

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ЭЛЕКТРОННОЕ
ДЕЛО»**

**ОПЦИЯ «ИПО (ПОДПИСЬ)» К ИНТЕГРАЦИОННОМУ ПРОГРАММНОМУ
ОБЕСПЕЧЕНИЮ СИСТЕМЫ АВТОМАТИЗАЦИИ ДЕЛОПРОИЗВОДСТВА И
ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА «ЭЛЕКТРОННОЕ ДЕЛО»
«ЭЛЕКТРОННОЕ ДЕЛО-СМДО»**

(ОПЦИЯ «ИПО (ПОДПИСЬ)»)

ВЕРСИЯ 20

Руководство пользователя ИПО (ПОДПИСЬ)

Листов 49

2024

Содержание

ВВЕДЕНИЕ.....	3
1. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ОПЦИИ «ИПО (ПОДПИСЬ)»	4
2. РЕАЛИЗОВАННЫЕ ВОЗМОЖНОСТИ ОПЦИИ «ИПО (ПОДПИСЬ)».....	5
3. УСЛОВИЯ ДЛЯ РАБОТЫ С ОПЦИЕЙ «ИПО (ПОДПИСЬ)».....	6
3.1. Версионность ИПО_СМДО, технические требования и условия использования опции «ИПО (Подпись)»	6
3.2. Лицензирование опции «ИПО (Подпись)»	8
3.3. Импорт сертификата с ID-карты в хранилище сертификатов текущего пользователя	8
3.4. Импорт атрибутных сертификатов в ПМС Авеста	16
4. НАСТРОЙКА ВКЛАДКИ «ЭЦП» ИПО_СМДО ДЛЯ ОПЦИИ «ИПО (ПОДПИСЬ)»	19
4.1. Параметры вкладки «ЭЦП» в настройках ИПО_СМДО	19
4.2. Выбор вида подписи для сохранения в СЭД	20
4.3. Выбор сертификата для использования по умолчанию при выработке ЭЦП	23
4.4. Секция «Дополнительно» на вкладке «ЭЦП» в настройках ИПО_СМДО	28
5. РАБОТА ОПЦИИ «ИПО (ПОДПИСЬ)»	30
5.1. Возможности функции подписания файлов в ИПО_СМДО с опцией «ИПО (Подпись)».....	30
5.2. Подписание файлов с использованием USB-токена в ИПО_СМДО с опцией «ИПО (Подпись)»	33
5.3. Подписание файлов с использованием ID-карты в ИПО_СМДО с опцией «ИПО (Подпись)».....	37
5.4. Проверка подписи в ИПО_СМДО с опцией «ИПО (Подпись)»	42
6. СВЕДЕНИЯ О РАЗРАБОТЧИКЕ	47
7. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ	48

ВВЕДЕНИЕ

Руководство пользователя к опции «ИПО (Подпись)» (далее – Руководство) содержит описание возможностей, условия и порядок работы пользователей со средствами ЭЦП, включая возможность работы с атрибутивными сертификатами и ID-картой, которые применяются к файлам документов, отправляемых и получаемых по СМДО.

Руководство не является полной документацией к опции «ИПО (Подпись)». Для использования функционала опции «ИПО (Подпись)» необходимо ознакомиться с остальными руководствами, входящими в комплект документации к ИПО_СМДО.

Работа опции «ИПО (Подпись)» регулируется отдельной лицензией в рамках эксплуатируемого модуля ИПО_СМДО.

В связи с тем, что ИПО_СМДО постоянно совершенствуется, в тексте Руководства возможны некоторые несоответствия, касающиеся описания пользовательского интерфейса.

1. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ОПЦИИ «ИПО (ПОДПИСЬ)»

В связи с развитием электронных сервисов растет и потребность в средствах электронной цифровой подписи (ЭЦП), которые широко используются в системах электронного документооборота, для подачи налоговых деклараций, статистической и иной отчетности в электронном виде, а также позволяют получить доступ к максимально широкому спектру электронных услуг и административных процедур.

ИПО_СМДО с опцией «ИПО (Подпись)» позволяет подписывать документы, отобранные к отправке по СМДО. В качестве носителей ключевой информации (далее – НКИ) могут использоваться как USB-носители AvPass, AvToken или AvBign (далее – USB-токены), так и ID-карты. Формирование ЭЦП выполняется с использованием основного сертификата, выданного юридическому или физическому лицу в ГосСУОК, а также атрибутивных сертификатов, в случае их наличия.

Атрибутивный сертификат – это структура данных с ЭЦП центра атрибутивных сертификатов, связывающая определенные значения атрибутов с идентификационной информацией о держателе. Атрибутивный сертификат выпускается к существующему сертификату (далее – основной сертификат), изданному РУЦ ГОСУОК. Для подписания файлов документов в ИПО_СМДО рекомендуется использовать базовый атрибутивный сертификат, в котором устанавливается (подтверждается) связь физического лица (далее – ФЛ) с юридическим лицом (далее – ЮЛ) с указанием идентификационных данных ЮЛ и должностью ФЛ.

2. РЕАЛИЗОВАННЫЕ ВОЗМОЖНОСТИ ОПЦИИ «ИПО (ПОДПИСЬ)»

Для возможности работы со средствами ЭЦП, включая возможность работы с атрибутивными сертификатами и ID-картами, в ИПО_СМДО **версии 20.36 и выше** разработана опция «ИПО (Подпись)». ИПО_СМДО с опцией «ИПО (Подпись)» взаимодействует с СЭД «Электронное ДЕЛО» начиная с версии 12.2.1. В опции «ИПО (Подпись)» реализованы следующие функции:

- выбор сертификата и НКИ для формирования ЭЦП в момент подписания файлов документа и для использования по умолчанию;
- назначение вида подписи при ее сохранении в СЭД;
- подписание отдельных или всех файлов в документе;
- подписание всех файлов в группе документов;
- проверка подписей и действительности сертификатов в исходящих документах, отправляемых по СМДО, и во входящих документах, полученных по СМДО;
- просмотр данных подписи, основного сертификата и атрибутивных сертификатов;
- актуализация данных в ИПО_СМДО после обновления СОС и сертификатов УЦ, выполненных в Персональном менеджере сертификатов, входящем в программный комплекс «Комплект Абонента АВЕСТ» (далее – ПМС Авеста).

ВАЖНО!!! В СЭД «Электронное ДЕЛО» начиная с версии 12.2.1 по 22.2 включительно отсутствует возможность работы со средствами ЭЦП с использованием атрибутивных сертификатов и ID-карт. Такая возможность доступна в СЭД после ее обновления до **версии 24.3** и выше.

3. УСЛОВИЯ ДЛЯ РАБОТЫ С ОПЦИЕЙ «ИПО (ПОДПИСЬ)»

3.1. Версионность ИПО_СМДО, технические требования и условия использования опции «ИПО (Подпись)»

Опция «ИПО (Подпись)» реализована в ИПО_СМДО **версии 20.36 и выше**. Состав и параметры технических средств, информационная и программная совместимость, необходимые для установки ИПО_СМДО с опцией «ИПО (Подпись)», должны соответствовать п. 2 Руководства администратора, входящего в комплект документации к ИПО_СМДО версии 20.

ВАЖНО!!! Для возможности использования опции «ИПО (Подпись)» на рабочих местах пользователей необходимо выполнить обновление ИПО_СМДО до **версии 20.36 или выше**.

ВАЖНО!!! Перед использованием функционала выработки ЭЦП опции «ИПО (Подпись)» на компьютере пользователя необходимо:

- импортировать сертификат подписанта в личное хранилище сертификатов текущего пользователя в случае использования USB-токена в качестве НКИ в процессе подписания (в ПМС Авеста сертификат подписанта должен находиться в папке «Личные сертификаты» и определяться как действительный) (см. руководство к ПМС Авеста);

- импортировать с ID-карты сертификат подписанта в хранилище текущего пользователя в случае использования ID-карты в качестве НКИ в процессе подписания (в ПМС Авеста сертификат подписанта должен находиться в папке «Сетевой справочник» и определяться как действительный) (см. [п. 3.3](#) настоящего Руководства);

- импортировать атрибутный сертификат в ПМС Авеста в случае необходимости его использования при выработке ЭЦП (в ПМС Авеста атрибутный сертификат должен отображаться в секции «Атрибутные сертификаты» при выделении основного сертификата в списке сертификатов секции «Личные сертификаты» или секции «Сетевой справочник»

сертификатов» и определяться как действительный) (см. [п. 3.4](#) настоящего Руководства).

ВАЖНО!!! При подписании файлов документов с использованием ID-карты необходимо на рабочих местах пользователей, работающих с опцией «ИПО (Подпись)», установить Клиентскую программу ([КП, NTClientSoftware](#)), предоставляемую РУП «Национальный центр электронных услуг» (далее – НЦЭУ) после прохождения Вашей организацией регистрации и отправки заявки на сайте НЦЭУ. Согласно п. 4 раздела «Общие положения» Соглашения с пользователем об условиях использования КП и КПСИС (утверждено НЦЭУ 12.01.2022 и [опубликовано на сайте НЦЭУ](#)) КП устанавливается на рабочих местах пользователей в целях выработки и проверки ЭЦП с применением средств ЭЦП, распространяемых в рамках ГосСУОК.

При работе с ID-картой на рабочем месте пользователя к его персональному компьютеру должен быть подключен считыватель ID-карты. Технические требования к считывателям ID-карт и список потенциальных поставщиков считывателей ID-карт опубликованы на [сайте Министерства связи и информатизации Республики Беларусь](#) (рис. 3.1):

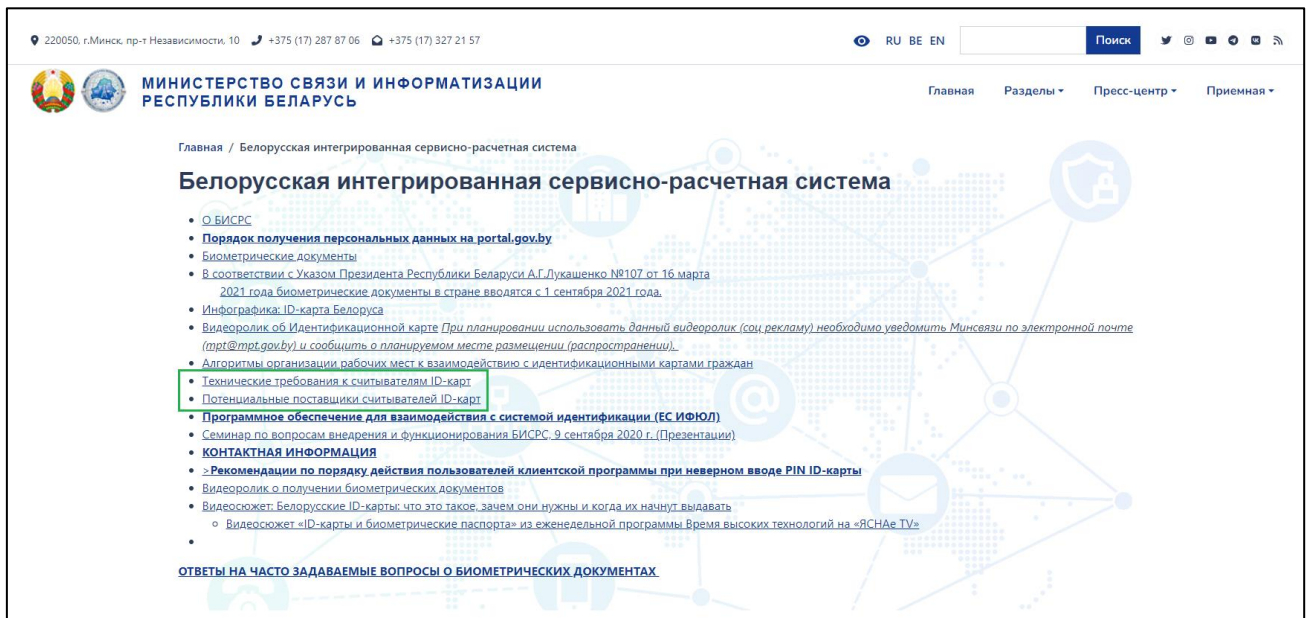


Рис. 3.1. Страница сайта Министерства связи и информатизации Республики Беларусь

ВАЖНО!!! При работе с ID-картой пользователь должен знать PIN1 и PIN2, предоставленные ему при получении ID-карты.

3.2. Лицензирование опции «ИПО (Подпись)»

Для работы ИПО_СМДО с опцией «ИПО (Подпись)» необходимо приобрести лицензию на опцию. После получения лицензионного ключа на использование ИПО_СМДО с опцией «ИПО (Подпись)» введите в настройках ИПО_СМДО на вкладке «Общие» полученную информацию о лицензии и нажмите кнопку **Активировать**. В списке доступных опций появится запись «ИПО (Подпись): Подписание файлов и расширенная проверка ЭЦП» (рис. 3.2):

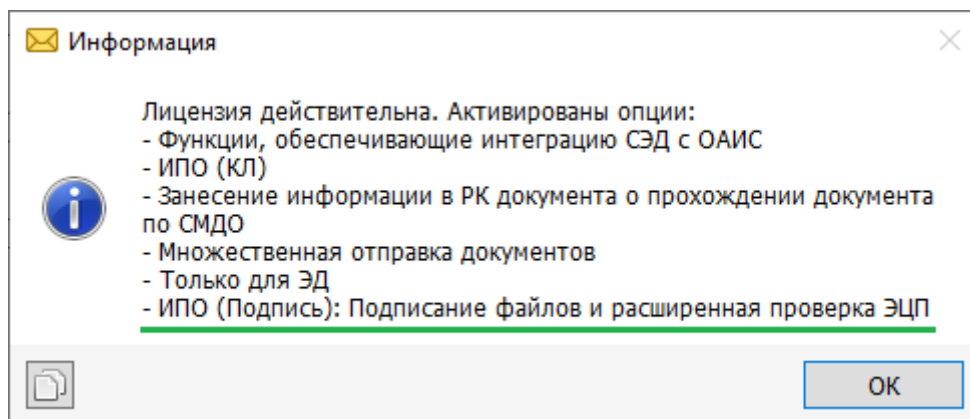


Рис. 3.2. Пример наличия опции «ИПО (Подпись)» в списке доступных опций после активации лицензии

Закройте ИПО_СМДО, следуя тексту сообщений. При следующем запуске ИПО_СМДО функционал опции «ИПО (Подпись)» станет доступен пользователю.

3.3. Импорт сертификата с ID-карты в хранилище сертификатов текущего пользователя

Идентификационная карта гражданина Республики Беларусь (ID-карта) – это биометрический документ, удостоверяющий личность, в виде пластиковой смарт-карты с интегральной микросхемой, содержащей электронное средство

биометрической идентификации и криптографический токен аутентификации, на котором записан сертификат физического лица (далее – СОК). СОК физического лица присутствует только на ID-карте и не поставляется в виде отдельного файла при выпуске ID-карты.

Для возможности выбора лица для подписания файлов документов с использованием ID-карты перед началом работы с опцией «ИПО (Подпись)» необходимо на рабочем месте пользователя выполнить импорт сертификата с ID-карты в хранилище сертификатов текущего пользователя. При импорте создается копия сертификата, а сам сертификат остается на ID-карте.

ВАЖНО!!! При работе с ID-картой к персональному компьютеру пользователя должен быть подключен считыватель для работы с ID-картой. В случае чтения карты по бесконтактному интерфейсу ID-карта прикладывается к устройству. Для чтения контактным способом ID-карта вставляется в считыватель. Если ID-карта распознана считывателем, то на устройстве загорается зеленый индикатор (обязательное условие для работы с ID-картой). Если есть проблемы с распознаванием ID-карты, то на устройстве загорится красный индикатор (работа с ID-картой не возможна).

ВАЖНО!!! При работе с ID-картой на персональном компьютере пользователя должна быть запущена [Клиентская программа](#), в настройках которой в качестве устройства выбрана ID-карта и **определен считыватель ID-карты**, подключенный к компьютеру пользователя (рис. 3.3):

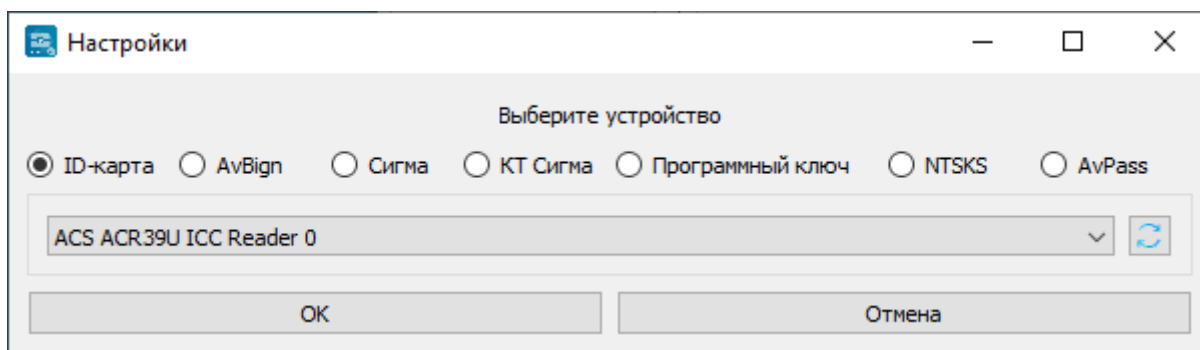


Рис. 3.3. Настройка КП для работы с ID-картой

ВАЖНО!!! При работе с ID-картой пользователь должен знать PIN1 и PIN2, предоставленные ему при получении ID-карты.

