КриптоАРМ 5
Руководство пользователя

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ПО РАБОТЕ С ПРОГРАММОЙ «КРИПТОАРМ» (версия 5)

ОГЛАВЛЕНИЕ

1 О РУКОВОДСТВЕ ПОЛЬЗОВАТЕЛЯ

Настоящий документ содержит описание эксплуатации "КриптоАРМ", универсального программного средства для шифрования и электронной подписи данных.

Руководство предназначено для широкого круга пользователей. В нем объясняются основные понятия в области криптографической защиты информации, подробно описывается работа с самой программой, от установки и настройки до конкретных задач. Функциональность программы позволяет решать задачи, связанные с созданием и проверкой электронной подписи, шифрованием и расшифрованием файлов, работой с криптопровайдерами и цифровыми сертификатами.

Материал располагается по принципу «Задача -> Решение». Описание сопровождается примерами и иллюстрациями.

2 БЫСТРЫЙ СТАРТ

В главе **Быстрый старт** вы найдете ответы на вопросы,

- что такое "КриптоАРМ"?
- что можно сделать с помощью этой программы?
- с чего начать?
- что требуется, чтобы приступить к шифрованию и электронной подписи?

Что такое "КриптоАРМ"?

“КриптоАРМ” — универсальная программа для шифрования и электронной подписи файлов. Программа используется для защиты информации, передаваемой по Интернету, электронной почте и на съемных носителях. Удобный графический интерфейс делает криптооперации простыми и быстрыми.

Подробнее о программе "КриптоАРМ" читайте в главе "Общие сведения о программе"

Что можно сделать с помощью "КриптоАРМ"?

С помощью программы "КриптоАРМ" вы сможете шифровать и подписывать файлы, управлять цифровыми сертификатами и криптопровайдерами, работать с ключевыми носителями и многое другое.

С чего начать?

Скачайте программу «КриптоАРМ». Чтобы по знакомится со всеми возможностями программы, вам не требуется временная лицензия. В течение 1 месяца со дня установки “КриптоАРМ” работает в режиме “Стандарт Плюс” с максимальным набором функциональных возможностей (для Некоммерческого использования). За это время вы сможете вдумчиво разобраться с программой и купить лицензию на ту версию, которая вам больше подходит.

Актуальную версию программы вы можете найти в разделе Центр загрузки официального сайта компании «Цифровые технологии» www.trusted.ru.

1. Ознакомьтесь с руководством пользователя. В нем даются подробные инструкции по выполнению любых задач по настройке программы и выполнению криптографических операций. Это можно делать во время работы в самой программе, пользуйтесь поиском по тексту руководства (Ctrl+F), это вам поможет быстро найти нужный раздел.
2. Просмотрите раздел "Часто задаваемые вопросы" в документе или на нашем сайте. Возможно, ваш вопрос ранее уже возникал и на него есть готовое решение или совет.
3. Если вы не найдете нужных ответов, задайте свой вопрос в техническую поддержку, для чего воспользуйтесь формой «Вопрос службе поддержки» на нашем сайте.

Что требуется, чтобы приступить к шифрованию и электронной подписи?

Для того чтобы приступить к работе с программой - зашифровать или подписать файл:

1. Получите **личный сертификат** в удостоверяющем центре (или создайте самоподписанный сертификат самостоятельно) и установите его в личное хранилище сертификатов.
2. Скачайте и установите корневой сертификат вашего удостоверяющего центра и актуальный список отзыва сертификатов.
3. Настройте программу "КриптоАРМ" под себя. Мы рекомендуем сразу создать шаблонные настройки, чтобы упростить для себя всю последующую работу.
4. Теперь вы можете подписывать и шифровать файлы.

3 НОВИНКИ ВЕРСИИ

"КриптоАРМ 5" Обновление 5.1

1. Режим "Квалифицированная подпись"

Для многих сегодня становится проблемой гарантировать, что получаемые электронные документы подписаны действительно квалифицированной электронной подписью. Для решения этой задачи мы ввели технологию, которая позволяет с точностью определять, является ли сертификат подписи квалифицированным или нет.

На портале Уполномоченного федерального органа в области электронной подписи Минкомсвязи размещается актуальный список аккредитованных удостоверяющих центров. Именно этот список используется новым «КриптоАРМ»ом в качестве фильтра при работе с электронной подписью.

Для работы только с квалифицированными сертификатами вам достаточно включить в программе режим «Квалифицированная подпись». Вам станут доступны только сертификаты, которые выданы аккредитованными удостоверяющими центрами и соответствуют требованиям к форме квалифицированного сертификата. То есть только квалифицированные сертификаты ключа проверки электронной подписи. Все остальные сертификаты скрываются. Проверка сертификатов, которыми подписаны электронные документы, выполняется также при включенном режиме.

2. Изменения коснулись самого вида программы

В новой версии мы отказались от упрощенного вида главного окна в пользу расширенного вида “Эксперт”. Теперь всю работу с программой “КриптоАРМ” вы сможете выполнять из единого окна.

3. Встроена временная лицензия для знакомства с программой без каких-либо ограничений

Чтобы упростить первые шаги по работе программы “КриптоАРМ”, мы изменили свою лицензионную политику. Теперь тем, кто впервые знакомится с возможностями программы, не требуется запрашивать у нашей компании временную лицензию. Лицензия автоматически устанавливается вместе с самой программой. В течение 1 месяца со дня установки “КриптоАРМ” работает в режиме “Стандарт Плюс” с максимальным набором функциональных возможностей.

4. “КриптоАРМ” 5.1 поддерживает новые национальные стандарты электронной подписи 2012

Определен порядок перехода на национальный стандарт ГОСТ Р 34.10-2012 в средствах электронной подписи для информации, не содержащей гостайну. Из документа ФСБ России № 149/7/1/3-58 от 31.01.2014 "О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования" мы узнаем, что для создания электронной подписи после 31 декабря 2018 года будет недопустимо использовать ГОСТ Р 34.10-2001.

В новом “КриптоАРМ”е мы поддержали стандарт электронной подписи ГОСТ Р 34.10-2012. И вместе с этим поддержали криптопровайдер “КриптоПро CSP” версий 3.9 и 4.0, проходящих сейчас сертификацию. Именно “КриптоПро CSP” 4.0 реализует новые алгоритмы ГОСТ Р 34.10-2012 по созданию и проверке электронной подписи.

5. Поддержка шифрования для JaCarta ГОСТ, eToken ГОСТ, Рутокен ЭЦП

В предыдущей версии “КриптоАРМ” 5.0 мы объявили о работе с аппаратными ключевыми носителями через интерфейс PKCS #11 с поддержкой российских криптоалгоритмов. Однако на тот момент мы реализовали взаимодействие только в области электронной подписи, формирования запросов на создание ключей ЭП, генерации и записи на носитель ключей проверки электронной подписи.

В работе над новой версией программы мы добились хороших результатов в шифровании данных с помощью отчуждаемых носителей JaCarta ГОСТ, eToken ГОСТ, Рутокен ЭЦП с “криптографией на борту”.

6. “КриптоАРМ” 5.1 с поддержкой Windows 8.1

В список поддерживаемых операционных систем добавилась еще одна. Новый “КриптоАРМ” работает с Microsoft Windows 8.1, вышедшей в октябре 2013 года.

4 Основные термины и понятия

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Для целей настоящего Федерального закона используются следующие основные понятия

1) **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) **сертификат ключа проверки электронной подписи** - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) **квалифицированный сертификат ключа проверки электронной подписи** (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

4) **владелец сертификата ключа проверки электронной подписи** - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) **ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) **ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) **удостоверяющий центр** - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) **аккредитация удостоверяющего центра** - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

9) **средства электронной подписи** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) **средства удостоверяющего центра** - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) **участники электронного взаимодействия** - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

12) **корпоративная информационная система** - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) **информационная система общего пользования** - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

5 Введение

5.1 Общие сведения о программе

Шифрование

- шифрование и расшифрование отдельных файлов, пакетов и архивов данных;
- перешифрование файла в адрес измененного списка получателей;
- размер шифруемых данных ограничен только файловой системой и доступным свободным местом;
- одновременное шифрование неограниченного количества файлов;
- удаление исходного файла после шифрования, в т.ч. гарантированное удаление;
- шифрование данных по стандарту PKCS#7,CMS;
- задание расширений выходных файлов (по умолчанию - *. enc).

Электронная подпись (ЭП)

- электронная подпись отдельных файлов, пакетов данных и архивов;
- варианты электронной подписи: первичная, дополнительная (подпись документа несколькими лицами) и заверяющая (иерархия электронных подписей с соблюдением чёткой последовательности подписи документов в организации);
- классический и усовершенствованный форматы ЭП;
- режим «Квалифицированная подпись» (технологию, которая позволяет с точностью определять, является ли сертификат подписи квалифицированным или нет)
- поддержка нового национального стандарта электронной подписи ГОСТ Р 34.10-2012
- применение расширенных свойств ЭП (время создания подписи, комментарий пользователя);
- электронная подпись, отделенная от подписываемых данных и совмещенная с данными);
- удаление файла после подписи, в т.ч. гарантированное удаление;
- размер подписываемых данных ограничен только файловой системой и доступным свободным местом;
- одновременная обработка неограниченного количества файлов;
- печать подписи на бумажный носитель.

Надежное хранение ключевой информации

- для хранения ключевой информации “КриптоАРМ” поддерживает работу с USB токенами и смарт-картами Rutoken S, Рутокен ЭЦП, eToken PRO (Java), eToken ГОСТ, Магистра CSP, КриптоПро Рутокен CSP, КриптоПро eToken CSP, УЭК
- поддержка интерфейса PKCS#11

Удостоверение точного времени подписи электронных документов

- ЭП со штампом времени;
- просмотр и проверка штампа времени на подписанном документе;
- просмотр и проверка штампа времени на ЭП.

Длительное (архивное) хранение электронных документов, подписанных усовершенствованной электронной подписи

- поддержка формата CAdES X Long (усовершенствованная электронная подпись);
- доказательство момента подписи документа и действительность сертификата ключа подписи на этот момент статусов при создании ЭП и проверке корректности ЭП;
- возможность доказательства корректности подписи и целостности файла даже после истечения срока действия сертификата подписи.

Автоматизация работы с программой

- индивидуальные настройки, которые могут ускорить выполнение однотипных операций;
- криптографические операции «одним кликом»;
- возможность удаленного администрирования рабочего места в PKI инфраструктуре.

Встраивание криптографии в информационные системы

"КриптоАРМ SDK" - библиотека криптографических функций (создана в соответствии со стандартами компонентной модели компании Microsoft). В комплект поставки входит документация для разработчиков, где описываются способы интеграции "КриптоАРМ" с внешними программами на уровне программного кода, приведены назначение, характеристики, функции программы, а также примеры использования основных операций.

- поддержка международных стандартов и рекомендаций в области защиты информации (X.509v1,v3, PKCS#7, PKCS#11, CMS, CAdES);
- соответствие требованиям законодательства Российской Федерации;
- предпроектный и проектный консалтинг со стороны специалистов в области защиты информации и электронной подписи;
- подробно документированные функции;
- постоянное развитие функциональных возможностей программного продукта;
- хорошо продуманный пользовательский интерфейс;
- техническая поддержка и сопровождение.

Создание рабочих мест в Инфраструктуре PKI

- поддержка работы с Microsoft Certificate Authority и ПАК «КриптоПро УЦ»;
- использование в качестве рабочего места для взаимодействия с Удостоверяющим центром
- просмотр информации и проверка текущего статуса цифрового сертификата, запроса;
- обновление списков отозванных сертификатов производится по всем удостоверяющим центрам (как корневому, так и промежуточным), входящим в Путь сертификации проверяемого сертификата;
- печать на бумажный носитель информации о сертификате, запросе;
- импорт и экспорт сертификатов, запросов, списков;
- работа со справочником назначений сертификатов;
- просмотр списка ключевых контейнеров.
- поддержка хранилища цифровых сертификатов для Active Directory

Управление криптопровайдерами (СКЗИ)

- поддержка российского сертифицированного криптопровайдера “КриптоПро CSP”
- поддержка стандартных криптопровайдеров, входящих в поставку ОС Windows
- поддержка криптопровайдеров, разработанных по технологии Microsoft CSP (”SignalCOM CSP”, “ViPNet CSP”, “AVEST CSP”, “Tumar CSP”);
- поддержка криптопровайдера КриптоПро УЭК CSP (СКЗИ “КриптоПро CSP” версии 3.6.1 вариант исполнения 8);
- просмотр списка установленных и разрешенных к использованию криптопровайдеров и их параметров;
- просмотр и фильтрация списка криптопровайдеров.

Модульная архитектура

- Модуль TSP предназначен для удостоверения точного времени создания электронных документов с помощью штампов времени
- Модуль OCSP предназначен для получения в реальном времени информации о статусе цифровых сертификатов
- Функциональность модуля “Клиент УЦ”, начиная с версии 4.7, включена в состав базового дистрибутива
- Для комплекта «КриптоАРМ СтандартPRO» модули TSP и OCSP включены в состав

5.2 Требования к аппаратуре и программному обеспечению

В этом разделе перечислены минимальные требования к аппаратной и программной части рабочего места, сервера, а также технические требования к сети, которые обеспечат стабильную работу программы «КриптоАРМ».

5.2.1 Поддерживаемые операционные системы

Программа «КриптоАРМ» работает в следующих операционных системах:

32-разрядные клиентские: Windows 8.1/8/7/Vista/XP
32-разрядные серверные: Windows Server 2008/2003
64-разрядные клиентские: Windows 8.1/8/7
64-разрядные серверные: Windows Server 2008 R2

5.2.2 Минимальные требования к аппаратной части

Технические требования к рабочему месту

Техническая характеристика	Минимальное значение
Процессор	Intel Celeron 1,8 ГГц
Оперативная память	256 Мбайт
Свободное место на жестком диске	35 Мбайт
Сетевой адаптер	100 Мбит

Технические требования к серверу

Техническая характеристика	Минимальное значение
Процессор	Intel Celeron 1,8 ГГц
Оперативная память	256 Мбайт

Свободное место на жестком диске	35 Мбайт
Сетевой адаптер	100 Мбит
Установленная операционная система (ОС)	2003 Server (32 бита)
Установленная СУБД	Microsoft Access, MySQL 5.0, Microsoft SQL
Microsoft Data Access Component	Требуется
Сервер	IIS 6.0

Технические требования к сети:

- все рабочие станции и сервер должны быть соединены локальной сетью производительностью не менее 100 Мбит/с;
- доступ к сети Интернет (для создания усовершенствованной подписи).

5.2.3 Минимальные требования к программной части

Для корректной установки и эксплуатации программы «КриптоАРМ» на рабочем месте необходимо наличие следующего программного обеспечения:

- сервис-паки XP SP2/ 2003 SP1 (в зависимости от установленной ОС);
- веб-браузер Microsoft Internet Explorer версии 6.0 и выше.

5.3 Требования к совместимости

5.3.1 Поддерживаемые криптопровайдеры

Предустановленные криптопровайдеры ОС MS Windows:

- Microsoft Base Cryptographic Provider v1.0
- Microsoft Base DSS Cryptographic Provider
- Microsoft Enhanced Cryptographic Provider v1.0
- Microsoft Strong Cryptographic Provider

Криптопровайдеры **КриптоПро CSP** (версии 2.0, 3.0, 3.6, 3.9, 4.0).
Разработчик- компания «КРИПТО-ПРО», Россия, www.cryptopro.ru

- Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
- Crypto-Pro GOST R 34.10-2001 KC1 CSP
- Crypto-Pro GOST R 34.10-2001 KC2 CSP
- Crypto-Pro Cryptographic Service Provider
- Crypto-ProSmartCard CSP (совместимость не протестирована)
- Crypto-ProHSM CSP (совместимость не протестирована)
- Crypto-ProHSMRSA CSP (совместимость не протестирована)
- CryptoProGOST R 34.10-2001 UEC CSP («КриптоПро CSP» для универсальной электронной карты)
- Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider
- Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider

Криптопровайдеры **Signal-COM CSP**

Разработчик - компания «Сигнал-КОМ», Россия, www.signal-com.ru

- Signal-COM CPGOST Cryptographic Provider
- Signal-COM Cryptographic Provider
- Signal-COM ECGOST Cryptographic Provider
- Signal-COM Enhanced Cryptographic Provider
- Signal-COM Special Cryptographic Provider

- **КриптоПро Рутокен CSP**, совместная разработка компаний «КРИПТО-ПРО» и «Актив», основанная на интеграции криптопровайдера «КриптоПро CSP» и USB-токена «Рутокен ЭЦП», Россия, http://www.rutoken.ru;

- **КриптоПро eToken CSP**, совместная разработка компаний «КРИПТО-ПРО» и Аладдин», основанная на интеграции криптопровайдера «КриптоПро CSP» и USB-токена eToken, Россия http://www.aladdin-rd.ru;

- **"Домен-К"** (ViPNet CryptoService), разработчик - компания «Инфотекс», Россия, http://www.infotecs.ru;

- **LISSI-CSP**, разработчик – компания «ЛИССИ-Софт», Россия, http://soft.lissi.ru (совместимость не протестирована);

- **Magistra CSP**, разработчик – компания «ПрограмПарк», Россия, http://www.cryptopro.ru/products/fkc/magistra (совместимость не протестирована);

- **AVEST CSP**, разработчик - компания "Авест", Республика Беларусь, http://www.avest.by;

- **Tumar CSP,** разработчик - компания "Гамма Технологии", Республика Казахстан, http://www.gamma.kz/;

5.3.2 Поддерживаемые отчуждаемые ключевые носители

Для надежного хранения ключевой информации в программе «КриптоАРМ» выполнена совместимость с рядом наиболее популярных моделей отчуждаемых носителей (токенов) российских компаний:

Модели JaCarta (компания «Aladdin», http://www.aladdin-rd.ru)

- смарт-карты JaCarta PKI, JaCarta ГОСТ,
- USB-токены JaCarta PKI, JaCarta PKI/Flash, JaCarta ГОСТ, JaCarta ГОСТ/Flash, JaCarta LT.

Модели eToken (компания «Aladdin», http://www.aladdin-rd.ru)

- смарт-карты eToken PRO (32K/64K), eToken PRO 72K (Java), eToken ГОСТ,
- USB-токены eToken PRO 72K (Java), eToken ГОСТ, eToken NG-FLASH (Java).

Модели Рутокен (компания «Актив», http://www.rutoken.ru)

- Рутокен S 32Кб, 64Кб и 128Кб
- Рутокен S ндв3 ФСТЭК 32Кб, 64Кб и 128Кб
- Рутокен ЭЦП, Рутокен ЭЦП серт. ФСБ, Рутокен ЭЦП micro, Рутокен ЭЦП micro серт ФСБ 64К

Универсальная электронная карта (компания ОАО «УЭК», сайт производителя)

5.3.3 Обработка сертификатов различных Удостоверяющих Центров

Пользователи приложения имеют возможность работать с сертификатами, выпущенными как российскими, так и зарубежными удостоверяющими центрами (УЦ):

- Обработка сертификатов УЦ из списка доверенных удостоверяющих центров ОГИЦ (поддерживающие алгоритм ГОСТ Р 34.11/34.10-2001), сайт Минкомсвязи РФ
- Обработка сертификатов УЦ, выпущенных с использованием сертифицированных средств издания сертификатов (КриптоПро УЦ, УЦ Московской области, ЗАО «Удостоверяющий Центр» Санкт-Петербурга, Национальный УЦ и др.)
- Обработка сертификатов, выпущенных с использованием несертифицированных (зарубежных) средств издания сертификатов (VerySign, Thawte).

5.4 Версии программы и система лицензирования

Версия «КриптоАРМ Старт»

Бесплатная версия программы. Разрешает подписывать и шифровать файлы с применением криптопровайдеров Microsoft. С помощью версии «Старт» вы можете проверять корректность электронной подписи при работе с криптопровайдером «КриптоПро CSP».

Версия «КриптоАРМ Стандарт»

Полнофункциональная версия программы. Предназначена для подписи и шифрования электронных данных. Поддерживает российские ГОСТ алгоритмы подписи и шифрования.

Версия «КриптоАРМ Стандарт Плюс»

Расширенная версия программы для шифрования и подписи данных. В отличие от стандартной версии, «КриптоАРМ Стандарт Плюс» поддерживает работу с токенами и смарт-картами с криптографией “на борту” и неизвлекаемыми ключами.

==========

Чтобы упростить первые шаги по изучению программы “КриптоАРМ”, мы изменили свою лицензионную политику. Теперь тем, кто впервые знакомится с воз-

можностями программы, не требуется запрашивать временную лицензию. В течение 30 дней с момента установки "КриптоАРМ" работает в режиме "Стандарт Плюс" с максимальным набором функциональных возможностей.

Ознакомительная версия НЕ для коммерческого использования.

По истечении 30 дней программа автоматически переключается на версию "Старт", которая имеет ряд ограничений по сравнению с полнофункциональной версией.

Для перехода на другую версию достаточно просто приобрести и установить специальную лицензию (переустанавливать программу не требуется).

5.5 Комплекты, в состав которых включен «КриптоАРМ»

КриптоАРМ Стандарт PRO	Комплект, состоящий из лицензий на «КриптоАРМ Стандарт», «КриптоПро TSP Client», «КриптоПро OCSP Client». Предназначен для создания и проверки усовершенствованного формата электронной подписи.
КриптоАРМ УЭК	Комплект, состоящий из лицензии на «КриптоАРМ Стандарт», единого дистрибутива на «КриптоАРМ» и «КриптоПро УЭК CSP», считывателя карт УЭК. Позволяет подписывать с помощью универсальной электронной карты (при наличии личного сертификата) абсолютно любые файлы.
КриптоТри	Комплект, состоящий из лицензии на «КриптоАРМ Стандарт», «КриптоПро CSP» 3.6 и ключевого носителя «Рутокен».
eToken КриптоАРМ	Комплект, состоящий из лицензии на «КриптоАРМ Стандарт», «КриптоПро CSP» 3.6 и ключевого носителя eToken PRO.
СКЗИ КриптоАРМ 4	4 версия «КриптоАРМ»а, имеет сертификаты соответствия ФСБ РФ.

6 Подготовка к работе с программой

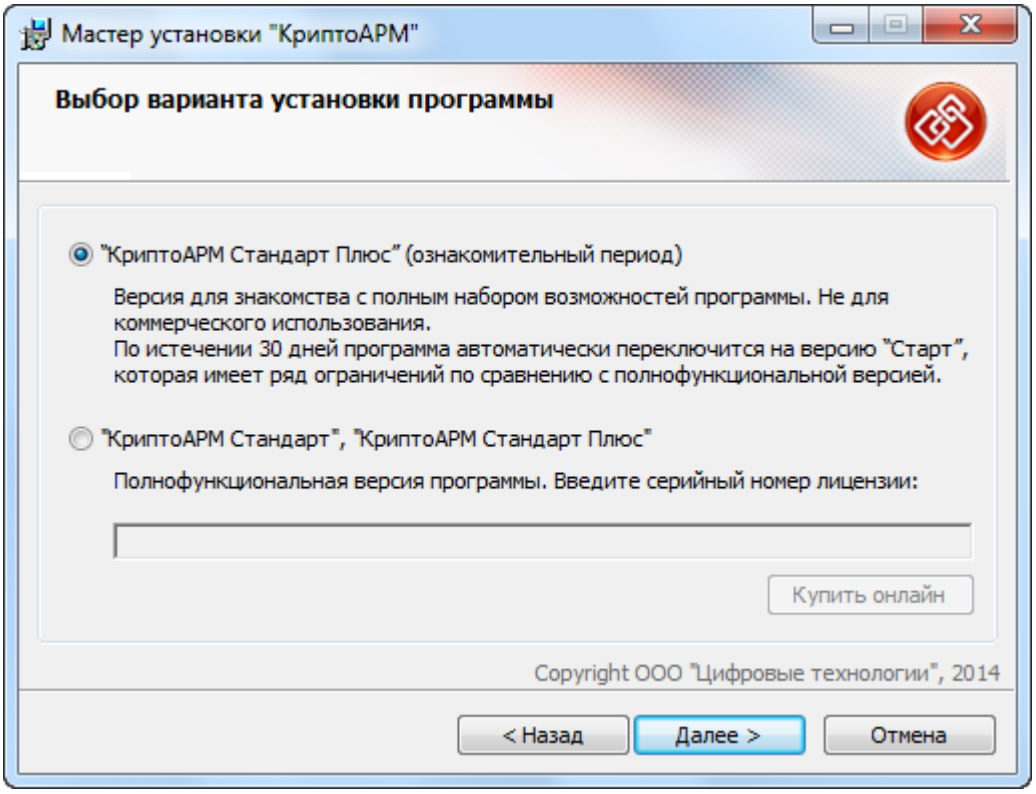
6.1 Установка программы

Установка программы «КриптоАРМ» в операционных системах Windows 2000/XP/2003 должна осуществляться пользователем, имеющим права Администратора системы.

Установка «КриптоАРМ» версии 4.5 и выше предполагает автоматическое обновление версии, ранее установленной на компьютере.

1. Для установки программы «КриптоАРМ» запустите на исполнение файл **Trusted-Desktop x.x.exe** (где x.x. – номер версии). Откроется мастер установки «КриптоАРМ». Нажмите **Далее** для продолжения установки или **Отмена** для выхода из мастера установки.
2. На следующем шаге выберите вариант установки:

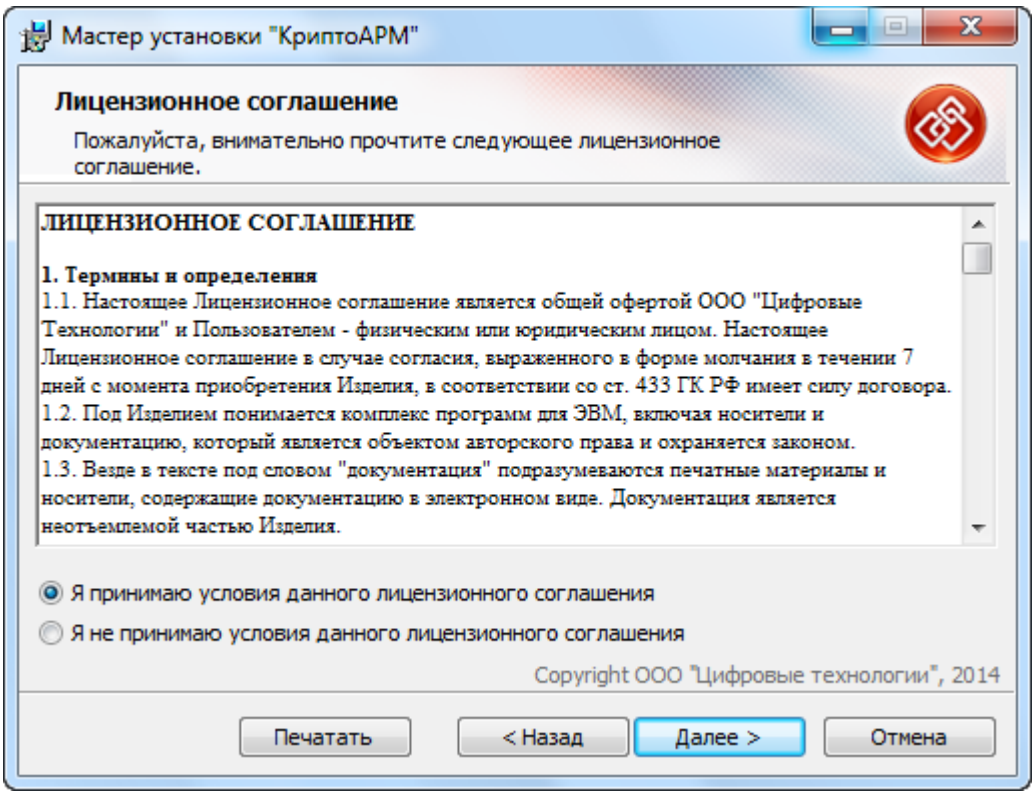
- «КриптоАРМ Стандарт Плюс» (ознакомительный период)
- Полнофункциональные версии «КриптоАРМ Стандарт», «КриптоАРМ Стандарт Плюс»



Об отличиях в версиях программы читайте в главе *Версии программы и система лицензирования.*

При выборе варианта «КриптоАРМ Стандарт», «КриптоАРМ Стандарт Плюс» в строке введите номер лицензионного ключа и нажмите **Далее.**

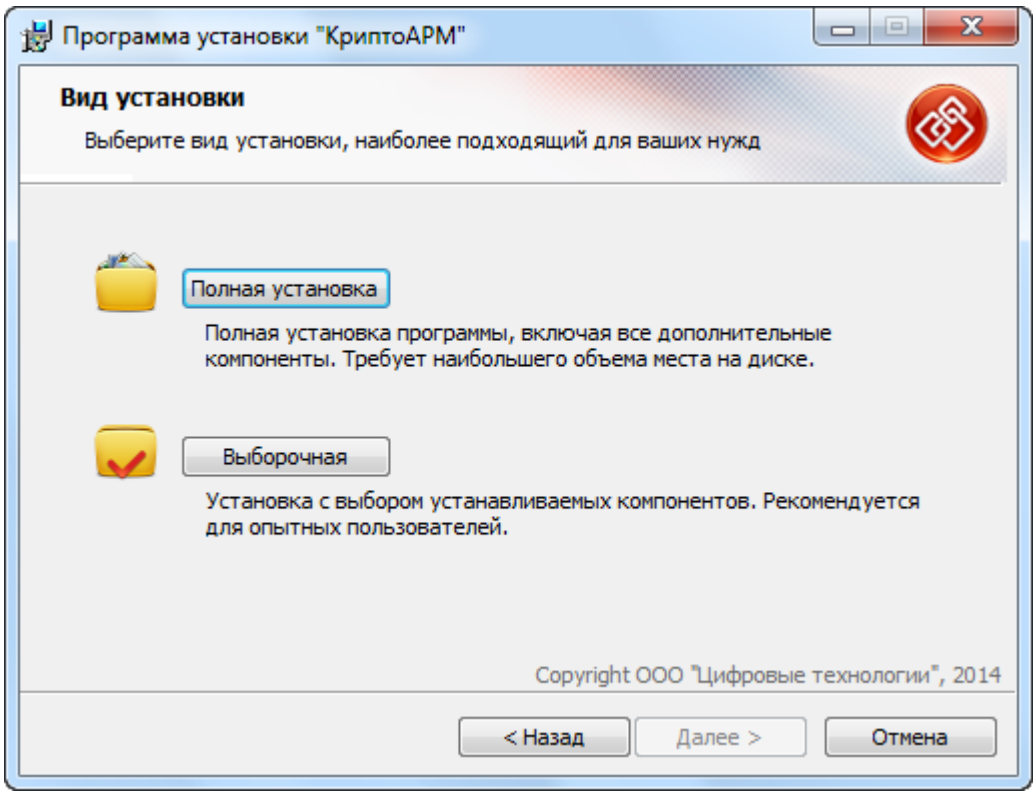
3. Ознакомьтесь с условиями лицензионного соглашения, в случае согласия отметьте соответствующий пункт и нажмите **Далее**.



4. Выберите вид установки программы.
   - Полная установка

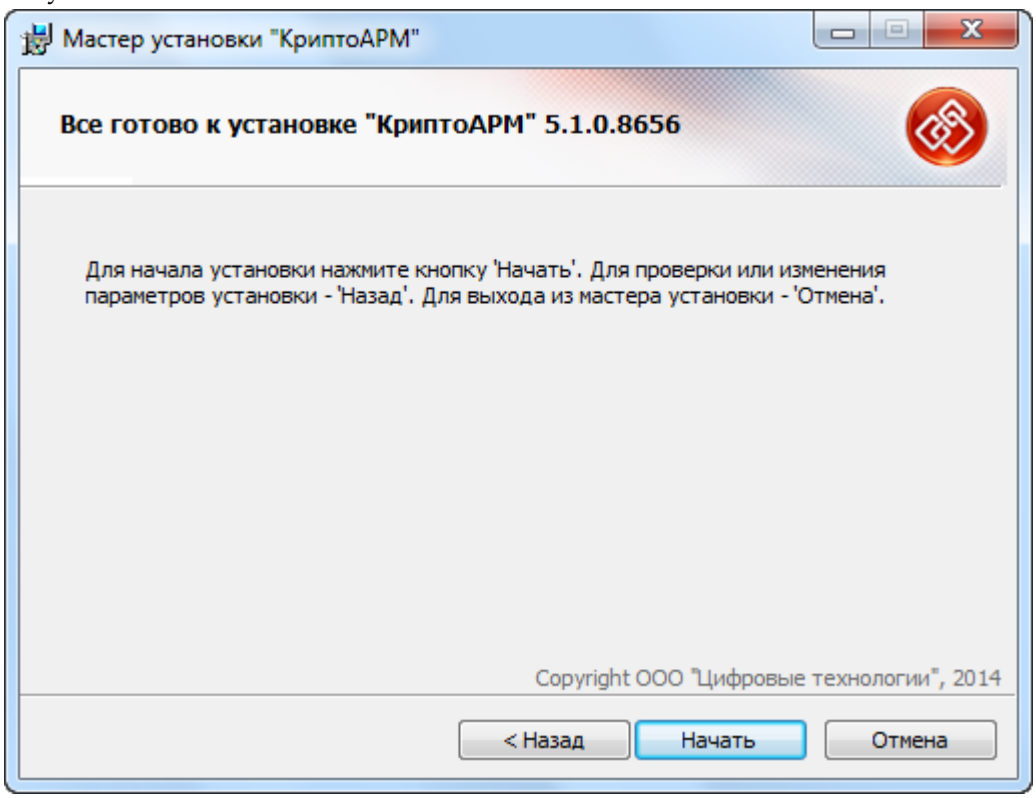
   Полная установка программы, включая все дополнительные компоненты. Требует наибольшего объема места на диске.
   - Выборочная установка

   Установка с выбором дополнительных компонентов (модулей к программе). Рекомендуется для опытных пользователей.



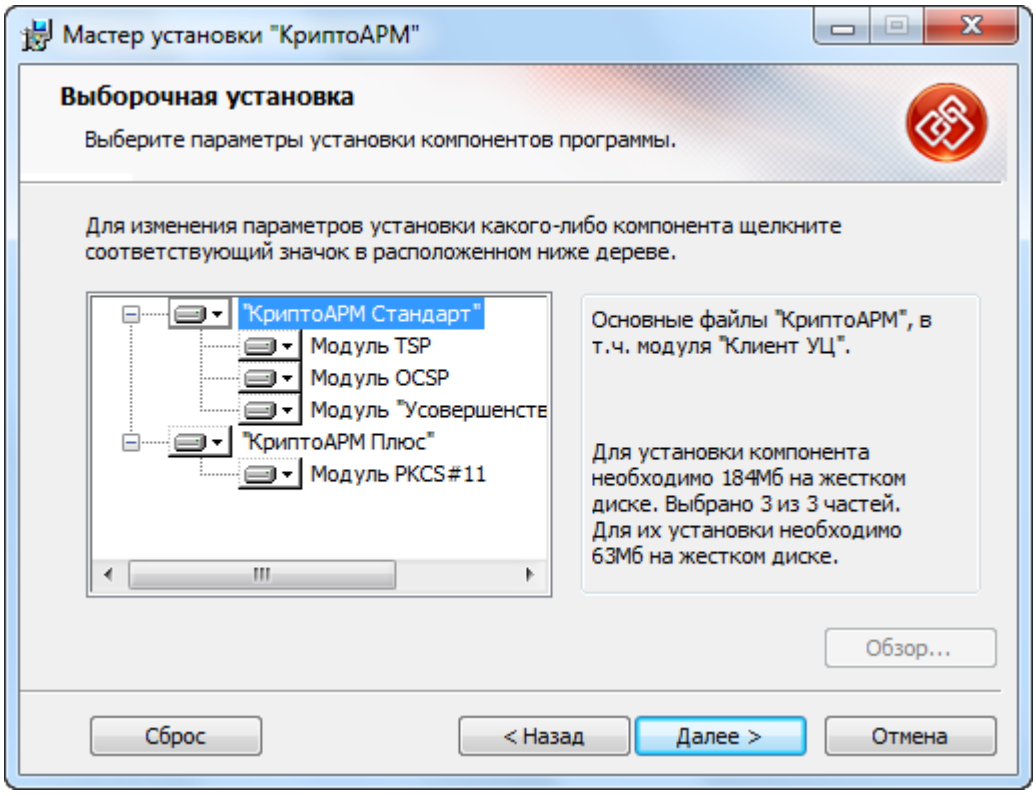
5. Следующий шаг зависит от того, какой вид установки вы выбрали.

При выборе **полной установки** вам просто нужно нажать на кнопку **Начать**, чтобы запустить процесс установки.



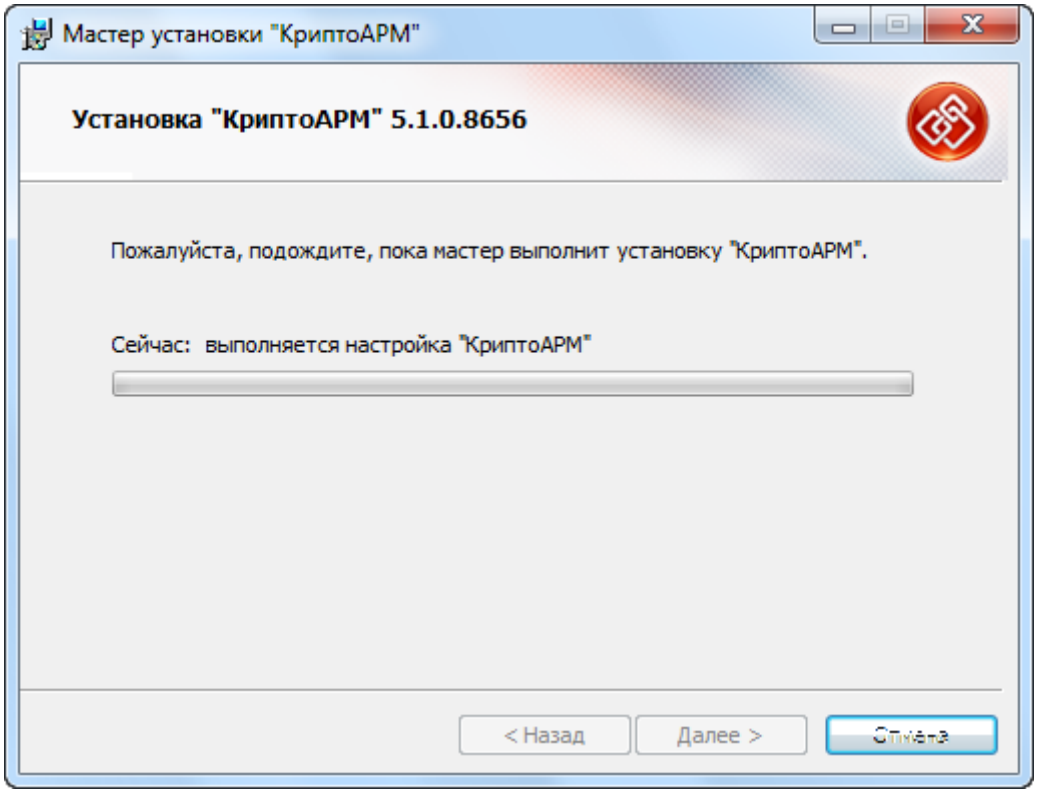
При **выборочной установке** вы можете указать:
- какие из модулей нужно установить

- директорию на вашем компьютере, куда приложение будет установлено.

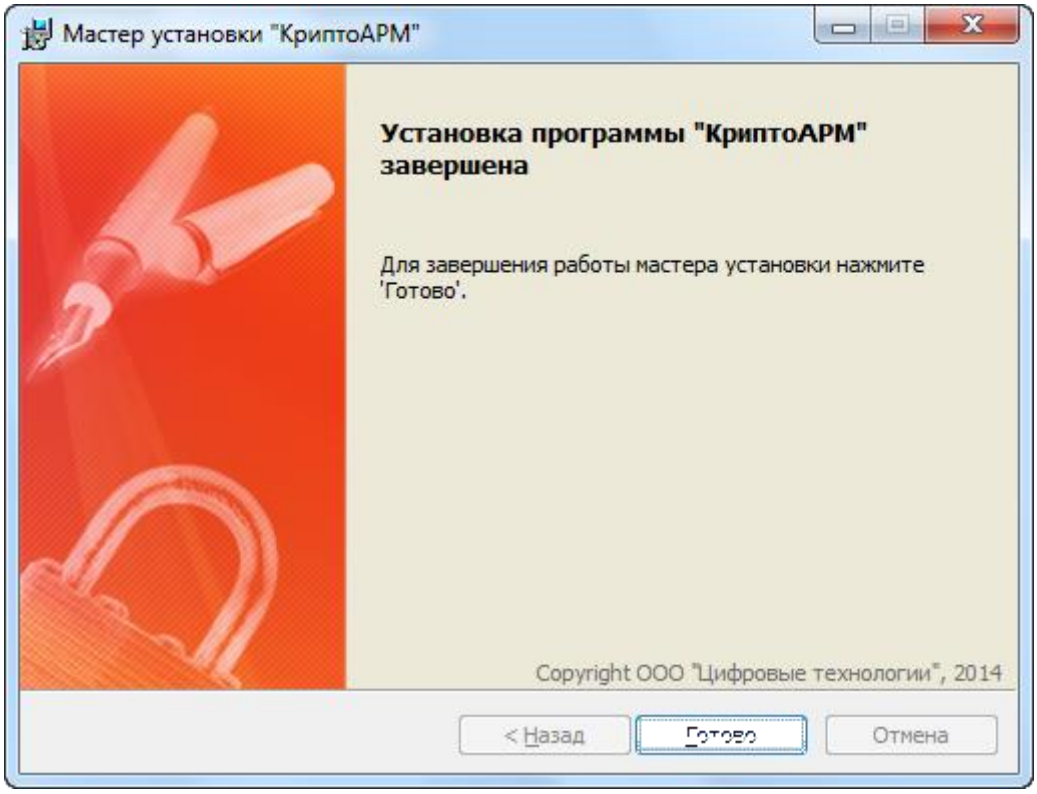


При установке версии «КриптоАРМ Стандарт Плюс» (ознакомительная версия) работа с дополнительными модулями будет доступна только в течение 30 дней с момента установки программы на компьютер. Чтобы дальше пользоваться возможностями модулей, вам необходимо будет приобрести и установить постоянную лицензию «Стандарт» или «Стандарт Плюс».

2. Начнется установка программы на компьютер.



3. По окончании установки нажмите кнопку **Готово**. Для завершения установки программы «КриптоАРМ» перезагрузите компьютер.



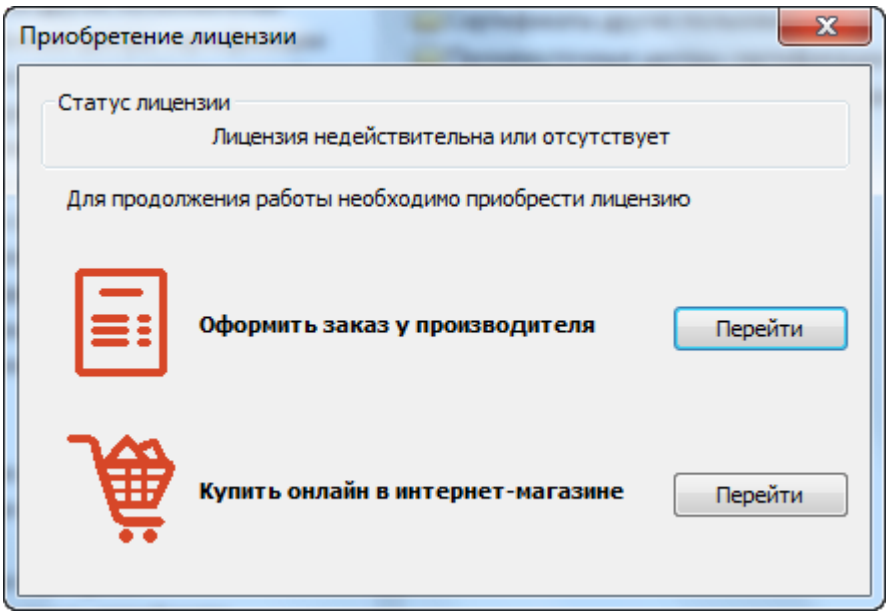
После установки программы

- в меню **Пуск > Программы** появится группа «**КриптоАРМ»**, которая содержит меню вызова главного окна программы «КриптоАРМ» и документации пользователя и программиста в формате PDF.

- в указанном при установке каталоге (по умолчанию в каталоге **Program Files**) будут созданы подкаталоги **Digt\Trusted\Desktop**.

Программа «КриптоАРМ» распространяется с уже введенным ключом временной лицензии, которая начинает действовать с момента установки и запуска программы. Временная лицензия выдается сроком на 1 месяц, после истечения которого пользователь должен приобрести постоянную лицензию. Об истечении срока действия временной лицензии приложение должно сигнализировать пользователю. Это реализуется на основе отображения уведомлений. За 10 дней до окончания срока действия временной лицензии программа будет предупреждать о необходимости приобрести постоянную лицензию.

Если пользователь не ввел постоянную лицензию в течение 30 дней с момента установки, по истечении ознакомительного периода программа автоматически переключается на версию "Старт", которая имеет ряд ограничений по сравнению с полнофункциональной версией.



6.2 Ввод информации о лицензии

Версия **«КриптоАРМ Старт»** не требует регистрации и время ее использования не ограничено. Версии **«КриптоАРМ Стандарт»** и «**КриптоАРМ Стандарт Плюс»** требуют ввода лицензионного ключа.
О том, как приобрести лицензию к программе «КриптоАРМ», читайте в главе Купить программу.

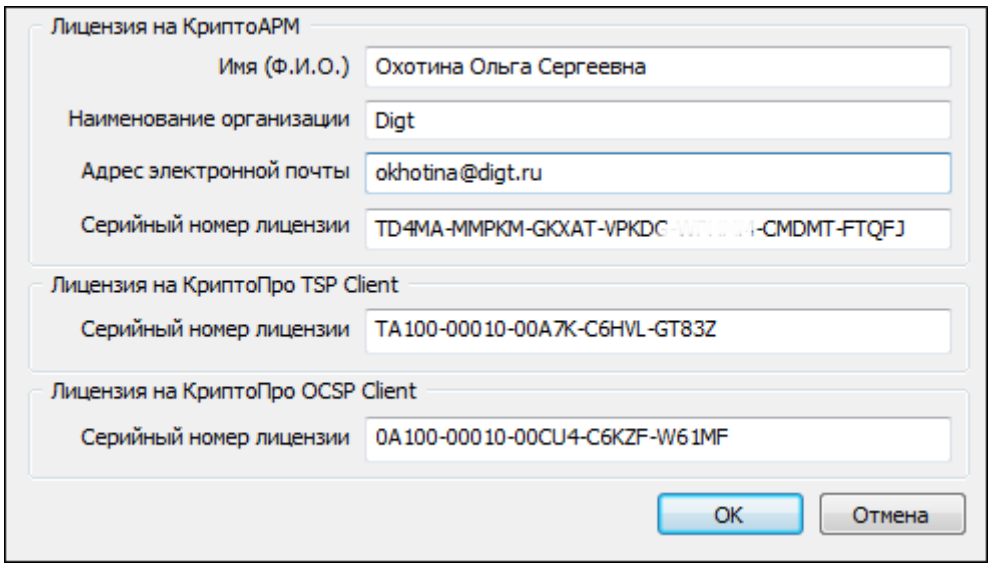
Регистрация продукта должна осуществляться пользователем, имеющим права администратора системы.

Зарегистрировать программу «КриптоАРМ» вы можете:

- через главное окно (**Помощь > О программе**)
- через значок на панели задач (**Установка лицензии**)

Чтобы зарегистрировать программу, выполните следующие шаги:

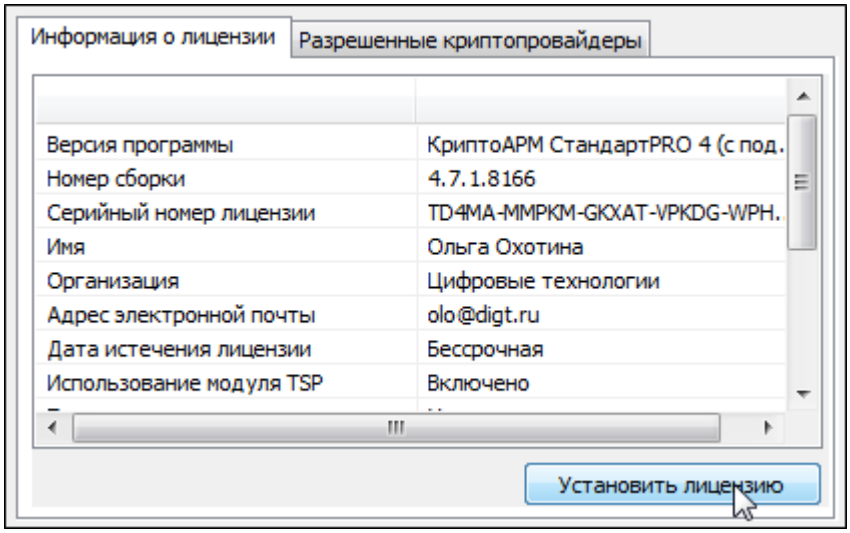
1. В окне **О программе** нажмите на кнопку **Установить лицензию**.
2. Доступ к функциональности программы «КриптоАРМ» и его модулям регулируется лицензиями. Введите информацию согласно выданной вам лицензии:



При успешной регистрации программы «КриптоАРМ» возникнет сообщение об этом.

В закладке **Информация о лицензии** отображается информация в соответствии с используемой лицензией на программу «КриптоАРМ»:

- версия продукта
- номер сборки дистрибутива программы
- серийный номер лицензии
- имя пользователя программы
- организация, которую представляет пользователь
- адрес электронной почты пользователя
- использование дополнительных модулей
- другие



При работе с Модулем TSP проверяется статус лицензии на программное обеспечение «КриптоПро TSP Client».

При работе с Модулем OCSP проверяется статус лицензии на программное обеспечение «КриптоПро OCSP Client».

При использовании лицензии к комплекту «КриптоАРМ СтандартPRO» автоматически включаются лицензии на модули TSP и OCSP.

Администратор имеет возможность выбора сертификатов (подписи, шифрования) не только с привязкой к закрытому ключу, но и из хранилища других пользователей.

6.3 Удаление программы

Удалить программу «КриптоАРМ» можно следующими способами:

- с помощью программы установки и удаления «КриптоАРМ»;
- стандартными средствами операционной системы Windows.

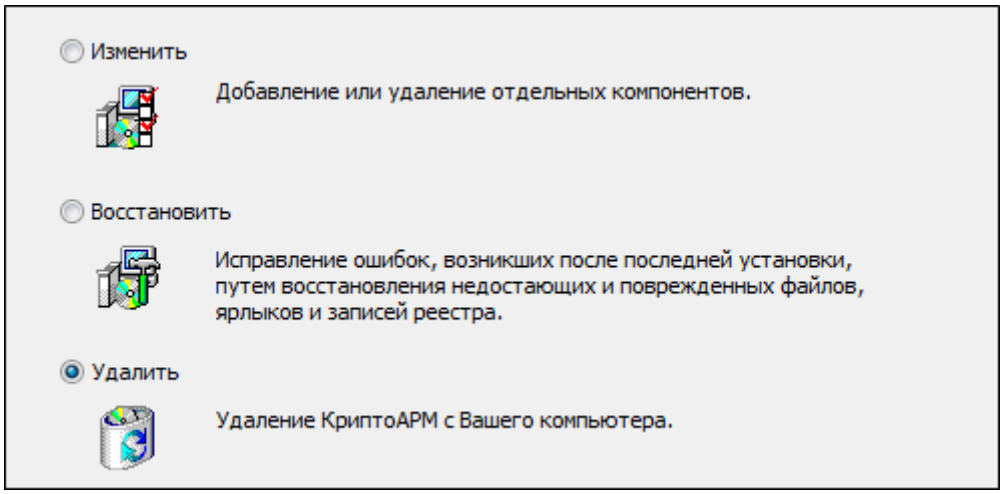
Для удаления «КриптоАРМ» стандартными средствами Windows:

1. Нажмите на кнопку **Пуск**, в главном меню Windows активизируйте команду **Настройка > Панель управления**.
2. Откроется окно **Панель управления**: активизируйте ярлык **Установка и удаление программ**.
3. Откроется одноименное окно, в котором перечислены программы, установленные на компьютере.
4. Выберите в списке программу «КриптоАРМ»: нажмите на кнопку **Удалить** и подтвердите решение об удалении.
5. Ход процесса удаления будет отображаться в виде индикатора прогресса в специальном окне. По завершении процесса программа «КриптоАРМ» будет удалена с компьютера и из списка элементов **Установленные программы**.

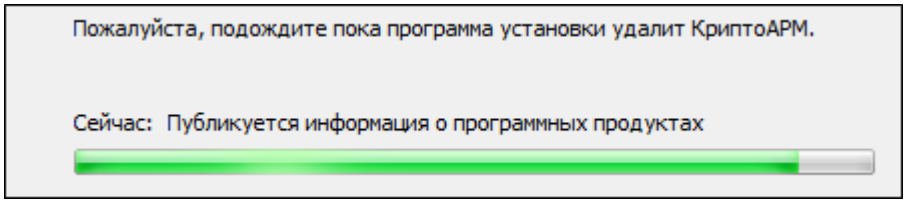
Для удаления «КриптоАРМ» с помощью программы установки:

1. Запустите на исполнение файл **TrustedDesktop x.x.exe** из дистрибутива программы. Откроется мастер установки «КриптоАРМ». Нажмите кнопку **Далее**.

2. Откроется окно, в котором выберите операцию **Удалить:**



3. Возникнет сообщение с предложением выполнить процедуру удаления: нажмите на кнопку **Удалить.**
4. Начнется удаление программы «КриптоАРМ». Ход процесса отображается в виде индикатора прогресса.



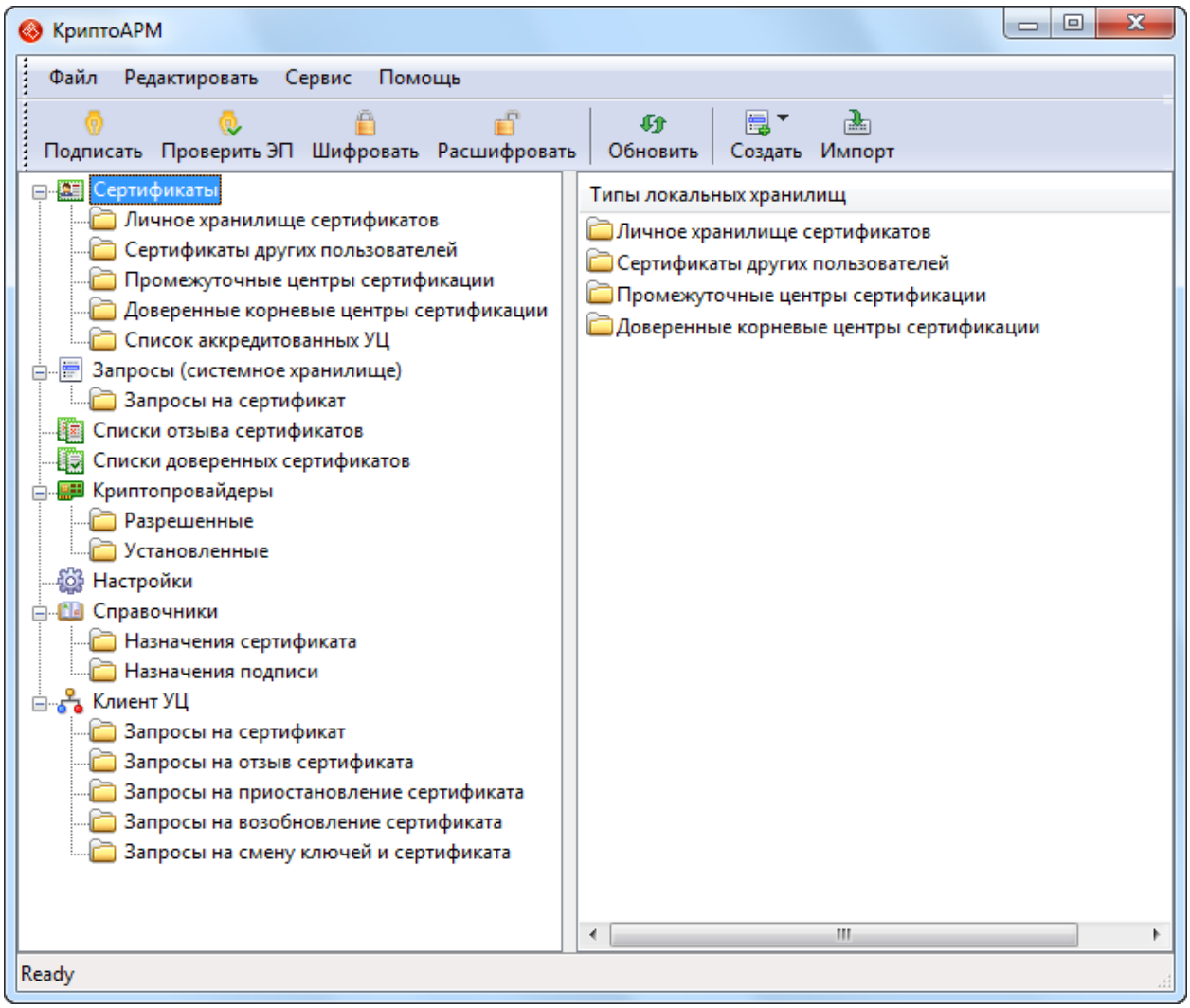
5. После завершения этого процесса возникнет сообщение с информацией о том, что программа удалена. Нажмите на кнопку **Готово**.

