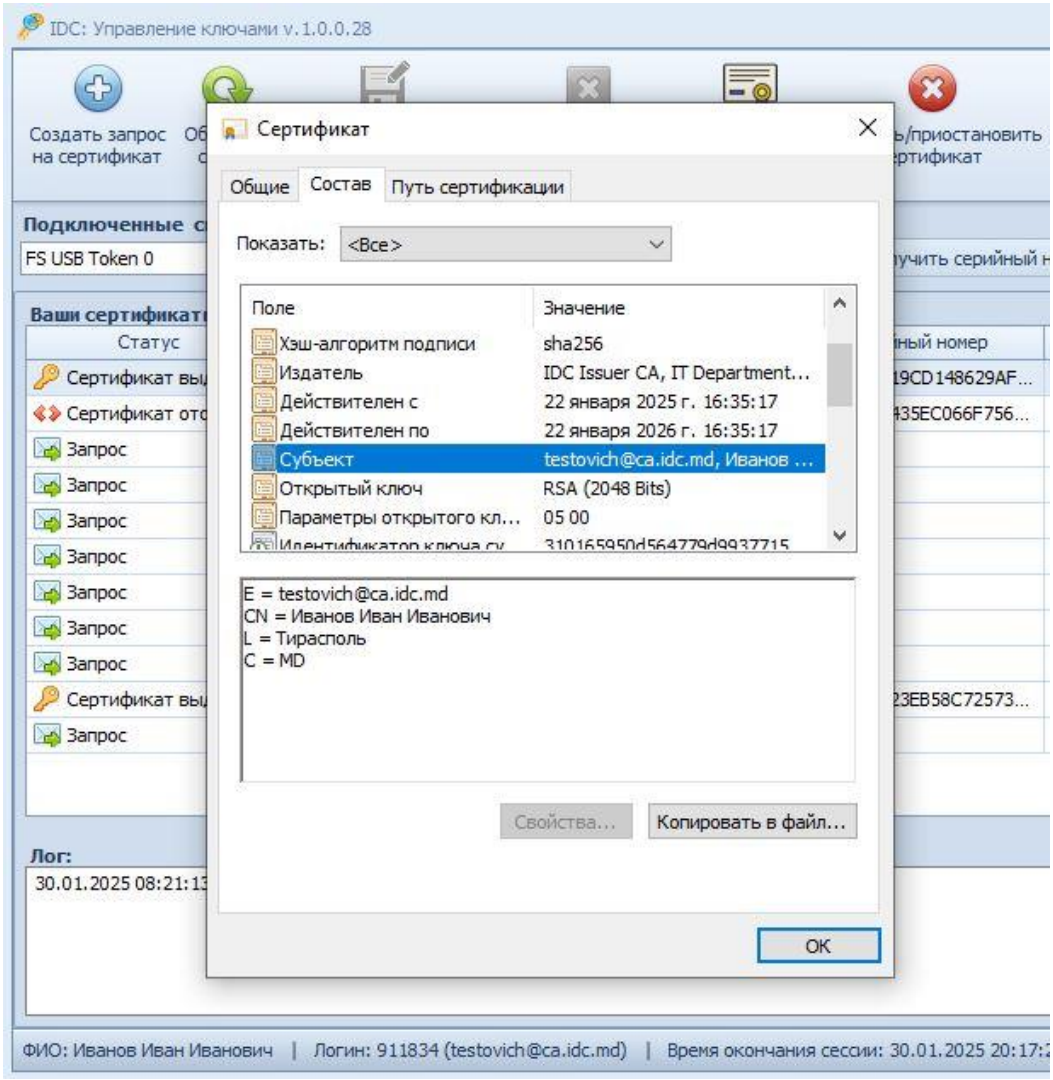



Рис.6.51

# 7. Токен

Токен для электронной подписи - это ключевой носитель для генерации ключей электронной подписи и записи сертификата открытого ключа электронной подписи.

Для работы с программой «IDC Управление ключами» в качестве ключевого носителя требуется использовать токен «Feitian ePass2003» (Рис.7.1).


Рис.7.1

Токен обладает высоким уровнем безопасности и соответствует стандартам «FIPS 140-2 level 3», а также «Common Criteria EAL 5+».

Формирование электронной подписи производиться внутри носителя.

«Руководство пользователя Токен ePass2003». содержит подробные инструкции по установке, настройке и использованию токена.

## 7.1. Авторизация операций

Программа «IDC Управление ключами» требует доступ к функциям и хранилищу токена для генерации ключевой пары, выпуска сертификатов и подписания заявлений электронной подписью. Этот доступ может быть предоставлен только с согласия владельца токена. Каждый раз, когда программа запрашивает доступ к токену, владельцу токена будет предложено ввести ПИН-код для подтверждения своего согласия (Рис. 7.2).