Чтобы выполнить импорт сертификата с ID-карты в хранилище сертификатов текущего пользователя, в настройках ИПО_СМДО на вкладке «ЭЦП» в секции «Дополнительно» нажмите кнопку **Действия с сертификатом ID-карты** (рис. 3.4):

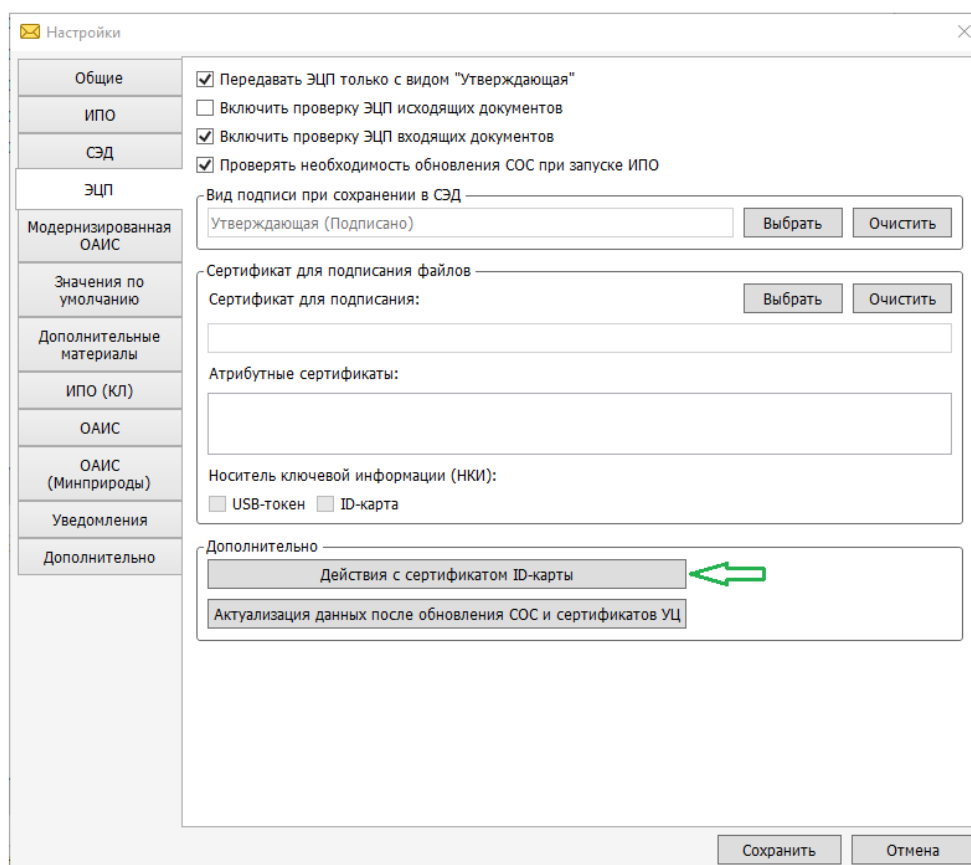


Рис. 3.4. Кнопка **Действия с сертификатом ID-карты** на вкладке «ЭЦП» в настройках ИПО_СМДО с опцией «ИПО (Подпись)»

В окне «Действия с сертификатом» поставьте флаг в параметре «Импортировать в хранилище текущего пользователя» и нажмите кнопку **Выполнить** (рис. 3.5):

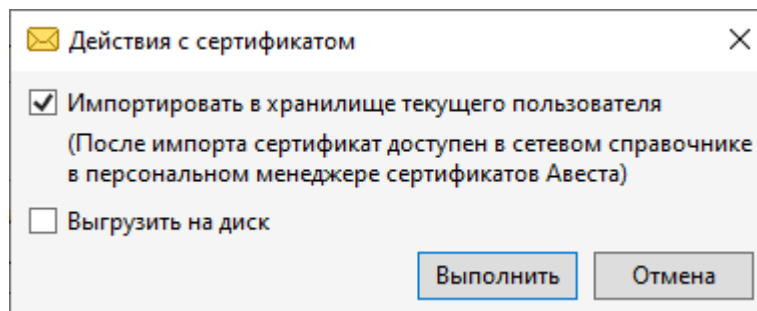


Рис. 3.5. Выбор действия для импорта сертификата с ID-карты в хранилище сертификатов текущего пользователя

Если ранее не была пройдена аутентификация в КП, то поднимется окно КП для ввода PIN1. Введите PIN1 и нажмите кнопку ОК (рис. 3.6):

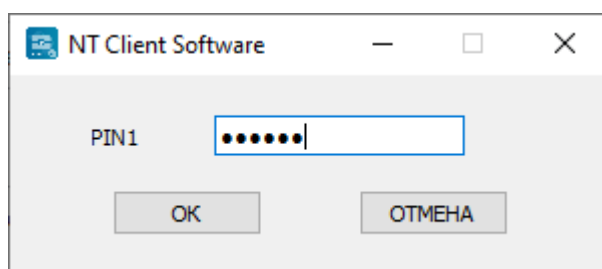


Рис. 3.6. Ввод PIN1 в окно КП

Затем поднимется окно КП для ввода PIN2. Если аутентификация в КП была пройдена ранее, то поднимется сразу окно КП для ввода PIN2. Введите PIN2 и нажмите кнопку ОК (рис. 3.7):

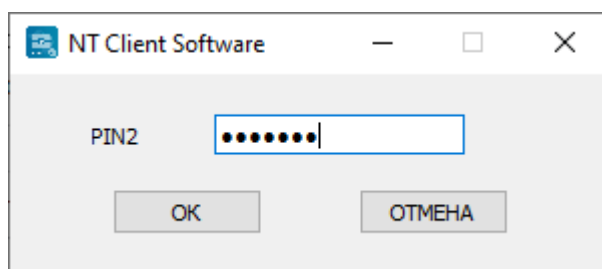


Рис.3.7. Ввод PIN2 в окно КП

После успешного завершения импорта сертификата с ID-карты в хранилище сертификатов текущего пользователя отобразится сообщение (рис. 3.8):

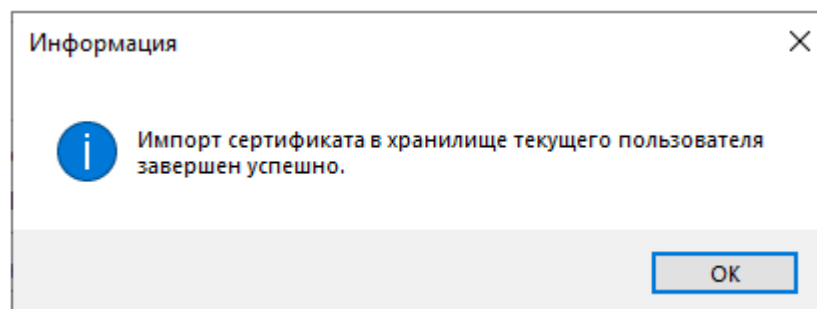


Рис. 3.8. Сообщение о завершении импорта сертификата с ID-карты в хранилище сертификатов текущего пользователя

После импорта сертификат будет доступен для просмотра в сетевом справочнике ПМС Авеста (рис. 3.9, рис. 3.10). Сертификат для ID-карты выдается РУЦ ГосСУОК на 10 лет, что позволяет по этому признаку быстрее найти его в списке сертификатов.

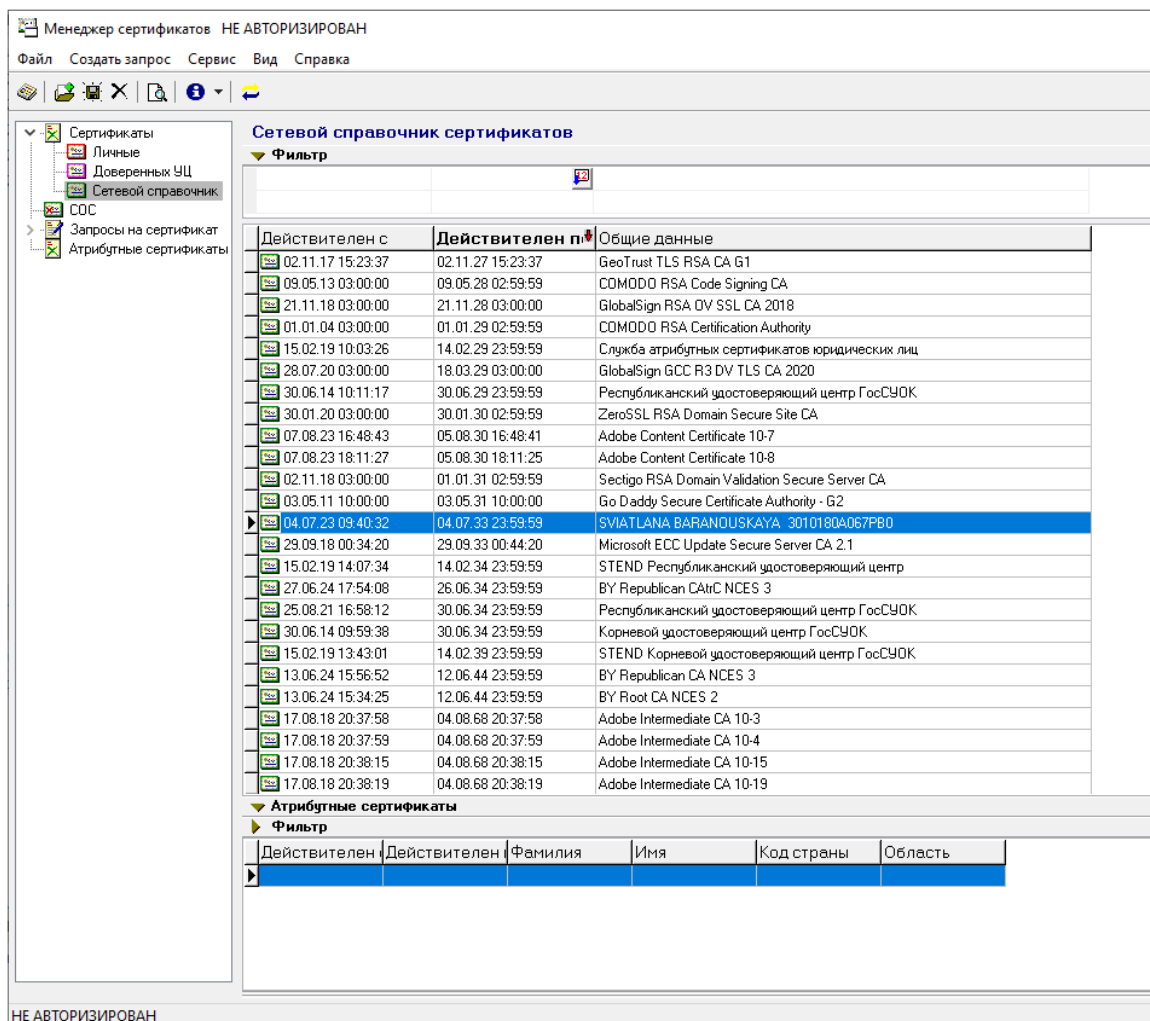


Рис. 3.9. Пример сертификата с ID-карты в сетевом справочнике ПМС Авеста

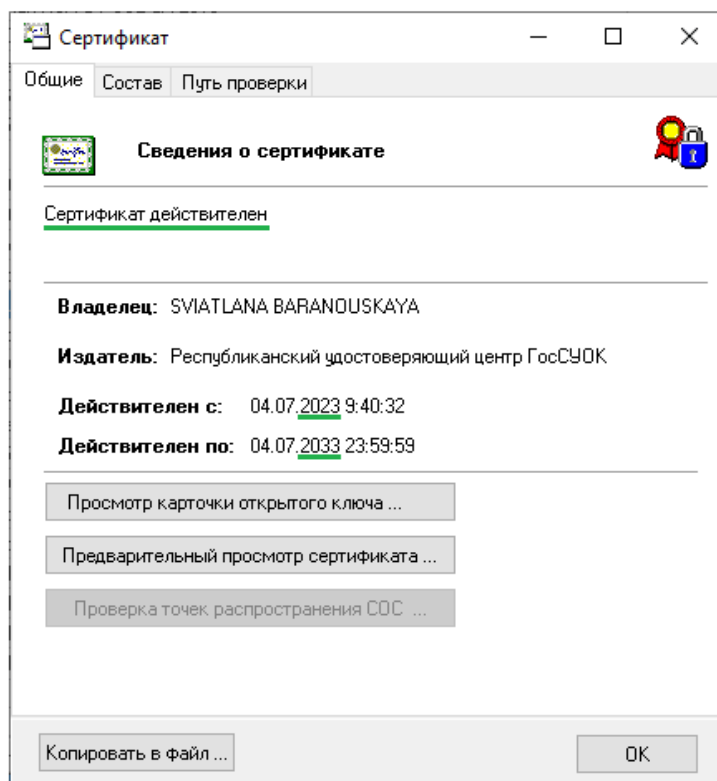


Рис. 3.10. Просмотр сертификата с ID-карты в ПМС Авеста

В процессе импорта сертификата с ID-карты в хранилище сертификатов текущего пользователя неверные действия пользователя могут сопровождаться сообщениями (рис. 3.11 – 3.15):

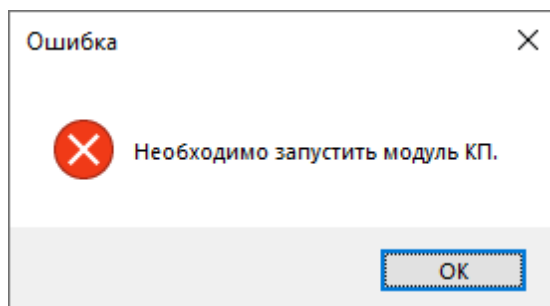


Рис. 3.11. Сообщение, если у пользователя не запущена КП

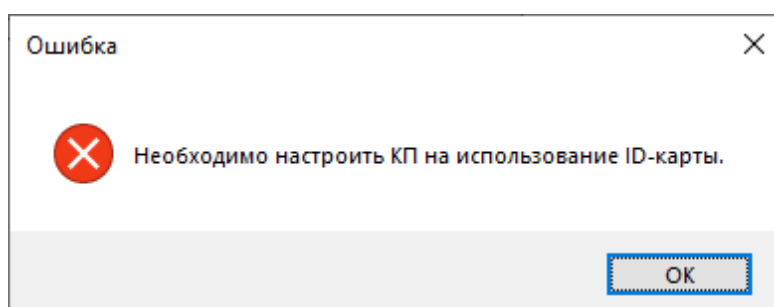


Рис. 3.12. Сообщение, если в настройках КП в качестве устройства не выбрана ID-карта

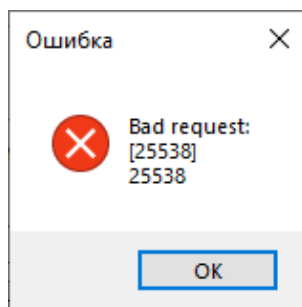


Рис. 3.13. Сообщение, если не верно введен PIN1

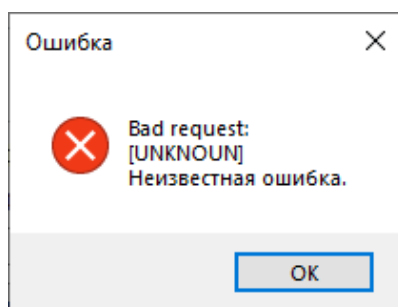


Рис. 3.14. Сообщение, если не верно введен PIN2

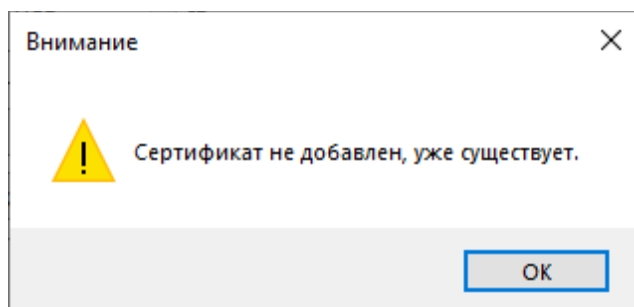


Рис. 3.15. Сообщение при импорте сертификата, если сертификат с ID-карты уже находится в хранилище сертификатов текущего пользователя

Для импорта сертификата с ID-карты в хранилище сертификатов текущего пользователя можно применить второй вариант: сначала сохранить его в виде файла с расширением **.cer** на диске персонального компьютера, а затем в ПМС Авеста выполнить его импорт (пункт меню Файл / Импорт сертификата/СОС, см. руководство к ПМС Авеста). Для этого в окне «Действия с сертификатом» поставьте флаг в параметре «Выгрузить на диск» и нажмите кнопку **Выполнить** (рис. 3.16):

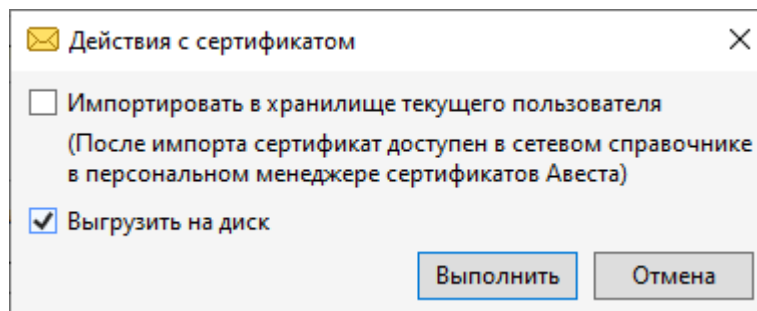


Рис. 3.16. Выбор действия для сохранения сертификата с ID-карты в виде файла с расширением **.cer** на диске персонального компьютера

Процесс сохранения сертификата на диске в виде файла аналогичен процессу его импорта в хранилище сертификатов текущего пользователя, описанному выше. В завершении процесса поднимется окно с данными сертификата, в котором нажмите кнопку **ОК** (пример на рис. 3.17):

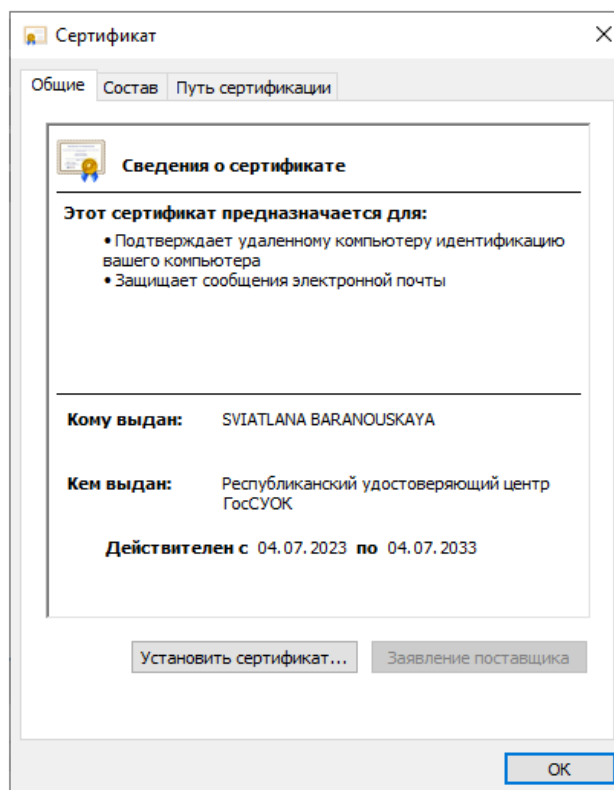


Рис. 3.17. Пример окна с данными сертификата, выгруженного с ID-карты

В результате выгрузки в папке, выбранной в процессе выгрузки в окне «Обзор папок», сертификат с ID-карты сохранится в виде файла с расширением **.cer**.

