



QIWI ЗАЩИТА

вер. 1.8

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

вер. 1.6

МОСКВА
8-495-783-5959

РОССИЯ
8-800-200-0059

ФАКС
8-495-926-4615

WEB
WWW.OSMP.RU

СОДЕРЖАНИЕ

1.	ГЛОССАРИЙ	3
2.	ВВЕДЕНИЕ.....	4
2.1.	НАЗНАЧЕНИЕ ПРИЛОЖЕНИЯ	4
2.2.	ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ	4
3.	БЫСТРЫЙ СТАРТ.....	5
3.1.	СОЗДАНИЕ СЕРТИФИКАТА.....	5
3.2.	СОЗДАНИЕ ПЕРСОНЫ ДЛЯ ПО QIWI КАССИР.....	5
4.	УСТАНОВКА И ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ.....	6
4.1.	УСТАНОВКА ПРИЛОЖЕНИЯ.....	6
4.2.	ГЛАВНОЕ ОКНО ПРИЛОЖЕНИЯ.....	8
5.	ПРЕДВАРИТЕЛЬНАЯ ПОДГОТОВКА	9
5.1.	ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ.....	9
5.2.	СОЗДАНИЕ ПЕРСОНЫ ДЛЯ ПО «QIWI КАССИР»	9
6.	ПОЛУЧЕНИЕ ДОСТУПА НА АГЕНТСКИЙ САЙТ	10
7.	СОЗДАНИЕ/УДАЛЕНИЕ ПЕРСОНЫ ДЛЯ QIWI КАССИР.....	15
7.1.	СОЗДАНИЕ ПЕРСОНЫ.....	15
7.2.	УДАЛЕНИЕ ПЕРСОНЫ ПО QIWI КАССИР	19
8.	ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	20
8.1.	СПИСОК СЕРТИФИКАТОВ.....	20
8.2.	СЕТЕВЫЕ НАСТРОЙКИ	20
8.3.	ЗАГРУЗКА ДРАЙВЕРОВ	22
8.4.	ЗАГРУЗКА ДОКУМЕНТАЦИИ.....	22
8.5.	О ПРОГРАММЕ.....	22
ПРИЛОЖЕНИЕ А:	РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ	24
ПРИЛОЖЕНИЕ Б:	ПОДГОТОВКА ЕТОКЕН К РАБОТЕ.....	25
ПРИЛОЖЕНИЕ В:	АВТОРИЗАЦИЯ НА САЙТЕ	29
ПРИЛОЖЕНИЕ Г:	СОХРАНЕНИЕ В СИСТЕМНОЕ ХРАНИЛИЩЕ.....	31
ПРИЛОЖЕНИЕ Д:	РАБОТА С «ФАЙЛОМ» СЕРТИФИКАТА	35
ПРИЛОЖЕНИЕ Е:	СИНХРОНИЗАЦИЯ ВРЕМЕНИ	42
СПИСОК РИСУНКОВ		43

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>Одноразовый пароль</i>	Пароль персоны, использующийся при генерации сертификата/авторизационных данных персоны. Если процесс генерации был завершен ошибкой – вам будет необходимо сгенерировать новый одноразовый пароль.
<i>eToken</i>	Персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП).
<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 <https://portal.osmp.ru> (<https://agent.osmp.ru>);
 - провайдерский <https://prov.osmp.ru>.
- Сгенерировать авторизационные данные персоны для ПО *QIWI Кассир*.

ВНИМАНИЕ



Для повышения уровня безопасности авторизационные данные рекомендуется хранить на eToken.

2.2. Технические требования

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

- около 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, Windows 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**).
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 п. [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**.
2. Выберите **Создание**.
3. Выберите тип хранилища.

СОВЕТ

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

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

ПРИМЕЧАНИЕ

Процесс создания персоны для ПО QIWI Кассир подробно описан в п. [7.1](#).

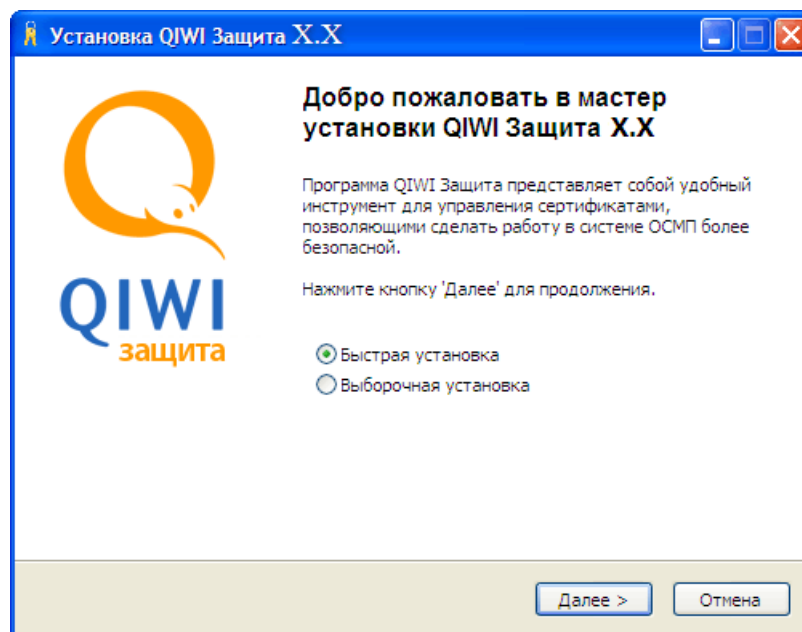
4. УСТАНОВКА И ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ

4.1. Установка приложения

Для установки приложения выполните следующее:

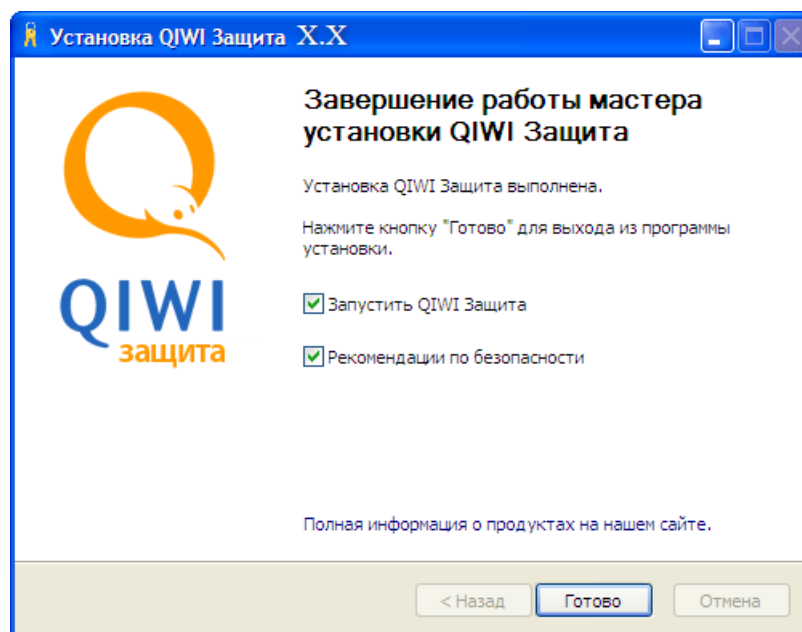
1. Скачайте последнюю версию приложения с сайта www.osmp.ru, раздел **Агентам→Скачать**.
2. Запустите файл *qiwiguard-x.x-ru-win.exe* (x.x – номер версии приложения) ([Рис. 1](#)).

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:
 - **Запустить QIWI Защита** – запустить приложение сразу после установки.
 - **Рекомендации по безопасности** – ознакомиться с рекомендациями по обеспечению безопасности при работе с *Системой*.

ПРИМЕЧАНИЕ

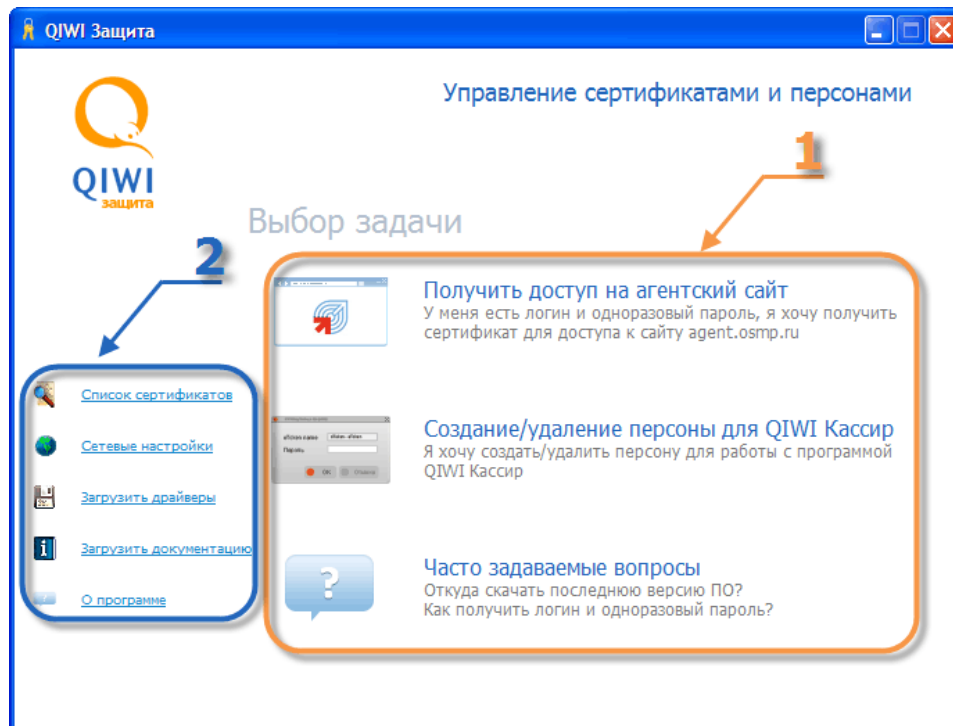
Для получения более подробной информации об этом или иных продуктах наших разработчиков нажмите на ссылку **Полная информация о продуктах на нашем сайте**.

