



QIWI ЗАЩИТА

вер. 2.1

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

вер. 1.9

МОСКВА
8-495-783-5959

РОССИЯ
8-800-200-0059

ФАКС
8-495-926-4615

WEB
WWW.QIWI.RU

СОДЕРЖАНИЕ

1.	ГЛОССАРИЙ	4
2.	ВВЕДЕНИЕ.....	5
2.1.	НАЗНАЧЕНИЕ ПРИЛОЖЕНИЯ.....	5
2.2.	ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ	5
3.	БЫСТРЫЙ СТАРТ	6
3.1.	СОЗДАНИЕ СЕРТИФИКАТА.....	6
3.2.	СОЗДАНИЕ ПЕРСОНЫ ДЛЯ ПО QIWI КАССИР	6
3.3.	ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ	7
4.	УСТАНОВКА И ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ.....	8
4.1.	УСТАНОВКА ПРИЛОЖЕНИЯ.....	8
4.2.	ГЛАВНОЕ ОКНО ПРИЛОЖЕНИЯ	10
5.	ПРЕДВАРИТЕЛЬНАЯ ПОДГОТОВКА	12
5.1.	ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ	12
5.2.	СОЗДАНИЕ ПЕРСОНЫ ДЛЯ ПО «QIWI КАССИР».....	12
6.	ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ	14
7.	СОЗДАНИЕ/УДАЛЕНИЕ ПЕРСОНЫ ДЛЯ QIWI КАССИР/QIWI КАССИР 1С	18
7.1.	СОЗДАНИЕ ПЕРСОНЫ	18
7.2.	УДАЛЕНИЕ ПЕРСОНЫ ПО QIWI КАССИР	22
8.	НАСТРОИТЬ ЭТОТ КОМПЬЮТЕР ДЛЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	23
9.	СЕРТИФИКАТЫ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ	26
9.1.	СОЗДАНИЕ ЗАЯВКИ НА СЕРТИФИКАТ ЭЦП	26
9.2.	УСТАНОВКА СЕРТИФИКАТА	35
10.	ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	37
10.1.	СПИСОК СЕРТИФИКАТОВ.....	37
10.2.	СЕТЕВЫЕ НАСТРОЙКИ	38
10.3.	ЗАГРУЗКА ДРАЙВЕРОВ	39
10.4.	ЗАГРУЗКА ДОКУМЕНТАЦИИ	39
10.5.	О ПРОГРАММЕ	40
11.	ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ.....	41
ПРИЛОЖЕНИЕ А:	РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ	43
ПРИЛОЖЕНИЕ Б:	ПОДГОТОВКА ЕТОКЕН К РАБОТЕ.....	44
ПРИЛОЖЕНИЕ В:	АВТОРИЗАЦИЯ НА САЙТЕ	48
ПРИЛОЖЕНИЕ Г:	СОХРАНЕНИЕ В СИСТЕМНОЕ ХРАНИЛИЩЕ	50
ПРИЛОЖЕНИЕ Д:	РАБОТА С «ФАЙЛОМ» СЕРТИФИКАТА	55
ПРИЛОЖЕНИЕ Е:	СИНХРОНИЗАЦИЯ ВРЕМЕНИ	63

ПРИЛОЖЕНИЕ Ж: ПОЛУЧЕНИЕ СЕРТИФИКАТА ЭЦП 64
СПИСОК РИСУНКОВ 65

1. ГЛОССАРИЙ

Термин	Определение
<i>Авторизация</i>	Проверка прав персоны и предоставление доступа к ресурсам в соответствии с ними.
<i>Персона</i>	Учетная запись, зарегистрированная на сайте для сотрудника агента, работающего с системой ОСМП. Персона имеет определенный набор прав доступа к системе.
<i>Псевдоним</i>	Имя пользователя, отображаемое при авторизации в приложениях ОСМП (например, в ПО <i>QIWI Кассир</i>).
<i>Сертификат</i>	Цифровой документ, используемый для идентификации персоны.

2. ВВЕДЕНИЕ

Данный документ представляет собой руководство по установке и использованию приложения *QIWI Защита*.

2.1. Назначение приложения

ПО *QIWI Защита* предназначено для повышения уровня безопасности при работе с *Системой ОСМП*.

Приложение позволяет:

- Сгенерировать сертификат для авторизации на сайтах ОСМП:
 - агентский agent.qiwi.com (portal.qiwi.com);
 - провайдерский prov.osmp.ru.
- Сгенерировать авторизационные данные персоны для ПО *QIWI Кассир*.

ВНИМАНИЕ



Для повышения уровня безопасности авторизационные данные рекомендуется хранить на eToken/

- Создать электронно-цифровую подпись и настроить электронный документооборот с *Системой ОСМП*.

2.2. Технические требования

Для работы приложения на локальном компьютере необходимо выполнение следующих требований к программному и аппаратному обеспечению:

- не менее 21 Мб свободного дискового пространства;
- разрешение экрана 1024x768 в режиме High/True Color;
- оперативной памяти не менее 64 Мб (рекомендуется 128 Мб);
- частота процессора не ниже 233 МГц;
- наличие подключения к сети Интернет;
- операционная система Microsoft Windows 9x, ME, 2000, XP, 2003, Vista, 7;
- драйвера для работы с ключом eToken версии 4.55 или выше.

3. БЫСТРЫЙ СТАРТ

3.1. Создание сертификата

Для создания сертификата выполните следующие действия:

1. Выберите пункт **Получить доступ на агентский сайт**.
2. Введите авторизационные данные персоны (**логин и одноразовый пароль для сертификата**).
3. Выберите тип хранилища.

СОВЕТ



Наиболее рекомендуемым хранилищем по соображениям безопасности является **eToken**.

4. Сохраните сертификат в хранилище.

ПРИМЕЧАНИЕ



Процесс создания сертификата подробно описан в разделе [6](#).

3.2. Создание персоны для ПО QIWI Кассир

Для создания авторизационных данных персоны выполните следующее:

1. Выберите пункт **Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С**.
2. Установите переключатель в положение **Создание**.
3. Выберите тип хранилища.

СОВЕТ



Наиболее рекомендуемым хранилищем по соображениям безопасности является **eToken**.

4. Введите авторизационные данные персоны (**псевдоним, логин, одноразовый пароль для сертификата и ID терминала**).
5. Сохраните информацию в хранилище.

ПРИМЕЧАНИЕ



Процесс управления авторизационными данными персон подробно описан в разделе [7.1](#).

3.3. Электронный документооборот

Для настройки электронного документооборота выполните следующее:

1. Если на вашем компьютере отсутствует ПО *КриптоПро CSP* или *ЭЦП Browser Plug-in*, выберите пункт **Настроить этот компьютер для электронного документооборота**.
2. Будет запущен мастер установки ПО *КриптоПро CSP* и *ЭЦП Browser Plug-in*, необходимых для получения и установки сертификата электронно-цифровой подписи (ЭЦП).
3. Выполните все шаги мастера.

ПРИМЕЧАНИЕ



Процесс установки ПО для электронного документооборота подробно описан в разделе [8](#).

4. Оформите заявку на сертификат ЭЦП: в главном окне программы выберите действие **Сертификаты электронно-цифровой подписи** → **Заявка на сертификат** и следуйте дальнейшим указаниям мастера.
5. После того как сертификат ЭЦП получен, установите сертификат на компьютер: в главном окне программы выберите действие **Сертификаты электронно-цифровой подписи** → **Установка сертификата**.

ПРИМЕЧАНИЕ



Процесс получения и установки сертификата ЭЦП подробно описан в разделе [9](#).

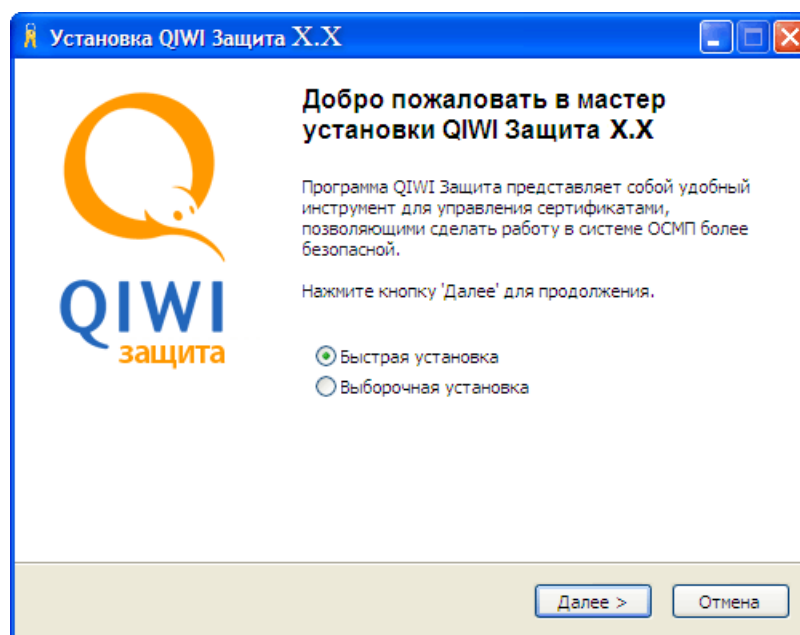
4. УСТАНОВКА И ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ

4.1. Установка приложения

Для установки приложения выполните следующее:

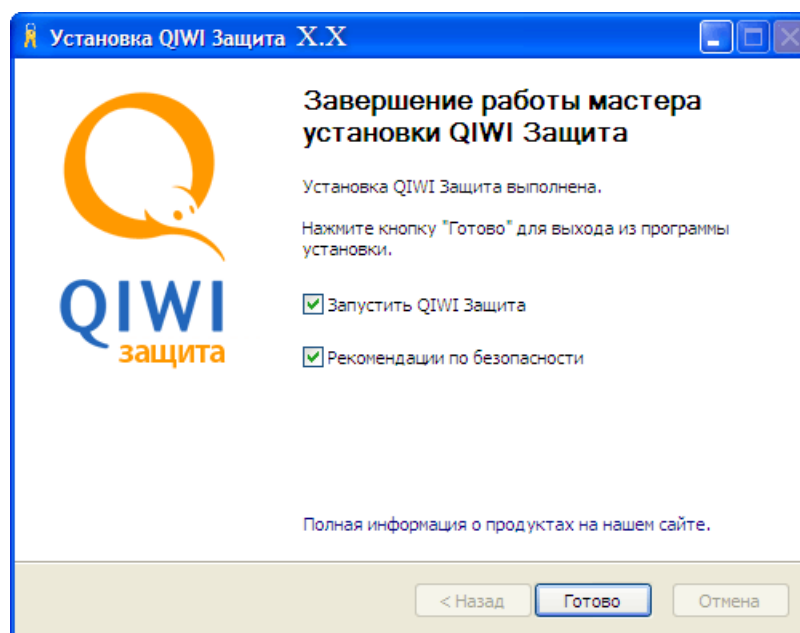
1. Скачайте последнюю версию приложения с сайта www.qiwi.ru, раздел **Бизнесу→Агентам→Скачать ПО**.
2. Запустите файл `qiwiguard-x.x-ru-win.exe` (x.x – номер версии приложения) ([Рис. 1](#)).

Рис. 1. Мастер установки



3. Выберите тип установки:
 - **Быстрая установка** – будет выполнена автоматическая установка приложения, и вы перейдете к финальному шагу ([Рис. 2](#)).
 - **Выборочная установка** – вам будет предложено:
 - ⊕ ознакомиться с лицензионным соглашением;
 - ⊕ выбрать папку установки;
 - ⊕ выбрать папку в меню *Пуск*.После чего вы перейдете к финальному шагу установки ([Рис. 2](#)).

Рис. 2. Финальный шаг установки



4. Снимите флаги, если вы не желаете выполнить данные действия:
 - **Запустить QIWI Защита** – запустить приложение сразу после установки.
 - **Рекомендации по безопасности** – ознакомиться с рекомендациями по обеспечению безопасности при работе с *Системой*.

ПРИМЕЧАНИЕ

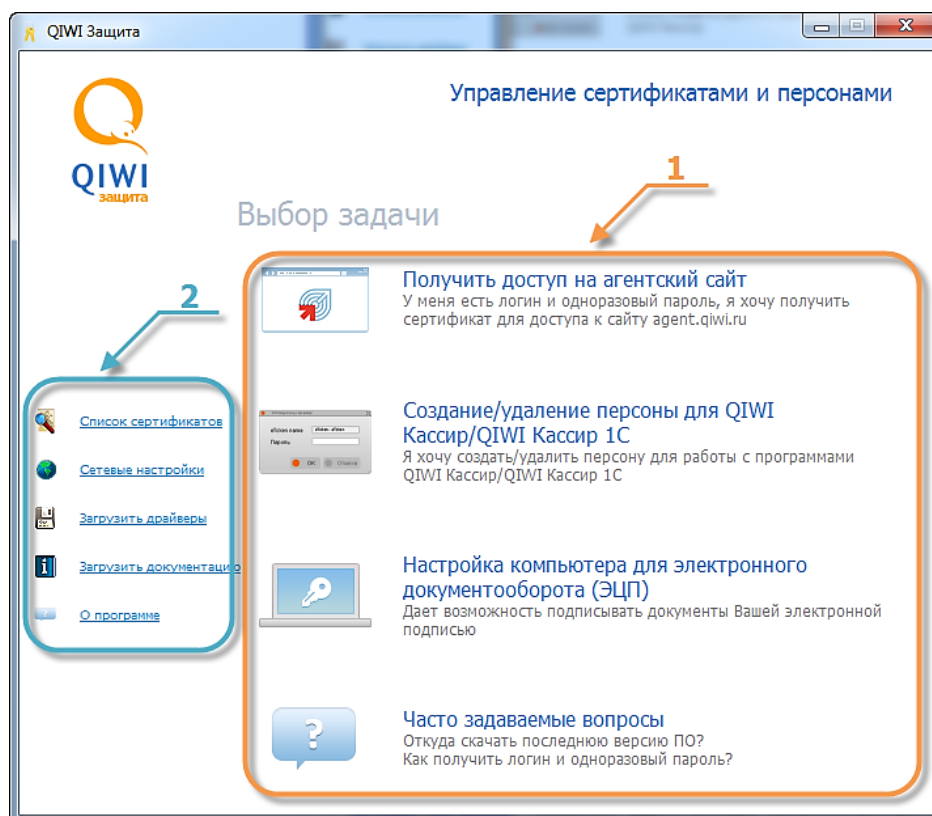
Для получения более подробной информации об этом или иных продуктах наших разработчиков нажмите на ссылку **Полная информация о продуктах на нашем сайте**.

5. Для завершения работы мастера нажмите кнопку **Готово**. Приложение будет установлено. На рабочем столе и в меню **Пуск** будут расположены соответствующие ярлыки.

4.2. Главное окно приложения

Главное окно приложения показано на [Рис. 3](#).

Рис. 3. Главное окно приложения



Главное окно приложения состоит из двух областей:

- **1 – Список основных задач:**
 - **Получить доступ на агентский сайт** – позволяет создать сертификат для доступа на сайты portal.qiwi.com, agent.qiwi.com и prov.osmp.ru. Подробнее о генерации сертификата см. в разделе [6](#).
 - **Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С** – позволяет создавать авторизационные данные персоны для работы с ПО *QIWI Кассир*, а также удалять их. Подробнее об управлении персонами см. в разделе [7](#).
 - **Настроить этот компьютер для электронного документооборота** – позволяет загрузить и установить ПО *КриптоПро CSP* или *ЭЦП Browser Plug-in* для получения возможности работать с электронной цифровой подписью (ЭЦП). Подробнее о настройке ПО для электронного документооборота см. в разделе [8](#).

Если ПО *КриптоПро CSP* и ПО *ЭЦП Browser Plug-in* установлены на компьютере пользователя, на месте пункта **Настроить этот компьютер для электронного документооборота** отображается пункт **Сертификаты электронно-цифровой подписи**.

- **Сертификаты электронно-цифровой подписи** – позволяет создать запрос на сертификат ЭЦП и установить полученный сертификат на компьютер пользователя. Сертификат необходим для подписания актов агента с помощью ЭЦП. Подробнее о работе с сертификатами ЭЦП см. в разделе [9](#).
- **Часто задаваемые вопросы** – список ответов на часто задаваемые вопросы.
- **2 – Список дополнительных возможностей:**
 - [Список сертификатов](#) – открывает системное хранилище сертификатов;
 - [Сетевые настройки](#) – позволяет задать сетевые настройки для доступа к Интернету;
 - [Загрузить драйверы](#) – позволяет загрузить драйверы, необходимые для работы с eToken в различных ОС;
 - [Загрузить документацию](#) – позволяет загрузить последнюю версию руководства пользователя;
 - [О программе](#) – открывает окно с информацией о приложении.