3.4. Импорт атрибутивных сертификатов в ПМС Авеста

При подписании файлов документов с использованием атрибутивных сертификатов, в случае их наличия у основного сертификата подписанта, перед началом работы с функционалом выработки ЭЦП опции «ИПО (Подпись)» необходимо на рабочем месте пользователя в ПМС Авеста выполнить импорт атрибутивных сертификатов к основному сертификату. Действия по импорту атрибутивных сертификатов не зависят от типа НКИ, используемого в процессе подписания файлов документов.

Для импорта атрибутивного сертификата запустите ПМС Авеста под учетной записью пользователя в операционной системе, поставьте флаг в параметре «Войти в систему без авторизации» и нажмите кнопку **ОК** (рис. 3.18):

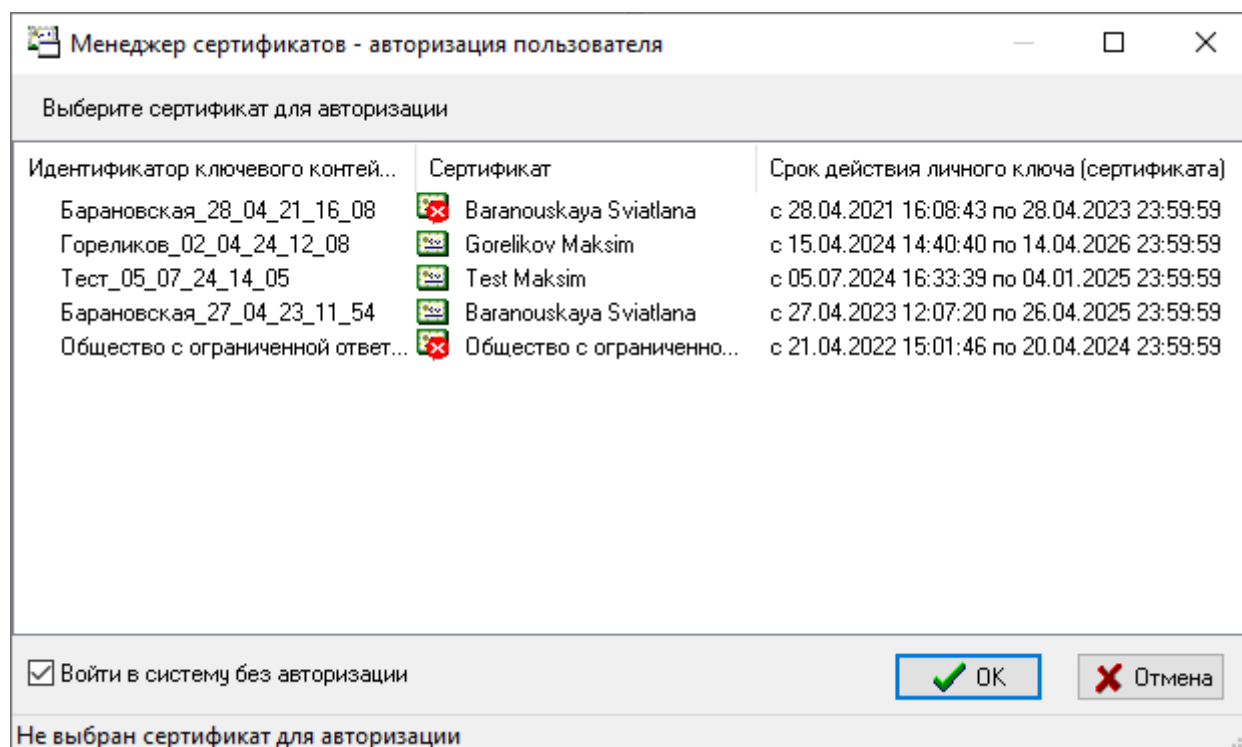


Рис. 3.18. Вход в ПМС Авеста без авторизации

Выберите пункт меню Файл / Импорт сертификата/СОС. В появившемся окне «Мастер импорта сертификатов» нажмите кнопку **Обзор** (рис. 3.19):

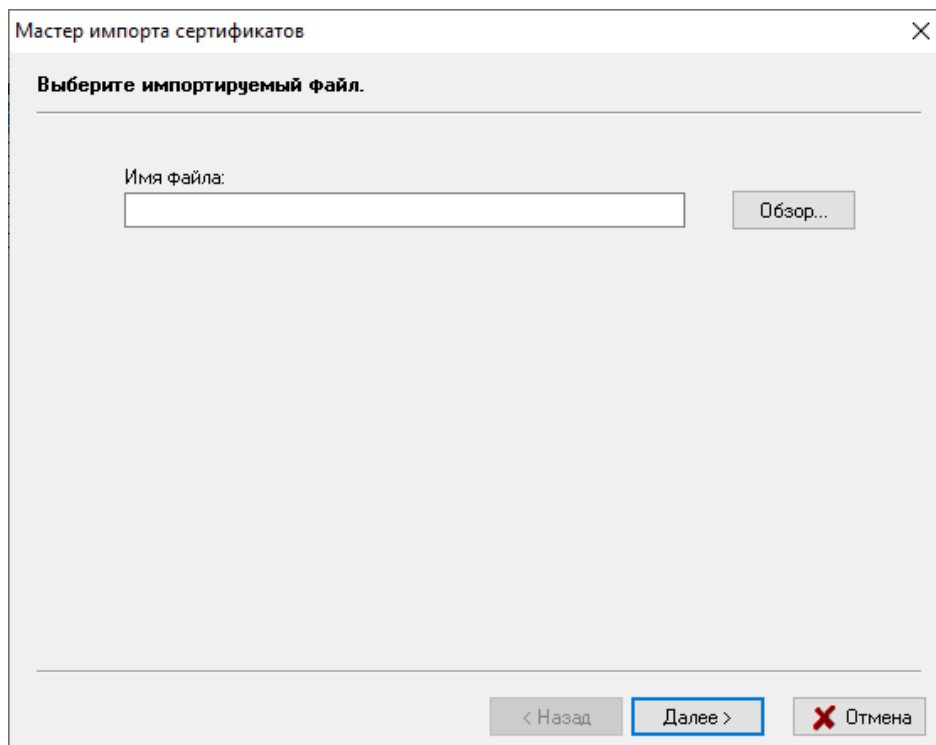


Рис. 3.19. Окно «Мастер импорта сертификатов» ПМС Авеста

В окне «Проводника» найдите нужный атрибутный сертификат (файл с расширением **.acr**) и нажмите кнопку **Открыть** (рис. 3.20):

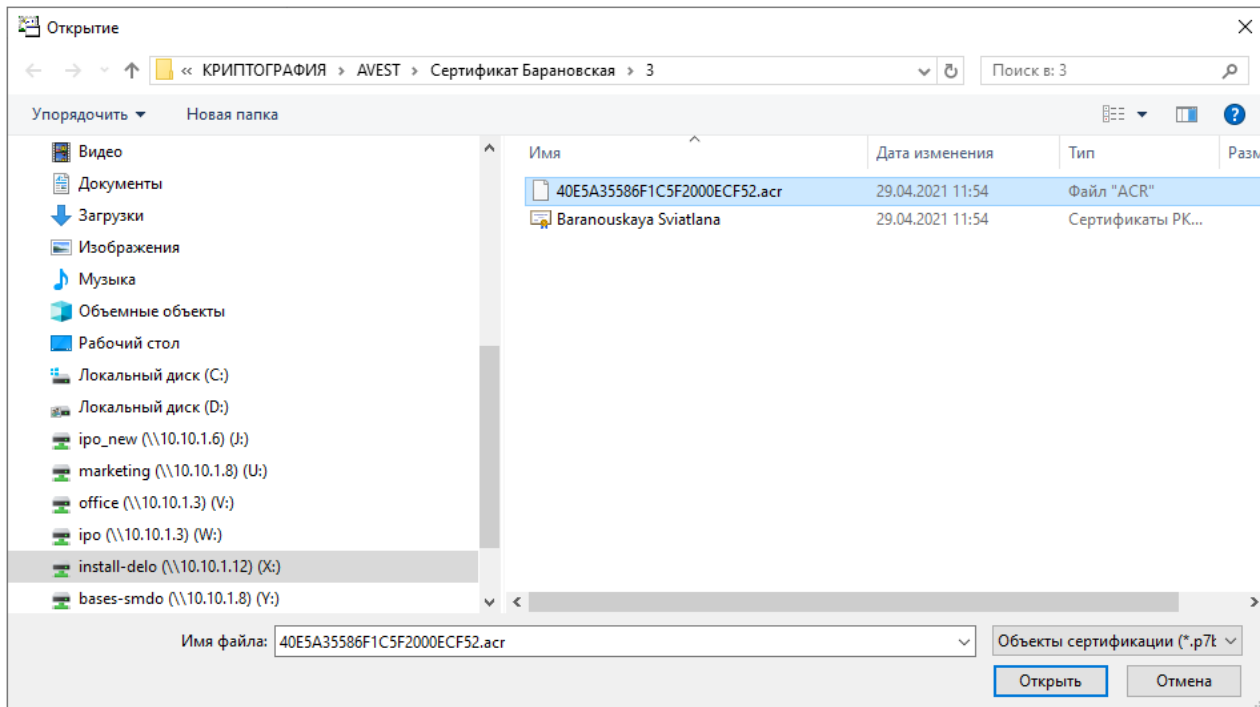


Рис. 3.20. Выбор атрибутного сертификата для его импорта в ПМС Авеста

Далее выполните действия, которые предлагает Мастер импорта сертификатов.

В результате импорта атрибутный сертификат отобразится в секции «Атрибутные сертификаты» (пример на рис. 3.21):

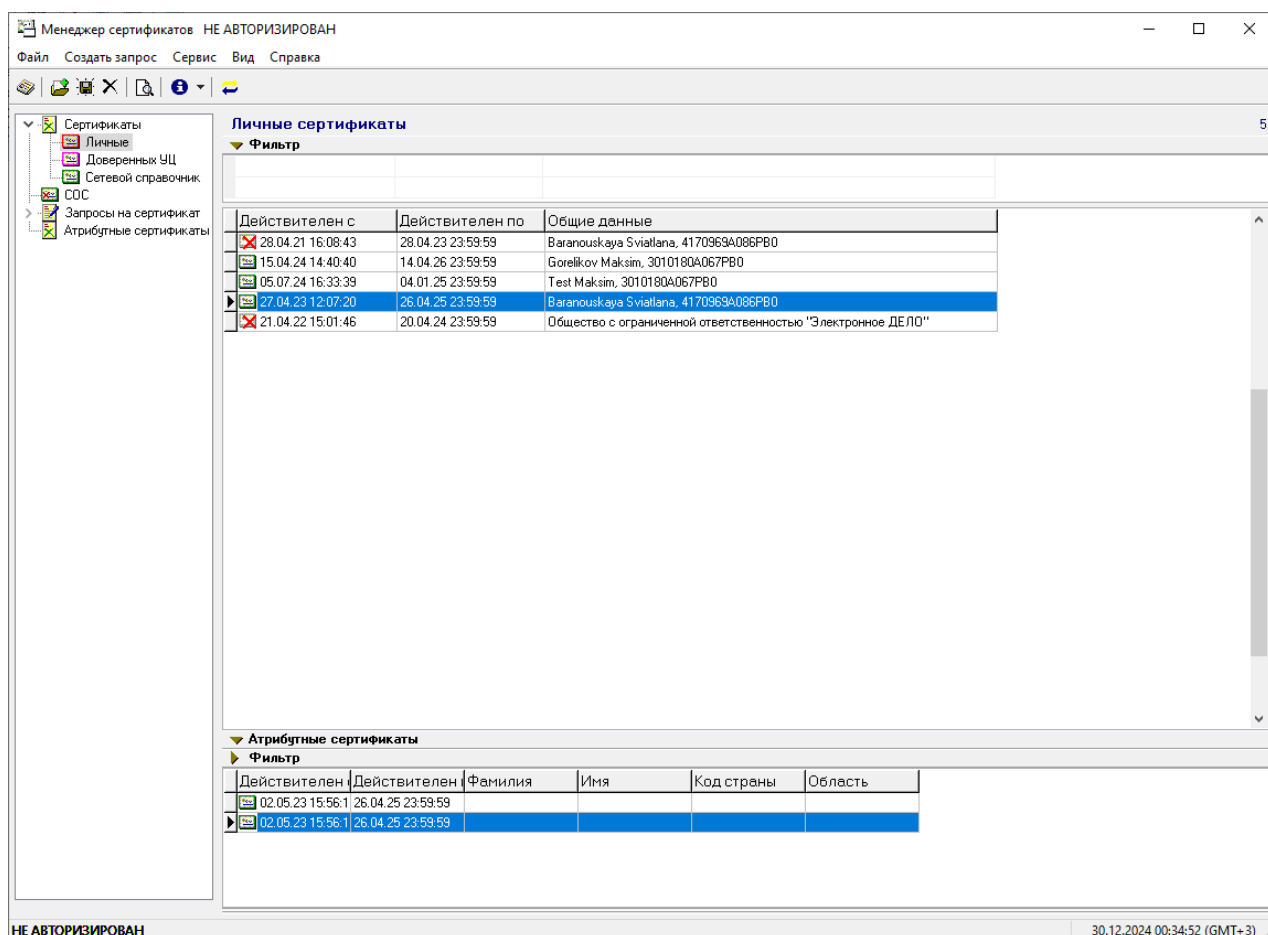


Рис. 3.21. Пример атрибутного сертификата, импортированного к основному сертификату в ПМС Авеста

При просмотре атрибутный сертификат в ПМС Авеста должен определяться как действительный.

Если у основного сертификата есть несколько атрибутных сертификатов, то в ПМС Авеста импортируйте все атрибутные сертификаты.

Более подробное описание действий по импорту атрибутного сертификата см. в руководстве к ПМС Авеста.

4. НАСТРОЙКА ВКЛАДКИ «ЭЦП» ИПО_СМДО ДЛЯ ОПЦИИ «ИПО (ПОДПИСЬ)»

4.1. Параметры вкладки «ЭЦП» в настройках ИПО_СМДО

Первые четыре параметра вкладки «ЭЦП» в настройках ИПО_СМДО доступны в базовом комплекте приложения. Их использование описано в п. 6.4 Руководства технолога, входящего в комплект документации к ИПО_СМДО версии 20.

При использовании опции «ИПО (Подпись)» в настройках ИПО_СМДО на вкладке «ЭЦП» становится доступной дополнительная область настроек (рис. 4.1):

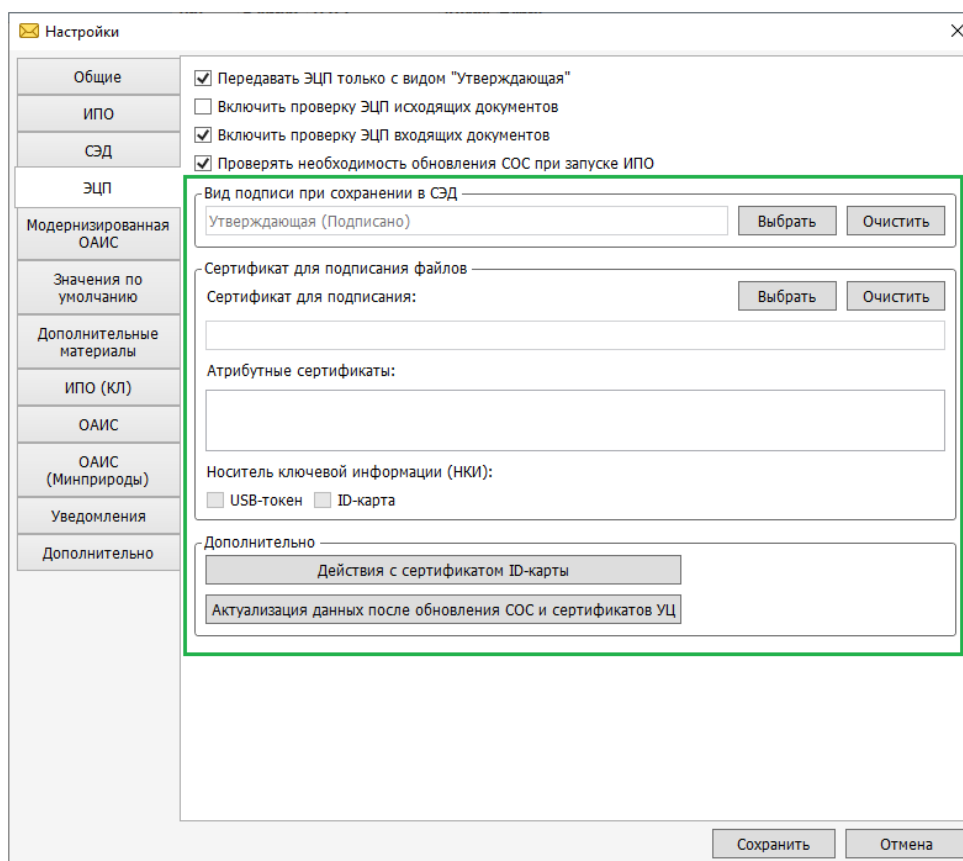


Рис. 4.1. Область настроек ЭЦП для опции «ИПО (Подпись)»

Работа с настройками ЭЦП для опции «ИПО (Подпись)» описана в следующих пунктах настоящего Руководства.