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 сгенерировать сертификат для доступа на сайты <https://portal.osmp.ru>, <https://agent.osmp.ru> и <https://prov.osmp.ru>. Подробнее о генерации сертификата см. в п. [5](#).
 - **Создание/удаление персоны для QIWI Кассир** – позволяет создавать авторизационные данные персоны для работы с ПО *QIWI Кассир*, а также удалять их. Подробнее об управлении персонами см. в п. [6](#).
 - **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 Е](#)).

На <https://agent.osmp.ru> вам необходимо зарегистрировать:

- **Получение доступа на агентский сайт** – персону.
- **Создание 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](#) <https://agent.osmp.ru>.

5.1. Получение доступа на агентский сайт

Для генерации сертификата вам потребуется зарегистрировать на сайте <https://agent.osmp.ru> 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 <https://agent.osmp.ru> 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

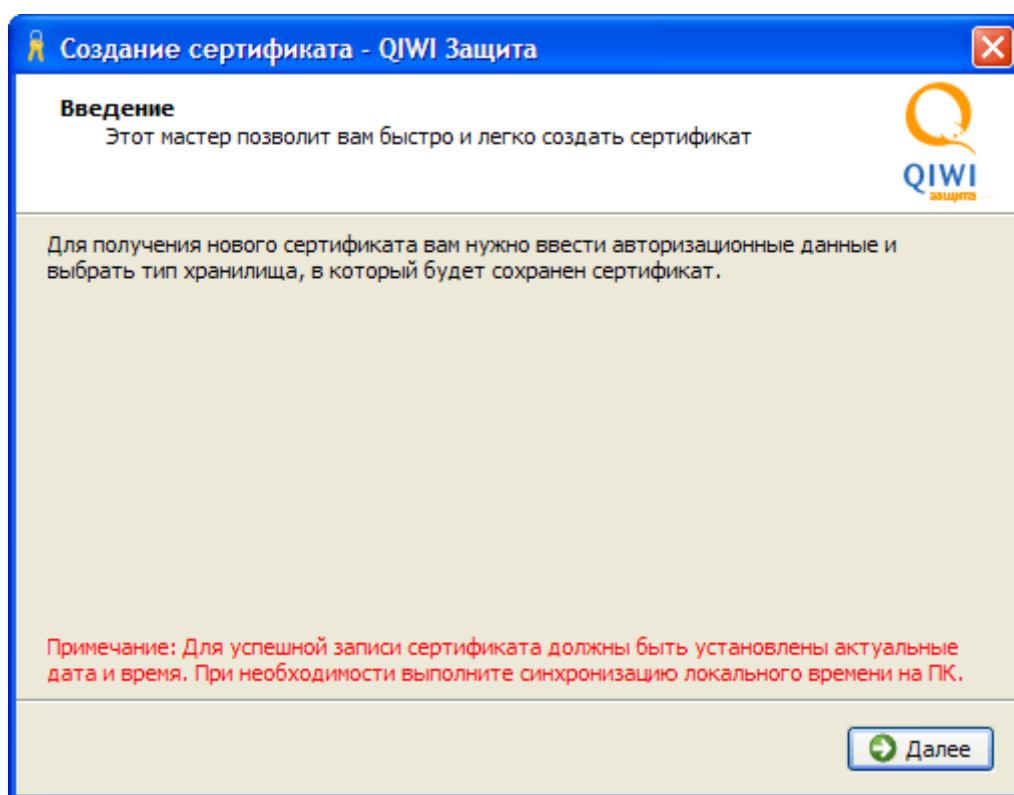
ВНИМАНИЕ

Перед генерацией сертификата в 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



2. Укажите данные персоны для генерации сертификата ([Рис. 5](#)):

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: persona

Пароль: 1234567

Показать пароль:

Назад Далее

- **Логин** – логин персоны;
- **Пароль** – одноразовый пароль персоны;
- **Показать пароль** – флаг позволяет отображать значение поля **Пароль**.

ПРИМЕЧАНИЕ

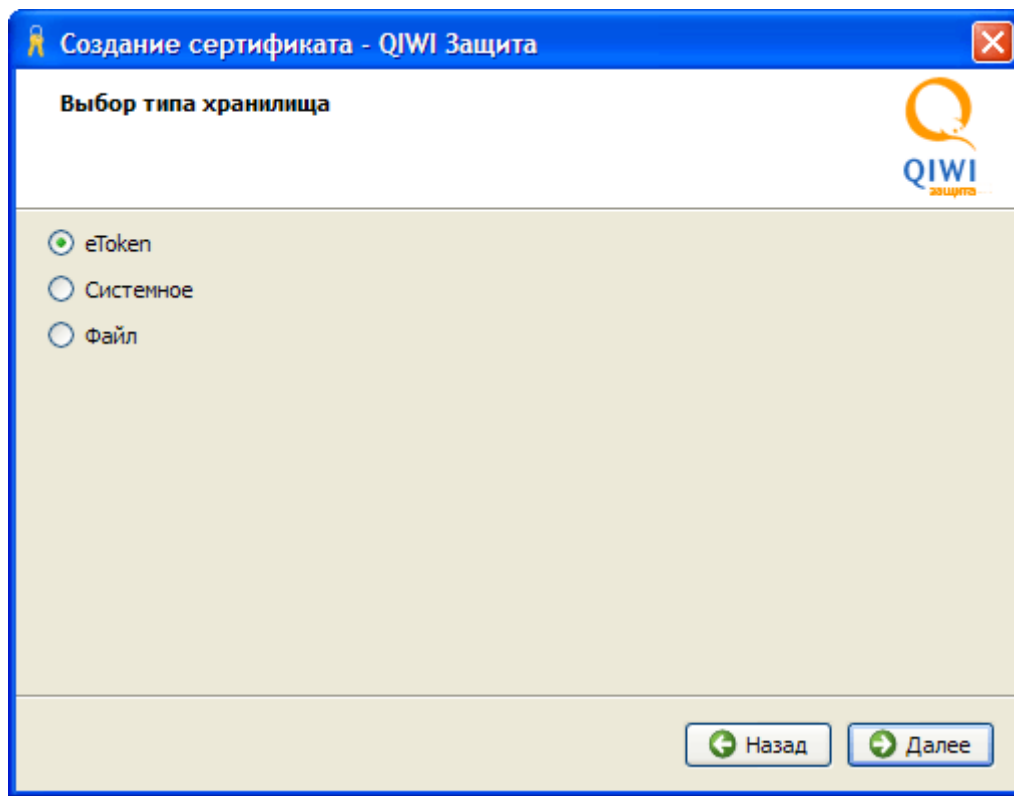
Далее описаны шаги генерации сертификата с типом хранилища **eToken**, т.к. он является наиболее рекомендуемым хранилищем по соображениям безопасности.

Процесс сохранения сертификата в другое хранилище описан в приложениях:

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

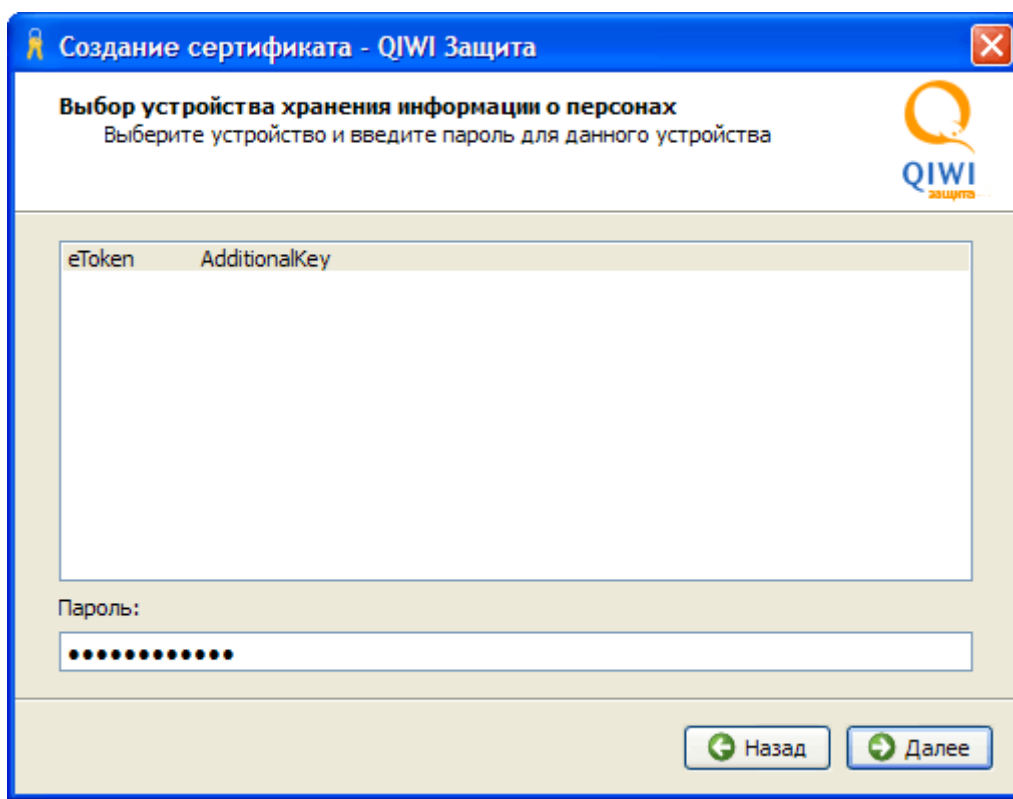
3. Выберите тип хранилища **eToken** (Рис. 6):

Рис. 6. Выбор хранилища сертификата



4. Выберите необходимое устройство из списка eToken и укажите пароль для него ([Рис. 7](#)).

