

ПРОГРАММА УПРАВЛЕНИЯ СЕРТИФИКАТАМИ OSMP PUS

ВЕР. 1.4

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ
вер. 1.0



**ОБЪЕДИНЕННАЯ СИСТЕМА
МОМЕНТАЛЬНЫХ ПЛАТЕЖЕЙ**

СОДЕРЖАНИЕ

1.	ГЛОССАРИЙ	3
2.	ВВЕДЕНИЕ	4
2.1.	НАЗНАЧЕНИЕ ПРОГРАММЫ	4
3.	БЫСТРЫЙ СТАРТ	5
3.1.	СОЗДАНИЕ СЕРТИФИКАТА	5
3.2.	УПРАВЛЕНИЕ ПЕРСОНАМИ	5
4.	ОСНОВНЫЕ СВЕДЕНИЯ	6
4.1.	ПРАВИЛА РАБОТЫ С ЕТОКЕН	6
4.2.	ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ	6
4.3.	УСТАНОВКА ПРИЛОЖЕНИЯ	7
4.4.	ГЛАВНОЕ ОКНО ПРОГРАММЫ	11
5.	ПОЛУЧЕНИЕ СЕРТИФИКАТА	13
5.1.	ПОЛУЧЕНИЕ ОДНОРАЗОВОГО ПАРОЛЯ	13
5.2.	ГЕНЕРАЦИЯ СЕРТИФИКАТА	14
6.	УПРАВЛЕНИЕ ПЕРСОНАМИ	16
6.1.	СОЗДАНИЕ ПЕРСОНЫ	16
6.2.	РЕДАКТИРОВАНИЕ/УДАЛЕНИЕ ПЕРСОНЫ	17
7.	ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	19
7.1.	ПРОСМОТР/УПРАВЛЕНИЕ УСТАНОВЛЕННЫМИ СЕРТИФИКАТАМИ	19
7.2.	НАСТРОЙКА ПРОКСИ-СЕРВЕРА	19
7.3.	ЗАГРУЗКА ДРАЙВЕРОВ	20
7.4.	ЗАГРУЗКА ДОКУМЕНТАЦИИ	20
7.5.	О ПРОГРАММЕ	20
8.	ВХОД НА САЙТ	22
ПРИЛОЖЕНИЕ А:	РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ	24
ПРИЛОЖЕНИЕ Б:	СОХРАНЕНИЕ СЕРТИФИКАТА В СИСТЕМНОМ ХРАНИЛИЩЕ	25
	СПИСОК РИСУНКОВ	27

1. ГЛОССАРИЙ

Термин	Определение
<i>Авторизация</i>	Проверка подлинности персоны.
<i>Псевдоним</i>	Имя пользователя, отображаемое при авторизации и работе в приложениях ОСМП (например, <i>ОСМП Термит</i>).
<i>Сертификат</i>	Цифровой документ, используемый для идентификации персоны.

2. ВВЕДЕНИЕ

Данный документ представляет собой руководство по установке и использованию приложения *OSMP PUS*, а также описывает порядок работы с программой при управлении сертификатами и авторизационными данными персон.

2.1. Назначение программы

Программа *OSMP PUS* предназначена для повышения уровня безопасности при работе с *Системой ОСМП*.

Безопасный доступ к Web сайту

OSMP PUS на основании логина и одноразового пароля генерирует пару ключей, необходимых для получения сертификата.

После успешной регистрации на сервере сертификат сохраняется на eToken и в дальнейшем используется для безопасного доступа к сайту.

ПРИМЕЧАНИЕ Одноразовый пароль предназначен для генерации только одного сертификата. После использования он блокируется сервером.

Авторизация в приложениях

Информация о персоне (логин, идентификатор терминала, *псевдоним*) сохраняется на ключе eToken и обеспечивает удобный способ авторизации в приложениях ОСМП, например *ОСМП Термит*.

3. БЫСТРЫЙ СТАРТ

3.1. Создание сертификата

Для получения сертификата выполните следующие действия:

1. Скачайте установочный файл *OSMP Pus* по [ссылке](#).
2. Установите приложение на локальный компьютер (подробнее см. в разделе [4.3](#)).
3. При необходимости зарегистрируйте новую персону с одноразовым паролем в дилерской части сайта ОСМП (<http://portal.osmp.ru>) (подробнее см. в разделе [5](#)).
4. Запустите *OSMP Pus*. Выберите пункт **Получить доступ на агентский сайт**.
5. Введите авторизационные данные персоны (логин и одноразовый пароль).
6. Выберите тип хранилища (подробнее см. в [Приложении А](#)):
 - eToken – наиболее рекомендуемое хранилище по соображениям безопасности,
 - Системное хранилище,
 - Файл.
7. Сертификат будет создан и сохранен в хранилище (подробнее см. в разделе [5.2](#)).