ВАЖНО!!! При подписании файлов документов с использованием ID-карты перед началом работы с настройками ЭЦП для опции «ИПО (Подпись)» Разработчик постоянно улучшает потребительские свойства ИПО и рекомендует всегда использовать последнюю актуальную версию продукта, которая доступна на официальном сайте компании по адресу <http://e-office.by/produkty/smdo> в разделе с пометкой **ВАЖНО**.

необходимо на рабочем месте пользователя выполнить импорт сертификата с ID-карты в хранилище текущего пользователя (см. [п. 3.3](#) настоящего Руководства).

ВАЖНО!!! При подписании файлов документов с использованием атрибутивных сертификатов, в случае их наличия, перед началом работы с настройками ЭЦП для опции «ИПО (Подпись)» необходимо на рабочем месте пользователя в ПМС Авеста выполнить импорт атрибутивных сертификатов к основному сертификату (см. [п. 3.4](#) настоящего Руководства).

4.2. Выбор вида подписи для сохранения в СЭД

Данная настройка позволяет выбрать вид ЭЦП при ее сохранении в СЭД (рис. 4.2):

Вид подписи при сохранении в СЭД

Выбрать Очистить

Рис. 4.2. Секция для выбора вида подписи на вкладке «ЭЦП» в настройках ИПО_СМДО с опцией «ИПО (Подпись)»

Для выбора вида подписи нажмите кнопку **Выбрать** – отобразится список из справочника «Виды подписей» СЭД (примеры окна на рис. 4.3 и рис. 4.3.1.):

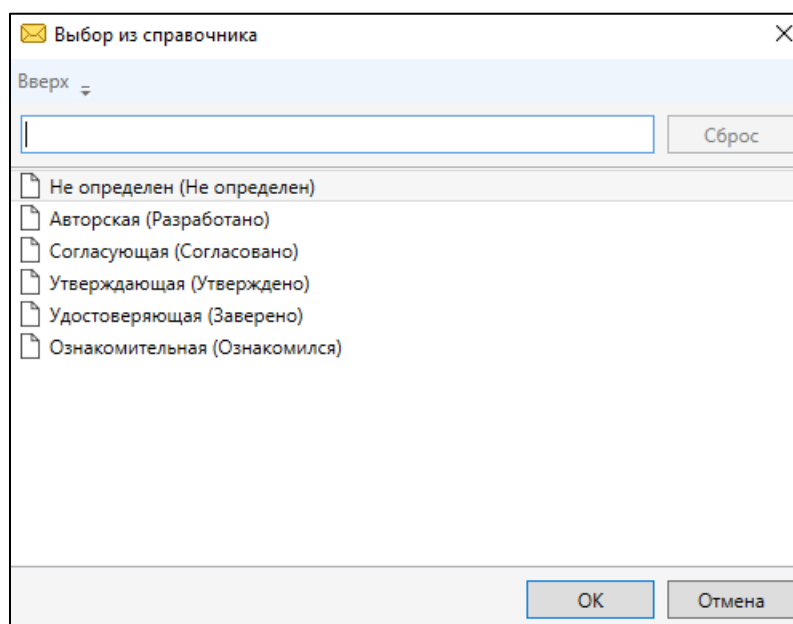


Рис. 4.3. Выбор вида подписи для версии СЭД 24.3 и выше

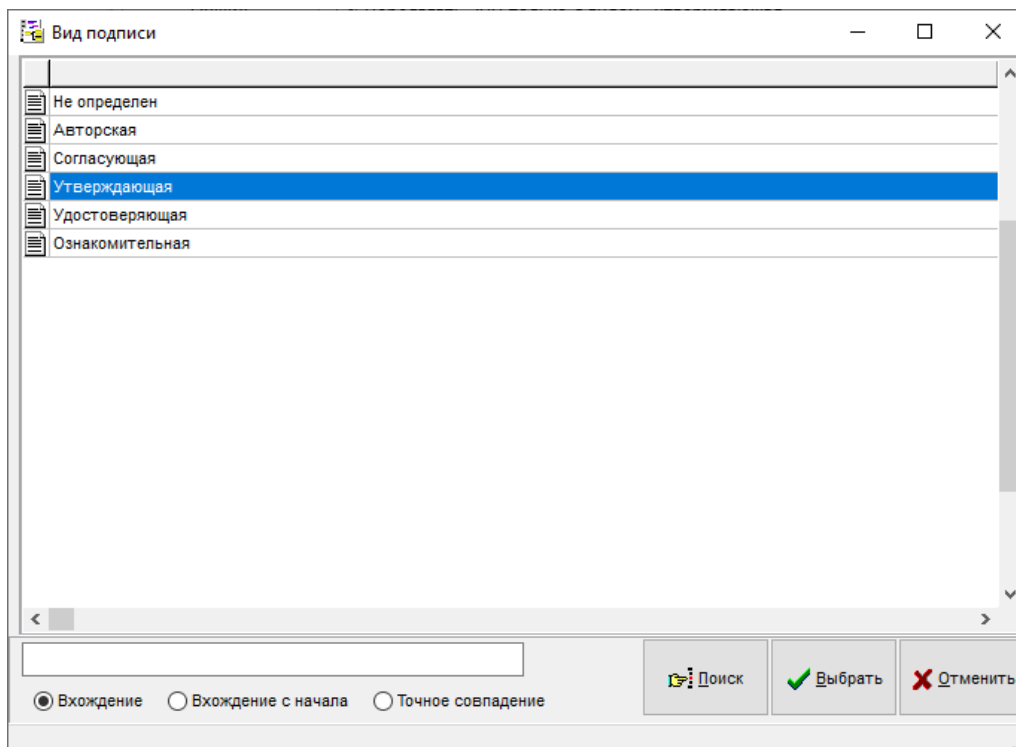


Рис. 4.3.1. Выбор вида подписи для версии СЭД 22.2 и ниже

Из списка видов подписей рекомендуем выбрать вид «Утверждающая». Затем нажмите кнопку **Выбрать**. В поле «Вид подписи при сохранении в СЭД» запишется вид подписи, в скобках запишется текст подписи (рис. 4.4):



Рис. 4.4. Вид подписи, выбранный из справочника СЭД «Виды подписи»

Нажатие на кнопку **Очистить** удаляет данные из поля.

Если поле «Вид подписи при сохранении в СЭД» в настройках ИПО_СМДО не заполнить и оставить пустым, то при сохранении ЭЦП в СЭД вид подписи запишется «Не определен» (примеры на рис. 4.5 и рис. 4.5.1):

ЭЦП файлов						Записей	1
<input checked="" type="checkbox"/> Файл	Вид подписи	Дата	Комментарий	Владелец сертификата	Пользоват		
<input checked="" type="checkbox"/> О перезаклучении договора на ИПО_мини 3Д.docx	Не определен	31.03.2025 13:00		Гулюк Игорь Вадимович, 'Общество с ограниченной ответственностью "Электронн...			

Рис. 4.5. Вид подписи «Не определен» при проверке ЭЦП
в СЭД версии 24.3 и выше

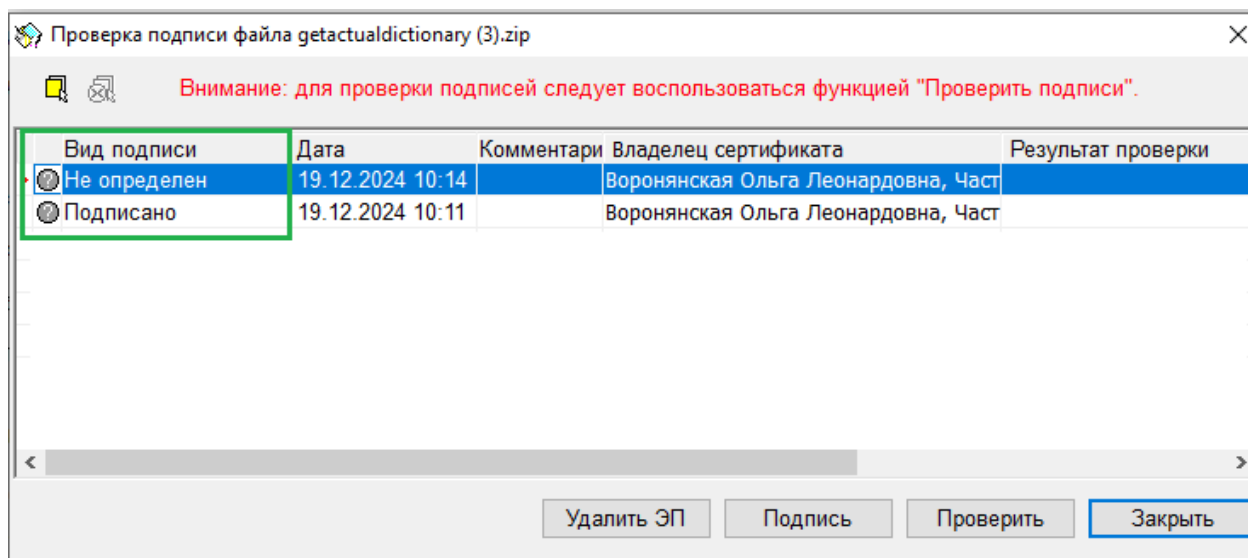


Рис. 4.5.1. Вид подписи «Не определен» при проверке ЭЦП
в СЭД версии 22.2 и ниже

ВАЖНО!!! Элемент справочника СЭД «Виды подписей» состоит из двух значений: вида подписи (не доступен для корректировки) и текста подписи (значение доступно для корректировки) (рис. 4.6 и рис. 4.6.1):



Рис. 4.6. Пример редактирования текста подписи с видом «Утверждающая»
в СЭД версии 24.3 и выше

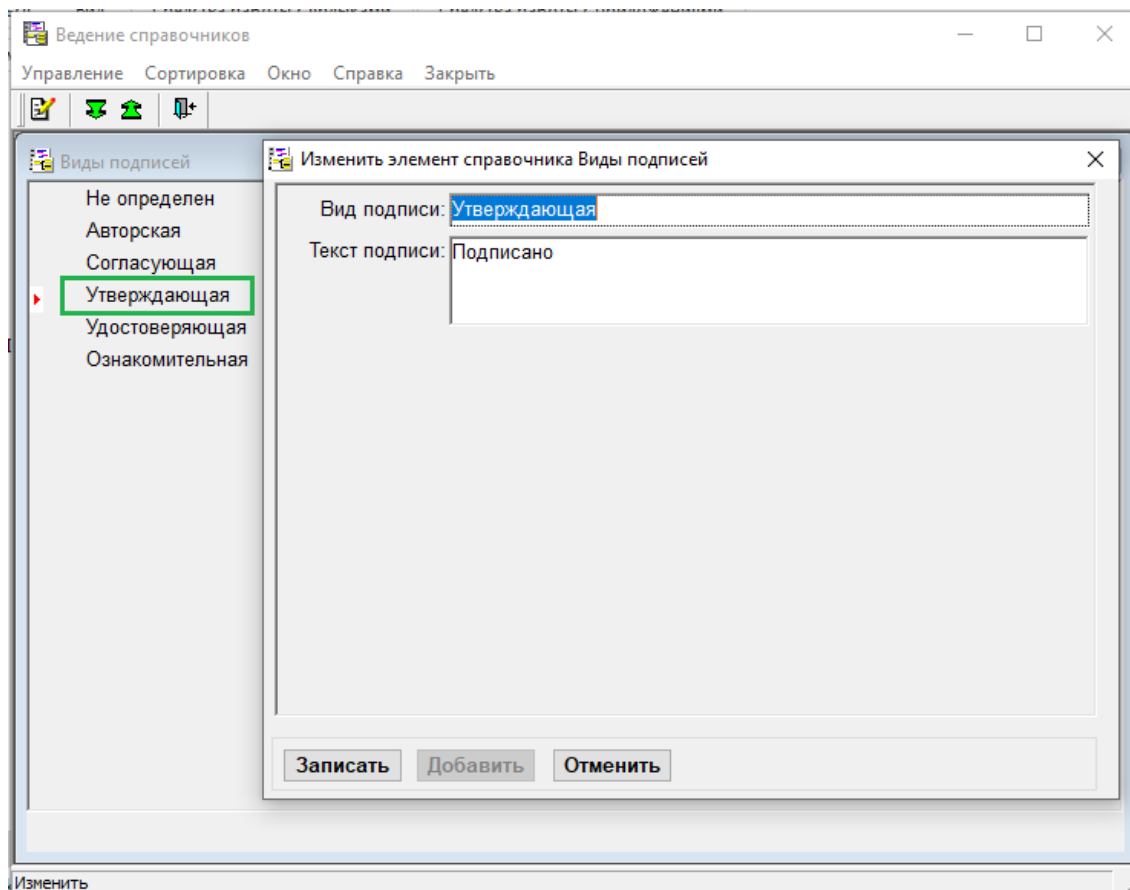


Рис. 4.6.1. Пример редактирования текста подписи с видом «Утверждающая» в СЭД версии 22.2 и ниже

При выработке и проверке ЭЦП в интерфейсе клиента ДЕЛА отображается **текст** подписи.

4.3. Выбор сертификата для использования по умолчанию при выработке ЭЦП

На вкладке «ЭЦП» в настройках ИПО_СМДО с опцией «ИПО (Подпись)» можно выбрать сертификат, который будет использоваться по умолчанию при подписании файлов документов (рис. 4.7):

Сертификат для подписания файлов

Сертификат для подписания: Выбрать Очистить

Атрибутные сертификаты:

☐ Носитель ключевой информации (НКИ)

☐ ID-карта

Рис. 4.7. Секция для назначения сертификата по умолчанию

Для выбора сертификата из хранилища сертификатов текущего пользователя нажмите кнопку **Выбрать**. Откроется окно выбора сертификата (пример на рис. 4.8):

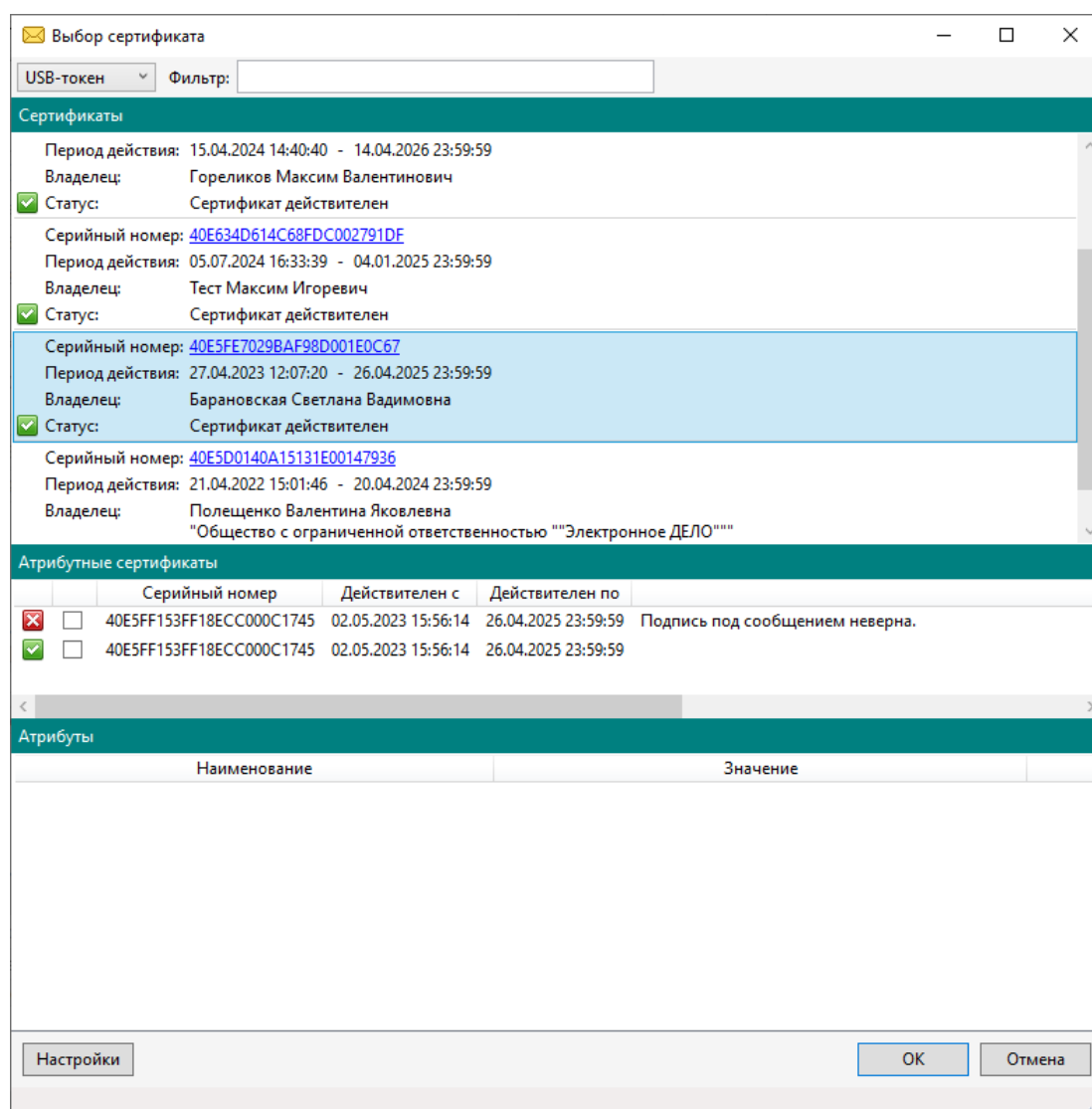
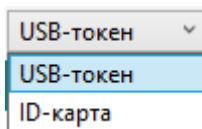


Рис. 4.8. Пример окна выбора сертификата

В верхнем левом углу окна «Выбор сертификата» размещен



переключатель выбора типа НКИ. По умолчанию отображается тип носителя USB-токен и сертификаты, находящиеся в личном хранилище текущего пользователя и выданные РУЦ ГосСУОК. При выборе в качестве НКИ ID-карты отображаются сертификаты, относящиеся к сетевому справочнику ПМС Авеста, выданные РУЦ ГосСУОК со сроком действия не менее 10 лет.