5. Предварительная подготовка

ВНИМАНИЕ

Перед работой с ПО QIWI Защита рекомендуется выполнить синхронизацию даты и времени (подробнее см. [Приложение E](#)).

На agent.qiwi.com вам необходимо зарегистрировать:

- для получения доступа на агентский сайт – персону.
- для создания персоны для ПО «QIWI Кассир» – персону и терминал.

Данный раздел содержит требования к персонам и терминалам. Подробнее о создании персон, терминалов и генерации одноразового пароля см. в Руководстве пользователя сайта agent.qiwi.com.

5.1. Получение доступа на агентский сайт

Для генерации сертификата вам потребуется зарегистрировать на сайте agent.qiwi.com персону:

- Роль персоны не должна быть **Продавец** или **Автомат**.
- Задать **Логин персоны**.
- Сгенерировать **Одноразовый пароль**.

ПРИМЕЧАНИЕ

Одноразовый пароль в процессе генерации можно использовать только один раз, после чего он блокируется сервером. Если процесс был завершен ошибкой, вам будет необходимо сгенерировать новый одноразовый пароль.

5.2. Создание персоны для ПО «QIWI Кассир»

На сайте agent.qiwi.com необходимо зарегистрировать:

- Персону:
 - Назначить роль – **Продавец**
 - Задать **Логин персоны**
 - Сгенерировать **Одноразовый пароль**

ПРИМЕЧАНИЕ

Одноразовый пароль в процессе генерации можно использовать только один раз, после чего он блокируется сервером. Если процесс был завершен ошибкой, вам будет необходимо сгенерировать новый одноразовый пароль.

- Терминал:
 - Задать тип терминала **QIWI Кассир**
 - Указать **Серийный номер** ПО *QIWI Кассир*.

6. ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ

ВНИМАНИЕ

Перед генерацией сертификата с помощью ПО QIWI Защита прочтите раздел [5](#).

Для получения доступа на агентский сайт необходимо сгенерировать сертификат. Для этого:

1. В главном окне приложения выберите действие **Получить доступ на агентский сайт** (см. [Рис. 3](#)).

Будет открыт *Мастер создания сертификатов* ([Рис. 4](#)).

Рис. 4. Мастер создания сертификатов

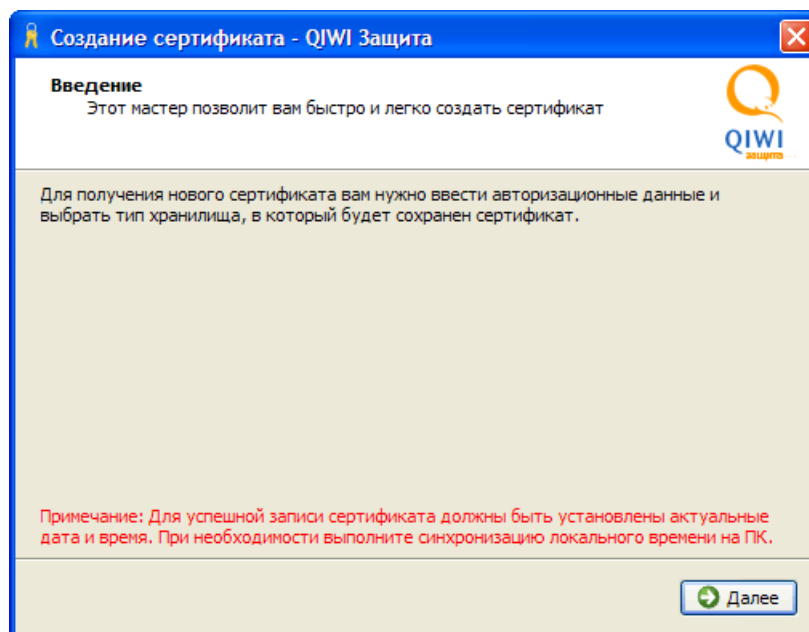


Рис. 5. Ввод авторизационных данных

Создание сертификата - QIWI Защита

Авторизационные данные
Введите логин и одноразовый пароль персоны, для которой вы хотите создать новый сертификат

Логин

Пароль

2. Укажите данные персоны для генерации сертификата ([Рис. 5](#)):
 - **Логин** – логин персоны;
 - **Пароль** – одноразовый пароль для сертификата.
 - **Показать пароль** – флаг позволяет отображать значение поля **Пароль**.

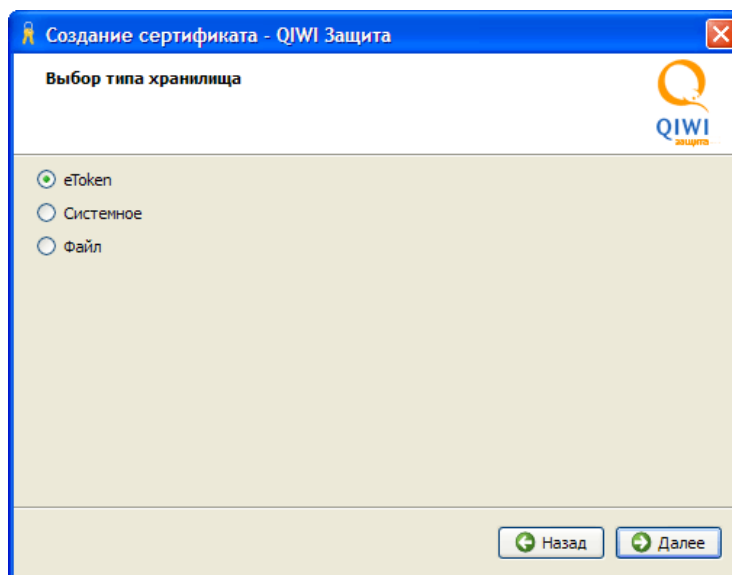
ПРИМЕЧАНИЕ

Далее описаны шаги генерации сертификата с типом хранилища eToken, т.к. он является наиболее рекомендуемым хранилищем по соображениям безопасности.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

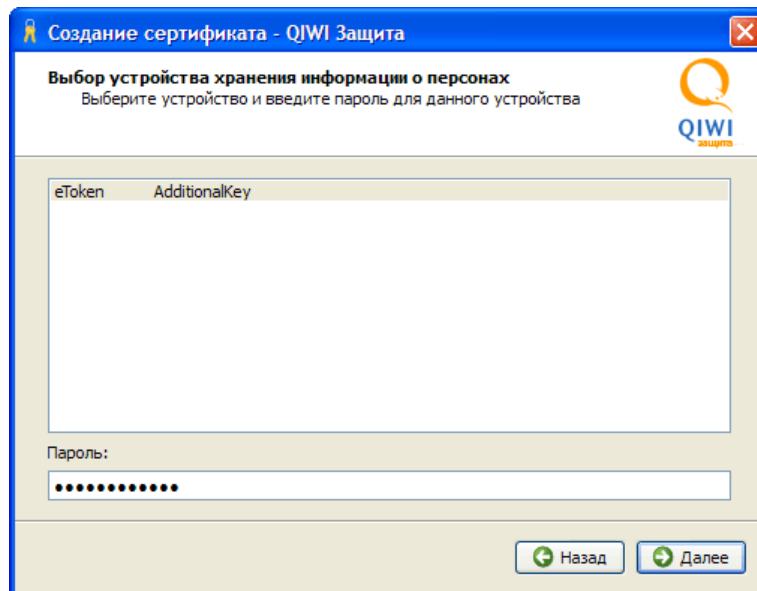
- Системное хранилище – [Приложение Г](#);
- Файл – [Приложение Д](#).

Рис. 6. Выбор хранилища сертификата



3. Выберите тип хранилища **eToken** (Рис. 6).
4. Выберите необходимое устройство из списка eToken и укажите пароль для него (Рис. 7).

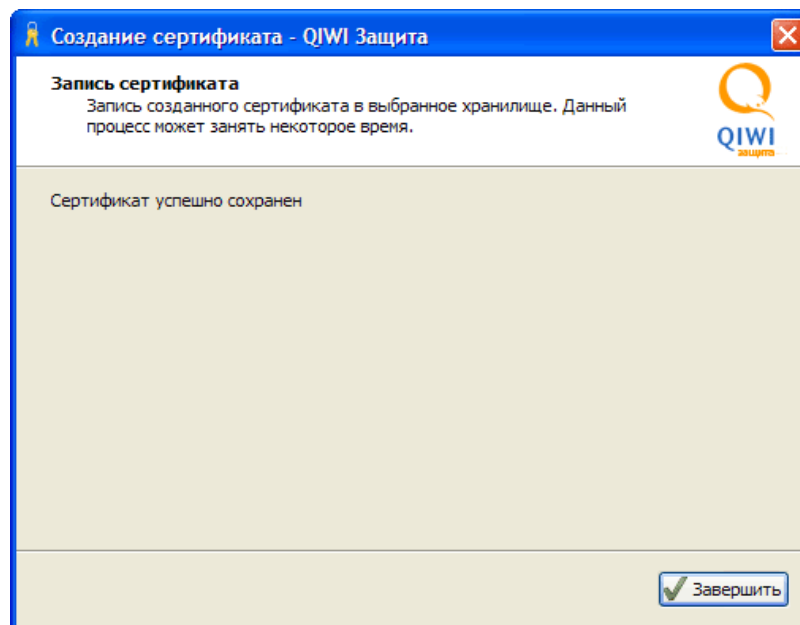
Рис. 7. Выбор устройства хранения информации

**ПРИМЕЧАНИЕ**

Если на eToken установлен пароль, требующий смены при первом использовании, вам будет предложено сменить его на постоянный (см. [Приложение Б](#))

5. Дождитесь сообщения «*Сертификат успешно сохранен*» и нажмите кнопку **Завершить** ([Рис. 8](#)).

Рис. 8. Запись сертификата



Сертификат сохранен на eToken, его можно использовать для входа на сайт.

Подробнее об авторизации на агентском сайте с помощью сертификата см. в [Приложении В](#).

7. СОЗДАНИЕ/УДАЛЕНИЕ ПЕРСОНЫ ДЛЯ QIWI КАССИР/QIWI КАССИР 1С

ПО *QIWI Защита* позволяет сгенерировать (а также удалить ранее созданные) авторизационные данные персоны для работы с ПО *QIWI Кассир*.

7.1. Создание персоны

ВНИМАНИЕ

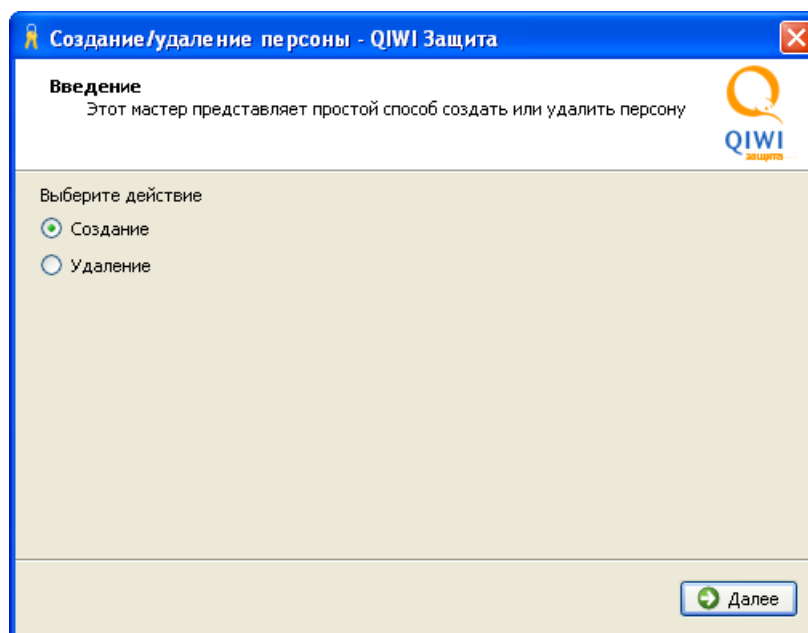
Перед созданием персоны с помощью ПО *QIWI Защита* прочтите раздел [5](#).

Для создания авторизационных данных персоны выполните следующее:

1. В главном окне приложения выберите **Создание/удаление персоны для QIWI Кассир/QIWI Кассир 1С** (см. [Рис. 3](#)).

Будет открыт *Мастер управления персонами* ([Рис. 9](#)).

Рис. 9. Мастер управления персонами



2. Выберите **Создание** и нажмите кнопку **Далее**.

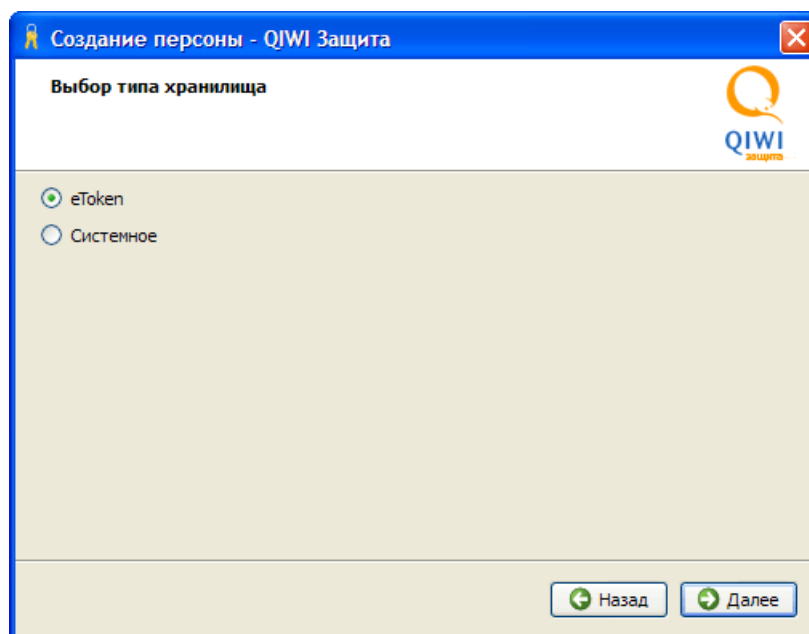
ВНИМАНИЕ

Далее описаны шаги при выборе типа хранилища **eToken**, т.к. это хранилище является наиболее безопасным.

При сохранении авторизационных данных персоны в системном хранилище обязательно прочтите [Приложение Г](#).

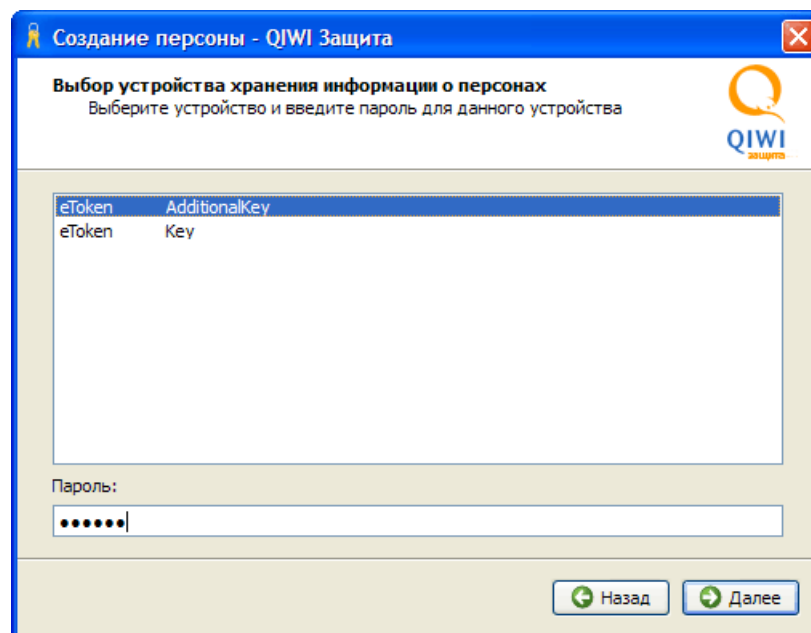
3. Выберите тип хранилища **eToken** ([Рис. 10](#)).

Рис. 10. Выбор устройства хранения информации о персонах



4. Выберите необходимый eToken и укажите пароль для него ([Рис. 11](#)).