Рис. 7. Выбор устройства хранения информации



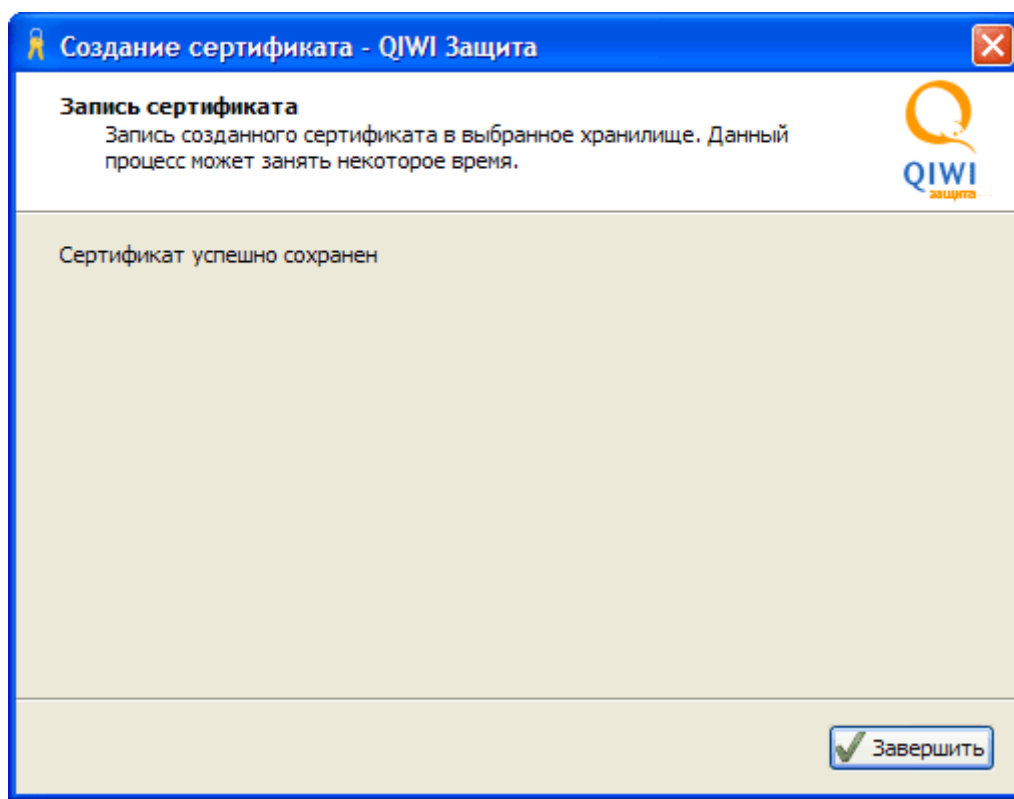
ПРИМЕЧАНИЕ



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

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

7.1. Создание персоны

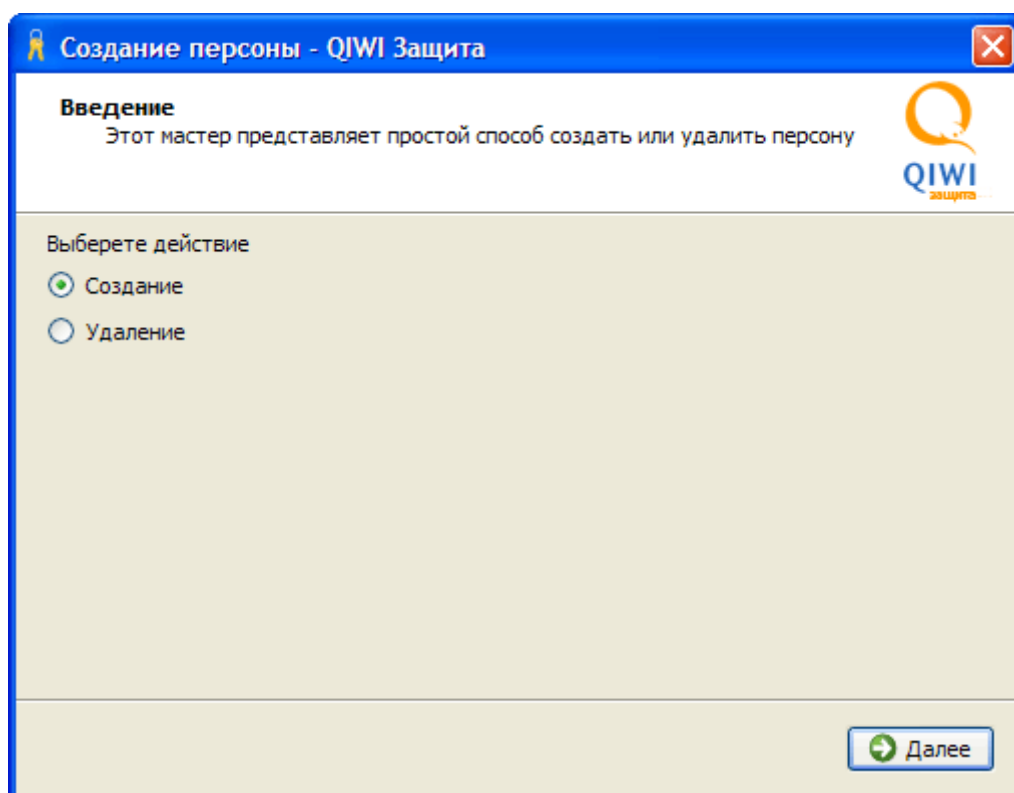
ВНИМАНИЕ

Перед созданием персоны в 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** (см. [Рис. 3](#)).
Будет открыт *Мастер управления персонами* ([Рис. 9](#)).

Рис. 9. Мастер управления персонами



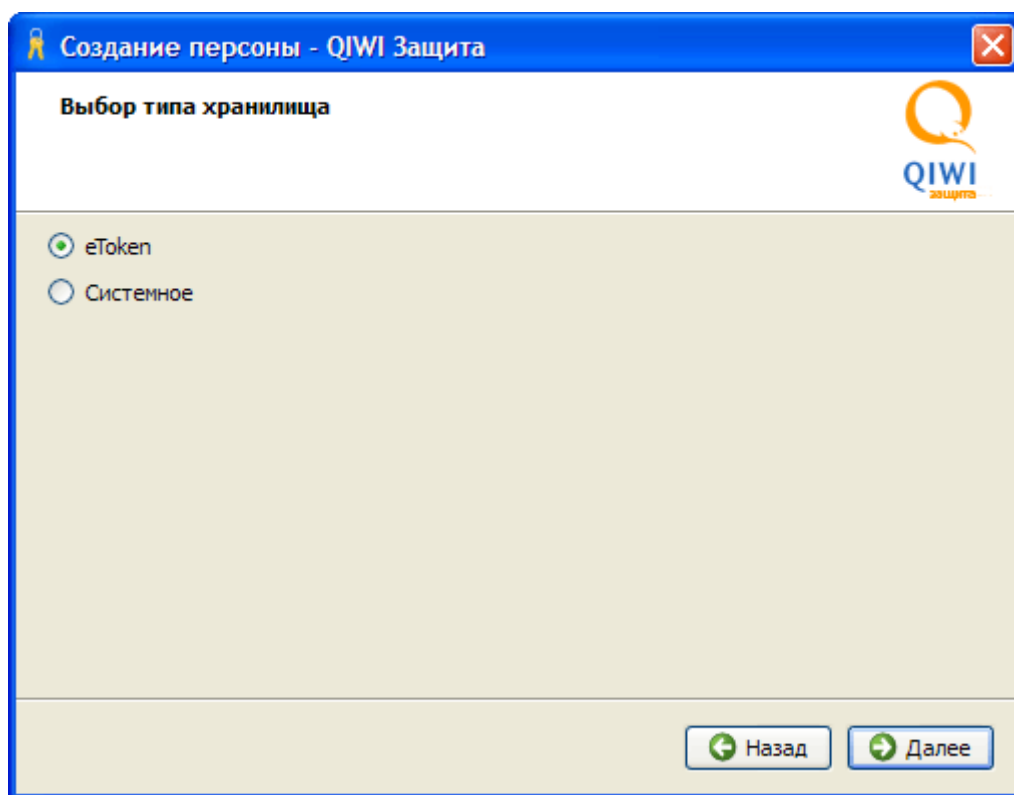
2. Выберите **Создание** и нажмите кнопку **Далее**.

ВНИМАНИЕ

Далее описаны шаги при выборе типа хранилища **eToken**, т.к. это хранилище является наиболее безопасным. При сохранении авторизационных данных персоны в системное хранилище обязательно прочтите [Приложение Г](#).