Для завершения процедуры удаления необходимо выполнить перезагрузку компьютера.

6.4 Варианты работы с программой

Вы можете работать с программой «КриптоАРМ», выбрав наиболее удобный для вас вариант:

- Главное окно программы, предназначено для выполнения криптоопераций, а также управления криптопровайдерами, сертификатами и настройками программы
- Значок на панели задач, который имеет контекстное меню с полным перечнем операций.
- Проводник Windows (контекстное меню файла)



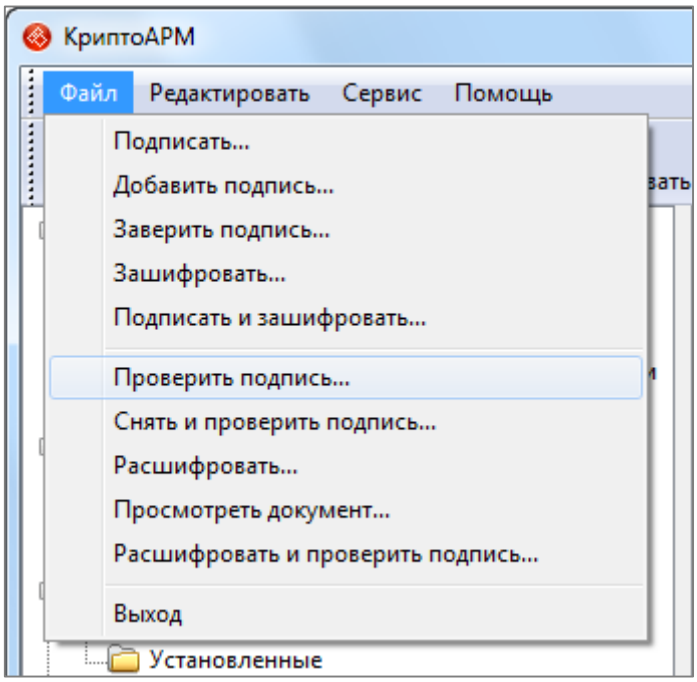
6.4.1 ГЛАВНОЕ ОКНО ПРОГРАММЫ

В левой части главного окна программы расположено дерево объектов, которое включает в себя основные разделы.

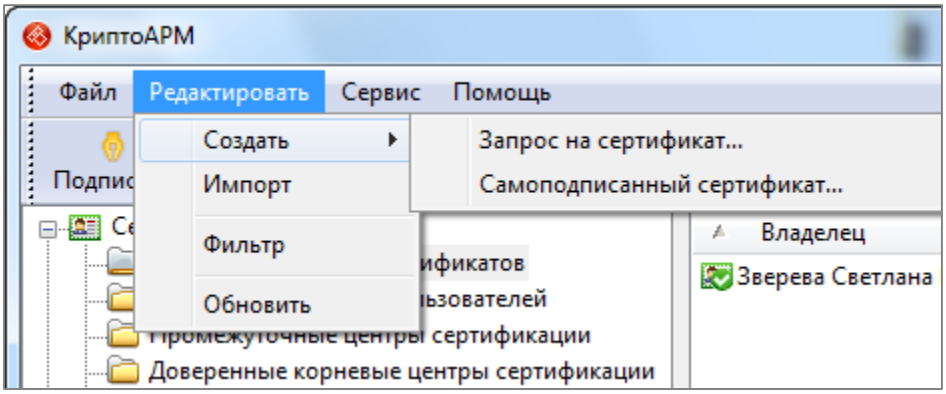
В правой части главного окна отображаются объекты, входящие в разделы дерева из левой части

Верхнее меню главного окна

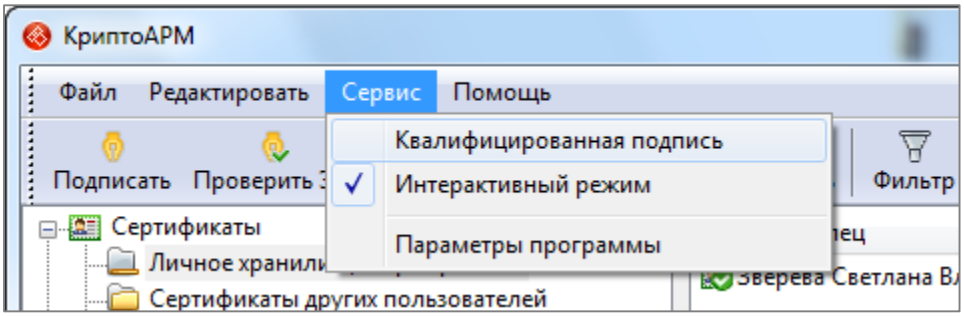
«Файл». Здесь вы можете выбирать нужную вам функцию и выходить из программы.



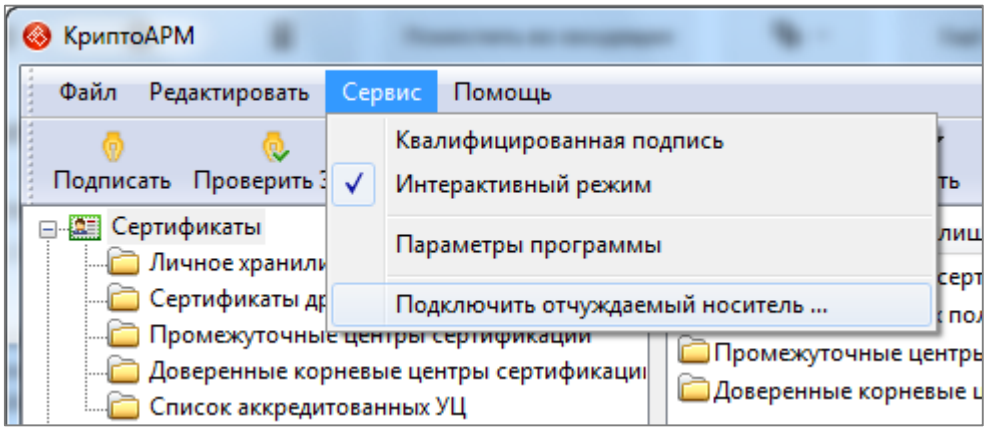
«Редактировать». В разделе доступны операции с выбранными в главном окне объектами (импорт, фильтр и др.)



«Сервис». Меню для установки режимов «Квалифицированная подпись», «Интерактивный режим» и настройки параметров программы.

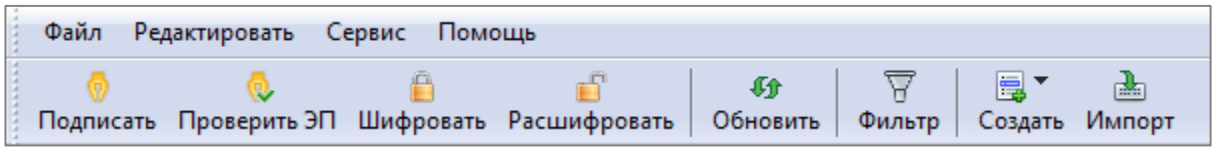


Если вы работаете с версиями «Стандарт» и «Стандарт Плюс», именно через это меню вы будете [подключать отчуждаемый ключевой носитель.]



«**Помощь**». Меню, через которое вы можете открыть руководство пользователя или руководство программиста, просмотреть общую информацию о программе «КриптоАРМ» и установить лицензию (через раздел «О программе»).

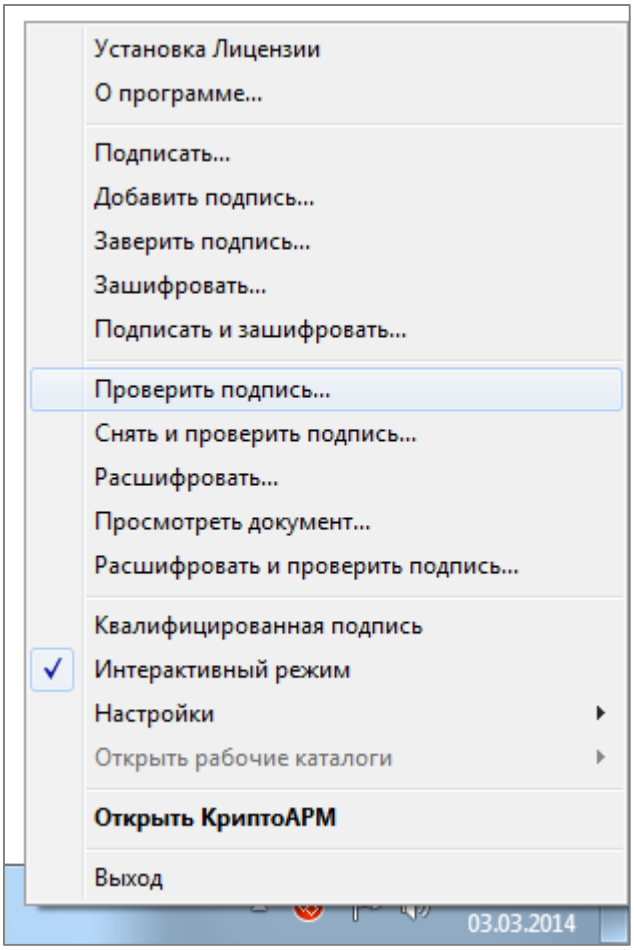
Для удобства основные операции с объектами вынесены в отдельную панель главного окна:



6.4.2 «КриптоАРМ» на панели задач

Вы можете работать с программой «КриптоАРМ» через уведомление на панели задач.

В общих настройках программы вы можете указать, чтобы «КриптоАРМ» присутствовал на панели задач в правом нижнем углу экрана компьютера для быстрого выполнения криптографических операций.



При двойном щелчке на значке «КриптоАРМ» открывается Главное окно программы.

Используя значок уведомления на панели задач, вы можете:

- установить лицензию к программе «КриптоАРМ»
- просмотреть информацию о программе «КриптоАРМ»
- подписывать файлы и проверять корректность подписи
- шифровать и расшифровывать файлы
- устанавливать пошаговый режим выполнения криптоопераций и режим «Квалифицированная подпись»
- выбирать настройки для выполнения криптоопераций
- работать через «КриптоАРМ» с рабочими каталогами (папки **Входящие/Исходящие**)
- переходить к работе с программой в главном окне

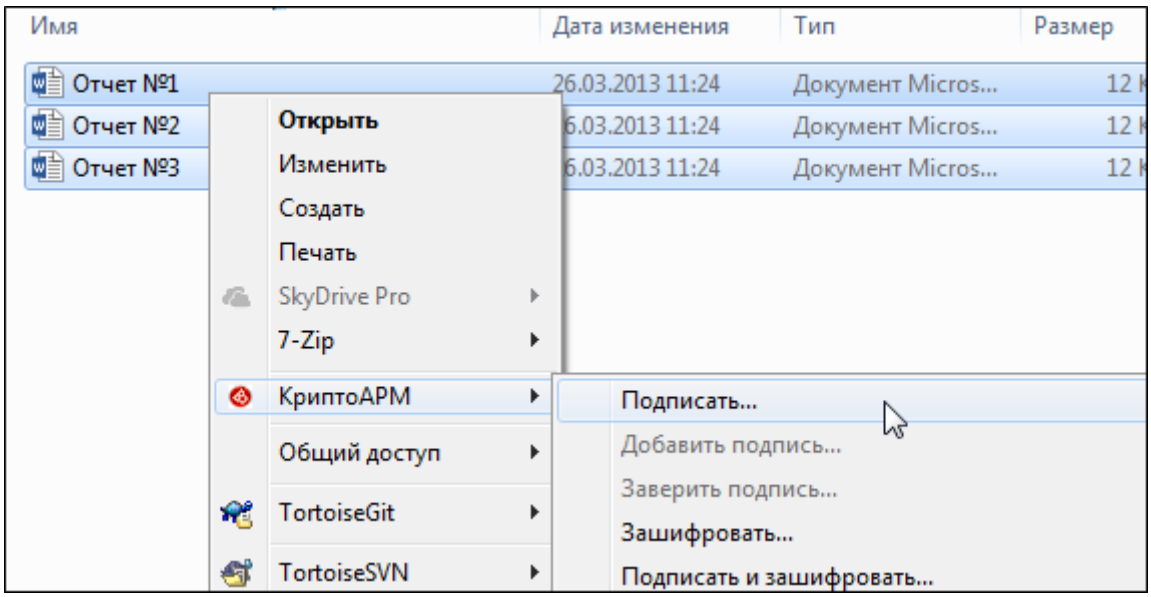
Для выполнения операций через панель задач:

1. Откройте программу «КриптоАРМ» (**Пуск > Программы >** «**КриптоАРМ»**)
2. Значок «**КриптоАРМ»** появится в правом углу на панели задач

3. Правой клавишей мыши откройте контекстное меню и выберите нужную операцию.
4. Далее следуйте шагам Помощника выбранной операции.

6.4.3 Интеграция в Проводник Windows

Вы можете работать с программой «КриптоАРМ» в Проводнике Windows через контекстное меню файлов.



Этот вариант позволяет быстро и удобно выполнять основные операции с электронными данными:

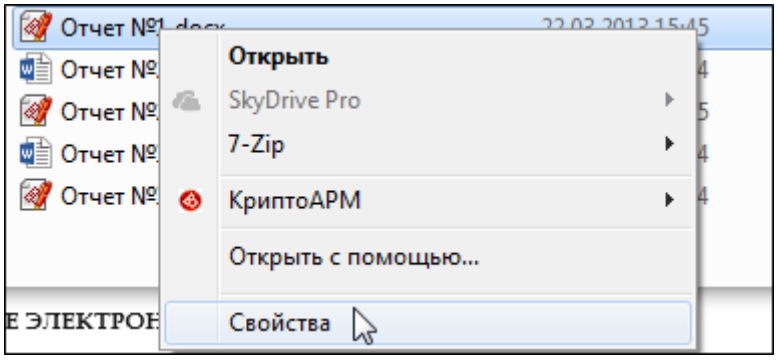
- подписывать электронной подписью
- проверять корректность подписи
- шифровать
- расшифровывать файлы
- одновременно шифровать и подписывать данные
- одновременно расшифровывать данные и проверять корректность электронной подписи
- устанавливать режимы выполнения криптоопераций
- выбирать настройки для выполнения криптоопераций

Для выполнения операций в Проводнике Windows:

1. Откройте в Проводнике папку, где находится файл, который необходимо зашифровать или подписать.
2. Правой клавишей мыши откройте контекстное меню файла или сразу нескольких файлов и выберите нужную операцию.
3. Далее следуйте шагам Помощника выбранной операции.

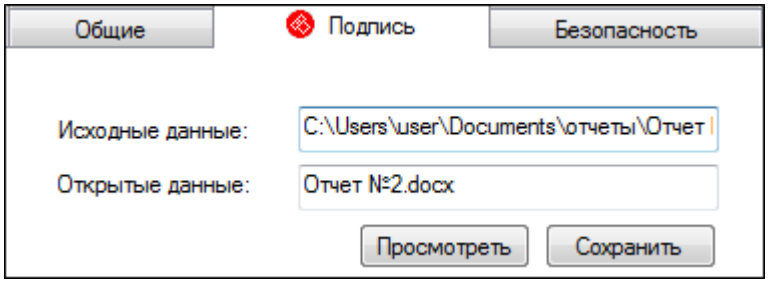
В случае если вы выбрали для операции сразу несколько файлов, они будут обработаны последовательно.

Начиная с версии 4.5 программа «КриптоАРМ» более тесно интегрирована с операционной системой Windows. Пользователь может работать с подписанными ЭП (тип совмещенной подписи) и/или зашифрованными электронными документами с помощью «КриптоАРМ» в Проводнике через стандартное окно свойств документов.



В окне **Свойства** появляются дополнительные закладки:

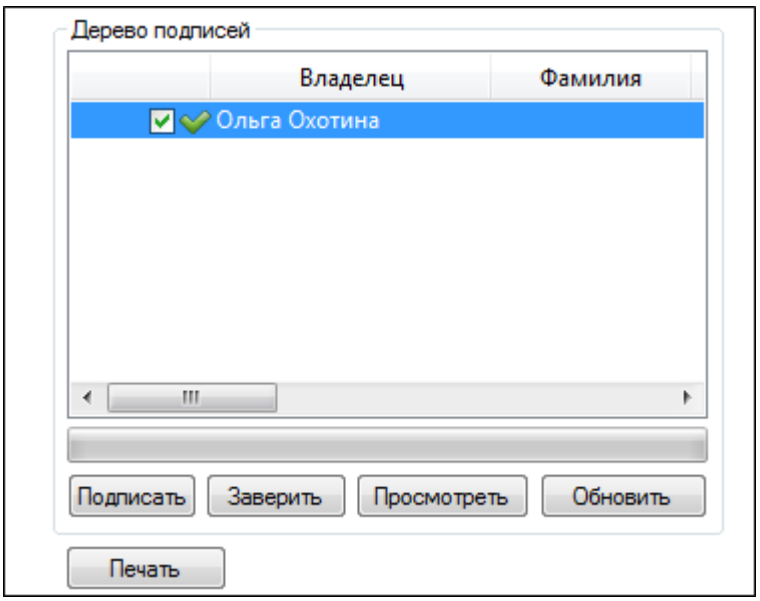
1. Закладка **Подпись.** В этой закладке вы можете:
    1) Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).



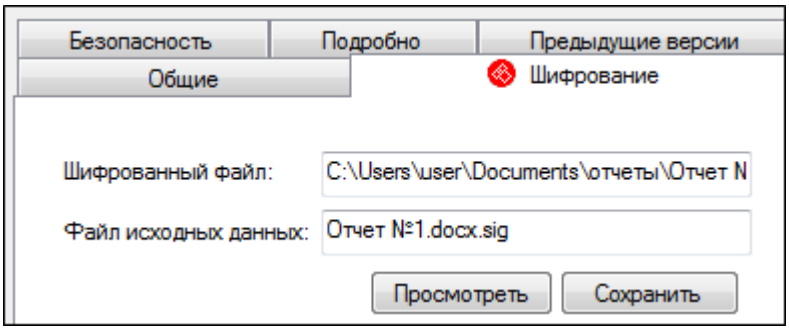
    2) Просмотреть следующую информацию (кнопка **Просмотреть**):

- о добавленной к файлу электронной подписи
- о сертификате, с помощью которого был подписан файл, и его статусе
- о штампах времени на подпись и подписываемые данных

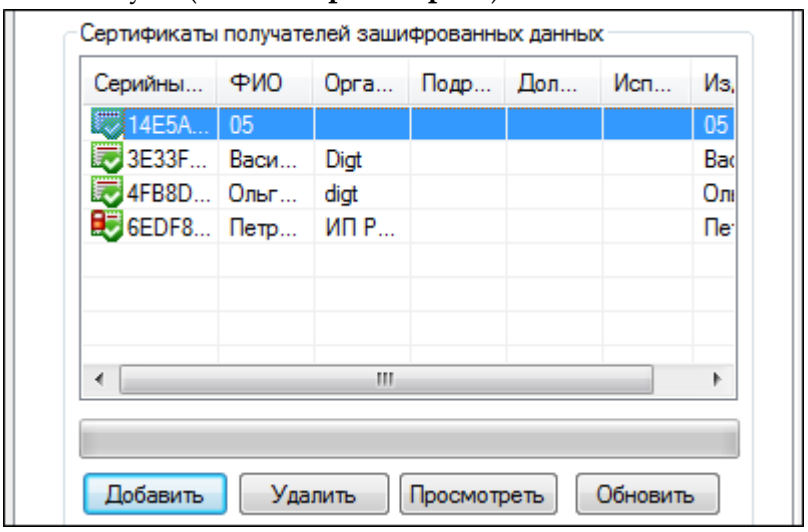
    1) Добавить подпись (кнопка **Подписать**).
    2) Заверить подпись (обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя)
    3) Распечатать информацию (кнопка **Печать**) о ЭП - в новом окне браузера MS IE будет сформирована печатная форма с информацией о подписи.
    4) Обновить информацию о подписи (кнопка **Обновить**).



2. Закладка **Шифрование.** В этой закладке вы можете:
   1) Просмотреть путь, по которому сохранен зашифрованный файл;
   2) Просмотреть зашифрованный файл (кнопка **Просмотреть** рядом со строкой **Файл исходных данных**);
   3) Сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);



   4) Просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**);



Сертификат расшифрования данных отмечается значком -  . Сертификатом расшифрования становится первый из списка сертификат получателей, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками.

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно).

При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы в адрес измененного списка получателей.

Также вы можете просмотреть результаты проверки корректности электронной подписи в любом стандартном окне ОС Windows и определить возможность расшифрования документа по специальному значку.

Данные значки по умолчанию не появляются, необходимо в параметрах программы включить проверку статуса документов с ЭП и шифрованных архивов в Проводнике.

Значок	Описание
	Подписанный документ (без проверки корректности ЭП в Проводнике)
	Подписанный документ, ЭП корректна
	Подписанный документ, подпись некорректна
	Подписанный документ, нет полного доверия к сертификатам подписи (отсутствует COC)
	Подписанный документ, подпись повреждена
	Операция проверки остановлена в случаях: • размер файла превышает ограничение, указанное в параметрах к программе • ЭП отделенная, и для нее отсутствует подписанный файл
	Шифрованный документ (без проверки в Проводнике)
	Шифрованный документ, можно расшифровать
	Шифрованный документ, можно расшифровать, но сертификат расшифрования недействителен
	Шифрованный документ, нет полного доверия к сертификату расшифрования
	Шифрованный документ, расшифровать нельзя

7 НАСТРОЙКИ И ПАРАМЕТРЫ ПРОГРАММЫ

Для того чтобы оперативно выполнять криптооперации, в программе «КриптоАРМ» реализована возможность устанавливать индивидуальные настройки и режимы работы. Для каждой ситуации вы можете установить индивидуальную настройку для выполнения криптографических операций, работы с сертификатами и т.п. (выбрать криптопровайдер, сертификаты, тип криптографических алгоритмов, указать получателей данных и др.)

Для обмена документами с бухгалтером вы можете установить одну настройку, с партнерами — вторую, с клиентами — третью и использовать каждую из них при взаимодействии с этими группами людей.

В этом разделе вы найдете следующую информацию:

- Как управлять настройками приложения
- Как настроить Параметры программы

7.1 ПАРАМЕТРЫ ПРОГРАММЫ

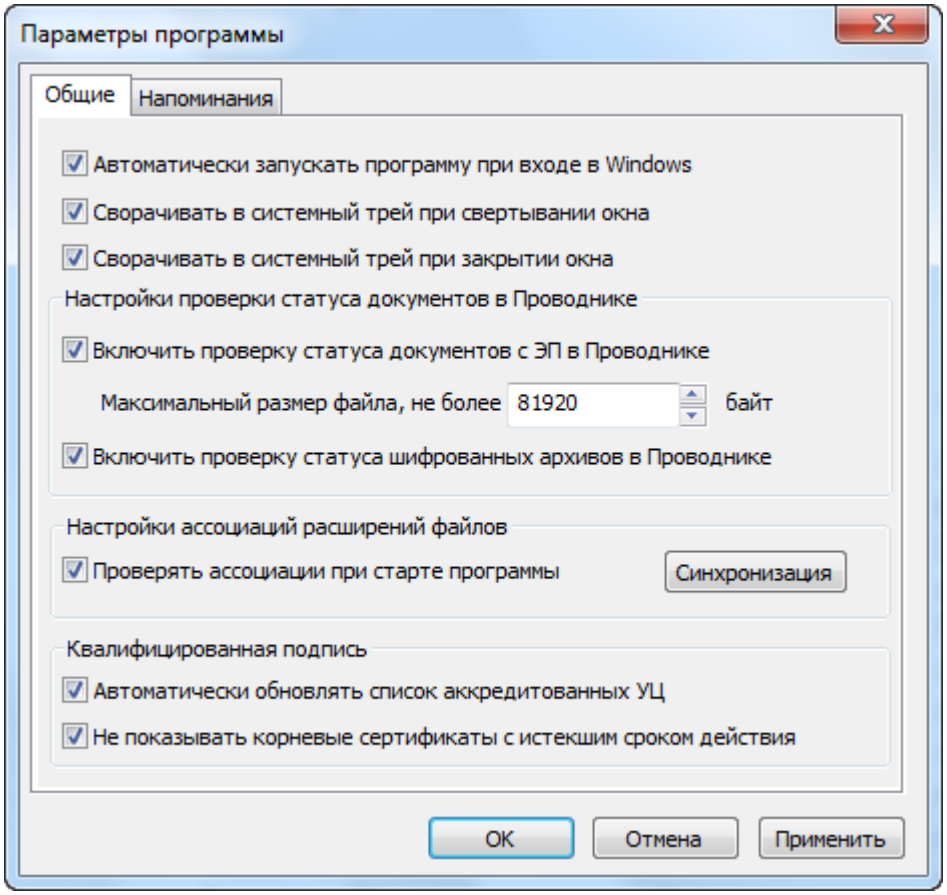
В главе **Параметры программы** вы найдете информацию о том,

- как создать общие установки приложения;
- как настроить напоминания о событиях.

7.1.1 ОБЩИЕ УСТАНОВКИ

Настроить базовые параметры программы вы можете через Главное окно программы. Для того чтобы настроить параметры «КриптоАРМ», выполните следующие шаги:

1. В главном окне в верхней панели инструментов откройте пункт меню **Сервис > Параметры программы**.
2. Откроется окно **Параметры программы**



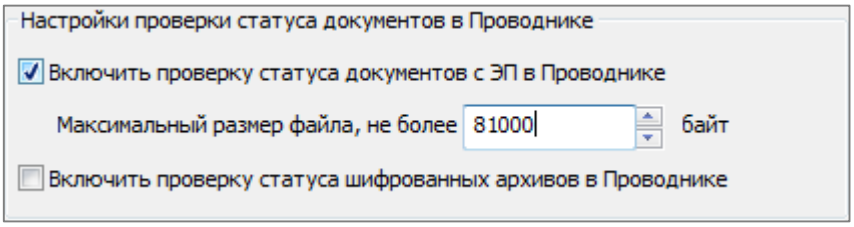
В окне вы можете настроить:

- Автоматический запуск программы при входе в Windows;
- Сворачивание главного окна программы в системный трей (панель задач) при свёртывании/ закрытии окна;
- Проверку статуса документов в Проводнике Windows;
- Настроить работу с квалифицированной подписью

Настройка проверки статуса документов в Проводнике

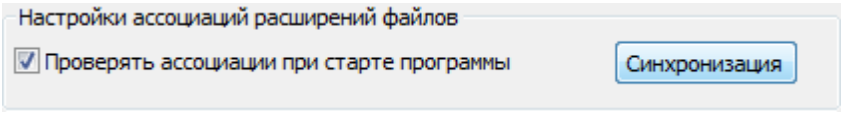
Автоматическая проверка статуса подписанных или зашифрованных документов может работать некорректно. Дело в том, количество overlays в операционной системе Windows ограничено 15-ю элементами. Если у вас установлено много программ, которые используют элементы overlays для отображения информации, то элементы приложения «КриптоАРМ» могут просто не попасть в это количество и соответственно не отображаться.

При настройке проверки статуса документов, подписанных электронной подписью, в Проводнике вы можете указать максимальный размер для проверяемых файлов. Это необходимо для того, чтобы не уменьшалась скорость работы компьютера при обработке файлов большого размера.



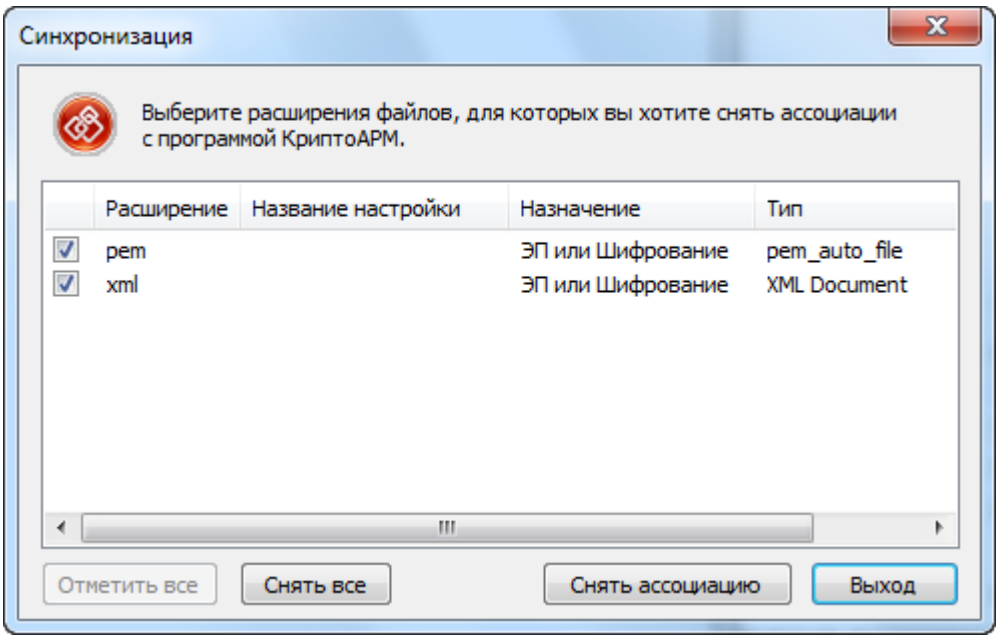
Проверка ассоциаций расширений файлов при старте программы «КриптоАРМ»

Для просмотра и редактирования списка файловых расширений, имеющих ассоциацию с программой «КриптоАРМ», нажмите на кнопку **Синхронизация**.



В окне **Сихронизация** содержится следующая информация об установленных ассоциациях:

- Расширение - название расширения для файла.
- Название настройки - настройка программы в «КриптоАРМ», в которой по умолчанию выбрано данное расширение.
- Назначение - назначение файлов с указанным расширением в программе «КриптоАРМ».
- Тип - определяемый Windows тип файла.



Кнопка **Снять ассоциацию** позволяет выборочно снять ассоциацию с файловых расширений.

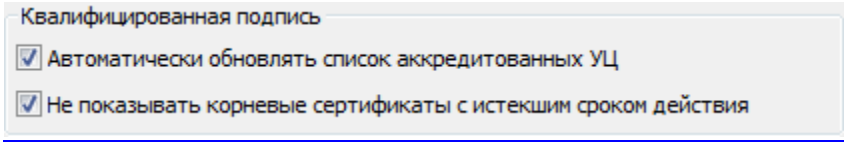
Чтобы снять ассоциацию с программой «КриптоАРМ» у всего списка файловых расширений, нажмите на кнопку **Отметить все** и затем **Снять все**.

Восстановить ассоциацию для расширений, которые указаны в настройках, можно в самой настройке, нажав кнопку **Установить ассоциацию**. Подробнее об этом читайте в главе Настройки операции подписи.

Настройка параметров работы с квалифицированной подписью

«КриптоАРМ» версии 5.1 и выше имеет специальный режим «Квалифицированная подпись» для работы только с сертификатами от аккредитованных УЦ

На портале Уполномоченного федерального органа в области электронной подписи Минкомсвязи размещается актуальный список аккредитованных удостоверяющих центров. Этот список используется «КриптоАРМ»ом в качестве фильтра при работе с электронной подписью. Список постоянно обновляется, поэтому удобнее настроить автоматическое обновление списка аккредитованных УЦ (чтобы не делать это каждый раз вручную). Здесь же вы можете отключить показ корневых сертификатов удостоверяющего центра с истекшим сроком действия:



7.1.2 Напоминания о событиях

С помощью программы «КриптоАРМ» вы можете настраивать предварительное напоминание для конкретного события, связанного со сроком действия

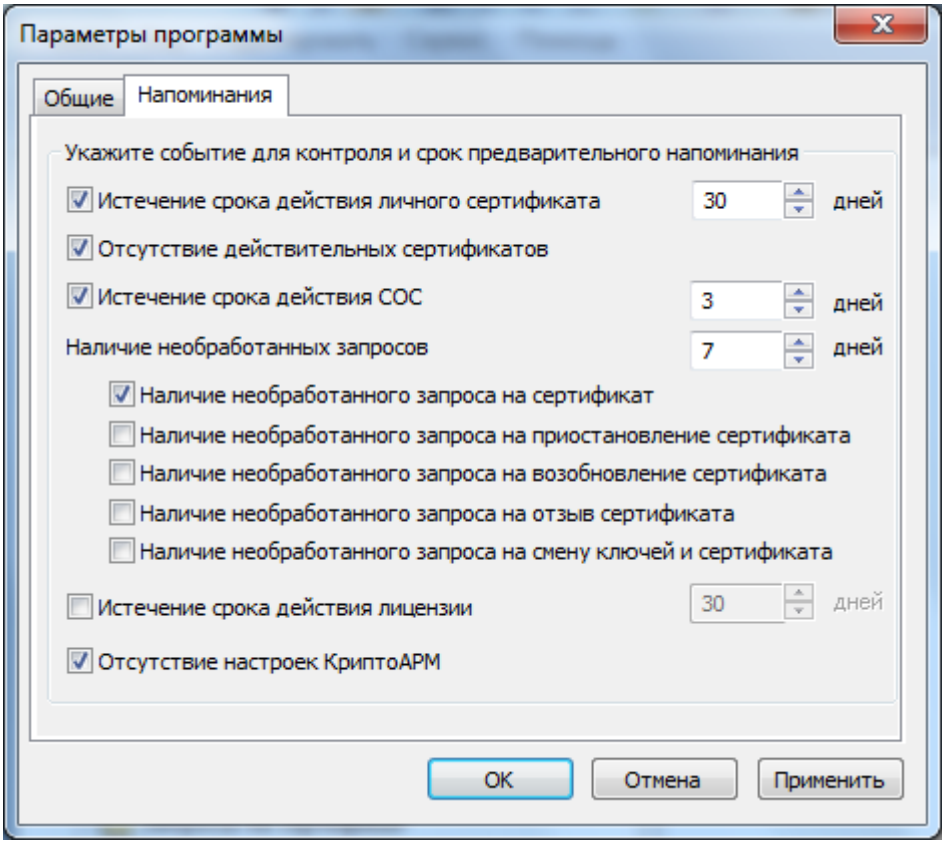
- личного сертификата;
- списка отзыва сертификатов;
- статуса запросов, переданных на рассмотрение в УЦ;
- лицензии приложение «КриптоАРМ».

Также вы можете активировать напоминание об отсутствие настроек «КриптоАРМ».

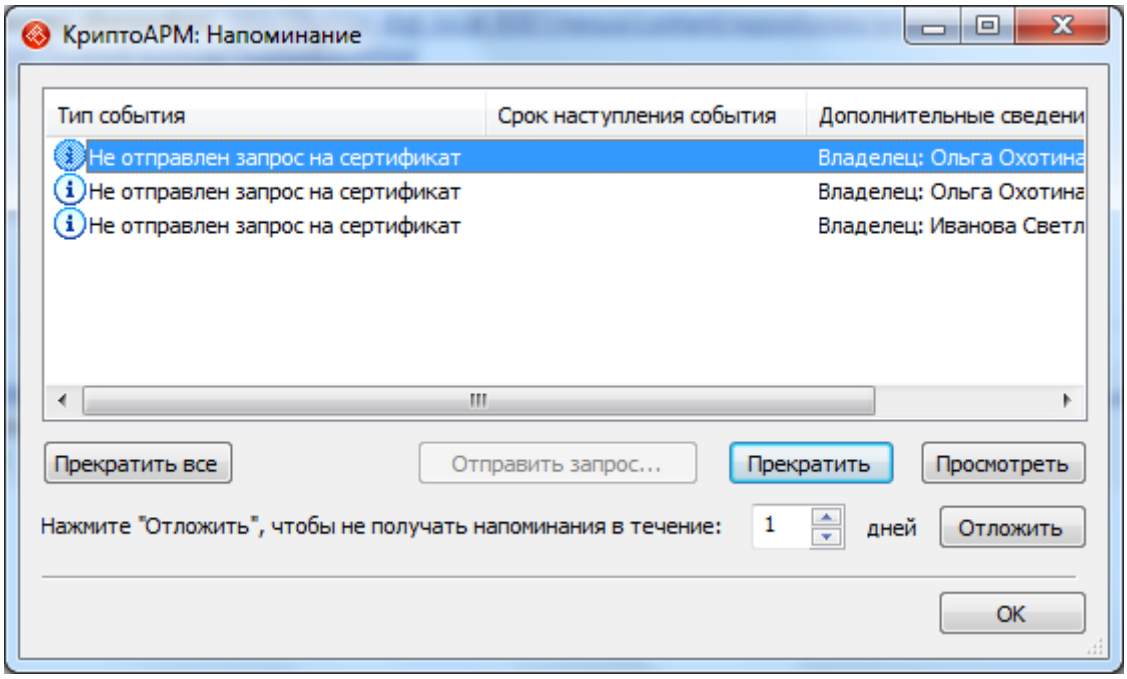
Настраивать напоминания о планируемых событиях, связанных с вышеназванными объектами, вы можете через главное окно программы.

Для того чтобы настроить напоминание:

1. В верхнем меню главного окна выберите пункт **Сервис > Параметры программы.**
2. Перейдите на вкладку **Напоминания** и укажите те события, срок действия которых необходимо контролировать, и срок предварительного напоминания об истечении действия указанного события:



При наступлении установленного срока предварительного напоминания об указанном событии откроется окно напоминания:



Вы можете отказаться от поступивших напоминаний:

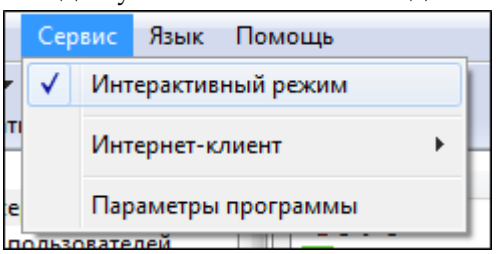
1. На срок в несколько дней (кнопка **Отложить**, которая станет доступна, если выделено одно или несколько напоминаний в списке).
2. Навсегда (кнопка **Прекратить все**, которая позволяет прекратить все напоминания в списке, и кнопка **Прекратить**, которая становится доступной только в случае, если выделено одно или несколько напоминаний в списке).

7.1.3 Режимы работы

При выполнении криптооперации вы можете проходить все шаги для указания нужных параметров либо использовать ранее созданную настройку для автоматизации процесса. О том, как установить параметры настройки читайте в главе Управление настройками программы. Соответственно, работу с «КриптоАРМ» вы можете вести в нескольких режимах:

- Интерактивный (пошаговый)

Если в программе установлен интерактивный режим, при выполнении операции вам будут доступны шаги Помощника для указания всех необходимых параметров.



При этом параметры, указанные вами заранее в настройке, используемой по умолчанию, будут автоматически подставляться в соответствующие поля. При необходимости вы можете указать другие параметры.

Для установки интерактивного режима установите флаг напротив строки **Интерактивный режим**.

- Неинтерактивный (автоматический)

Предназначен для автоматизации процесса выполнения криптоопераций. При неинтерактивном режиме программа использует в качестве шаблона ту настройку, которую вы установили, как "по умолчанию".

В этом случае во время операции программой запрашивается ввод только тех параметров, которые не указаны в данной настройке. Остальные шаги операции выполняются программой автоматически согласно указанным параметрам в настройке.

Для установки неинтерактивного режима удалите флаг напротив строки **Интерактивный режим**.

Начиная с версии 5.1 в программу добавлен режим «Квалифицированная подпись». Подробнее о режиме читайте в главе **Работа с квалифицированными сертификатами**.

7.2 Управление настройками

В главе **Управление настройками** вы найдете информацию о том, какие параметры вы можете настроить для выполнения криптоопераций. О том, как создать новую настройку и какие операции вы можете выполнять с уже созданными настройками, читайте в главе Операции с настройками.

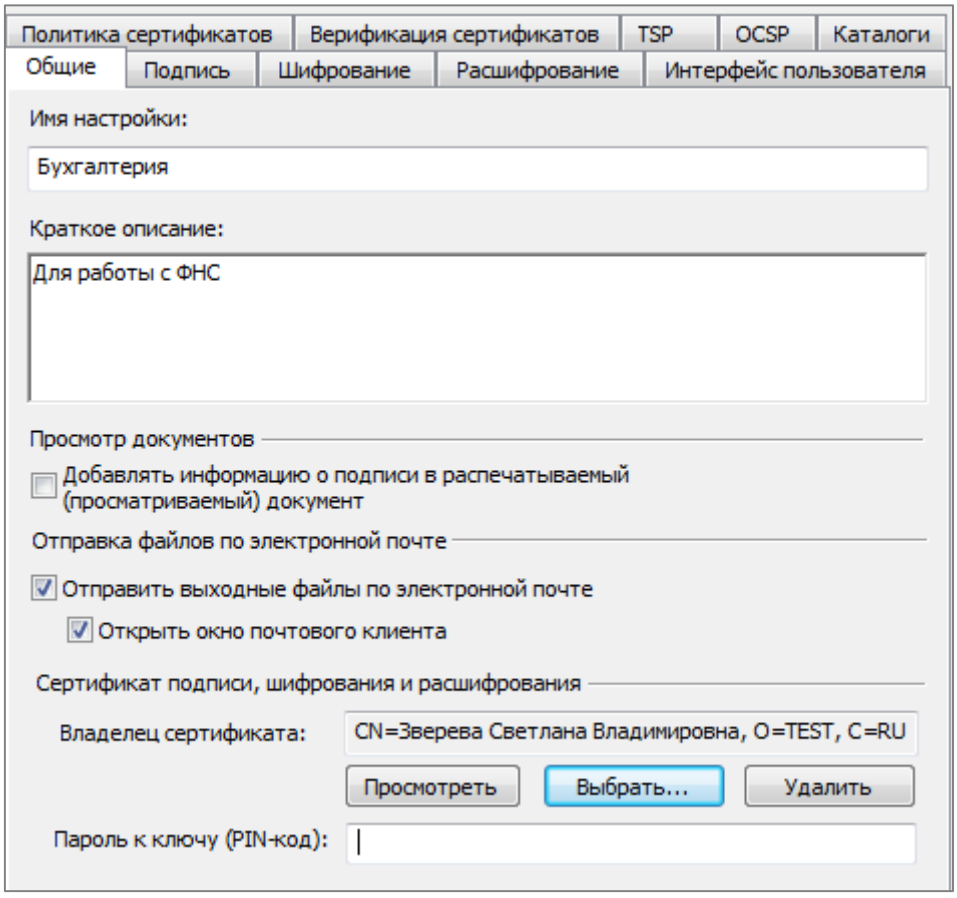
Вы можете указать параметры для общей настройки, а также параметры настройки для:

- выполнения операций подписи, шифрования и расшифрования
- настройки вида программы (ее интерфейса)
- использования политик сертификатов
- верификации сертификатов
- использования служб TSP и OSCP
- настройки каталогов хранения файлов

7.2.1 Общие настройки

Для установки общих параметров в настройке выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры подписи которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**
2. Откроется окно **Параметры настройки**. Выберите закладку окна **Общие** и укажите:
   - Имя настройки,
   - Краткое описание настройки (для чего будет использоваться настройка),
   - Требуется ли добавлять информацию о подписи в распечатываемый (просматриваемый) документ,
   - Следует ли отправлять выходные данные по электронной почте,
   - Сертификат, который будет использоваться для подписи/шифрования и расшифрования
   - Пароль к ключу (PIN-код) (дополнительная опция, которую мы советуем использовать крайне осторожно, только в тех ситуациях, когда хочется избавиться от ручного ввода пин-кода, даже с учетом понижения уровня защищенности)

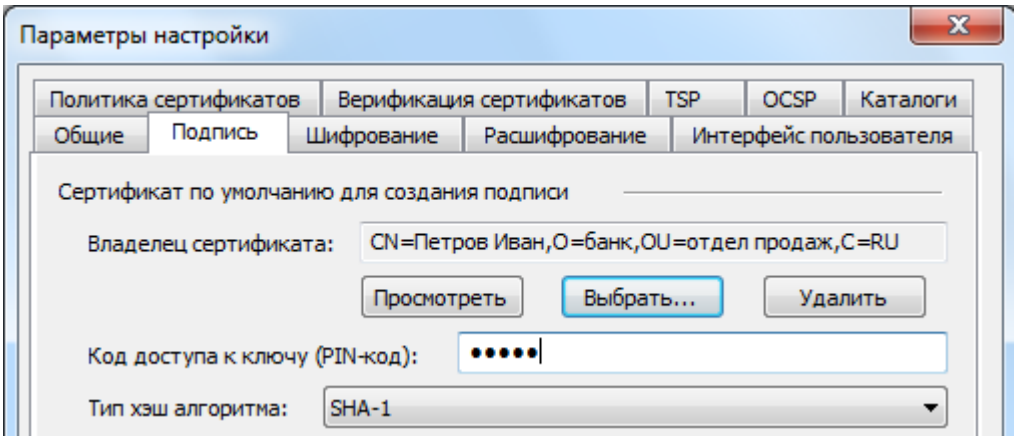


7.2.2 НАСТРОЙКИ ОПЕРАЦИИ ПОДПИСИ

Для установки параметров подписи в настройке выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры подписи которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**
2. Откроется окно **Параметры настройки**. Выберите закладку окна **Подпись.**
3. Укажите сертификат по умолчанию для создания подписи.

1) Выберите сертификат (кнопка **Выбрать**). При этом в поле **Владелец сертификата** отобразится информация о владельце указанного сертификата. Выбранный вами сертификат можно при необходимости удалить из настроек (кнопка **Удалить**), а также просмотреть общую и детальную информацию о нем (кнопка **Просмотреть**).



2) В поле **Код доступа к ключу** вы можете ввести пин-код к закрытому ключу выбранного сертификата.

Помните, что хранение кода доступа к закрытому ключу в настройке может быть небезопасным.

3) Выберите тип хэш-алгоритма, на основе которого будет создаваться ЭП.

4. Вы также можете указать другие настройки:
   1) Из выпадающего списка выбрать **Формат подписи**:

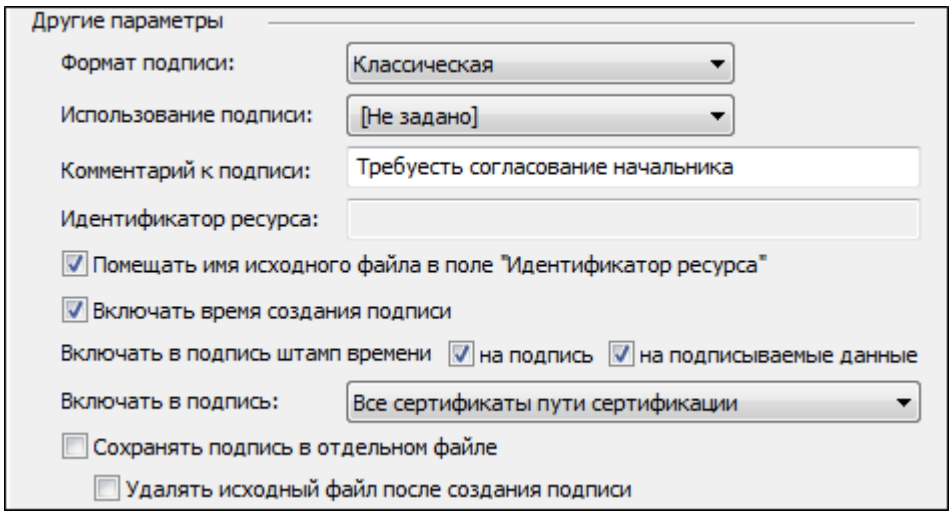
- классическая

Содержимое ключей и сертификатов позволяет установить авторство электронного документа, однако в используемом сегодня формате ЭП не фиксируется время её создания и статус сертификата открытого ключа на момент подписи (действителен, отозван, приостановлен), что в конечном счете затрудняет юридически значимый электронный документооборот и процедуру доказательства подлинности ЭП.

- усовершенствованная

Усовершенствованная электронная подпись. Предназначена для разрешения споров между подписывающей и проверяющей сторонами, которые могут возникать в отдаленном будущем, даже годы спустя момента их создания.

Для работы с усовершенствованной ЭП организации требуется использование услуг доверенных служб (Служба штампов времени и Служба актуальных статусов), а также наборов данных (кросс-сертификаты, списки отзывов), которые необходимы для документов с ЭП длительного хранения (в том случае, когда срок хранения превышает срок действия сертификата, которым были документы подписаны).



2) **Использование подписи;**

Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

3) **Комментарий к подписи;**

Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

4) **Идентификатор ресурса;**

Под идентификатором ресурса понимается:

- путь до исходного, подписываемого файла (на компьютере или в Интернете, где находится данный файл)
- имя файла (указывается для того, чтобы в случае изменения имени файла получатель подписанного документа смог определить первоначальное его название).

5) **Включить время создания подписи;**

При установке флага - в файл подписи будет включено время подписи.

6) **Включить штамп времени**

- **на подписываемые данные;**

При установке этого флага в файл ЭП будет включен штамп времени на исходные данные.

Штамп времени на документе удостоверяет время создания документа для последующего разрешения конфликтов, связанных с использованием электронного документа. Эта возможность способствует обеспечению неотказуемости от подписи.

Наличие штампа времени в подписанном документе позволяет продлевать срок действия ЭП. Такой штамп удостоверяет, например, что подпись была создана до того, как сертификат ключа подписи был аннулирован (отозван). Таким образом, сохраняется возможность использования отозванного сертификата для проверки ЭП, созданных до момента отзыва. Эта проблема актуальна для всех систем электронного документооборота.

- **на подпись**

При установке этого флага в файл ЭП будет включен штамп времени на создаваемую электронную подпись.

Флаг доступен только при установленной лицензии на модуль TSP.

7) **Включить в подпись:**

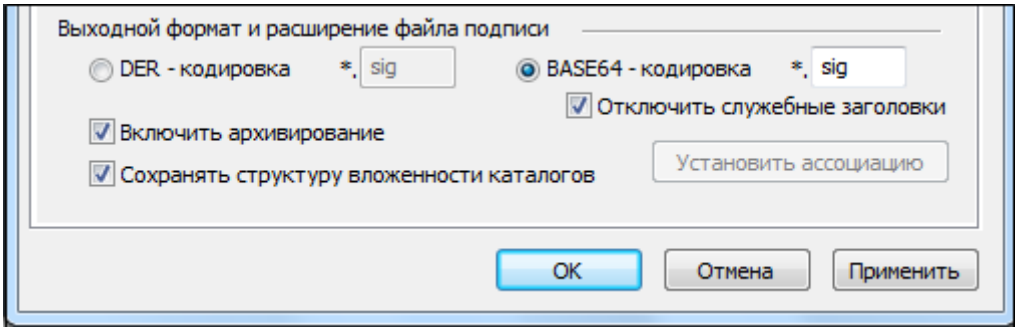
- только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.

8) **Сохранить подпись в отдельном файле;**

При установке флага будет создана отделенная электронная подпись на файле (например, может быть удобна в том случае, если вы отправляете документ человеку, который не использует «КриптоАРМ» и ему важна не столько подпись, сколько сами данные).

При отсутствии флага - будет сформирована электронная подпись, включающая в себя файл с исходными данными (в этом случае документ и ЭП будут храниться вместе). Такая подпись называется совмещенной.

5. Установите параметры выходного формата и расширения файла подписи:



1) **Кодировка и расширение;**

- DER encoded binary X.509

Платформенно-независимый метод хранения сертификатов. Может использоваться для их передачи между компьютерами.

Расширения подписанного файла *.sig, *.p7s.

- Base64 encoded X.509

Вариант кодирования, разработанный для использования совместно с S/MIME (безопасным протоколом электронной почты). Файл использует ASCII-символы, благодаря чему может пройти неповрежденным через все почтовые шлюзы.

Для этого варианта кодирования вы можете указать флаг **Отключить служебные заголовки** (в этом случае в файле подписи не будут использоваться заголовки, указывающие начало и окончание блока с подписанными данными. Заголовки необходимы для того, чтобы можно было выполнять проверку ЭП более ранними версиями программы «КриптоАРМ»).

2) **Включить архивирование;**

Вы можете указать требуется ли заархивировать подписанные файлы.

3) **Сохранять структуру вложенности каталогов;**

В архиве можно сохранять структуру вложенности каталогов.

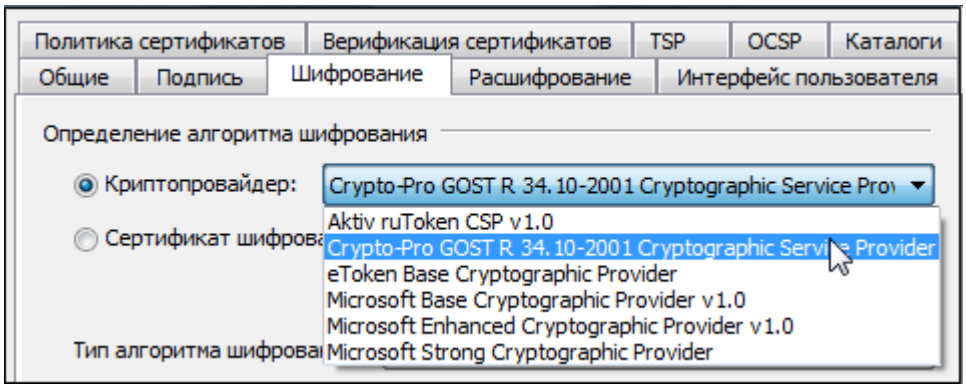
При развертывании корпоративной системы электронного документооборота для подписанных файлов можно установить специальные расширения, отличные от стандартных. Для того чтобы при работе с программой «**КриптоАРМ»** эти файлы обрабатывались, необходимо занести новые расширения в список так называемых «ассоциаций». Добавьте необходимое расширение и нажмите на кнопку **Установить ассоциацию.** Для снятия ассоциации с расширения нажмите на кнопку **Снять ассоциации**.

Настроив все необходимые параметры подписи, сохраните внесенные изменения (кнопка **Применить** или **ОК**).

7.2.3 Настройки операции шифрования

Для установки параметров шифрования выполните следующие шаги:

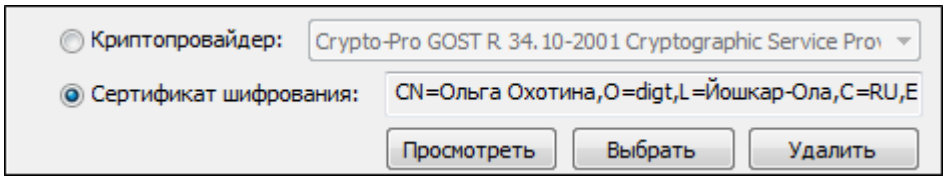
1. В настройке в дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры шифрования которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**
2. Откроется окно **Параметры настройки.** Выберите закладку окна **Шифрование**.
3. Определите алгоритм шифрования:
   1) В выпадающем списке выберите тип **Криптопровайдера**, который будет использован при шифровании данных;



Данный режим шифрования может быть выбран при отсутствии личного сертификата шифрования (В этом случае личный сертификат не выбирается).