Рис. 11. Выбор устройства хранения информации

**ПРИМЕЧАНИЕ**

Если на eToken установлен пароль, требующий смены при первом использовании, вам будет предложено сменить его на постоянный (подробнее см. в пункте 1 [Приложения Б](#)).

Рис. 12. Ввод информации о персоне

Создание/удаление персоны - QIWI Защита

Ввод информации о персоне
Введите информацию о персоне, которая должна быть записана в хранилище

Псевдоним:

Логин:

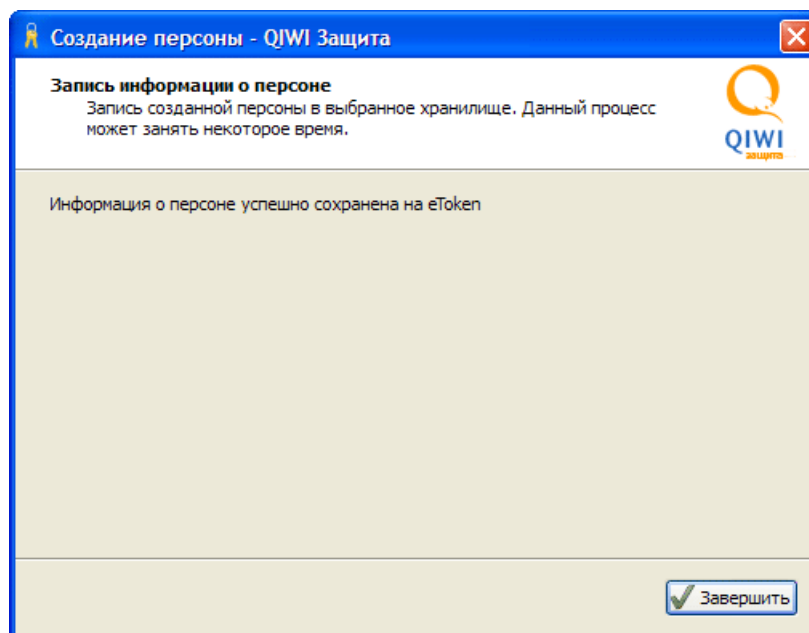
ID терминала:

Пароль:

Показать пароль

5. Введите данные персоны и нажмите кнопку **Далее** (Рис. 12):
 - **Псевдоним** – введите любое имя учетной записи, которое в дальнейшем будет использоваться для авторизации в ПО *QIWI Кассир*.
 - **Логин** – логин персоны.
 - **ID терминала** – номер терминала.
 - **Пароль** – одноразовый пароль для сертификата.
 - **Показать пароль** – флаг позволяет отображать значение поля **Пароль**.
6. Дождитесь сообщения «*Информация о персоне успешно сохранена на eToken*» и нажмите кнопку **Завершить** (Рис. 13).

Рис. 13. Успешная запись данных



Авторизационные данные персоны сохранены на eToken.

7.2. Удаление персоны ПО QIWI Кассир

Для удаления авторизационных данных персоны в главном окне приложения выберите (см. [Рис. 3](#)).

С помощью мастера управления персонами выполните следующее:

1. Выберите **Удалить**.
2. Выберите тип хранилища:
 - **eToken**;

ПРИМЕЧАНИЕ



Вам будет предложено выбрать необходимый **eToken** и указать пароль к нему.

- **Системное хранилище**;
3. Выберите псевдоним персоны, авторизационные данные которой необходимо удалить.
4. Нажмите кнопку **Далее**.

Авторизационные данные персоны будут удалены.

8. НАСТРОИТЬ ЭТОТ КОМПЬЮТЕР ДЛЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

ПО *QIWI Защита* позволяет установить программное обеспечение для получения и установки сертификата ЭЦП.

При открытии ПО *QIWI Защита* автоматически выявляет наличие установленных программ *КриптоПро CSP* и *ЭЦП Browser Plug-in*. Если хотя бы одна из программ не установлена на компьютере пользователя, то ПО *QIWI Защита* предложит установку указанных программ.

ВНИМАНИЕ



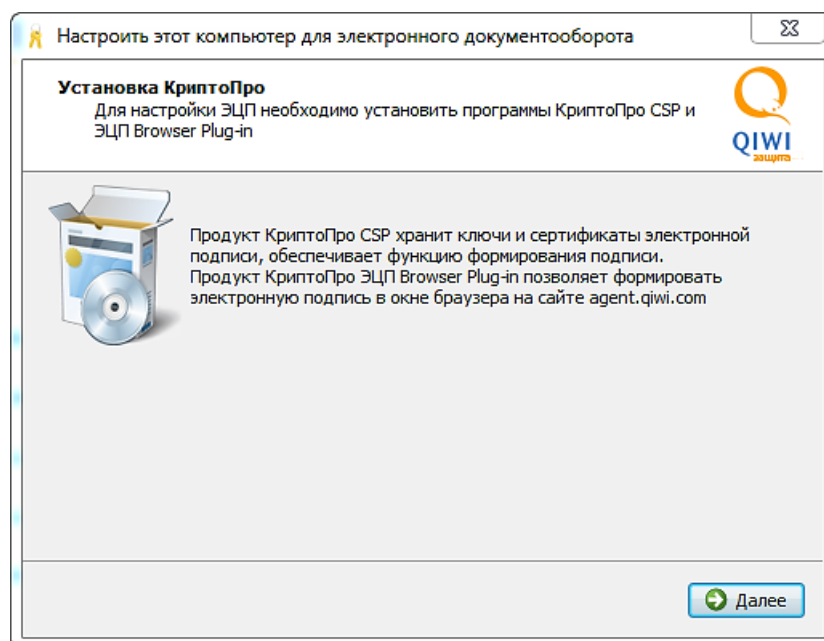
На компьютере с оперативной системой *Windows 7* все действия должны производиться под учетной записью администратора ПК.

Для установки ПО *КриптоПро CSP* и *ЭЦП Browser Plug-in* сделайте следующее:

1. В главном окне приложения выберите действие **Настроить этот компьютер для электронного документооборота** (см. [Рис. 3](#)).

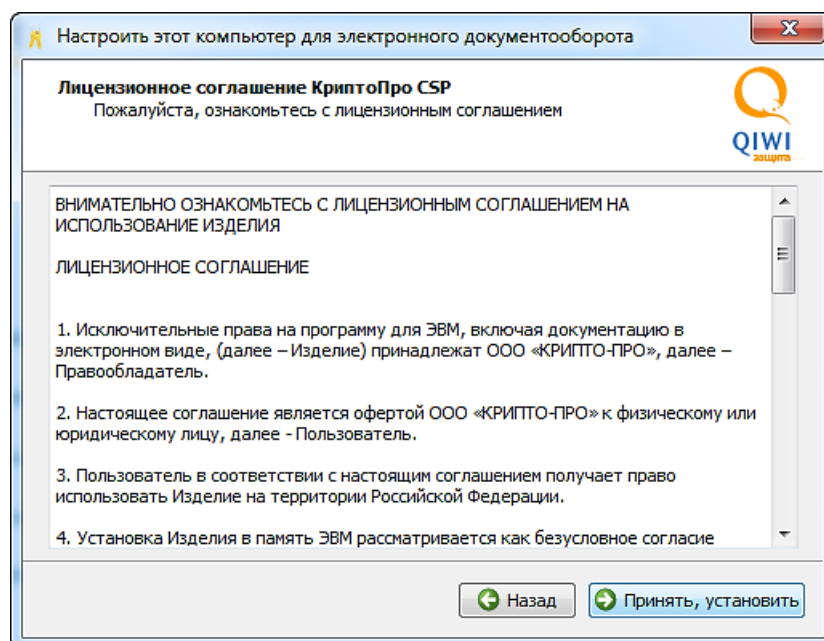
Будет открыт мастер настройки компьютера для электронного документооборота ([Рис. 14](#)).

Рис. 14. Подтверждение установки ПО



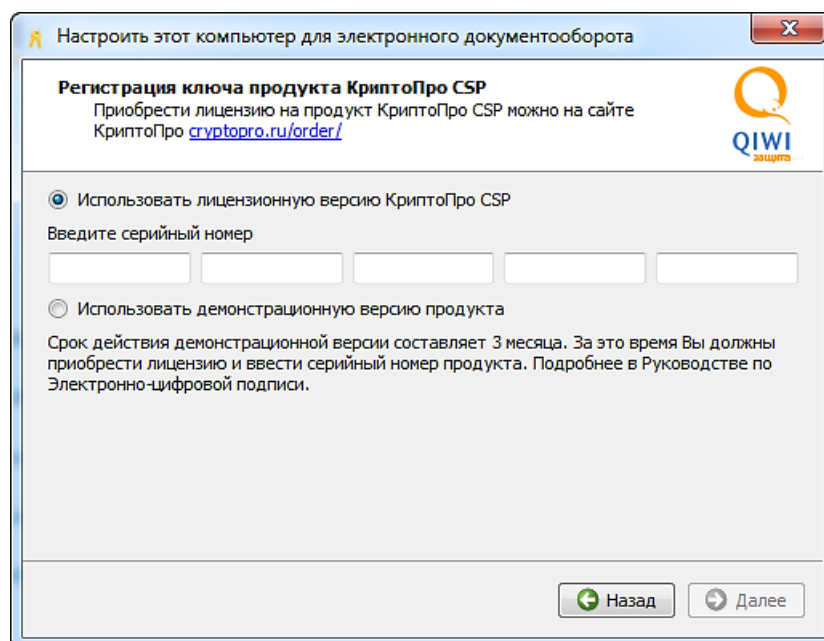
2. Нажмите кнопку **Далее**.
3. Ознакомьтесь с лицензионным соглашением и подтвердите свое согласие, нажав кнопку **Принять, установить** ([Рис. 15](#)).

Рис. 15. Лицензионное соглашение



4. В окне **Регистрация ключа продукта КристоПРО CSP** выберите один из пунктов (Рис. 16):

Рис. 16. Регистрация ключа продукта КристоПро CSP



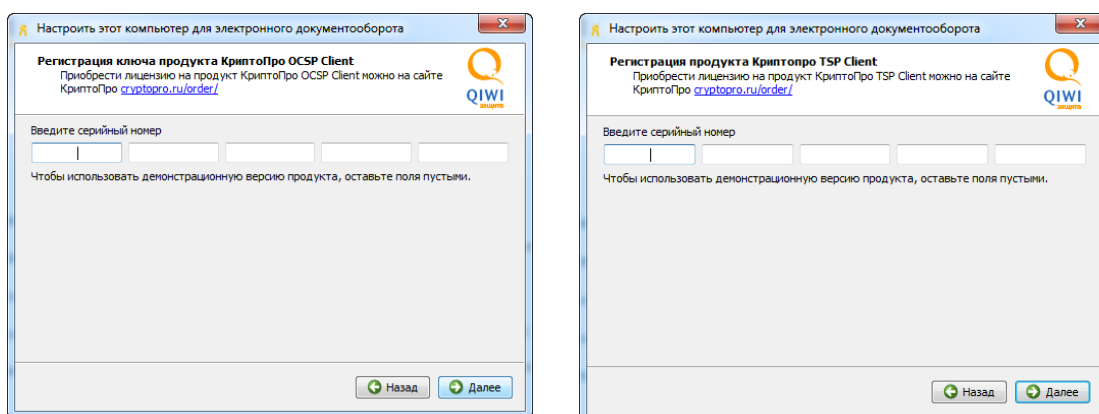
- **Использовать лицензионную версию продукта** - при выборе данного пункта необходимо указать серийный номер продукта в полях **Введите серийный номер**.

ВНИМАНИЕ

Приобрести лицензию на продукт КриптоПро CSP можно на сайте КриптоПро <http://cryptopro.ru/order/OrderForm.aspx>.

- **Использовать демонстрационную версию КриптоПро CSP** - при выборе данного пункта вводить серийный номер не надо, но возможность использовать ПО бесплатно доступна только в течение трех месяцев, после чего необходимо будет приобрести лицензию.
5. Нажмите кнопку **Далее**.
 6. В окне **Регистрация ключа продукта КриптоПро OCSP Client** и в окне **Регистрация продукта КриптоПро TSP Client** введите серийные номера продуктов *КриптоПро OCSP Client* и *TSP Client*. Если Вы еще не приобрели лицензии на них, оставьте поля пустыми (в последнем случае возможность использовать ПО бесплатно доступна только в течение трех месяцев, после чего необходимо будет приобрести лицензию). Затем нажмите кнопку **Далее** (Рис. 17).

Рис. 17. Регистрация ключа продукта КриптоПро OCSP Client и КриптоПро TSP Client



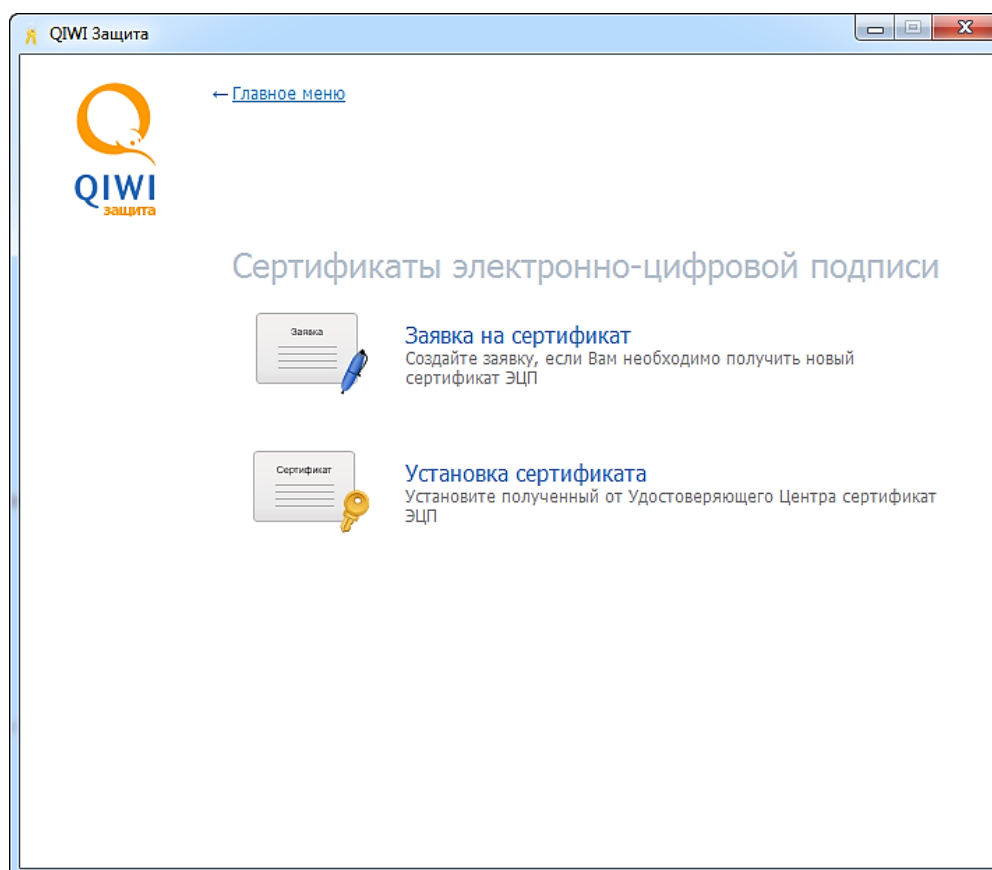
7. Дождитесь окончания установки ПО *КриптоПро CSP* и *ЭЦП Browser Plug-in*.
8. На последнем шаге мастера, выберите один из предложенных вариантов перезагрузки ПК:
 - **Перезагрузить сейчас** – рекомендуется выбрать данный пункт. Компьютер перезагрузится самостоятельно, после нажатия кнопки. После перезагрузки ПО QIWI Защита запустится автоматически.
 - **Перезагрузить позже** – пользователю придется самостоятельно провести аппаратную перезагрузку компьютера и вручную открыть ПО QIWI Защита.
9. Продолжите настройку для получения возможности подписывать документы в электронном виде. Для этого создайте запрос на получение сертификата ключа ЭЦП и/или установите уже полученный от Удостоверяющего Центра сертификат в хранилище (см. далее).

9. СЕРТИФИКАТЫ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

При выборе данного пункта можно оформить заявку на получение сертификата ЭЦП или произвести установку ранее полученного от удостоверяющего центра сертификата ЭЦП на компьютер ([Рис. 18](#)):

- Для оформления заявки на сертификат ЭЦП в главном окне программы выберите действие **Сертификаты электронно-цифровой подписи** → **Заявка на сертификат** (подробнее смотрите главу [9.1](#)).