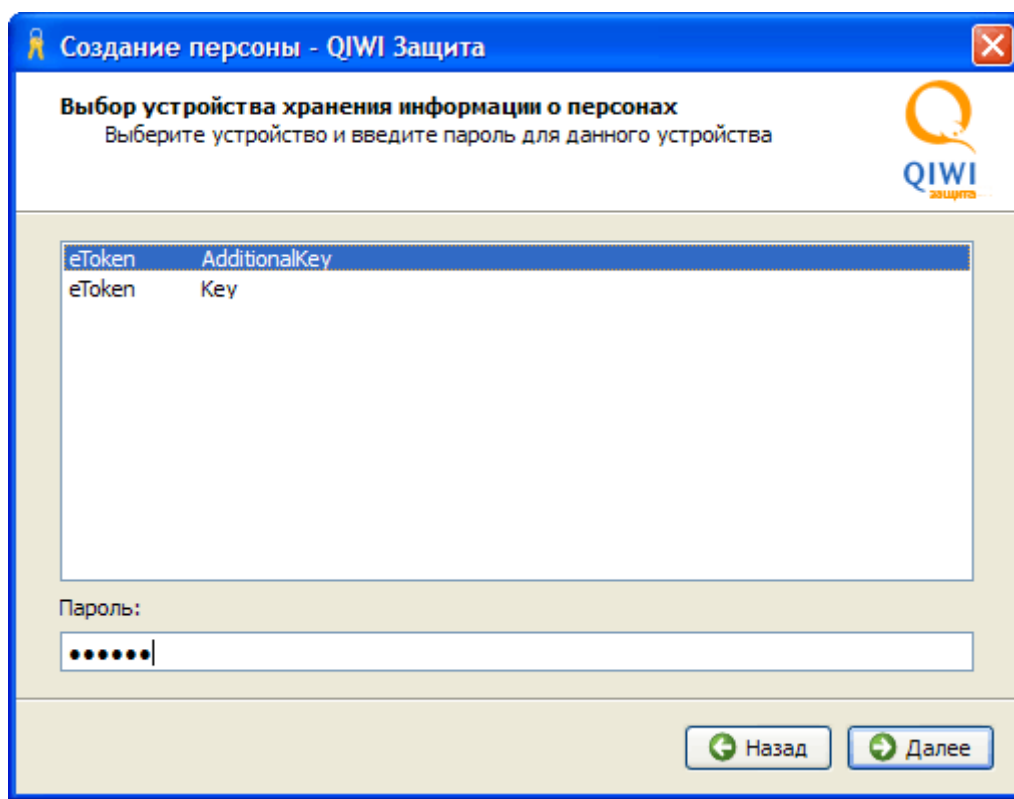
3. Выберите тип хранилища **eToken** (Рис. 10).

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 в пункте 1 [Приложения Б](#)).

5. Введите данные персоны и нажмите кнопку **Далее** ([Рис. 12](#)):

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:

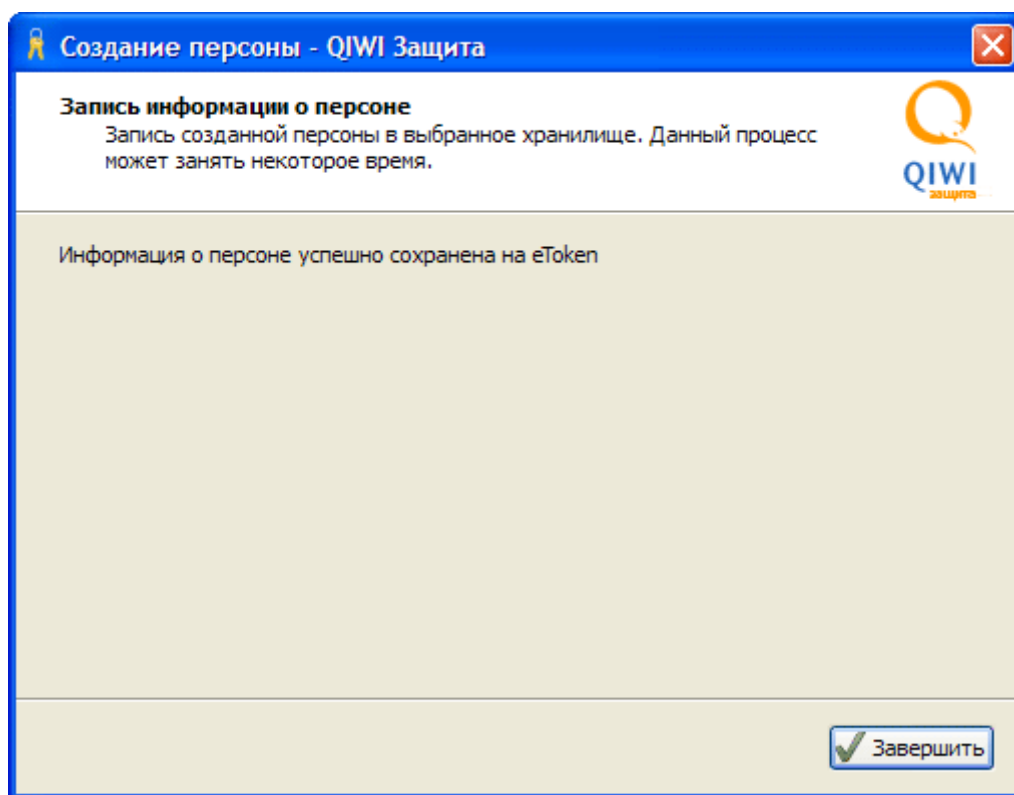
Пароль:

Показать пароль:

- **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**.

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 **Создание/удаление персоны для QIWI Кассир** (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. 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.

8.1. Список сертификатов

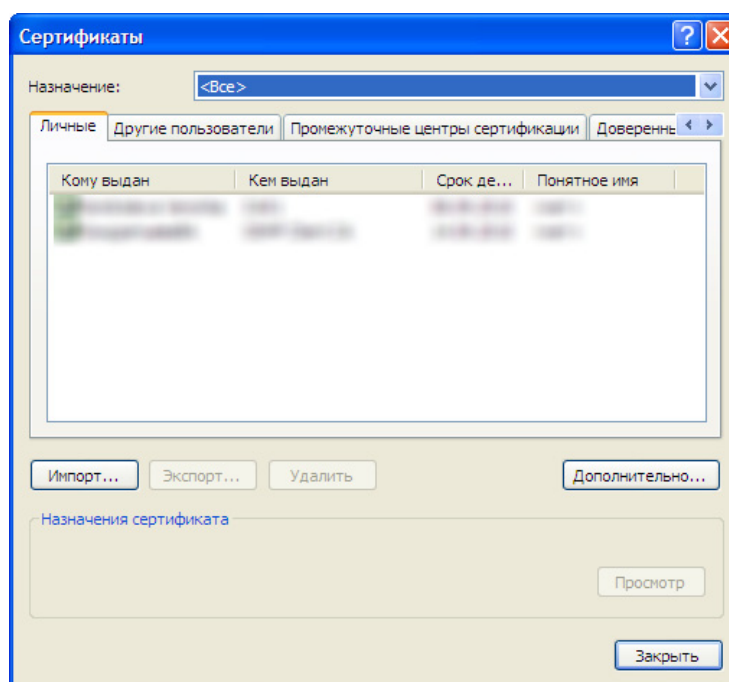
Для просмотра сертификатов, установленных в системе, выберите **Список сертификатов** в главном окне приложения (см. [Рис. 3](#)). Будет открыто окно **Сертификаты** ([Рис. 14](#)).

ПРИМЕЧАНИЕ



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

Рис. 14. Системные сертификаты

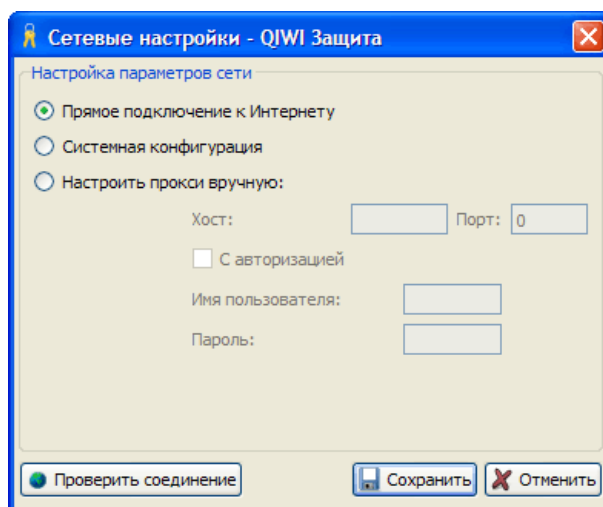


8.2. Сетевые настройки

Для изменения сетевых настроек выполните следующее:

1. В главном окне приложения выберите **Сетевые настройки** (см. [Рис. 3](#)). Будет открыто диалоговое окно **Сетевые настройки** ([Рис. 15](#)).

Рис. 15. Сетевые настройки



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:

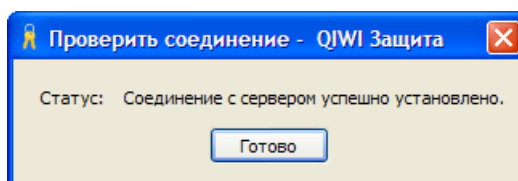
ПРИМЕЧАНИЕ

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. 16](#)).

Рис. 16. Успешное соединение с сервером



8.3. 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. 17](#)).

Рис. 17. Загрузка драйверов

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

- **еToken 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*.
- **еToken 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*.
- **еToken драйвер для Ubuntu (32-бит)** – позволяет установить драйвер для работы с eToken в операционной системе *Ubuntu 9.04*.

8.4. Загрузка документации

Для получения руководства пользователя к текущей версии ПО:

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

Документ будет загружен.

8.5. О 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. 18](#)).