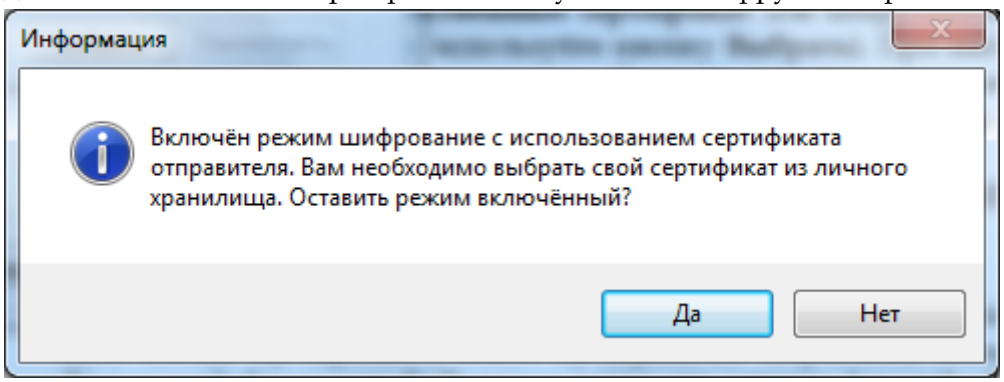
Необходимость выбора криптопровайдера обусловлена тем, что не все криптопровайдеры совместимы, например, нельзя одновременно зашифровать в адрес ключей (сертификатов), созданных на «КриптоПро CSP» и Microsoft Base Cryptographic Provider v1.0.

   2) либо укажите **Сертификат шифрования**;

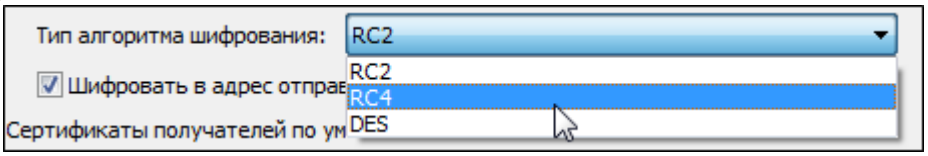


Для смены сертификата, который будет использован при шифровании данных, нажмите на кнопку **Выбрать**. Выбранный вами сертификат можно при необходимости удалить из настройки (кнопка **Удалить**), а также просмотреть общую и детальную информацию о нем (кнопка **Просмотреть);**

При выборе личного сертификата проверяется его статус. Личный сертификат автоматически добавляется в список сертификатов получателей шифруемого файла.



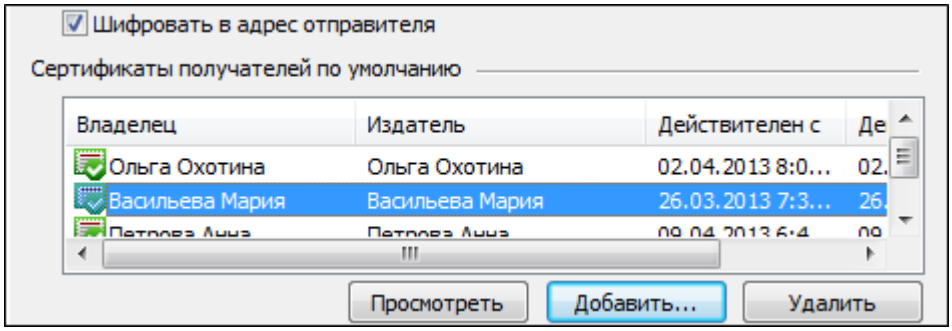
3) в выпадающем списке выберите **Тип алгоритма шифрования** (в зависимости от используемого криптопровайдера).



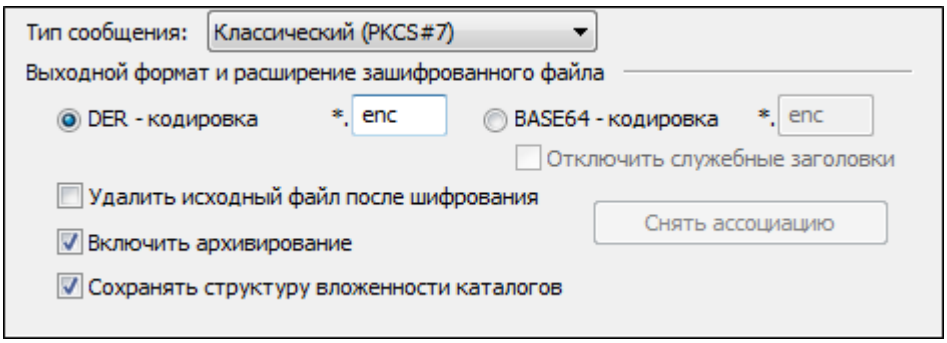
В случае использования криптопровайдера «SafeSign CSP Version 1.0» рабочим алгоритмом шифрования является только RC4.

4) для того чтобы вы смогли расшифровать зашифрованный файл, установите флаг **Шифровать в адрес отправителя**. В этом случае сертификат шифрования попадет в список сертификатов получателей по умолчанию.

4. В окне **Сертификаты получателей по умолчанию** укажите сертификаты, которые будут использоваться настройкой по умолчанию для шифрования данных (кнопка **Добавить**). Вы можете указать личные сертификаты, так и сертификаты других пользователей.



5. Вы можете настроить выходные форматы данных, которые будут использоваться по умолчанию для шифрования данных в этой настройке:



1) **Кодировка и расширение;**

Например, *.enc, *.p7m, *.pem.

Для формата в BASE64-кодировке вы можете указать флаг **Отключить служебные заголовки** (в этом случае в файле подписи не будут использоваться заголовки, указывающие начало и окончание блока с подписанными данными. Заголовки необходимы для того, чтобы можно было выполнять проверку ЭП более ранними версиями программы «КриптоАРМ»).

Регистрация дополнительных расширений файлов, которые должны ассоциироваться с программой «КриптоАРМ». При развертывании корпоративной системы электронного документооборота для зашифрованных файлов можно установить специальные расширения, отличные от стандартных. Для того чтобы при работе с программой «КриптоАРМ» эти файлы обрабатывались, необходимо занести новые расширения в список так называемых «ассоциаций». Добавьте необходимое расширение и нажмите на кнопку **Установить ассоциацию.** Для снятия ассоциации с расширения нажмите на кнопку **Снять ассоциации**.

2) **Удалить исходные файлы после выполнения операции**.

В этом случае исходный файл, выбранный пользователем для шифрования, будет удален после успешного завершения операции

3) **Включить архивирование;**

Вы можете указать требуется ли заархивировать зашифрованные файлы.

4) **Сохранять структуру вложенности каталогов;**

В архиве можно сохранить структуру вложенности каталогов.

6. Настроив все необходимые параметры шифрования, сохраните внесенные изменения (кнопка **Применить**).

7.2.4 Настройки операции расшифрования

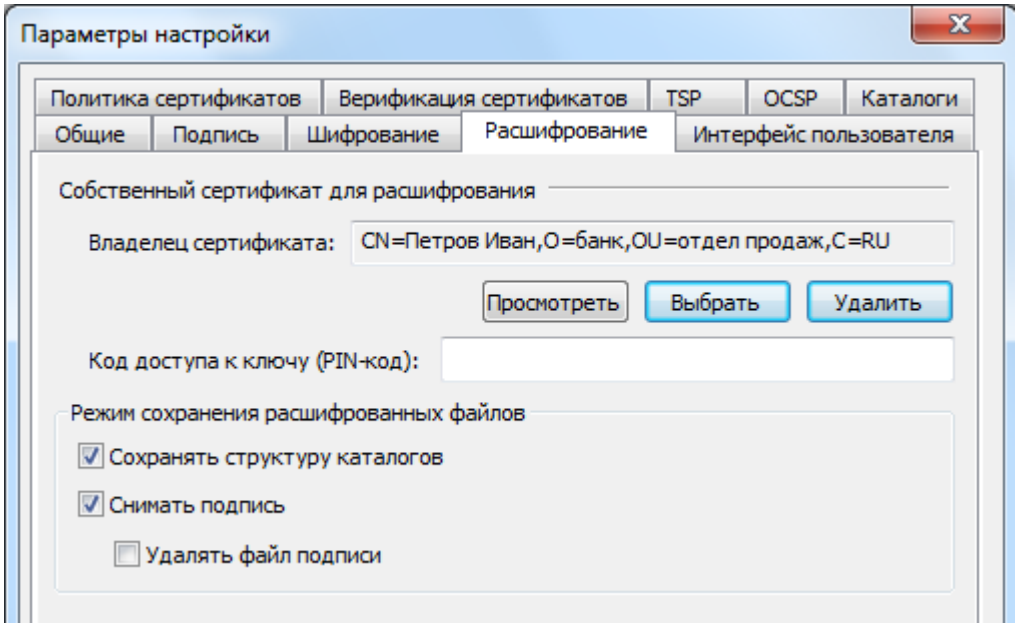
Для установки параметров расшифрования:

1. Для установки параметров расшифрования в настройке в дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры шифрования которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**
2. Откроется окно **Параметры настройки**. Выберите закладку окна **Расшифрование**.
3. Выберите сертификат, который будет использоваться данной настройкой по умолчанию для расшифрования (кнопка **Выбрать**). В текстовом поле **Владелец сертификата** отобразится информация о владельце указанного сертификата. Выбранный вами сертификат можно при необходимости удалить из настроек профиля (кнопка **Удалить**), а также просмотреть общую и детальную информацию о нем (кнопка **Просмотреть**).

4. В поле **Код доступа к ключу** вы можете ввести пин-код к закрытому ключу выбранного сертификата.

Но обратите внимание, хранение кода доступа к закрытому ключу в настройке может быть небезопасным.

5. Установите режим сохранения расширенных файлов. Укажите, требуется ли
- сохранять исходную структуру каталогов при расшифровании;
- снимать электронную подпись с документа и удалять файл подписи.
6. Настроив все необходимые параметры расшифрования, сохраните внесенные изменения (кнопка **Применить**).



7.2.5 Настройки управления интерфейсом

Для установки параметров пользовательского интерфейса выбранной настройки, выполните следующие шаги:

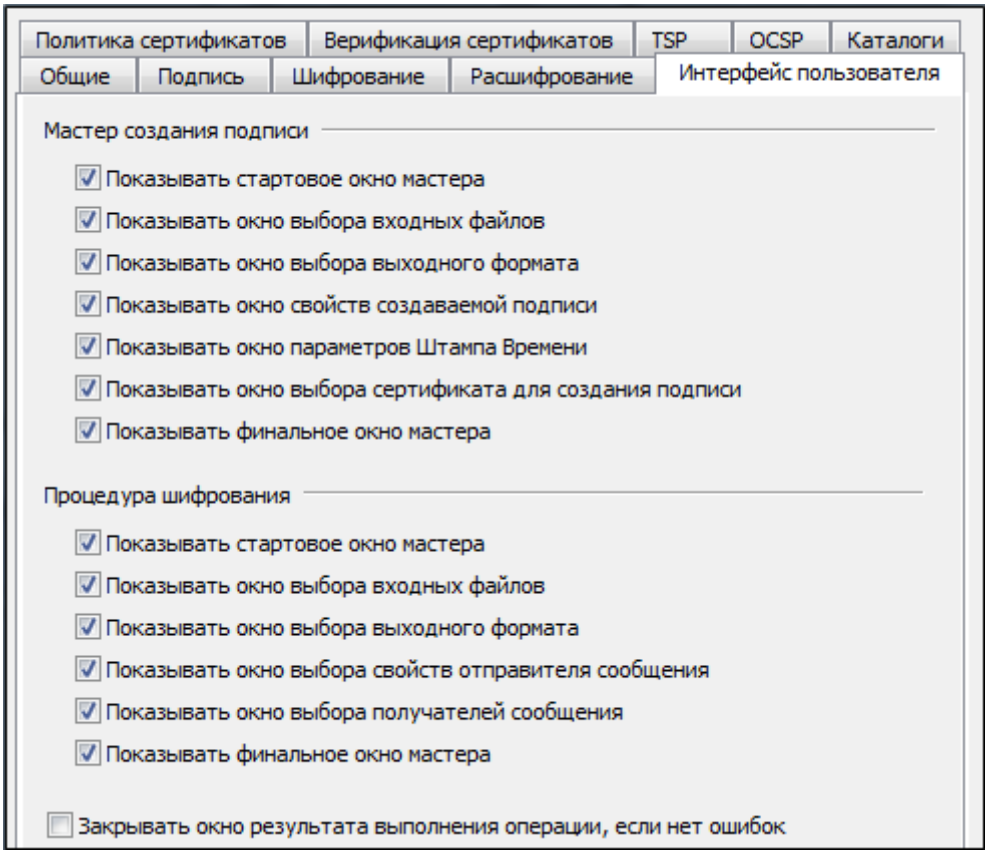
1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры пользовательского интерфейса которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**

2. Откроется окно **Параметры настройки**. Выберите закладку окна **Интерфейс пользователя**. В этом подкаталоге вы можете индивидуально настроить пользовательский интерфейс для следующих видов операций:
- электронная подпись;
- шифрование.

3. Установите флаги напротив полей, описывающих те элементы интерфейса, которые должны показываться при проведении криптоопераций:

- Стартовое окно мастера (для подписи и шифрования);
- Окно выбора списка входных файлов (для подписи и шифрования);

- Окно выбора выходного формата (для подписи и шифрования);
- Окно свойств создаваемой ЭП (для подписи);
- Окно параметров Штампа Времени (для подписи);
- Окно выбора сертификата для создания ЭП (для подписи);
- Окно выбора свойств отправителя сообщения (для шифрования);
- Окно выбора получателя сообщения (для шифрования);
- Финальное окно мастера (для подписи и шифрования).



Вы можете настроить ход операции таким образом, что при отсутствии ошибок в результате выполнения операции финальное окно будет автоматически закрываться - для этого установите флаг напротив строки **Закрывать окно результата выполнения операции, если нет ошибок**.

4. Настроив необходимые параметры интерфейса пользователя, сохраните внесенные изменения (кнопка **Применить**).

7.2.6 Настройки использования политик сертификатов

Вы можете настроить фильтры сертификатов подписи и шифрования по их назначениям, если этого требует политика организации, а также редактировать справочник назначений.

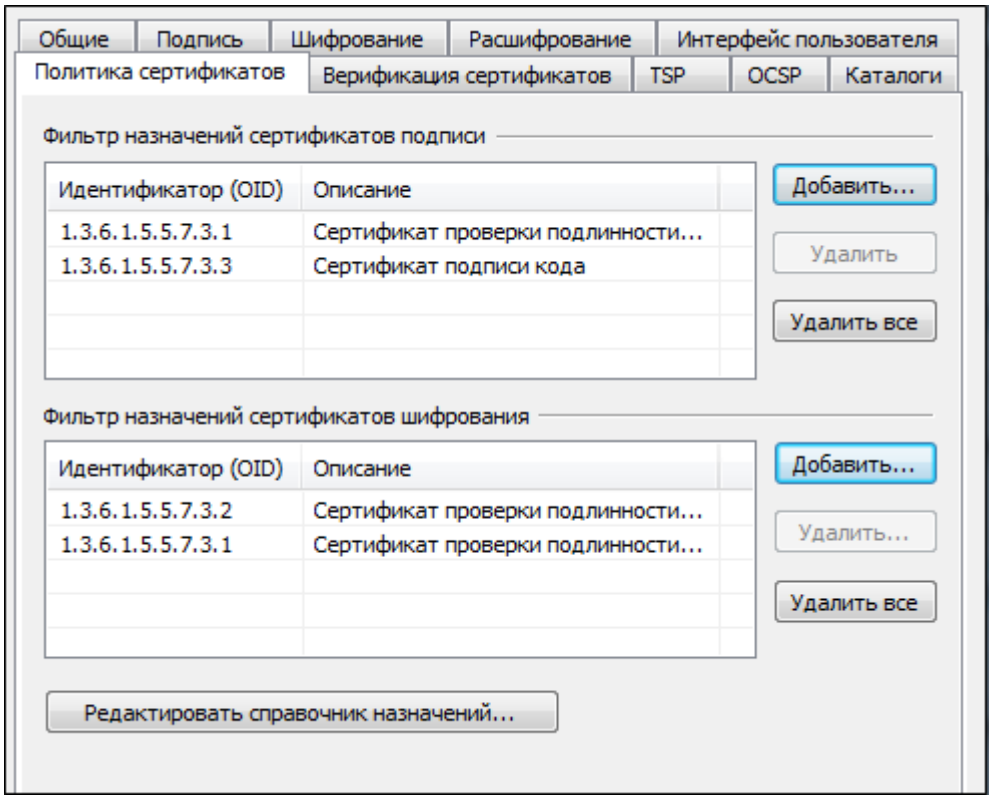
Детали настройки справочника назначений вы можете узнать у вашего системного администратора.

Для настройки параметров политики сертификатов, выполните следующие шаги:

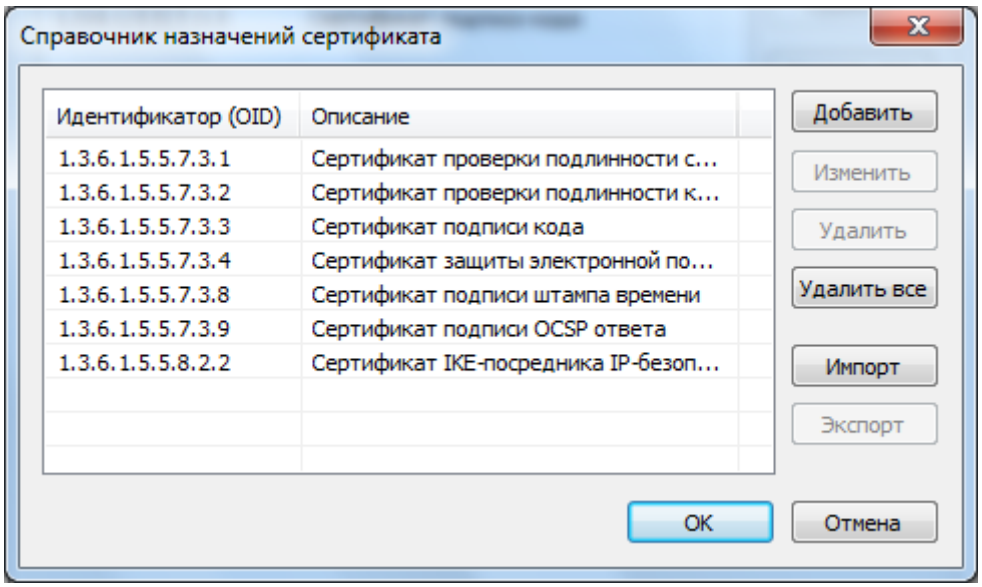
1. В дереве элементов главного окна выберите раздел **Настройки**. В правой панели главного окна отобразится список установленных настроек работы с программой.

Выберите настройку, параметры политики сертификатов которой вы хотите установить, в контекстном меню объекта или на панели инструментов выберите пункт **Свойства**.

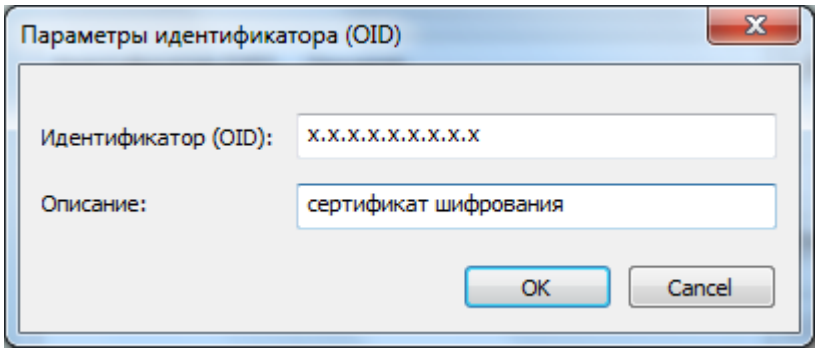
2. Откроется окно **Параметры настройки**. Выберите закладку окна **Политика сертификатов**. В этом окне вы можете настроить фильтры назначений сертификатов подписи и шифрования, а также редактировать справочник назначений.



3. Для формирования фильтра необходимо предварительно занести требуемые назначения сертификатов в справочник назначений.
   Если в настройке установлен фильтр сертификатов для конкретной операции, то в окне выбора сертификата для выполнения этой операции будут доступны только те сертификаты, которые определены в соответствии с установленным фильтром.
4. Выбор идентификаторов (OID) осуществляется из справочника назначений (кнопка **Добавить**). Изначально справочник заполнен некоторыми значениями. Чтобы добавить новый OID в справочник, необходимо нажать на кнопку **Редактировать справочник назначений**. Появится форма редактирования справочника назначений сертификата.



- для добавления нового идентификатора нажмите на кнопку **Добавить**. Откроется окно ввода параметров политики. Введите идентификатор (OID) и его описание. В справочник назначений добавится новая запись;



- изменить параметры идентификатора можно, выбрав в списке необходимый OID и нажав на кнопку **Изменить.** Откроется окно **Параметры идентификатора**, в котором внесите требуемые изменения;
- для удаления OID из справочника нажмите на кнопку **Удалить**, кнопка **Удалить все** позволяет удалить весь список OID данного справочника;
- вы также можете импортировать OID **в формате .xml** в справочник (кнопка **Импорт**) или экспортировать имеющийся в справочнике OID (кнопка **Экспорт**);

5. Установив параметры политики сертификатов, сохраните внесенные изменения (кнопка **Применить**).

7.2.7 Настройки верификации сертификатов

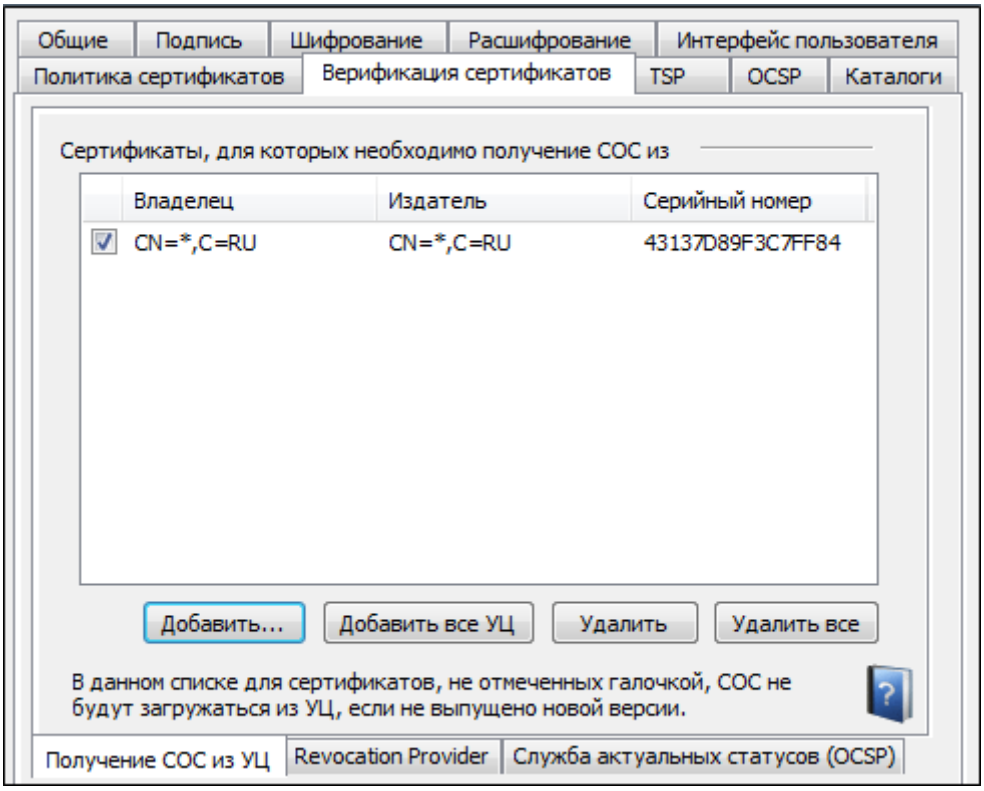
Для установки параметров верификации сертификатов выбранной настройки, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры верификации сертификатов которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**
2. Откроется окно **Параметры настройки**. Выберите закладку **Верификация сертификатов**.

Вы можете установить настройку для проверки статуса сертификатов четырьмя способами:

1) на основе полученного из удостоверяющего центра актуального списка отзыва сертификатов;
2) через Revocation Provider;
3) с помощью Службы актуальных статусов (OCSP);
4) с помощью списка доверенных сертификатов.

3. Откройте закладку, соответствующую выбранному вами типу проверки, и занесите сертификаты, которые требуется проверять именно этим способом:
   - получение COC из УЦ;
   - Revocation Provider;
   - Служба актуальных статусов (OCSP)



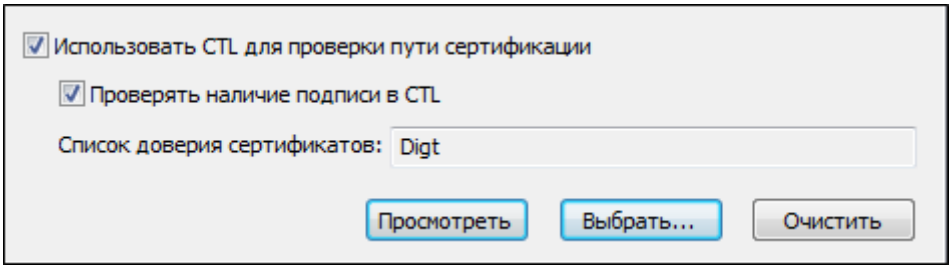
Чтобы проверять статусы сертификатов (личных и других пользователей) способами Получение COC из УЦ или Revocation Provider для всех Удостоверяющих центров (корневые сертификаты которых установлены в хранилище Доверенные корневые центры сертификации), нажмите на кнопку **Добавить все УЦ**.

Вы можете удалить из списка выбранные сертификаты, выделив их и нажав на кнопку **Удалить**. Если вы хотите удалить весь список сертификатов, нажмите кнопку **Удалить все**.

На вкладке **Получение COC из УЦ** рядом с каждым выбранным сертификатом расположена галочка. Если она установлена, COC будет всегда загружаться из удостоверяющего центра. Если же галочка убрана, то COC будет подгружаться только в том случае, если на сервере выпущена новая версия COC или его срок действия истек. «КриптоАРМ» узнаёт о выпуске нового COC по дате планового обновления, указанного в самом COC. Если список отозванных сертификатов будет выпущен внепланово (раньше срока), то его обновление необходимо будет запустить вручную. Узнать о том, как обновить COC из УЦ, можно в разделе Операции с сертификатами.

Детали настройки параметров верификации сертификатов вы можете узнать у системного администратора.

3. Если необходимо проверить сертификат с помощью списка доверенных сертификатов, отметьте в настройках "Использовать CTL для проверки пути сертификации".



4. Далее из хранилища сертификатов необходимо **Выбрать** списки доверенных сертификатов. Если хранилище пусто, то с помощью кнопки **Импорт** установите список.
5. Вы можете удалить выбранный ранее список доверия, нажав на **Очистить**.
6. Настроив необходимые параметры, сохраните внесенные изменения (кнопка **Применить**).

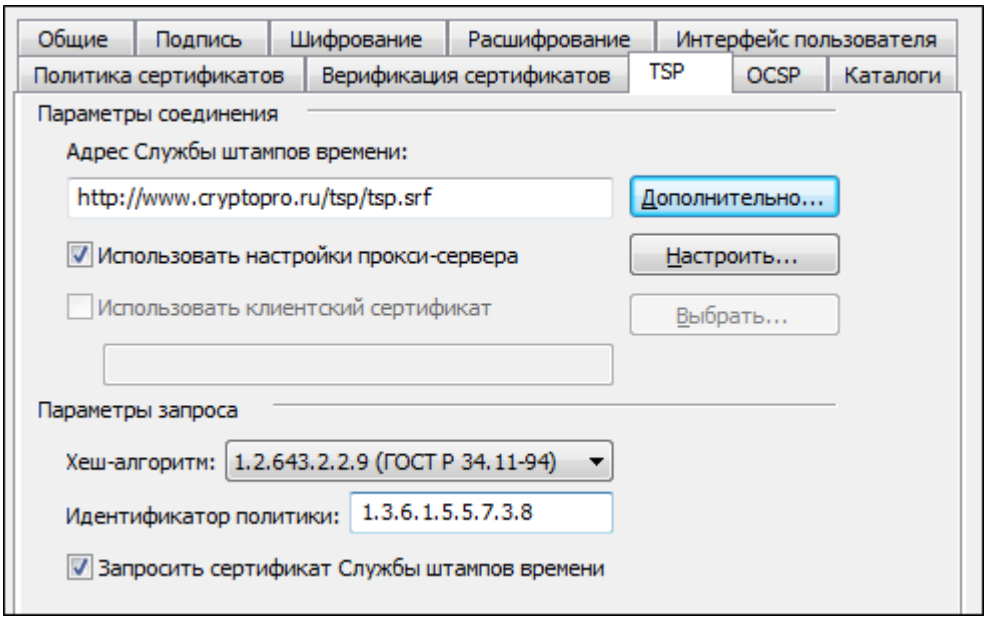
7.2.8 Настройки использования службы TSP

Служба штампов времени используется для простановки штампов времени на документы – данных, защищенных ЭП Службы, содержащих надежную информацию о времени существования электронного документа. Штампы времени используются для привязки факта существования каких-либо данных ко времени.

Для настройки параметров штампа времени, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, параметры получений штампов времени которого вы хотите установить, или на панели инструментов выберите пункт **Свойства.**

2. Откроется окно **Параметры настройки**. Выберите закладку окна **TSP**, в которой укажите параметры соединения со Службой Штампов Времени и параметры запроса.



Детали настройки параметров работы со Службой вы можете узнать у системного администратора.

3. Установив параметры штампа времени, сохраните внесенные изменения (кнопка **Применить**).

7.2.9 Настройки использования службы OCSP

С помощью Службы актуальных статусов сертификатов вы можете в онлайн-режиме проверять статус сертификатов на основе протокола OCSP (Online Certificate Status Protocol).

Для настройки параметров доступа к службе:

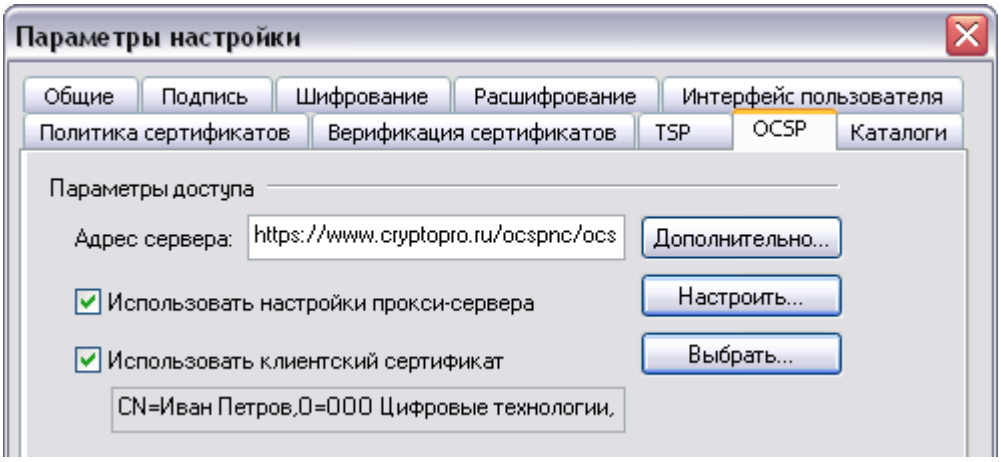
1. В дереве элементов главного окна выберите раздел **Настройки**. В правой панели главного окна отобразится список установленных настроек работы с программой. Выберите настройку, для которой вы хотите установить параметры OCSP, в контекстном меню объекта или на панели инструментов выберите пункт **Свойства**.
2. Откроется окно **Параметры настройки**. Выберите закладку окна **OCSP**, в которой укажите параметры соединения со Службой Актуальных статусов:
   - адрес сервера

Формат адреса: <протокол>://<сервер>[:порт][/путь]. В качестве протокола вы можете указать "http" и "https"

   - настройки прокси-сервера, если при подключении к службе OCSP используется прокси-сервер

Формат адреса: <протокол>://<сервер>[:порт]. В качестве протокола вы можете указать "http" и "https"

   - клиентский сертификат, если доступ к службе OCSP выполняется по цифровым сертификатам (чтобы активировать режим выбора клиентского сертификата, в строке с адресом сервера должен быть указан протокол "https").



Детали настройки параметров работы со Службой вы можете узнать у системного администратора (или в руководстве администратора для программы «КриптоАРМ»).

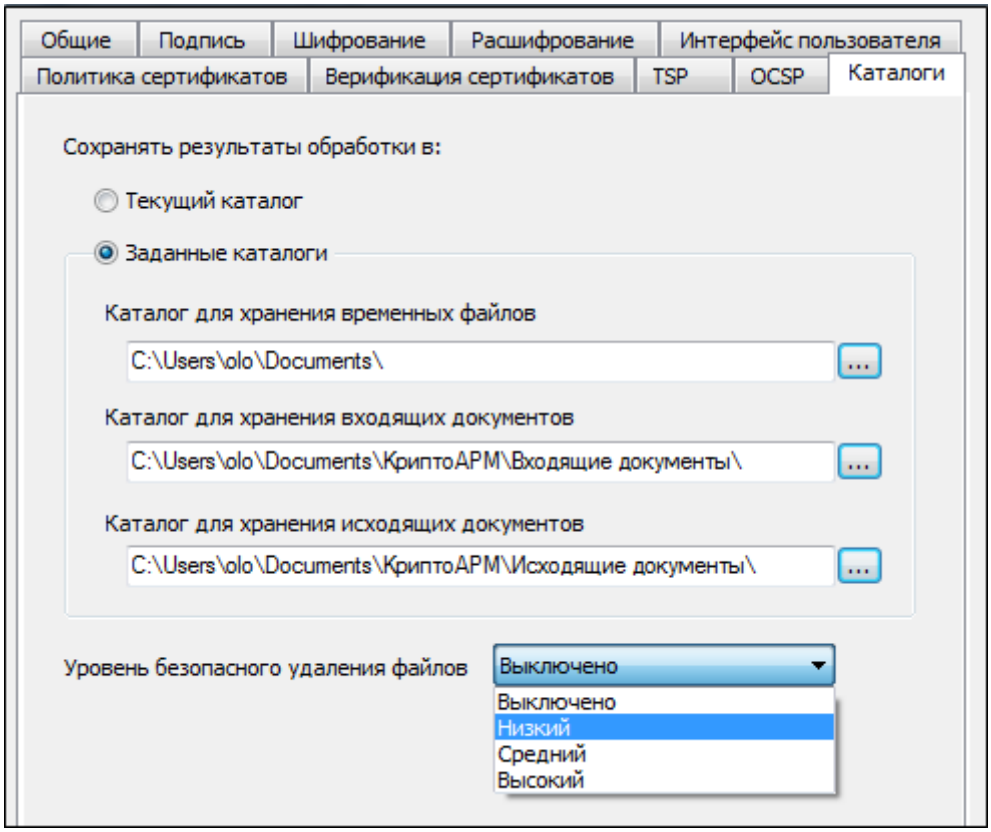
3. Установив параметры доступа, сохраните внесенные изменения (кнопка **Применить**).

7.2.10 Настройки каталогов хранения файлов

Вы можете установить собственные каталоги для хранения файлов, а также уровень безопасного удаления файлов. Для этого выполните следующие шаги:

1. В дереве объектов главного окна выберите раздел **Настройки**. В контекстном меню объекта, параметры которого вы хотите настроить, или на панели инструментов выберите пункт **Свойства.**

2. Откроется окно **Параметры настройки**. Выберите закладку **Каталоги**.



В этом подкаталоге вы можете указать следующие настройки:

1) сохранять результаты обработки в **Текущий каталог**;
2) указать специальные **Каталоги для хранения временных файлов**;

Эта настройка позволяет установить собственный каталог пользователя для временных файлов вместо системного.

На этот каталог можно установить права доступа только для пользователей, работающих с данной настройкой. Это ограничит несанкционированный доступ к временным данным, которые могут содержать конфиденциальную информацию.

По умолчанию используется системный каталог. Обычно это "c:\Documents and Settings\<имя пользователя>\Local Settings\Temp\".

3) указать специальные **Каталоги для хранения входящих документов,** в которых будут храниться исходные документы, полученные в результате проведения операции Снятия и проверки электронной подписи.
4) указать специальные **Каталоги для хранения исходящих документов**;
5) настроить **Уровень безопасного удаления файлов**.

При обычном удалении с жесткого диска, файл помечается как удаленный, и занимаемое им место освобождается. Но при этом сами данные файла остаются на диске, и, в силу особенности строения файловых систем, эти данные еще можно извлечь с диска.

Чтобы избежать такого восстановления, перед удалением файл можно перезаписать случайными данными. Такой файл невозможно восстановить обычными программными средствами. Также можно сделать несколько проходов перезаписи, что значительно усложнит восстановление или сделает его невозможным даже специальными программными средствами

Настройка уровня безопасного удаления задает количество проходов перезаписи случайными данными, перед удалением временных файлов, созданных программой «КриптоАРМ» при операциях с подписанными и шифрованными данными.

Можно выбрать четыре уровня безопасного удаления:

- **Выключено** - перезапись случайными данными не будет производиться.
- **Низкий** - Перед удалением будет произведена однократная перезапись случайными данными.
- **Средний** - Перед удалением будет произведена семикратная перезапись случайными данными.
- **Высокий** - Перед удалением перезапись случайными данными будет произведена тридцать пять раз.

Скорость обработки файлов большого объема может уменьшиться при включении Высокого уровня удаления.

7.3 Операции с настройками

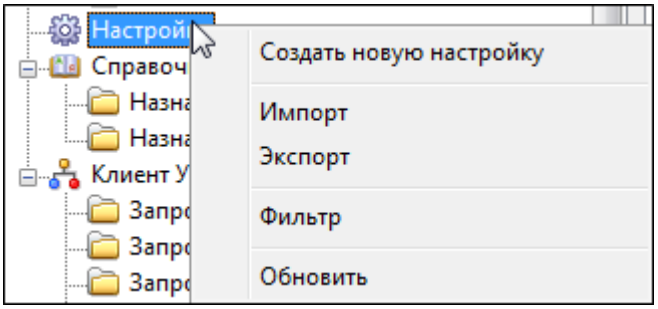
Доступны следующие операции с настройками:

- Создание настройки
- Переименование настройки
- Создание копии настройки
- Установка настройки по умолчанию
- Фильтрация настроек
- Сортировка настроек в списке
- Импорт настройки
- Экспорт настройки
- Удаление настройки

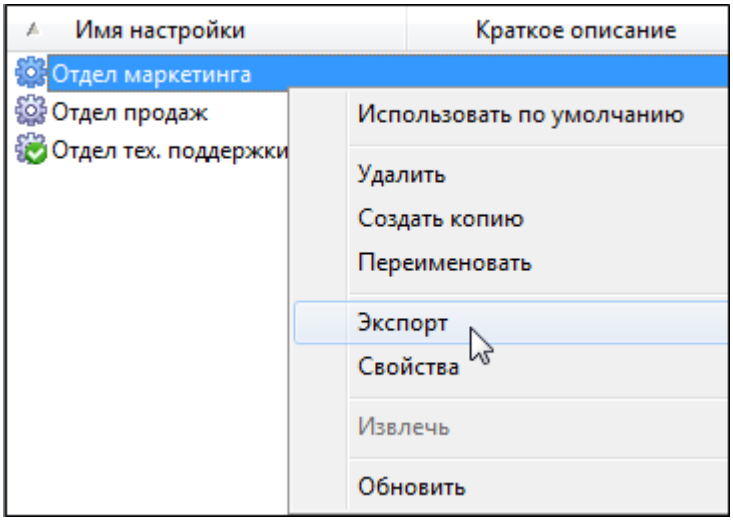
Операции с настройками вы можете выполнять через:

- Панель инструментов

- Контекстное меню раздела **Настойки**



- Контекстное меню объекта



7.3.1 Создание новой настройки

Для создания новой настройки выполнения операций:

2. В дереве элементов главного окна выберите раздел **Настройки** и вызовите его контекстное меню правой клавишей мыши. Выберите пункт **Создать новую настройку**.
3. Откроется окно **Параметры настройки.**

В создаваемой настройке вы можете установить следующие параметры:

- общие параметры (название, описание и т.п.)
- параметры подписи
- параметры шифрования
- параметры расшифрования
- параметры управления интерфейсом пользователя
- параметры использования политик сертификатов
- параметры верификации сертификатов
- параметры работы с TSP-службой (Службой штампов времени)
- параметры работы с OCSP-службой (Службой актуальных статусов)

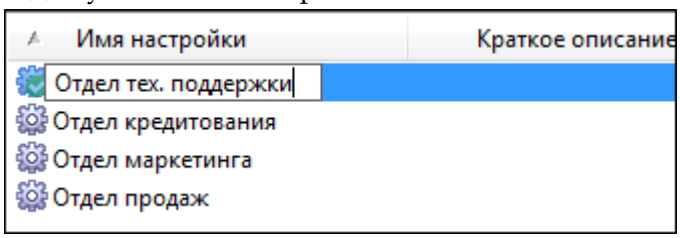
О том, как установить параметры настройки криптоопераций, читайте в главе Управление настройками приложения.

4. Сохраните указанные параметры настройки (кнопка **Применить**).
5. Созданная настройка отобразится в списке настроек.

7.3.2 Переименование настройки

Чтобы переименовать настройку:

1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта или на панели инструментов выберите пункт **Переименовать**.
2. Введите новое имя для указанной настройки:

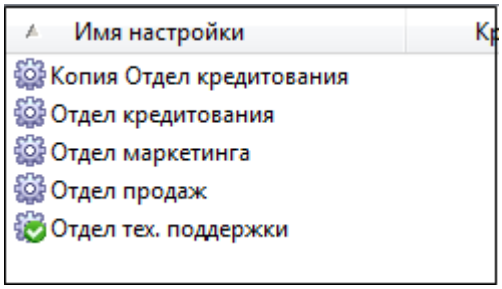


3. Настройка будет переименована.

7.3.3 Создание копии настройки

Чтобы создать копию существующей настройки:

1. В дереве элементов главного окна выберите раздел **Настройки.** В правой панели главного окна выберите настройку (или группу настроек), копию которой необходимо создать.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Создать копию.**
3. В списке настроек появится настройка "Копия (название копируемой настройки)".



7.3.4 Установка настройки по умолчанию

Вы можете установить одну из используемых вами настроек как "используемую по умолчанию" (она будет использоваться автоматически, когда не указана ни одна из настроек).

Для того чтобы установить настройку по умолчанию:

1. В дереве элементов главного окна выберите раздел **Настройки.** В контекстном меню объекта, который хотите использовать по умолчанию, или на панели инструментов выберите пункт **Использовать по умолчанию.**
2. При этом указанная настройка будет установлена как "Настройка по умолчанию".

Настройка, установленная по умолчанию, обозначается пиктограммой  .

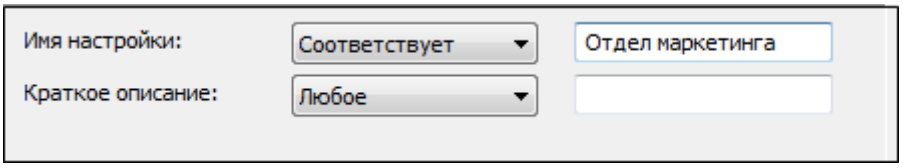
7.3.5 Фильтрация настроек

Вы можете фильтровать настройки в списке последующим параметрам:

- имя настройки
- краткое описание

Чтобы отфильтровать настройки:

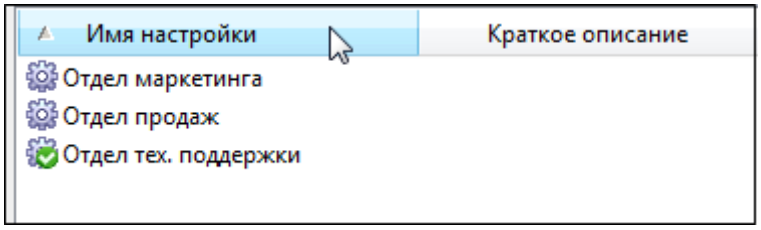
1. В разделе **Настройки** в контекстном меню выберите пункт **Фильтр**.
2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать настройки «КриптоАРМ»:



7.3.6 Сортировка настроек в списке

Вы можете сортировать настройки в списке по следующим параметрам:

- имя настройки
- краткое описание



7.3.7 Экспорт настройки

При обновлении или переустановке программы «КриптоАРМ» рекомендуется экспортировать используемые в работе настройки выполнения операций в XML-формат.

Чтобы экспортировать настройку в файл:

1. В правой панели главного окна, выберите настройку (или группу настроек), которые необходимо экспортировать, в контекстном меню объекта или на панели инструментов выберите пункт **Экспорт**.
2. В окне проводника введите имя экспортируемого файла с настройкой:
3. Указанная настройка будет экспортирована в файл в формате .xml.

При экспорте нескольких настроек, будет создаваться один .xml файл, содержащий все экспортируемые настройки.

7.3.8 Импорт настройки

При обновлении или переустановке программы «КриптоАРМ» вы можете импортировать ранее сохраненные в XML-формате настройки выполнения операций.

Чтобы импортировать файл с настройкой:

1. В дереве элементов главного окна выберите раздел **Настройки**. В контекстном меню раздела **Настройки** или на панели инструментов выберите пункт **Импорт**.
2. В окне проводника выберите файл с настройками в формате **.xml**
3. В раздел **Настройки** будет импортирована указанная настройка.

7.3.9 Удаление настройки

Для удаления настройки:

1. В правой панели главного окна, выберите настройку (или группу настроек), которую необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить**.
2. На запрос системы подтвердите свое решение.
3. Указанная настройка будет удалена из списка.

8 Работа с программой

8.1 Операции с сертификатами

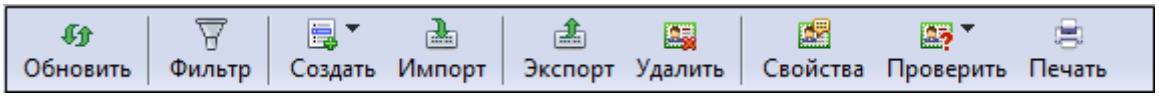
Цифровой сертификат представляет собой электронный документ, включающий открытый ключ и информацию о владельце данного ключа, заверенную Удостоверяющим Центром электронной подписью.

Вам доступны следующие операции с сертификатами:

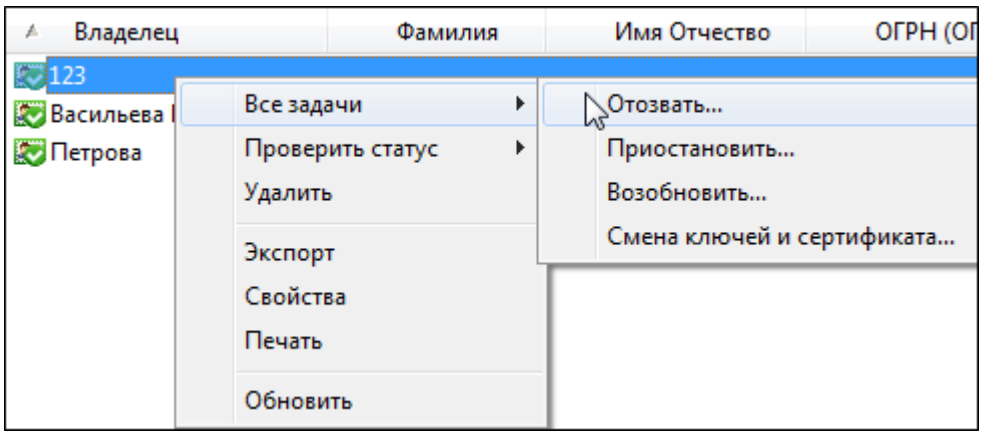
- Получение сертификата
- Создание самоподписанного сертификата
- Импорт сертификата
- Хранение сертификата
- Проверка статуса сертификата
- Просмотр информации о сертификате
- Фильтрация сертификатов
- Сортировка сертификатов
- Экспорт сертификатов
- Удаление сертификатов
- Печать сертификата

Операции с сертификатами можно выполнять через:

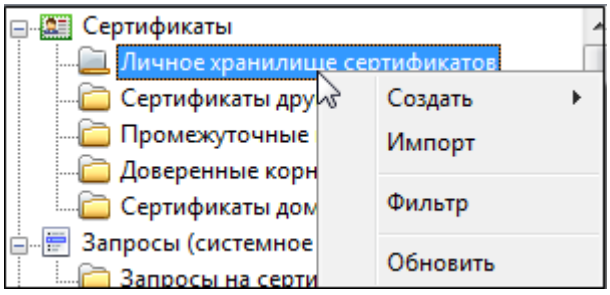
- панель инструментов



- контекстное меню сертификата



- контекстное меню раздела в главном окне программы



8.1.1 Получение нового сертификата

Получение нового сертификата выполняется в соответствии с регламентом работы, определенным Центром регистрации (плановая смена ключей и сертификатов) при внеплановой смене ключей и сертификатов (отзыв ранее действующего сертификата)

Получить новый сертификат вы можете на основании поданного в Удостоверяющий центр запроса на сертификат. В процессе создания запроса производится генерация ключей и запись их на ключевой носитель.

О том, как создать запрос на сертификат читайте в разделе Операции с запросами на сертификат.

Центр регистрации передает запрос на получение нового сертификата в Центр сертификации, где и происходит формирование сертификата. Выпущенный сертификат устанавливается пользователем в хранилище сертификатов своего рабочего места (на компьютер).

В процессе установки сертификата также автоматически производится его запись на ключевой носитель . В дальнейшем данный сертификат может быть повторно установлен на рабочее место пользователя (например, при потере сертификата в результате сбоя компьютера или операционной системы) или на другое рабочее место (в случае перехода пользователя на другое рабочее место). В этом случае сертификат с ключевого носителя устанавливается с помощью программы «КриптоАРМ».

8.1.2 Создание самоподписанного сертификата

Самоподписанный сертификат – сертификат, изданный самим пользователем, без обращения к доверенной стороне Удостоверяющему центру. Самоподписанный сертификат

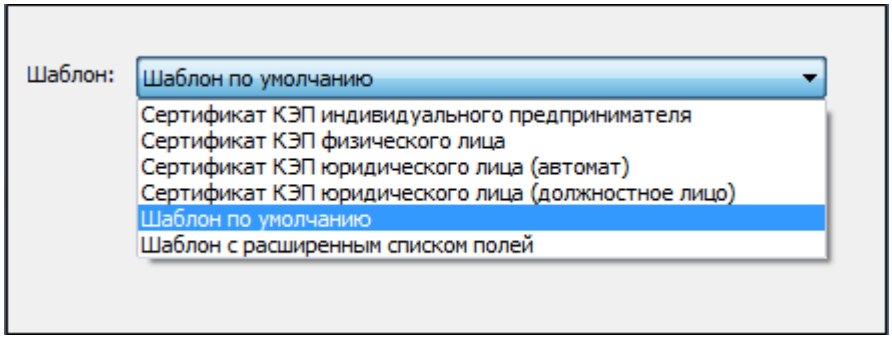
является одновременно личным и корневым (устанавливается в Личное хранилище сертификатов и «Доверенные корневые центры сертификации»).

Самоподписанные сертификаты используются для обмена зашифрованными или подписанными документами между людьми, доверяющими друг другу, например, друзьями, коллегами. Обменявшись такими сертификатами между собой, они могут пересылать друг другу подписанные и зашифрованные электронные данные, не беспокоясь при этом, что информация может быть перехвачена, искажена и использована против их интересов.

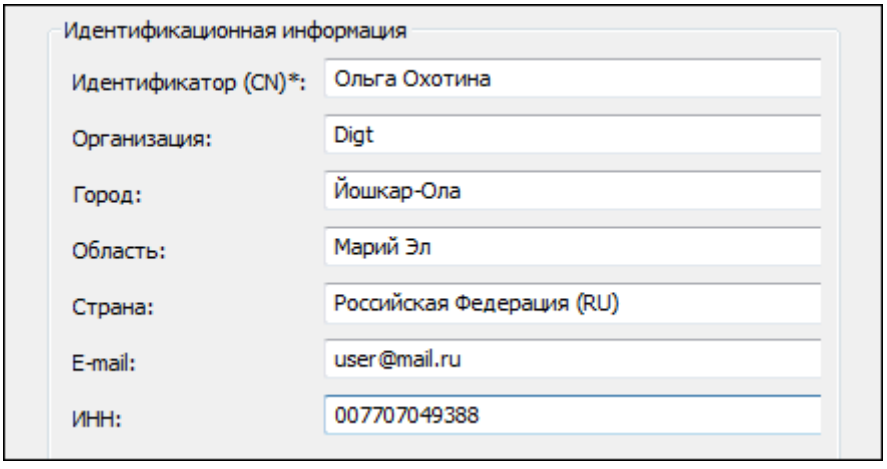
Важно помнить, что использование самоподписанных сертификатов не позволяет решать конфликтные ситуации, возникающие при обмене конфиденциальными данными, с помощью суда.

Для создания самоподписанного сертификата, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Сертификаты**. Вызовите правой клавишей мыши контекстное меню и выберите пункт **Создать > Самоподписанный сертификат**. Откроется Мастер создана самоподписанного сертификата.
2. На первом шаге ознакомьтесь с порядком и требованиями создания самоподписанного сертификата. Нажмите **Далее**.
3. На следующем шаге из выпадающего списка выберите шаблон сертификата:



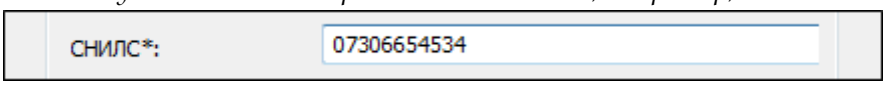
4. Укажите идентификационную информацию о владельце будущего сертификата, в зависимости от того, какой шаблон вы выбрали на предыдущем шаге.



Поля отмеченные знаком «» являются обязательными для заполнения.*

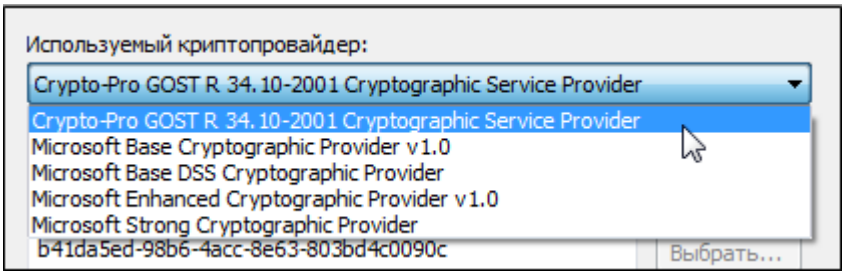
Обратите внимание, если вы указываете ИНН юридического лица, номер всегда должен начинаться с «00», например 007707049388.

СНИЛС указывается без пробелов и знаков «-», например, 07306654534.



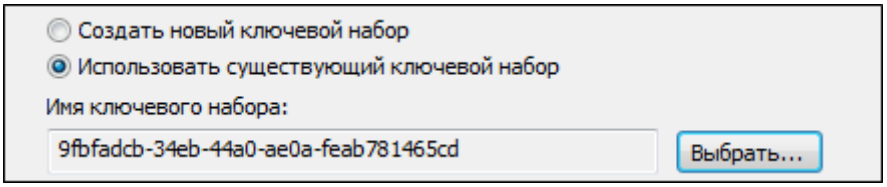
5. В открывшемся окне **Параметры ключа** в выпадающем списке выберите укажите следующие настройки:

1) **Используемый криптопровайдер.**

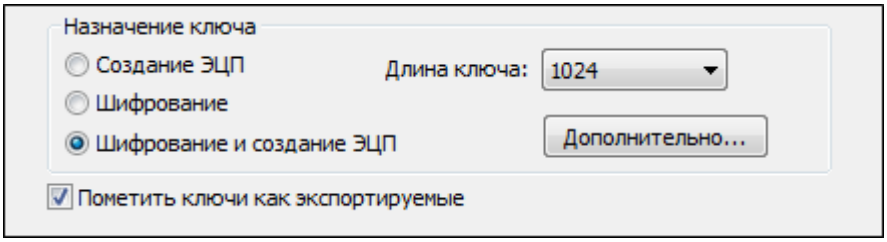


2) Выберите вариант создания ключевого набора.

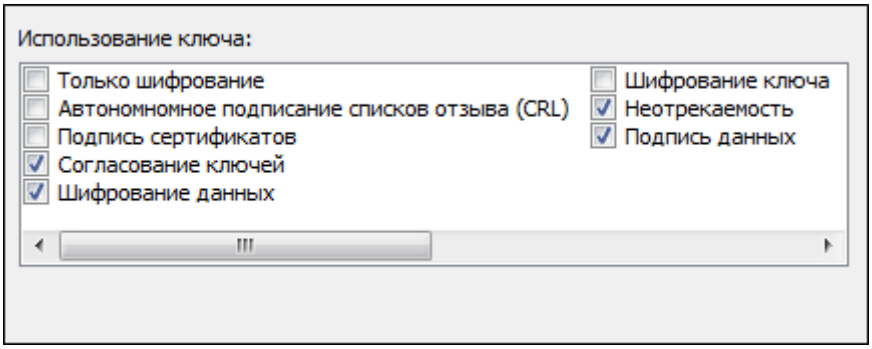
- **Создать ключевой набор** сертификат будет создан на основе нового ключевого набора.
- **Использовать существующий ключевой набор** – выберите ключевой набор, который будет использован при создании сертификата, из списка существующих (кнопка **Выбрать**).