Примеры отображения сертификатов для разных типов носителей представлены на рис. 4.9:

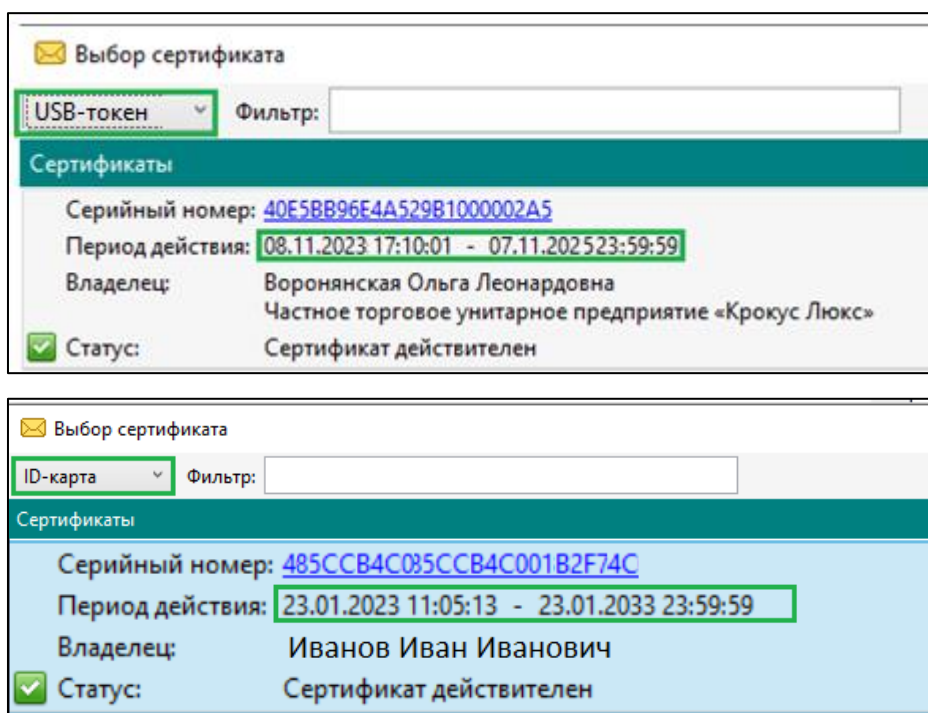
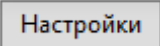


Рис. 4.9. Примеры сертификатов для разных типов НКИ

Визуально сертификаты отличаются только периодом действия. Сертификаты для USB-токенов выдаются на 1 или 2 года, сертификаты для ID-карт выдаются на 10 лет.

Для отображения данных атрибутивных сертификатов предназначены секции «Атрибутивные сертификаты» и «Атрибуты» (см. [рис. 4.8](#)).

Рядом с кнопкой выбора типа НКИ расположено поле «Фильтр», которое предназначено для отбора сертификатов по заданному критерию. По умолчанию поле пустое.

В левом нижнем углу размещена кнопка , которая поднимает окно с дополнительными возможностями (рис. 4.10):

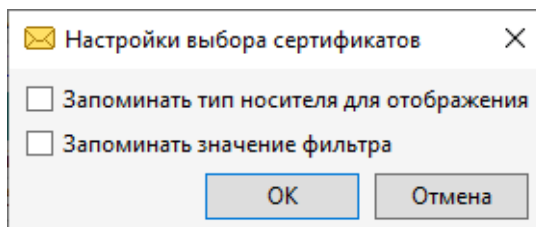
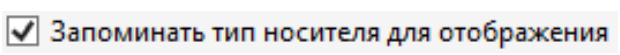
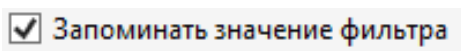


Рис. 4.10. Окно для сохранения настроек при выборе сертификата

-  — позволяет запомнить выбранный тип носителя «ID-карта» при каждом поднятии окна. По умолчанию окно «Выбор сертификата» открывается с установленным носителем «USB-токен»;
-  — позволяет сохранить значение, введенное в поле «Фильтр» при каждом открытии окна «Выбор сертификата»;
- По умолчанию флаги сняты. Выберите нужные для сохранения параметры и нажмите кнопку **ОК**. По нажатию кнопки **Отмена** настройки не сохраняются.

В секции **Сертификаты** окна «Выбор сертификата» выберите нужный сертификат при помощи клика левой клавишей мыши по его записи. Запись сертификата поменяет цвет на голубой.

Если у выбранного сертификата есть атрибутивные сертификаты, то для просмотра атрибутов атрибутивного сертификата выделите запись нужного атрибутивного сертификата в секции **Атрибутивные сертификаты** при помощи клика левой клавишей мыши. Запись атрибутивного сертификата поменяет цвет на голубой и в секции **Атрибуты** отобразятся значения атрибутов атрибутивного сертификата (пример на рис. 4.11):

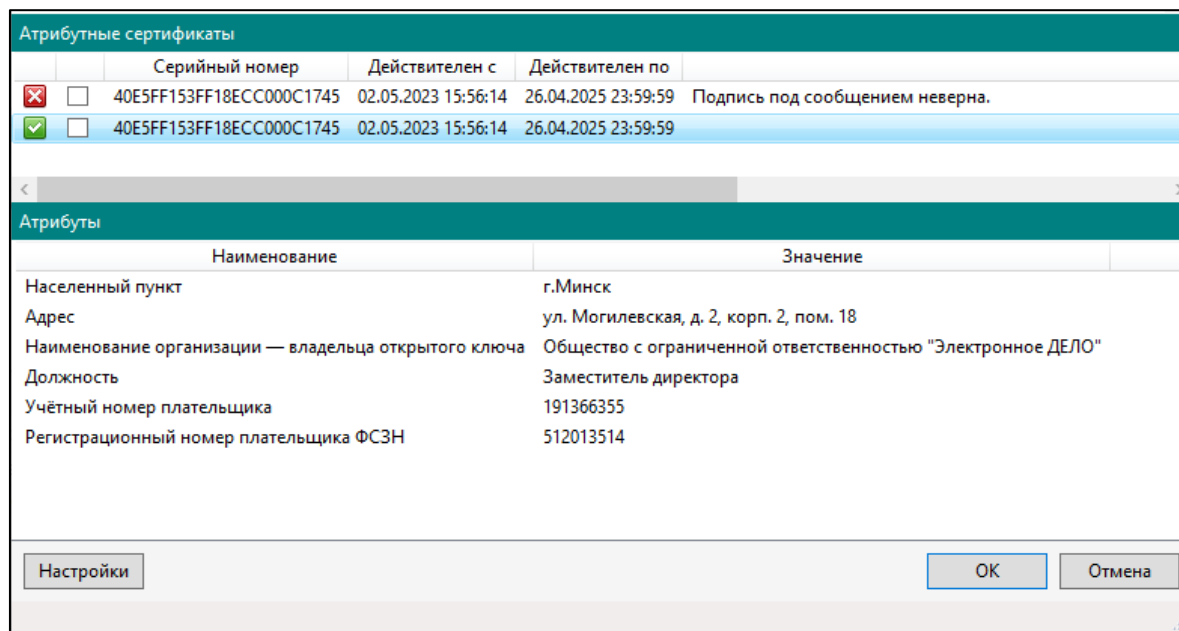


Рис. 4.11. Пример части окна «Выбор сертификата» с выбранным атрибутивным сертификатом и его атрибутами

Для включения нужного атрибутивного сертификата в ЭЦП при ее выработке поставьте флаг в записи атрибутивного сертификата в секции **Атрибутные сертификаты** (рис. 4.12):

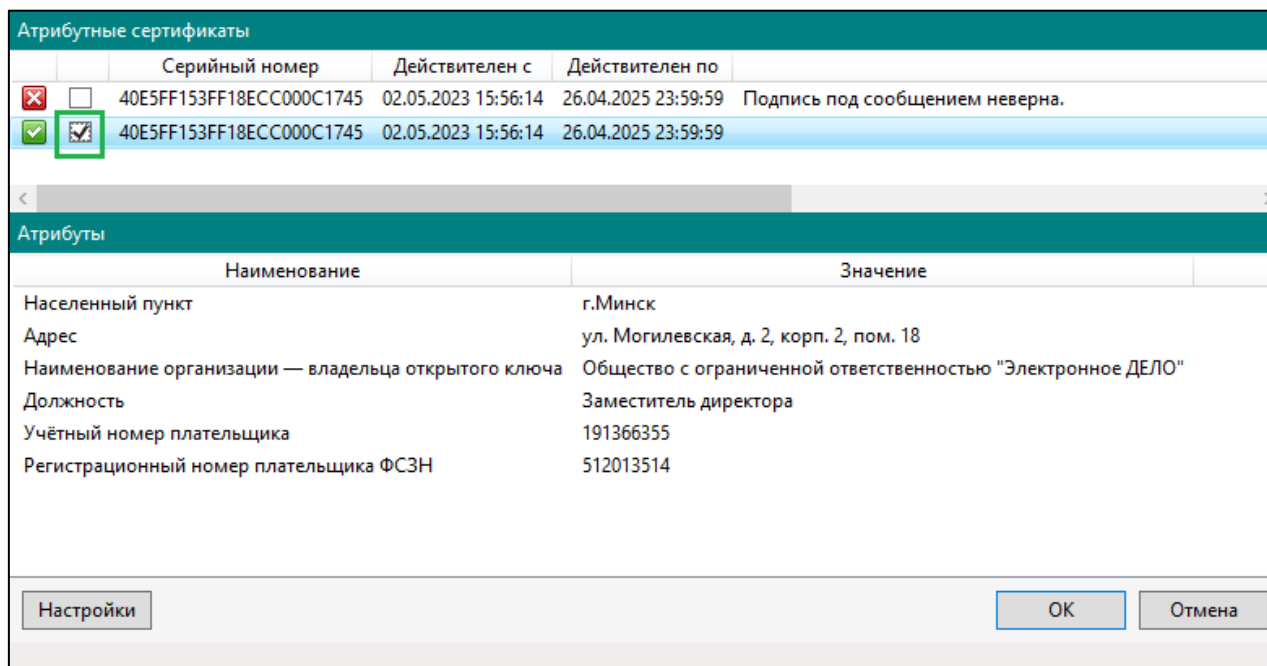


Рис. 4.12. Выбор нужного атрибутивного сертификата для включения в ЭЦП при помощи выставления флага

Завершив действия в окне «Выбор сертификата» подтвердите выбор, нажав кнопку **ОК**, или отмените выбор, нажав кнопку **Отмена**.

Если сертификат был выбран в окне «Выбор сертификата», то в секции «Сертификат для подписания файлов» на вкладке «ЭЦП» отобразятся сведения о нем (пример на рис. 4.13):

Сертификат для подписания файлов

Сертификат для подписания: Выбрать Очистить

Барановская Светлана Вадимовна

Атрибутные сертификаты:

40E5FF153FF18ECC000C1745

Носитель ключевой информации (НКИ):

☒ USB-токен ☐ ID-карта

Рис. 4.13. Пример сертификата, выбранного для использования по умолчанию при подписании файлов документов

Кнопка **Очистить** очищает поля секции «Сертификат для подписания файлов».

Если сертификат для использования по умолчанию не выбран на вкладке «ЭЦП» в настройках ИПО_СМДО с опцией «ИПО (Подпись)», то при каждом подписании файла будет подниматься окно «Выбор сертификата».

Для сохранения настроек на вкладке «ЭЦП» нажмите кнопку **Сохранить**.

Для отмены настроек на вкладке «ЭЦП» воспользуйтесь кнопкой **Отмена**.

4.4. Секция «Дополнительно» на вкладке «ЭЦП» в настройках ИПО_СМДО

В секции «Дополнительно» размещены кнопки, запускающие следующие функции:

Дополнительно

Действия с сертификатом ID-карты

Актуализация данных после обновления СОС и сертификатов УЦ

- **Действия с сертификатом ID-карты** – открывает окно с дополнительными действиями с сертификатом ID-карты (см. [п. 3.3](#)).

- **Актуализация данных после обновления СОС и сертификатов УЦ** — запускает актуализацию данных после обновления СОС и сертификатов УЦ.

В связи с тем, что обновления СОС и сертификатов УЦ во время работы ИПО_СМДО происходит сторонним программным обеспечением (например, в ПМС Авеста), а для проверки ЭЦП необходимо иметь актуальные данные, рекомендуем перед проверкой подписи запускать в ИПО_СМДО актуализацию СОС и сертификатов УЦ.

После завершения актуализации отобразится информационное сообщение (рис. 4.14):

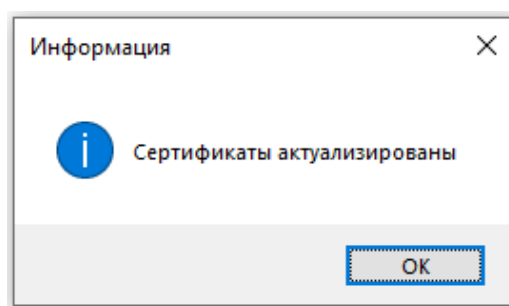


Рис. 4.14. Сообщение о завершении процесса актуализации данных в ИПО_СМДО после обновления СОС и сертификатов УЦ

5. РАБОТА ОПЦИИ «ИПО (ПОДПИСЬ)»

5.1. Возможности функции подписания файлов в ИПО_СМДО с опцией «ИПО (Подпись)»

Все файлы документов, отобранных из СЭД для отправки по СМДО, подписываются в логической папке «Для отправки».

В опции «ИПО (Подпись)» реализованы следующие возможности подписания файлов:

- подписание в документе выборочных или всех файлов;
- подписание всех файлов в нескольких выделенных документах.

Подписание файлов одного документа:

Подписание файлов одного документа осуществляется по кнопке **Подписать**, расположенной в секции **ФАЙЛЫ** логической папки «Для отправки» (рис. 5.1):

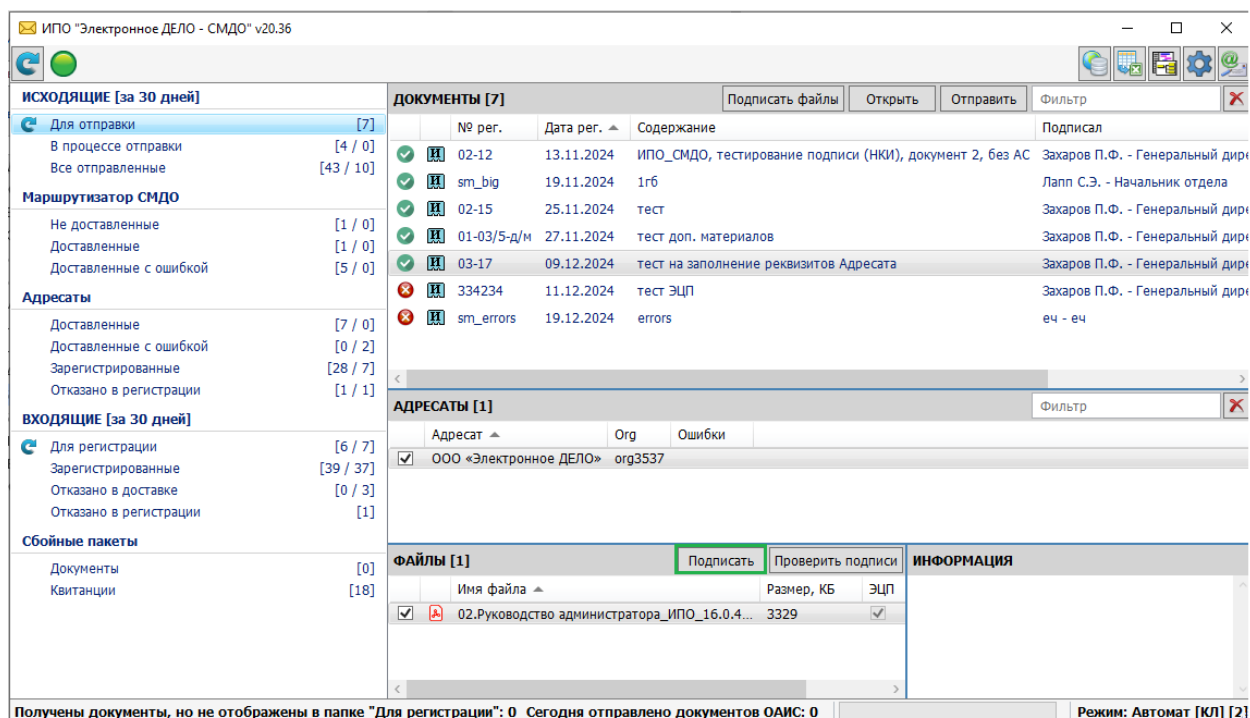


Рис. 5.1. Кнопка **Подписать** в секции **ФАЙЛЫ** для подписи файлов одного документа