Рис. 18. О программе



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.

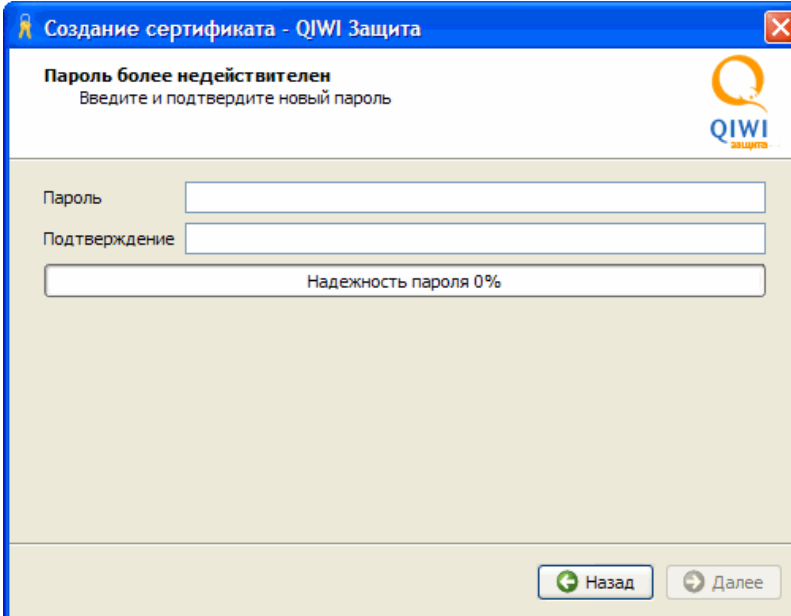
Приложение содержит инструкции:

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. 19).

Рис. 19. 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.

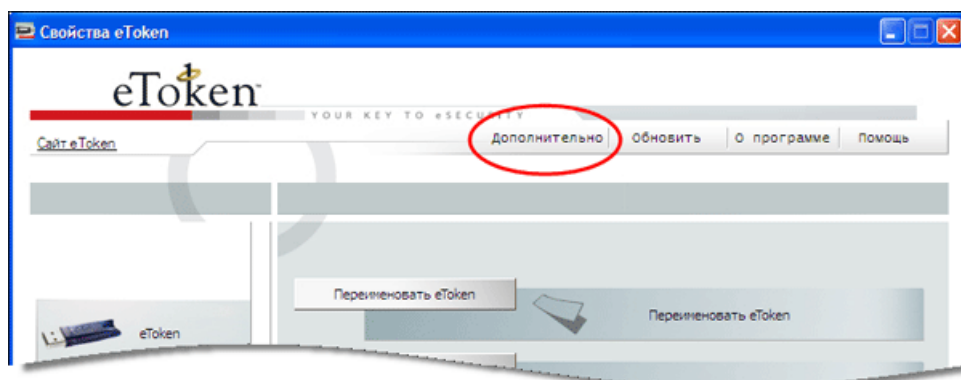
ПРИМЕЧАНИЕ

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

Для смены пароля администратора выполните следующее:

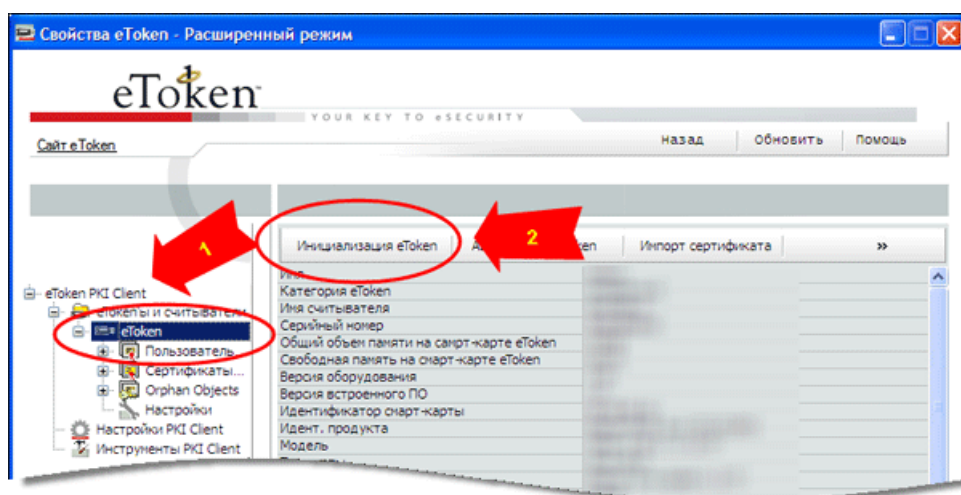
1. Перейдите **Пуск** → **Все программы** → **eToken** → **eToken Properties**.
2. В Свойствах eToken выберите вкладку **Дополнительно** ([Рис. 20](#)).

Рис. 20. Свойства eToken



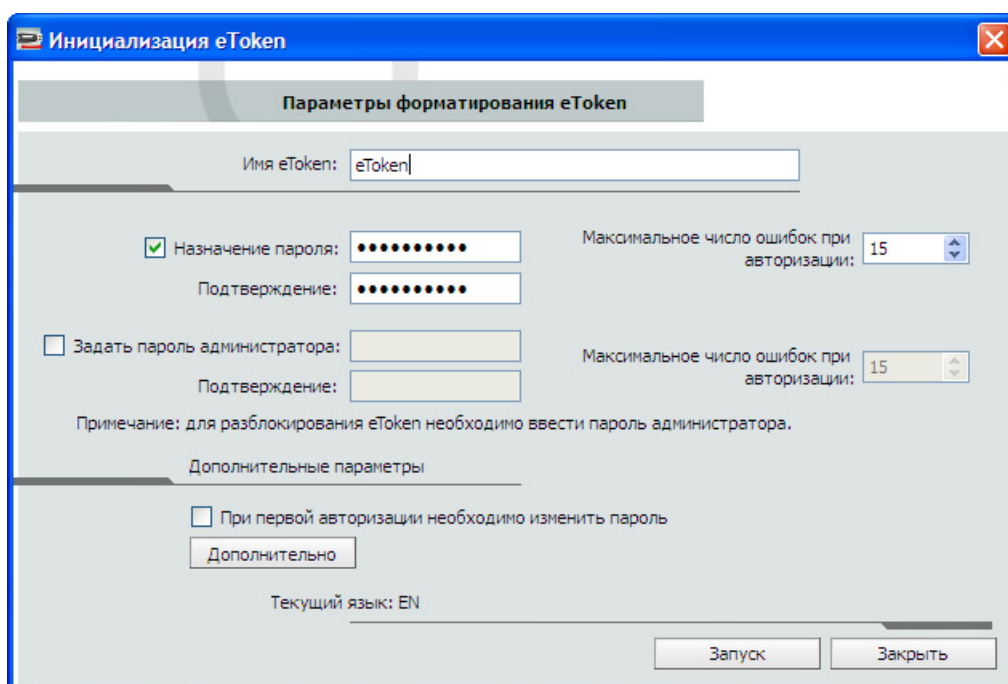
3. Выберите eToken и нажмите кнопку **Инициализация eToken** ([Рис. 21](#)).

Рис. 21. Выбор инициализации eToken



Будет открыто диалоговое окно **Инициализация eToken** (Рис. 22).

Рис. 22. Параметры форматирования eToken




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

Будет выполнено форматирование eToken и пароль администратора будет изменен.

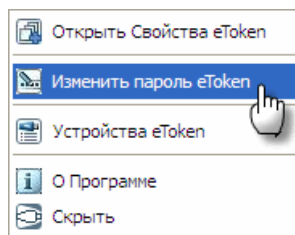
3. Смена пароля eToken с помощью драйвера

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**:

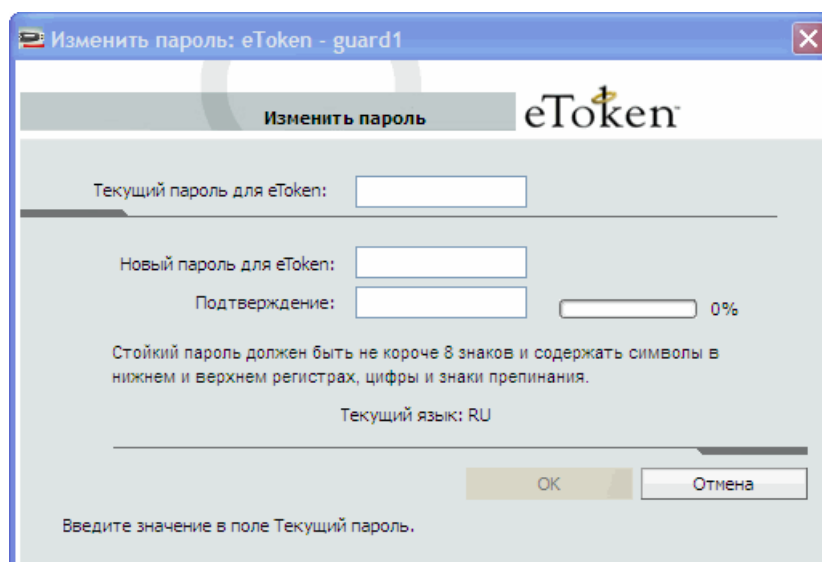
Рис. 23. Смена пароля eToken



3. Введите данные:

- **Текущий пароль для eToken** – введите действующий пароль;
- **Новый пароль** и **Подтверждение** – введите новый пароль.