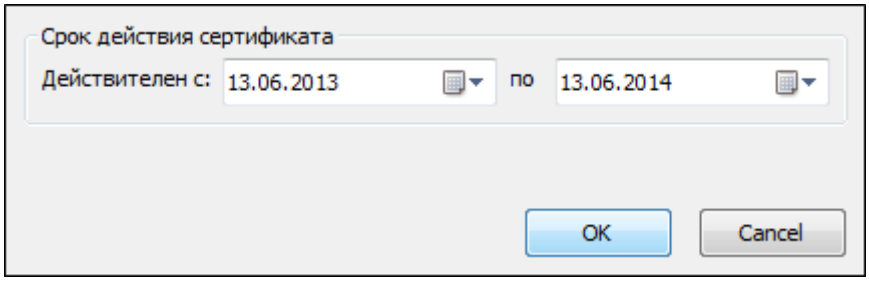
3) Установите переключатель напротив необходимого **Назначения ключа** сертификата.



4) Вы также можете выбрать дополнительное назначение ключа, нажав на кнопку **Дополнительно**. В списке назначений использования ключа выберите необходимое:



В разделе **Срок действия сертификата** автоматически проставляется дата, **с** которой сертификат действителен (текущее системное время) и дата, **по** которую сертификат действителен (1 год вперед от текущего времени). Эти даты вы можете отредактировать.

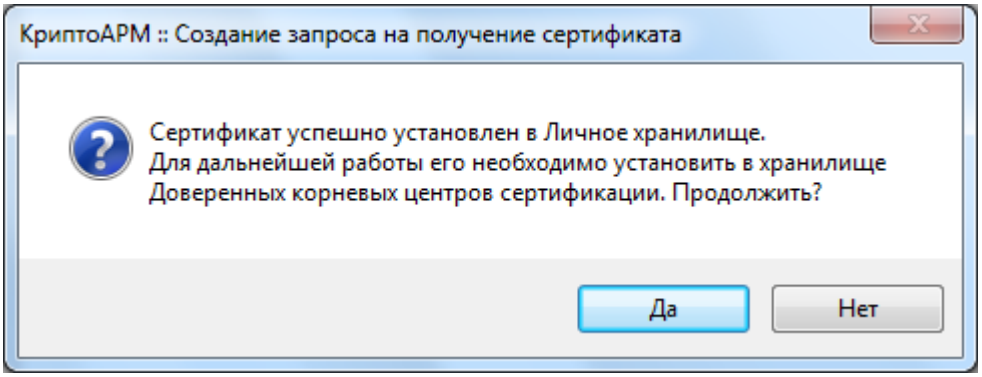


5) Укажите необходимую **Длину ключа**. Чем длиннее ключ, тем он надежнее.

6) **Пометить ключи как экспортируемые**.

Если вы отметите этот флаг, то сможете проводить экспорт сертификата вместе с закрытыми ключами

6. На основе указанных данных будет сформирован самоподписанный сертификат открытого ключа. После завершения операции возникнет окно с информацией о ее результатах. Нажмите **Готово**.
7. На запрос системы установите пароль на носитель и подтвердите его.
8. На запрос системы установить ли самоподписанный сертификат в хранилище Доверенных корневых центром сертификации, нажмите на кнопку **Да**.



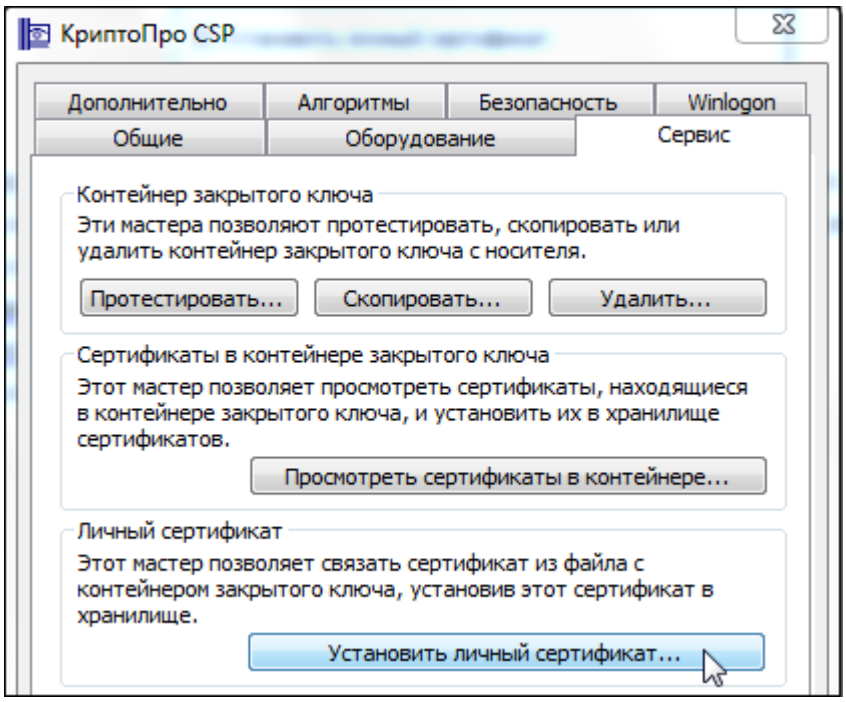
8.1.3 Импорт сертификата

Импорт сертификатов может понадобиться для выполнения следующих задач:

- Установка сертификата, который был отправлен вам в файле другим пользователем, компьютером или центром сертификации;
- Восстановление поврежденного или утерянного сертификата, заархивированного ранее;
- Установка сертификата и связанного с ним закрытого ключа с компьютера, на котором владелец сертификата его использовал ранее.

Первичная установка в хранилище личного сертификата ГОСТ может выполняться как средствами криптопровайдера «КриптоПро CSP», так и средствами программы «КриптоАРМ».

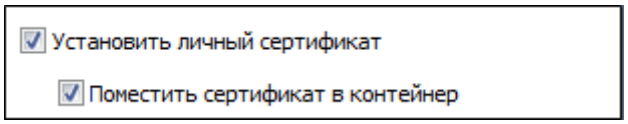
Установка личного сертификата средствами «КриптоПро CSP» осуществляется непосредственно в окне криптопровайдера «КриптоПро CSP», закладка Сервис.



Установка личного сертификата средствами программы «КриптоАРМ»

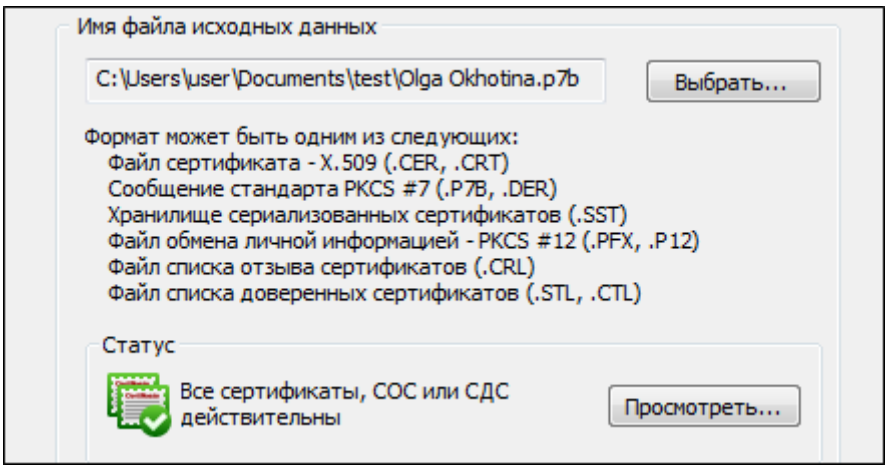
Чтобы установить сертификат с помощью «КриптоАРМ», выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Сертификаты.** Откроется список хранилищ сертификатов.
2. Выберите хранилище, куда необходимо импортировать сертификат, в контекстном меню раздела или на панели инструментов выберите пункт **Импорт**.
3. Откроется стандартный **Мастер установки сертификата**, позволяющий установить цифровой сертификат в хранилище для дальнейшего использования. Ознакомьтесь с порядком выполнения операции.
4. Если вы устанавливаете личный сертификат, в этом же окне установите флаг напротив строки **Установить личный сертификат**. Кроме того, вы можете установить флаг **Поместить сертификат в контейнер** (в этом случае в ключевом контейнере будет храниться не только ключевая пара, но и сам сертификат):

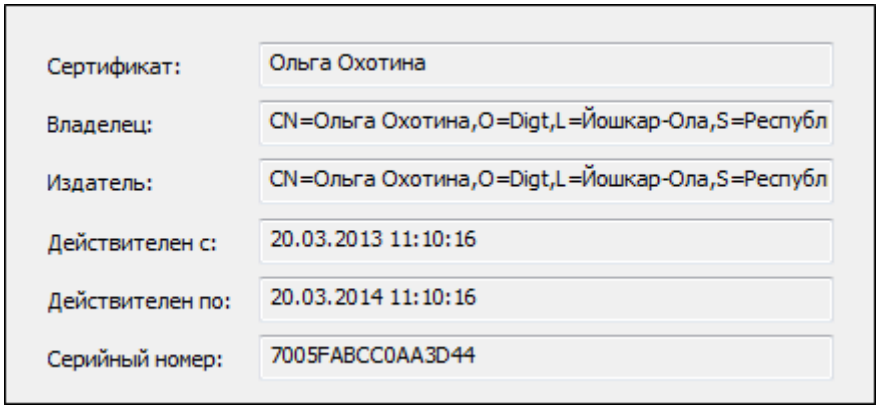


5. В следующем окне укажите файл, содержащий импортируемый сертификат. Система позволяет импортировать сертификаты следующих форматов:

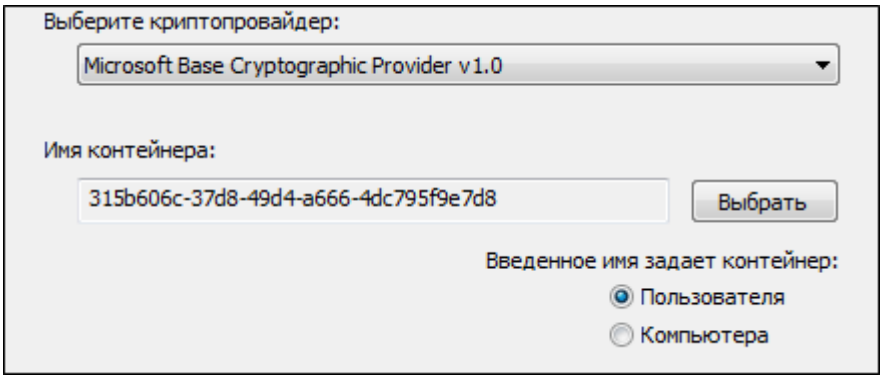
- Файл сертификата X.509 (.CER, CRT)
- Сообщение стандарта PKCS #7 (. P7B, .DER)
- Хранилище сериализованных сертификатов (.SST) – несколько сертификатов, объединенных в один файл.
- Файл обмена личной информацией – PKCS #12



6. Если вы устанавливаете личный сертификат, на следующем этапе откроется окно, содержащее информацию о нем (данные о владельце и издателе сертификата, срок действия и серийный номер):

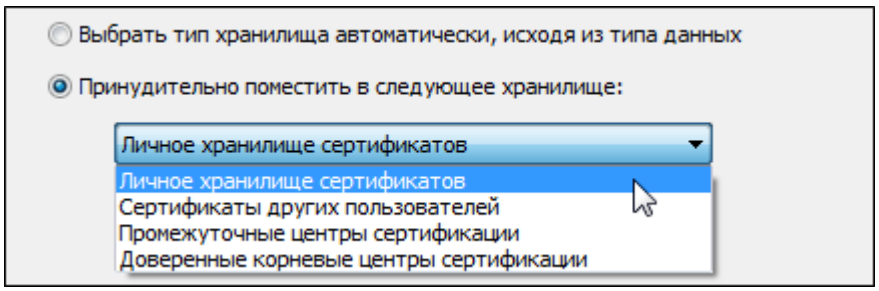


7. Если на первом этапе вы установили флаг **Поместить сертификат в контейнер**, откроется окно, в котором вам нужно
   5) Выбрать криптопровайдер;
   6) Выбрать из списка имя ключевого контейнера (перед этим вставьте ключевой носитель, на котором храниться данный контейнер);
   7) Укажите, что введенное имя задает контейнер пользователя.



8. Если на первом шаге вы не установили флаг **Установить личный сертификат,** то система вам предложит указать хранилище, в котором будет храниться импортируемый сертификат:

- Автоматический (тип хранилища выбирается системой);
- Для ручного выбора хранилища, в выпадающем меню выберите необходимое хранилище.



9. После завершения операции возникнет сообщение об успешном импорте сертификата.

8.1.4 Загрузка сертификатов из «КриптоПро УЦ»

Вы также можете загружать сертификаты, выдаваемые Удостоверяющим центром «КриптоПро УЦ».

Обязательным условием для получения сертификатов из «КриптоПро УЦ» является наличие

- у пользователя личного сертификата, выданного данным УЦ
- в корневом хранилище корневого сертификата данного УЦ
- в хранилище действующего СОС

Для загрузки сертификатов:

1. В верхнем меню главного окна выберите **Сервис>Загрузить сертификаты из КриптоПро УЦ**.
2. Откроется окно **Загрузка сертификатов из «КриптоПро УЦ»**, где вы можете настроить параметры доступа к службе «КриптоПро УЦ» и выбрать сертификат аутентификации пользователя для TLS соединения, а также настроить параметры прокси-сервера.
3. Откроется окно, в списке которого выберите сертификаты тех пользователей УЦ, с которыми планируете обмениваться электронными документами.
4. Далее откроется стандартный Мастер установки сертификатов в хранилище.

8.1.5 Хранение сертификатов

Программа «КриптоАРМ» в качестве хранилищ использует поддерживаемые криптопровайдером типы, а также стандартные хранилища сертификатов, входящих в операционную систему Windows.

Название хранилища сертификатов	Описание хранилища
Личное хранилище сертификатов	Личные сертификаты, используемые вами и связанные с вашими закрытыми ключами.
Сертификаты других пользователей	Сертификаты пользователей, с которыми вы обмениваетесь шифрованными или подписанными данными.
Промежуточные центры сертификации	Сертификаты промежуточных центров сертификации.

Доверенные корневые центры сертификации	Автоматически подписанные сертификаты от ЦС, которые неявным образом являются доверенными. Здесь хранятся сертификаты, изданные сторонними ЦС, Microsoft, а также вашей организацией (если организация располагает собственным сервером сертификатов). Хранилище также содержит самоподписанные сертификаты.
Доверенные издатели сертификатов	Сертификаты доверенных издателей сертификатов.

8.1.6 Проверка статуса сертификата

Использование сертификата можно условно разделить на два этапа

1) проверка статуса сертификата

2) если статус «действителен», использование сертификата для выполнения криптографических операций.

Каждый раз при обращении к сертификату программа «КриптоАРМ» проверяет его статус.

Существует **четыре типа проверки статуса сертификатов**:

1. По локальному списку отзыва сертификатов (COC)
2. По COC из Удостоверяющего центра
3. С использованием Revocation Provider
4. В OCSP службе
5. С помощью списка доверенных сертификатов

Типы проверки приведены по возрастанию значимости

Статус сертификата проверяется по следующим параметрам:

Параметры проверки	Пояснение
Проверка срока действия сертификата	Проверяется, истек или нет срок действия цифрового сертификата
Проверка корректности электронной подписи выдавшего сертификат Удостоверяющего центра	Для заверения вашего личного цифрового сертификата используется электронная подпись Удостоверяющего центра, в котором вы получили свой сертификат. Для того чтобы статус вашего сертификата был "Действителен", необходимо иметь установленный корневой сертификат и актуальный список отзыва сертификатов.
Построение цепочки (до корневого сертификата УЦ)	Доверие к личному сертификату пользователя определяется на основе цепочки сертификатов. Начальным элементом цепочки является корневой сертификат УЦ, хранящийся в хранилище **Доверенные корневые центры сертификации**.
Проверка действительности сертификата по спискам отзыва сертификатов	По умолчанию при работе с сертификатами в «КриптоАРМ» их статус проверяется по COC, установленному в хранилище **Промежуточные центры сертификации**. Но

	также возможно выполнить проверку сертификата по **СОС, полученному из УЦ**, или с помощью **Revocation Provider**.
С помощью списка доверенных сертификатов	Чтобы проверить статус сертификата с помощью списка доверенных сертификатов необходимо отметить "Использовать CTL для проверки пути сертификации" в настройках по умолчанию в разделе Параметры верификации сертификатов".

Статусы сертификатов
Возможны 3 статуса действительности сертификатов, выданных УЦ:

-  «действителен»
-  «недействителен»
-  «неизвестен»

Сертификат является действительным, если:

1. Подпись Удостоверяющего центра под сертификатом корректна.
2. Срок действия сертификата не истек.
3. Сертификат используется для тех целей, для которых был создан.
4. Сертификат не отозван и его действие не приостановлено.

Чтобы проверить статус сертификата:

1. В дереве элементов главного окна выберите раздел **Сертификаты.** Далее выберите нужное вам **хранилище**, в котором выберите сертификат для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус**

- По локальному списку отзыва сертификатов (списку, установленному в хранилище **Списки отзыва сертификатов**);
- По списку отзыва из Удостоверяющего центра (в онлайн-режиме по локальной сети);
- С использованием Revocation Provider;
- Проверить в OCSP службе.

При проверке статуса сертификата могут возникнуть следующие сообщения:

Сообщение	Пояснения
Истёк срок действия сертификата	Сертификат, которым подписаны данные, просрочен
Невозможно построить цепочку для сертификата	Невозможно построить цепочку сертификатов от клиентского сертификата до сертификата доверенного УЦ
Произошла ошибка при обновлении СОС	Настройки системы безопасности не предполагают обновлений СОС; библиотека CPCRLUpdate.dll отсутствует или не зарегистрирована

Произошла ошибка при открытии хранилища	Нет прав доступа к хранилищу сертификатов
COC найден, однако возник сбой при его обработке	COC хранится в неизвестном формате
COC найден, однако он нуждается в обновлении	Дата обновления COC истекла, необходимо обновить COC в УЦ, для того чтобы сертификат был действительным
Ошибка при сопоставлении COC и сертификата	Ошибка в процессе поиска клиентского сертификата в последнем выпущенным УЦ COC
Сертификат содержится в COC	Сертификат недействителен (отозван в УЦ по какой-либо причине и занесен в COC)

Для того чтобы упростить процедуру проверки статуса сертификата, вы можете в настройках выполнения операций указать параметры проверки (верификации) сертификатов. Для выбранных сертификатов в процессе работы всегда автоматически будет использоваться указанный вами способ проверки.

Проверка статуса сертификата по локальному COC

«КриптоАРМ» поддерживает способ проверки статуса цифрового сертификата по локальному списку отзыва сертификатов (COC), периодически обновляемого Удостоверяющим центром согласно Регламенту данного УЦ.

Чтобы проверить статус сертификата, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Сертификаты -** нужное вам **хранилище**, в котором выберите сертификат (или группу сертификатов) для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус> по локальному COC**.

Статусы сертификатов

Статус	Пояснение
«действителен»	Выполняются все условия действительности сертификата
«недействителен»	• Срок действия сертификата истек • Есть непросроченный COC и в нем находится указанный сертификат • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП • Не удалось получить COC из УЦ (если выполняется обязательная проверка по COC, полученному из УЦ)
«неизвестен»	Статус, возможный только для сертификатов, которым не требуется проверка по COC, полученному из УЦ • отсутствует COC • COC просрочен

Возможные ошибки обновления COC

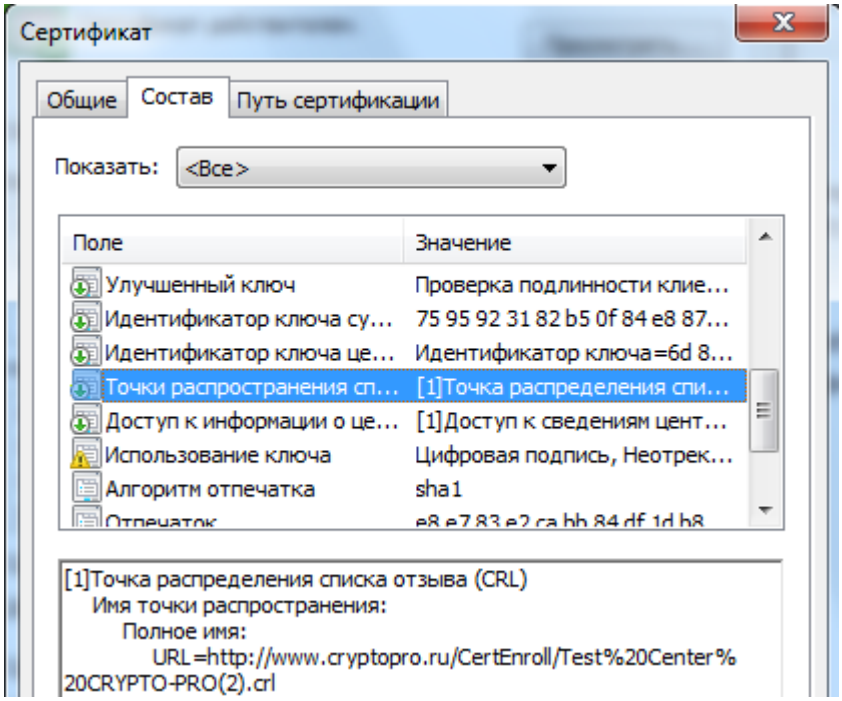
Ошибка	Объяснение
0x80092004 (Cannot find object or property.)	1. Не найден издатель проверяемого сертификата. 2. Файл COC не соответствует проверяемому сертификату.
0x80092007 (The specified certificate is self signed.)	Проверяемый сертификат - самоподписанный. Нет смысла проверять самоподписанный сертификат по COC, т.к. COC подписывается тем же самым самоподписанным сертификатом.

Проверка статуса сертификата по COC из УЦ

«КриптоАРМ» позволяет проверять статус цифрового сертификата в режиме получения (и их участия в процедурах проверок) COC в онлайн-режиме из CDP и/или сетевого справочника системы.

Для использования возможности получения COC из УЦ необходимо соблюдение следующих условий:

1. В проверяемом сертификате должно присутствовать расширение «**Точка распространения COC / CRL Distribution Point (CDP)**». При этом если значений (URL'ов) в расширении несколько, то программа «КриптоАРМ» будет пытаться скачать COC по всем адресам до первого успешного скачивания. Поддерживаются часто используемые протоколы - "ftp", "http" и "file".



2. По одной из точек распространения COC (оптимально, если по первой) можно скачать COC с помощью веб-браузера, например Microsoft Internet Explorer. При этом, не вводя никакой дополнительной информации (имени пользователя, пароля, перехода по ссылкам).

Протестировать можно следующим образом:

- закрыть все окна Internet Explorer (т.к. они могут хранить параметры доступа к серверу);
- запустить Internet Explorer и вставить в поле адреса URL из точки распространения COC (например, для сертификата тестового УЦ «КриптоПро» - http://www.cryptopro.ru/CertEnroll/Test%20Center%20CRYPTO-PRO.crl);

- нажать Enter, после чего Internet Explorer должен сразу предложить сохранить скачанный файл COC;
- сохранить COC в файл и открыть его проводником Windows (должна без ошибок открыться форма просмотра COC).

Чтобы проверить статус сертификата:

1. В дереве элементов главного окна выберите раздел **Сертификаты -** нужное вам хранилище, в котором выберите сертификат (или группу сертификатов) для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус> по COC из УЦ**.

Статусы сертификатов

Статус	Пояснение
«действителен»	Выполняются все условия действительности сертификата
«недействителен»	• Срок действия сертификата истек • Есть непросроченный COC и в нем находится указанный сертификат • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП
«неизвестен»	Статус, возможный только для сертификатов, которым не требуется проверка по COC, полученному из УЦ • отсутствует COC • COC просрочен • не удалось получить COC из УЦ

Возможные ошибки обновления COC

Ошибка	Объяснение
0x800C0005	Ошибка скачивания COC по сети, например, файл не найден или нет доступа.
0x80092004 (Cannot find object or property.)	1. Не найден издатель проверяемого сертификата. 2. Файл COC не соответствует проверяемому сертификату.
0x80092007 (The specified certificate is self-signed.)	Проверяемый сертификат - самоподписанный. Нет смысла проверять самоподписанный сертификат по COC, т.к. COC подписывается тем же самым самоподписанным сертификатом

Проверка статуса сертификата с помощью Revocation Provider

При работе с сертификатами в «КриптоАРМ» их статус можно проверить с помощью **Revocation Provider** (если на компьютере пользователя установлен «КриптоПро Revocation Provider»).

Чтобы проверить статус сертификата:

1. В дереве элементов главного окна выберите раздел **Сертификаты -** нужное вам хранилище, в котором выберите сертификат (или группу сертификатов) для проверки.

2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус > с использованием Revocation Provider.**

Статус	Пояснение
«действителен»	Выполняются все условия действительности сертификата
«недействителен»	• Срок действия сертификата истек • Из OCSP Службы получен ответ "Сертификат отозван" или сертификат включен в список отзыва, опубликованный УЦ (в зависимости от типа Revocation Provider: Microsoft или «КриптоПро») • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП
«неизвестен»	Статус, возможный только для сертификатов, которым не требуется проверка по СОС, полученному из УЦ • отсутствует СОС • СОС просрочен • не удалось получить СОС из УЦ

Проверка статуса сертификата в OCSP службе

«КриптоАРМ» поддерживает способ проверки статуса цифрового сертификата в OCSP службе (при установленной лицензии на модуль OCSP). При проверке статуса сертификата по OCSP формируется запрос в службу OCSP и его отправка по адресу, прописанному в сертификате или указанному в настройках групповых политик.

Если сертификат не имеет атрибута, содержащего адрес службы OCSP, то параметры доступа к службе берутся из текущей установленной по умолчанию настройке.

Если сертификат содержит адрес службы или несколько адресов, то параметры доступа в службу (такие как настройки прокси-сервера или сертификат аутентификации) берутся из OCSP профиля. При этом программа будет повторно пытаться получить OCSP ответ для каждого адреса OCSP до тех пор, пока не будет получен ответ со статусом (сертификат действителен или сертификат недействителен).

Если ни по одному из адресов, указанных в сертификате, не был получен ответ со статусом сертификата, то проверяется статус сертификата в службе, адрес которой указан в настройке.

Чтобы проверить статус сертификата:

1. В дереве элементов главного окна выберите раздел **Сертификаты -** нужное вам хранилище, в котором выберите сертификат (или группу сертификатов)для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус> В службе OCSP**

Статус	Пояснение
«действителен»	Выполняются все условия действительности сертификата

«недействителен»	• Срок действия сертификата истек • Из OCSP Службы получен ответ "Сертификат отозван" • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП
«неизвестен»	Ошибка доступа к службе OCSP

Проверка сертификата с помощью списка доверенных сертификатов

Чтобы проверить статус сертификата:

1. Необходимо отметить "Использовать CTL для проверки пути сертификации" в настройке верификации сертификатов.

2. После произведенных действий все сертификаты, корневой сертификат которых не включен в список доверенных сертификатов, станут недействительными.

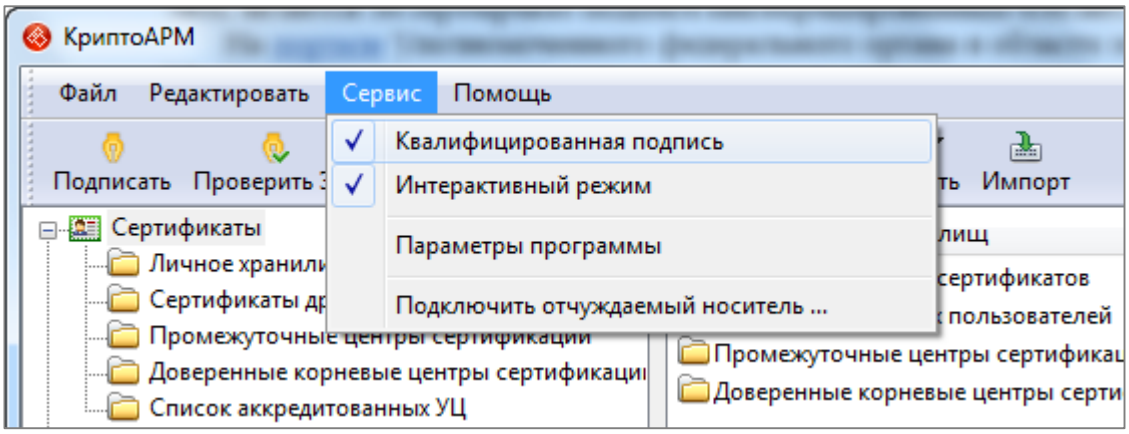
Статус	Пояснение
«действителен»	Выполняются все условия действительности сертификата
«недействителен»	• Срок действия сертификата истек • Есть непросроченный COC, и в нем находится указанный сертификат • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП • Не удалось получить COC из УЦ (если выполняется обязательная проверка по COC, полученному из УЦ)
«неизвестен»	Ошибка доступа к службе OCSP

8.1.7 Работа с квалифицированными сертификатами

Для многих сегодня становится проблемой гарантировать, что получаемые электронные документы подписаны действительно квалифицированной электронной подписью. Для решения этой задачи мы ввели технологию, которая позволяет с точностью определять, является ли сертификат подписи квалифицированным или нет.

Режим «Квалифицированная подпись»

Для работы только с квалифицированными сертификатами вам достаточно включить в программе «КриптоАРМ» режим «Квалифицированная подпись». Для этого в верхнем меню главного окна откройте **Сервис** и установите флаг напротив строки **Квалифицированная подпись.**

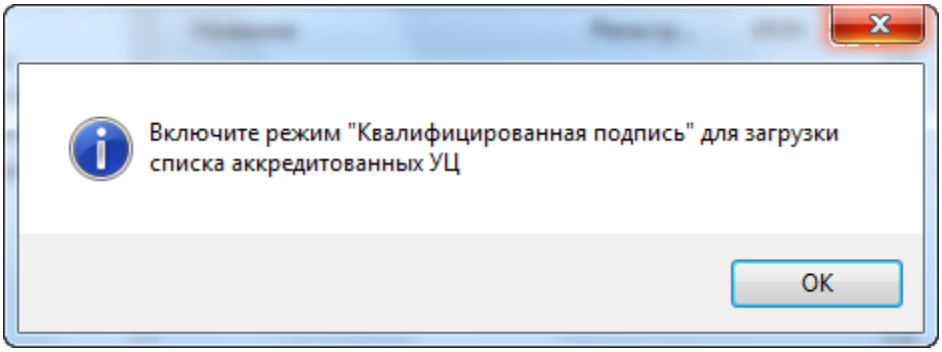


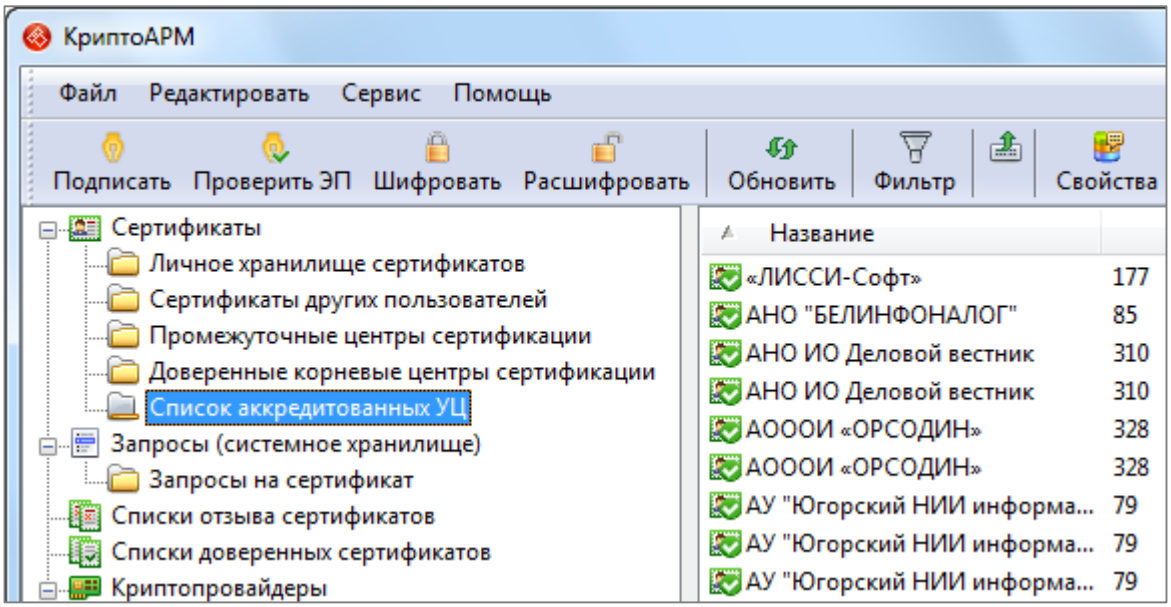
При включенном режиме **Квалифицированная подпись** вам станут доступны только сертификаты, которые выданы аккредитованными удостоверяющими центрами и соответствуют требованиям к форме квалифицированного сертификата. То есть только квалифицированные сертификаты ключа проверки электронной подписи. Все остальные сертификаты скрываются. Проверка сертификатов, которыми подписаны электронные документы, выполняется также при включенном режиме.

Просмотр списка аккредитованных удостоверяющих центров

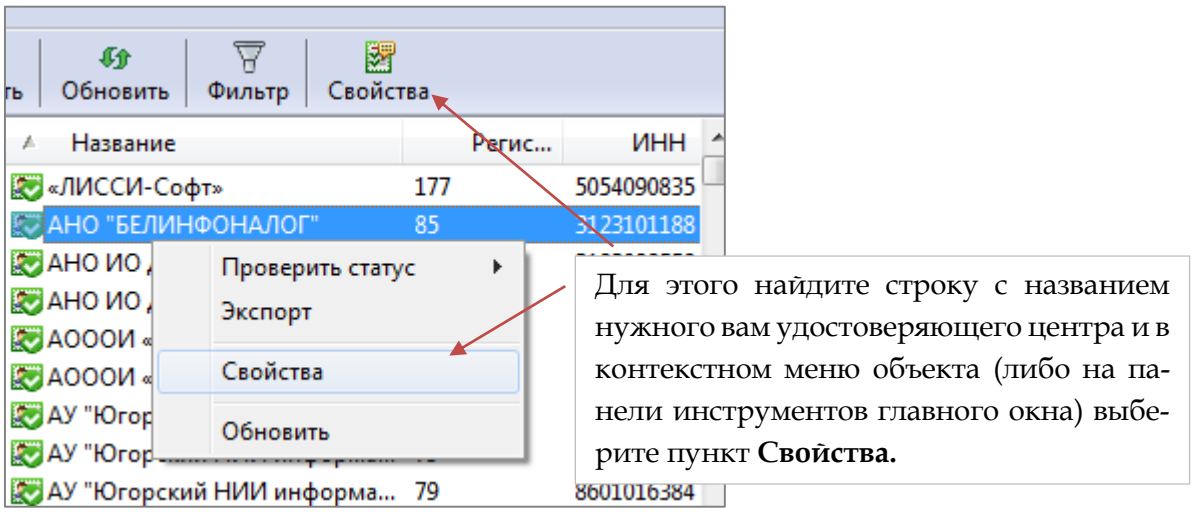
На портале Уполномоченного федерального органа в области электронной подписи Минкомсвязи размещается актуальный список аккредитованных удостоверяющих центров. Именно этот список используется программой «КриптоАРМ» в качестве фильтра при работе с электронной подписью. Список отображается в отдельной папке **Список аккредитованных УЦ.**

Чтобы загрузить актуальный список аккредитованных УЦ, предварительно включите режим «Квалифицированная подпись» (Сервис > Квалифицированная подпись)



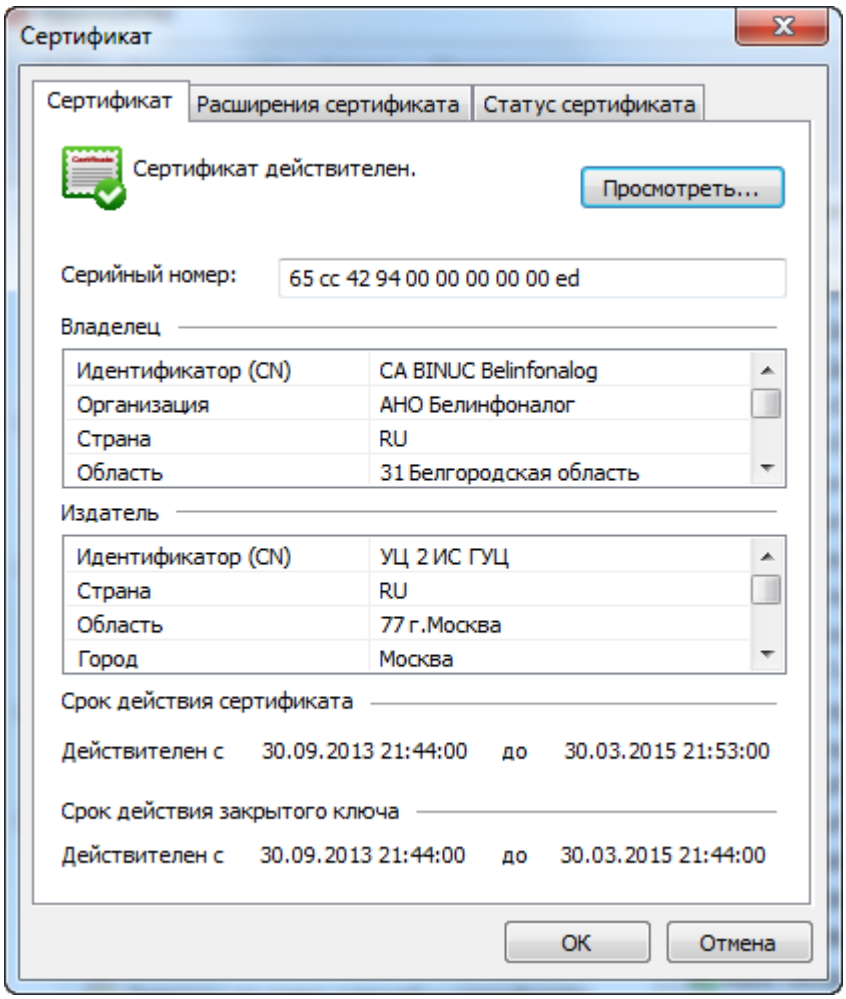


Вы можете просмотреть подробную информацию о корневом сертификате каждого удостоверяющего центра в списке.



Откроется окно **Сертификат**, в котором вы можете узнать подробную информацию о сертификате:

- серийный номер, владелец, издатель, срок действия сертификата и закрытого ключа (закладка **Сертификат**),
- расширения сертификата: использование ключа, политики сертификата и др. (закладка **Расширения сертификата**),
- общий статус проверки полного пути сертификации (закладка **Статус сертификата**)



8.1.8 Просмотр информации о сертификате

Для просмотра информации о сертификате выполните следующие шаги:

1. Выберите необходимый из списка и дважды щелкните по нему мышью, либо вызовите правой клавишей мыши контекстное меню и выберите пункт **Свойства**.
2. Откроется окно **Сертификат** для просмотра подробной информации о сертификате. В окне сертификат вам будут доступны 3 закладки:
   1) Сертификат;
   2) Расширения сертификата;
   3) Статус сертификата.
3. В закладке **Сертификат** доступна следующая информация:
   - Статус сертификата;
   - Серийный номер сертификата;
   - Сведения о владельце сертификата;
   - Сведения об издателе сертификата;
   - Срок действия сертификата (с какого и до какого периода действителен сертификат).
4. В закладке **Расширения сертификата** доступна следующая информация**:**
   - Варианты использования ключа;
   - Средство ЭП владельца;

- Политики сертификата;
- Средства ЭП и УЦ издателя.

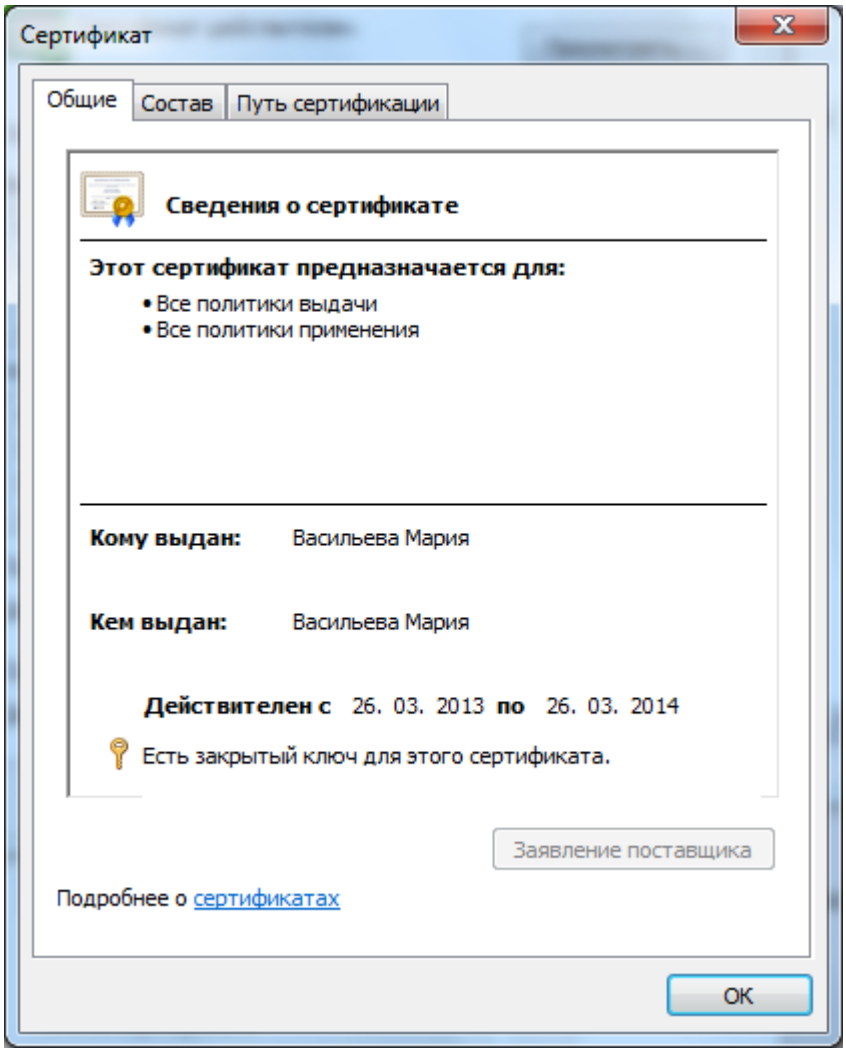
5. В закладке **Статус сертификата** отображен общий статус проверки полного пути сертификации. В этой закладке вы можете проверять статус сертификата.

Информацию о сертификате вы также можете просмотреть через стандартное окно просмотра свойств сертификата Windows. Для этого в окне просмотра информации о сертификате в закладке **Сертификат** нажмите на кнопку **Сертификат**, либо в закладке **Статус сертификата > Просмотреть**.

Откроется стандартное окно просмотра свойств сертификата Windows.

Окно содержит три закладки:

- Общие
- Состав
- Путь сертификации



1. В закладке **Общие** дается базовая информация о сертификате.
2. В закладке **Состав** даны более подробные сведения о сертификате: представлен перечень атрибутов сертификата и их значения.

В таблице перечислены основные сведения о составе сертификата:

Сведения о сертификате	Поля	Значения полей

Поля V1	Версия	Номер версии протокола X.509
	Серийный номер	Уникальный серийный номер, присвоенный сертификату центром сертификации. Серийный номер уникален для всех сертификатов, выданных определенным центром сертификации
	Алгоритм подписи	Алгоритм хеширования, который центр сертификации использует для электронной подписи сертификата
	Издатель	Сведения о центре сертификации, выдавшем данный сертификат
	Действителен с	Начальная дата срока действия сертификата
	Действителен по	Конечная дата срока действия сертификата
	Субъект	Имя лица или центра сертификации, которым выдан сертификат. Если центр сертификации находится на сервере члена домена организации, это будет отличительное имя в организации. В ином случае это может быть полное имя и адрес электронной почты или другой идентификатор.
	Открытый ключ	Длина и тип открытого ключа, связанного с сертификатом
Расширения	Улучшенный ключ	Назначения, для которых сертификат может быть использован
	Идентификатор ключа субъекта	Обеспечивает идентификацию сертификатов, включающих конкретный открытый ключ
	Идентификатор ключа центра сертификатов	Обеспечивает идентификацию открытого ключа, связанного с закрытым ключом, который используется для подписи Удостоверяющим центром сертификата
	Точки распространения списка отзыва сертификата (COC)	«КриптоАРМ» позволяет проверять статус цифрового сертификата в режиме получения COC в онлайн-режиме из CDP. Для того чтобы проверять статус сертификата подобным образом, в сертификате должно присутствовать расширение «Точка распространения COC / CRL Distribution Point (CDP)». При этом если значений (URL'ов) в расширении несколько, то программа «КриптоАРМ» будет пытаться скачать COC по всем адресам до первого успешного скачивания. Поддерживаются часто используемые протоколы: "ftp", "http" и "file"
	Доступ к информации о центрах сертификации	Предоставляет информацию о ЦС, которым выдан просматриваемый сертификат: 1. Поле содержит информацию о списке корневых сертификатов Центра сертификации (URL)

		2. Адреса OCSP Служб
	Использование ключа	Варианты использования закрытого ключа (например, Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных и др.)
Критические расширения	Использование ключа	Варианты использования закрытого ключа
Свойства	Алгоритм отпечатка	Алгоритм хеширования, который генерирует сводку данных (или отпечаток) для электронных подписей
	Отпечаток	Сводка данных (или отпечаток) для электронных подписей

3. В закладке **Путь сертификации** отображается место сертификата в **цепочке доверия** (или сертификационный путь) - от корневого сертификата Удостоверяющего центра до просматриваемого сертификата.
   Удостоверяющим центрам, сертификаты которых хранятся в хранилище доверенных корневых центров сертификации, оказывается по умолчанию большое доверие. Это позволяет всем выпущенным ими сертификатам наследовать доверие от ЦС. Если в сертификационном пути присутствует только один сертификат, то такие сертификаты называются **самоподписанными**. Все корневые ЦС имеют такие сертификаты.
4. В нижней части окна отображается информация о владельце сертификата, статусе сертификата и подробности о статусе.

Информация о сертификате также доступна в финальном окне всех криптографических операций.

8.1.9 Фильтрация сертификатов

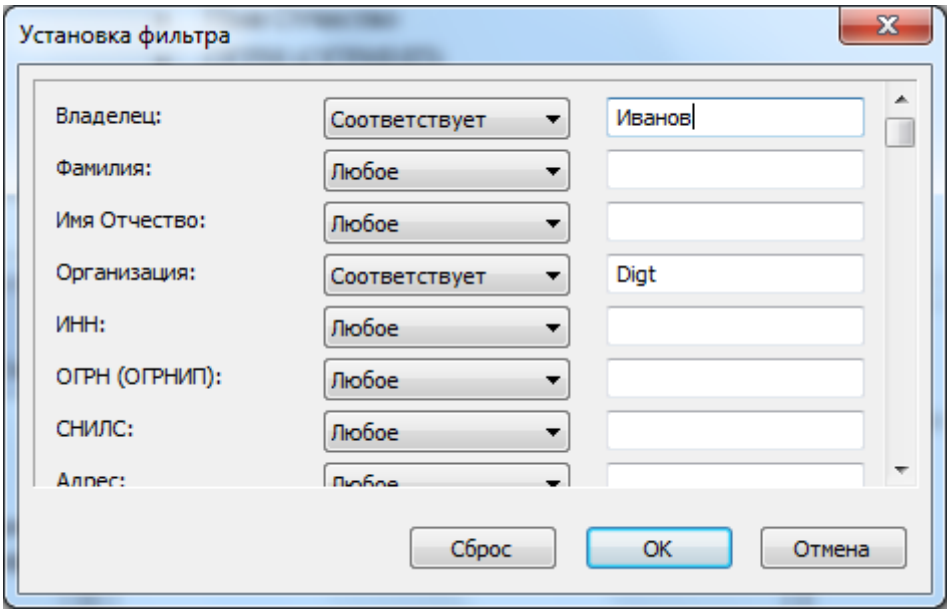
Вы можете фильтровать сертификаты в списке по следующим параметрам:

- Владелец
- ФИО
- Организация
- ОГРН (ОГРНИП)
- СНИЛС
- Адрес
- Электронная почта
- Серийный номер
- Издатель
- Дата, с которой сертификат действителен
- Дата, по которую сертификат действителен.

Для того чтобы отфильтровать сертификаты в списке:

1. В разделе **Сертификаты** выберите папку с тем типом сертификатов, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.

2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать сертификаты:

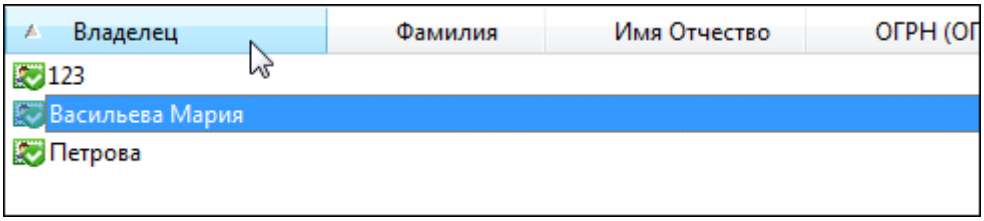


8.1.10 Сортировка сертификатов в списке

В программе «КриптоАРМ» реализована возможность сортировать цифровые сертификаты в списке.

Сортировка может выполняться по следующим параметрам:

- Владелец
- Фамилия
- Имя Отчество
- ОГРН (ОГРНИП)
- СНИЛС
- Адрес
- Издатель



8.1.11 Печать сертификата

Для печати сертификата выполните следующие шаги:

1. Откройте хранилище сертификатов, выберите необходимый сертификат (или группу сертификатов), в контекстном меню объекта или на панели инструментов выберите пункт **Печать.**
2. В новом окне браузера Microsoft Internet Explorer будет сформирована печатная форма сертификата.
3. Для вывода на печать формы сертификата на панели инструментов браузера нажмите на кнопку **Печать.**

8.1.12 Экспорт сертификата

Программа «КриптоАРМ» позволяет экспортировать сертификат из хранилища в файл.

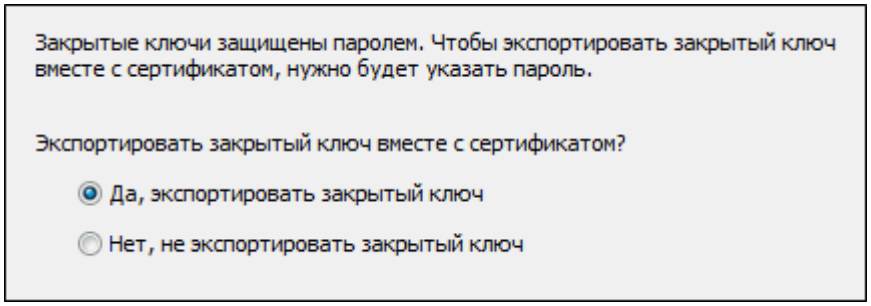
Экспорт сертификата может понадобиться для выполнения следующих задач:

- Архивирование сертификата;
- Архивирование сертификата и связанного с ним закрытого ключа;
- Копирование сертификата для использования на другом компьютере;
- Удаление сертификата и его закрытого ключа с компьютера владельца сертификата для установки на другом компьютере.

Когда сертификат экспортируется, он копируется из хранилища сертификатов в файл, использующий стандартный формат хранения сертификатов.

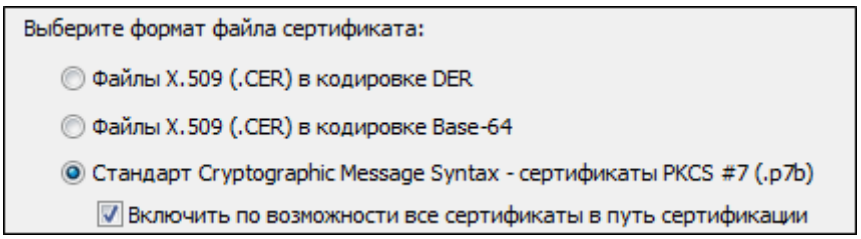
Для экспорта сертификата, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Сертификаты.** Откроется список хранилищ сертификатов. Выберите хранилище, в котором содержится сертификат для экспортирования.
2. В правой панели главного окна выделите с сертификат (или группу сертификатов), который необходимо экспортировать, в контекстном меню объекта или на панели задач выберите пункт **Экспорт**.
   Если экспортируемый сертификат – ГОСТ, введите пароль для доступа к ключевому контейнеру.
3. Откроется стандартный диалог **Мастер экспорта сертификатов**. Ознакомьтесь с порядком экспорта сертификатов и нажмите на кнопку **Далее**.
4. Вы можете экспортировать закрытый ключ вместе с сертификатом. Для этого поставьте переключатель напротив пункта **Да, экспортировать закрытый ключ**. В случае выбора пункта **Нет, не экспортировать закрытый ключ** будет произведена операция экспорта только сертификата (и его открытого ключа).



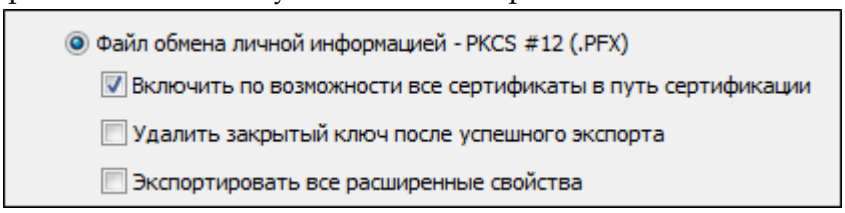
   Если при создании запроса на сертификат вы не пометили ключи как "экспортируемые", то вы сможете экспортировать сертификат (без закрытого ключа). В этом случае переключатель **Да, экспортировать закрытый ключ** будет заблокирован.
5. Если вы экспортируете только сертификат (без закрытого ключа), то в следующем окне выберите следующие форматы экспортируемого файла:

- Файлы в DER-кодировке X.509 (.CER)
- Файлы в Base64-кодировке X.509 (.CER)
- Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)



6. Если вы экспортируете сертификат с закрытым ключом, то вам будет доступен только один формат экспортируемого файла - файл обмена личной информацией - PKCS#12 (.PFX). При этом вы имеете возможность:

- включить по возможности все сертификаты в путь сертификата;
- включить усиленную защиту (требуется IE 5.0, NT 4.0 SP4 или выше);
- удалить закрытый ключ после успешного экспорта.



7. Для обеспечения безопасности следует защитить закрытый ключ паролем.
8. Укажите имя экспортируемого файла и путь экспорта.
9. По окончании операции возникнет сообщение об успешном экспорте сертификата.

8.1.13 Удаление сертификата

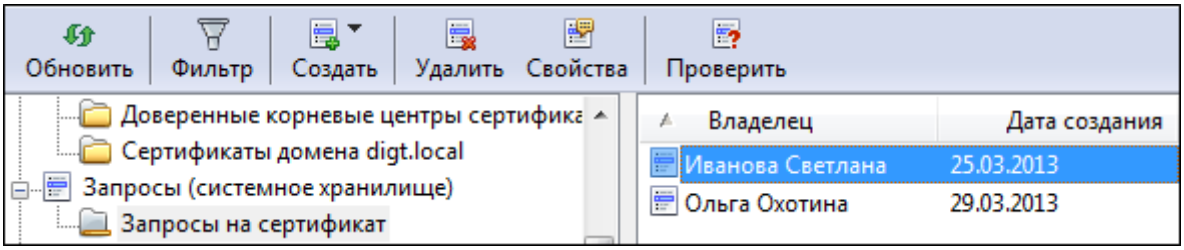
Чтобы удалить сертификат:

1. В дереве элементов главного окна выберите раздел **Сертификаты.** Откроется список хранилищ сертификатов.
2. Выберите хранилище, из которого необходимо удалить сертификат.
3. В правой панели главного окна выделите строку с сертификатом (или группу сертификатов), который необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить.**
4. Подтвердите решение удалить сертификат.
5. Сертификат будет успешно удален из хранилища.