3.2. Управление персонами

Для создания/редактирования/удаления информации о персоне выполните следующее:

1. Скачайте установочный файл *OSMP Pus* по [ссылке](#).
2. Установите приложение на локальный компьютер (подробнее см. в разделе [4.3](#)).
3. При необходимости зарегистрируйте новую персону с одноразовым паролем (а также терминал определенного типа) в дилерской части сайта ОСМП (<http://portal.osmp.ru>) (подробнее см. в разделе [5](#)).
4. Запустите *OSMP Pus*. Выберите пункт **Управление персонами**.
5. Выберите нужное действие (**Создать, Редактировать, Удалить**).
6. Выберите тип хранилища (подробнее см. в [Приложении А](#)):
 - eToken – наиболее рекомендуемое хранилище по соображениям безопасности,
 - Системное хранилище,
 - Файл.
7. Выполните одно из следующих действий:
 - *При создании персоны* – введите авторизационные данные (логин и одноразовый пароль персоны, а также ID терминала). Сохраните информацию в хранилище.
 - *При редактировании персоны* – измените ID терминала. Сохраните информацию в хранилище.
 - *При удалении персоны* – выберите нужную персону.

4. ОСНОВНЫЕ СВЕДЕНИЯ

4.1. Правила работы с eToken

При работе с eToken рекомендуется придерживаться следующих правил:

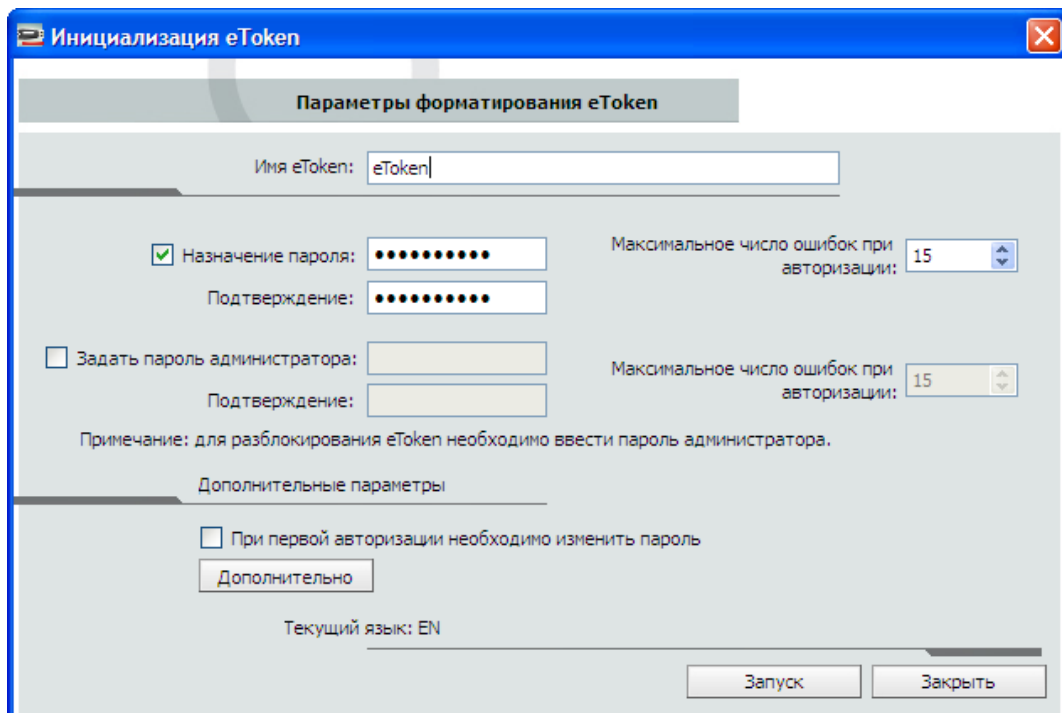
1. В начале работы новым ключом eToken **обязательно** смените пароль, установленный по умолчанию.
2. Создайте пароль администратора eToken. Для этого:

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

- 2.1. В **Свойствах eToken** выберите вкладку **Дополнительно**.
- 2.2. Выберите eToken и нажмите кнопку **Инициализация eToken** (Рис. 1).
В открывшемся окне установите флаг напротив строки **Установить пароль администратора**, задайте пароль.
- 2.3. Нажмите кнопку **Запуск**.

ВНИМАНИЕ! При инициализации eToken с него будет удалена вся информация.