Рис. 24. Смена пароля

A screenshot of a dialog box titled 'Изменить пароль: eToken - guard1'. The dialog has a header bar with the text 'Изменить пароль' and the eToken logo. Below the header, there are three input fields: 'Текущий пароль для eToken:', 'Новый пароль для eToken:', and 'Подтверждение:'. To the right of the 'Подтверждение:' field is a progress indicator showing '0%'. Below the input fields, there is a text box containing the password strength requirements: 'Стойкий пароль должен быть не короче 8 знаков и содержать символы в нижнем и верхнем регистрах, цифры и знаки препинания.' Below this text is a label 'Текущий язык: RU'. At the bottom right, there are two buttons: 'OK' and 'Отмена'. At the bottom left, there is a note: 'Введите значение в поле Текущий пароль.'

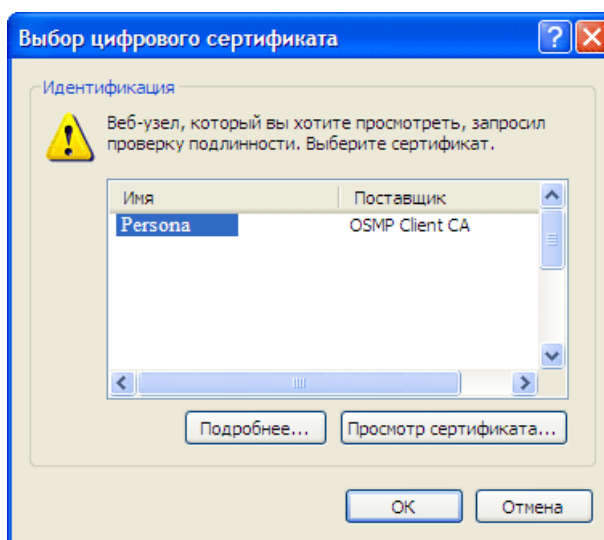
ПРИЛОЖЕНИЕ В: Авторизация на сайте

Для авторизации на агентском сайте ОСМП выполните следующее:

1. Перейдите по ссылке на необходимый сайт <https://portal.osmp.ru>, <https://agent.osmp.ru> или <https://prov.osmp.ru>.

Будет открыто диалоговое окно **Выбор сертификата** (Рис. 25).

Рис. 25. Выбор сертификата при входе на сайт



2. Выберите нужный сертификат.

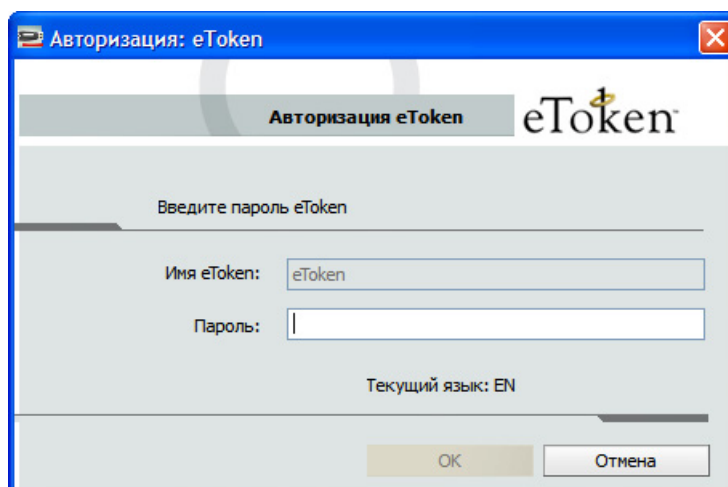
ПРИМЕЧАНИЕ



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. 26)

Рис. 26. Ввод пароля eToken

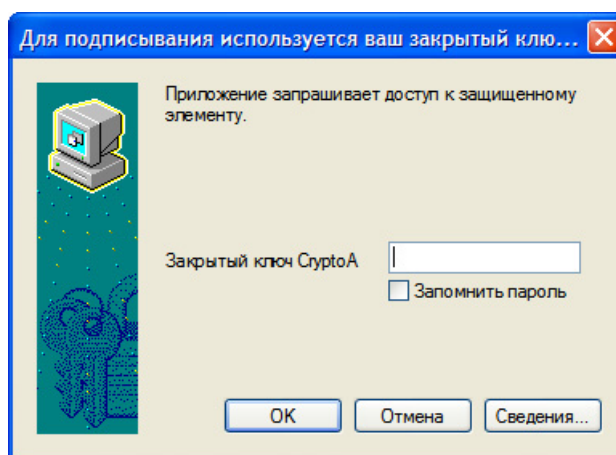


- Системное хранилище (Рис. 27)

ПРИМЕЧАНИЕ

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

Рис. 27. 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 пользователя сайта https://agent.osmp.ru](https://agent.osmp.ru) (раздел «Активация сертификата»).

ПРИЛОЖЕНИЕ Г: Сохранение в Системное хранилище

ВНИМАНИЕ

Системное хранилище является менее защищенным, чем **eToken**. Использовать сертификат вы сможете только на 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**
 1. Выберите пункт **Получить доступ на агентский сайт.**
 2. Введите авторизационные данные персоны (**логин** и **одноразовый пароль**).
 3. Выберите тип хранилища **Системное.**
 4. Перейдите к [ШАГУ 2.](#)
- **Создание персоны для QIWI Кассира**
 1. Выберите пункт **Создание/удаление персоны для QIWI Кассир.**
 2. Выберите **Создание.**
 3. Выберите тип хранилища **Системное.**
 4. Введите данные персоны ([Рис. 28](#)):

Рис. 28. Ввод информации о персоне

Создание/удаление персоны - QIWI Защита

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

Псевдоним: QIWI Кассир

Логин: Person

ID терминала: 555555

Пароль: 123456

Показать пароль

Выберете тип доступа: Для текущего пользователя
 Для всех пользователей

Назад Далее

- ✦ **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>.

5. 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

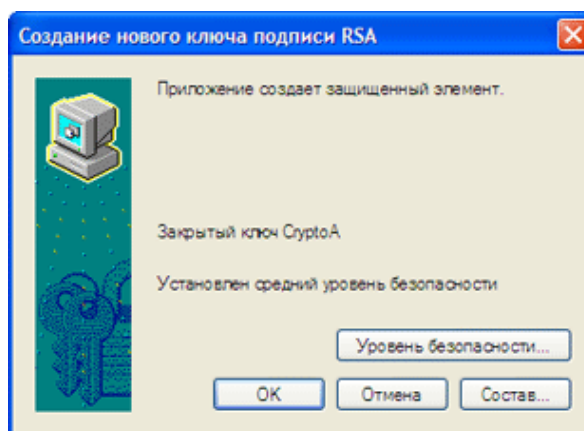
Сохранить авторизационные данные **для всех пользователей** можно только под учетной записью с правами **Администратора**.

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

ШАГ 2. Генерация ключа подписи RSA

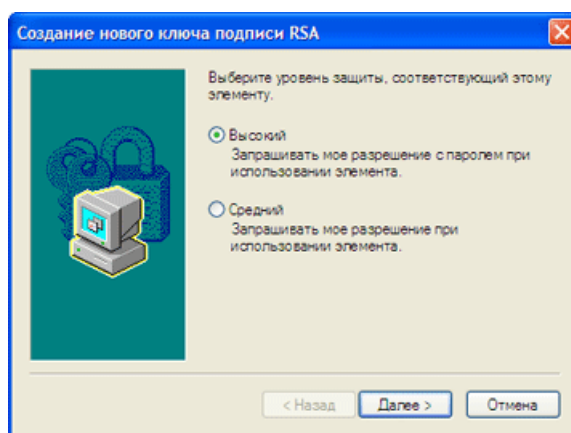
1. Нажмите кнопку **Уровень безопасности** ([Рис. 29](#)).

Рис. 29. Создание нового ключа подписи RSA



2. Выберите уровень защиты и нажмите кнопку **Далее**> ([Рис. 30](#)):

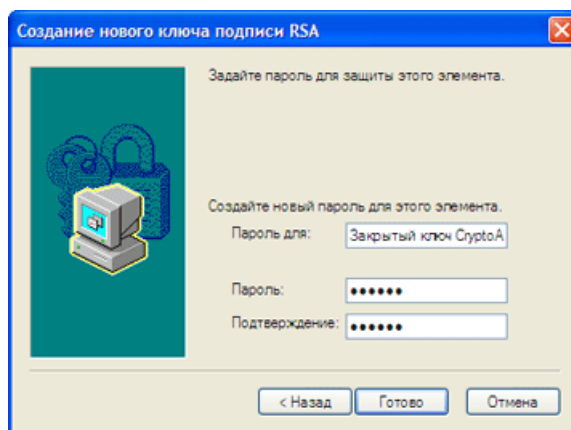
Рис. 30. Выбор уровня защиты

**ПРИМЕЧАНИЕ**

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

- **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** ([Рис. 31](#))

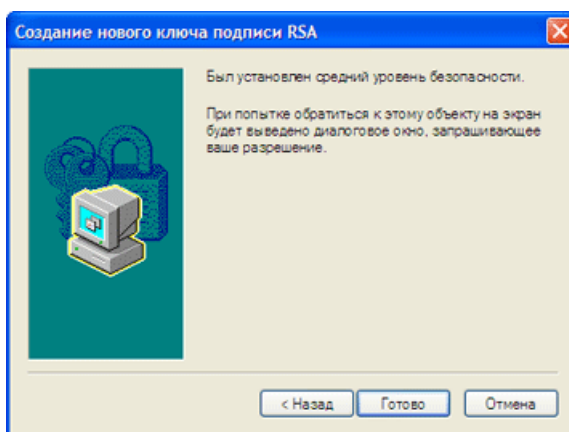
Рис. 31. Установка пароля сертификата

**ПРИМЕЧАНИЕ**

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

- **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** ([Рис. 32](#))

Рис. 32. Информация об авторизации при среднем уровне безопасности системного хранилища



Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. [Рис. 29](#)).