Кнопка **Подписать** активна, только при наличии файлов в секции **ФАЙЛЫ**, в противном случае кнопка будет не активна (рис. 5.2):

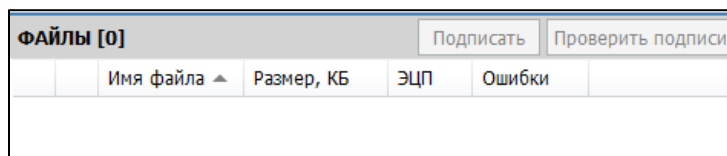


Рис. 5.2. Неактивная кнопка **Подписать** в секции **ФАЙЛЫ** в логической папке «Для отправки»

Подписание файлов может выполняться независимо от наличия у них ранее сформированных ЭЦП (рис. 5.3):

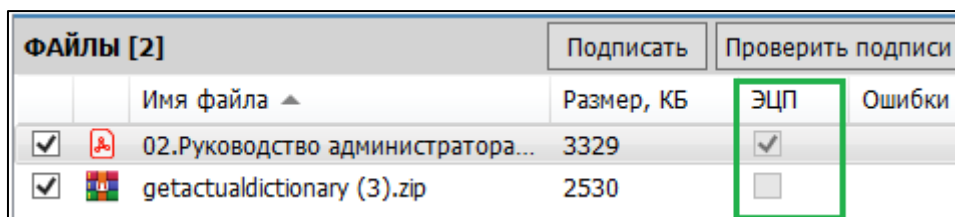


Рис. 5.3. Отметка о наличии ЭЦП у файлов

ВАЖНО!!! При нажатии кнопки **Подписать** в секции **ФАЙЛЫ** подпись формируется для файлов, отмеченных флагами в списке файлов (рис. 5.4):

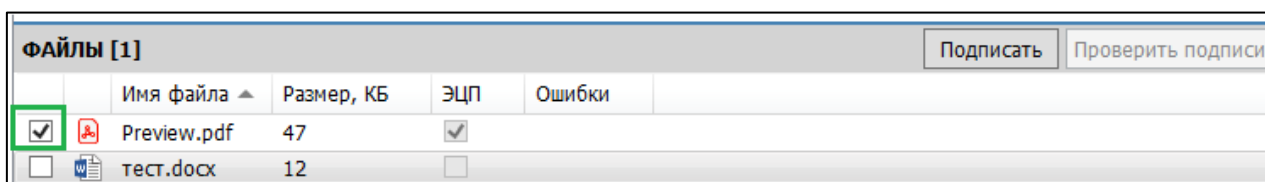


Рис. 5.4. Выбор файлов в секции **ФАЙЛЫ**

Дальнейшие действия пользователя зависят от настроек вкладки «ЭЦП» и типа НКИ, используемого для подписания файлов (см. [п. 5.2](#), [п. 5.3](#) настоящего Руководства).

Подписание всех файлов в выделенных документах:

Подписание сразу всех файлов в выделенных документах осуществляется по кнопке **Подписать файлы** в секции **ДОКУМЕНТЫ** логической папки «Для отправки» (рис. 5.5):

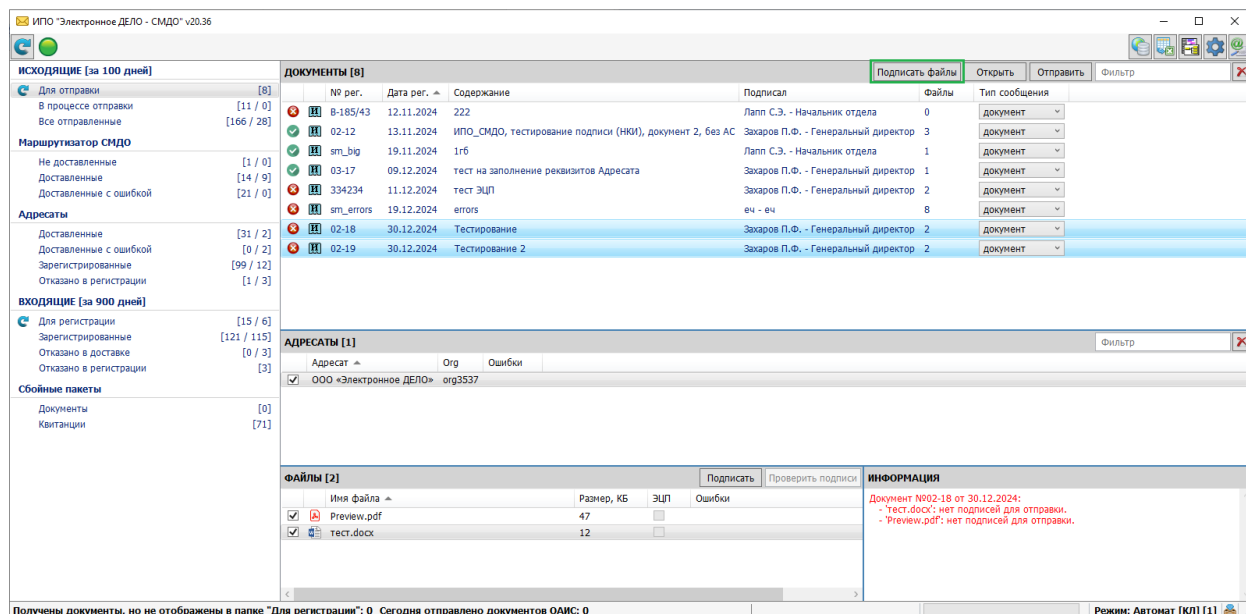


Рис. 5.5. Кнопка **Подписать файлы** в секции **ДОКУМЕНТЫ** для подписи всех файлов выделенных документов

Выделение документов в секции **ДОКУМЕНТЫ** осуществляется стандартными способами: клик левой клавишей мыши + Ctrl – выделение отдельных записей, клик левой клавишей мыши + Shift – выделение списка записей от ранее выделенной до текущей, к которой применяется выделение. При выделении записи документов окрашиваются в голубой цвет.

После нажатия кнопки **Подписать файлы** поднимется окно с запросом на продолжение операции (рис. 5.6):

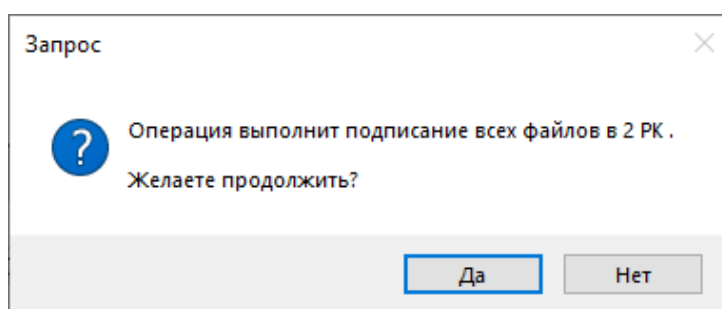


Рис. 5.6. Окно с запросом на продолжение операции подписания всех файлов выделенных документов

Нажмите на кнопку **Да**, если хотите продолжить операцию подписания. Нажмите на кнопку **Нет** для отмены операции подписания.

ВАЖНО!!! При выполнении подписания файлов, вызванного нажатием кнопки **Подписать файлы** в секции **ДОКУМЕНТЫ**, подписываются все файлы документов, выделенных на момент нажатия кнопки.

Дальнейшие действия пользователя зависят от настроек вкладки «ЭЦП» и типа НКИ, используемого для подписания файлов (см. [п. 5.2](#), [п. 5.3](#) настоящего Руководства).

5.2. Подписание файлов с использованием USB-токена в ИПО_СМДО с опцией «ИПО (Подпись)»

После нажатия в логической папке «Для отправки» кнопки **Подписать** в секции **ФАЙЛЫ** или кнопки **Подписать файлы** в секции **ДОКУМЕНТЫ** в случае, если в настройках ИПО_СМДО на вкладке «ЭЦП» не выбран сертификат для использования по умолчанию, поднимется окно «Выбор сертификата» (пример на рис. 5.7):

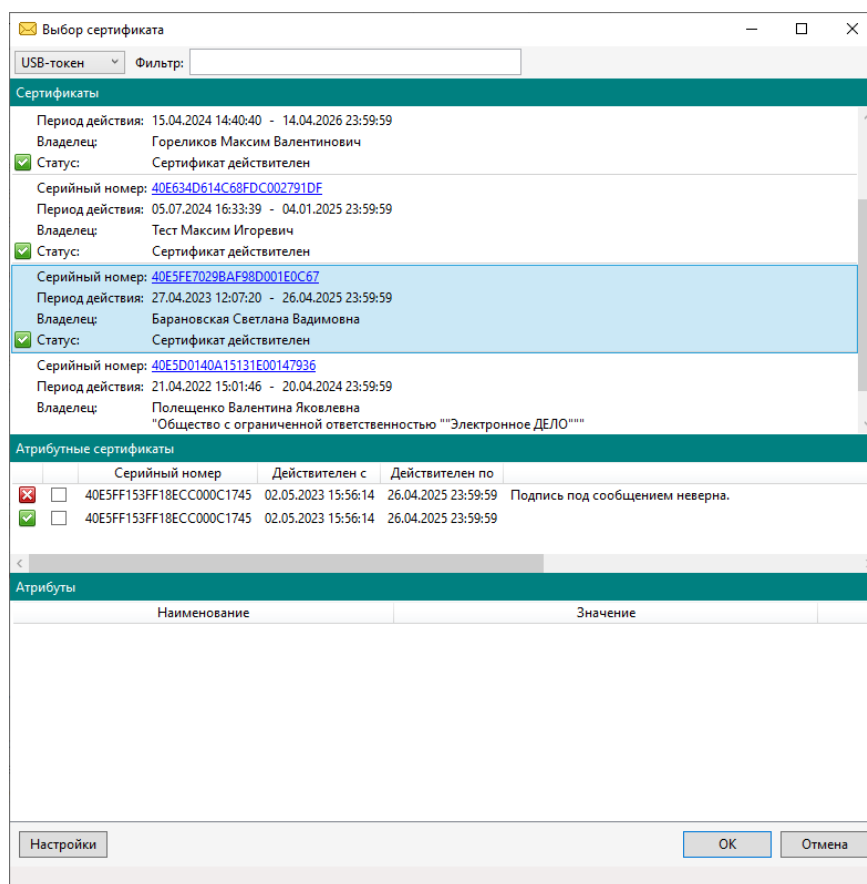
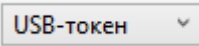


Рис. 5.7. Пример окна «Выбор сертификата» с выбранным типом носителя USB-токен

В окне «Выбор сертификата» в качестве НКИ должен быть выбран . Следуя правилам работы в окне «Выбор сертификата», описанным в [п. 4.3](#) настоящего Руководства, выберите нужный основной сертификат и атрибутный сертификат, в случае необходимости его использования. Завершите выбор нажатием кнопки **ОК**. При нажатии кнопки **Отмена** в окне «Выбор сертификата» процесс подписания файлов будет отменен.

Далее поднимется окно СКЗИ Авеста для ввода пароля к контейнеру с закрытым ключом (рис. 5.8). Если на вкладке «ЭЦП» в настройках ИПО_СМДО был выбран сертификат для использования по умолчанию с типом НКИ USB-токен, то окно СКЗИ Авеста для ввода пароля к контейнеру с закрытым ключом поднимется сразу после начала процесса подписания файлов.

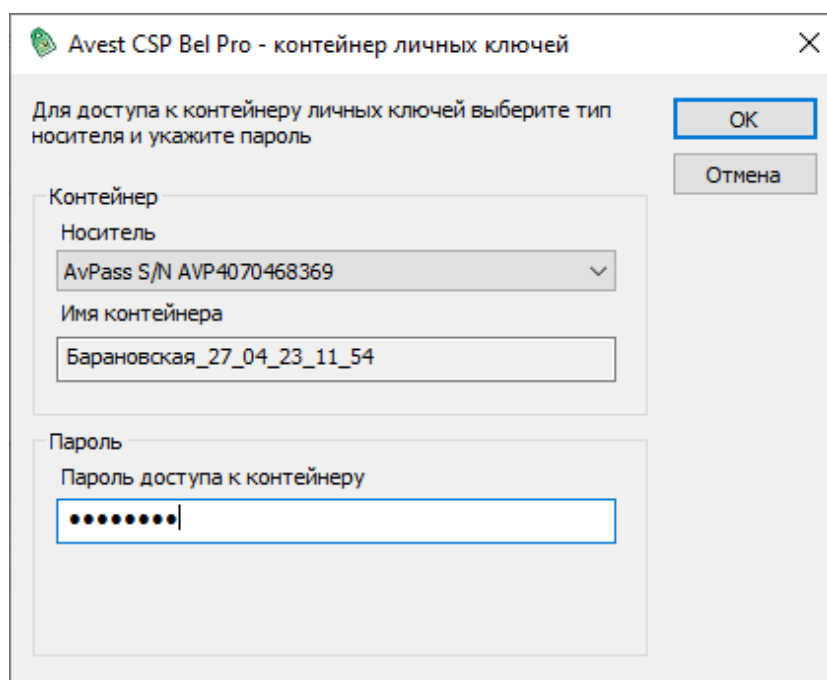


Рис. 5.8. Окно СКЗИ Авеста для ввода пароля к контейнеру с закрытым ключом

Введите пароль и нажмите кнопку **ОК** для продолжения подписания файлов. Если хотите отменить подписание файлов, нажмите кнопку **Отмена**.

При завершении подписания файлов в зависимости от кнопки, запустившей процесс подписания, выдается одно из сообщений (рис. 5.9, рис. 5.10):

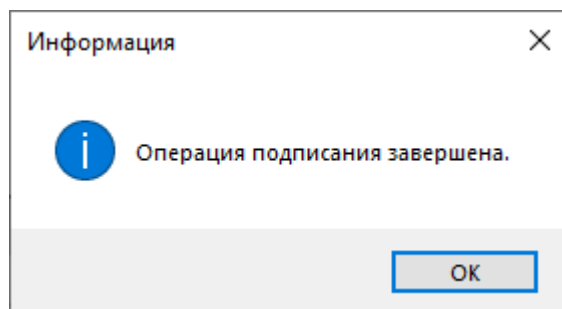


Рис. 5.9. Сообщение о завершении процесса подписания файлов одного документа (запущен по нажатию кнопки **Подписать** в секции **ФАЙЛЫ**)

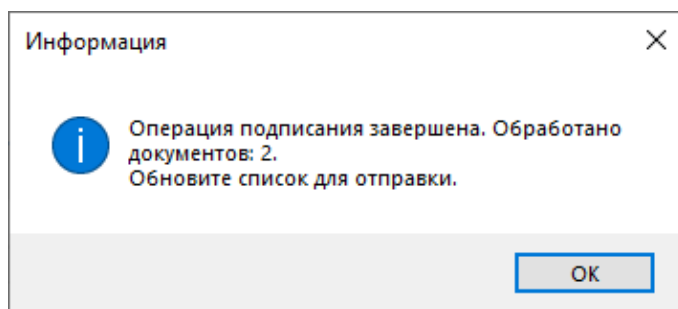


Рис. 5.10. Сообщение о завершении процесса подписания файлов нескольких выделенных документов (запущен по нажатию кнопки **Подписать файлы** в секции **ДОКУМЕНТЫ**)

В процессе подписания файлов документов с использованием USB-токена в ИПО_СМДО с опцией «ИПО (Подпись)» неверные действия пользователя могут сопровождаться сообщениями (рис. 5.11, рис. 5.12):

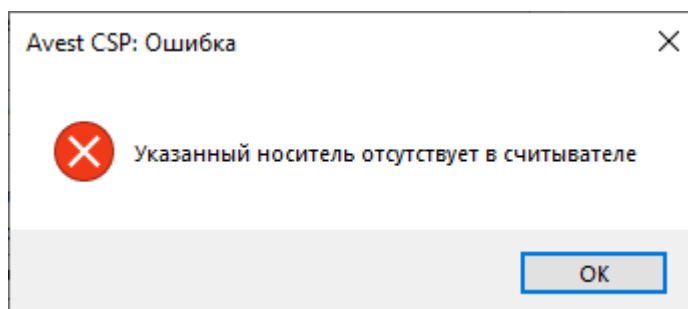


Рис. 5.11. Сообщение, если у пользователя не подключен USB-токен, или на подключенном USB-токене отсутствует требуемый контейнер с закрытым ключом

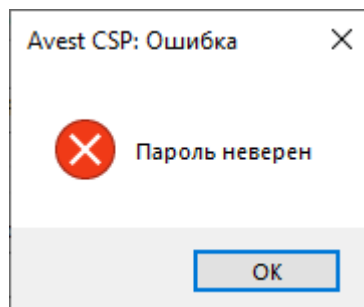


Рис. 5.12. Сообщение, если пользователь ввел неверный пароль к контейнеру с закрытым ключом

Сформированные подписи файлов добавляются в РК документа в СЭД и доступны в ней для проверки и просмотра сведений (пример на рис. 5.13 и рис. 5.13.1):

ЭЦП файлов							Записей 1
<input checked="" type="checkbox"/> Файл	Вид подписи	Дата	Комментарий	Владелец сертификата	Пользователь	<input checked="" type="checkbox"/> Результат прове...	↑
<input checked="" type="checkbox"/> Образец гарантийного письма для переноса базы (ЗОО).doc	Не определен	09.07.2025 12:28		Гулюк Игорь Вадимович Общество с ограниченной ответственностью "Электронн...		✓ Подпись: действительна; Сертификат: действителен	