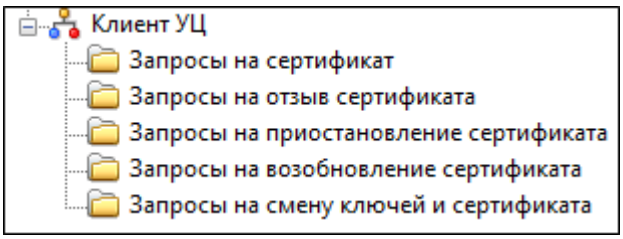
8.2 Операции с запросами на сертификат

Запрос в Удостоверяющий центр - это сообщение, содержащее необходимую информацию для выполнения регламентных процедур над сертификатом (выпуск и отзыв сертификата, приостановление и возобновление его действия, обновление сертификата или ключа).

- запросами на сертификат;



- всеми типами PKI-запросов(в разделе **Клиент УЦ**).

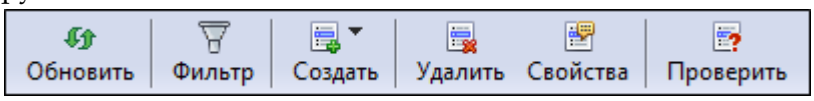


Доступны следующие операции с запросами:

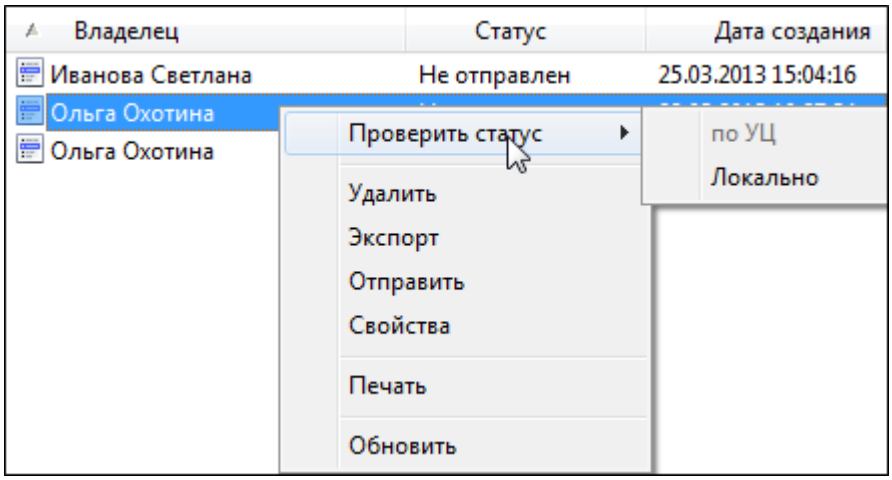
- Создание запроса
- Передача запроса в УЦ на рассмотрение
- Проверка статуса обработки запроса
- Просмотр информации о запросе
- Фильтрация запросов
- Сортировка запросов
- Печать запроса
- Удаление запроса

Эти операции можно выполнять через:

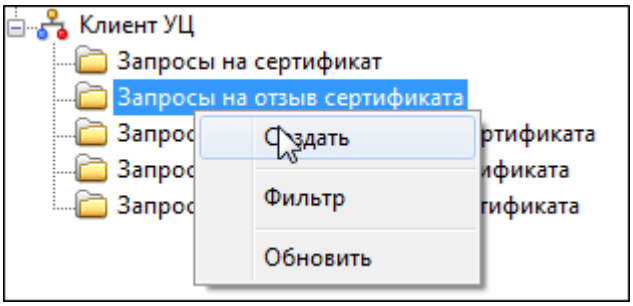
- панель инструментов



- контекстное меню объекта



- контекстное меню раздела



8.2.1 Создание запроса

С помощью программы «КриптоАРМ» вы можете создавать запросы следующих типов:

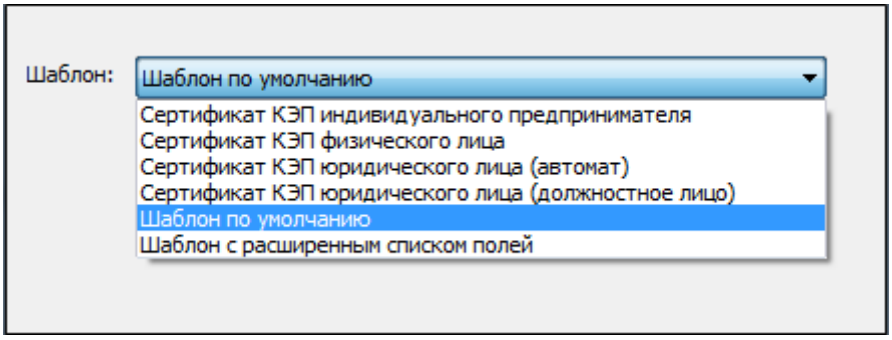
- запрос на получение сертификата
- запрос на приостановление действия сертификата
- запрос на возобновление действия сертификата
- запрос на отзыв сертификата
- запрос на смену ключей и сертификата

Запрос на получение сертификата

Для того чтобы получить личный цифровой сертификат для выполнения криптографических операций, необходимо создать запрос на сертификат и направить его на рассмотрение в Удостоверяющий центр (УЦ).

Для создания запроса на получение сертификата в УЦ:

1. В дереве элементов главного окна выберите раздел **Запросы**. Вызовите правой клавишей мыши контекстное меню и выберите пункт **Создать > Запрос на сертификат**.
2. Откроется стандартный Мастер создания запроса. Ознакомьтесь с порядком и требованиями создания запроса на получение сертификата.
3. На следующем шаге из выпадающего списка выберите шаблон сертификата:



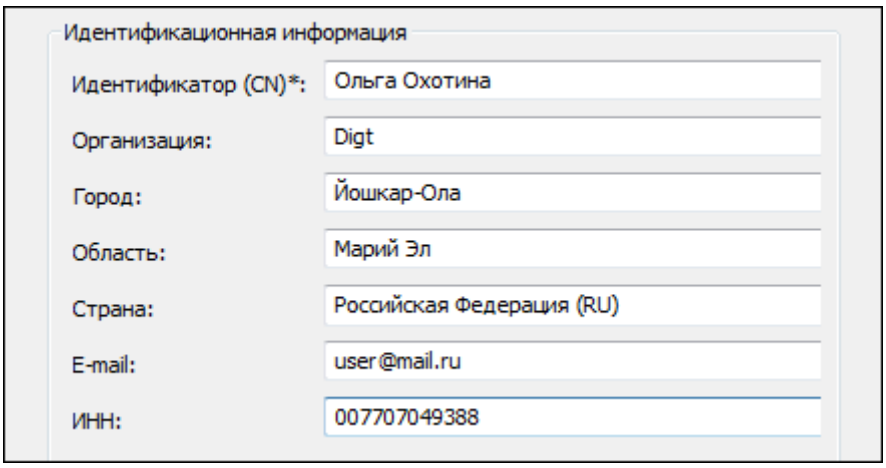
- шаблон по умолчанию

При создании запроса на сертификат по «шаблону по умолчанию» необходимо ввести базовую информацию о владельце: **Идентификатор**, **Организация**, **Город**, **Область**, **Страна**, **E-Mail** и **ИНН**;

- шаблон с расширенным списком полей

При создании запроса на сертификат по «шаблону с расширенным списком полей» дополнительно к базовой информации добавляется следующая: **Должность, Подразделение, Регион, Населенный пункт, Адрес**.

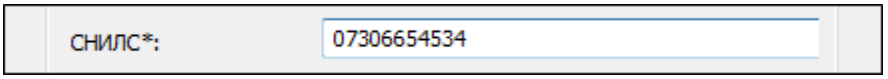
2. Откроется окно **Основная информация**, в котором, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце будущего сертификата:



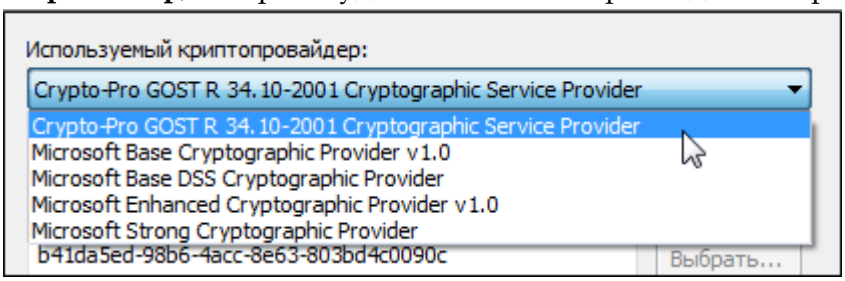
Поля в шаблоне отмеченные знаком «» являются обязательными для заполнения.*

Обратите внимание, если вы указываете ИНН юридического лица, номер всегда должен начинаться с «00», например 007707049388.

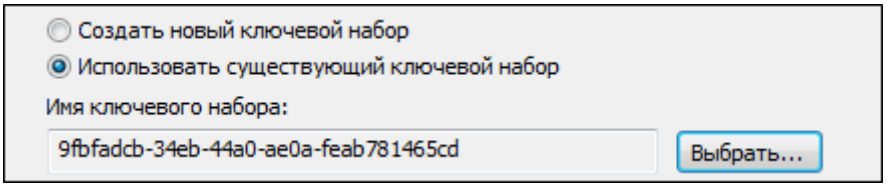
СНИЛС указывается без пробелов и знака «-», например, 07306654534.



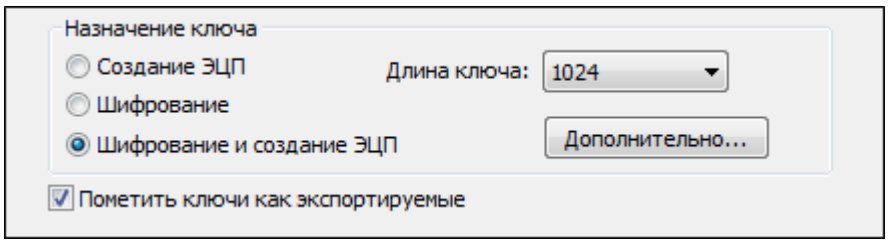
3. Далее в окне **Параметры ключа** укажите следующие настройки:
   1) **Криптопровайдер,** который будет использован при создании сертификата.



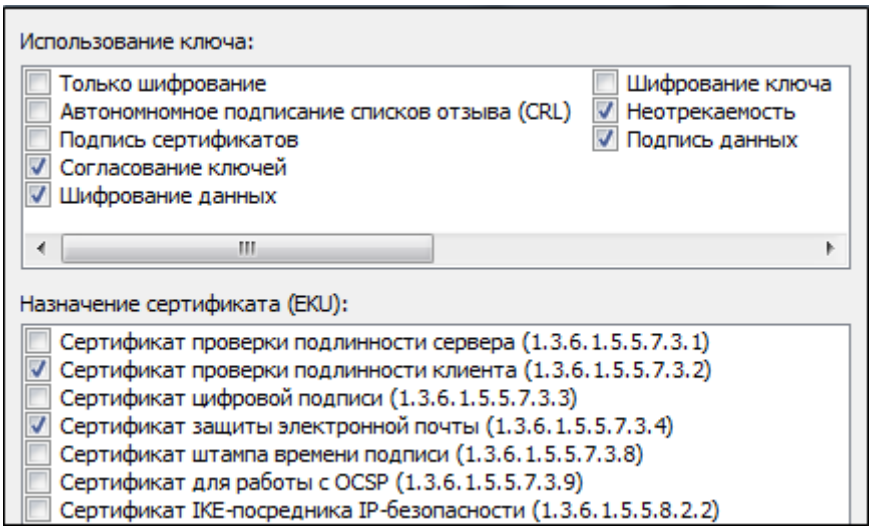
   2) Выберите вариант создания ключевого набора.
   - **Создать ключевой набор** сертификат будет создан на основе нового ключевого набора.
   - **Использовать существующий ключевой набор** – выберите ключевой набор, который будет использован при создании сертификата, из списка существующих (кнопка **Выбрать**).



   3) Установите переключатель напротив необходимого **Назначения ключа** сертификата.



4) Вы также можете выбрать дополнительное назначение ключа, нажав на кнопку **Дополнительно**. В списке назначений использования ключа и назначений сертификата (EKU) выберите необходимое:

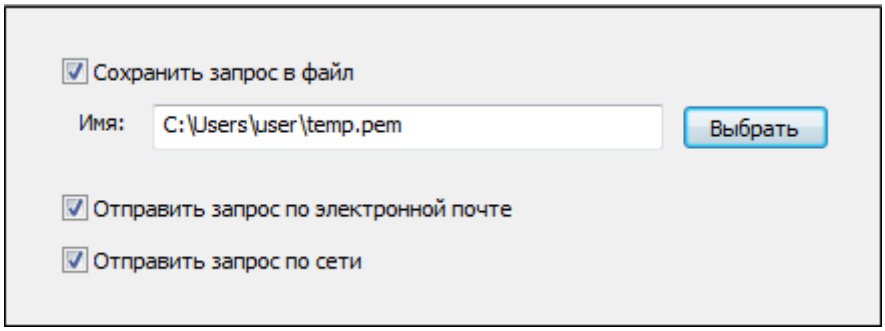


4) Укажите необходимую **Длину ключа**. Чем длиннее ключ, тем он надежнее.

5) **Пометить ключи как экспортируемые**.

Если вы отметите этот флаг, то сможете проводить экспорт сертификата вместе с закрытыми ключами

4. Укажите, каким образом вы хотите отправить запрос на обработку:



- на отчуждаемом ключевом носителе, предварительно сохранив запрос в файл;
- по электронной почте:

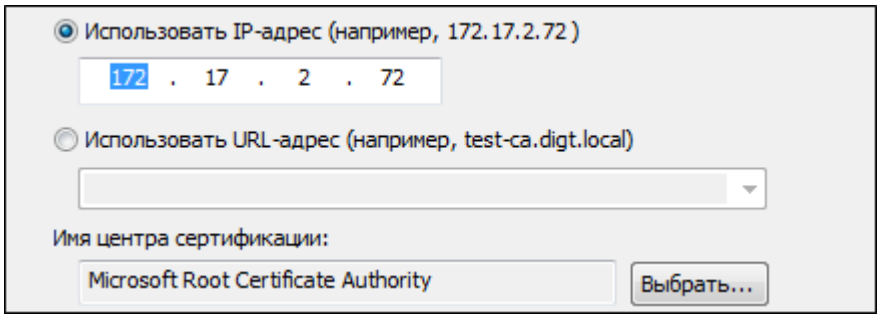
Для этого на следующем шаге укажите тему письма, e-mail и комментарии к письму.

Outlook *Если для отправки электронных писем вы используете программу Outlook, то сначала вам будет предложено подтвердить отправку письма. При этом отправка письма не выполняется, если программа не запущена, а будет выполнена только после запуска Outlook.*

The Bat! *В отличие от Outlook, программа сначала запускается, а потом просит подтвердить отправку письма.*

- в онлайн-режиме (через веб-службу ЦС)

Укажите адрес веб-службы УЦ (IP-адрес или URL-адрес) и сертификат корневого Удостоверяющего центра:



5. На основе указанных данных будет сформирован запрос на сертификат открытого ключа. После завершения операции возникнет окно с информацией о ее результатах.
6. Для ГОСТ сертификата выберите ключевой носитель, куда должен быть сохранен сформированный запрос (Реестр, дискета, USB брелок).
7. На запрос системы установите пароль на данный носитель и подтвердите его.

Остальные типы запросов

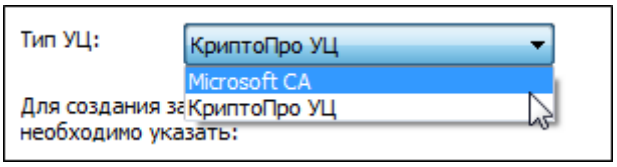
С помощью раздела Клиент УЦ вы можете создавать следующие типы запросов:

- запрос на отзыв сертификата;
- запрос на приостановление сертификата;
- запрос на возобновление сертификата;
- запрос на смену ключей и сертификата.

Создать запрос вы можете двумя способами:

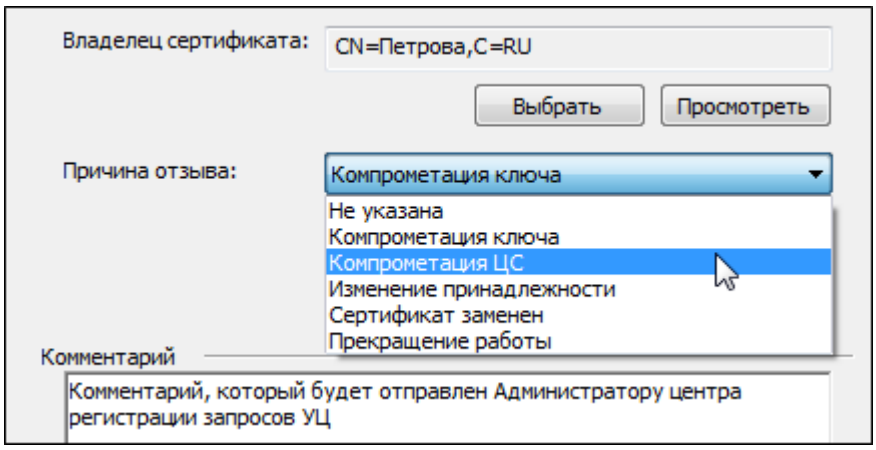
- В разделе **Сертификаты**, в контекстном меню сертификата указать пункт**Все задачи,** а затем выбрать необходимое действие.
- В разделе **Запросы > Запросы на …**, в контекстном меню раздела или на панели инструментов, указав пункт **Создать**.

1. Откроется стандартный Мастер создания запроса. Ознакомьтесь с порядком формирования запроса. На первом шаге вам потребуется указать тип Удостоверяющего центра, в котором будет обрабатываться запрос.



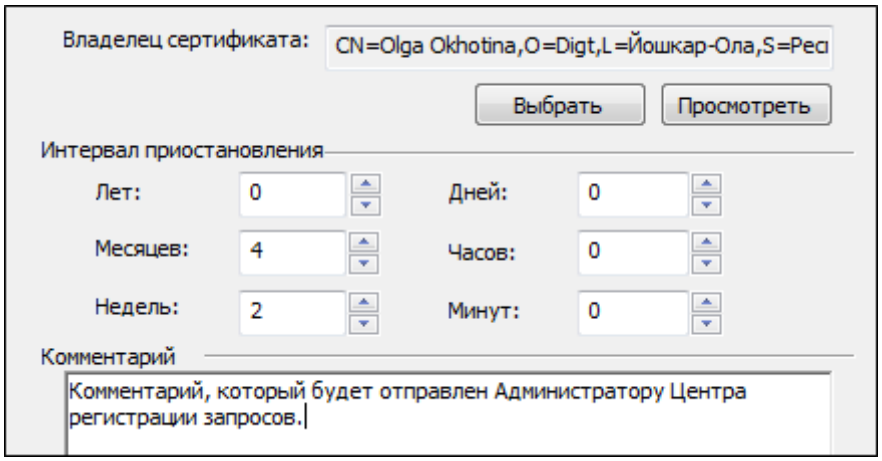
2. Следующий шаг зависит то типа запроса, который вы создаете.
   - Для типа запроса на **отзыв сертификата**.

Выберите личный сертификат, который необходимо отозвать, укажите причину, по которой необходимо отозвать данный сертификат, и добавьте комментарий для Администратора Центра регистрации Удостоверяющего центра.



- Для запроса на **приостановление сертификата.**

Выберите личный сертификат, действие которого необходимо на время приостановить, и укажите интервал приостановления (лет/ месяцев/недель /дней/ часов/минут). Добавьте комментарий для Администратора Центра регистрации Удостоверяющего центра.

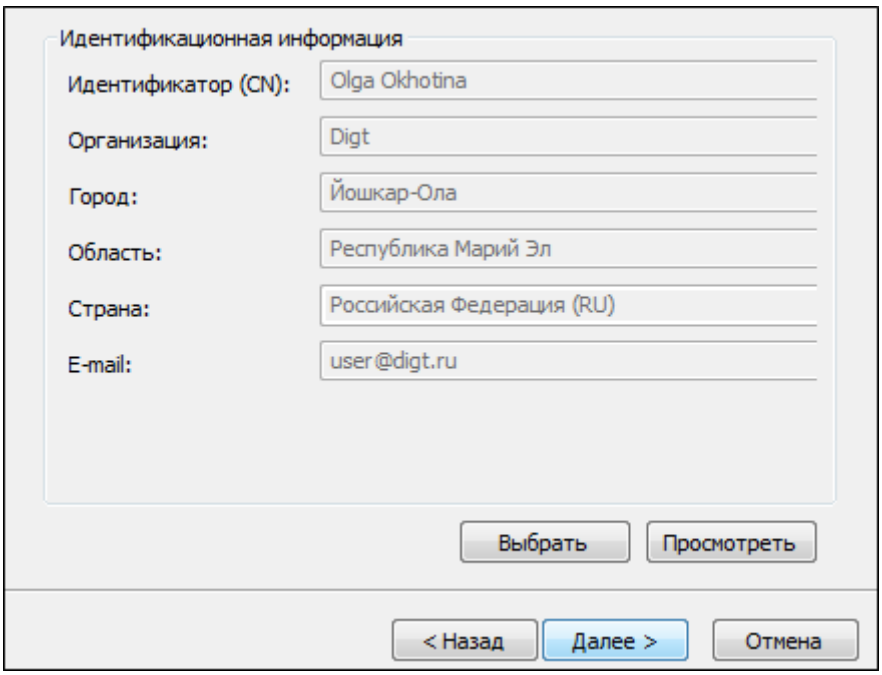


- Для запроса на **возобновление сертификата.**

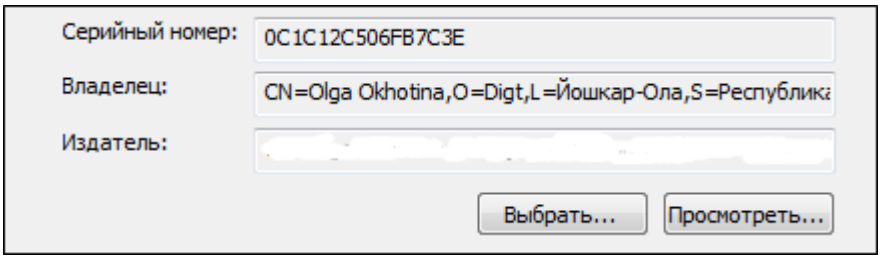
Выберите личный сертификат, действие которого необходимо возобновить. Добавьте комментарий для Администратора Центра регистрации Удостоверяющего центра.

- Для запроса на **смену ключей и сертификата**.

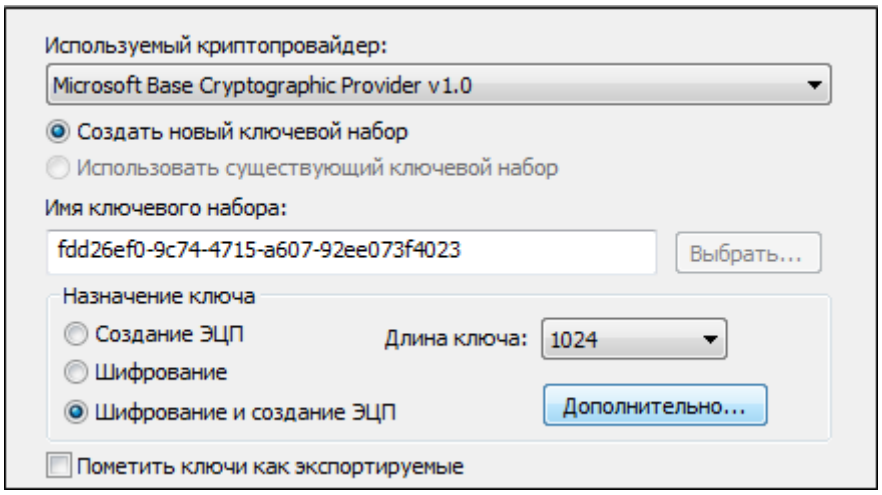
Выберите личный сертификат, который необходимо обновить.



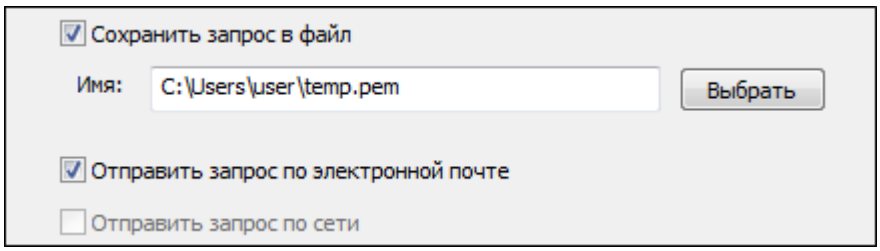
3. Далее укажите сертификат, которым будет подписан запрос, направляемый в удостоверяющий центр.



Обратите внимание, что для запроса на смену ключей и сертификатов вам нужно сначала будет указать параметры ключа, связанного с сертификатом (ключевой набор и варианты использования ключа), а затем вы перейдете на шаг выбора сертификата подписи запроса.



4. Укажите, каким образом вы хотите отправить запрос на обработку:



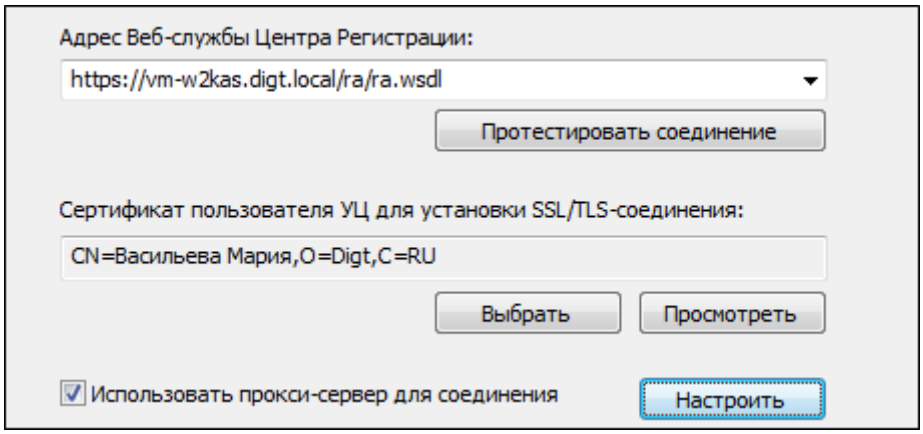
- на отчуждаемом ключевом носителе, предварительно сохранив запрос в файл
- по электронной почте - для этого на следующем шаге укажите тему письма, e-mail и комментарии к письму.

Outlook *Если для отправки электронных писем вы используете программу Outlook, то сначала вам будет предложено подтвердить отправку письма. При этом отправка письма не выполняется, если программа не запущена, а будет выполнена только после запуска Outlook.*

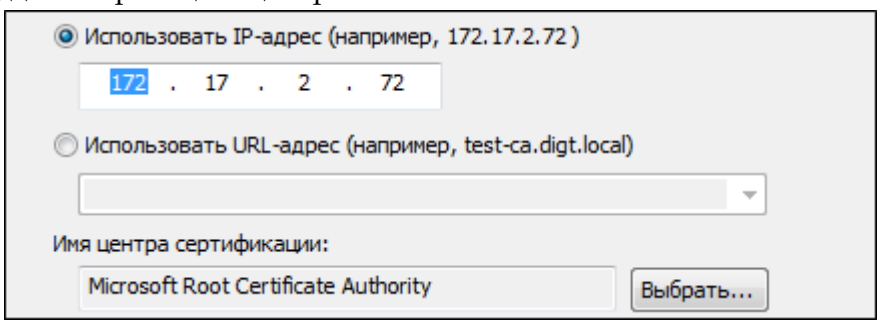
The Bat! *В отличие от Outlook, программа сначала запускается, а потом просит подтвердить отправку письма.*

- в онлайн-режиме (через веб-службу ЦС)

Для «КриптоПро УЦ» **-у**кажите WDSL-адрес данной веб-службы и сертификат пользователя УЦ для установки защищенного SSL\TLS. Кроме этого настройте параметры соединения с прокси-сервером, если того требует УЦ, в который вас обслуживает.



Для Microsoft CA - Укажите адрес веб-службы УЦ (IP-адрес или URL-адрес) и сертификат корневого Удостоверяющего центра:



5. На основе указанных данных будет сформирован запрос в УЦ. После завершения операции возникнет окно с информацией о ее результатах.
6. Для ГОСТ-сертификата укажите пароль.
7. Сформированный запрос отобразится в списке запросов раздела **Запросы > Запросы на…**

Вы также можете передать ранее созданный запрос в УЦ на рассмотрение в онлайн режиме, воспользовавшись кнопкой ***Отправить*** *на панели инструментов.*

8.2.2 Проверка статуса обработки запроса

Для каждого типа запросов существует возможность проверки их статуса следующими способами:

Тип запроса	Способ проверки статуса запроса
Запрос на сертификат	Проверка **по УЦ** (онлайн-проверка статуса запроса. Возможные статусы запросов: "В ожидании", "Отклонен", "Обработан"). Программа позволяет проверять статус обработки запроса в Удостоверяющем центре, если в политике УЦ указана опция "Отложенная выдача сертификатов". Проверка **локально** (заключается в поиске в личном хранилище сертификата, полученного по запросу. Возможные статусы "В ожидании", "Обработан").
Запрос на приостановление действия сертификата	Проверка **по УЦ** (онлайн-проверка статуса запроса. Возможные статусы запросов: "В ожидании", "Отклонен", "Обработан"). Проверка **по СОС** (заключается в получении последнего СОС из УЦ и поиске сертификата в нем. Возможные статусы "В ожидании", "Обработан").
Запрос на возобновление действия сертификата	Проверка **по УЦ** (онлайн-проверка статуса запроса. Возможные статусы запросов: "В ожидании", "Отклонен", "Обработан"). Проверка **по СОС** (заключается в получении последнего СОС из УЦ и поиске сертификата в нем. Возможные статусы "В ожидании", "Обработан")
Запрос на отзыв сертификата	Проверка **по УЦ** (онлайн-проверка статуса запроса. Возможные статусы запросов: "В ожидании", "Отклонен", "Обработан"). Проверка **по СОС** (заключается в получении последнего СОС из УЦ и поиске сертификата в нем. Возможные статусы "В ожидании", "Обработан").
Запрос на обновление ключей/ сертификата	Проверка **по УЦ** (онлайн-проверка статуса запроса. Возможные статусы запросов: "В ожидании", "Отклонен", "Обработан"). Программа позволяет проверять статус обработки запроса в Удостоверяющем центре, если в политике УЦ указана опция "Отложенная выдача сертификатов". Проверка **локально** (заключается в поиске в личном хранилище сертификата, полученного по запросу. Возможные статусы "В ожидании", "Обработан").

Чтобы проверить статус обработки запроса:

1. В дереве элементов главного окна выберите раздел **Клиент УЦ > Запросы на …** В правой панели главного окна выделите строку с запросом (или группу запросов на

сертификат), статус которого необходимо проверить, вызовите правой клавишей мыши контекстное меню и выберите пункт **Проверить статус > Способ проверки.**

2. Когда сертификат будет издан УЦ, вы можете установить его в хранилище ваших личных сертификатов. Процедура установки сертификата описана в главе Операции с сертификатами.

8.2.3 Просмотр информации о запросе

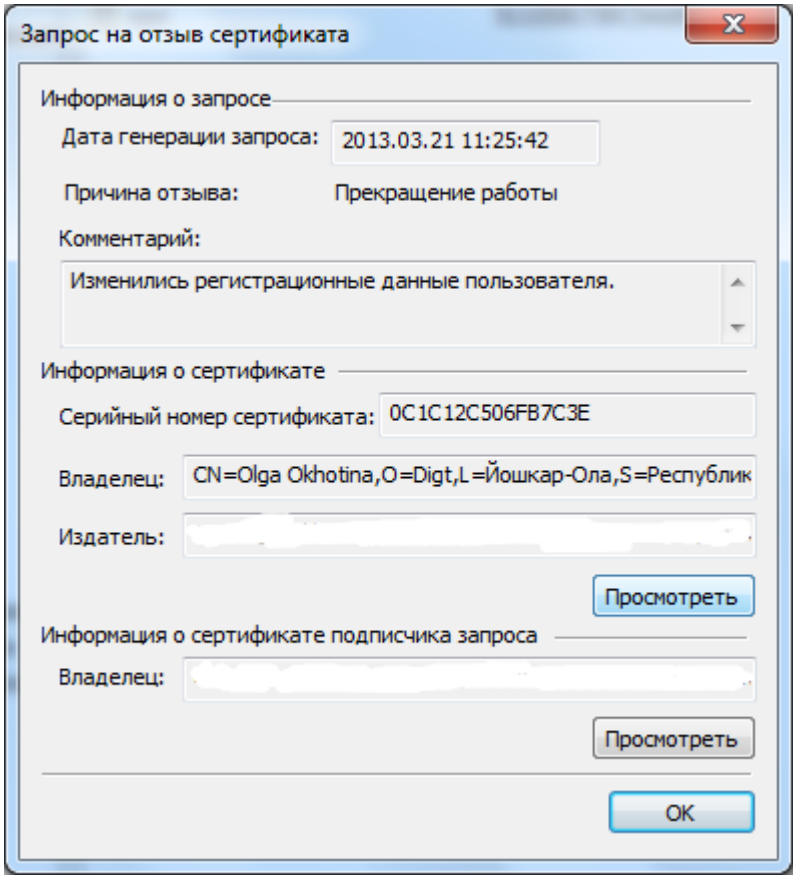
Вы можете просматривать следующую информацию о созданных вами запросах:

- Данные о самом запросе (дата создания запроса, данные по планируемой операции - созданию, приостановлении, отзыву, возобновлению, смене ключей, а также комментарий)
- Данные о сертификатах
  - о сертификате, над которым выполняется операция;
  - о сертификате подписчика запроса.

Для того чтобы просмотреть информацию о запросе в УЦ:

1. В разделе **Запросы** выберите папку с тем типом запроса, который необходимо просмотреть. В контекстном меню выберите пункт **Свойства.**
2. В открывшемся окне вы сможете просмотреть подробную информацию

– о запросе, переданном в УЦ;
– о сертификате, относительно которого был сформирован запрос;
– о сертификате подписчика запроса.



Вы также можете просматривать информацию о запросах в финальном окне всех криптографических операций.

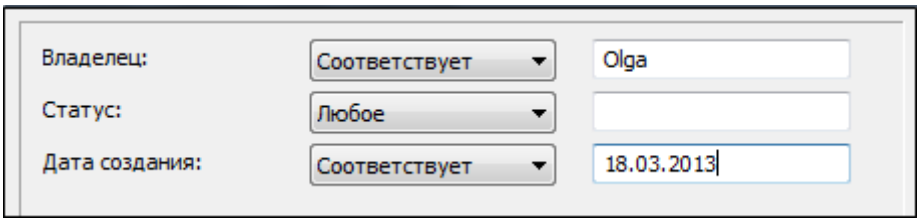
8.2.4 Фильтрация запросов

Вы можете фильтровать запросы в списке по следующим параметрам:

- владелец
- электронная почта
- организация
- дата создания

Для того чтобы отфильтровать запросы в списке:

1. В разделе **Запросы** выберите папку с тем типом запросов, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр.**
2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать запросы:

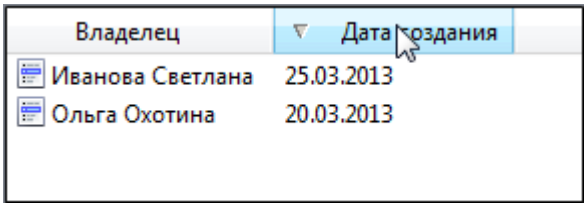


8.2.5 Сортировка запросов в списке

В программе «КриптоАРМ» реализована возможность сортировать запросы в удостоверяющей центр в списке.

Сортировка может выполняться по следующим параметрам:

- имя владельца запроса
- статус отправки запроса в Удостоверяющий центр
- дата создания запроса



8.2.6 Печать запроса

Для печати запроса выполните следующие действия:

1. Откройте хранилище запросов (системное хранилище), выберите необходимый запрос (или группу запросов), в контекстном меню объекта или на панели задач выберите пункт **Печать:**
2. В новом окне браузера MS Internet Explorer будет сформирована печатная форма запроса.
3. Для вывода на печать формы запроса на панели инструментов браузера нажмите на кнопку **Печать**.

8.2.7 Удаление запроса

Для удаления запроса на сертификат:

1. В дереве элементов главного окна выберите раздел **Запросы> Запросы на сертификат**. В правой панели главного окна выделите строку с запросом на сертификат (или группу запросов на сертификат), который необходимо удалить, в контекстное меню объекта или на панели инструментов выберите пункт **Удалить**.
2. Подтвердите решение удалить запрос на сертификат.
3. Запрос будет удален из хранилища.

8.3 Операции со списками отзыва сертификатов

Список отзыва сертификатов (COC/CRL) – документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было временно приостановлено.

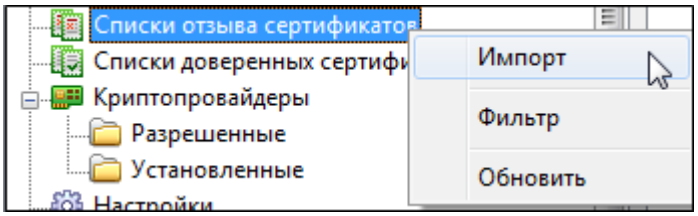
Доступны следующие операции со списками отзыва сертификатов:

- Установка COC в хранилище
- Настройка автоматического обновления списков
- Просмотр информации о списках
- Фильтрация COC
- Сортировка COC
- Экспорт COC
- Удаление COC

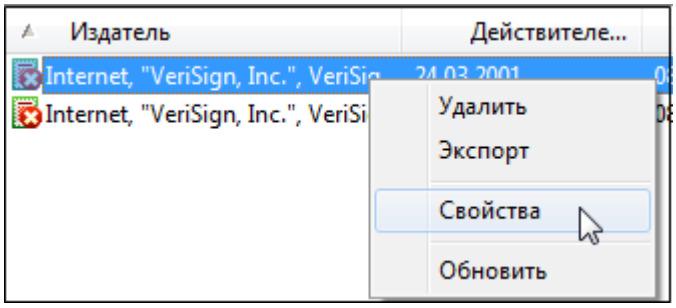
Эти операции можно выполнять через:

- панель инструментов

- контекстное меню раздела



- контекстное меню объекта

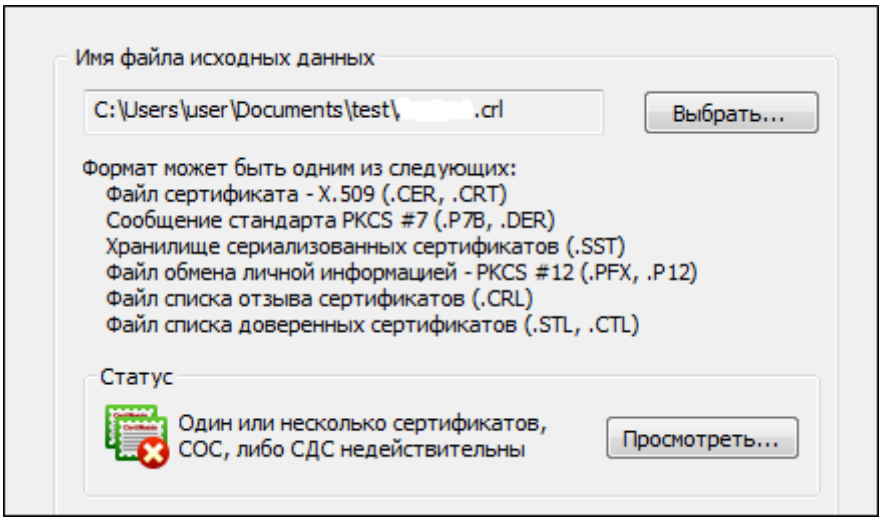


8.3.1 Установка списков отзыв в хранилище

Для установки списка в хранилище СОС, необходимо выполнить операцию импорта списка.

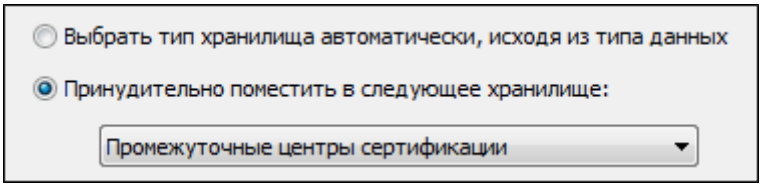
Для того чтобы импортировать список отзыва, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Списки отзыва сертификатов**.
2. В контекстное меню объекта (пункт **Редактировать** или контекстное меню на самом разделе) или на панели инструментов выберите пункт **Импорт**.
3. Откроется стандартный диалог Мастер установки сертификата и СОС.
4. Выберите импортируемый файл СОС в формате **.crl**:



5. Укажите хранилище, куда будет импортирован список отзыва сертификатов.

Списки отзыва сертификатов всегда необходимо устанавливать в системное хранилище **Промежуточные центры сертификации**, так как система PKI работает только с СОС из хранилища Промежуточных ЦС.



6. После завершения операции возникнет сообщение об успешном импорте СОС.

8.3.2 Просмотр информации о списках

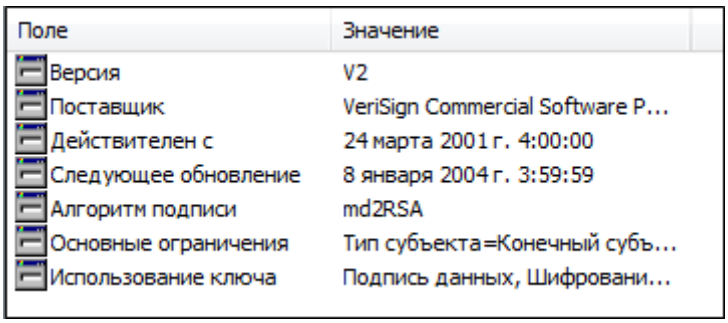
В правой панели главного окна доступна базовая информация о списках отзыва:

- Имя субъекта, выпустившего СОС (издатель);
- Срок истечения действия СОС (действителен с / действителен по).

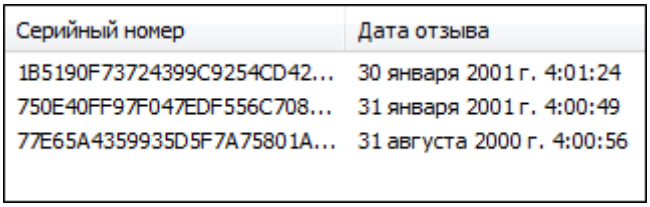
Для просмотра детальной информации о **Списке отзыва сертификатов,** выполните следующие шаги:

1. Выберите необходимый СОС из списка, в контекстном меню объекта или на панели задач выберите пункт **Свойства.**
2. Откроется форма с информацией о **Списке отзыва сертификатов (СОС)**:

- В закладке **Общие** содержится общая информация о просматриваемом списке отзыва:



- В закладке **Список отзыва** дается подробная информация о каждом сертификате, входящем в просматриваемый список



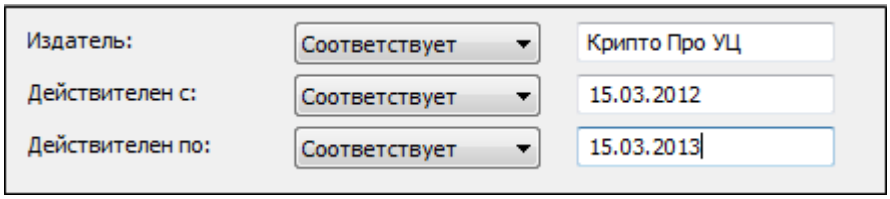
8.3.3 Фильтрация списков отзыва

Вы можете фильтровать СОС в списке по следующим параметрам:

- Издатель;
- Дата, с которой СОС действителен;
- Дата, по которую СОС действителен.

Для того чтобы отфильтровать списки отзыва сертификатов:

8) В разделе **Списки отзыва сертификатов** выберите папку с тем типом списков, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.
9) В окне **Установка фильтра** установите параметры, по которым необходимо отобрать СОС:

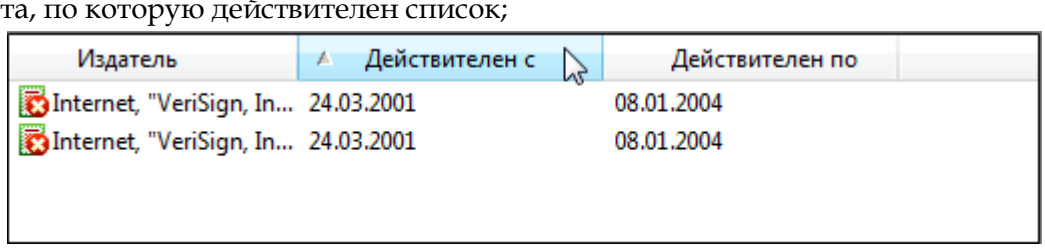


8.3.4 Сортировка списков отзыва

В программе «КриптоАРМ» реализована возможность сортировать списки отзыва сертификатов.

Сортировка может выполняться по следующим параметрам:

- имя издателя списка отзыва;
- дата, с которой действителен список;
- дата, по которую действителен список;

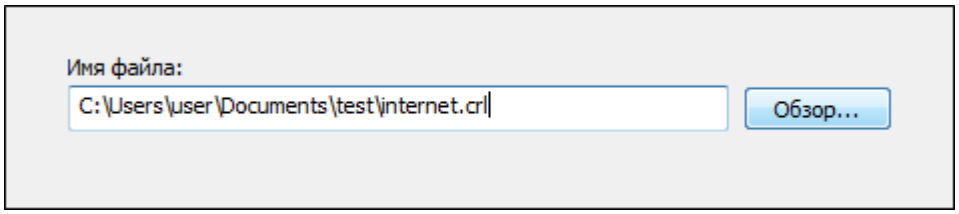


8.3.5 Экспорт списков отзыва

Программа позволяет экспортировать списки отзыва сертификатов (COC) в хранилище.

Для того чтобы экспортировать список отзыва:

1. В дереве элементов главного окна выберите раздел **Списки отзыва сертификатов**.
2. В правой панели главного окна выделите **COC** (или группу COC), который необходимо экспортировать, в контекстном меню объекта или на панели задач выберите пункт **Экспорт**.
3. Откроется стандартный диалог **Мастер экспорта сертификатов**, позволяющий выбрать экспортируемый файл COC.
4. Введите имя файла Списка отзыва сертификата.



5. В заключение возникнет сообщение об успешном экспорте COC.

8.3.6 Удаление списков отзыва

Система позволяет удалять списки отзыва сертификатов (COC) из хранилища.

Для того чтобы удалить список отзыва:

1. В дереве элементов главного окна выберите раздел **Списки отзыва сертификатов**.
2. В правой панели главного окна выделите строку со списком отзыва сертификатов (или группу COC), который необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить.**
3. Подтвердите решение удалить список отзыва.
4. В случае подтверждения список отзыва сертификатов будет удален из хранилища.

8.4 Операции со списками доверенных сертификатов

Список доверенных сертификатов (СДС/CTL) – Certificate Trust List. Это механизм, который позволяет администратору указать набор доверенных ЦС. Преимуществом указанного механизма является возможность передачи списков доверия по незащищенному каналу, поскольку они подписаны электронной подписью.

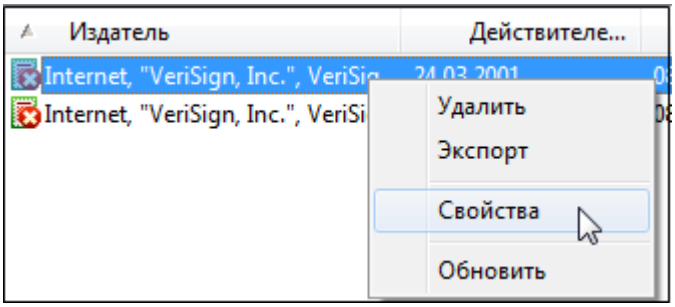
Доступны следующие операции со списками доверенных сертификатов:

- Создание СДС
- Установка СДС в хранилище
- Просмотр информации о списке
- Фильтрация списков
- Сортировка списков
- Экспорт списков
- Удаление списков

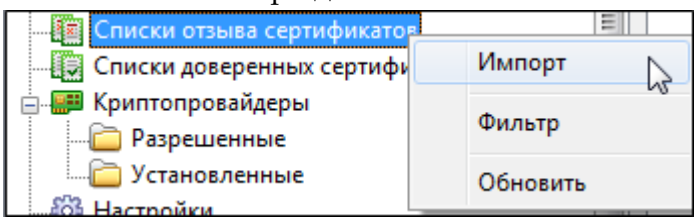
Операции со списками доверенных сертификатов можно выполнять через:

- Панель инструментов

- Контекстное меню объекта



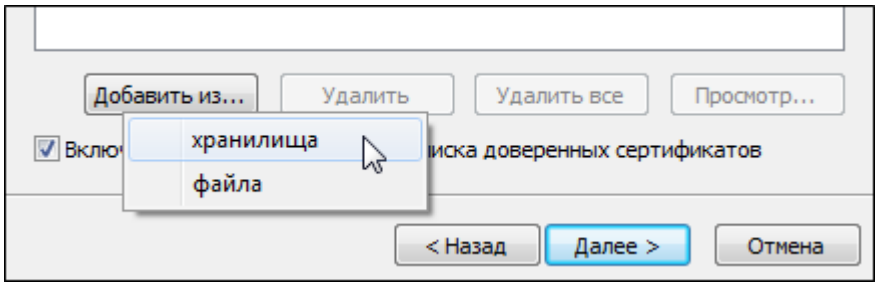
- Контекстное меню раздела



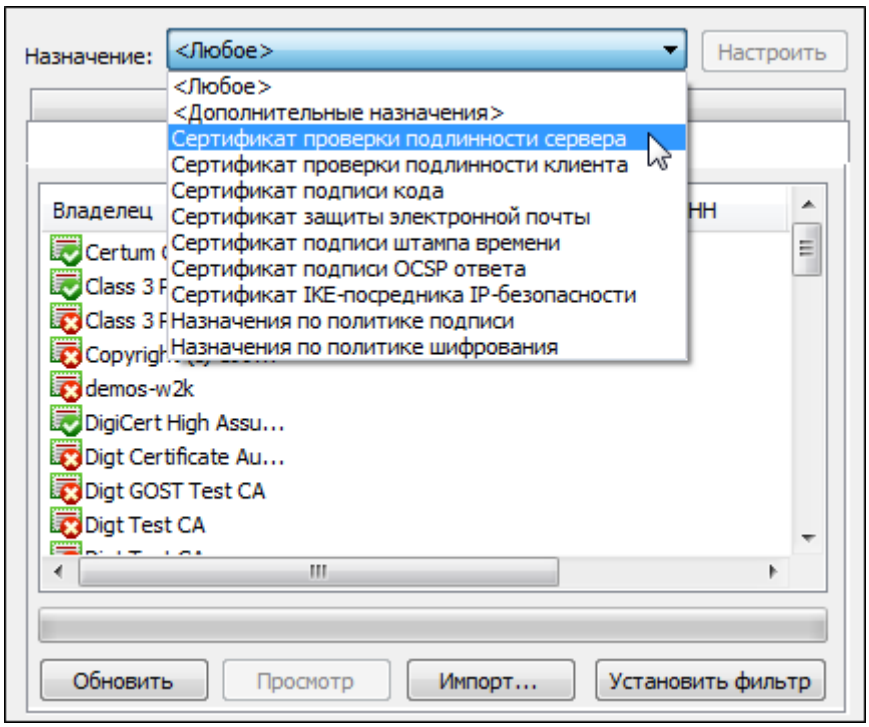
8.4.1 Создание списка

Для того чтобы создать список доверенных сертификатов:

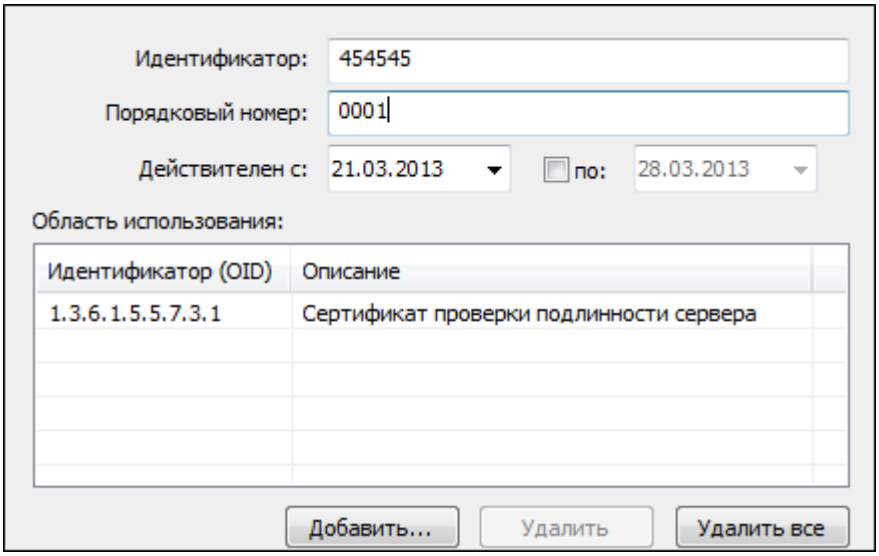
1. В дереве элементов главного окна выберите раздел **Списки доверенных сертификатов**.
2. В контекстное меню объекта (пункт **Редактировать** или контекстное меню на самом разделе) или на панели инструментов выберите пункт **Создать**.
3. Откроется **Мастер создания списка доверенных сертификатов** (СДС). Ознакомьтесь с порядком и требованиями для создания списка.
4. Из хранилища или файла выберите сертификаты УЦ, к которым должно осуществляться доверие:



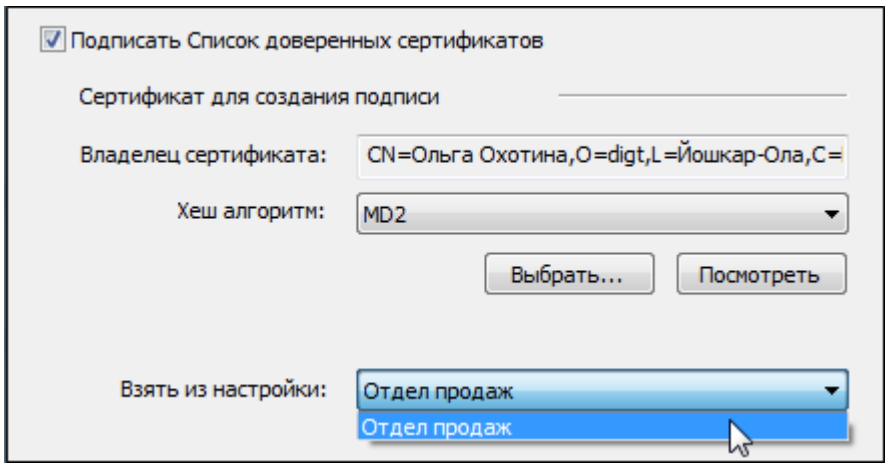
Для упрощения поиска сертификатов «КриптоАРМ» позволяет фильтровать сертификаты в списке по их назначению.



5. Далее необходимо заполнить дополнительные параметры Списка доверенных сертификатов: идентификатор, порядковый номер, время действия списка доверия и область использования сертификатов в списке (идентификатор и описание).



6. При необходимости вы можете подписать создаваемый список доверенных сертификатов электронной подписью. Для этого поставьте флаг напротив строки **Подписать Список доверенных сертификатов**. При этом станет доступен раздел, где вы сможете указать параметры подписи Списка доверенных сертификатов или взять параметры из готовой настройки подписи.



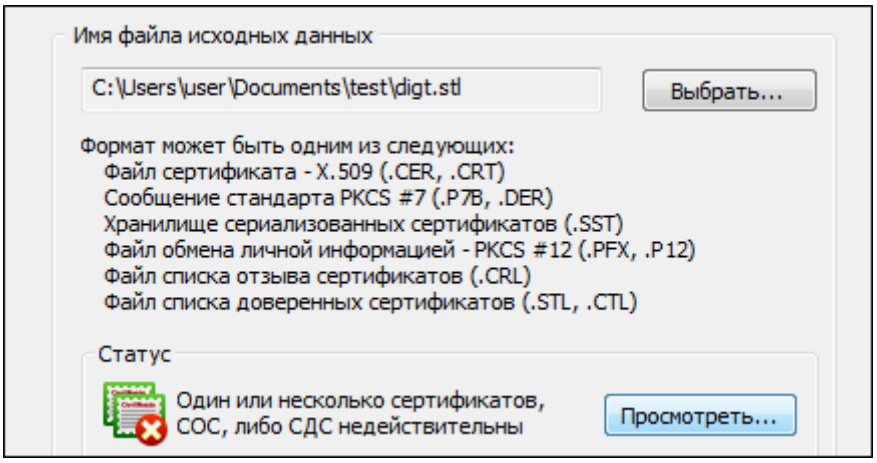
7. После сбора данных нажмите **Готово** для завершения мастера создания СДС.