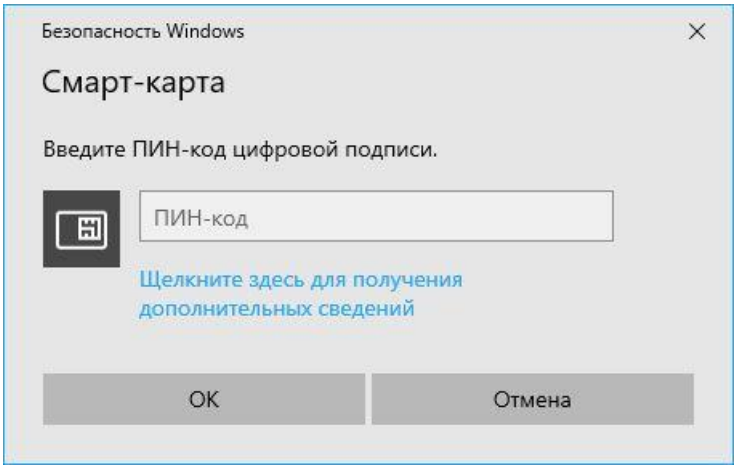



Рис.7.2

Для получения подробной информации о том, как и в каких случаях используется разрешение на доступ к функциям токена, Вам следует обратиться к пунктам руководства:

- 6.3 «Создание запроса на сертификат».
- 6.5 «Запись сертификата на ключевой носитель».
- 6.6 «Приостановление действия сертификата».
- 6.7 «Возобновление действия сертификата».
- 6.8 «Аннулирование действия сертификата».
- 7.3 «Удаление ключей и сертификатов».

## 7.2. Смена ПИН-кода

Для смены ПИН-кода токена:

- Выберите токен из выпадающего списка «Подключенные смарт-карты» (Рис.7.3).

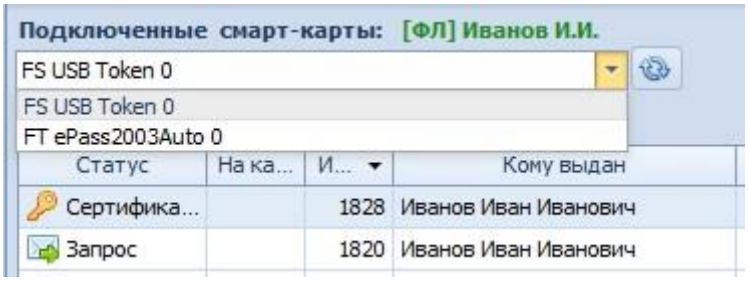



Рис.7.3

- Нажмите кнопку «Сменить PIN-код карты» (Рис.7.4).


Рис.7.4

- Откроется окно «Смена PIN-кода токена» (Рис.7.5).

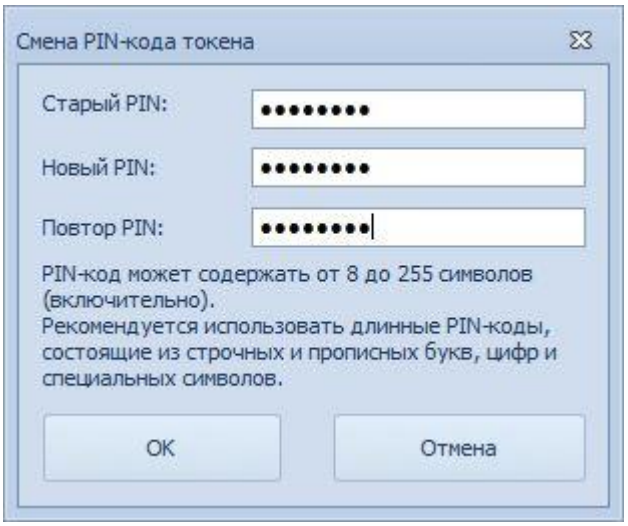



Рис.7.5

1. Введите действующий ПИН-код токена в поле «Старый PIN».
2. Введите новый ПИН-код токена в поле «Новый PIN».

   Надежный ПИН-код должен состоять не менее чем из 8 символов и содержать комбинацию заглавных и строчных букв, цифр и специальных символов. Не используйте распространенные фразы или личную информацию в паролях.

3. Введите еще раз новый ПИН-код токена в поле «Повтор PIN».
4. Нажмите кнопку «OK».

Если действующий ПИН-код введен некорректно, программа выдаст сообщение об ошибке (Рис.7.6).