Рис. 18. Меню «Сертификаты электронно-цифровой подписи»



- Для установки сертификата ЭЦП в главном окне программы выберите действие **Сертификаты электронно-цифровой подписи** → **Установка сертификата** (подробнее смотрите главу [9.2](#)).

9.1. Создание заявки на сертификат ЭЦП

При выборе данного шага откроется мастер создания заявки на сертификат.

1. В первом окне мастера укажите, получает ли ваша организация сертификат впервые, выбрав пункт **Да** или **Нет** ([Рис. 19](#)).

ВНИМАНИЕ

Если реквизиты (в т.ч. банковские) вашей организации после получения предыдущего сертификата изменились или вы получали сертификата на ДРУГОЕ юридическое лицо, выберите пункт **Да**.

Рис. 19. Выбор повторного или первого получения сертификата

Запрос на выпуск сертификата ЭЦП

Ваша организация получает сертификат в УЦ Инфотекс в первый раз?
Укажите нужную опцию для заявки

Да
После нажатия кнопки "Далее" Вам необходимо будет указать реквизиты Вашей организации

Нет
В сертификате будут указаны реквизиты Вашей организации, взятые из запроса, который отправлялся в Удостоверяющий Центр ранее

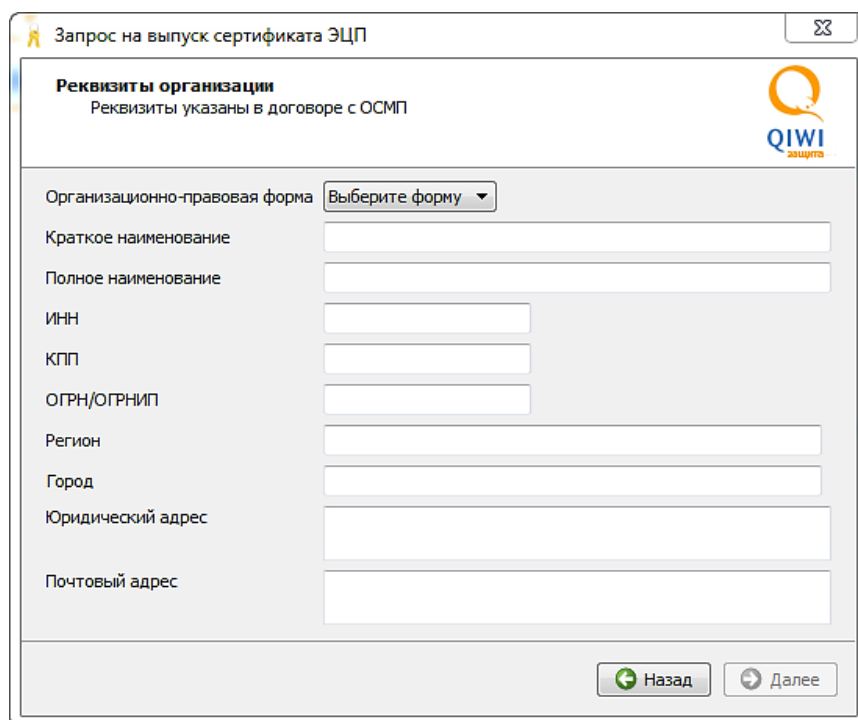
Далее

2. Нажмите кнопку **Далее**.
3. В окне **Реквизиты организации** укажите данные организации (Рис. 20). Пункты: **Краткое наименование, КПП, Юридический адрес** и **Почтовый адрес** - заполняются только в том случае, если организация получает сертификат впервые. Поле **КПП** не требуется заполнять индивидуальным предпринимателям.

СОВЕТ

Данные реквизиты также указаны в договоре ОСМП.

Рис. 20. Реквизиты организации



Запрос на выпуск сертификата ЭЦП

Реквизиты организации
Реквизиты указаны в договоре с ОСМП

QIWI защита

Организационно-правовая форма Выберите форму ▾

Краткое наименование

Полное наименование

ИНН

КПП

ОГРН/ОГРНИП

Регион

Город

Юридический адрес

Почтовый адрес

Назад Далее

4. Нажмите кнопку **Далее**.
5. Если вы получаете сертификат впервые, то в следующем окне мастера введите банковские реквизиты и нажмите кнопку **Далее** (Рис. 21). Если вы уже получали сертификат ранее, то ввод банковских реквизитов будет автоматически пропущен.

СОВЕТ



Данные реквизиты также указаны в договоре ОСМП.

Рис. 21. Ввод банковских реквизитов

Запрос на выпуск сертификата ЭЦП

Банковские реквизиты
Реквизиты указаны в договоре с ОСМП

QIWI защита

Наименование банка

БИК

к/с

р/с

Назад Далее

- Укажите данные будущего владельца сертификата (Рис. 22). Поле **Должность** заполнять не обязательно, если организация – индивидуальный предприниматель.

Рис. 22. Ввод данных будущего владельца сертификата

Запрос на выпуск сертификата ЭЦП

Данные будущего владельца сертификата
Данные сотрудника организации, для которого запрашивается выпуск сертификата

QIWI защита

Фамилия

Имя

Отчество

СНИЛС (если можете указать)

Должность в организации

Подразделение

Телефон

Факс

E-mail

Назад Далее

ВНИМАНИЕ

Будьте внимательнее при указании e-mail. В дальнейшем на указанную почту вам будет отправлен счет на оплату сертификата.

7. Нажмите кнопку **Далее**.
8. Укажите тип документа, подтверждающего полномочия будущего владельца сертификата на подписание документов от лица организации ([Рис. 23](#)).

Рис. 23. Указание документа, подтверждающего полномочия на подписание документов от лица организации

Запрос на выпуск сертификата ЭЦП

Данные будущего владельца сертификата
Данные сотрудника организации, для которого запрашивается выпуск сертификата

Тип документа, подтверждающего полномочия владельца сертификата на подписание документов

Устав
 Свидетельство
 Доверенность

Реквизиты доверенности

Укажите номер доверенности и дату выдачи. Например, № 123 от 01.01.2012

Назад Далее

Если в качестве документа выбран тип **Доверенность**, то в поле **Реквизиты доверенности** введите номер и дату выдачи.

9. Нажмите кнопку **Далее**.
10. Укажите, является ли будущий владелец сертификата руководителем организации, и нажмите кнопку **Далее** ([Рис. 24](#)).

Рис. 24. Указание должности будущего владельца сертификата

Запрос на выпуск сертификата ЭЦП

Данные будущего владельца сертификата
Данные сотрудника организации, для которого запрашивается выпуск сертификата

Является ли будущий владелец сертификата руководителем организации?

Руководитель

Не руководитель

Назад Далее

11. Если вы указали пункт **Руководитель**, то перейдите к следующему пункту. Если вы выбрали пункт **Не руководитель**, то в следующем окне введите данные руководителя организации и нажмите кнопку **Далее** (Рис. 25).

Рис. 25. Ввод информации о руководителе организации

Запрос на выпуск сертификата ЭЦП

Данные о руководителе организации
Данные руководителя организации, для сотрудника которой запрашивается выпуск сертификата

Укажите сведения о **руководителе** организации

ФИО

Должность в организации

Документ, на основании которого действует

Устав

Свидетельство

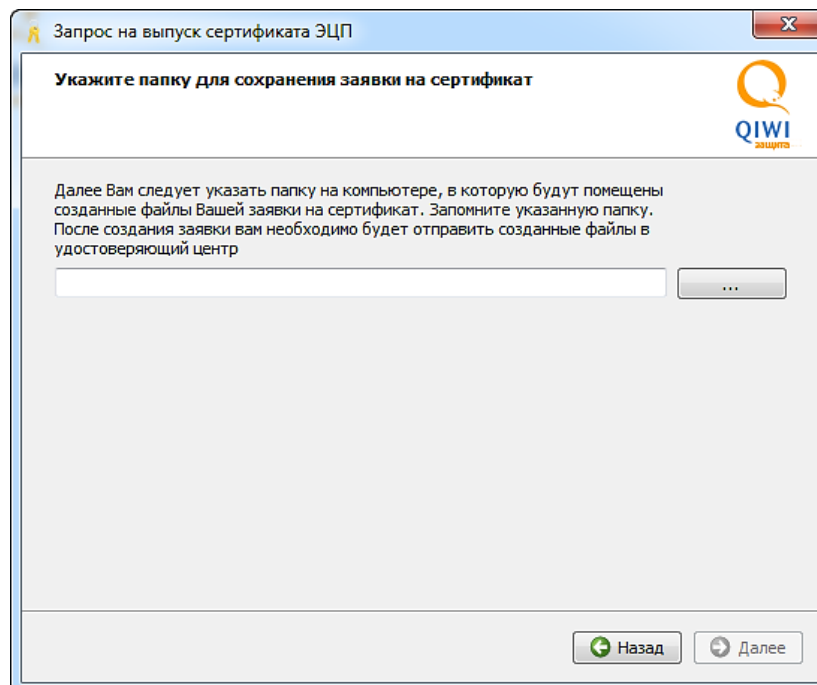
Доверенность

Реквизиты доверенности

Назад Далее

12. Укажите папку, в которой будут сохранены созданные файлы **CertReq.p10** и **заявка.html**, которые по окончании работы мастера нужно будет отправить в удостоверяющий центр:

Рис. 26. Задание адреса для сохранения заявки на сертификат



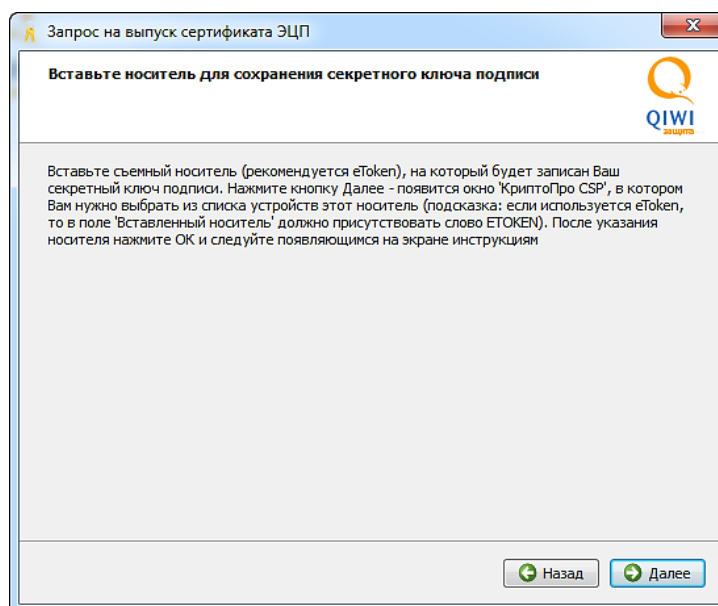
ВНИМАНИЕ



Запомните указанную папку. После создания запроса вам необходимо будет отправить созданные файлы в Удостоверяющий Центр.

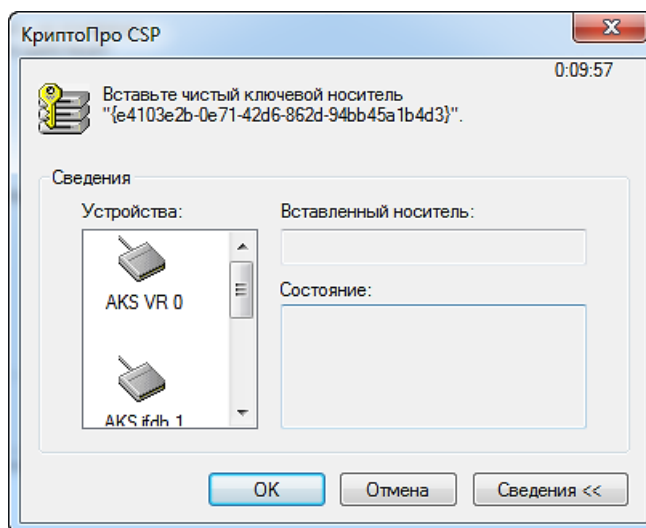
13. В следующем окне внимательно ознакомьтесь с информацией и нажмите кнопку **Далее** (Рис. 27).

Рис. 27. Информация о работе с носителем информации



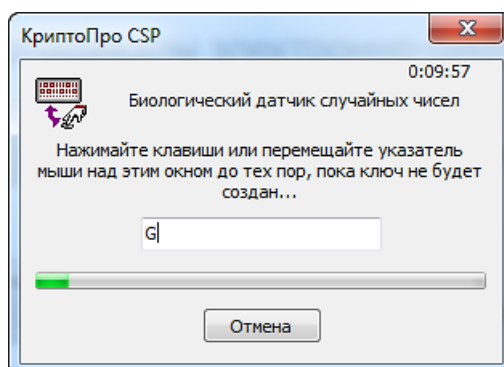
14. В появившемся окне **КриптоПро CSP** из списка устройств выберите внешний носитель, на который будут записаны ключи ЭЦП (выберите устройство, у которого в поле **Вставленный носитель** будет присутствовать слово **ETOKEN**) (Рис. 28).

Рис. 28. Выбор внешнего носителя



15. Нажмите кнопку **ОК**.
16. Откроется окно **Биологический датчик случайных чисел** (Рис. 29). Нажимайте на клавиатуре любые клавиши или перемещайте указатель мыши до тех пор, пока зеленый индикатор выполнения не дойдет до конца.

Рис. 29. Биологический датчик случайных чисел



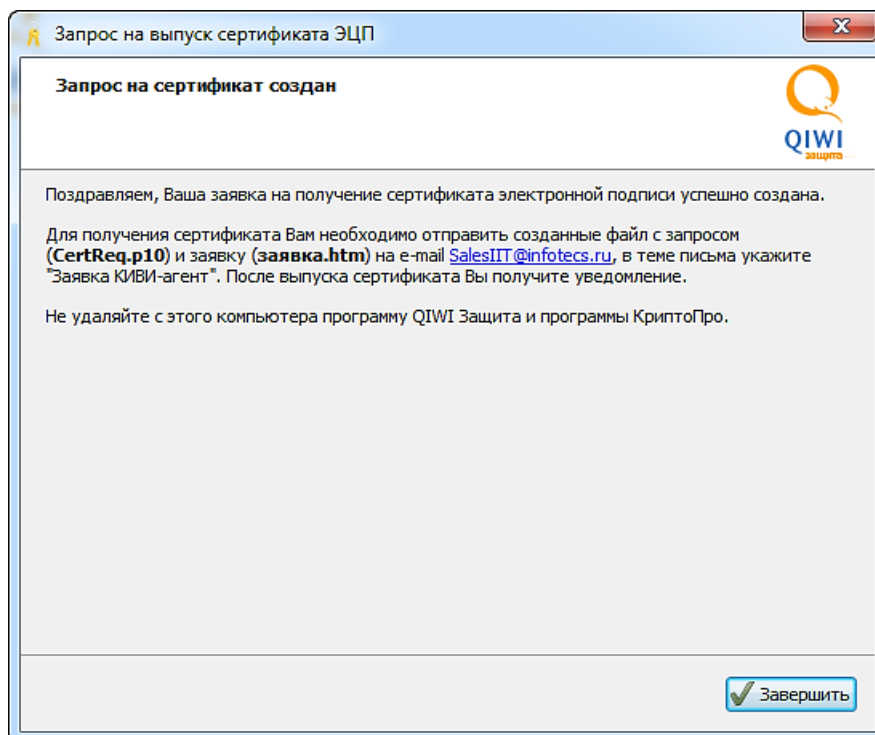
17. В новом окне укажите pin-код на контейнер (если в качестве контейнера ранее была выбрана смарт-карта eToken, то укажите пароль от этой смарт-карты), в который будут помещены созданные ключи ЭЦП, и нажмите кнопку **ОК**.

ВНИМАНИЕ

Pin-код необходимо обязательно запомнить и записать, так как он понадобится в дальнейшем. Pin-код должен быть известен только владельцу сертификата.

18. В окне **Запрос на сертификат создан** нажмите кнопку **Завершить** (Рис. 30).