3. Нажмите кнопку **ОК**.

Вы будете возвращены в *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:

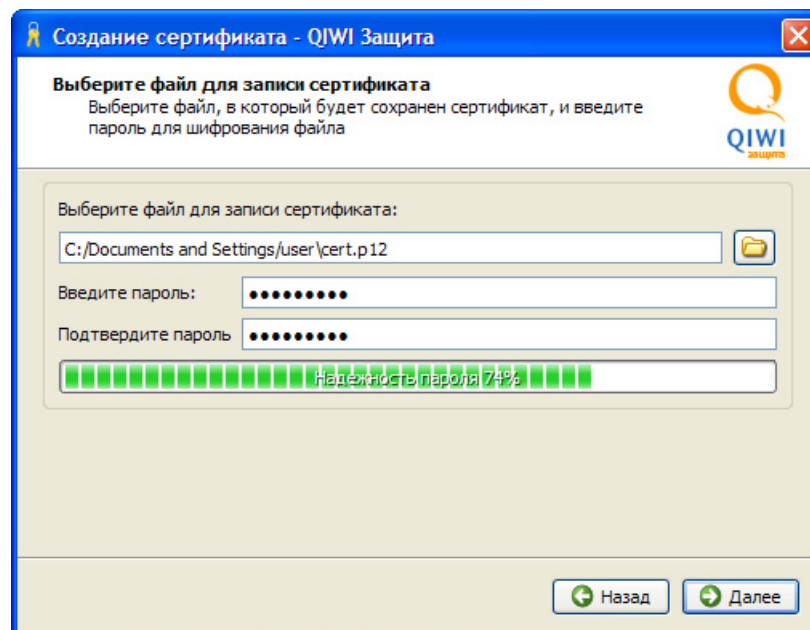
1. [Сохранению сертификата в «Файл»](#)
2. [Экспорту сертификата в системное хранилище](#).

1. Сохранение сертификата в «Файл»

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

1. Пройдите шаги с 1 по 4 описанные в п. [5](#).
2. Выберите тип хранилища **Файл**.
Вы перейдете к следующему шагу ([Рис. 33](#)).

Рис. 33. 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](#)).

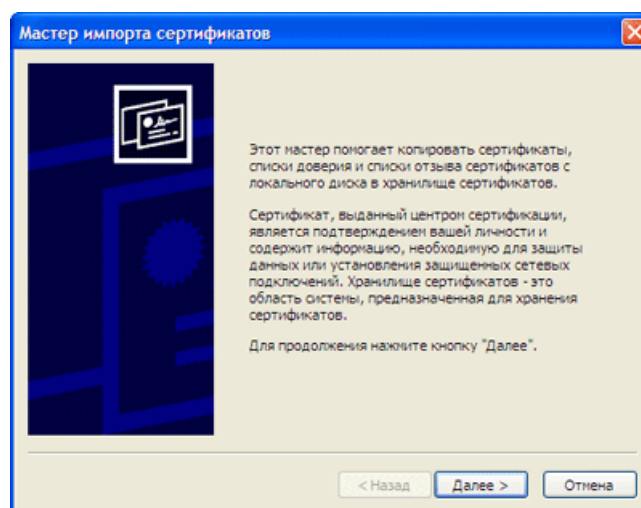
Сертификат будет сохранен в файле.

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. 34](#)).

Рис. 34. Мастер импорта сертификатов

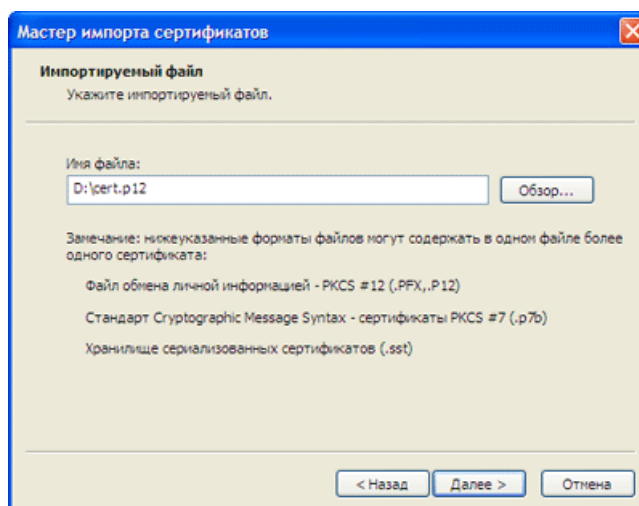


2. Для перехода к первому шагу нажмите кнопку **Далее**.
3. Подтвердите или укажите расположение файла сертификата.
4. Нажмите кнопку **Далее** ([Рис. 35](#)).

ПРИМЕЧАНИЕ

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

Рис. 35. Импортируемый файл

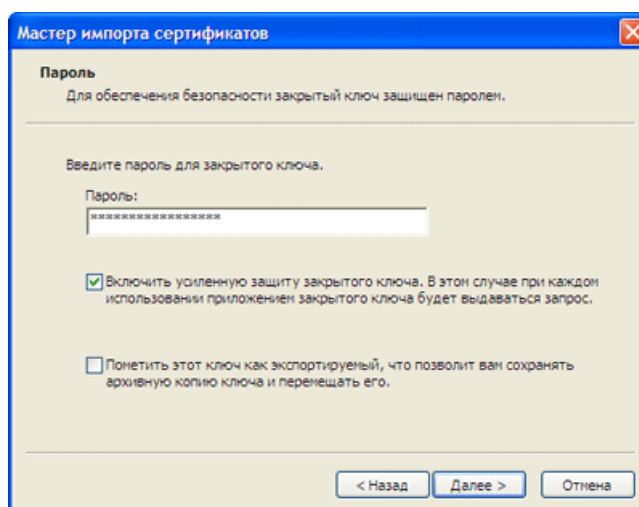


5. Установите флаг **Включить усиленную защиту ключа** (Рис. 36).

ПРИМЕЧАНИЕ

Установка данного флага необходима в целях повышения уровня защиты.

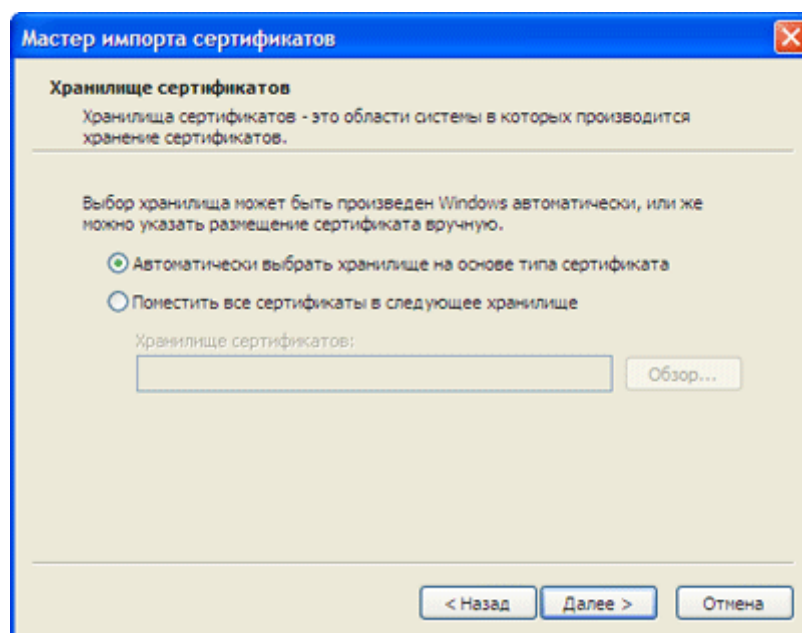
Рис. 36. Ввод пароля для файла сертификата



6. Введите пароль для доступа к файлу и нажмите кнопку **Далее**.

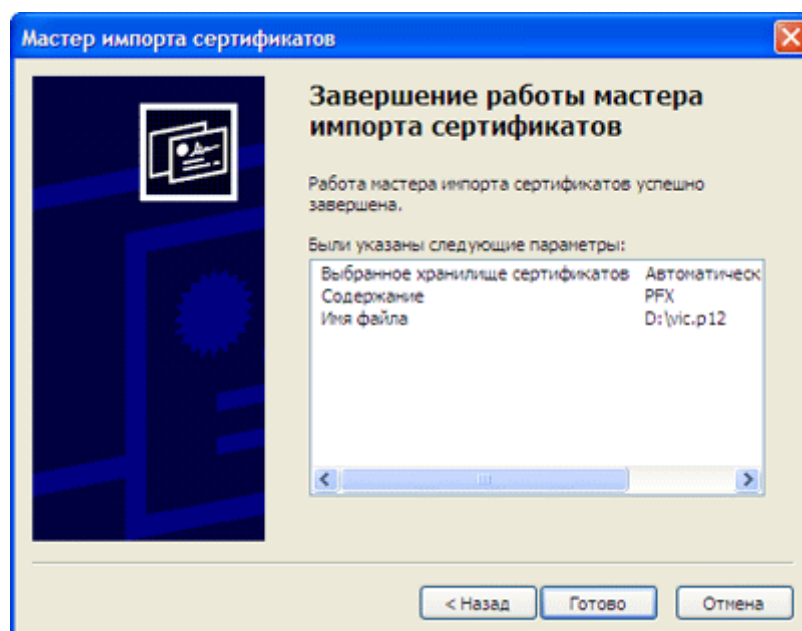
7. Выберите **Автоматически выбрать хранилище на основе типа сертификата** и нажмите кнопку **Далее** (Рис. 37).