Рис. 5.13. Пример проверки в РК документа подписи файла, сформированной в ИПО_СМДО с опцией «ИПО (Подпись)», для версии СЭД 24.3 и выше

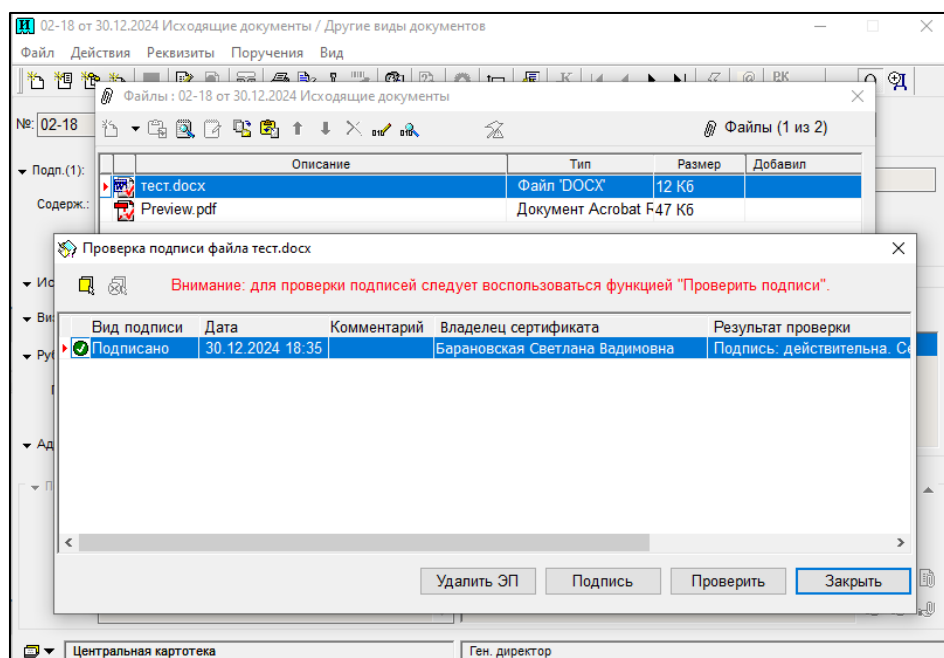


Рис. 5.13.1. Пример проверки в РК документа подписи файла, сформированной в ИПО_СМДО с опцией «ИПО (Подпись)», для версии СЭД 22.2 и ниже

5.3. Подписание файлов с использованием ID-карты в ИПО_СМДО с опцией «ИПО (Подпись)»

После нажатия в логической папке «Для отправки» кнопки **Подписать** в секции **ФАЙЛЫ** или кнопки **Подписать файлы** в секции **ДОКУМЕНТЫ** в случае, если в настройках ИПО_СМДО на вкладке «ЭЦП» не выбран сертификат для использования по умолчанию, поднимется окно «Выбор сертификата» (пример на рис. 5.14):

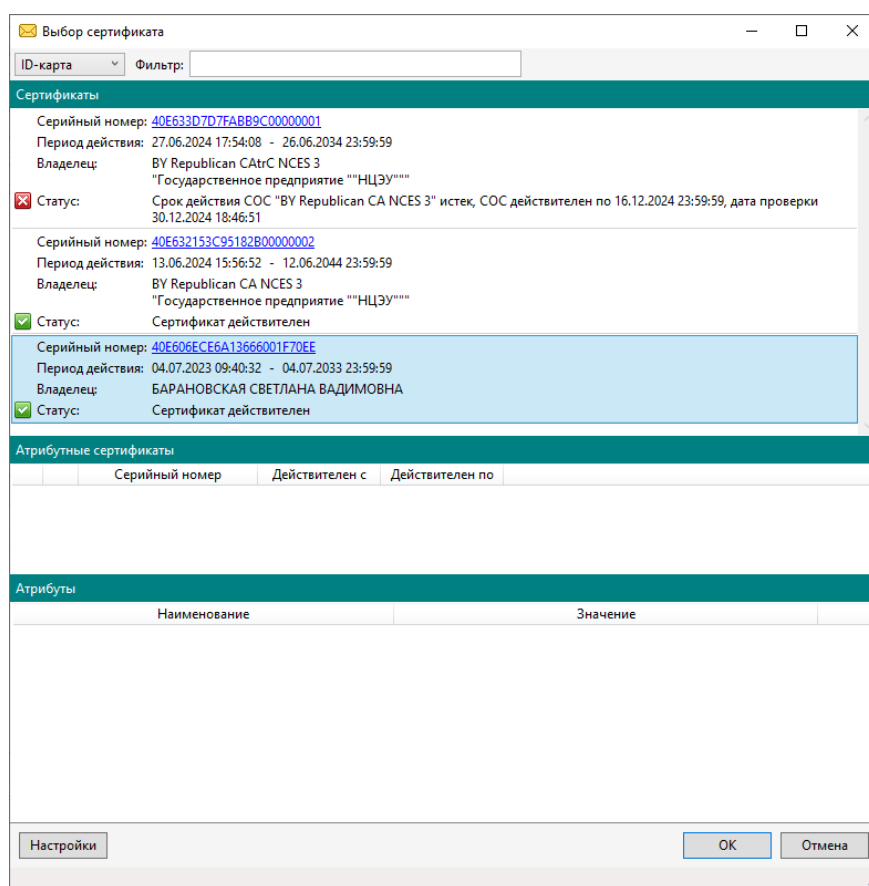
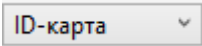


Рис. 5.14. Пример окна «Выбор сертификата» с выбранным типом носителя ID-карта

В окне «Выбор сертификата» в качестве НКИ должна быть выбрана . Следуя правилам работы в окне «Выбор сертификата», описанным в [п. 4.3](#) настоящего Руководства, выберите нужный основной сертификат и атрибутный сертификат, в случае необходимости его использования. Завершите выбор нажатием кнопки **ОК**. При нажатии кнопки

Отмена в окне «Выбор сертификата» процесс подписания файлов будет отменен.

ВАЖНО!!! При работе с ID-картой к персональному компьютеру пользователя должен быть подключен считыватель для работы с ID-картой. В случае чтения карты по бесконтактному интерфейсу ID-карта прикладывается к устройству. Для чтения контактным способом ID-карта вставляется в считыватель. Если ID-карта распознана считывателем, то на устройстве загорается зеленый индикатор (обязательное условие для работы с ID-картой). Если есть проблемы с распознаванием ID-карты, то на устройстве загорится красный индикатор (работа с ID-картой не возможна).

ВАЖНО!!! При работе с ID-картой на персональном компьютере пользователя должна быть запущена [Клиентская программа](#), в настройках которой в качестве устройства выбрана ID-карта и **определен считыватель ID-карты**, подключенный к компьютеру пользователя (рис. 5.15):

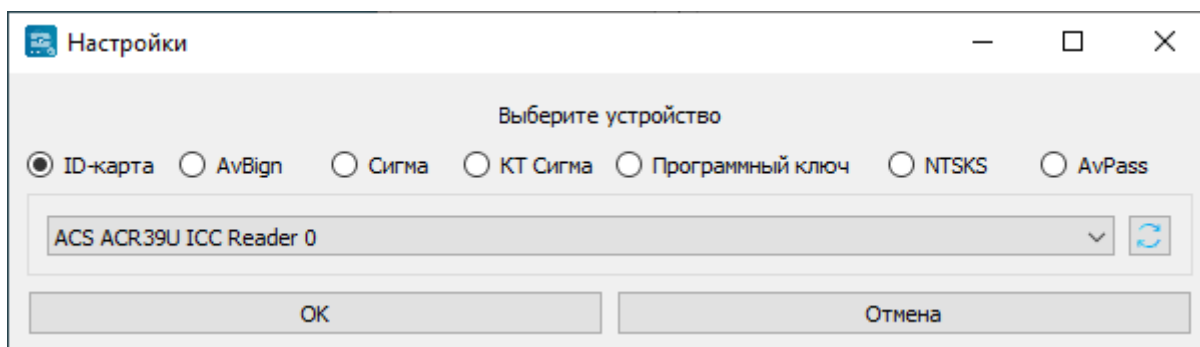


Рис. 5.15. Настройка КП для работы с ID-картой

ВАЖНО!!! При работе с ID-картой пользователь должен знать PIN1 и PIN2, предоставленные ему при получении ID-карты.

Далее, если ранее не была пройдена аутентификация в КП, поднимется окно КП для ввода PIN1. Если на вкладке «ЭЦП» в настройках ИПО_СМДО был выбран сертификат для использования по умолчанию с типом НКИ ID-карта, и ранее не была пройдена аутентификация в КП, то окно КП для ввода PIN1 поднимется сразу после начала процесса подписания файлов. Введите PIN1 и нажмите кнопку **ОК** (рис. 5.16):

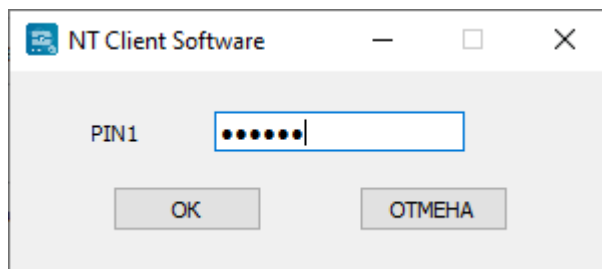


Рис. 5.16. Ввод PIN1 в окно КП

Затем поднимется окно КП для ввода PIN2. Если аутентификация в КП была пройдена ранее, то поднимется сразу окно КП для ввода PIN2. Введите PIN2 и нажмите кнопку **ОК** (рис. 5.17):

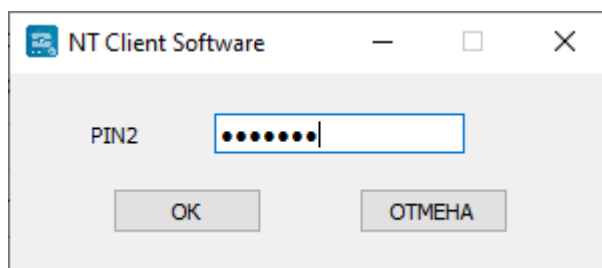


Рис. 5.17. Ввод PIN2 в окно КП

ВАЖНО!!! Так как КП поднимает окно для ввода PIN2 для каждого подписываемого файла, то необходимо вводить значение PIN2 и нажимать кнопку **ОК** столько раз, сколько окон для ввода PIN2 поднимает КП. Нажатие на кнопку **ОТМЕНА** приведет к отмене операции подписания файла, для которого запрашивается ввод PIN2.

При завершении подписания файлов в зависимости от кнопки, запустившей процесс подписания, выдается одно из сообщений (рис. 5.18, рис. 5.19):

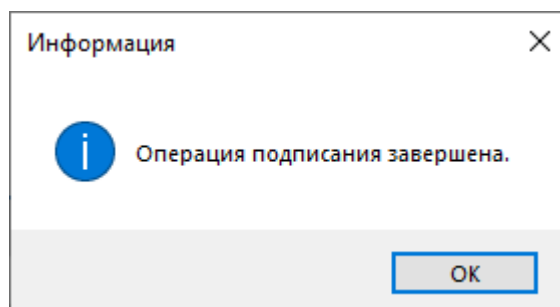


Рис. 5.18. Сообщение о завершении процесса подписания файлов одного документа (запущен по нажатию кнопки **Подписать** в секции **ФАЙЛЫ**)

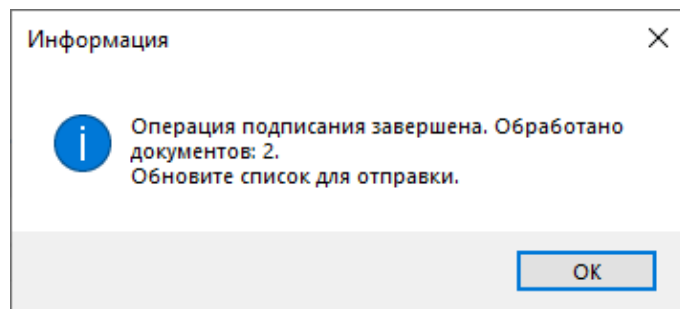


Рис. 5.19. Сообщение о завершении процесса подписания файлов нескольких выделенных документов (запущен по нажатию кнопки **Подписать файлы** в секции **ДОКУМЕНТЫ**)

В процессе подписания файлов документов с использованием ID-карты в ИПО_СМДО с опцией «ИПО (Подпись)» неверные действия пользователя могут сопровождаться сообщениями (рис.5.20 – 5.23):

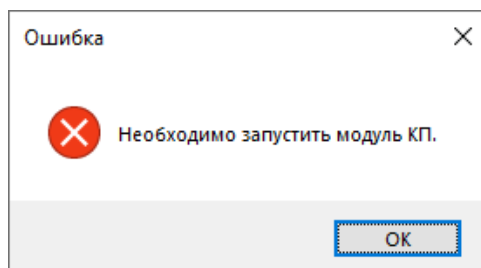


Рис. 5.20. Сообщение, если у пользователя не запущена КП

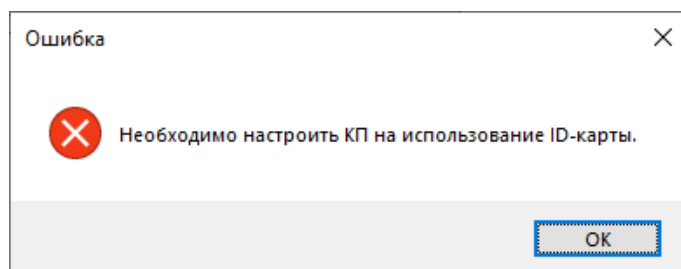


Рис. 5.21. Сообщение, если в настройках КП в качестве устройства не выбрана ID-карта

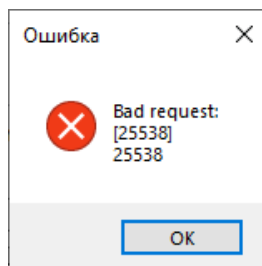


Рис. 5.22. Сообщение, если не верно введен PIN1

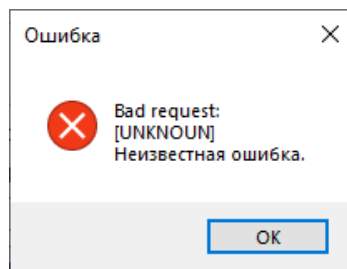


Рис. 5.23. Сообщение, если не верно введен PIN2

Сформированные подписи файлов добавляются в РК документа в СЭД и доступны в ней для проверки и просмотра сведений (пример на рис. 5.24 и рис. 5.24.1):

ЭЦП файлов							Записей 1
Файл	Вид подписи	Дата	Комментарий	Владелец сертификата	Пользователь	Результат проверки	
Введение в систему.pdf	Не определен	09.07.2025 18:09		БАРАНОВСКАЯ СВЕТЛАНА ВАДИМОВНА		✓ Подпись: действительна; Сертификат: действителен	

Рис. 5.24. Пример проверки в РК документа подписи файла, сформированной в ИПО_СМДО с опцией «ИПО (Подпись)», для версии СЭД 24.3 и выше

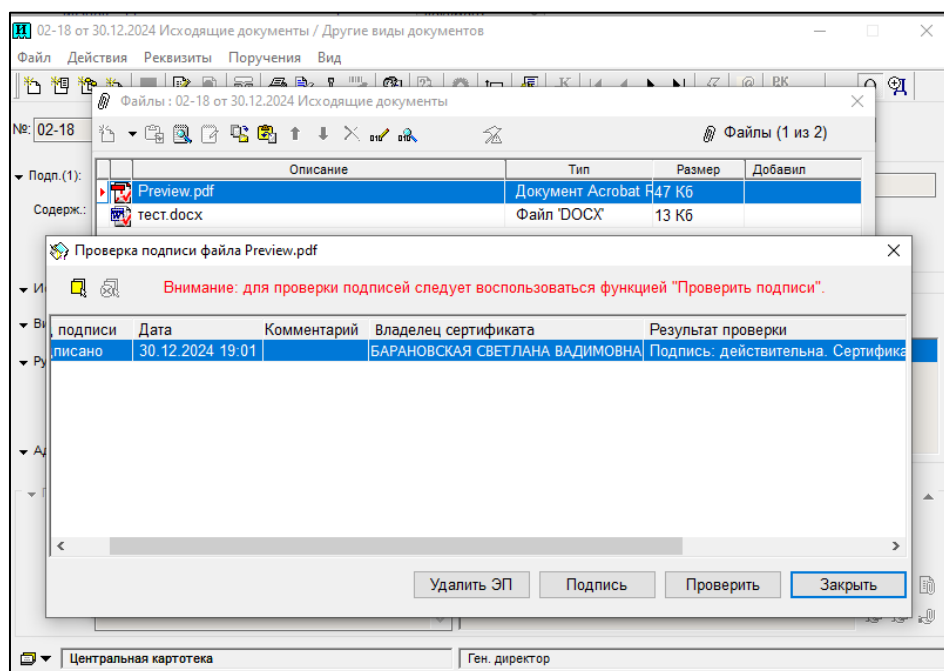


Рис. 5.24.1. Пример проверки в РК документа подписи файла, сформированной в ИПО_СМДО с опцией «ИПО (Подпись)», для версии СЭД 22.2 и ниже

ВАЖНО!!! В РК документа СЭД «Электронное ДЕЛО» версии 22.2 и ниже подписи, сформированные в ИПО_СМДО с опцией «ИПО (Подпись)» с Разработчик постоянно улучшает потребительские свойства ИПО и рекомендует всегда использовать последнюю актуальную версию продукта, которая доступна на официальном сайте компании по адресу <http://e-office.by/produkty/smdo> в разделе с пометкой **ВАЖНО**.