Рис. 30. Завершение создания запроса на сертификат

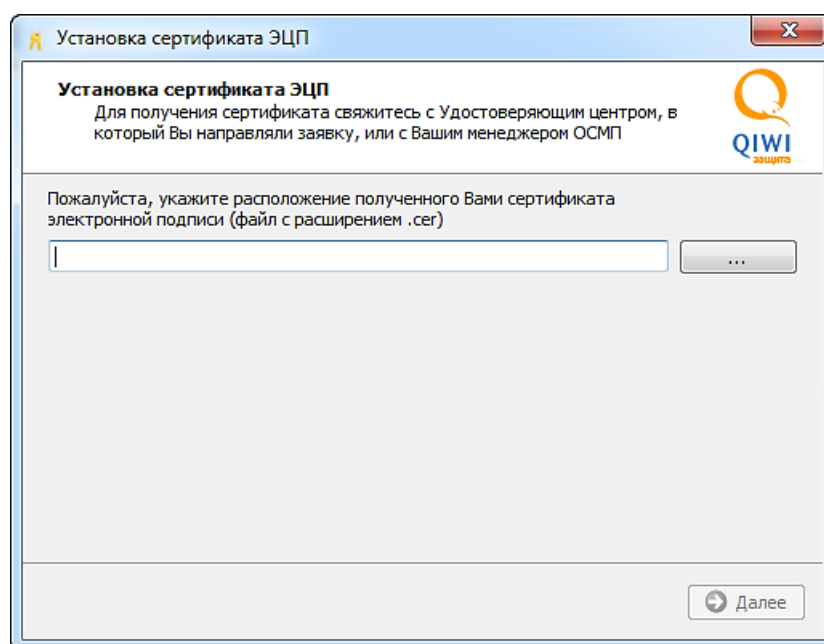


9.2. Установка сертификата

После того как сертификат ЭЦП получен (подробнее о том, как получить сертификат, смотрите в [Приложении Ж](#)) установите его, выполнив следующие действия:

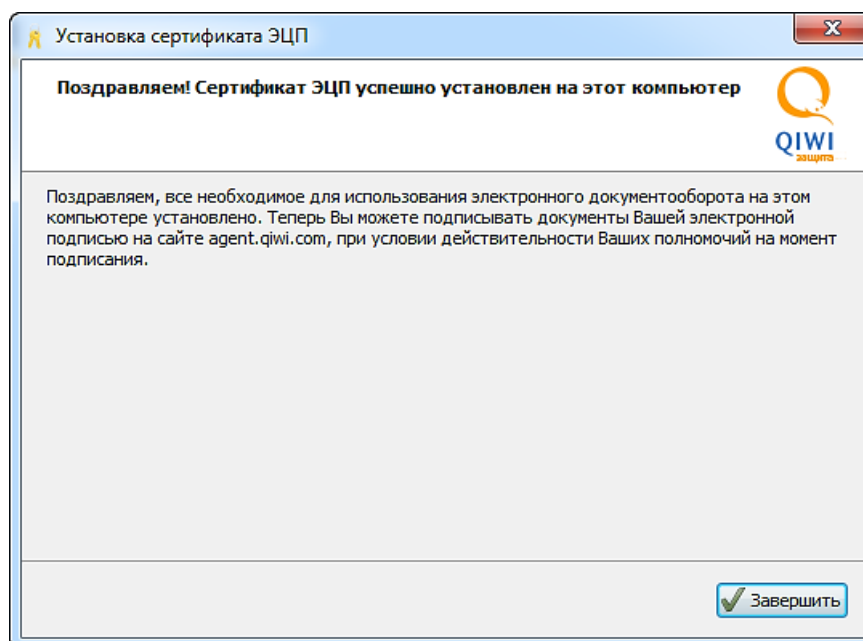
1. В главном окне ПО *QIWI Защита* выберите пункт **Сертификаты электронно-цифровой подписи** → **Установка сертификата**.
2. В окне мастера установки сертификата нажмите кнопку **Обзор** и выберите файл полученного сертификата ([Рис. 31](#)).

Рис. 31. Выбор расположения сертификата



3. Нажмите кнопку **Далее**.
4. В окне **Завершения установки сертификата** нажмите кнопку **Завершить** ([Рис. 32](#)).

Рис. 32. Завершение установки сертификата



Установка сертификата завершена.

10. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Приложение реализует следующие дополнительные возможности:

- [Список сертификатов](#) – открывает системное хранилище сертификатов;
- [Сетевые настройки](#) – позволяет задать сетевые настройки для доступа к Интернету;
- [Загрузить драйверы](#) – позволяет загрузить драйверы, необходимые для работы с eToken в различных ОС;
- [Загрузить документацию](#) – позволяет загрузить последнюю версию руководства пользователя;
- [О программе](#) – открывает окно с информацией о приложении.

10.1. Список сертификатов

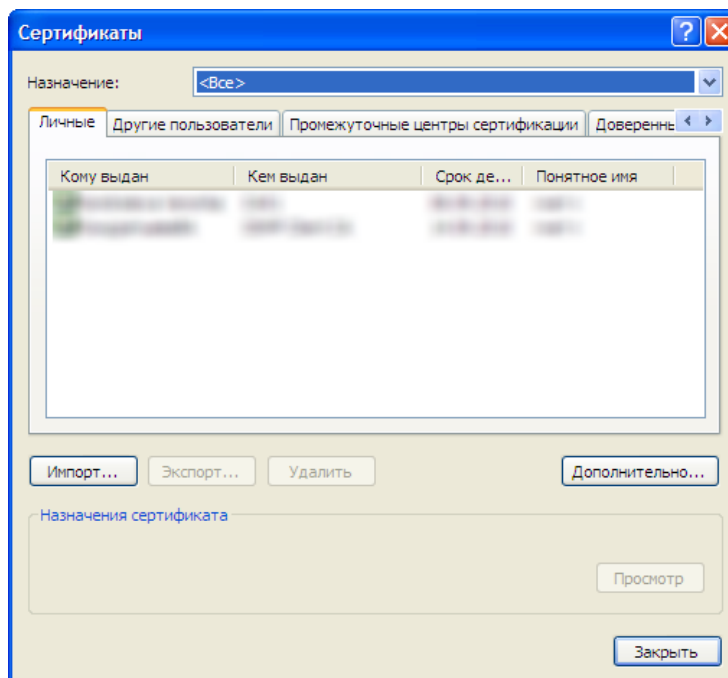
Для просмотра сертификатов, установленных в системе, выберите **Список сертификатов** в главном окне приложения (см. [Рис. 3](#)). Будет открыто окно **Сертификаты** ([Рис. 33](#)).

ПРИМЕЧАНИЕ



На вкладке **Личные** отображаются сертификаты, выданные данному пользователю ОС.

Рис. 33. Системные сертификаты

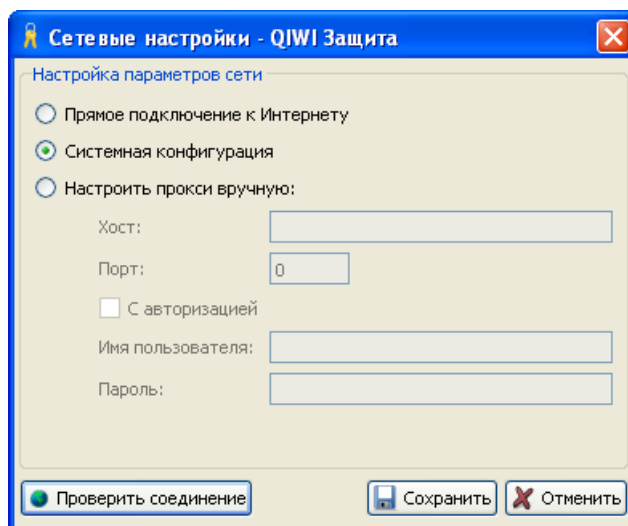


10.2. Сетевые настройки

Для изменения сетевых настроек выполните следующее:

1. В главном окне приложения выберите **Сетевые настройки** (см. [Рис. 3](#)).
Будет открыто диалоговое окно **Сетевые настройки** ([Рис. 34](#)).

Рис. 34. Установки прокси



2. Задайте необходимые настройки:
 - **Прямое подключение к Интернету** – соединение с сетью Интернет без прокси-сервера.
 - **Системная конфигурация** – при подключении будут использованы настройки свойств обозревателя.

ВНИМАНИЕ



Для использования данного типа подключения в *Свойствах обозревателя* должен быть установлен флаг **Автоматическое определение параметров**.

Проверить флаг можно, выполнив переход **Пуск**→**Панель управления**→**Свойства обозревателя**→**Подключения**→**Настройка сети**.

- **Настроить прокси вручную** – позволяет задать следующие настройки прокси:

ПРИМЕЧАНИЕ



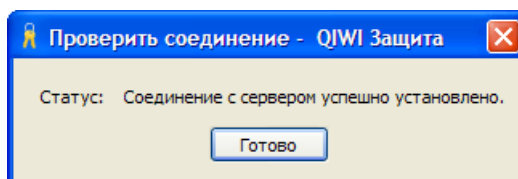
Информацию о прокси-сервере запросите у вашего системного администратора.

- ⊕ **Хост** – адрес прокси-сервера.
- ⊕ **Порт** – порт подключения к прокси-серверу.

- ⊕ **Авторизация** – установите флаг, если на прокси-сервере используется авторизация:
 - ❖ **Имя пользователя** и **Пароль** – укажите авторизационные данные подключения к прокси-серверу (если требуется).
- 3. Нажмите кнопку **Сохранить**.
- 4. Нажмите кнопку **Проверить соединение**.

Если все настройки были заданы правильно, вы увидите сообщение ([Рис. 35](#)).

Рис. 35. Успешное соединение с сервером



10.3. Загрузка драйверов

1. Для загрузки драйверов для работы с eToken выберите **Загрузить драйверы** в главном окне приложения (см. [Рис. 3](#)).
2. Появится список драйверов для различных операционных систем ([Рис. 36](#)).

Рис. 36. Загрузка драйверов

eToken драйвер для ОС Microsoft Windows (32-бит)
eToken драйвер для ОС Microsoft Windows (64-бит)
eToken драйвер для ОС Ubuntu 9.04 (32-бит)

- **eToken драйвер для ОС Microsoft Windows (32-бит)** – позволяет установить драйвер для работы с eToken в следующих 32-битных ОС: *Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008*.
- **eToken драйвер для ОС Microsoft Windows (64-бит)** – позволяет установить драйвер для работы с eToken в следующих 64-битных ОС: *Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008*.
- **eToken драйвер для Ubuntu (32-бит)** – позволяет установить драйвер для работы с eToken в операционной системе *Ubuntu 9.04*.

10.4. Загрузка документации

Для получения руководства пользователя к текущей версии ПО:

1. Выберите пункт **Загрузить документацию** в главном окне приложения ([Рис. 3](#)).
2. С помощью окна проводника укажите место, куда будет сохранен документ.
3. Нажмите кнопку **Сохранить**.

Документ будет загружен.

10.5.0 программе

Просмотреть информацию о приложении можно, выбрав пункт **О программе** в главном окне приложения (см. [Рис. 3](#)).

Будет открыто окно с информацией о приложении ([Рис. 37](#)).

Рис. 37. О программе



11. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

Ошибка 202 при записи сертификата

Проблема: при попытке записать сертификат возникает ошибка данных запроса 202

Решение:

- Убедитесь в том, что вы вводите существующий логин;
- Проверьте правильность написания логина или фамилии персоны (отсутствие недопустимых символов);
- Возможно настройки сети не позволяют сформировать запрос на получение сертификата. Попробуйте отправить запрос в другом интернет канале.

Ошибка «Неверный пароль» при получении сертификата

Проблема: при получении сертификата возникает ошибка, с неверным паролем.

Решение: проверять, чтобы персона обладала нужными правами + привязка к терминалу, номер которого вводится в киви-защите.

Ошибка 49 при записи сертификата

Проблема: при попытке записать сертификат для приложения QIWI Кассир возникает ошибка 49

Данная ошибка возникает в том случае, если на ключе eToken уже присутствует сертификат для данной персоны.

Решение: удалить предыдущий сертификат.

Если удаление ненужных сертификатов не помогает, то необходимо произвести форматирование etoken

Потерян pin-код eToken

Проблема: pin-код неверно введен 10 раз, eToken заблокирован.

Решение:

1. Зайдите в свойства eToken;
2. Выберите пункт меню **Разблокировать eToken**;
3. Укажите пароль администратора;
4. Произведите разблокировку.

ВНИМАНИЕ



В том случае, если вы не знаете пароля администратора, то проблему решит только форматирование eToken с уничтожением всех данных.

Pin-код отформатированного eToken

Вопрос: какой pin-код у eToken после форматирования?

Ответ: 123467890 (если при инициализации не задавался иной).

Не определяется eToken

Проблема: eToken подключен, но система его не видит.

Решение:

- Проверьте правильность установки eToken в слоте;
- Вставьте eToken в другой слот;
- Перезагрузите компьютер;
- Переустановите драйверы eToken.

Перед установкой драйверов, необходимо сохранить путь к ранее установленным драйверам, и при переустановке указать этот путь.

ПРИМЕЧАНИЕ



Драйвера eToken должны быть установлены на системном диске с операционной системой.

Где взять eToken

Вопрос: где я могу приобрести eToken, и какая модель мне нужна?

Ответ: вам нужна модель ключа eToken pro java. По вопросам приобретения обращайтесь к курирующему менеджеру.

Форматирование eToken

Вопрос: как отформатировать eToken?

Ответ: откройте свойства eToken и выберите пункт меню **Инициализация** → **Форматирование**.

Вместимость eToken

Вопрос: сколько сертификатов можно сохранить на одном eToken.

Ответ: по умолчанию на eToken можно сохранить 5 сертификатов. Для того чтобы увеличить объем ключа, необходимо при инициализации (форматировании) на вкладке **Дополнительно** задать нужное количество сертификатов.

ПРИЛОЖЕНИЕ А: Рекомендации по безопасности

Для предотвращения несанкционированного проведения платежей с другого оборудования необходимо осуществить «привязку» каждого Терминала к серийному номеру оборудования. Определить серийный номер конкретного типа Терминала можно следующим образом:

- *QIWI Кассир* – в окне авторизации, нажав кнопку **Инфо** (либо в меню приложения, выбрав **QIWI→Помощь→О программе**).
- *QIWI POS Nurit* – в меню POS терминала, выбрав **Сервис→Серийный номер**.
- *Автомат самообслуживания* – в разделе **Монитор терминалов** личного кабинета агента. Серийный номер указан в поле **Инфо** после версии ПО.

Серийный номер необходимо указать в поле **Привязан к SN** в разделе **Редактирование терминала** (в личном кабинете агента).

Для снижения ущерба и локализации источника в случае кражи учётных данных Персоны (под *Персоной* понимается учетная запись для доступа к Системе), необходимо при проведении платежей использовать учётные записи с минимальным набором прав *Продавец*. Кроме того, следует произвести привязку Персон к Терминалам, с которых эти Персоны проводят платежи.

Для защиты от кражи компьютерными вирусами авторизационных данных персон необходимо использовать антивирусные средства защиты компьютеров, с которых ведётся работа с Системой. Рекомендуется также использовать криптоключи eToken Pro. Настоятельно не рекомендуется заходить в Систему с общедоступных компьютеров (например, с компьютеров в интернет-кафе).

На компьютерах, используемых для работы с Системой, рекомендуется ограничить доступ в сеть Интернет (кроме платежных серверов Системы). Также воздержаться от открытия подозрительных писем с вложениями. При получении такого письма от имени Оператора Системы рекомендуется переслать его в адрес sb@osmp.ru.

ПРИЛОЖЕНИЕ Б: Подготовка eToken к работе

Перед началом использования eToken необходимо отформатировать, а также сменить пароль администратора, установленный по умолчанию.