8.4.2 Установка списка в хранилище

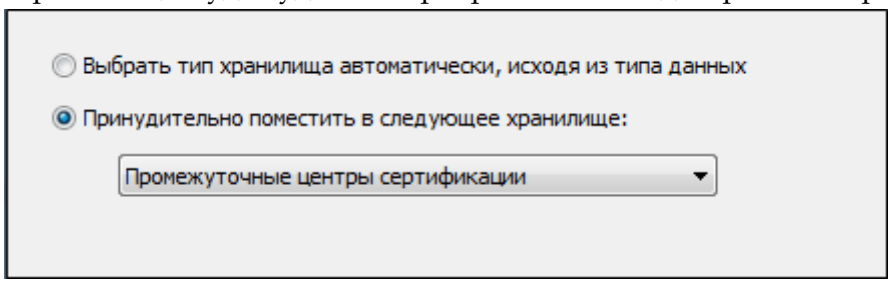
Для установки списка в хранилище, необходимо выполнить операцию импорта списка.

Для того чтобы импортировать список:

1. В дереве элементов главного окна выберите раздел **Списки доверенных сертификатов**.
2. В контекстное меню объекта (пункт **Редактировать** или контекстное меню на самом разделе) или на панели инструментов выберите пункт **Импорт**.
3. Откроется стандартный диалог Мастер установки сертификата и СОС.
4. Выберите импортируемый файл СДС (в формате. stl):



5. Укажите хранилище, куда будет импортирован список доверенных сертификатов.



Списки доверенных сертификатов всегда необходимо устанавливать в системное хранилище **Промежуточные центры сертификации**.

6. После завершения операции возникнет сообщение об успешном импорте СДС.

8.4.3 Просмотр информации о списке

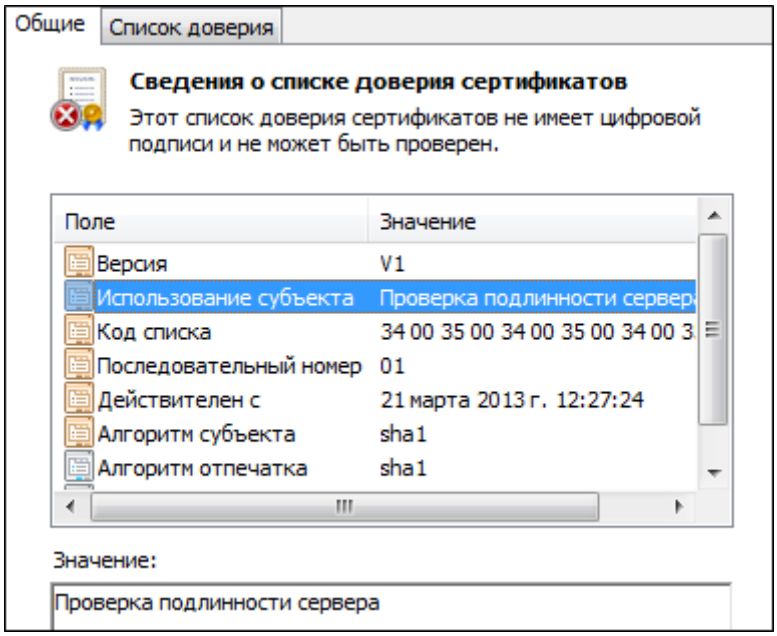
В правой панели главного окна доступна базовая информация о списках доверенных сертификатов:

- Идентификатор;
- Срок действия СДС (действителен с / действителен по);
- Области применения;
- Сертификат подписи.

Для просмотра подробной информации о **Списке доверенных сертификатов**, выполните следующие шаги:

1. Выберите необходимый СДС из списка, в контекстном меню объекта или на панели задач выберите пункт **Свойства**:
2. Откроется форма с информацией о **Списке доверенных сертификатов)**:

- В закладке **Общие** содержится общая информация о просматриваемом списке:



- В закладке **Список доверия** дается подробная информация о каждом сертификате, входящем в просматриваемый список.

8.4.4 Фильтрация списка

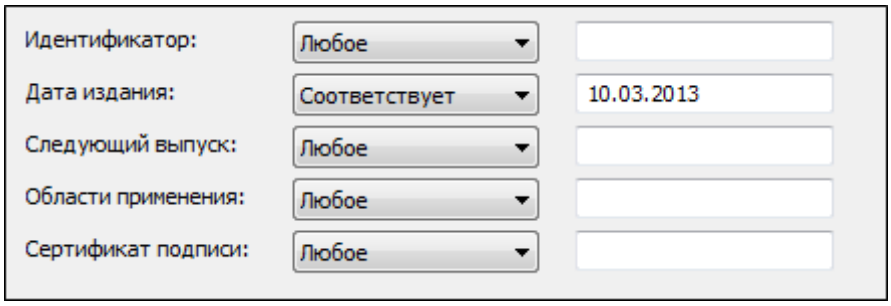
Вы можете фильтровать списки доверенных сертификатов (СДС) по следующим параметрам:

- издатель;
- дата, с которой СДС действителен;
- дата, по которую СДС действителен;
- идентификатор использования;
- область применения;
- сертификат подписи.

Для того чтобы отфильтровать списки доверенных сертификатов:

1. В разделе **Списки доверенных сертификатов** выберите папку с тем типом списков, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.

2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать СДС:

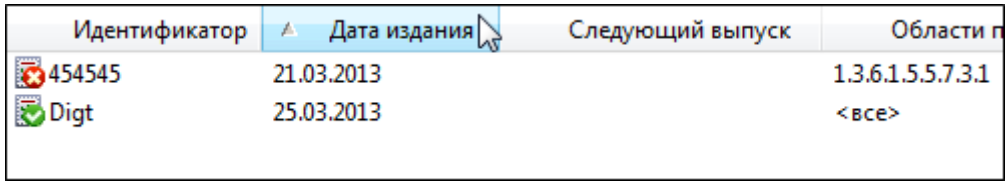


8.4.5 Сортировка списков

В программе «КриптоАРМ» реализована возможность сортировать списки доверенных сертификатов в общем списке.

Сортировка может выполняться по следующим параметрам:

- Идентификатор (имя издателя списка отзыва);
- Дата издания (дата, с которой действителен список);
- Следующий выпуск (дата, по которую действителен список);
- Области применения (идентификатор использования);
- Сертификат подписи.



8.4.6 Экспорт списков

Программа позволяет экспортировать списки доверенных сертификатов (СДС) в хранилище.

Для того чтобы экспортировать список доверенных сертификатов:

1. В дереве элементов главного окна выберите раздел **Списки доверенных сертификатов**.
2. В правой панели главного окна выделите список (или группу списков), который необходимо экспортировать, в контекстном меню объекта или на панели задач выберите пункт **Экспорт**.
3. Откроется стандартный диалог **Мастер экспорта сертификатов**, позволяющий выбрать экспортируемый файл СДС.
4. Введите имя файла Списка доверенных сертификатов.

5. В заключение возникнет сообщение об успешном экспорте списка.

8.4.7 Удаление списка

Система позволяет удалять списки доверенных сертификатов (СДС) из хранилища.
Чтобы удалить список:

1. В дереве элементов главного окна выберите раздел **Списки доверенных сертификатов**.
2. В правой панели главного окна выделите строку со списком доверенных сертификатов (или группу списков), который необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить**.
3. Подтвердите решение удалить список.
4. В случае подтверждения список доверенных сертификатов будет удален из хранилища.

8.5 Операции с криптопровайдерами

Криптопровайдер (CSP, Cryptographic Service Provider) — независимый программный модуль, интегрированный в Windows и содержащий библиотеку криптографических функций со стандартизованным интерфейсом. Криптопровайдер выполняет следующие криптографические функции:

- формирование/проверка электронной подписи (ЭП),
- шифрование информации,
- хранение ключей всех типов.

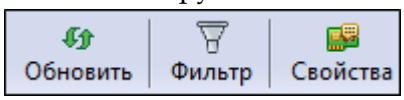
Криптопровайдер предназначен для авторизации, обеспечения конфиденциальности и юридической значимости электронных документов при обмене ими между пользователями, контроля целостности информации и др.

Доступны следующие операции с криптопровайдерами:

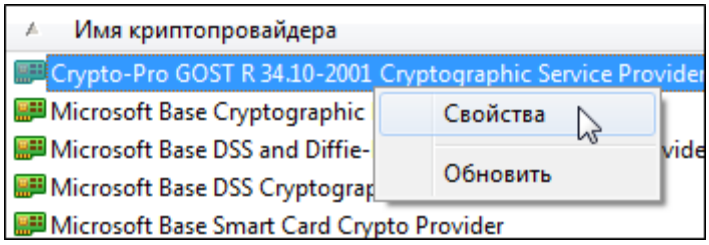
- Просмотр свойств криптопровайдера
- Фильтрация криптопровайдеров

Эти операции можно выполнять через:

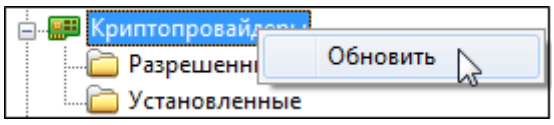
- Панель инструментов



- Контекстное меню объекта



- Контекстное меню раздела



8.5.1 Просмотр свойств криптопровайдера

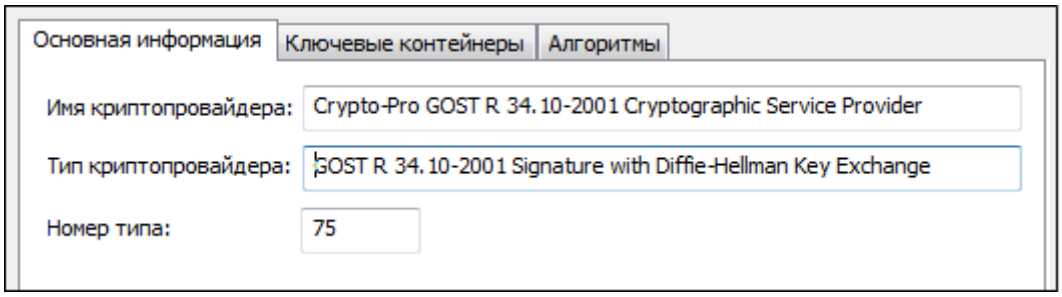
Чтобы просмотреть свойства криптопровайдера:

1. В дереве элементов главного окна выберите **Криптопровайдеры> Установленные.** В правой панели главного окна отобразится полный перечень криптопровайдеров, установленных в операционной системе. Для просмотра свойства криптопровайдера выберите необходимый криптопровайдер из списка и в контекстном меню объекта или на панели инструментов выберите пункт **Свойства.**

1. Откроется окно **Параметры криптопровайдера**. Информация по свойствам криптопровайдера представлена 3 закладками:
   - Основная информация;
   - Ключевые контейнеры;
   - Алгоритмы.

1) Основная информация;

Закладка содержит такие данные, как имя провайдера, тип провайдера и номер типа.



2) Ключевые контейнеры;

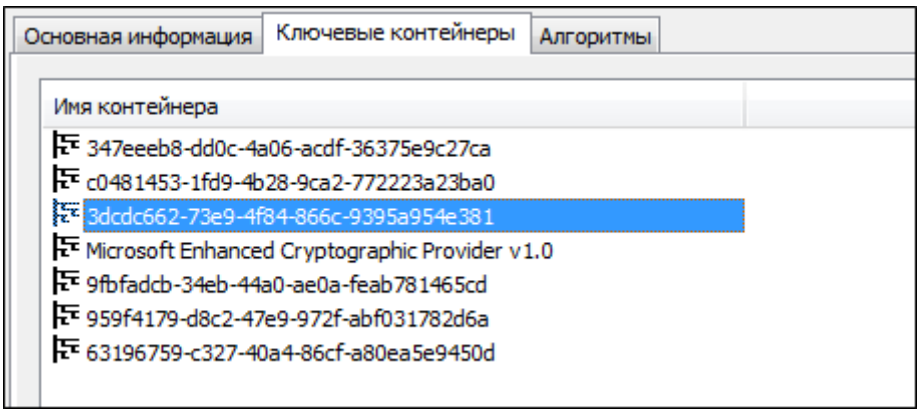
Закладка содержит такие данные, как имя провайдера, тип провайдера и номер типа

При формировании закрытые ключи записываются на ключевой носитель (ключевой контейнер).

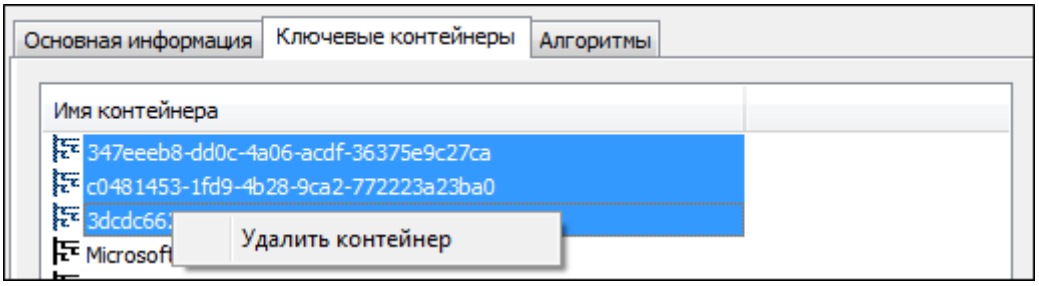
Ключевой контейнер может содержать:

- ключ подписи;
- ключ шифрования;
- ключ подписи и ключ шифрования одновременно.

Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п. Каждый контейнер (независимо от типа носителя) является полностью самостоятельным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми (и соответствующими им открытыми) ключами.

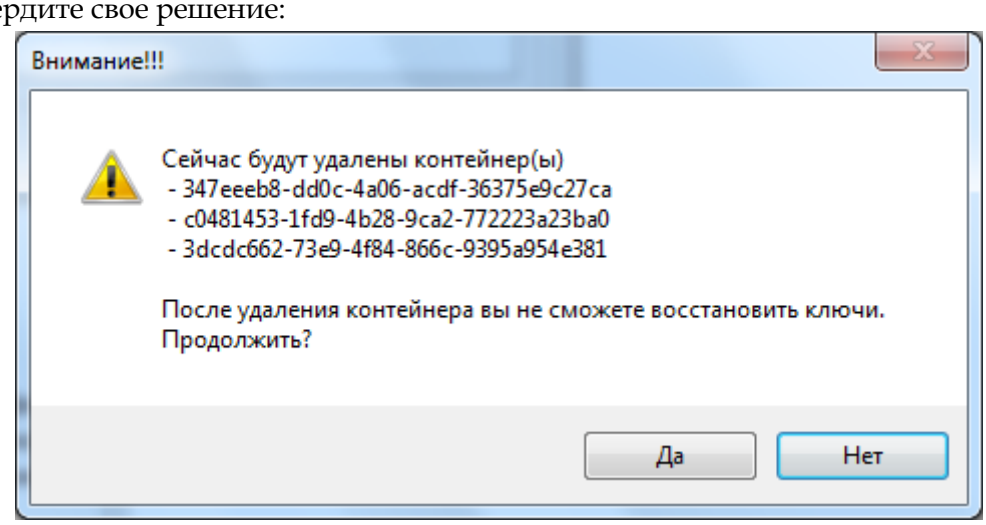


В этой закладке вы также может удалять ключевые контейнеры. Для этого выберите контейнер, который необходимо удалить, и щелкните на нем правой клавишей мыши: выберите **Удалить** Откроется окно с предупреждением.



Обратите внимание, что при удалении контейнера восстановить ключевую пару будет невозможно.

Подтвердите свое решение:



Ключевой контейнер будет удален из общего списка для выбранного криптопровайдера.

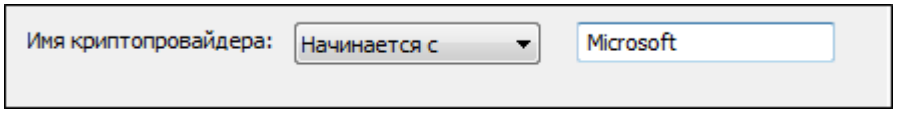
3) Алгоритмы;

Закладка содержит информацию об используемых алгоритмах:

8.5.2 Фильтрация криптопровайдеров

Для того чтобы отфильтровать криптопровайдеры в списке по имени:

1. В разделе **Криптопровайдеры** выберите папку с тем типом объектов, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.
2. В окне **Установка фильтра** установите параметр, по которым необходимо отобрать криптопровайдеры:



8.6 Операции со справочниками назначений (политик) сертификата

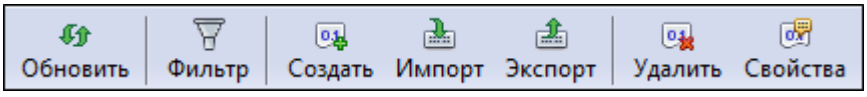
Программа «КриптоАРМ» позволяет добавить к создаваемой подписи или сертификату информацию о его назначении, например, гриф согласования, гриф утверждения и т.п.

С помощью программы «КриптоАРМ» в справочнике вы можете:

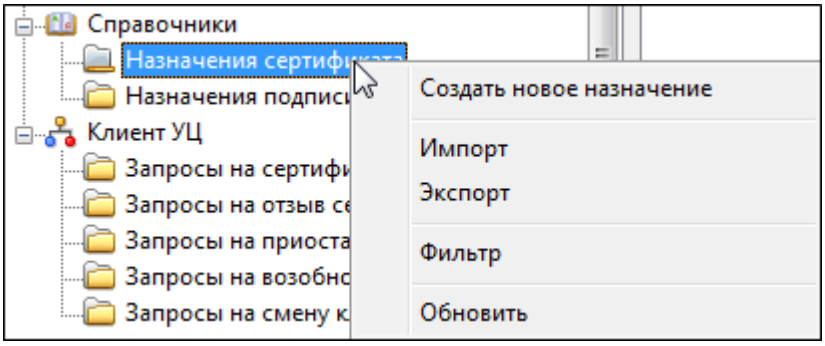
- Создавать новые назначения подписей;
- Просматривать свойства назначений;
- Фильтровать назначения в списке.
- Сортировать назначения
- Импортировать назначения;
- Экспортировать назначения;
- Удалять назначения подписей.

Эти операции со справочниками вы можете выполнять через:

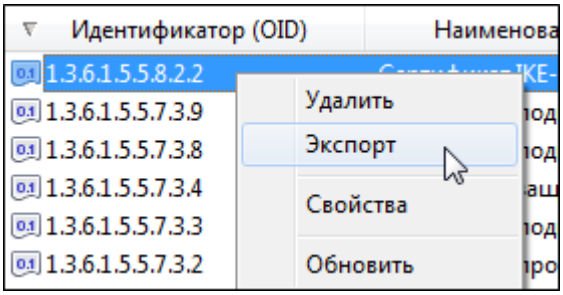
- Панель инструментов



- Контекстное меню раздела



- Контекстное меню объекта

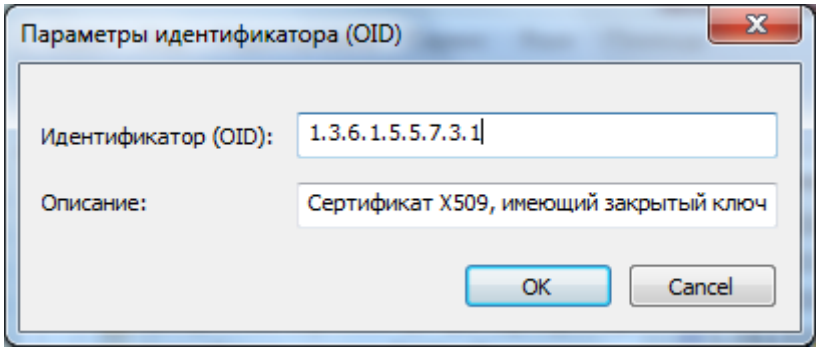


8.6.1 Создание нового назначения

Чтобы создать новое назначение сертификата или подписи:

1. В дереве элементов главного окна выберите раздел **Справочники > Назначения сертификатов** для добавления назначения сертификата или **Справочники > Назначения подписи** для добавления назначения подписи. В правой панели главного окна отобразится список установленных назначений.
2. Чтобы создать новое назначение, в контекстном меню раздела выберите пункт **Создать новое назначение** или на панели инструментов **Создать**.

3. Появится окно ввода параметров политики. Введите идентификатор (OID) и его описание:

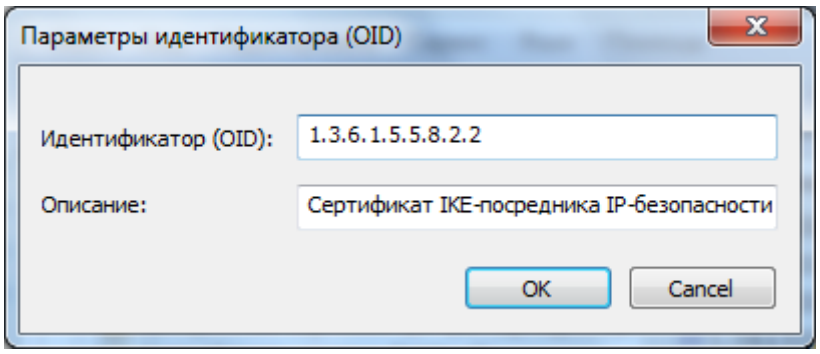


4. В справочник назначений добавится новая запись.

8.6.2 Просмотр свойств назначения

Чтобы просмотреть свойства OID-а:

1. В дереве элементов главного окна выберите раздел **Справочники > Назначения сертификатов** для просмотра свойств назначения сертификата или **Справочники > Назначения подписи** для просмотра свойств назначения подписи. В правой панели главного окна отобразится список установленных назначений сертификатов. Чтобы просмотреть свойства назначения сертификата, выберите его из списка, в контекстном меню объекта или на панели инструментов выберите пункт **Свойства**.
2. Появится окно **Параметры политики**, в котором отобразится информация о идентификаторе (OID) и его описание:



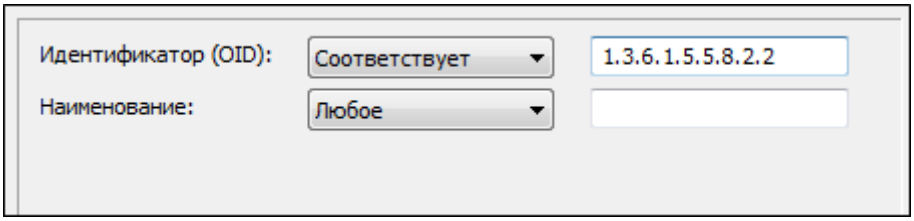
8.6.3 Фильтрация назначений

Вы можете фильтровать назначения в списке по следующим параметрам:

- идентификатор сертификата (OID)
- наименование

Для того чтобы отфильтровать назначения сертификатов:

1. В разделе **Справочники > Назначения сертификатов** или в разделе **Справочники > Назначения подписи** в контекстном меню выберите пункт **Фильтр**.
2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать назначения:

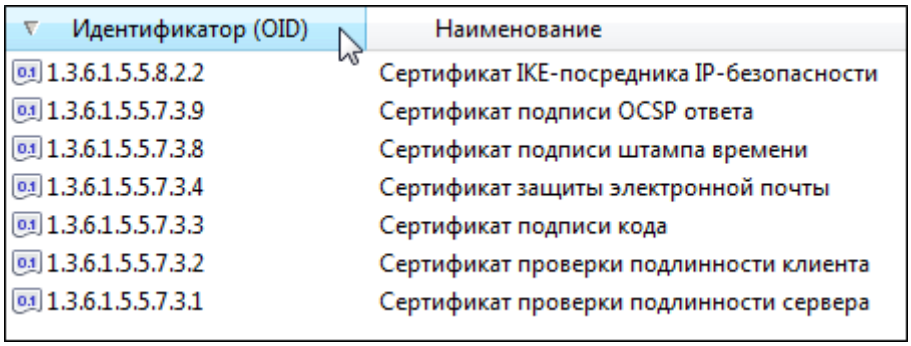


8.6.4 Сортировка назначений в списке

В программе «КриптоАРМ» реализована возможность сортировать назначения в справочнике.

Сортировка может выполняться по следующим параметрам:

- идентификатор (OID)
- наименование назначения



8.6.5 Импорт назначения

Чтобы импортировать назначение сертификата **в формате .xml**:

1. В дереве элементов главного окна выберите раздел **Справочники > Назначения сертификатов** для импорта назначений сертификатов или **Справочники >**

Назначения подписи для импорта назначений подписи. В правой панели главного окна отобразится список установленных назначений. Чтобы импортировать назначение, на панели инструментов выберите пункт **Импорт**.

2. В окне проводника выберите файл с OID в формате **.xml**
3. В справочник назначений будет импортировано новое назначение.

8.6.6 Экспорт назначения

Чтобы экспортировать назначение сертификата **в формате .xml**:

1. В дереве элементов главного окна выберите раздел **Справочники > Назначения сертификатов** для экспорта назначений сертификатов или **Справочники > Назначения подписи** для экспорта назначений подписи. В правой панели главного окна отобразится список установленных назначений. Чтобы экспортировать назначение (или группу назначений), выберите его из списка. В контекстном меню объекта или на панели инструментов выберите пункт **Экспорт**:
2. В окне проводника введите имя экспортируемого файла с OID
3. Назначение сертификата будет экспортировано в файл с OID в формате .xml.

Вы можете экспортировать сразу все назначения, для этого в контекстном меню на разделе **Назначения сертификата/Назначения подписи** или на панели инструментов выберите пункт **Экспорт**.

При одновременном экспорте всех или нескольких назначений, будет создаваться один .xml файл, содержащий все экспортируемые назначения.

8.6.7 Удаление назначения

Чтобы удалить назначение сертификата из справочника:

1. В дереве элементов главного окна выберите раздел **Справочники > Назначения сертификатов** для удаления назначения сертификатов или **Справочники > Назначения подписи** для удаления назначения подписи. В правой панели главного окна отобразится список установленных назначений. Выберите назначение (или группу назначений) из списка, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить**.
2. На запрос системы подтвердите свое решение.
3. Выбранное назначение будет удалено из справочника назначений сертификатов.

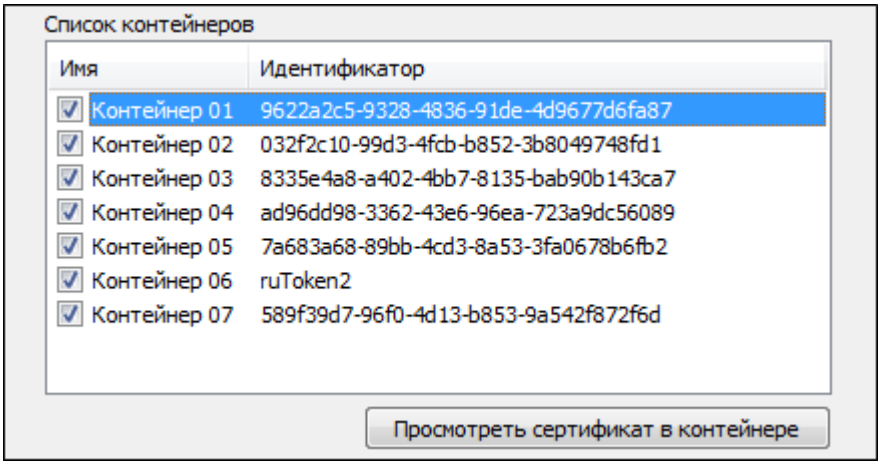
8.7 Операции с ключевыми носителями

С помощью программы «КриптоАРМ Стандарт» вы можете подключать отчуждаемые ключевые носители и импортировать сертификаты с них в личное хранилище пользователя.

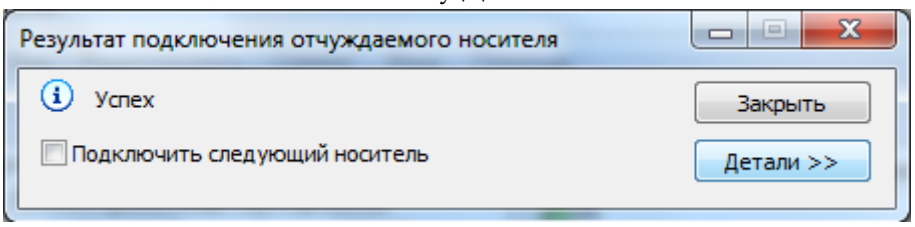
На сегодняшний день работа с отчуждаемыми носителями через «КриптоАРМ» реализована только для «КриптоПро CSP» и «КриптоПРО УЭК CSP». Работать с отчуждаемыми носителями, используя другие криптопровайдеры (например, стандартные Windows), вы можете, но только через средства самого криптопровайдера (а не программы «КриптоАРМ»).

В верхнем меню главного окна выберите пункт **Сервис > Подключить отчуждаемый носитель.** Далее следуйте указаниям **Помощника подключения отчуждаемого носителя:**

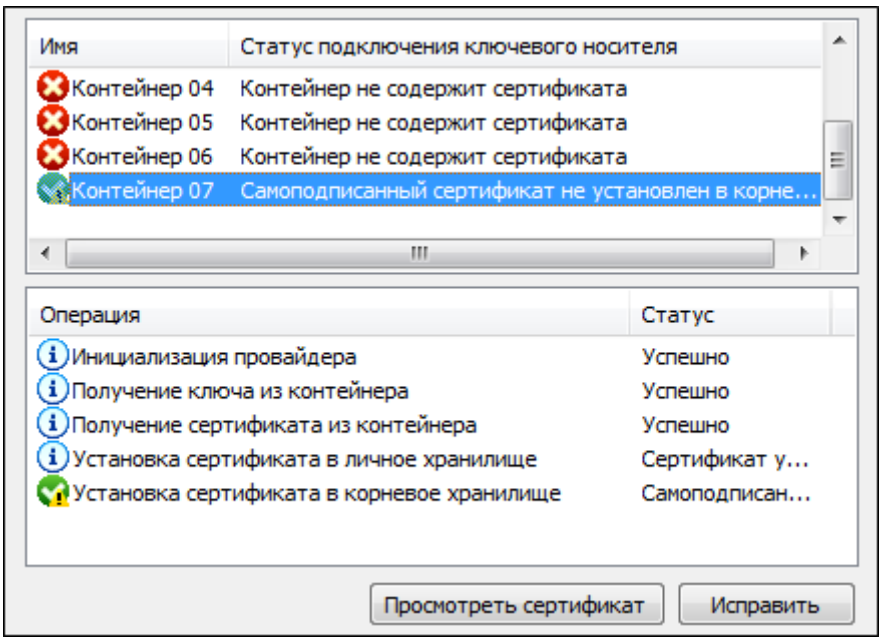
1. На первом шаге ознакомьтесь с порядком и требованиями к подключению отчуждаемого носителя. Нажмите **Далее.**
2. В следующем окне выберите тип криптопровайдера и ключевого носителя. В качестве ключевого носителя может выступать дискета или смарт-карта/USB токен. Для продолжения вставьте носитель и нажать кнопку **Далее**.
3. Выберите в списке контейнеров сертификаты для установки. Вы можете просмотреть информацию о сертификате, выбрав контейнер и нажав на кнопку **Просмотреть сертификат в контейнере**. Для завершения операции нажмите на кнопку **Готово**.



4. При обращении к контейнеру введите pin-код.
5. Далее возникнет окно с результатом выполнения операции. Вы можете просмотреть дополнительную информацию о статусе импорта сертификатов с отчуждаемого носителя, нажав на кнопку **Детали**.



6. В окне результата выполнения операции можно просмотреть журнал операций. В случае возникновения замечаний, их можно исправить, выбрав их в журнале и нажав на кнопку **Исправить**.



7. Чтобы закрыть окно результата выполнения операции, нажмите на кнопку **Закрыть**. Чтобы подключить следующий отчуждаемый носитель, поставьте флаг **Подключить следующий носитель**. При нажатии на кнопку **Закрыть** вновь откроется мастер подключения отчуждаемого носителя.

*Импортированный с ключевого носителя сертификат можно просмотреть в **личном хранилище сертификатов** пользователя.*

8.8 Работа с электронной подписью (ЭП)

8.8.1 Виды электронных подписей

В Федеральном законе Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" в статье 5 «Виды электронных подписей» описаны виды электронных подписей и их отличительные признаки.

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

2. **Простой электронной подписью** является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3. **Неквалифицированной электронной подписью** является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

4. **Квалифицированной электронной подписью** является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

8.8.2 Создание электронной подписи

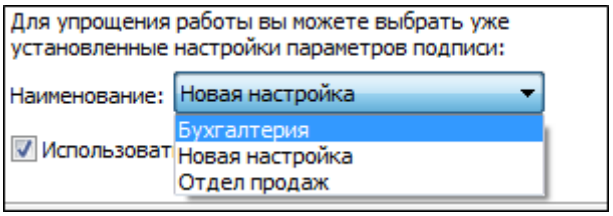
С помощью программы «КриптоАРМ» вы можете подписать отдельный файл или папку файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными)

Подписать данные вы можете через:

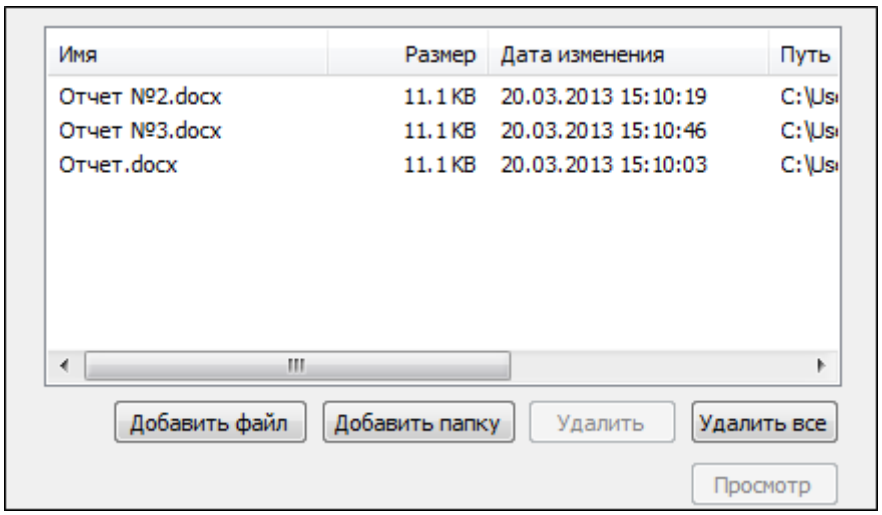
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт **Подписать**. Далее следуйте рекомендациям Помощника по выполнению операции:

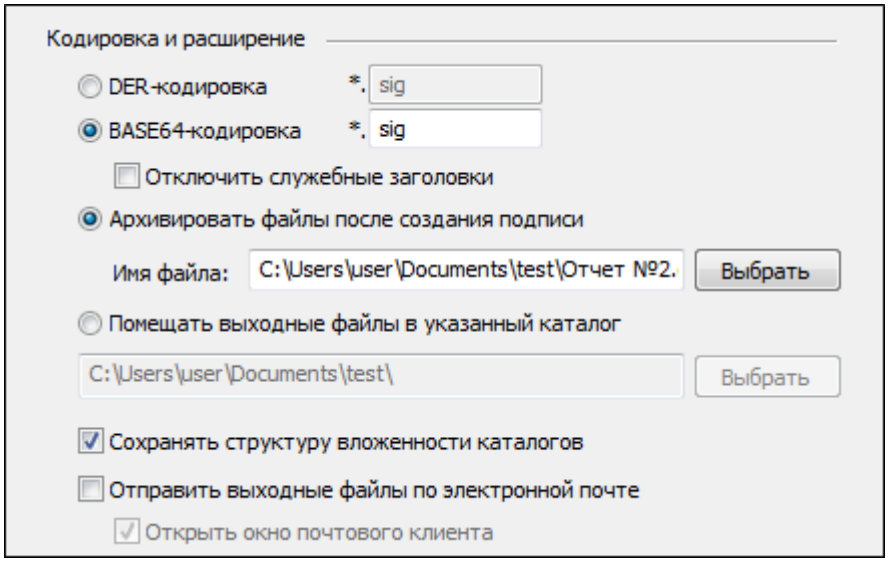
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки **Добавить папку** и **Добавить файл** соответственно).



3. В открывшемся окне укажите настройки для выходного формата файла.



1) **Кодировка и расширение;**
   - DER encoded binary X.509. Расширения подписанного файла *.sig, *.p7s.
   - Base64 encoded X.509.Для этого варианта кодирования вы можете указать фла

2) **Отключить служебные заголовки.**

3) Расширения подписанного файла *.sig.

4) **Архивировать файлы после создания подписи;**

В строке **Имя файла** укажите путь до архива и имя создаваемого архива.

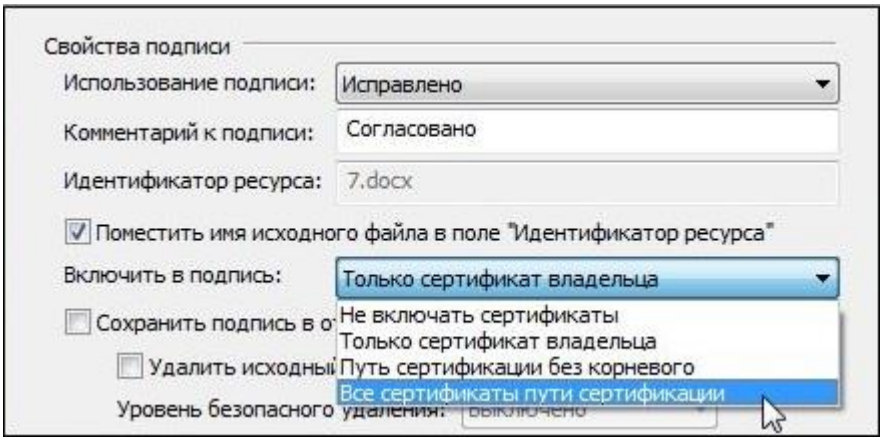
5) **Помещать выходные файлы в указанный каталог;**

Если выбрать этот режим и оставить поле ввода пути к каталогу не заполненным, то выходные файлы будут формироваться в каталоге входных файлов.

6) **Сохранять структуру вложенности каталогов;**

7) **Отправить выходные файлы по электронной почте.**

4. Далее введите необходимые свойства подписи.



1) **Использование подписи;**

Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

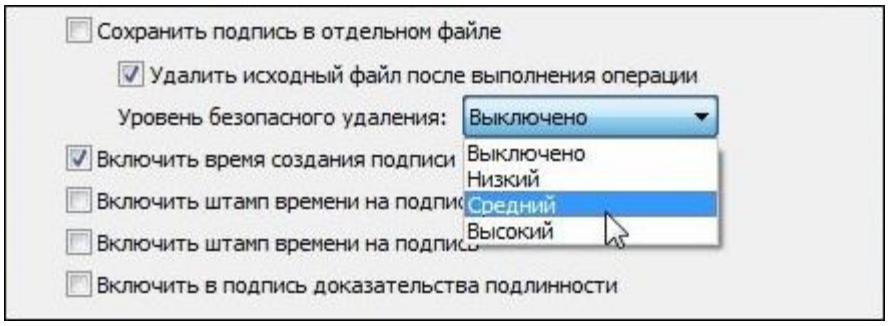
2) **Комментарий к подписи;**

Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

3) **Идентификатор ресурса;**

4) **Включить в подпись:**

- только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.



5) **Сохранить подпись в отдельном файле;**

Если установить этот флаг, то будет создана отделенная подпись. Если не устанавливать флаг, будет сформирована совмещенная подпись.

6) **Удалить исходный файл после выполнения операции;**

Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции.

7) **Уровень безопасного удаления**

Подробнее о настройке параметров уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

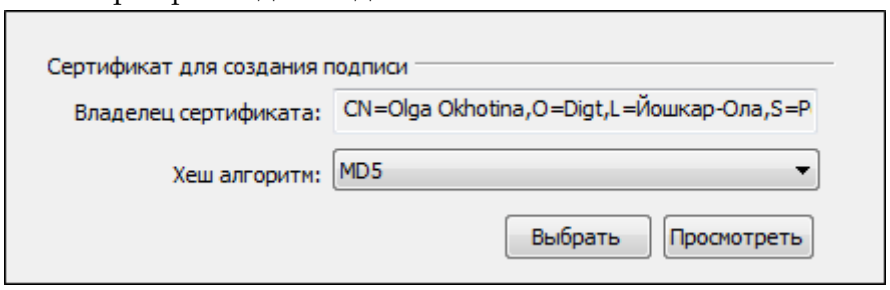
8) **Включить время создания подписи;**

При установке флага - в файл подписи будет включено время подписи.

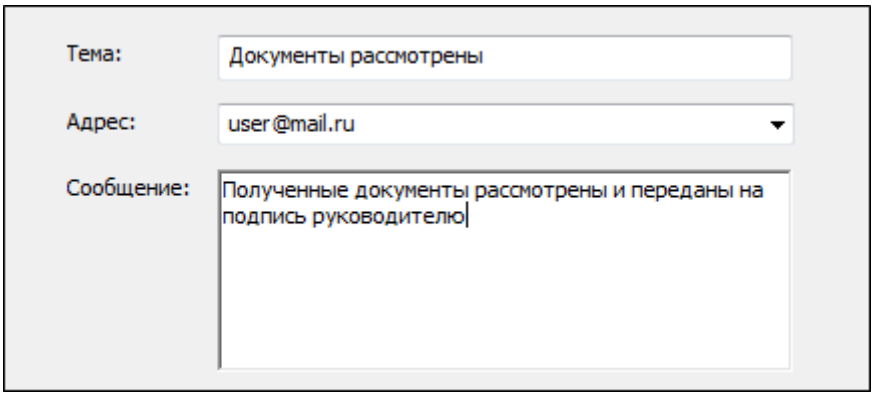
9) Флаги **Включить штамп времени на подписываемые данные и Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.
10) Флаг **Включить в подпись доказательства подлинности** доступен только при установленной лицензии на «КриптоАРМ СтандартPRO».

Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

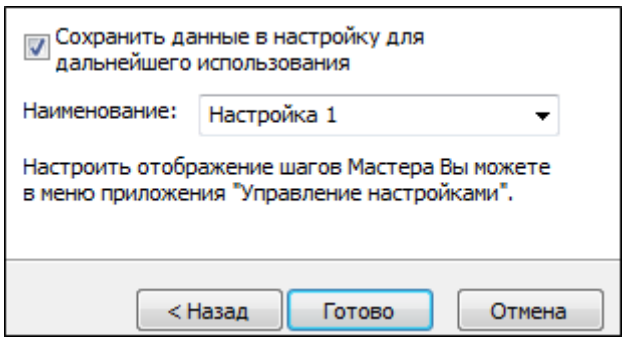
5. Если был установлен флаг **Включить штамп времени на подписываемые данные**, на следующем шаге укажите параметры Службы штампов времени.
6. Укажите личный сертификат для создания ЭП.



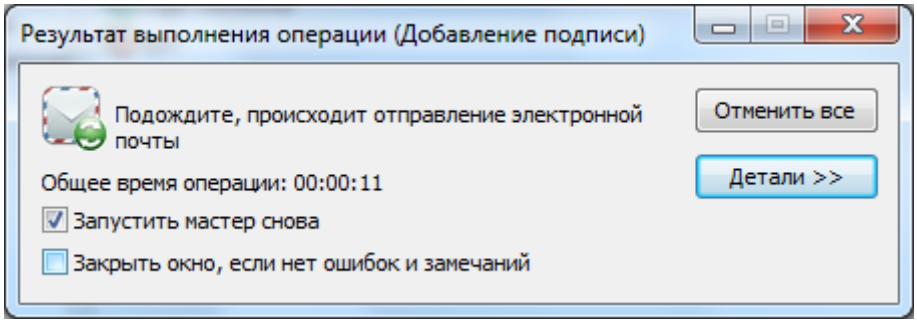
7. Для доступа к выбранному ключевому контейнеру (ГОСТ сертификата) введите пароль.
8. Для отправки подписанных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:



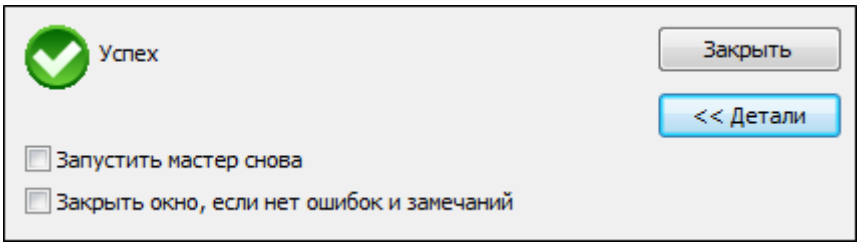
9. После сбора данных для создания ЭП возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Указанные параметры ЭП можно сохранить в настройку в качестве шаблона для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



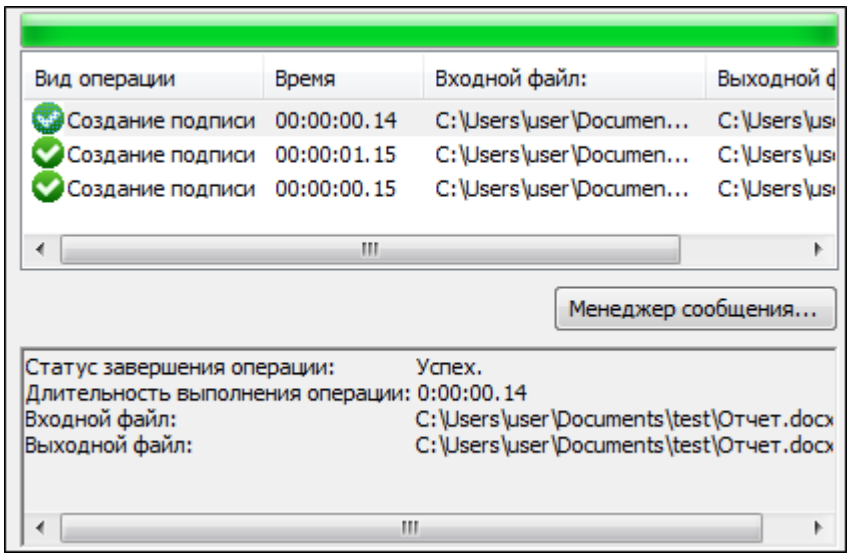
10. Начнется процесс подписи файла. Остановить процесс можно, нажав на кнопку **Отмена**.
11. При отправке подписанных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.



12. Сформированный файл ЭП по умолчанию будет сохранен в тот же каталог, в котором находится файл с исходными данными. Имя файла ЭП совпадает с именем подписываемого файла, дополненным расширением (расширение соответствует выбранному выходному формату). Если файл с таким именем уже существует, сохраните его под другим именем, например.
13. После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах создания подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали**.

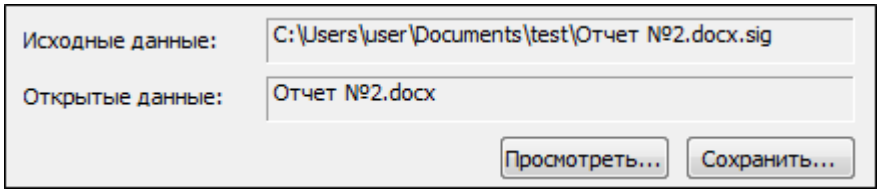


Если вы хотите просмотреть информацию об ЭП и сертификате подписчика, выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.



Откроется окно **Управление подписанными данными,** в котором вы можете:

1) Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).



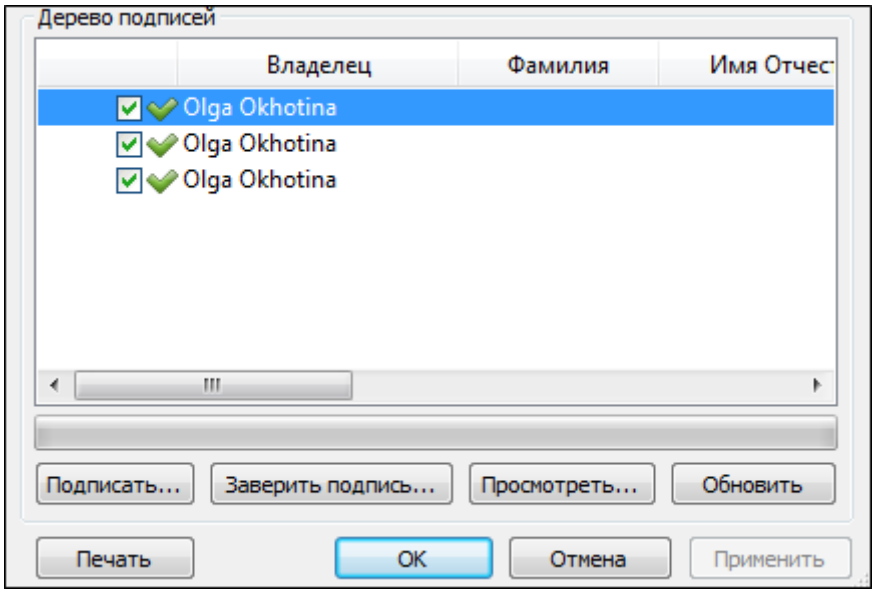
2) Просмотреть следующую информацию (кнопка **Просмотреть**):

- о добавленной к файлу электронной подписи
- о сертификате, с помощью которого был подписан файл, и его статусе
- о штампах времени на подпись и подписываемые данных

3) Добавить подпись.

4) Заверить подпись(обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя)

5) Распечатать информацию (кнопка **Печать**) о ЭП - в новом окне браузера MS IE будет сформирована печатная форма с информацией о подписи.



8.8.3 Добавление соподписи (параллельной подписи)

Программа «КриптоАРМ» позволяет добавлять электронные подписи к уже подписанному файлу. Такой вариант подписи используется, когда необходимо подписать файл нескольким пользователям (например, при согласовании документа сотрудниками одного отдела). При этом соподпись и первичная подпись будут иметь равный статус (равнозначны).

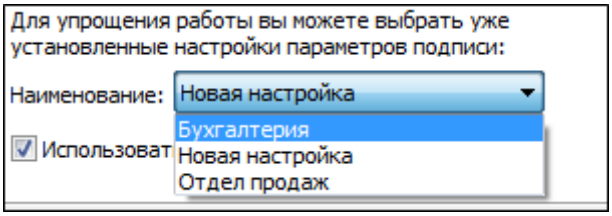
С помощью программы «КриптоАРМ» вы можете добавить электронную подпись к отдельному подписанному файлу или к папке подписанных файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными).

Добавить подпись к подписанному файлу (создать соподпись) вы можете через:

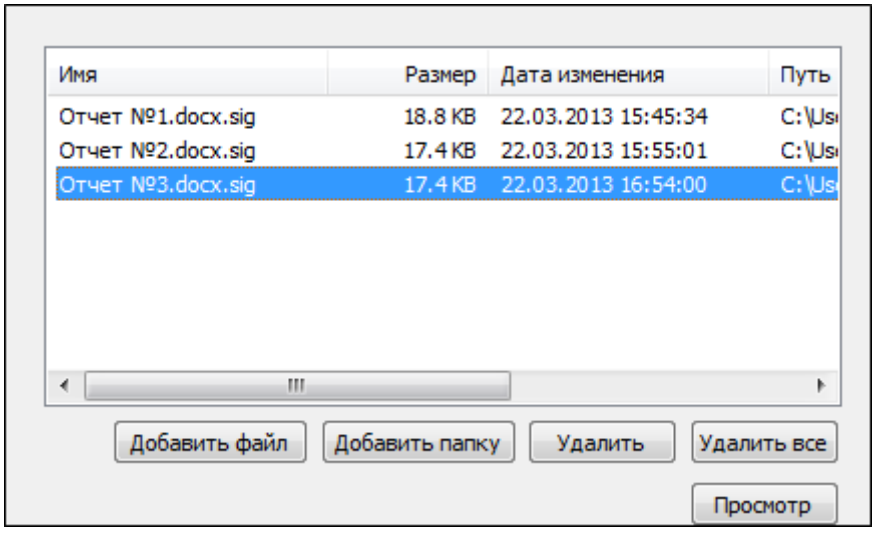
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Добавить подпись**. Далее следуйте рекомендациям Помощника по выполнению операции:

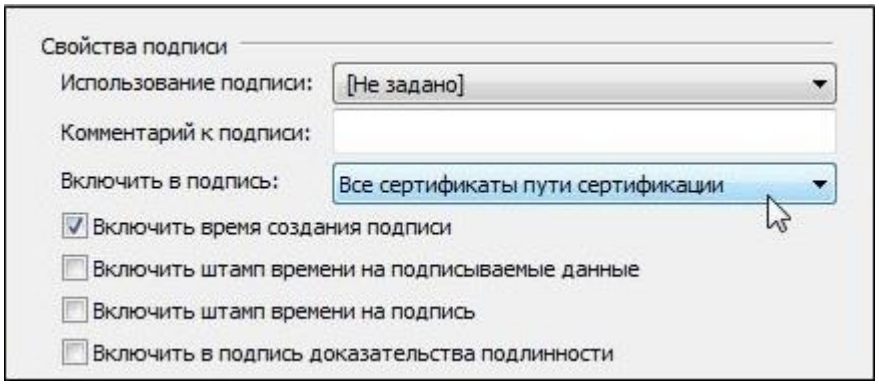
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек создания подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки **Добавить папку** и **Добавить файл** соответственно):



3. В окне **Параметры подписи** введите необходимые свойства добавляемой подписи.



1) **Использование подписи;**

Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

2) **Комментарий к подписи;**

Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

3) **Включить в подпись:**

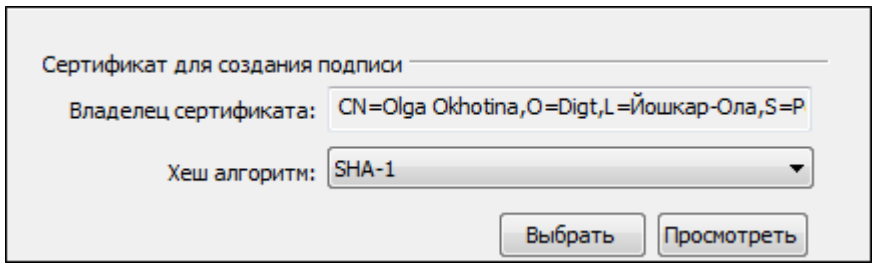
- только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.

4) Опции **Включить штамп времени на подписываемые данные и Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.

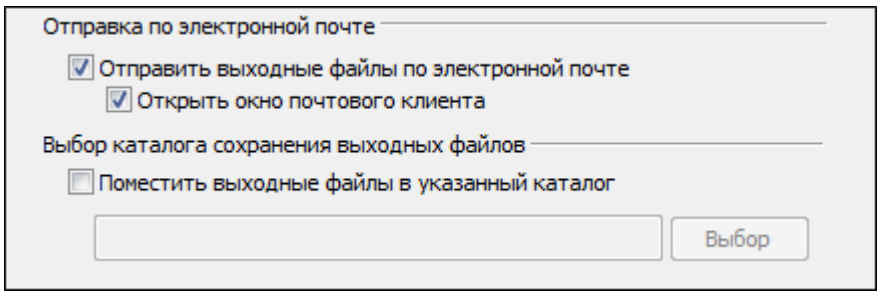
5) Опция **Включить в подпись доказательства подлинности** доступна только при установленной лицензии на «КриптоАРМ СтандартPRO».

Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

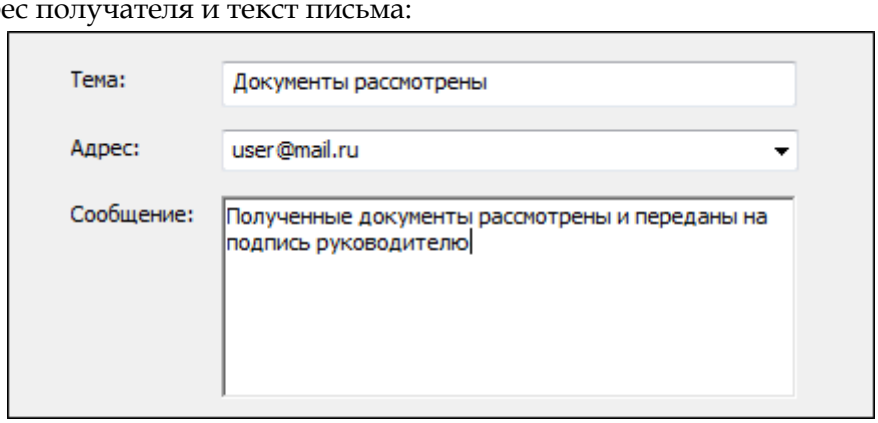
3. Далее выберите личный сертификат, который будете использовать для создания дополнительной ЭП.