использованием ID-карты, не могут быть удалены из РК, т.к. указанные версии СЭД не поддерживают работу со средствами ЭЦП с использованием ID-карты. При попытке удалить ЭЦП выводится сначала запрос на подтверждение удаления ЭЦП (рис. 5.25), и при нажатии в нем кнопки **ДА** выдается ошибка (рис. 5.26):

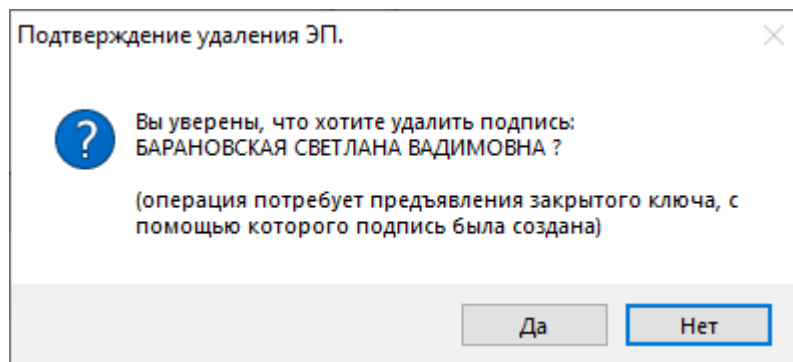


Рис. 5.25. Запрос на подтверждения удаления ЭЦП в «толстом» клиенте СЭД «Электронное ДЕЛО» версии 22.2 и ниже

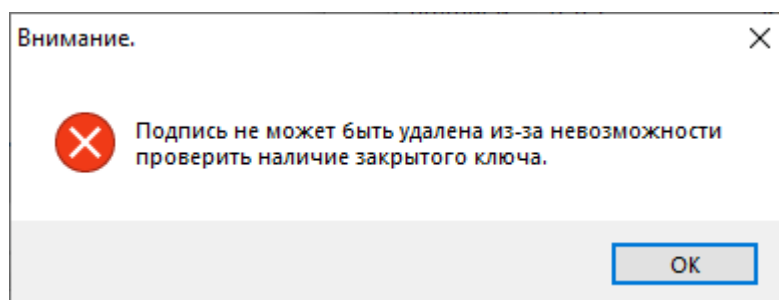


Рис. 5.26. Ошибка при попытке удаления ЭЦП, сформированной в ИПО_СМДО с опцией «ИПО (Подпись)» с использованием ID-карты

5.4. Проверка подписи в ИПО_СМДО с опцией «ИПО (Подпись)»

Функционал по проверке подписи в ИПО_СМДО с опцией «ИПО (Подпись)» реализован по нажатию кнопки **Проверить подписи**, расположенной в секции **ФАЙЛЫ** во всех логических папках кроме папок **ИСХОДЯЩИЕ / В процессе отправки** и **ВХОДЯЩИЕ / Сбойные пакеты / Квитанции** (рис. 5.27):

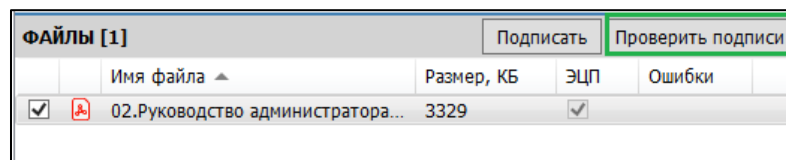


Рис. 5.27. Кнопка **Проверить подписи** в секции **ФАЙЛЫ**

Если в секции **ФАЙЛЫ** нет ни одного файла, или в файле, выделенном для проверки подписи, нет ни одной ЭЦП, то кнопка не активна (рис. 5.28):

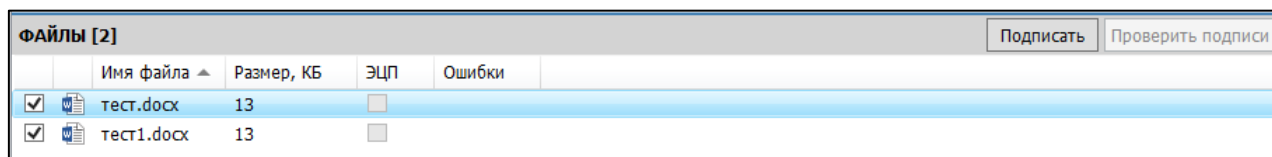


Рис. 5.28. Неактивная кнопка **Проверить подписи** для файла, у которого нет ни одной ЭЦП

Проверка подписи выполняется для всех ЭЦП одного файла. Для этого выделите нужный файл в секции **ФАЙЛЫ** левым кликом мыши и нажмите кнопку **Проверить подписи**. Откроется окно «Проверка ЭЦП» с результатами проверки (пример на рис. 5.29):

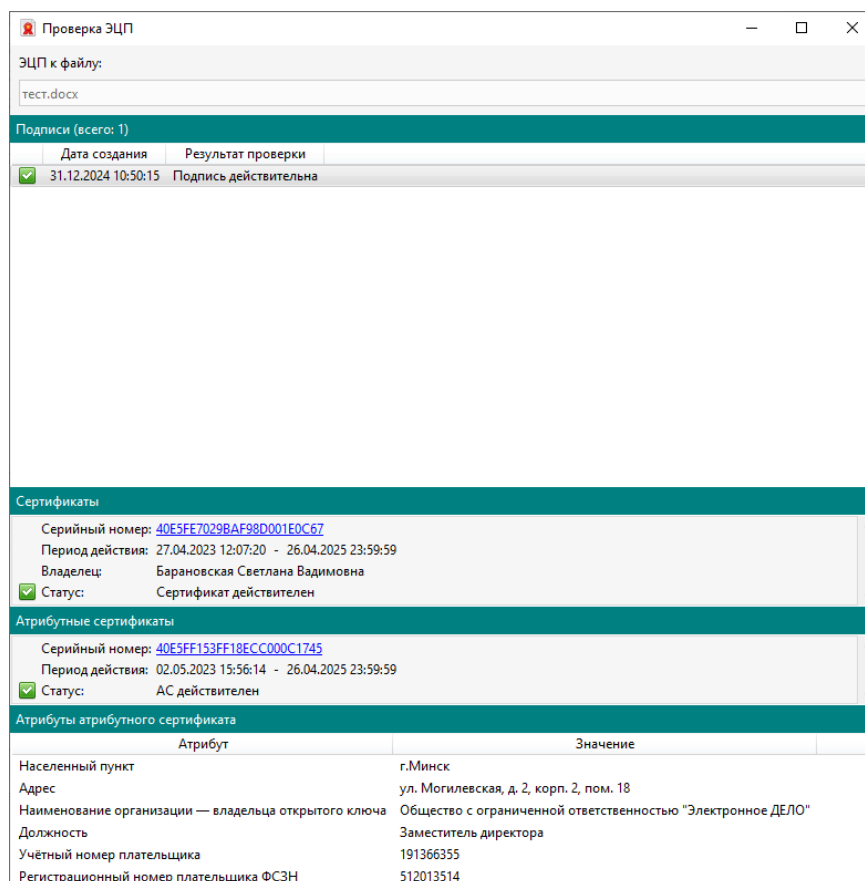


Рис. 5.29. Пример результатов проверки подписей и сертификатов

В поле «ЭЦП к файлу» окна «Проверка ЭЦП» отображается название проверяемого файла. В секции «Подписи» приведен список ЭЦП с датами создания и с результатами проверки. В заголовке секции «Подписи» указывается количество ЭЦП в списке. В секции «Сертификаты» содержатся данные сертификата, на базе которого была выработана ЭЦП, и указаны результаты проверки действительности сертификата. Если ЭЦП была выработана с использованием атрибутного сертификата, то в секции «Атрибутные сертификаты» отображаются сведения об атрибутном сертификате и результаты проверки действительности атрибутного сертификата, а в секции «Атрибуты атрибутного сертификата» отображается список атрибутов и их значений.

Для просмотра сведений о подписи дважды кликните левой клавишей мыши по выбранной записи в секции «Подписи». Откроется окно «Цифровая подпись» (рис. 5.30):

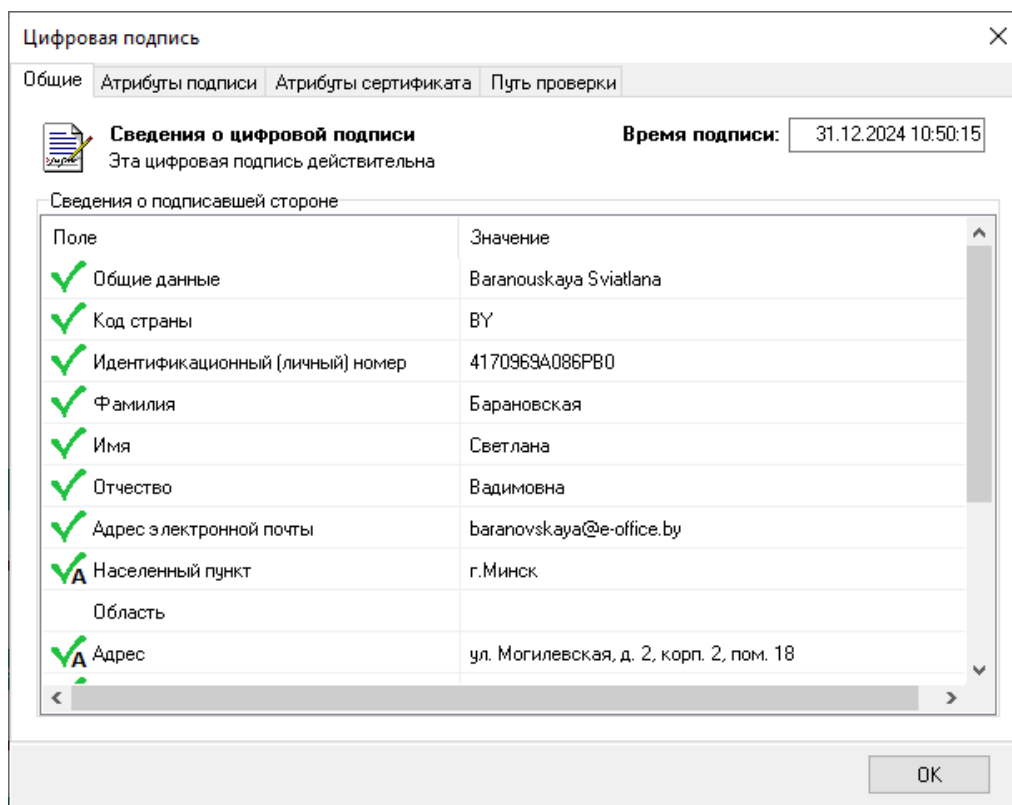


Рис. 5.30. Пример окна со сведениями о подписи

Закройте окно, нажав кнопку **ОК**.

Для просмотра сведений о сертификате кликните левой клавишей мыши по серийному номеру сертификата в секции «Сертификаты». Откроется окно Авеста «Сертификат» со сведениями о сертификате (пример на рис. 5.31).

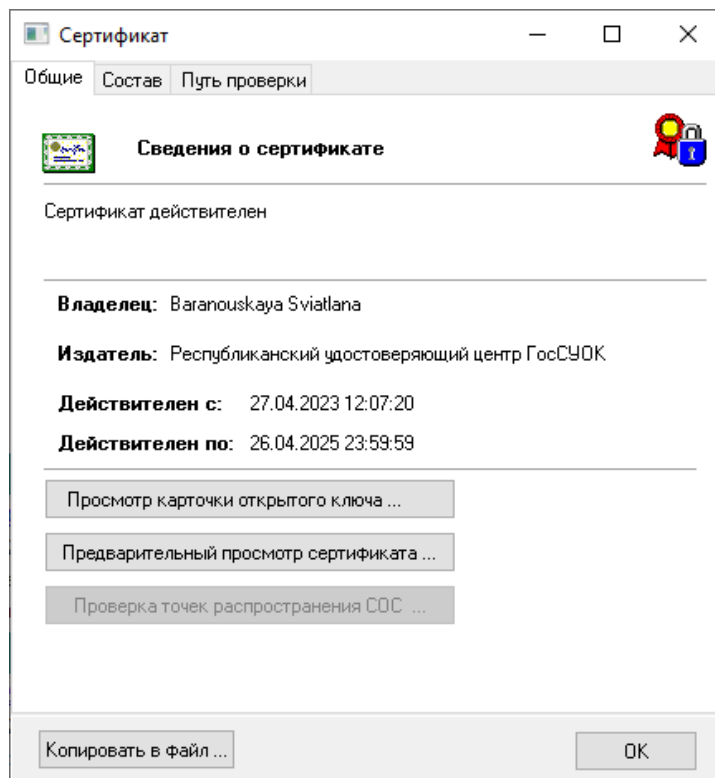


Рис. 5.31. Пример окна со сведениями о сертификате

Закройте окно, нажав кнопку **ОК**.

Для просмотра сведений об атрибутом сертификате кликните левой клавишей мыши по серийному номеру атрибутного сертификата в секции «Атрибутные сертификаты». Откроется окно Авеста «Атрибутный сертификат» со сведениями об атрибутом сертификате (пример на рис. 5.32).

Закройте окно, нажав кнопку **ОК**.

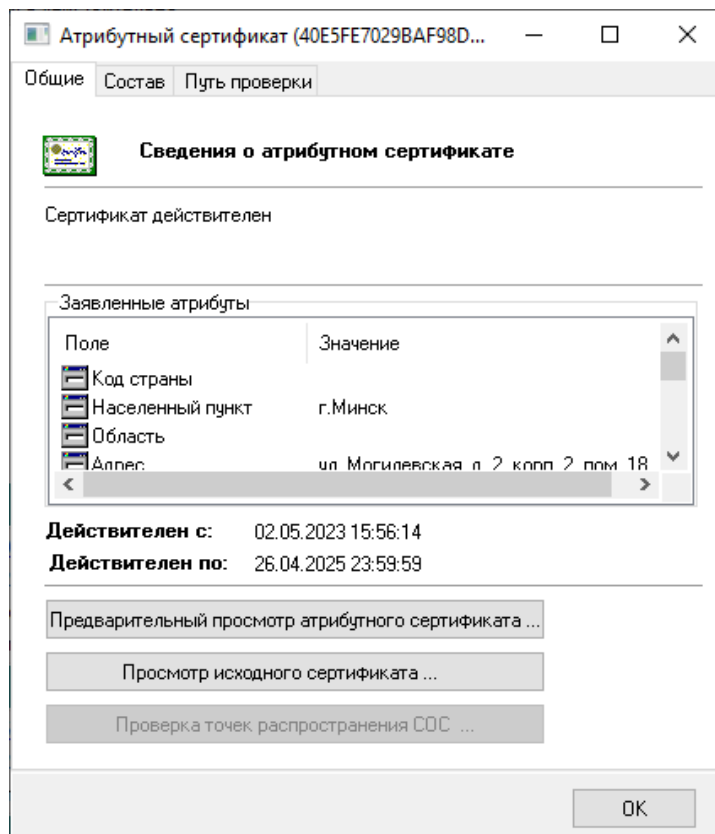


Рис. 5.32. Пример окна со сведениями об атрибутном сертификате

6. СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Руководство пользователя к опции «ИПО (Подпись)» интеграционного программного обеспечения системы автоматизации делопроизводства и электронного документооборота «Электронное ДЕЛО» «Электронное ДЕЛО – СМДО» версии 20 разработано ООО «Электронное ДЕЛО».

Адрес: 220007, Республика Беларусь, г. Минск, ул. Могилевская, дом 2, корпус 2, помещение 8.

Сайт: www.e-office.by

Электронная почта: ced@e-office.by

Консультативную помощь можно получить по тел.:

8(017)235-06-99 – сопровождение ИПО_СМДО;

8(017)396-68-89 – приобретение лицензии опции «ИПО (Подпись)»;

8(017)396-68-90 – отдел внедрения и сопровождения;

8(017)396-68-91 – отдел технической поддержки.

8(017)270-42-79 – отдел разработки ПО.

7. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АИС МВ	Автоматизированная информационная система «Межведомственное взаимодействие»
АС	Атрибутный сертификат – структура данных с электронной цифровой подписью центра атрибутных сертификатов, связывающая определенные значения атрибутов с идентификационной информацией о держателе
ГосСУОК	Государственная система управления открытыми ключами
ИПО_СМДО	Интеграционное программное обеспечение версии 20, разработанное для информационного обмена документами между АИС МВ и СЭД «Электронное ДЕЛО» по Формату взаимодействия версии 3.0
ИПО_СМДО с опцией «ИПО (Подпись)»	ИПО_СМДО с реализованным функционалом работы со средствами ЭЦП, включая возможность работы с атрибутными сертификатами и ID-картой
НКИ	Носитель ключевой информации
НЦЭУ	РУП «Национальный центр электронных услуг»
Модуль КП	Клиентская программа, предоставляемая НЦЭУ и используемая в целях выработки и проверки ЭЦП с применением средств ЭЦП, распространяемых в рамках ГосСУОК.
ПМС Авеста	Персональный менеджер сертификатов ЗАО «Авест»
РК	Регистрационная карточка документа в СЭД «Электронное Дело»
СМДО	Система межведомственного документооборота государственных органов Республики Беларусь
СОК	Сертификат открытого ключа
СОС	Список отозванных сертификатов, используется при проверке электронной цифровой подписи

СЭД	Система электронного документооборота «Электронное ДЕЛО»
ЭЦП	Электронно-цифровая подпись
AvPass	Вид НКИ, выполненный в виде USB-токена
AvBign	Вид НКИ, выполненный в виде USB-токена
ID-карта	Идентификационная карта – официальный документ, удостоверяющий личность, в том числе в электронных системах разных уровней и назначений, обычно выполненный в формате пластиковой карты.