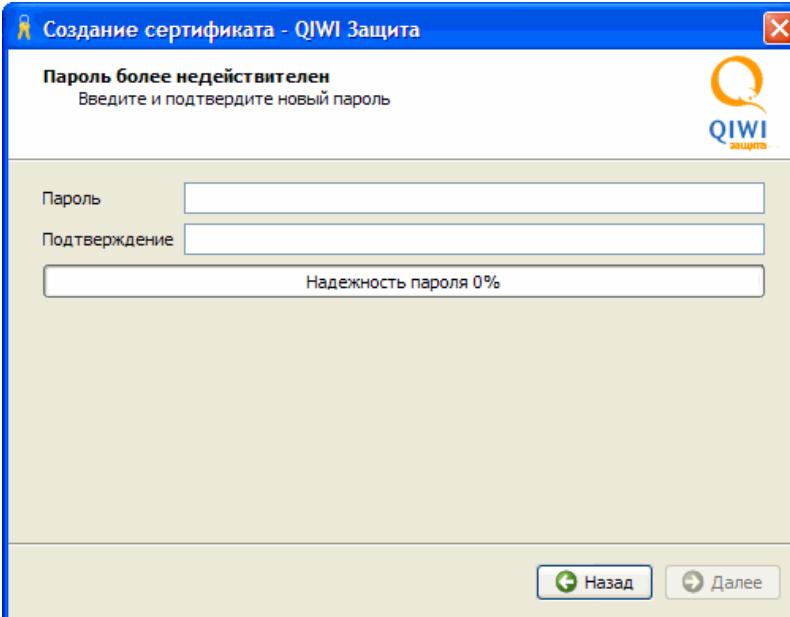
Приложение содержит инструкции:

1. [Смена пароля в ПО QIWI Защита](#) – процесс смены пароля на постоянный в случае, если вы уже начали, например, генерировать сертификат.
2. [Форматирование eToken](#) – процесс форматирования и смены пароля с помощью драйвера eToken.
3. [Смена пароля eToken](#) – смена пароля через драйвер.

1. Смена пароля в ПО QIWI Защита

Мастер создания сертификата/персоны выполняет проверку пароля eToken. Если на eToken установлен пароль, требующий смены при первом использовании, вам будет предложено сменить его на постоянный (Рис. 38).

Рис. 38. Сообщение о необходимости смены пароля на eToken



В полях **Пароль** и **Подтверждение** укажите новый пароль и нажмите кнопку **Далее**.

ПРИМЕЧАНИЕ



В случае, если в интерфейсе ПО QIWI Защита сменить пароль к eToken не удалось, это можно сделать с помощью драйвера eToken (см. пункт 3 данного Приложения).

2. Форматирование eToken

ВНИМАНИЕ



При выполнении описанных ниже действий с eToken будет удалена вся информация.

Перед началом использования eToken необходимо отформатировать, а также сменить пароль администратора, установленный по умолчанию.

ПРИМЕЧАНИЕ

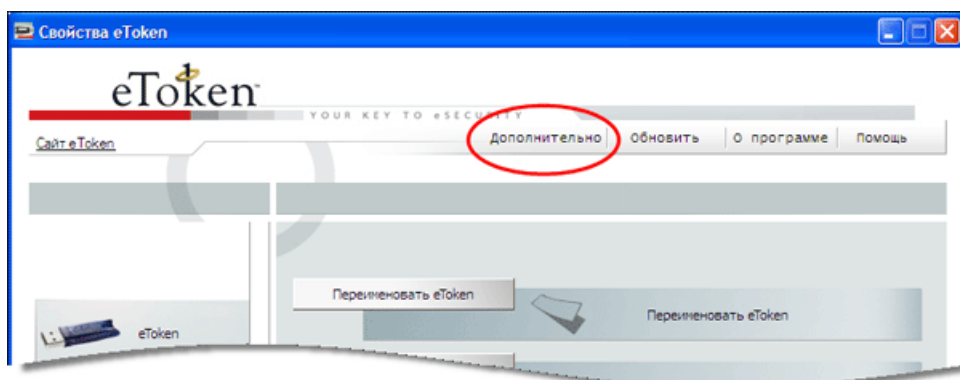


Пароль администратора позволяет разблокировать ключ, заблокированный вследствие превышения максимального числа попыток авторизации.

Для смены пароля администратора выполните следующее:

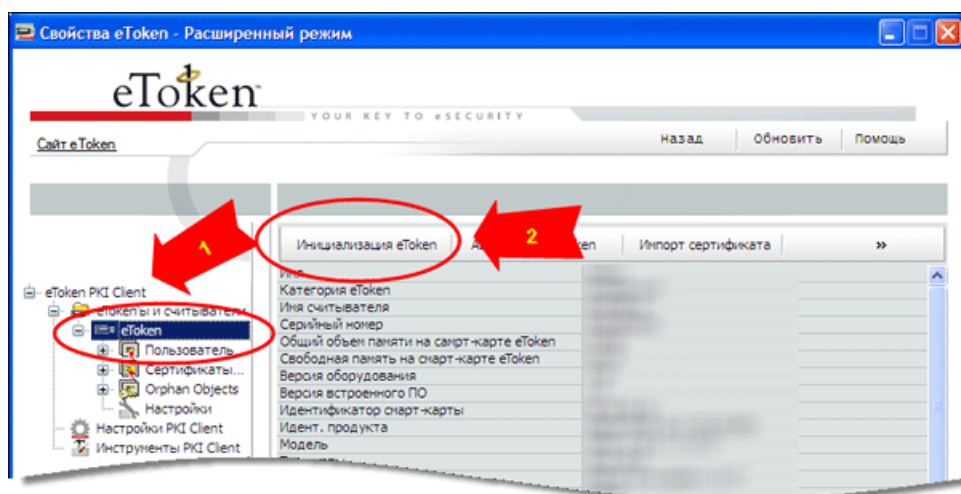
1. Перейдите **Пуск** → **Все программы** → **eToken** → **eToken Properties**.
2. В Свойствах eToken выберите вкладку **Дополнительно** (Рис. 39).

Рис. 39. Свойства eToken



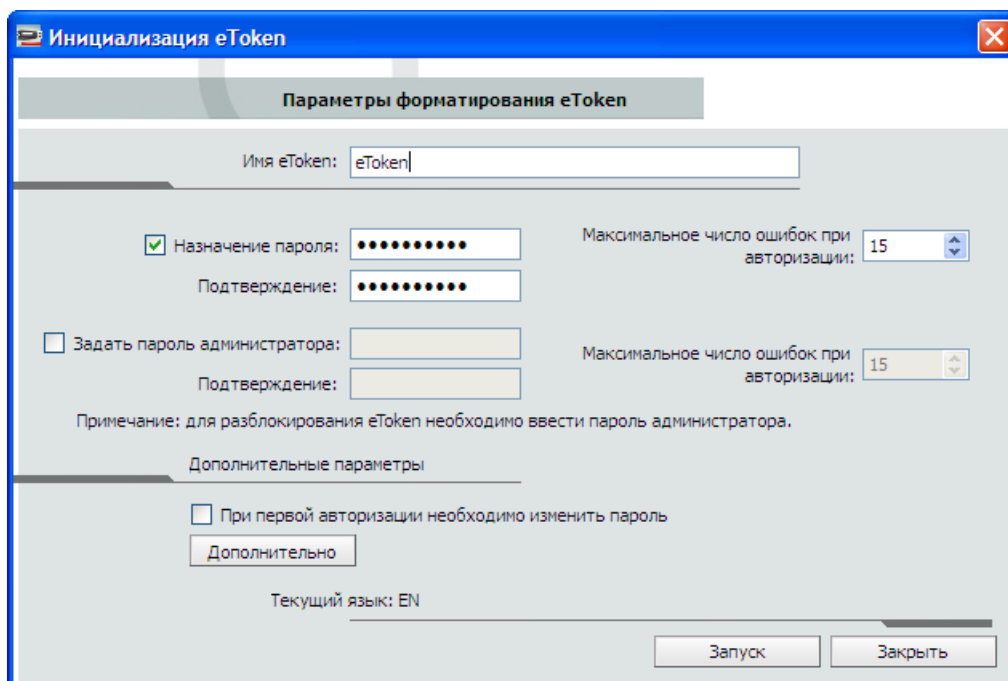
3. Выберите eToken и нажмите кнопку **Инициализация eToken** (Рис. 40).

Рис. 40. Выбор инициализации eToken



Будет открыто диалоговое окно **Инициализация eToken** (Рис. 41).

Рис. 41. Параметры форматирования eToken



- Установите флаг **Задать пароль администратора** и задайте пароль.
- Нажмите кнопку **Запуск**.

Будет выполнено форматирование eToken и пароль администратора будет изменен.

3. Смена пароля eToken

В случае если требуется только сменить пароль, а не форматировать eToken, выполните следующее:


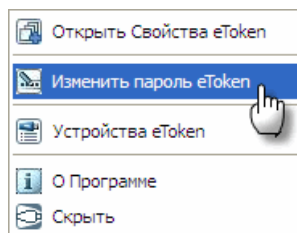
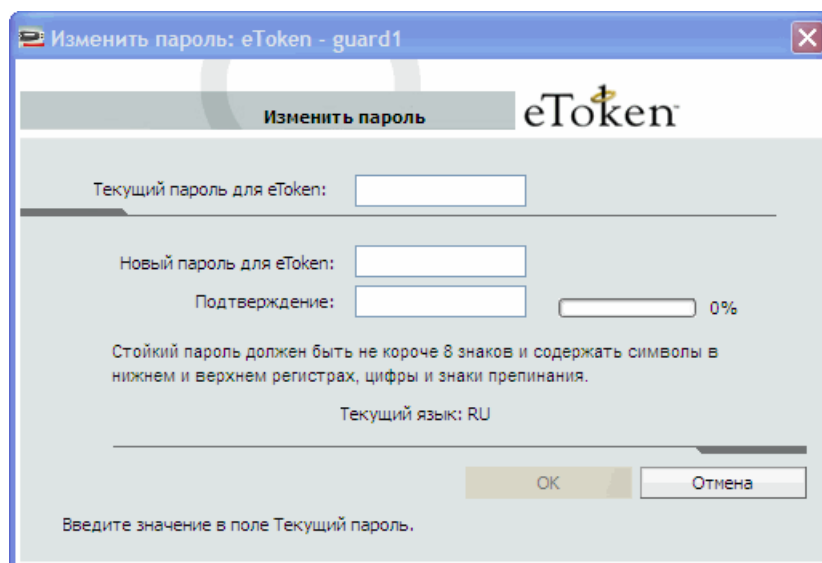
1. Нажмите правой кнопкой мыши на иконке **PKI Client**  в системном лотке.
2. Выберите пункт **Изменить пароль eToken**:

Рис. 42. Смена пароля eToken



3. Введите данные:
 - **Текущий пароль для eToken** – введите действующий пароль;
 - **Новый пароль** и **Подтверждение** – введите новый пароль.

Рис. 43. Смена пароля

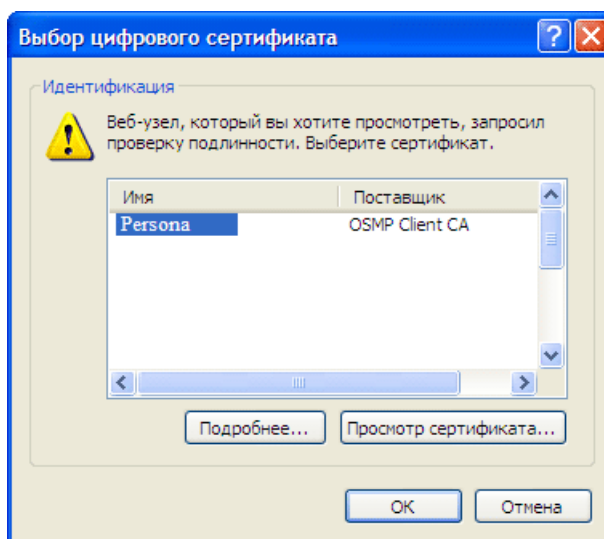


ПРИЛОЖЕНИЕ В: Авторизация на сайте

Для авторизации на агентском сайте ОСМП выполните следующее:

1. Перейдите по ссылке на необходимый сайт agent.qiwi.com, portal.qiwi.com или prov.osmp.ru.
Будет открыто диалоговое окно **Выбор сертификата** (Рис. 44).

Рис. 44. Выбор сертификата при входе на сайт



2. Выберите нужный сертификат.

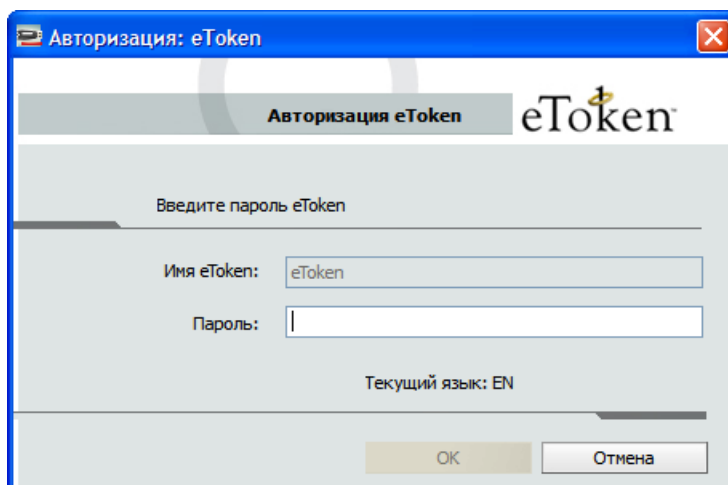
ПРИМЕЧАНИЕ



Сертификаты различаются по имени владельца, которое было задано при создании персоны на агентском сайте (в полях **Фамилия**, **Имя** и **Отчество**).

3. Введите пароль для хранилища сертификата:
 - eToken (Рис. 45)

Рис. 45. Ввод пароля eToken

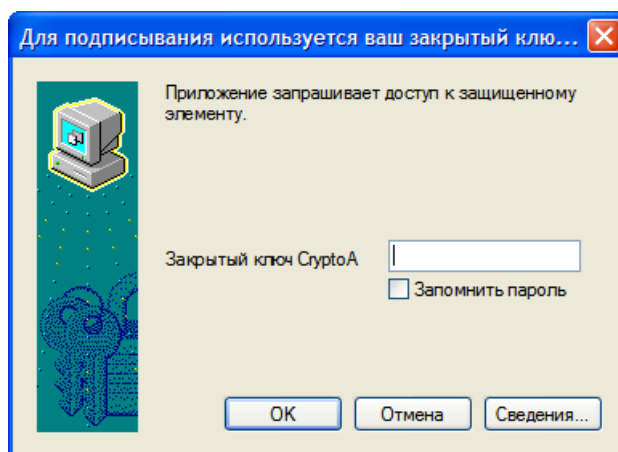


- Системное хранилище ([Рис. 46](#))

ПРИМЕЧАНИЕ

Пароль будет запрошен, если при создании сертификата вы выбрали высокий уровень безопасности системного хранилища.

Рис. 46. Ввод пароля для закрытого ключа в системном хранилище



После этого вы перейдете на сайт и получите доступ ко всем функциям в соответствии с ролью персоны.

ВНИМАНИЕ

При первой авторизации вам будет необходимо пройти процедуру подтверждения сертификата. Подробнее см. в [Руководстве по работе с сайтом](#) (раздел «Активация сертификата»).

ПРИЛОЖЕНИЕ Г: Сохранение в системное хранилище

ВНИМАНИЕ

Системное хранилище является менее защищенным, чем eToken. Использовать сертификат вы сможете только на том локальном компьютере, на котором он был сгенерирован.