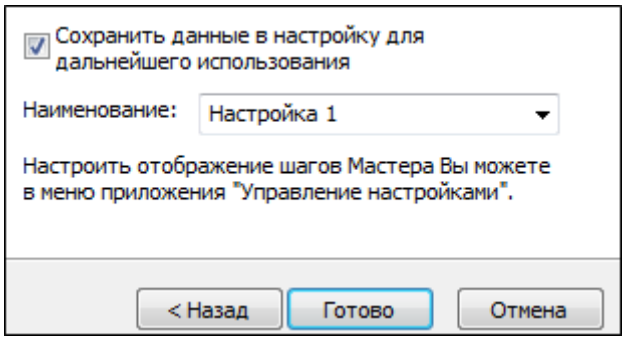
В этом же окне укажите, будете ли вы отправлять выходные файлы по электронной почте:



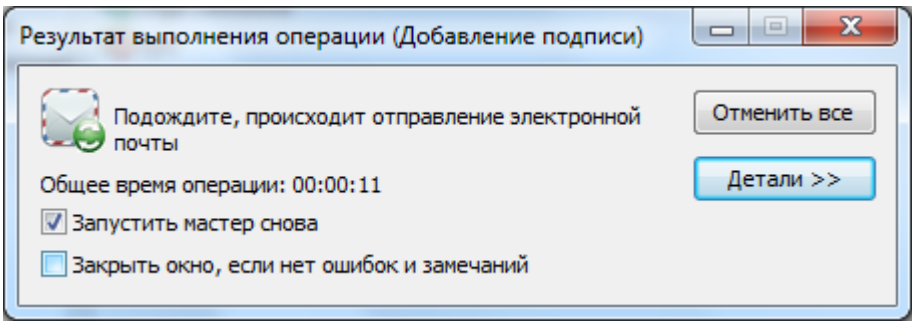
4. Для отправки подписанных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:



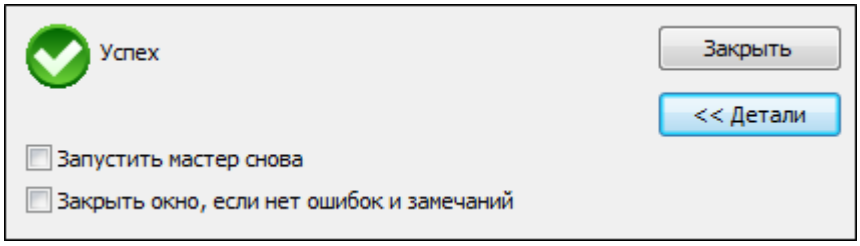
5. Если на ранее вы установили флаг **Включить штамп времени на подписываемые данные**, в следующем окне укажите параметры Службы штампов времени.
6. После сбора данных для добавления подписи возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Для продолжения нажмите на кнопку **Готово**.
   Указанные параметры добавления ЭП можно сохранить в настройку в качестве шаблона для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



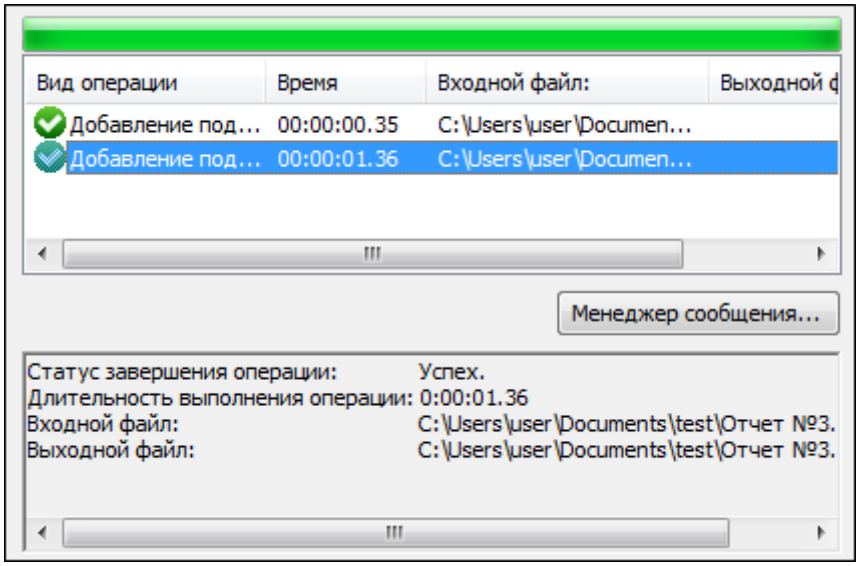
7. Данные будут подписаны с использованием вашего личного сертификата. Начнется процесс подписи файла. Вы можете прервать его, нажав на кнопку **Отмена**.
8. При отправке подписанных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.



9. После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах добавления подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите на кнопку **Детали**:

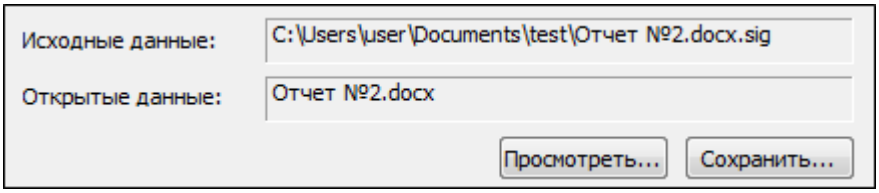


Если вы хотите просмотреть **Дерево подписей**, выделите строчку с операцией и нажмите на кнопку **Менеджер сообщения**. Откроется окно **Управление подписанными данными**, которое содержит дерево подписей:



В окне **Управление подписанными данными** вы можете, выполнить следующие операции:

1) Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**);

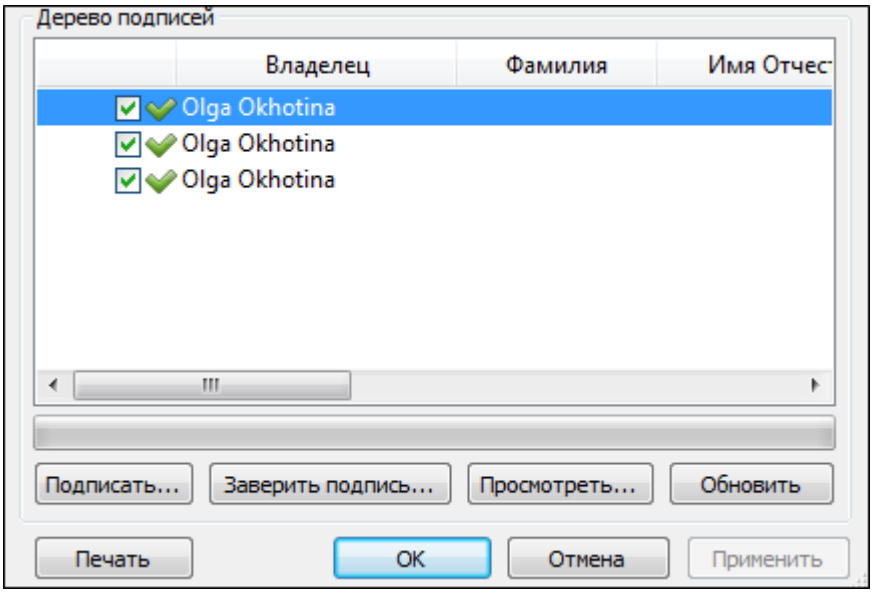


2) Просмотреть и распечатать информацию (кнопка **Просмотреть**).

- о добавленной к файлу электронной подписи;
- о сертификате, с помощью которого был подписан файл, и его статусе;
- о штампах времени на подпись и подписываемые данных;

3) Добавить подпись к уже имеющимся.

4) Добавить заверяющую подпись (обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя).



8.8.4 Добавление заверяющей подписи

Программа «КриптоАРМ» позволяет заверить подпись другой электронной подписью (создать цепочку электронных подписей). В этом случае каждая следующая ЭП подписывает ту ЭП, которой первоначально был подписан файл.

Такой вариант подписи ("заверяющая подпись") используется, когда необходимо заверить исходную подпись файла одной или несколькими электронными подписями других должностных лиц. Цепочка подписей может состоять из 2 уровней: первичная подпись и заверяющие подписи над ней.

Следует помнить, что для проверки подписей, составляющих цепочку, необходимо, чтобы у адресата имелись в наличии корневые сертификаты, подтверждающие подлинность личных сертификатов пользователей, подписавших файл.

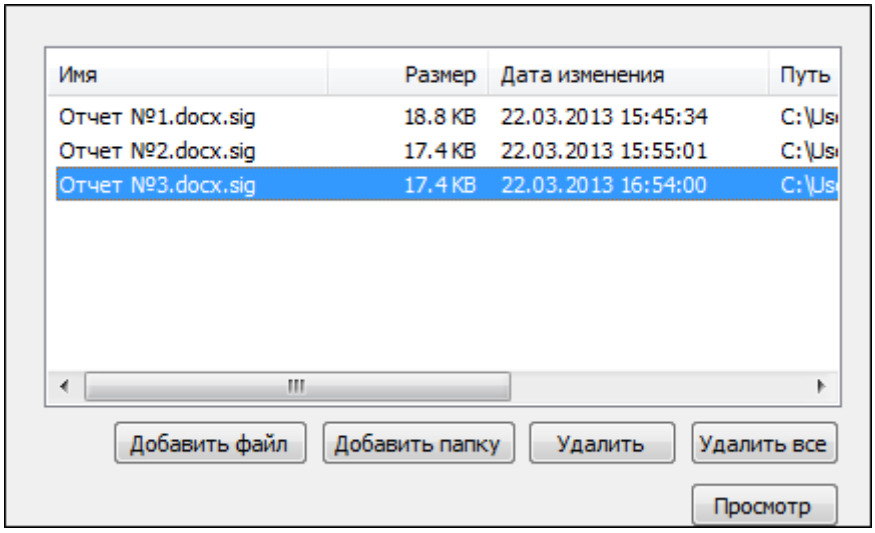
С помощью программы «КриптоАРМ» вы можете заверить своей электронной подписью отдельный подписанный файл или папки подписанных файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными).

Выполнять операции заверения подписи можно для отдельного файла и группы файлов через:

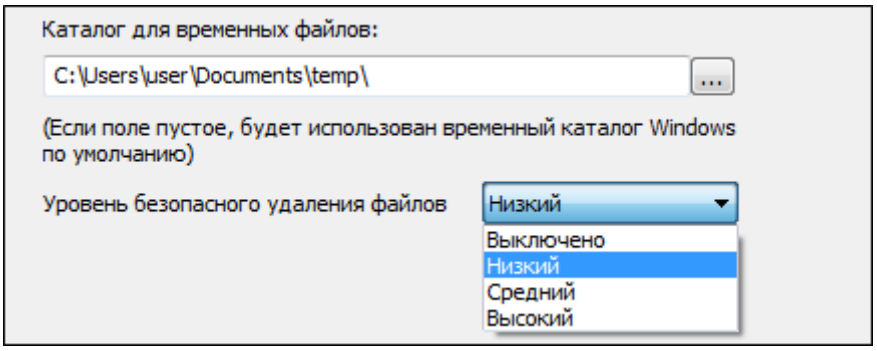
- главное окно
- значок на панели задач
- контекстное меню файла

Для того чтобы заверить подпись файла, выберите пункт меню **Заверить подпись**. Далее следуйте рекомендациям Помощника по выполнению операции:

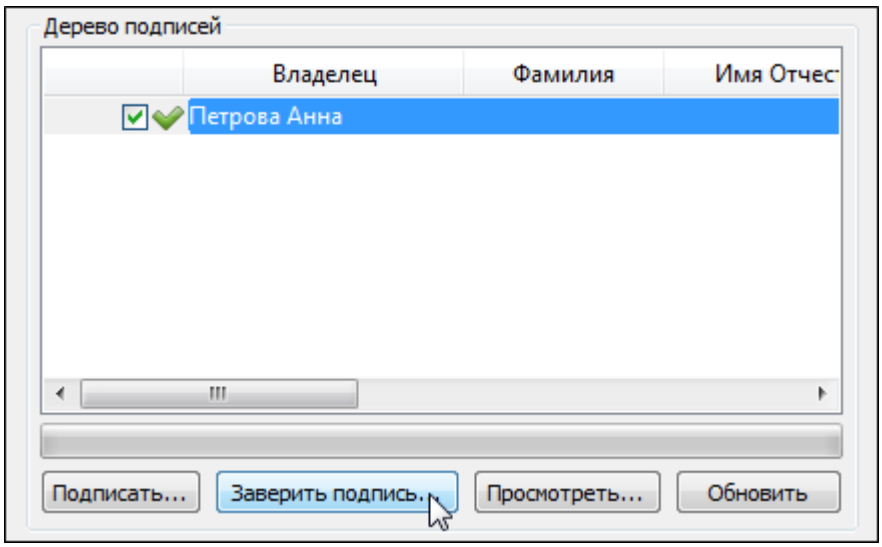
1. Выберите папку с файлами или отдельный файл, которые необходимо заверить электронной подписью (кнопки **Добавить папку** и **Добавить файл** соответственно).



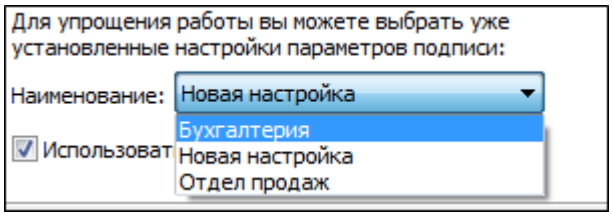
2. Установите параметры безопасности и удаления файлов.



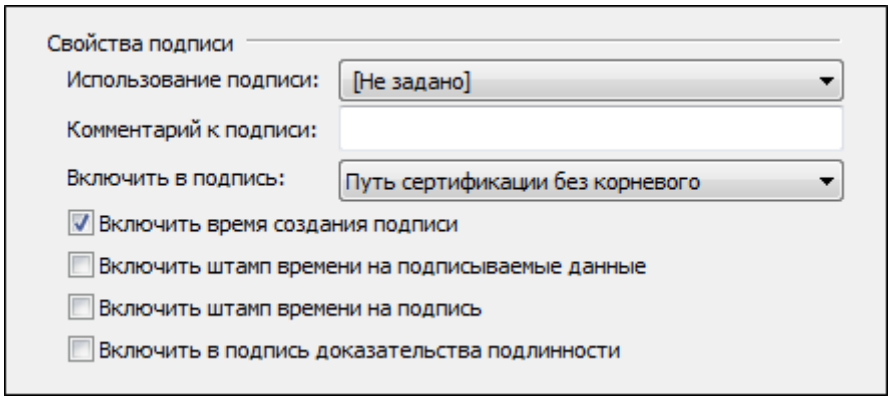
3. После сбора данных для создания заверяющей подписи возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Для продолжения нажмите на кнопку **Готово**.
4. Откроется окно **Управление подписанными данными** (для каждого файла, подпись которого необходимо заверить, откроется свое окно)**.** В поле **Дерево подписей** выберите подпись, которую необходимо заверить, и нажмите на кнопку **Заверить подпись**.



5. Откроется помощник по созданию ЭП. Для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для создания подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**:



6. В окне параметры подписи введите необходимые свойства добавляемой подписи



1) **Использование подписи;**

Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

2) **Комментарий к подписи;**

Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

3) **Включить в подпись:**

- только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;

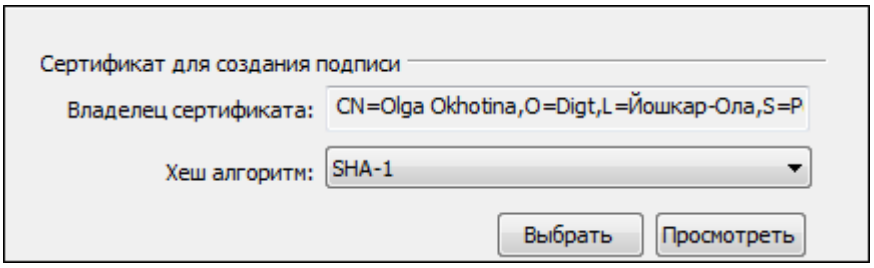
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.

4) Флаги **Включить штамп времени на подписываемые данные** и **Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.

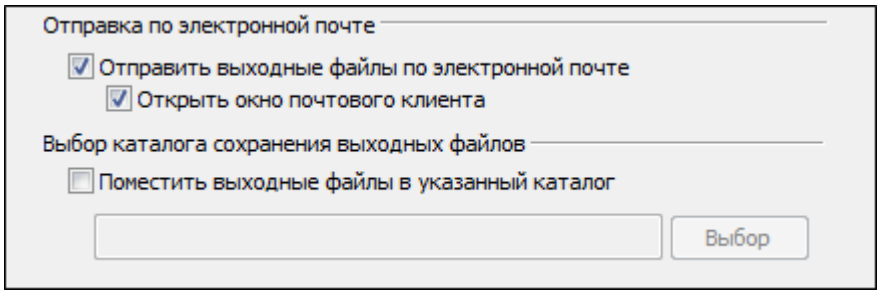
5) Флаг **Включить в подпись доказательства подлинности** доступен только при установленной лицензии на «КриптоАРМ СтандартPRO».

Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

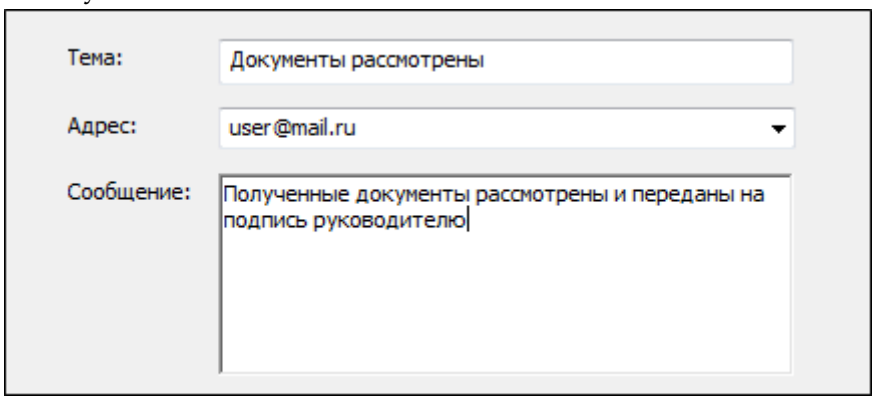
7. Если на ранее вы установили флаг **Включить штамп времени на подписываемые данные**, в следующем окне укажите параметры Службы штампов времени.
8. Далее выберите личный сертификат, который будете использовать для создания ЭП (кнопка **Выбрать**).



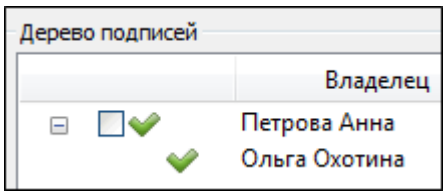
В этом же окне укажите, будете ли вы отправлять выходные файлы по электронной почте:



9. Для отправки подписанных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:

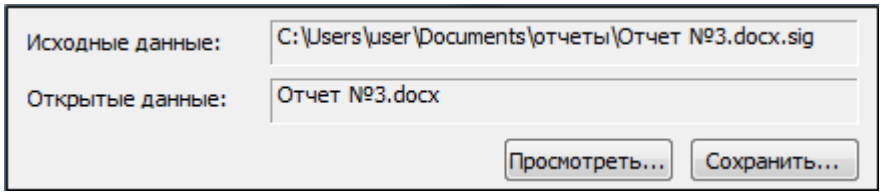


10. Данные для заверения подписи собраны. Нажмите на кнопку **Готово**.
11. Данные будут подписаны. В результате операции в окне **Управление подписанными данными** появится значок заверяющей подписи (в иерархии заверяющая подпись будет подписью второго уровня).



В окне **Управление подписанными данными** вы можете:

1) Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).

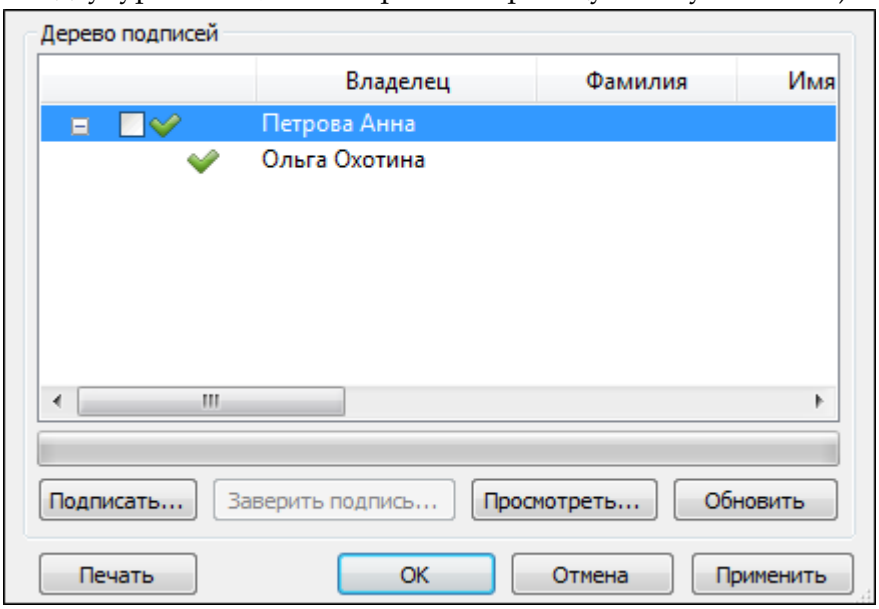


2) Просмотреть информацию (кнопка **Просмотреть**)

- о заверяющей ЭП (атрибуты и алгоритмы подписи);
- о сертификате, с помощью которого был подписан файл, и его статусе;
- о штампах времени на подпись и подписываемые данных.

3) Добавить соподпись.

4) Заверить первичную подпись еще одной заверяющей (обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя).



8.8.5 Проверка электронной подписи

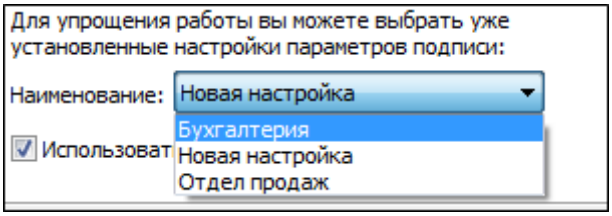
С помощью программы «КриптоАРМ» вы можете проверить корректность электронной подписи отдельного файла или папки файлов (при этом будет проверена подпись каждого файла, входящего в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными).

Проверить корректность электронной подписи вы можете через:

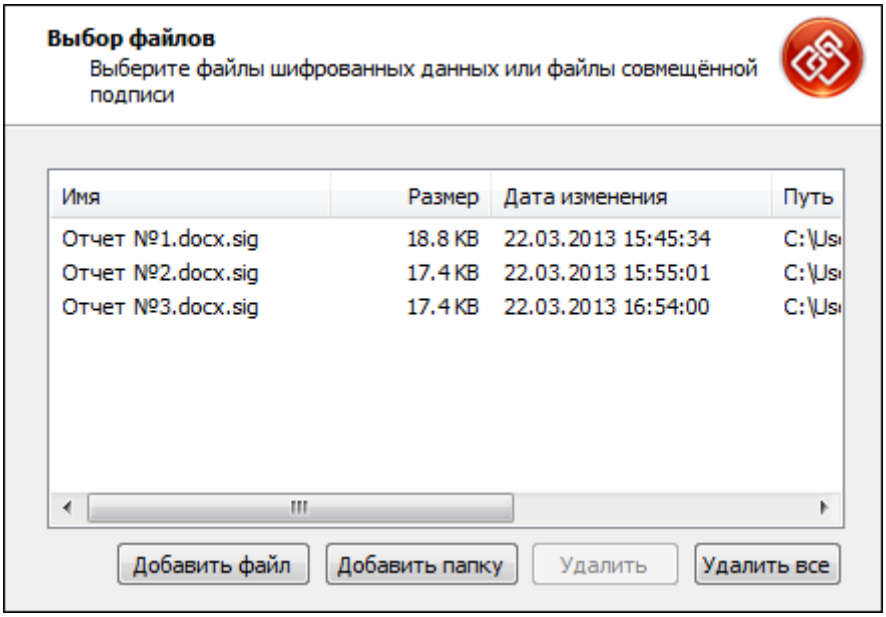
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Проверить подпись**. Далее следуйте указаниям Помощника проверки электронной подписи:

1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



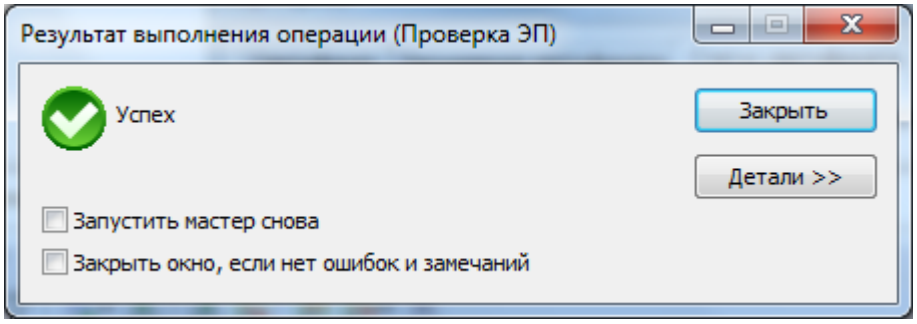
2. Выберите файл или папку файлов, подписанных ЭП, корректность которых необходимо проверить (кнопки **Добавить папку** и **Добавить файл**).



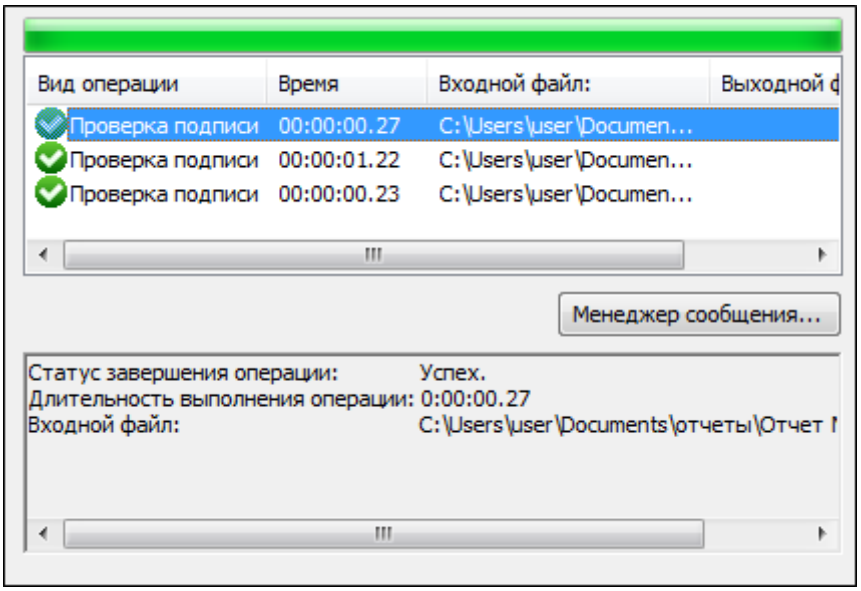
3. После сбора данных для снятия и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения операции нажмите на кнопку **Готово**.

   Если в файле подписи содержится одна подпись (нет дополнительных и/ или заверяющих), то проверяется корректность ЭП и действительность сертификата отправителя. Если в файле ЭП содержится более одной подписи, то проверяется корректность каждой подписи в коллекции.

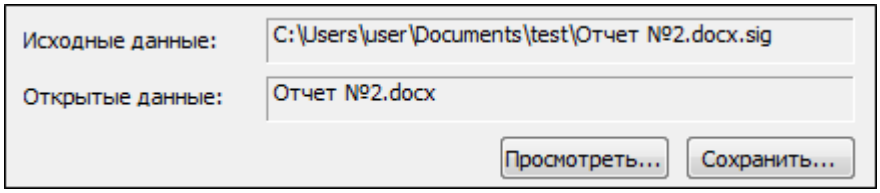
4. Откроется окно **Результат выполнения операции**, в котором отобразится статус операции. Если одна или несколько подписей не действительны, это будет отражено в статусе. Чтобы просмотреть детальную информацию о результатах проверки подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите на кнопку **Детали.**



5. Если вы хотите просмотреть информацию о проверяемой ЭП и сертификате подписчика, выделите необходимую запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**. Откроется окно Управление подписанными данными.

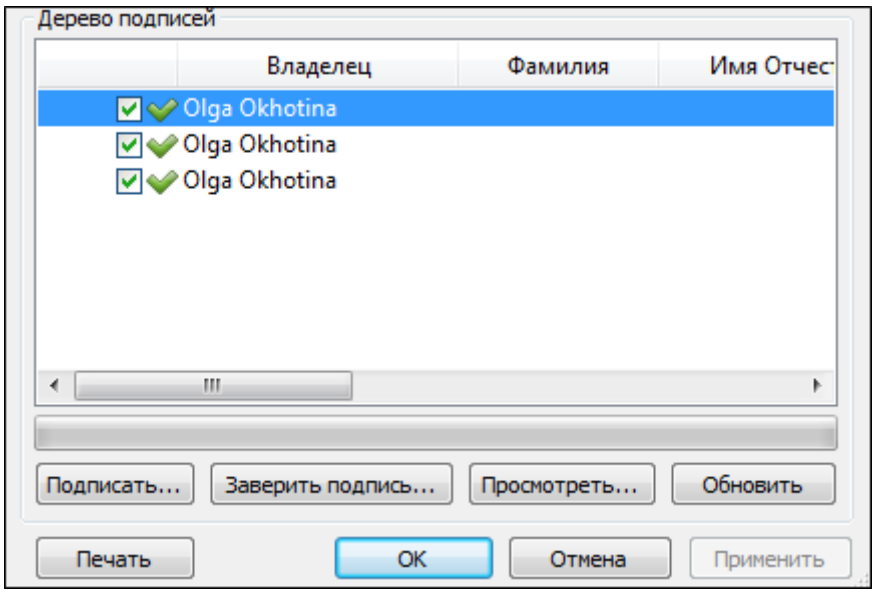


Вы можете просмотреть исходный файл и сохранить его по указанному пути (кнопки **Просмотреть** и **Сохранить** напротив поля **Открытые данные**).



В случае, если просматриваемый документ является документом Microsoft Word или Microsoft Excel, и на компьютере установлен пакет Microsoft Office, можно настроить добавление информации о подписи в конец документа (в случае с Microsoft Excel на отдельный лист). Включить добавление информации о подписи можно в выбранной по умолчанию настройке на странице общих параметров.

Отчет о проверке подписи можно просмотреть, выбрав запись в поле **Дерево подписей** и нажав на кнопку **Просмотреть**. Откроется окно с информацией о подписи, сертификате и его статусе.



8.8.6 Снятие и проверка подписи

При проверке совмещенной подписи сначала выполняется снятие подписи с данных и сохранение подписанных данных в отдельный файл, а после этого - собственно проверка корректности подписи.

С помощью программы «КриптоАРМ» вы можете снять и проверить корректность ЭП отдельного файла или папки файлов (при этом будет снята и проверена подпись каждого файла, входящего в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными).

Снять и проверить корректность электронной подписи вы можете через:

- главное окно
- значок на панели задач
- контекстное меню

Для того чтобы снять и проверить корректность ЭП, выберите пункт меню **Снять и проверить**. Шаги Помощника данной операции соответствуют шагам Помощника проверки подписи.

8.9 Шифрование данных

Шифрование — это преобразование данных в вид, недоступный для чтения без соответствующей информации (ключа шифрования). Задача состоит в том, чтобы обеспечить конфиденциальность, скрыв информацию от лиц, которым она не предназначена, даже если они имеют доступ к зашифрованным данным.

Для того чтобы зашифровать файл, вам потребуется открытый ключ получателя зашифрованных данных. Расшифровать данные получатель сможет, используя свой закрытый ключ.

С помощью программы «КриптоАРМ» вы можете зашифровать отдельный файл или папку файлов (при этом будет зашифрован отдельно каждый файл, входящий в указанную папку. Зашифрованные файлы автоматически сохраняются в папку с исходными данными).

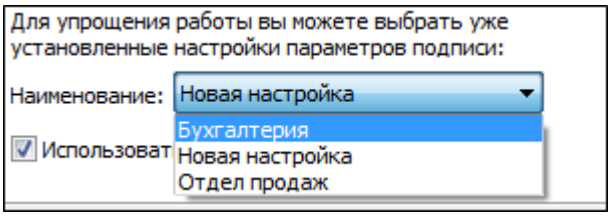
8.9.1 Шифрование

Зашифровать файл вы можете через:

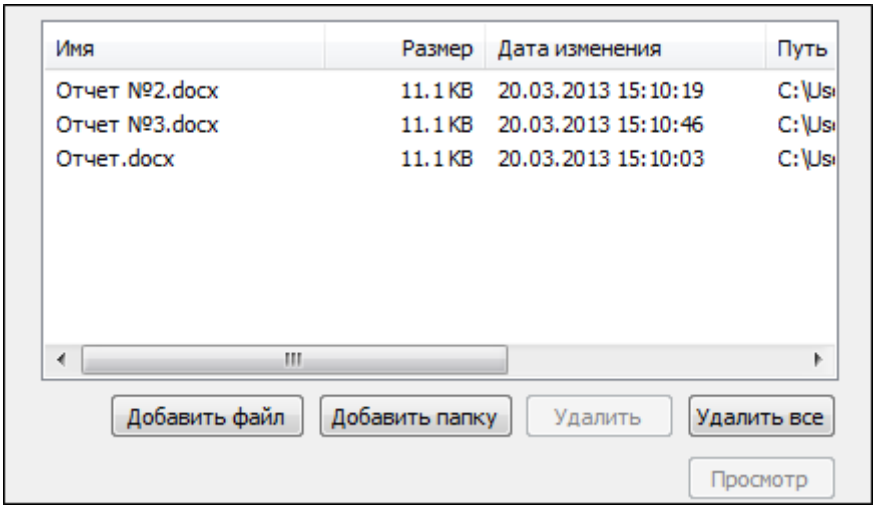
- главное окно
- значок на панели задач
- контекстное меню файла

Для того чтобы зашифровать файл, следуйте рекомендациям Мастера выполнения операции:

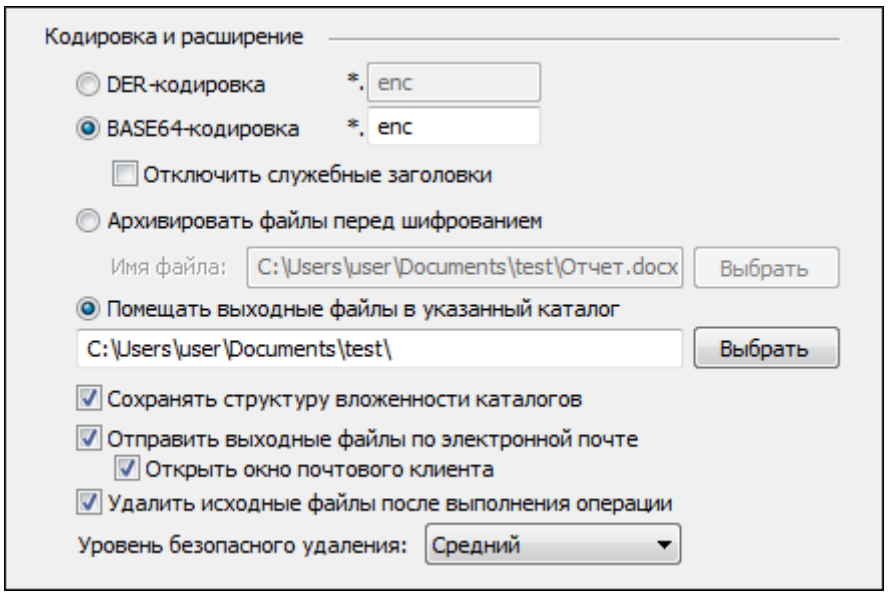
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для шифрования файлов. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию.**



2. Выберите папку с файлами или отдельный файл, которые необходимо зашифровать (кнопки **Добавить папку** и **Добавить файл** соответственно).



3. В открывшемся окне укажите настройки для выходного формата файла.



1) **Кодировка и расширение;**

- DER encoded binary X.509
- Base64 encoded X.509.Для этого варианта кодирования вы можете указать флаг **Отключить служебные заголовки.**

Расширения зашифрованного файла *.enc, *.p7m, *.pem.

2) **Архивировать файлы перед шифрованием;**

В строке **Имя файла** укажите путь до архива и имя создаваемого архива.

3) **Помещать выходные файлы в указанный каталоге;**

Если выбрать этот режим и оставить поле ввода пути к каталогу не заполненным, то выходные файлы будут формироваться в каталоге входных файлов.

4) **Сохранять структуру вложенности каталогов;**

5) **Отправить выходные файлы по электронной почте;**

6) **Удалить исходный файл после выполнения операции;**

Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции.

7) **Уровень безопасного удаления**

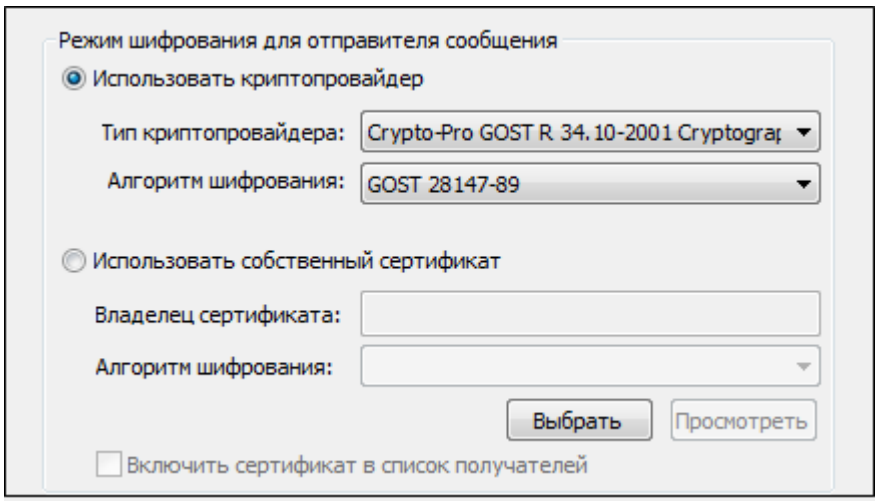
Подробнее о настройке параметров уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

4. В окне **Свойства шифрования в**ыберите режим шифрования данных.

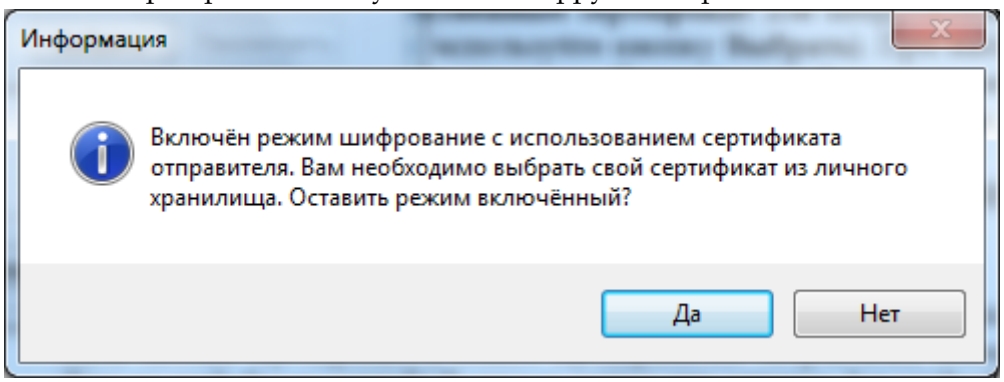
Для этого поставьте переключатель напротив соответствующей строки:

- **Использовать криптопровайдер** (в этом случае в выпадающем списке выберите необходимый тип криптопровайдера и алгоритм шифрования)

*В случае использования криптопровайдера «**SafeSign CSP Version 1.0**» рабочим алгоритмом шифрования является только RC4.*

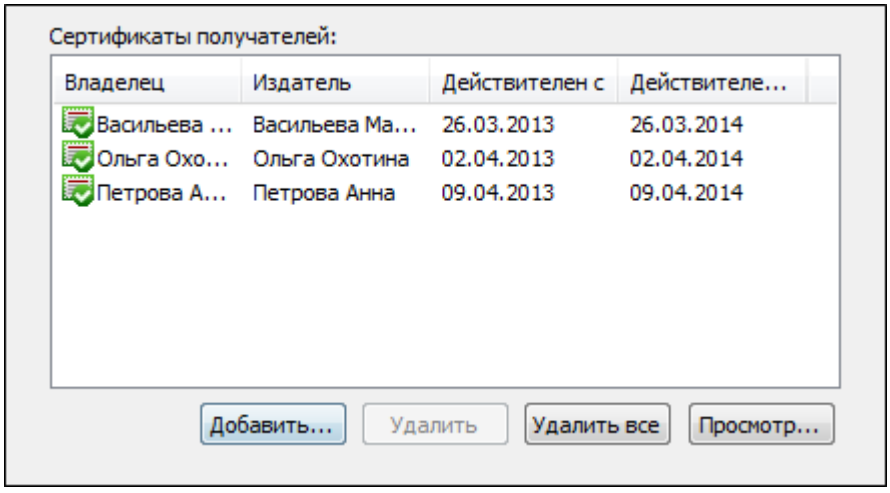


- **Использовать собственный сертификат** для шифрования (Для выбора личного сертификата используйте кнопку **Выбрать)**. При выборе личного сертификата проверяется его статус. Личный сертификат автоматически добавляется в список сертификатов получателей шифруемого файла.



Подробнее о настройке параметров шифрования вы можете прочитать в разделе *Настройки операции шифрования*.

3. На следующем шаге выберите сертификаты получателей шифруемого файла, используя кнопку **Добавить**.

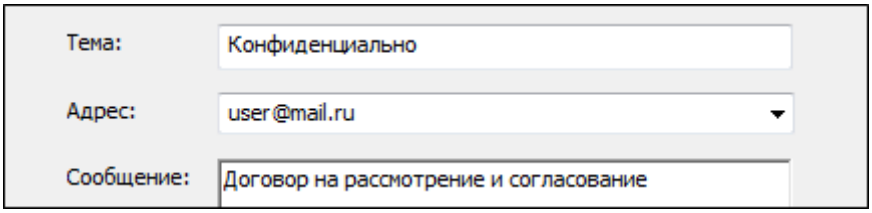


Чтобы иметь возможность расшифровать зашифрованный вами файл, вы должны добавить личный сертификат в список сертификатов получателей зашифрованного файла.

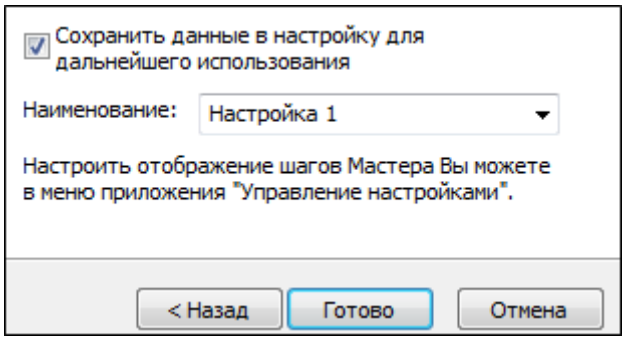
Если на предыдущем шаге вы включили режим, при котором для шифрования будет использоваться ваш личный сертификат, на шаге выбора сертификатов получателей он автоматически будет занесен в список.

Обратите внимание, для шифрования необходимо, чтобы ключи отправителя и получателя могли быть использованы для шифрования данных.

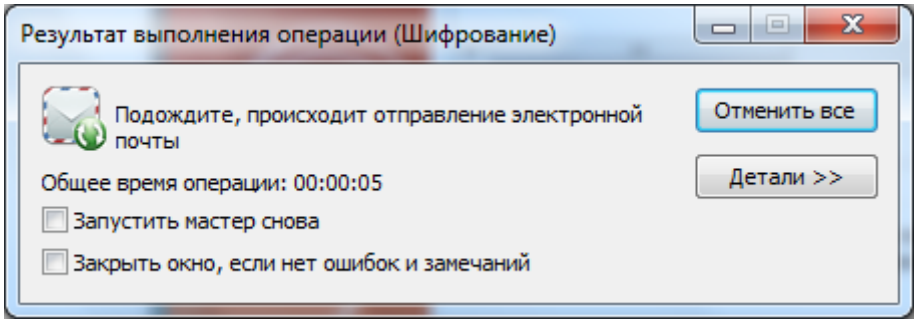
4. Для отправки зашифрованных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:



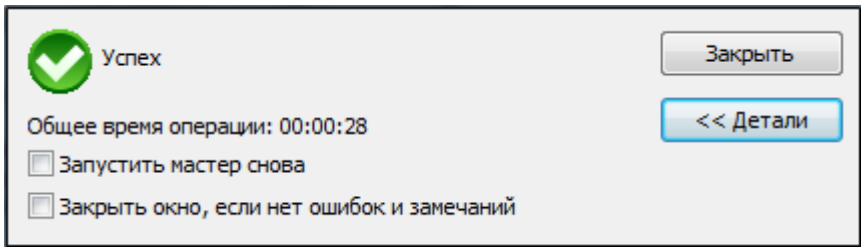
5. После завершения сбора параметров для выполнения шифрования возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был зашифрован файл и сертификат получателя (-ей). Для продолжения нажмите на кнопку **Готово**.
   Введенные в Мастер шифрования данные можно сохранить в настройку для дальнейшего использования. Для этого поставьте галочку в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



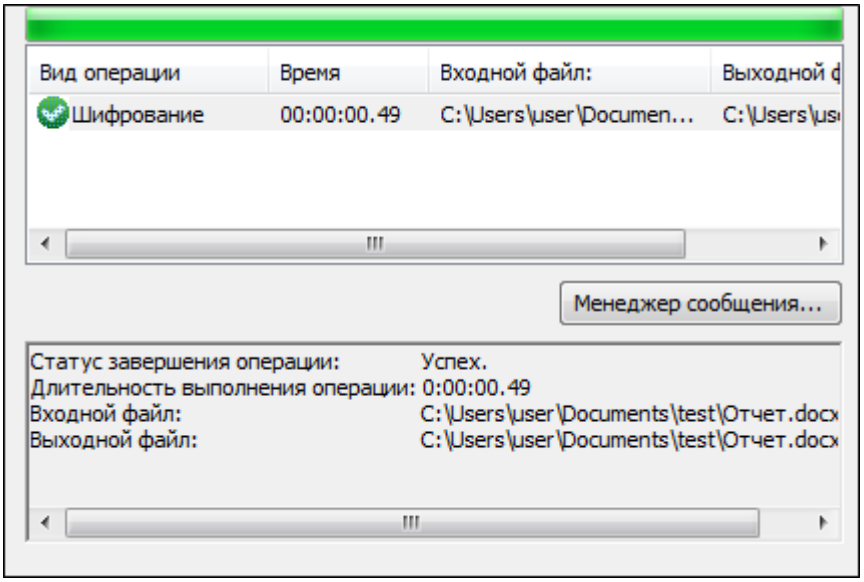
6. Начнется процесс шифрования данных. Вы можете прервать его, нажав на кнопку **Отмена**.
7. При отправке зашифрованных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.



8. Далее возникнет окно **Результат выполнения операции** со статусом завершения операции.

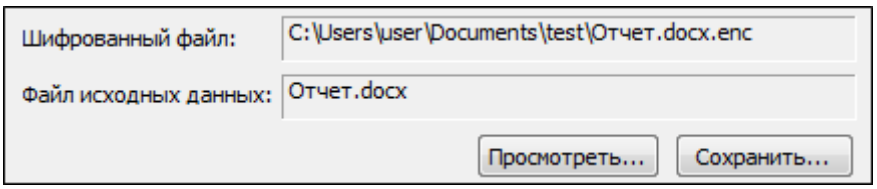


Чтобы просмотреть детальную информацию о результатах шифрования и используемых параметрах: имя исходного файла, имя выходного (зашифрованного) файла, статус операции, длительность выполнения операции, нажмите на кнопку **Детали.**

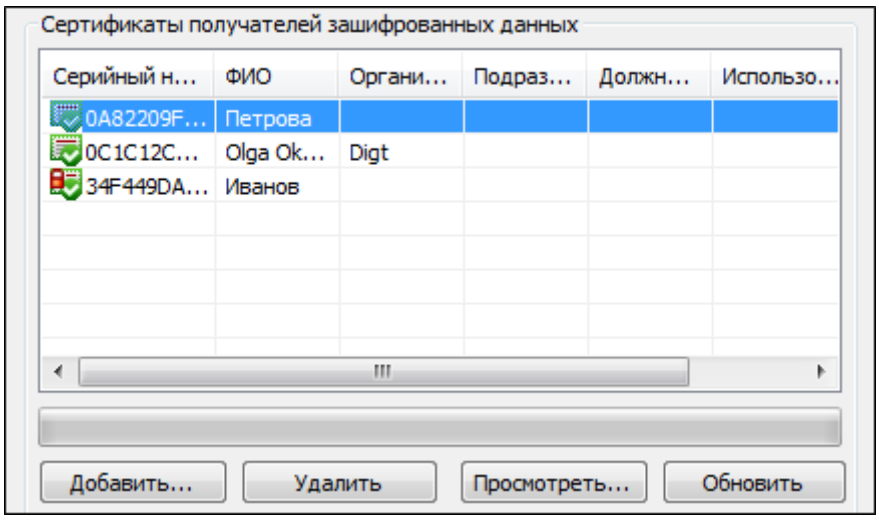


Вы можете отредактировать список получателей зашифрованных данных, просмотреть и сохранить исходные данные.

1. Выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.
2. Откроется окно **Управление шифрованными данными**, в котором вы можете:
    1) Просмотреть путь, по которому сохранен зашифрованный файл;
    2) Просмотреть зашифрованный файл (кнопка **Просмотреть** рядом со строкой **Файл исходных данных**);



    3) Сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);
    4) Просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**);



Сертификат расшифрования данных отмечается значком - . Сертификатом расшифрования становится первый из списка сертификат получателей, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками.

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно).

При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы в адрес измененного списка получателей.

8.9.2 Расшифрование

С помощью программы «КриптоАРМ» вы можете расшифровать:

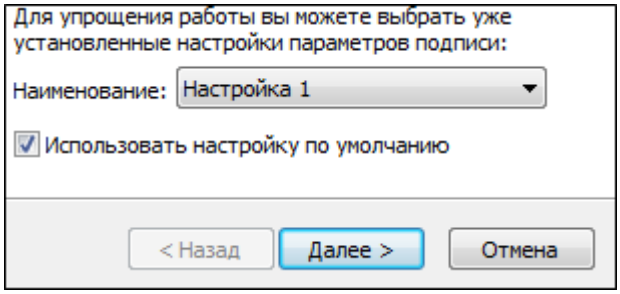
- отдельный файл;
- папку файлов (при этом будет расшифрован каждый файл, входящий в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными).

Расшифровать данные вы можете через:

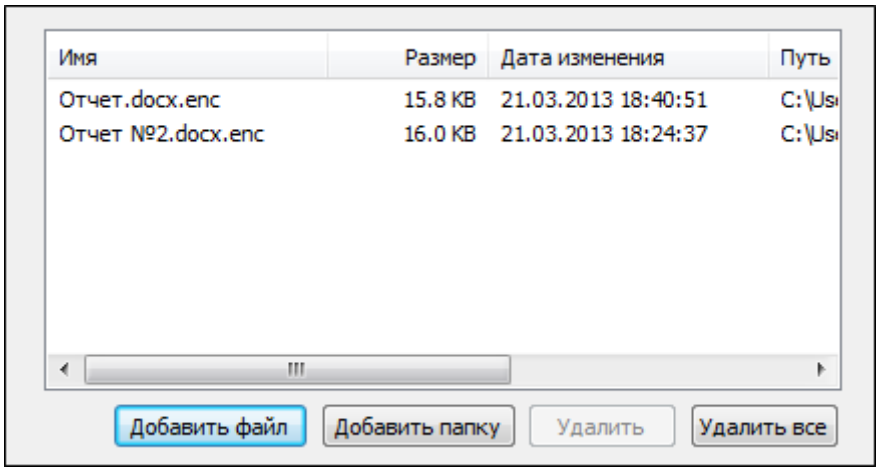
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Расшифровать**. Далее следуйте рекомендациям Помощника по выполнению операции:

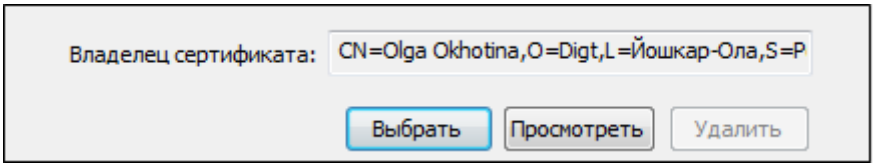
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек расшифрования файлов. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите файл или папку файлов, которые необходимо расшифровать (кнопки **Добавить папку** и **Добавить файл**). Также вы можете выбрать архив с файлами.

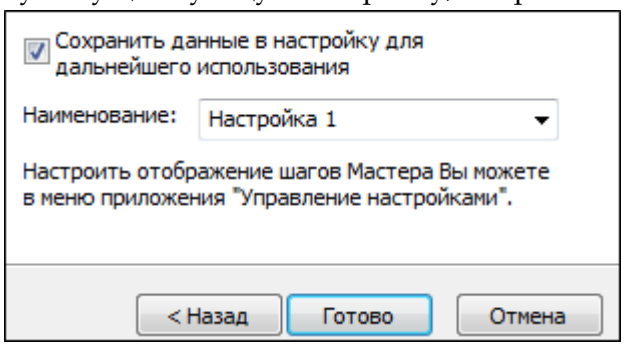


3. В следующем окне выберите предпочтительный сертификат расшифрования (кнопка **Выбрать**). Указанный сертификат вы можете просмотреть, нажав на кнопку **Просмотреть**.



4. После завершения сбора данных для расшифрования возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения нажмите на кнопку **Готово**.

   Указанные данные можно сохранить в настройку для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.

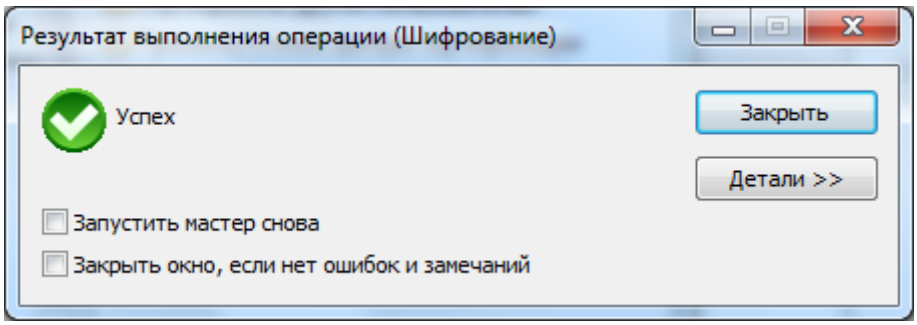


5. Начнется процесс расшифрования файла. Вы можете прервать его, нажав на кнопку **Отменить все.**

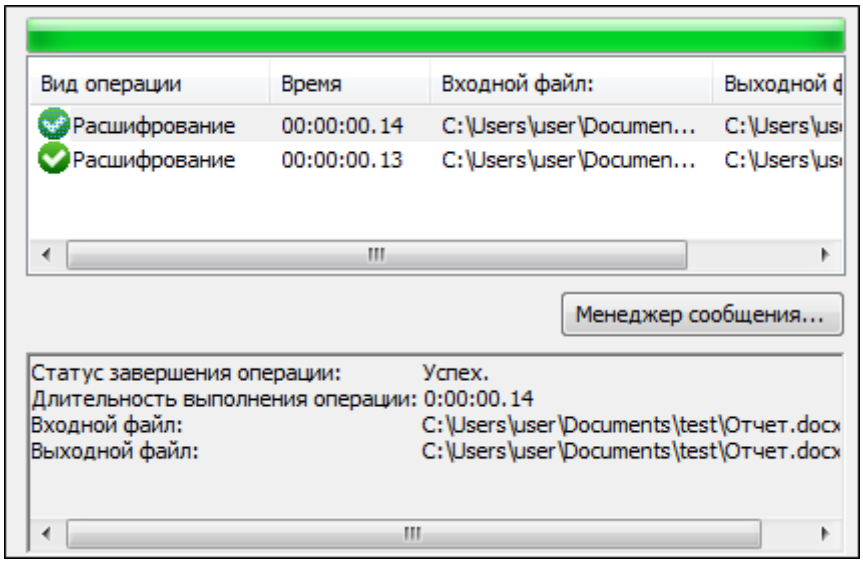
Данные будут расшифрованы и по умолчанию сохранены в тот же каталог, в котором находится исходный (зашифрованный) файл данных. При этом имя расшифрованного файла совпадает с именем зашифрованного файла, но не имеет расширения ***.enc**. Если файл с таким именем уже существует, сохраните его под другим именем.