Рис. 37. Выбор размещения сертификата



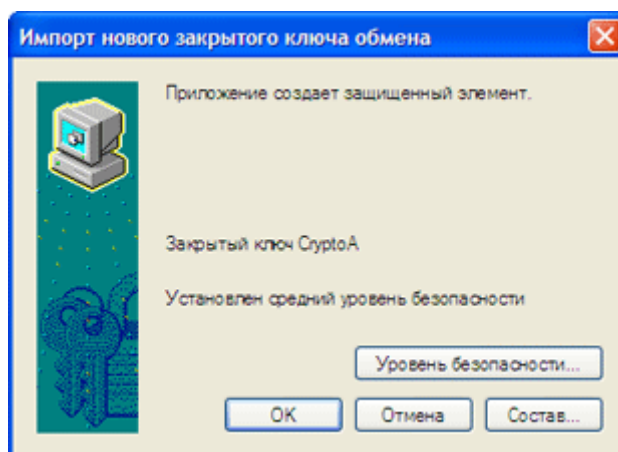
Будет выполнен импорт сертификата, и *Мастер импорта сертификатов* отобразит параметры импорта (Рис. 38).

Рис. 38. Параметры импорта сертификата



8. Нажмите кнопку **Готово**.
Импорт сертификата в системное хранилище будет завершен и вам будет предложено задать уровень безопасности сертификата (Рис. 39).

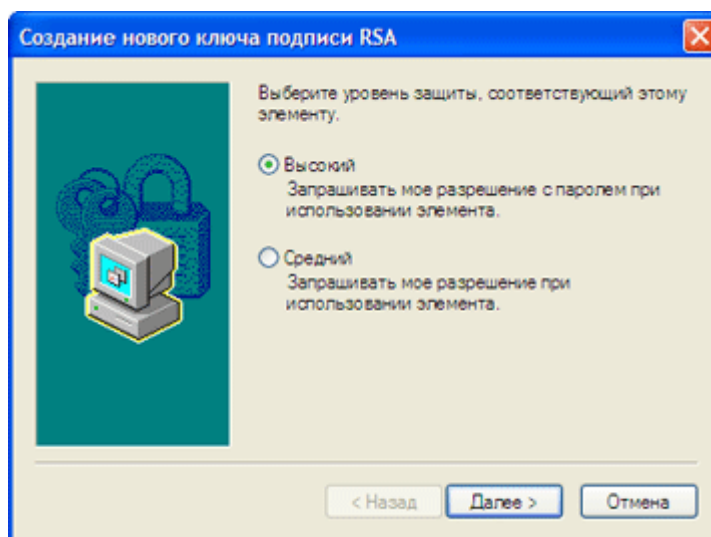
Рис. 39. Создание защищенного элемента



9. Нажмите кнопку **Уровень безопасности**.

Будет открыто диалоговое окно с выбором уровня защиты ([Рис. 40](#)).

Рис. 40. Выбор уровня безопасности



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

СОВЕТ

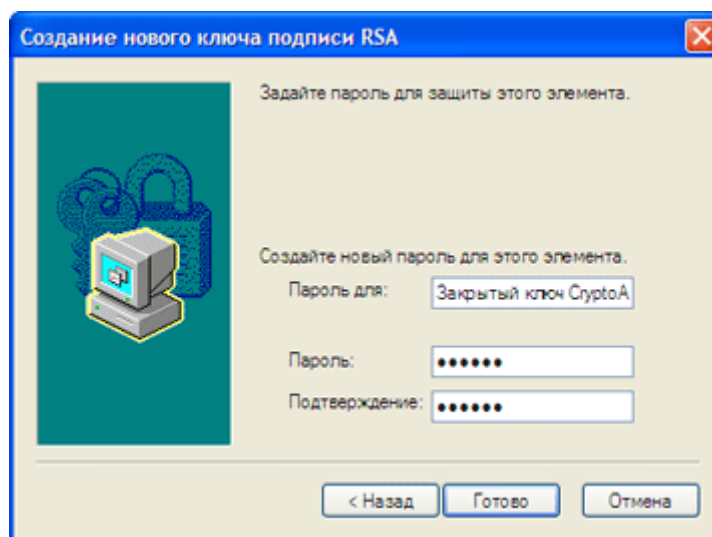
В целях повышения уровня защиты установите **Высокий уровень**.

1. **Высокий уровень** – задайте пароль для сертификата и нажмите кнопку **Готово** ([Рис. 41](#)).

ПРИМЕЧАНИЕ

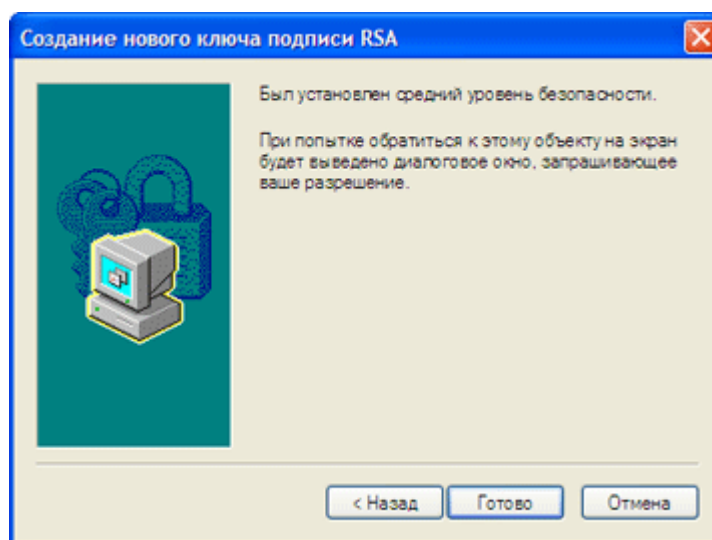
Данный пароль необходимо будет вводить при авторизации на сайте ОСМП. Подробнее об авторизации на сайте см. в [Приложении В](#).

Рис. 41. Установка пароля сертификата



2. **Средний уровень** – прочитайте информацию о процессе авторизации и нажмите кнопку **Готово** ([Рис. 42](#)).

Рис. 42. Информация об авторизации при среднем уровне безопасности системного хранилища

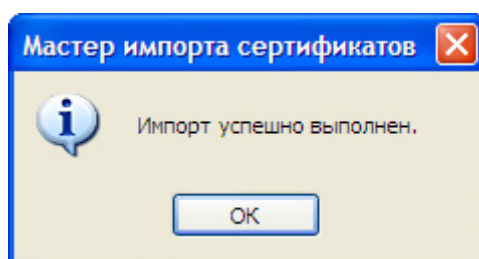


Вы будете возвращены к первому шагу *Мастера создания нового ключа подписи RSA* (см. [Рис. 39](#)).

11. Нажмите кнопку **ОК**.

Будет открыто диалоговое окно, информирующее об успешном импорте сертификата ([Рис. 43](#)).

Рис. 43. 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».

СПИСОК РИСУНКОВ

Рис. 1. Мастер установки.....	6
Рис. 2. Финальный шаг установки.....	7
Рис. 3. Главное окно приложения.....	8
Рис. 4. Мастер создания сертификатов	10
Рис. 5. Ввод авторизационных данных.....	11
Рис. 6. Выбор хранилища сертификата	12
Рис. 7. Выбор устройства хранения информации	13
Рис. 8. Запись сертификата	14
Рис. 9. Мастер управления персонами	15
Рис. 10. Выбор устройства хранения информации о персонах.....	16
Рис. 11. Выбор устройства хранения информации.....	17
Рис. 12. Ввод информации о персоне.....	18
Рис. 13. Успешная запись данных	19
Рис. 14. Системные сертификаты.....	20
Рис. 15. Сетевые настройки	21
Рис. 16. Успешное соединение с сервером.....	22
Рис. 17. Загрузка драйверов	22
Рис. 18. О программе	23
Рис. 19. Сообщение о необходимости смены пароля на eToken.....	25
Рис. 20. Свойства eToken.....	26
Рис. 21. Выбор инициализации eToken	27
Рис. 22. Параметры форматирования eToken.....	27
Рис. 23. Смена пароля eToken	28
Рис. 24. Смена пароля	28
Рис. 25. Выбор сертификата при входе на сайт.....	29
Рис. 26. Ввод пароля eToken	30
Рис. 27. Ввод пароля для закрытого ключа в системном хранилище	30
Рис. 28. Ввод информации о персоне.....	31
Рис. 29. Создание нового ключа подписи RSA.....	32
Рис. 30. Выбор уровня защиты	33
Рис. 31. Установка пароля сертификата.....	33
Рис. 32. Информация об авторизации при среднем уровне безопасности системного хранилища ..	34
Рис. 33. Выбор файла для записи сертификата	35
Рис. 34. Мастер импорта сертификатов	36
Рис. 35. Импортируемый файл.....	37
Рис. 36. Ввод пароля для файла сертификата.....	37
Рис. 37. Выбор размещения сертификата.....	38
Рис. 38. Параметры импорта сертификата	38
Рис. 39. Создание защищенного элемента	39
Рис. 40. Выбор уровня безопасности.....	39
Рис. 41. Установка пароля сертификата.....	40
Рис. 42. Информация об авторизации при среднем уровне безопасности системного хранилища ..	40
Рис. 43. Успешный импорт сертификата	41