Для сохранения в системное хранилище вам необходимо выполнить следующие шаги:

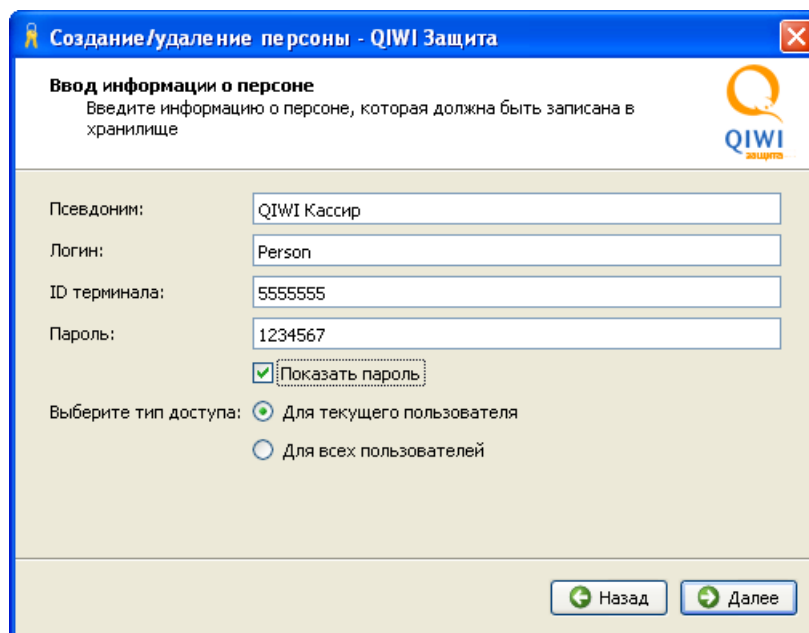
1. [Указать данные персоны в ПО QIWI Защита.](#)
2. [Сгенерировать ключ подписи RSA.](#)
3. [Завершить генерацию сертификата/создания персоны в ПО QIWI Защита.](#)

ШАГ 1. Ввод данных персоны

В зависимости от выполнения типа операции выполните следующее:

- **Получение доступа на агентский сайт:**
 - Выберите пункт **Получить доступ на агентский сайт.**
 - Введите авторизационные данные персоны (**логин** и **одноразовый пароль**).
 - Выберите тип хранилища **Системное.**
 - Перейдите к [ШАГУ 2.](#)
- **Создание персоны для QIWI Кассира:**
 - Выберите пункт **Создание/удаление персоны для QIWI Кассир.**
 - Выберите **Создание.**
 - Выберите тип хранилища **Системное.**

Рис. 47. Ввод информации о персоне



- Введите данные персоны (Рис. 47):
 - ⊕ **Псевдоним** – введите любое имя учетной записи, которое в дальнейшем будет использоваться для авторизации в ПО QIWI Кассир.
 - ⊕ **Логин** – логин персоны.
 - ⊕ **ID терминала** – номер терминала.
 - ⊕ **Пароль** – одноразовый пароль.
 - ⊕ **Показать пароль** – флаг позволяет отображать значение поля Пароль.

ПРИМЕЧАНИЕ

На данном шаге указываются данные персоны и терминала, ранее зарегистрированных на сайте <https://agent.osmp.ru>.

- Выберите тип доступа:
 - ⊕ **Для текущего пользователя** – авторизационные данные персоны сможет использовать только тот пользователь операционной системы Windows, под которым был выполнен вход в Систему.
 - ⊕ **Для всех пользователей** – авторизационные данные персоны сможет использовать любой пользователь операционной системы Windows.

ВНИМАНИЕ

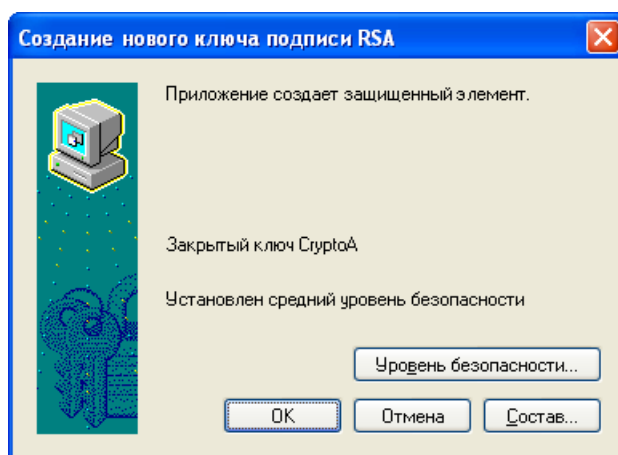
Сохранить авторизационные данные для всех пользователей можно только под учетной записью с правами Администратора.

- Нажмите кнопку **Далее**.
- Перейдите к [ШАГУ 2](#).

ШАГ 2. Генерация ключа подписи RSA

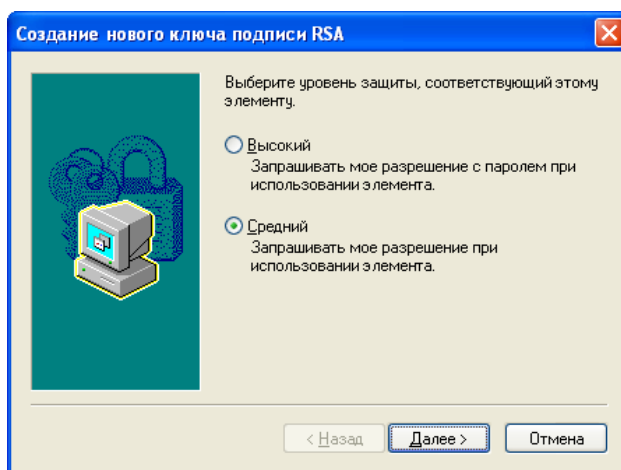
1. Нажмите кнопку **Уровень безопасности** ([Рис. 48](#)).

Рис. 48. Создание нового ключа подписи RSA



2. Выберите уровень защиты и нажмите кнопку **Далее** ([Рис. 49](#)):

Рис. 49. Выбор уровня защиты



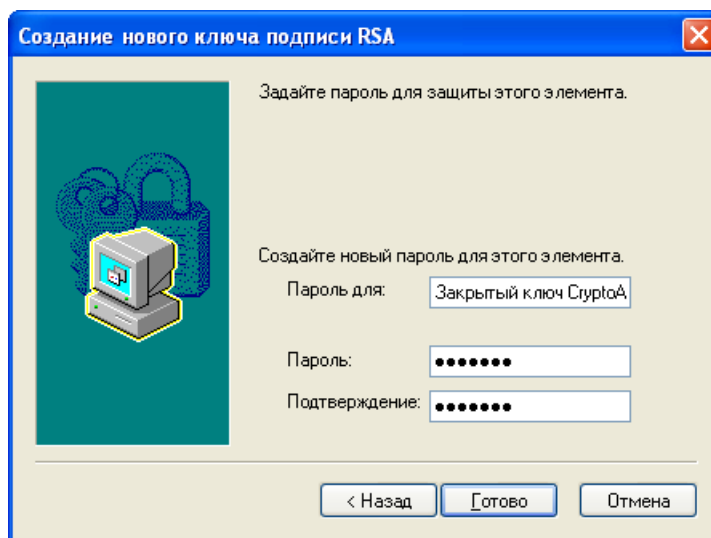
ПРИМЕЧАНИЕ



Для повышения уровня защиты установите **Высокий уровень**.

- **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** (Рис. 50):

Рис. 50. Установка пароля сертификата



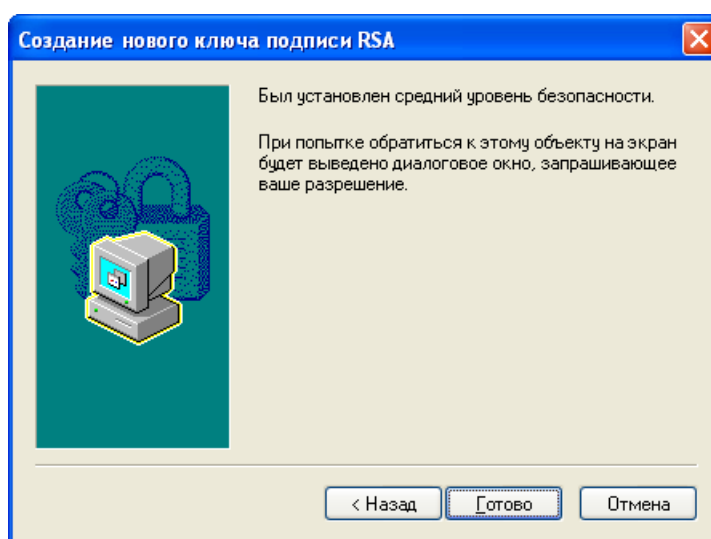
ПРИМЕЧАНИЕ



Данный пароль необходимо будет вводить при авторизации на сайте QIWI. Подробнее об авторизации на сайте см. в [Приложении В](#).

- **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** (Рис. 51):

Рис. 51. Информация об авторизации при среднем уровне безопасности системного хранилища



Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. [Рис. 48](#)).

3. Нажмите кнопку **ОК**.

Вы будете возвращены в главное окно ПО *QIWI Защита*.

ШАГ 3. Завершение генерации сертификата/создания персоны

Дождитесь отображения информации об окончании записи сертификата/данных персоны и нажмите кнопку **Завершить** (см. [Рис. 8](#)).

ПРИЛОЖЕНИЕ Д: Работа с «Файлом» сертификата

ВНИМАНИЕ

Файл служит только для переноса файла сертификата. Данная процедура не является безопасной и не рекомендована для использования. В процессе переноса файл может попасть к злоумышленникам, что может привести к значительному материальному ущербу и невозможности работы с Системой.

Приложение содержит инструкцию по следующим действиям:

1. [Сохранение сертификата в «Файл»](#).
2. [Экспорт сертификата в системное хранилище](#).

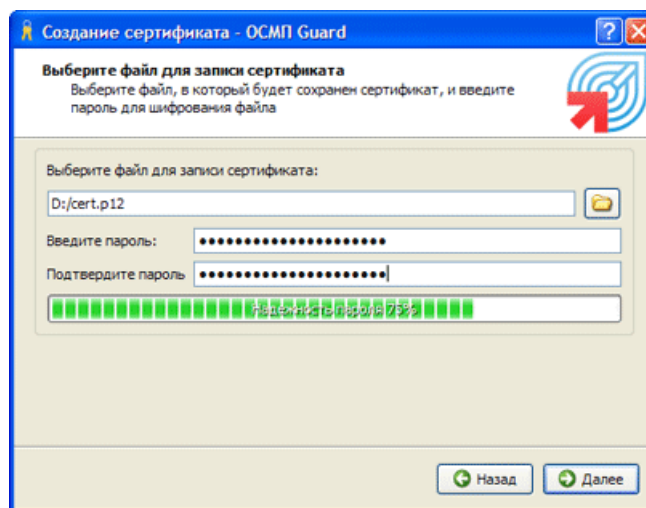
1. Сохранение сертификата в «Файл»

Для сохранения сертификата в **Файл** выполните следующее:

1. Пройдите шаги с 1 по 4, описанные в разделе [6](#).
2. Выберите тип хранилища **Файл**.

Вы перейдете к следующему шагу ([Рис. 52](#)).

Рис. 52. Выбор файла для записи сертификата



3. Выберите файл для записи сертификата.

ПРИМЕЧАНИЕ

Укажите путь к файлу, используя кнопку , или укажите его вручную.

ВНИМАНИЕ

По умолчанию сертификат предлагается сохранить на рабочий стол под именем cert.p12. Изменяемая часть имени сертификата – cert (.p12 расширение файла). Если вы решили изменить имя файла, убедитесь что расширение осталось без изменения.

4. **Задайте пароль.** Данный пароль необходимо будет ввести при импорте сертификата в системное хранилище.

ПРИМЕЧАНИЕ

Для сохранения сертификата в файл уровень надежности должен быть не менее 75%.

5. Нажмите кнопку **Далее**.
Вы будете возвращены в *Мастер создания сертификатов*.
6. Дождитесь, пока *Мастер создания сертификатов* отобразит информацию об окончании записи сертификата, и нажмите кнопку **Завершить** (см. [Рис. 8](#)).

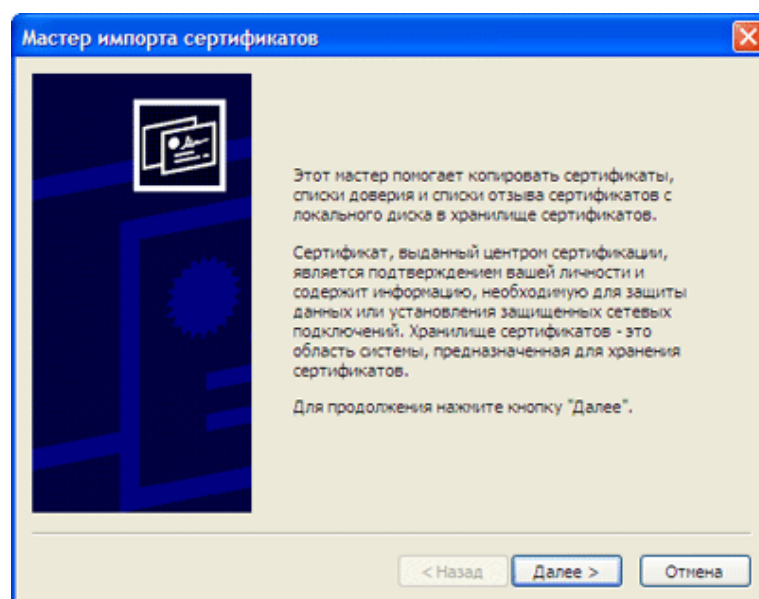
Сертификат будет сохранен в файле.

2. Экспорт сертификата

Для экспорта файла сертификата в системное хранилище выполните следующее:

1. Щелкните дважды левой кнопкой мыши по файлу сертификата.
Будет запущен *Мастер импорта сертификатов* ([Рис. 53](#)).

Рис. 53. Мастер импорта сертификатов

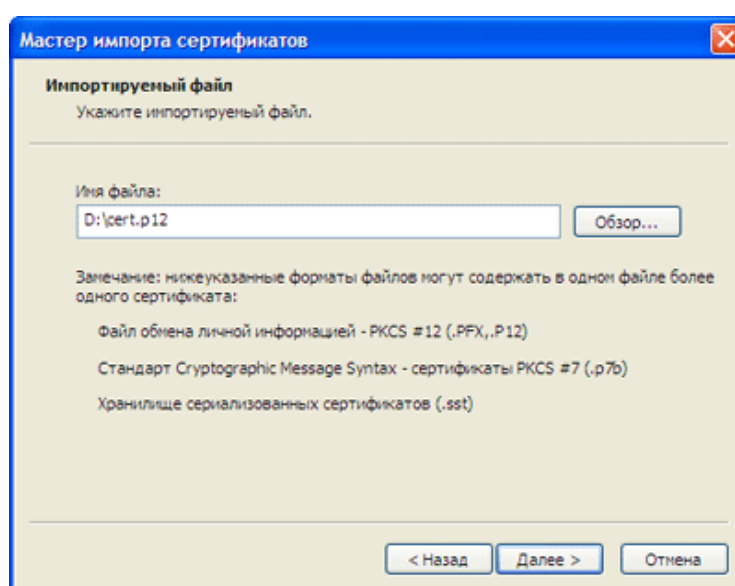


2. Для перехода к первому шагу нажмите кнопку **Далее**.
3. Подтвердите или укажите расположение файла сертификата.
4. Нажмите кнопку **Далее** (Рис. 54).

ПРИМЕЧАНИЕ

По умолчанию указан файл сертификата, с помощью которого был запущен *Мастер импорта сертификатов*.

Рис. 54. Импортируемый файл

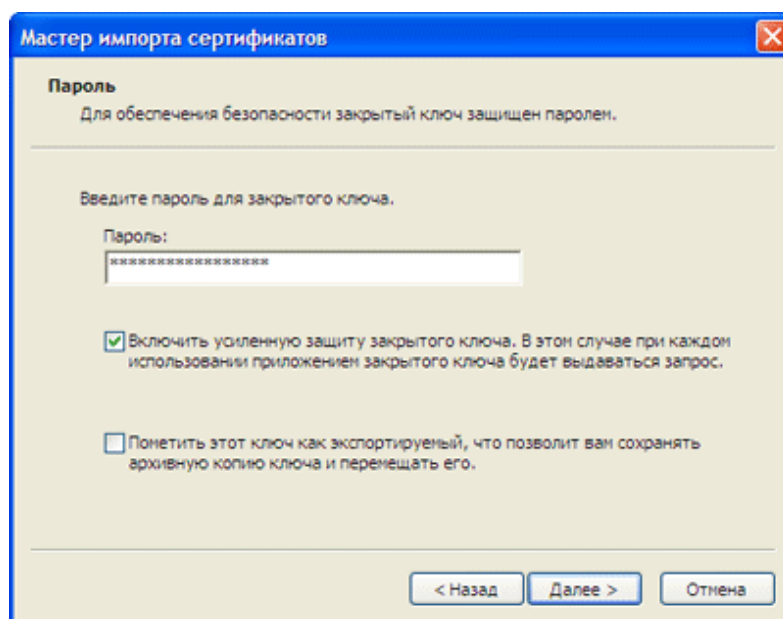


5. Установите флаг **Включить усиленную защиту ключа** (Рис. 55).