Если сертификат ГОСТ, введите пароль доступа к нему.

После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах расшифрования и используемых параметрах: имя исходного файла, имя выходного (расшифрованного) файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали.**



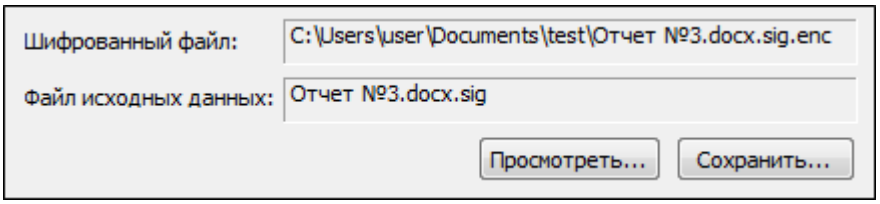
Если вы хотите просмотреть информацию о сертификате расшифрования и сертификатах получателей или изменить список получателей зашифрованных данных, выделите необходимую запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.



Откроется окно **Управление шифрованными данными**, в котором вы можете:

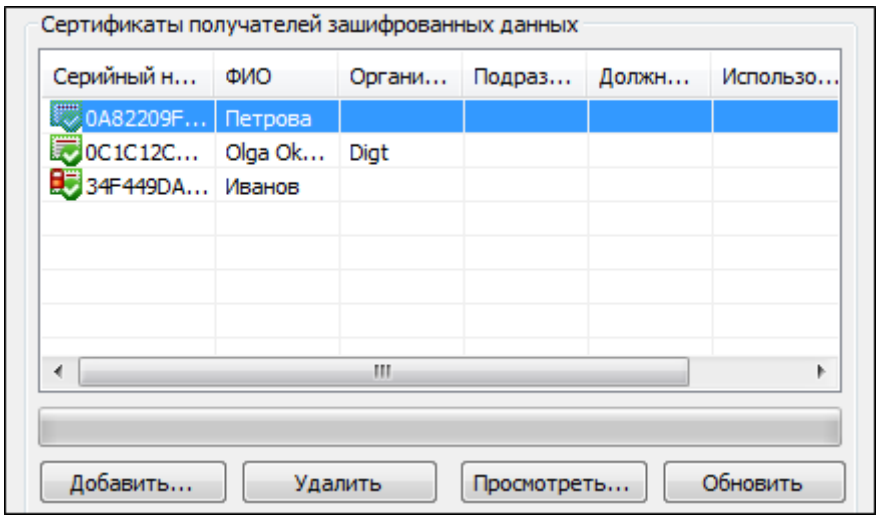
1) Просмотреть путь, по которому сохранен зашифрованный файл;

2) Просмотреть зашифрованный файл (кнопка **Просмотреть** напротив строки **Файл исходных данных**);



3) Сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);

4) Просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**).



Сертификат расшифрования данных отмечается значком - . Сертификатом расшифрования становится первый из списка сертификат получателя, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно). При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы в адрес измененного списка получателей.

8.10 Комбинированные операции

В главе **Комбинированные операции** вы найдете информацию о том,

- как зашифровать и подписать файл
- как расшифровать и проверить подпись файла

8.10.1 Создание подписи и шифрование

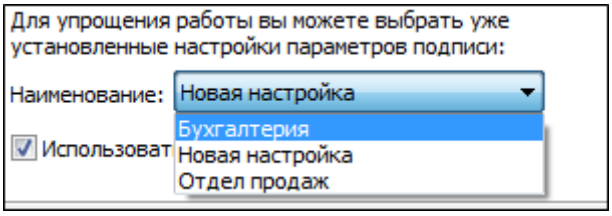
С помощью программы «КриптоАРМ» вы можете зашифровать и подписать отдельный файл или папку (при этом будет зашифрован и подписан отдельно каждый файл, входящий в указанную папку. Зашифрованные и подписанные файлы автоматически сохраняются в папку с исходными данными).

Подписать и зашифровать данные за одну операцию вы можете через:

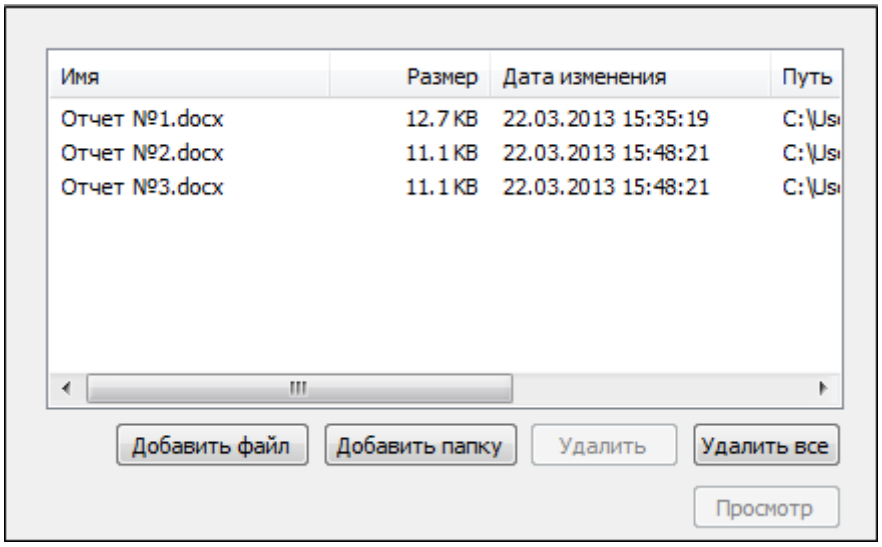
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Подписать и зашифровать**. Далее следуйте рекомендациям Мастера выполнения операции:

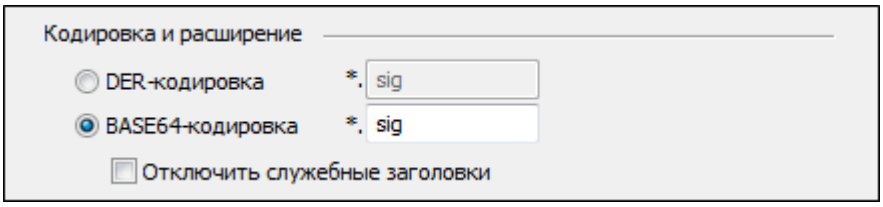
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи и шифрования. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, установите флаг в пункте **Использовать настройку по умолчанию**.



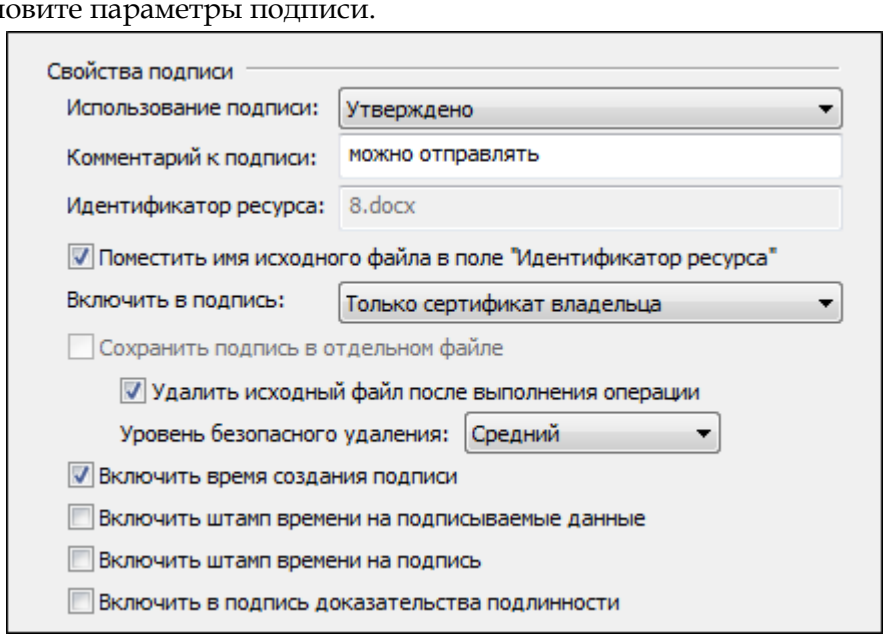
2. Выберите отдельный файл и папку с файлами, которые необходимо зашифровать и подписать (кнопки **Добавить файл** и **Добавить папку** соответственно).



3. Первым этапом укажите параметры для создания электронной подписи данных. Сначала укажите выходной формат файла подписи: кодировку и расширение выходного файла.
   - DER encoded binary X.509. Расширения подписанного файла *.sig, *.p7s.
   - Base64 encoded X.509.Для этого варианта кодирования вы можете указать флаг **Отключить служебные заголовки.** Расширения подписанного файла *.sig.



4. Далее установите параметры подписи.



1) **Использование подписи;**

Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

2) **Комментарий к подписи;**

Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

3) **Включить в подпись:**

- только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.

4) **Идентификатор ресурса;**

5) **Удалить исходный файл после выполнения операции;**

Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции.

6) **Уровень безопасного удаления**

Подробнее о настройках уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

7) **Включить время создания подписи;**

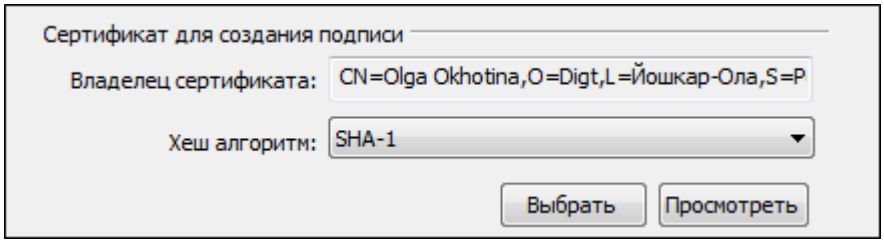
При установке флага - в файл подписи будет включено время подписи.

8) Флаги **Включить штамп времени на подписываемые данные и Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.

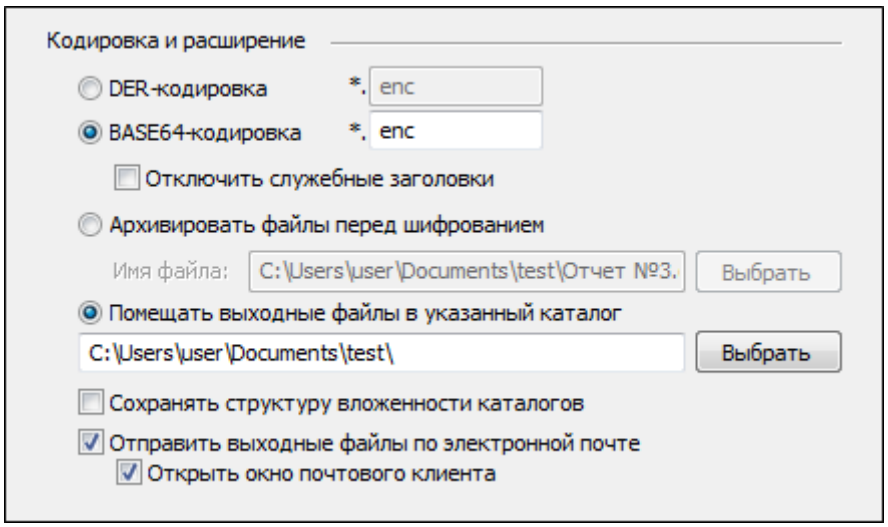
9) Флаг **Включить в подпись доказательства подлинности** доступен только при установленной лицензии на «КриптоАРМ СтандартPRO».

Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

5. Если был установлен флаг **Включить в подпись Штамп Времени**, в следующем окне укажите параметры Службы Штампов Времени.
6. Выберите личный сертификат для создания ЭП (кнопка **Выбрать**).



7. Для доступа к выбранному ключевому контейнеру (ГОСТ сертификата) введите пароль.
8. Вторым этапом укажите параметры для шифрования данных**.** Укажите настройки для выходного формата файла.



1) **Кодировка и расширение;**

- DER encoded binary X.509
- Base64 encoded X.509.Для этого варианта кодирования вы можете указать флаг **Отключить служебные заголовки.**
  Расширения зашифрованного файла *.enc**,** *.p7m, *.pem.

2) **Архивировать файлы перед шифрованием;**

В строке **Имя файла** укажите путь до архива и имя создаваемого архива.

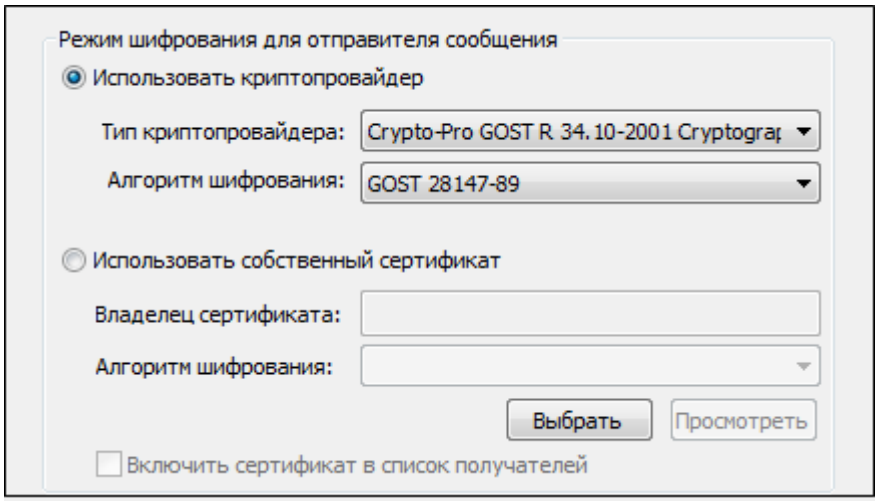
3) **Помещать выходные файлы в указанный каталог;**

Если выбрать этот режим и оставить поле ввода пути к каталогу не заполненным, то выходные файлы будут формироваться в каталоге входных файлов.

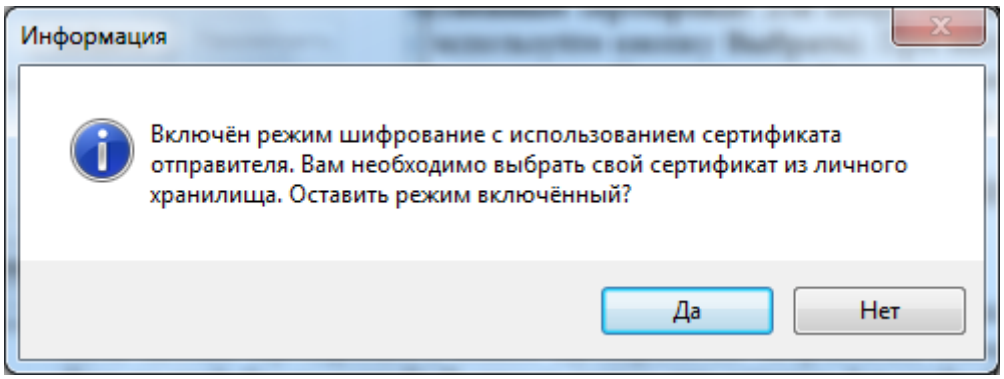
4) **Сохранять структуру вложенности каталогов;**
5) **Отправить выходные файлы по электронной почте.**

9. В окне **Свойства шифрования в**ыберите режим шифрования данных.
   Для этого поставьте переключатель напротив соответствующей строки:
   - **Использовать криптопровайдер** (в этом случае в выпадающем списке выберите необходимый тип криптопровайдера и алгоритм шифрования)

*В случае использования криптопровайдера «**SafeSign CSP Version 1.0**» рабочим алгоритмом шифрования является только RC4.*



- **Использовать собственный сертификат** для шифрования (Для выбора личного сертификата используйте кнопку **Выбрать)**. При выборе личного сертификата проверяется его статус. Личный сертификат автоматически добавляется в список сертификатов получателей шифруемого файла.

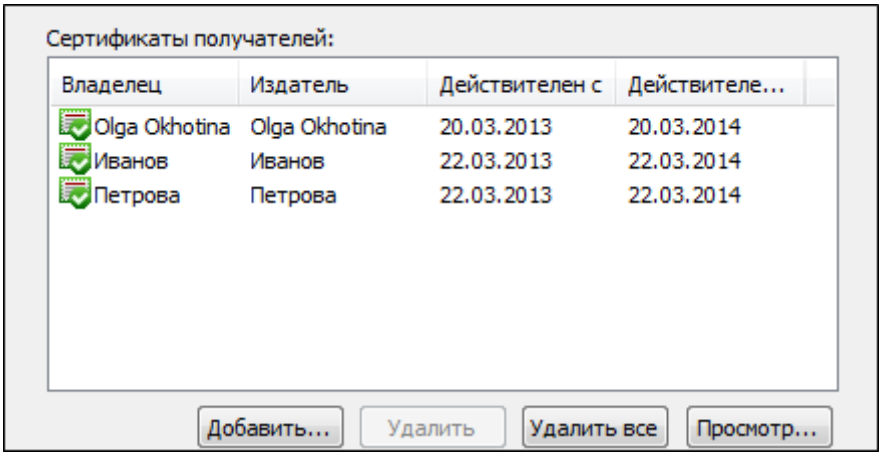


Подробнее о настройке параметров шифрования вы можете прочитать в разделе Настройки операции шифрования.

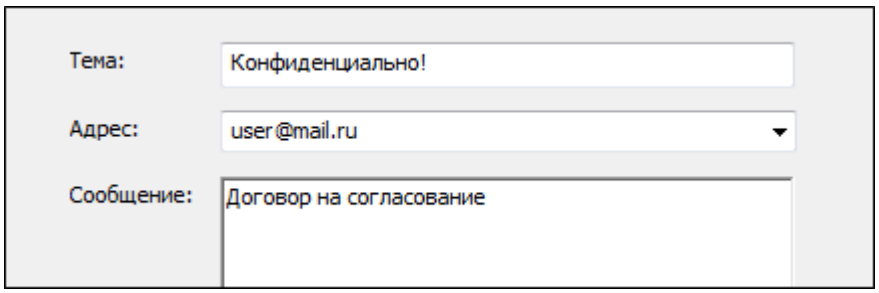
10. На следующем шаге выберите сертификаты получателей шифруемого файла, используя кнопку **Добавить**.

Чтобы иметь возможность расшифровать зашифрованный вами файл, вы должны добавить личный сертификат в список сертификатов получателей зашифрованного файла. Если на предыдущем шаге вы включили режим, при котором для шифрования будет использоваться ваш личный сертификат, на шаге выбора сертификатов получателей он автоматически будет занесен в список.

Обратите внимание, для шифрования необходимо, чтобы ключи отправителя и получателя могли быть использованы для шифрования данных.

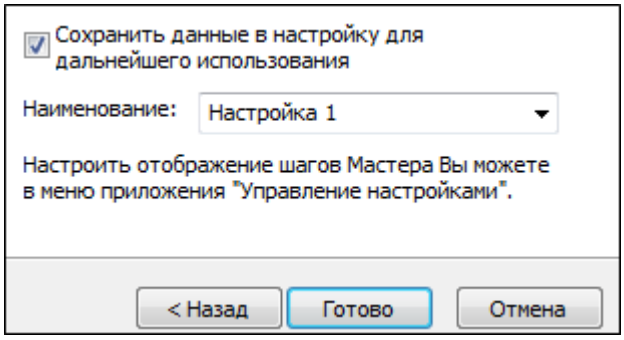


11. Для отправки подписанных и зашифрованных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:

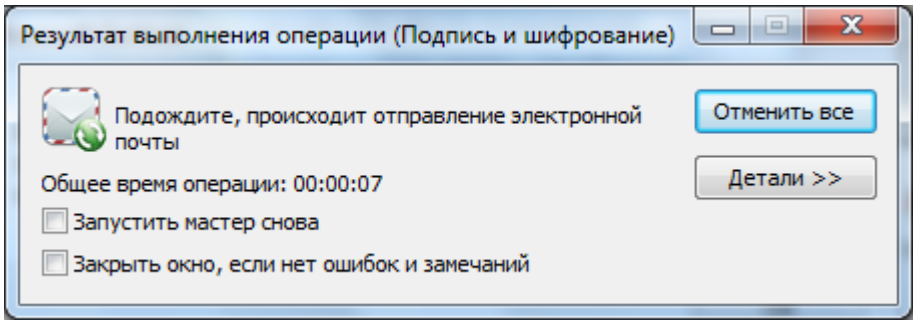


12. После завершения сбора параметров для выполнения шифрования возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был зашифрован файл и сертификат получателя (-ей). Для продолжения нажмите кнопку **Готово**.

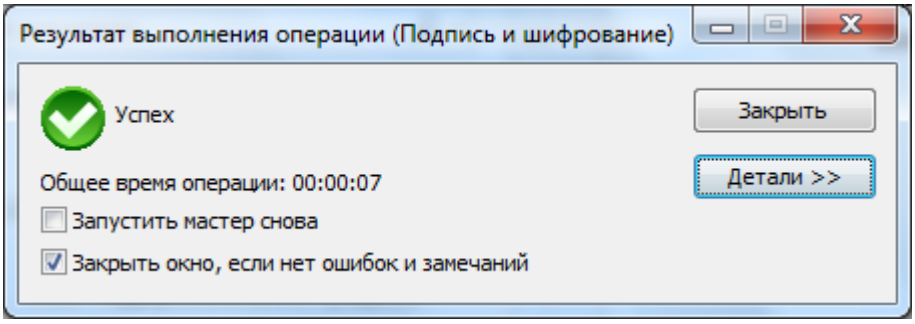
    Все указанные параметры можно сохранить в настройку для дальнейшего использования. Для этого установите флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



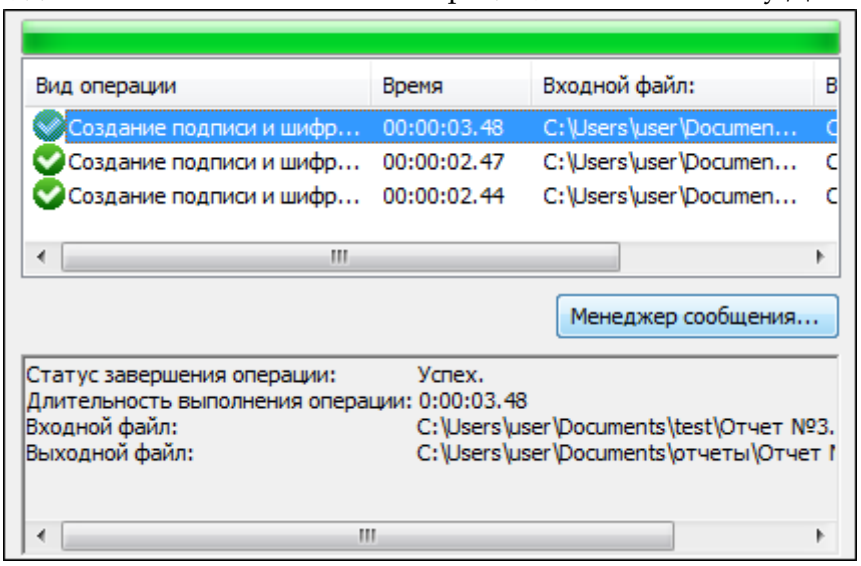
13. Начнется процесс подписи и шифрования файла. Вы можете прервать его, нажав на кнопку **Отмена**.
14. При отправке подписанных и зашифрованных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.



15. Далее возникнет окно **Результат выполнения операции** со статусом завершения операции.



Чтобы просмотреть детальную информацию о результатах шифрования и используемых параметрах: имя исходного файла, имя выходного (зашифрованного) файла, статус операции, длительность выполнения операции, нажмите кнопку **Детали**.



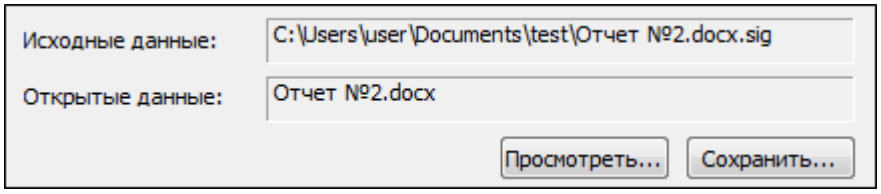
Вы можете отредактировать список получателей зашифрованных и подписанных данных, просмотреть и сохранить исходные данные.

1. Выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.
2. Откроется окно **Управление шифрованными данными**, в котором вы можете:

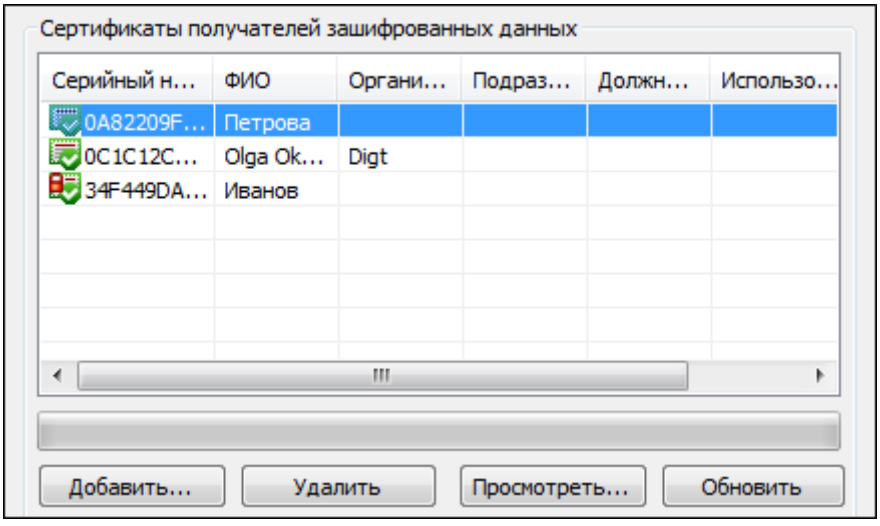
   1) Просмотреть путь, по которому сохранен зашифрованный файл;

   2) Просмотреть зашифрованный файл (кнопка **Просмотреть** напротив строки **Файл исходных данных**);

   3) Сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);



   4) Просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**);



Сертификат расшифрования данных отмечается значком . Сертификатом расшифрования становится первый из списка сертификат получателей, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно). При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы и подписаны в адрес измененного списка получателей.

8.10.2 Расшифрование и проверка подписи

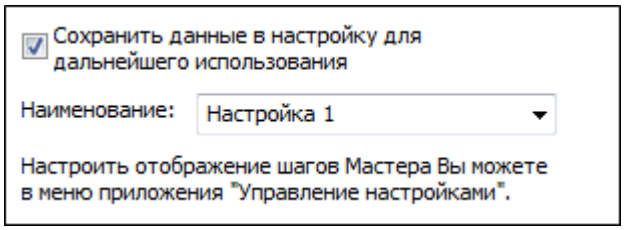
С помощью программы «КриптоАРМ» вы можете расшифровать и проверить ЭП отдельного файла или группы файлов, папку с файлами (при этом каждый файл, входящий в указанную папку, будет расшифрован и проверена подпись) или зашифрованные архивы

Расшифровать файл и проверить электронную подпись за одну операцию вы можете через:

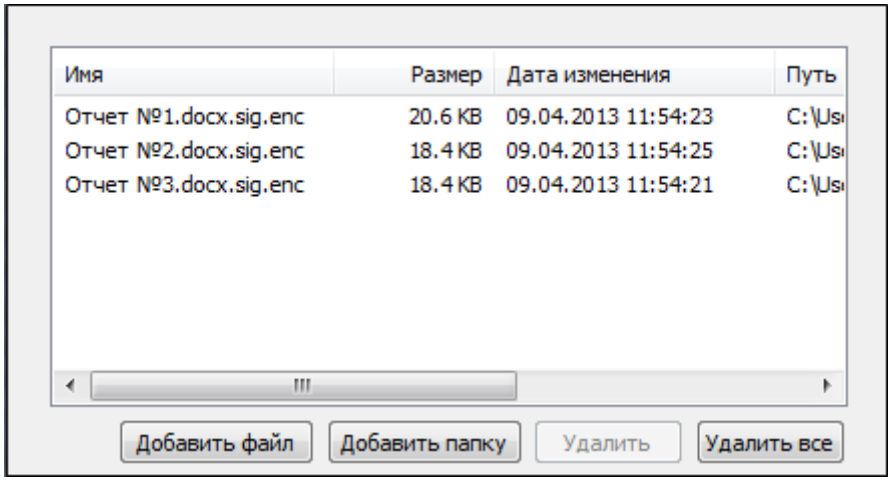
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Расшифровать и проверить подпись**. Далее следуйте рекомендациям Мастера по выполнению операции:

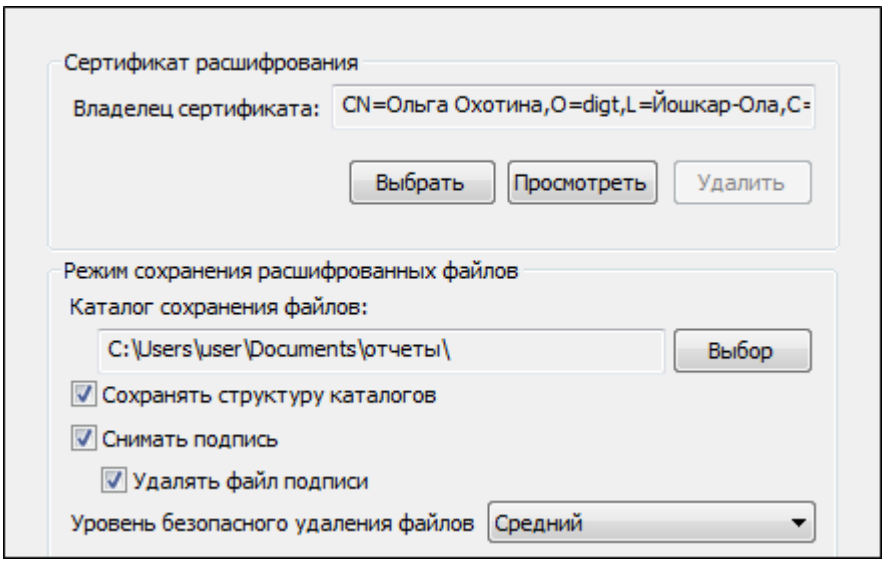
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи и расшифрования. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите один или несколько файлов с зашифрованными и подписанными данными (кнопки **Добавить файл** / **Добавить папку**).



3. В следующем окне выберите предпочтительный сертификат расширования (кнопка **Выбрать**). Указанный сертификат вы можете просмотреть, нажав на кнопку **Просмотреть**.



В данном окне также можно выбрать:

1) Каталог сохранения файлов, если поле каталога оставить пустым, то по результатам операции файлы будут сохранены в текущем каталоге.

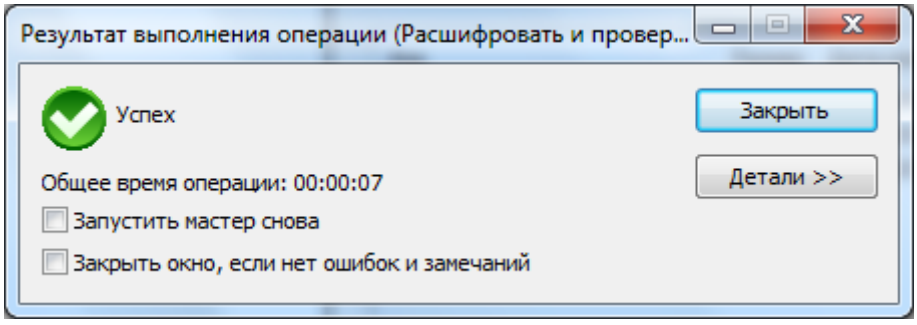
2) Сохранить структуру каталогов - при включении сохраняет структуру каталогов для выбранных файлов.

3) Снимать подпись - при проверке отделяет файл подписи от исходного файла.

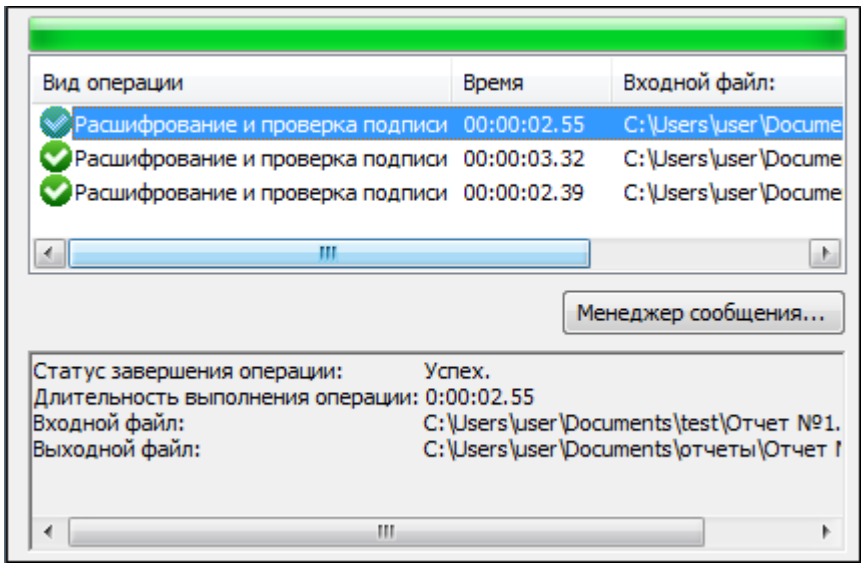
4) Удалять файл подписи - после снятия подписи удаляет файл подписи, оставляя только исходный файл.

5) Уровень безопасного удаления файлов. Подробнее о настройках уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

4. После завершения сбора данных для расшифрования и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения нажмите на кнопку **Готово**.
5. Данные будут расшифрованы и по умолчанию сохранены в тот же каталог, в котором находится исходный файл данных. Имя нового файла совпадает с именем подписанного и зашифрованного файла (только без дополнительного расширения). Если файл с таким именем уже существует, сохраните его под другим именем. Далее проверяется корректность ЭП и действительность сертификата отправителя.
6. После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах проверки подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали.**

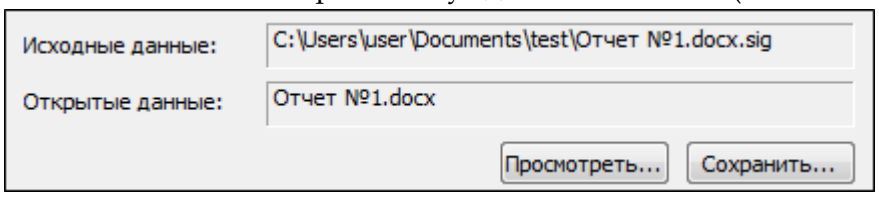


Если вы хотите просмотреть информацию об ЭП и сертификате подписчика, выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.



Откроется окно **Управление подписанными данными,** в котором вы можете:

1) Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).



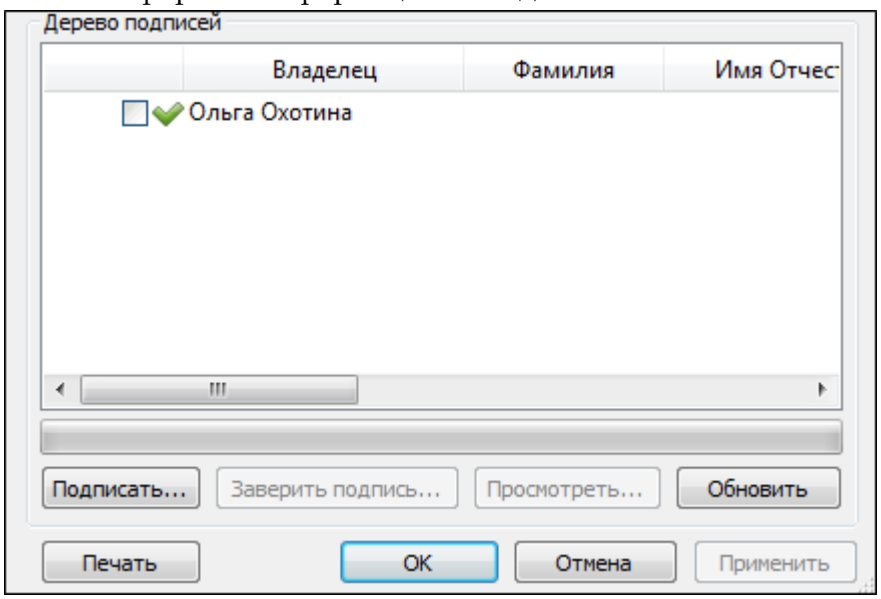
2) Просмотреть следующую информацию (кнопка **Просмотреть**):

- о добавленной к файлу электронной подписи
- о сертификате, с помощью которого был подписан файл, и его статусе
- о штампах времени на подпись и подписываемые данных

3) Добавить подпись.

4) Заверить подпись(обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя)

5) Распечатать информацию (кнопка **Печать**) о ЭП - в новом окне браузера MS IE будет сформирована печатная форма с информацией о подписи.



8.11 Просмотр документов

Программа «КриптоАРМ» позволяет просматривать исходные данные зашифрованного файла или файла, содержащего совмещенную подпись.

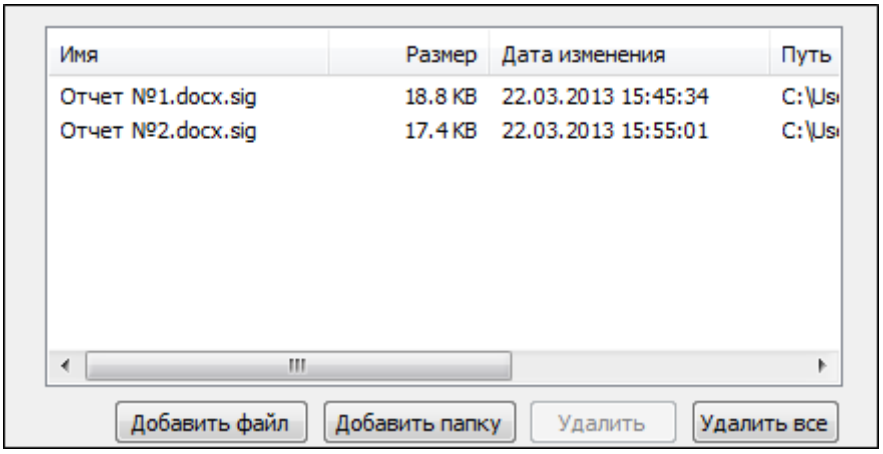
Для просмотра исходных данных зашифрованного документа, необходимо иметь сертификат расшифрования.

Просмотреть исходные данные зашифрованного файла или файла, содержащего ЭП, вы можете через:

- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Просмотреть документ.** Далее следуйте рекомендациям Мастера выполнения операции:

1. Выберите один или несколько файлов, которые необходимо просмотреть (кнопки **Добавить файл** и **Добавить папку** соответственно)



2. После завершения сбора параметров для выполнения операции возникнет окно с информацией о статусе операции. Для продолжения нажмите на кнопку **Готово**.
3. Исходные данные документа будут открыты для просмотра.

9 Модуль TSP

Кроме заверения документов электронной подписью, вы можете удостоверять точное время их создания. Это позволяет предотвращать возможные конфликты при обмене документами между партнерами, коллегами и т.п.

Использование штампов времени в электронном документообороте позволяет создавать официальное доказательство факта существования документа на определённый момент времени.

Модуль поддержки Службы Штампов времени (TSA). «**КриптоАРМ Стандарт Модуль TSP»** поддерживает работу с сервисом Служба штампов времени российского разработчика средств криптографической защиты информации — компании «Крипто-Про».

В главе **Модуль TSP** вы найдете информацию о том,

- Как получить штамп в службе штампов времени
- каким образом можно просмотреть штамп времени

«КриптоАРМ Старт» НЕ поддерживает работу со Службой штампов времени.

В случае работы со сторонним сервисом штампов времени дополнительно устанавливать ничего не требуется.

Если вы хотите использовать собственный сервис штампов времени, то необходима покупка сервера службы Штампов Времени, например, от компании «КриптоПро» - КриптоПро TSP Server.

Если планируется использовать ГОСТ алгоритмы, то необходима покупка ГОСТ-ового криптопровайдера «КриптоПро CSP».

Схема получения штампа времени:

1. Настройте параметры для работы со Службой штампа времени
2. Получить штамп времени на документ вы можете во время операции электронной подписи документа.
3. В финальном окне операции создания электронной подписи или операции проверки электронной подписи документа вы можете просмотреть информацию штампа времени, сформированную на подписанном документе.

В окне **Управление подписанными данными** откройте информацию о подписи (двойным кликом на ней или нажав на кнопку **Просмотреть**):

Закладка	Информация в закладке
Подпись	Информация об атрибутах подписи, времени ее создания, используемых алгоритмах подписи и хеширования.
Сертификат	Информация о сертификате: статус сертификата /действителен и др./, номер, данные о владельце и издателе, сроках действия сертификата и его использовании
Статусы сертификата	Общий статус проверки полного пути сертификации (о статусах сертификата читайте подробнее в главе **Проверка статуса сертификата**). Кроме этого, в закладке вы можете установить способ, каким проверять статус сертификатов (по локальному СОС, по СОС, полученного из УЦ, с использованием Revocation Provider, проверить в OCSP службе)
Штампы времени	• свойства штампа времени (время в штампе, точность штампа времени (мкс), идентификатор политики); • свойства Службы штампов времени (наименование службы); • сертификат Службы (содержится в том случае, если во время подписи документа в качестве одного из параметров штампа времени вы указали **Запросить сертификат Службы штампов времени**)

10 Модуль OCSP

Модуль OCSP к программе «КриптоАРМ» поддерживает работу с сервисом Службы актуальных статусов российского разработчика средств криптографической защиты информации — компании «КРИПТО-ПРО».

«КриптоАРМ Старт» не поддерживает работу со Службой актуальных статусов.

Служба актуальных статусов — это доверенный субъект Инфраструктуры открытых ключей (PKI), который предназначен для онлайновой проверки статуса сертификатов на основе протокола OCSP (Online Certificate Status Protocol).

Служба OCSP распространяет информацию о статусах сертификатов и имеет следующие преимущества по сравнению со списками отзыва сертификатов (COC):

- информация о статусе сертификатов всегда актуальна. Служба может получать информацию об изменении статусов сертификатов в реальном времени и распространять её клиентам.
- меньший объём OCSP-ответа. Объём ответа службы фиксирован и сравнительно мал, в то время как списки отзыва сертификатов могут иметь большой объём. Это позволяет уменьшить время реакции приложений и может иметь решающее значение при создании долговременного архива документов с ЭП для уменьшения объёма единиц хранения.

Проверка электронной подписи на подлинность требует наличия дополнительных данных, называемых доказательствами подлинности. «Доказательства Подлинности» включают

- сертификаты ЦС наряду со статусом отзыва, в форме COC или же в форме информации о статусе сертификата (OCSP), предоставляемые через онлайн-услуги
- свидетельство того, что подпись была создана заведомо до определенного момента времени. В качестве такового может выступать штамп времени или привязанные ко времени учетные записи в протоколах (time - marking).

«Доказательства подлинности» могут собираться подписывающей и/или проверяющей стороной. Явное присутствие идентификатора регламента подписи должно быть обусловлено требованиями этого регламента.

Дополнительно читайте о том, какие параметры доступа в службу OCSP необходимо настроить для успешного получения улучшенной подписи.

Работа с OCSP службой потребует версию программы «КриптоАРМ Стандарт» и лицензию на Модуль OCSP или «КриптоАРМ СтандартPRO».

В случае работы со сторонним сервисом актуальных статусов дополнительно устанавливать ничего не требуется. Если же требуется использование собственного сервиса актуальных статусов, то необходима покупка сервера службы, например, от компании «КриптоПро» - «КриптоПро OCSP Server».

Если планируется использовать ГОСТ алгоритмы, то необходима покупка ГОСТ-ового криптопровайдера «КриптоПро CSP» или «Signal COM CSP».

11 Перечень сокращений

CRL	CRL Distribution Point
CRL Distribution Point	Certificate Revocation List (Списокотзывасертификатов)
LDAP	Lightweight Directory Access Protocol (Упрощенныйпротоколдоступаксправочнику)
Microsoft CA	Microsoft Certification Authority (Удостоверяющий центр от компании Microsoft)
OCSP	Online Certificate Status Protocol (Протоколактуальныхстатусовсертификатов)
OID	Идентификатор объекта (АСН.1)
PKC	Сертификат открытого ключа (Public Key Certificate)
PKI	Public Key Infrastructure (АналогИОК)
TSA	Time Stamping Authority (Службаштамповвремени)
TSP	ДоверенныйСлужба (Trusted Service Provider)
ИОК	Инфраструктура Открытых Ключей (PKI)
ОС	Операционная система
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СОС	Списокотзывасертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЦС	Центр Сертификации (CA)
CAdES	Усовершенствованная ЭП
CAdES X Long	Усовершенствованная ЭП с расширенными доказательствами подлинности
PKC	Сертификат открытого ключа (Public Key Certificate)
ЭП	Электронная подпись (ранее использовался термин ЭЦП, электронная цифровая подпись)

12 Часто задаваемые вопросы

В главе **Часто задаваемые вопросы** вы найдете информацию по следующим темам:

- Тестирование и приобретение программы «КриптоАРМ»
- Использование программы «КриптоАРМ»
- Ошибки, возможные при работе с программой «КриптоАРМ»

12.1 Тестирование и приобретение программы «КриптоАРМ»

Мы изучали возможности программы «КриптоАРМ» версии «Стандарт Плюс» в течение 30-дневного ознакомительного периода. Что требуется, что перейти на работу в постоянном режиме?

Дальнейшие действия зависят от выбранной вами версии:

Версия «Старт» не требует покупки лицензии.

Версии «Стандарт» и «Стандарт Плюс» требуют наличия лицензий (бессрочной или годовой по выбору). Постоянная лицензия выдается разработчиком/поставщиком программы «КриптоАРМ» после оплаты стоимости лицензии.

При получении лицензионного ключа введите регистрационные данные «КриптоАРМ»> «Помощь» > «О программе» > «Установить лицензию».

Будьте внимательны при заполнении регистрационных данных ключа: вводите только ту информацию, которая была указана при получении лицензии. При вводе дополнительных данных в форму регистрации лицензионный ключ окажется недействительным.

Установили «КриптоПро CSP» и «КриптоАРМ», использовали временные лицензионные ключи. Недавно приобрели лицензию: требуется ли переустанавливать ПО для работы?

Переустановка программ не требуется. Достаточно зарегистрировать оба лицензионных ключа:

Для ПО «КриптоАРМ»: Панель Управления – «КриптоАРМ» – Помощь – О программе – Установить лицензию.

Для ПО «КриптоПро CSP»: Панель Управления – «КриптоПро CSP» – Общее - Ввод лицензии.

Могут ли на одном компьютере работать несколько пользователей, используя одну лицензию «КриптоАРМ»?

Чтобы использовать «КриптоАРМ» на одном компьютере несколькими пользователями достаточно одной лицензии.

Можно ли обойтись одной лицензией, если один пользователь работает то на стационарном компьютере, то на ноутбуке?

В случае работы одного пользователя на нескольких компьютерах требуется по одной лицензии на каждое рабочее место.

Требуется ли дополнительно покупать «КриптоПро TSP Client» или «КриптоПро OCSP Client», для того чтобы работали модули TSP и OCSP?

При приобретении модулей TSP и OCSP покупателю будет предоставляться лицензия как на этот модуль, так и на «КриптоПро TSP Client» и «КриптоПро OCSP Client». Дополнительной оплаты не требуется.

12.2 Использование программы «КриптоАРМ»

Каков порядок действий при выходе из строя смарт-карты или токена, содержащего сертификат подписи или шифрования и ключевую пару сотрудников?

Такие ключевые носители, как правило, восстановлению не подлежат (нет никакой гарантии, что при попытке восстановления не будет сбит хотя бы один бит информации). Если дубля (точнее, контейнера с ключами) не имеется, единственное решение - формировать новую ключевую пару и получать новый сертификат.

В последующем необходимо (и всегда рекомендуется!) иметь резервную копию ключевого носителя (резервную копию контейнера можно выполнить с помощью программы «КриптоАРМ») и хранить копию в надежном месте.

Почему размер зашифрованного файла увеличивается почти в два раза?

Размер зашифрованного файла зависит от того, какой вариант шифрования вы выбираете:

Если выбираете шифрование в p7s, то выходной файл будет в der-кодировке.

Если выбираете вариант pem, то он будет в кодировке Base64, что, естественно, приводит к увеличению размера на 33%.

Если же вы подписываете и шифруете одновременно и в обоих случаях используете Base64 кодировку, то выходной файл будет больше аналогичного бинарного в 1,33 * 1,33 = 1,77 раза.

Чем отличается использование самоподписанных сертификатов от сертификатов, выданных официальным Удостоверяющим центром?

Сертификат – это электронный или печатный документ, удостоверяющий соответствие между парой цифровых ключей и их владельцем. В корпоративных и иных системах такие сертификаты выдаются специальным органом – Удостоверяющим центром. В этом случае получатель подписанного вами электронного документа может проверить подлинность и корректность данных отправителя, обратившись к этому УЦ, доверенной стороне.

Самоподписанный сертификат формируется самим пользователем за счет возможностей, заложенных в программу “КриптоАРМ”, т.е. сам удостоверяет соответствие своих ключей и себя, как их владельца. Использование таких сертификатов возможно при личной переписке или в тех организациях, где такая возможность специально оговорена регламентом использования электронной подписи.

Для использования сертификата вне организации для обеспечения юридически значимого документооборота необходимо использовать сертификаты, выданные сторонней организацией, Удостоверяющим центром. Одними из ведущих УЦ на территории РФ являются КриптоПро УЦ, Ekey УЦ и ряд других. Если требуется использовать квалифицированный сертификат, то необходимо обратиться к одному из аккредитованных удостоверяющих центров. На портале Уполномоченного федерального органа в области электронной подписи Минкомсвязи размещается актуальный список аккредитованных УЦ.

12.3 Ошибки, возможные при работе с программой «КриптоАРМ»

После ввода купленной лицензии статус лицензии «Лицензия недействительна».

Версия установленного вами дистрибутива программы "КриптоАРМ" не соответствует версии лицензии, которую вы устанавливаете. Установите дистрибутив, соответствующий лицензии, и лицензионный ключ подойдет.

При попытке зашифровать документы на конечной стадии ошибка «Указан неправильный тип поставщика (CSP). (0x80090014)».

1. Проверьте наличие лицензий на программу «КриптоАРМ Стандарт» и СКЗИ «КриптоПро CSP».

2. Обновите версию программы «КриптоАРМ» до последней с сайта trusted.ru

При создании и шифровании подписи возникает внутренняя ошибка 0x80090020.

Возможно, вы создали ключевую пару при помощи криптопровайдера Microsoft Base DSS and Diffie-Hellman CryptographicProvider или другого RSA криптопровайдера, а сертификат был выпущен в УЦ, использующем ГОСТ-алгоритмы.

«КриптоАРМ» такую ситуацию отрабатывает некорректно, да и с организационной точки зрения некорректно смешивать алгоритмы открытых ключей в пути сертификации.

Для исправления ошибки необходимо получить новый сертификат в том же УЦ, но при помощи ГОСТ-ового криптопровайдера, например:

- Crypto-Pro Cryptographic Service Provider
- Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
- Crypto-Pro GOST R 34.10-94 Cryptographic Service Provider.

При подписании документа или проверке подписи возникает ошибка: "Статус сертификата: недействителен, ошибка построения пути сертификации."

Сообщение "ошибка построения пути сертификации" говорит о том, что вам необходимо установить на рабочем месте корневой сертификат удостоверяющего центра. Если у вас его нет, скачайте с официального сайта удостоверяющего центра или по ссылке в составе сертификата. Для просмотра ссылки необходимо:

1. В личном хранилище сертификатов открыть сертификат;
2. Нажать на кнопку "Просмотреть";
3. Выбрать вкладку "Состав";
4. Выбрать "Доступ информации о центре сертификации";
5. По ссылке скачать корневой сертификат удостоверяющего центра;
6. Принудительно установить сертификат в папку: "Доверенные корневые центры сертификации".

«КриптоАРМ» сообщает, что "Произошла ошибка при получении последней версии СОС из УЦ".

Для использования возможности получения списка отозванных сертификатов из УЦ необходимо соблюдение следующих условий:

1. В проверяемом сертификате должно присутствовать расширение "Точки распространения списков отзыва/CRL Distribution Point (CDP)", в котором должен быть указан правильный URL (адрес) СОС.

2. По одной (оптимально, если по первой) из точек распространения СОС (из п.1) можно скачать СОС браузером Internet Explorer, не вводя при этом никакой дополнительной информации (имени пользователя, пароля, перехода по ссылкам).

3. В настройках Internet Explorer не должна быть включена автоматическая настройка прокси-сервера. Для проверки этого запустите “Internet Explorer” -> меню “Сервис” -> пункт “Свойства обозревателя” -> закладка “Подключения” -> кнопка “Настройка сети” -> должны быть сброшены флажки “Автоматическое определение параметров” и “Использовать скрипт автоматической настройки”.

13 Техническая поддержка

По вопросам технической поддержки программы «КриптоАРМ» обращайтесь:

- На сайт: http://www.trusted.ru/support/question
- По электронной почте: support@trusted.ru
- По телефонам: 8 (800) 555-65-81 (звонок бесплатный), 8(499) 70-59-110.

Получить техническую поддержку вы можете по Интернету через программу «КриптоАРМ». Для этого в главном окне программы в верхнем меню выберите пункт **Помощь -> О программе.** Откроется окно **О программе**, в котором нажмите на кнопку **Поддержка**. Загрузится страница с формой, заполнив которую, вы можете отправить свой вопрос в службу технической поддержки.

14 Купить программу

Купить программу «КриптоАРМ» вы можете:

1. Непосредственно в компании "Цифровые технологии". Для этого отправьте письмо с запросом на покупку лицензии по адресу **sales@trusted.ru** или сделайте заказ на официальном сайте компании. На адрес поставщика продукта вышлите следующие данные:

- Полное название продукта (с указанием необходимых модулей)
- Необходимое количество лицензий
- Имя контактного лица
- Название компании
- Контактный e-mail

2. У официальных партнеров компании "Цифровые технологии" (ИТ-разработчики, удостоверяющие центры, системные интеграторы, интернет-магазины). Полный список региональных компаний-партнеров и их контактную информацию вы найдете **на сайте в разделе "Купить"**

В течение 5 рабочих дней после оплаты лицензии по электронной почте вам будет выслан **лицензионный ключ**.

15 О компании-разработчике

Компания "Цифровые технологии" – российский разработчик и поставщик программного обеспечения в области защиты информации, телекоммуникаций и Интернет-сервисов. Основным направлением работы компании является криптографическая защита информации:

- разработка кроссплатформенных решений в области защиты данных,
- встраивание российских сертифицированных криптографических алгоритмов в прикладные и бизнес-приложения,
- создание систем авторизации и аутентификации пользователей,
- консалтинг в области использования средств криптографической защиты информации (СКЗИ) в государственной и коммерческой среде. Особое внимание уделяется внедрению и применению отечественных стандартов защиты в российской практике.

Компания "Цифровые технологии" имеет **лицензии ФСБ (ФАПСИ)** на проектирование, производство, распространение и обслуживание сертифицированных шифровальных средств информационных систем, систем и комплексов телекоммуникации, не связанных с обработкой сведений, составляющих государственную тайну.

Официальными партнерами компании являются ведущие российские ИТ-компании – "КРИПТО-ПРО", Aladdin, "Актив" и другие.

Компания "Цифровые технологии"
424019, Россия, Республика Марий Эл, г. Йошкар-Ола, ул. Петрова, д.1, а/я 67

Общие вопросы info@trusted.ru
Вопросы приобретения продукта info@trusted.ru
Техническая поддержка support@trusted.ru
Подробнее о программных продуктах и решениях компании www.trusted.ru