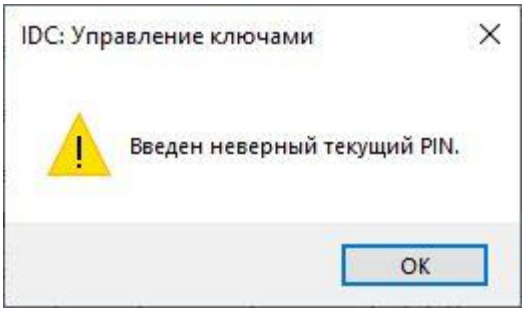



Рис.7.6

Если введенные ПИН-коды в поля «Новый PIN» и «Повтор PIN» не совпадают, будет выдано сообщение об ошибке (Рис.7.7).

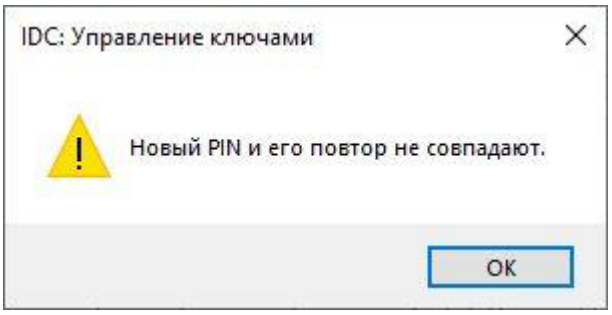



Рис.7.7

- В случае успешного завершения операции по смене ПИН-кода токена, в области отображения технической информации «Лог» появится запись «PIN токена успешно изменен».

## 7.3. Удаление ключей и сертификатов

Токен имеет ограниченный объем памяти, который позволяет хранить несколько контейнеров с ключевыми парами и сертификатами одновременно.

Удаление неиспользуемых ключей и связанных с ними сертификатов позволяет освободить память токена.

При удалении копии сертификата с токена, ассоциированная с ним ключевая пара (закрытый и открытый ключ) также удаляется. Однако копия сертификата, хранящаяся в реестре сертификатов Удостоверяющего центра, остается доступной для просмотра и записи на любой носитель, кроме токена (см.п.7.4 «Просмотр детальной информации о сертификате»).

Удалению подлежат сертификаты со статусом:

1. «Сертификат выдан» с вышедшим сроком действия.
2. «Сертификат отозван».

Для удаления сертификата:

- Выберите токен из выпадающего списка «Подключенные смарт-карты» (Рис.7.8).

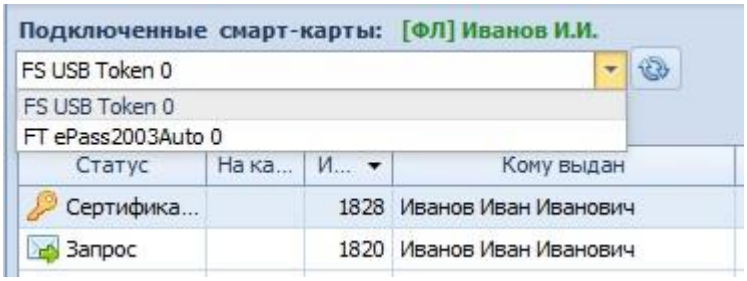



Рис.7.8

- Выберите интересующий Вас сертификат из списка «Ваши сертификаты». Убедитесь в том, что в колонке «На карте» отображается пиктограмма (см. Рис.7.9).