ПРИМЕЧАНИЕ

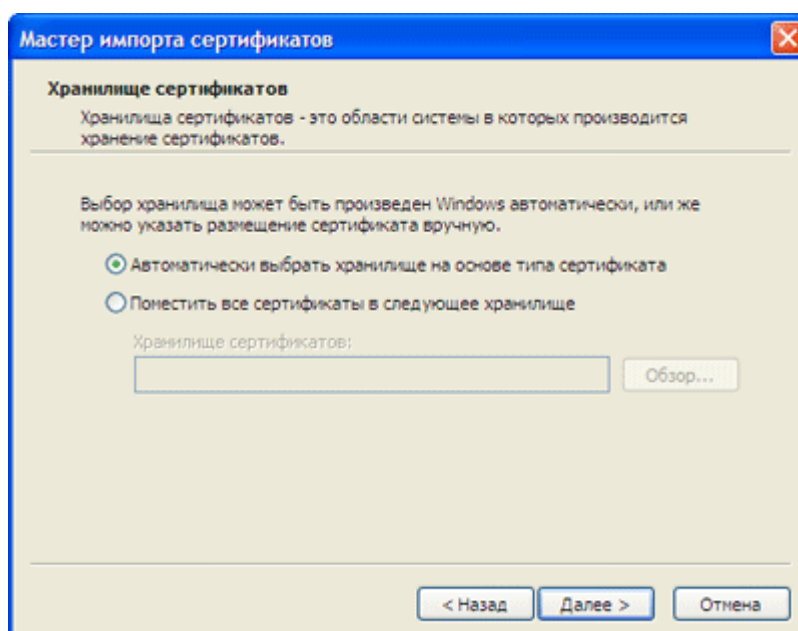
Установка данного флага необходима в целях повышения уровня защиты.

Рис. 55. Ввод пароля для файла сертификата



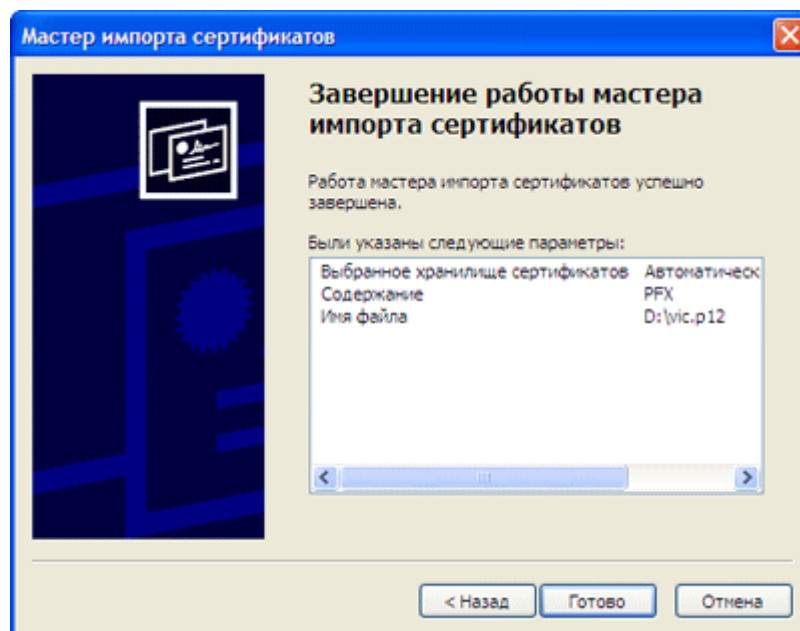
6. Введите пароль для доступа к файлу и нажмите кнопку **Далее**.
7. Выберите **Автоматически выбрать хранилище на основе типа сертификата** и нажмите кнопку **Далее** (Рис. 56).

Рис. 56. Выбор размещения сертификата



Будет выполнен импорт сертификата, и *Мастер импорта сертификатов* отобразит параметры импорта (Рис. 57).

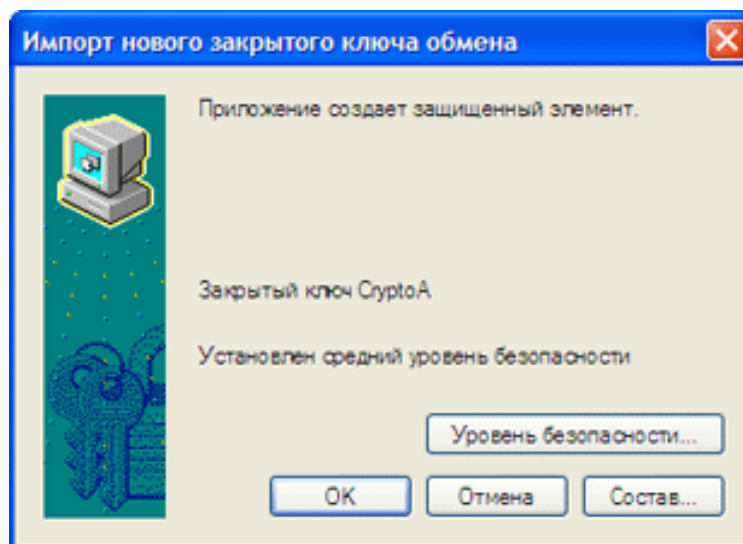
Рис. 57. Параметры импорта сертификата



8. Нажмите кнопку **Готово**.

Импорт сертификата в системное хранилище будет завершен и вам будет предложено задать уровень безопасности сертификата (Рис. 58).

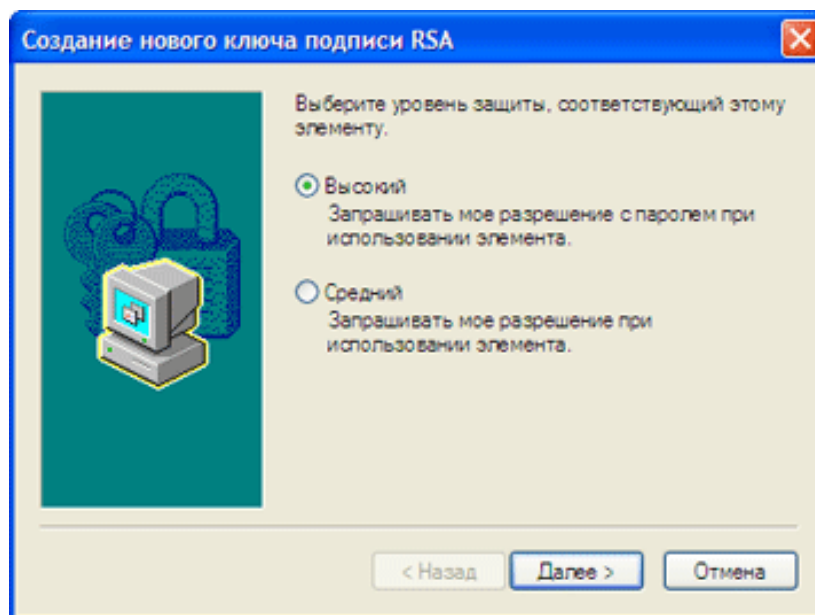
Рис. 58. Создание защищенного элемента



9. Нажмите кнопку **Уровень безопасности**.

Будет открыто диалоговое окно с выбором уровня защиты (Рис. 59).

Рис. 59. Выбор уровня безопасности



10. Выберите уровень безопасности и нажмите кнопку **Далее>**.

СОВЕТ

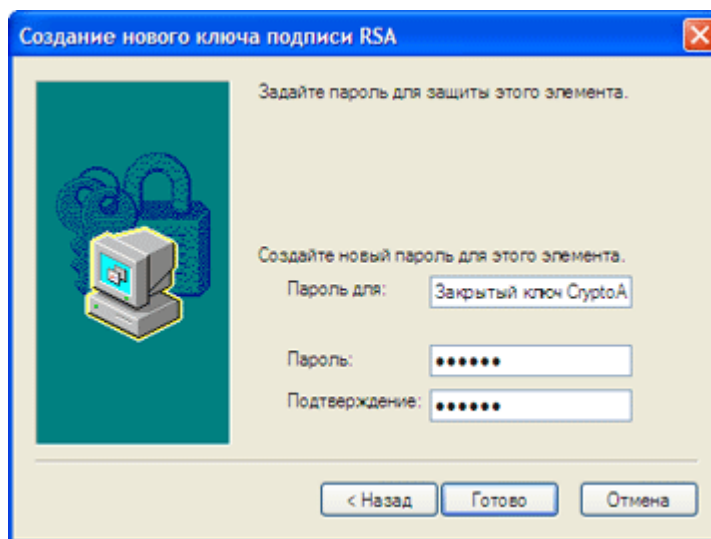
В целях повышения уровня защиты установите **Высокий уровень**.

- **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** (Рис. 60).

ПРИМЕЧАНИЕ

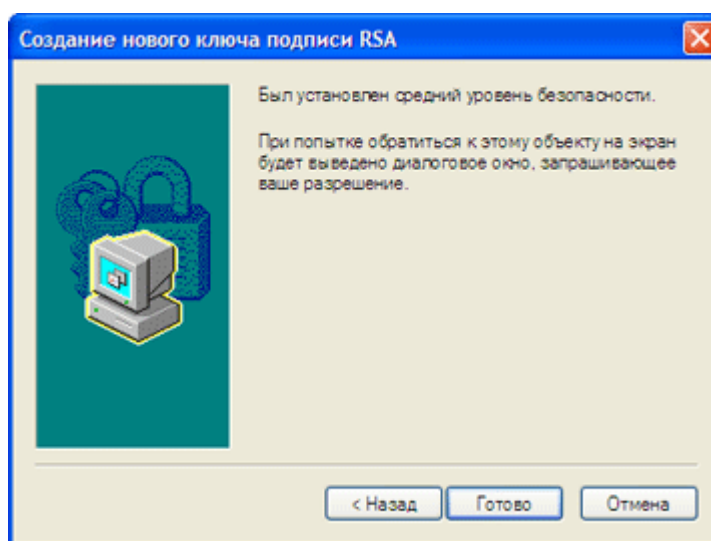
Данный пароль необходимо будет вводить при авторизации на сайте ОСМП. Подробнее об авторизации на сайте см. в [Приложении В](#).

Рис. 60. Установка пароля сертификата



- **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** (Рис. 61).

Рис. 61. Информация об авторизации при среднем уровне безопасности системного хранилища

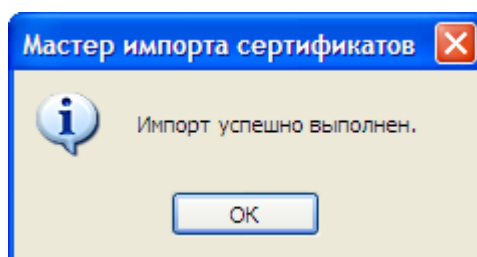


Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. Рис. 58).

11. Нажмите кнопку **ОК**.

Будет открыто диалоговое окно, информирующее об успешном импорте сертификата (Рис. 62).

Рис. 62. Успешный импорт сертификата



12. Нажмите кнопку **ОК**.
Настройки сертификата будут заданы.

ПРИЛОЖЕНИЕ Е: Синхронизация времени

Windows XP

Для синхронизации локального времени выполните следующее:

1. Выберите **Пуск→Панель управления→Дата и время**.
2. Выберите вкладку **Время Интернета**.
3. Нажмите кнопку **Обновить сейчас**.

При успешной синхронизации вы увидите сообщение «Время было успешно синхронизировано».

Windows Vista и Windows 7

Для синхронизации локального времени выполните следующее:

1. Выберите **Пуск→Панель управления→Дата и время**.
2. Перейдите на вкладку **Время Интернета**.
3. Нажмите кнопку **Изменить параметры**.
4. Нажмите кнопку **Обновить сейчас**.

При успешной синхронизации вы увидите сообщение «Время было успешно синхронизировано».

ПРИЛОЖЕНИЕ Ж: Получение сертификата ЭЦП

Для получения сертификата в удостоверяющем центре (далее УЦ) выполните следующее:

1. Отправьте созданные в приложении файл (**CertReq.p10**) и заявку (**заявка.htm**) на e-mail SalesIIT@infotecs.ru. В теме письма укажите «Заявка КИВИ-агент». Используйте электронную почту, указанную вами ранее при создании запроса на сертификат.
2. Получите в ответном письме счет на оплату и оплатите его.
3. Получите по электронной почте уведомление о готовности сертификата (процедура изготовления может занять до 10-ти дней с момента оплаты счета) и заберите его лично в ближайшем офисе, указанном сотрудником УЦ в письме.

ПРИМЕЧАНИЕ



При получении сертификата в УЦ (центральном офисе или региональном представительстве) при себе необходимо иметь:

- распечатанное заполненное заявление на сертификат ключа подписи (файл с заявлением вы получите от сотрудника УЦ в письме с подтверждением готовности сертификата);
- ксерокопию паспорта будущего владельца сертификата (копии всех страниц, где есть записи, заверенные подписью руководителя и печатью организации);

В случае если сертификат ключа подписи получает не владелец сертификата, а его уполномоченный представитель, ему дополнительно при себе требуется иметь:

- нотариально заверенную доверенность на получение сертификата ключа подписи, выданную ему будущим владельцем сертификата;
- копию своего паспорта.

Специалисты УЦ могут записать сертификат как на электронный носитель, предоставленный агентом, так и выдать его на своем электронном носителе.

СПИСОК РИСУНКОВ

Рис. 1. Мастер установки	8
Рис. 2. Финальный шаг установки	9
Рис. 3. Главное окно приложения	10
Рис. 4. Мастер создания сертификатов	14
Рис. 5. Ввод авторизационных данных	15
Рис. 6. Выбор хранилища сертификата	16
Рис. 7. Выбор устройства хранения информации	16
Рис. 8. Запись сертификата	17
Рис. 9. Мастер управления персонами	18
Рис. 10. Выбор устройства хранения информации о персонах.....	19
Рис. 11. Выбор устройства хранения информации.....	20
Рис. 12. Ввод информации о персоне	21
Рис. 13. Успешная запись данных	22
Рис. 14. Подтверждение установки ПО.....	23
Рис. 15. Лицензионное соглашение.....	24
Рис. 16. Регистрация ключа продукта КриптоПро CSP.....	24
Рис. 17. Регистрация ключа продукта КриптоПро OCSP Client и Криптопро TSP Client.....	25
Рис. 18. Меню «Сертификаты электронно-цифровой подписи»	26
Рис. 19. Выбор повторного или первого получения сертификата	27
Рис. 20. Реквизиты организации.....	28
Рис. 21. Ввод банковских реквизитов	29
Рис. 22. Ввод данных будущего владельца сертификата	29
Рис. 23. Указание документа, подтверждающего полномочие на подписание документов от лица организации.....	30
Рис. 24. Указание должности будущего владельца сертификата	31
Рис. 25. Ввод информации о руководителе организации.....	31
Рис. 26. Задание адреса для сохранения заявки на сертификат.....	32
Рис. 27. Информация о работе с носителем информации.....	33
Рис. 28. Выбор внешнего носителя	33
Рис. 29. Биологический датчик случайных чисел	34
Рис. 30. Завершение создания запроса на сертификат.....	34
Рис. 31. Выбор расположения сертификата	35
Рис. 32. Завершение установки сертификата	36
Рис. 33. Системные сертификаты	37
Рис. 34. Установки прокси.....	38
Рис. 35. Успешное соединение с сервером	39
Рис. 36. Загрузка драйверов.....	39
Рис. 37. О программе	40
Рис. 38. Сообщение о необходимости смены пароля на eToken	44
Рис. 39. Свойства eToken	45
Рис. 40. Выбор инициализации eToken.....	46
Рис. 41. Параметры форматирования eToken	46
Рис. 42. Смена пароля eToken	47
Рис. 43. Смена пароля.....	47
Рис. 44. Выбор сертификата при входе на сайт	48
Рис. 45. Ввод пароля eToken	49
Рис. 46. Ввод пароля для закрытого ключа в системном хранилище.....	49
Рис. 47. Ввод информации о персоне	51
Рис. 48. Создание нового ключа подписи RSA.....	52

Рис. 49. Выбор уровня защиты	52
Рис. 50. Установка пароля сертификата	53
Рис. 51. Информация об авторизации при среднем уровне безопасности системного хранилища ...	53
Рис. 52. Выбор файла для записи сертификата	55
Рис. 53. Мастер импорта сертификатов	56
Рис. 54. Имортируемый файл	57
Рис. 55. Ввод пароля для файла сертификата	58
Рис. 56. Выбор размещения сертификата	58
Рис. 57. Параметры импорта сертификата	59
Рис. 58. Создание защищенного элемента	59
Рис. 59. Выбор уровня безопасности	60
Рис. 60. Установка пароля сертификата	61
Рис. 61. Информация об авторизации при среднем уровне безопасности системного хранилища ...	61
Рис. 62. Успешный импорт сертификата	62