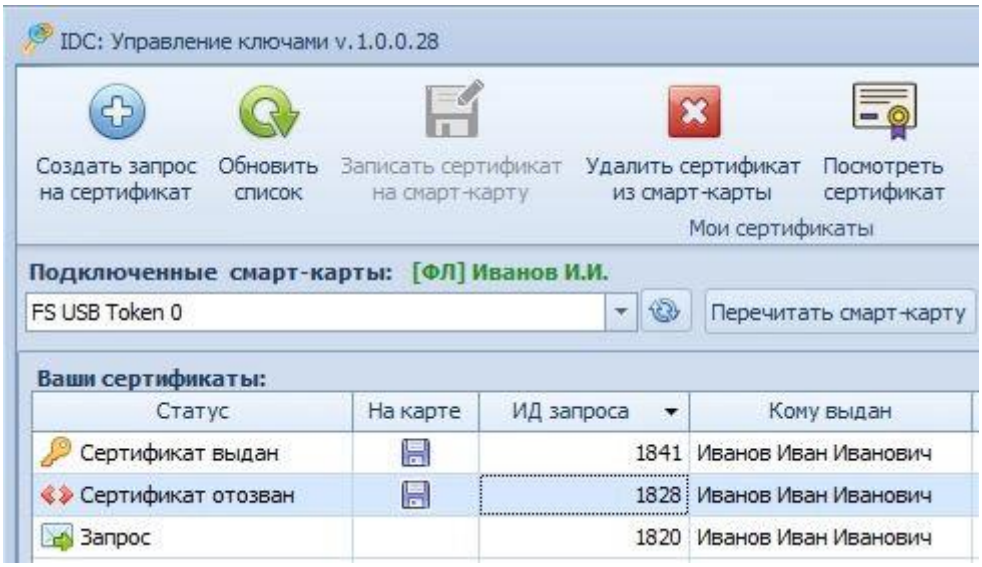



Рис.7.9

*Внимание! Возможность удаления сертификата доступна только для сертификатов, записанных на токен.*

*см. п.6.5 «Запись сертификата на ключевой носитель».*

- Нажмите кнопку меню «Удалить сертификат из смарт-карты» (Рис.7.10).

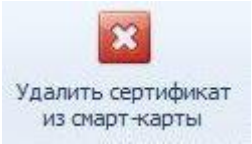



Рис.7.10

- Нажмите кнопку «Да», чтобы подтвердить удаление сертификата (Рис.7.11).

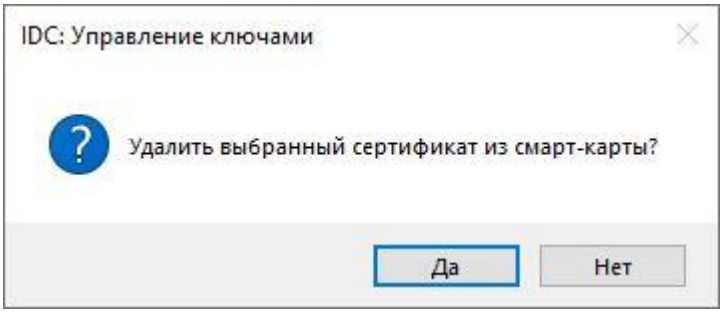



Рис.7.11

- Откроется форма «Смарт-карта» (Рис.7.12). Введите ПИН-код Вашего токена и нажмите кнопку «Ок» чтобы разрешить программе выполнить запрос в токен на выполнение операции удаления сертификата.

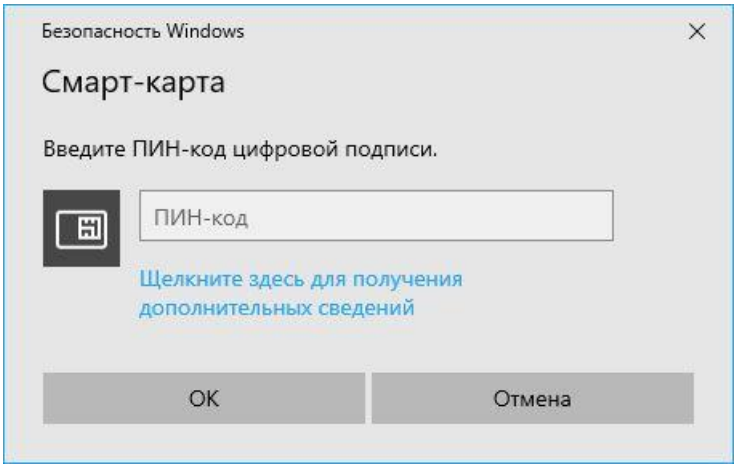



Рис.7.12

- Нажмите кнопку «Ок» чтобы закрыть окно с сообщением (Рис.7.13).

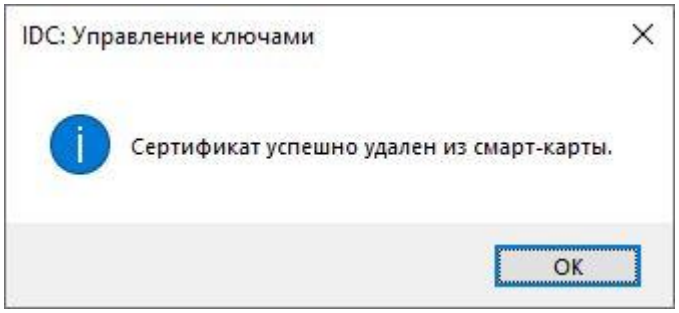



Рис.7.13

- После успешного выполнения процедуры по удалению сертификата, в списке сертификатов «Ваши сертификаты» в колонке «На карте» не будет отображаться пиктограмма, которая указывает на наличие сертификата на токене (Рис.7.14).


Рис.7.14