Рис. 1. Установка пароля администратора



4.2. Технические требования

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

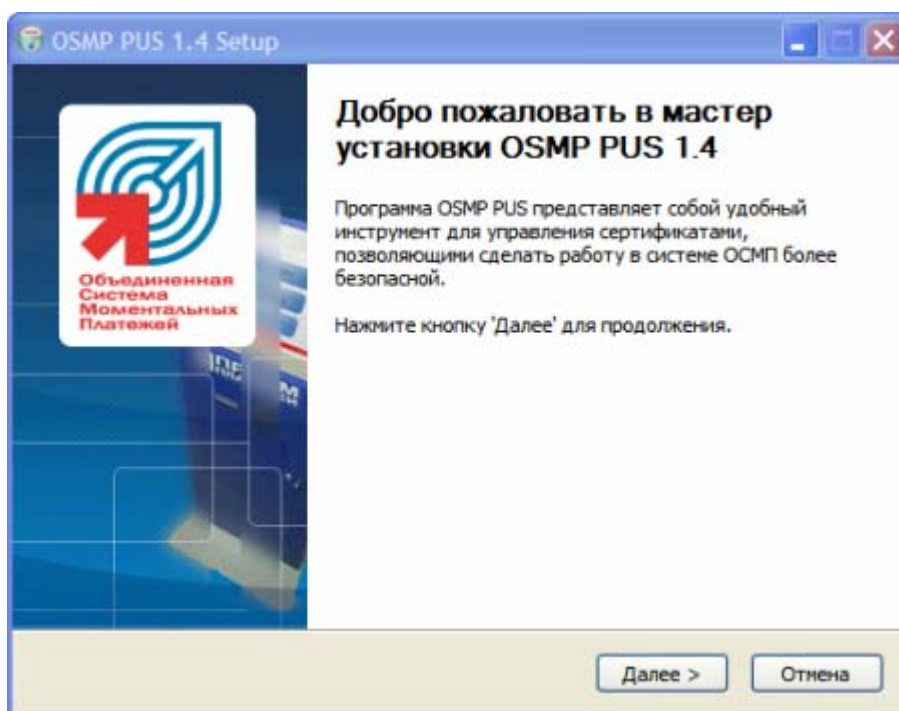
- около 20 Мб свободного дискового пространства;
- разрешение экрана 1024x768 в режиме High/True Color;
- оперативной памяти не менее 64 Мб (рекомендуется 128 Мб);
- частота процессора не ниже 233 МГц;
- наличие локальной сети для связи с сервером;
- операционная система Microsoft Windows 9x, ME, 2000, XP, 2003, Vista, MacOS, Linux;
- драйвера для работы с ключом eToken версии 4.55 или выше.

4.3. Установка приложения

Для того чтобы установить программу *OSMP Pus*, выполните следующее:

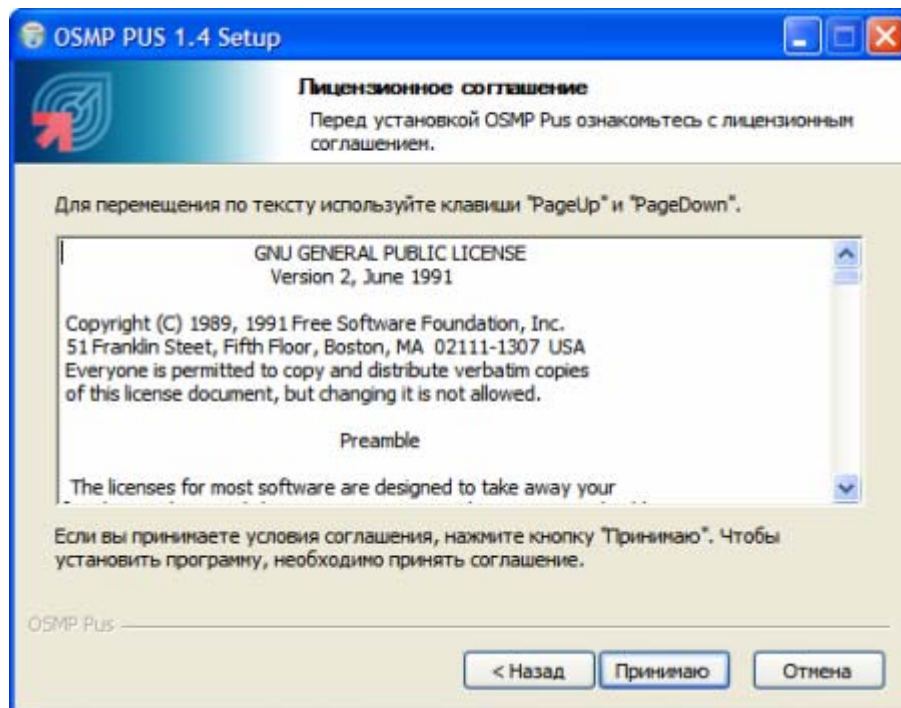
1. Скопируйте файл `pus-x.x-win.exe` (x.x – номер версии приложения) в любое место на вашем компьютере.
2. Запустите файл. При этом будет запущен **Мастер установки** (Рис. 2).

Рис. 2. Первый шаг установки



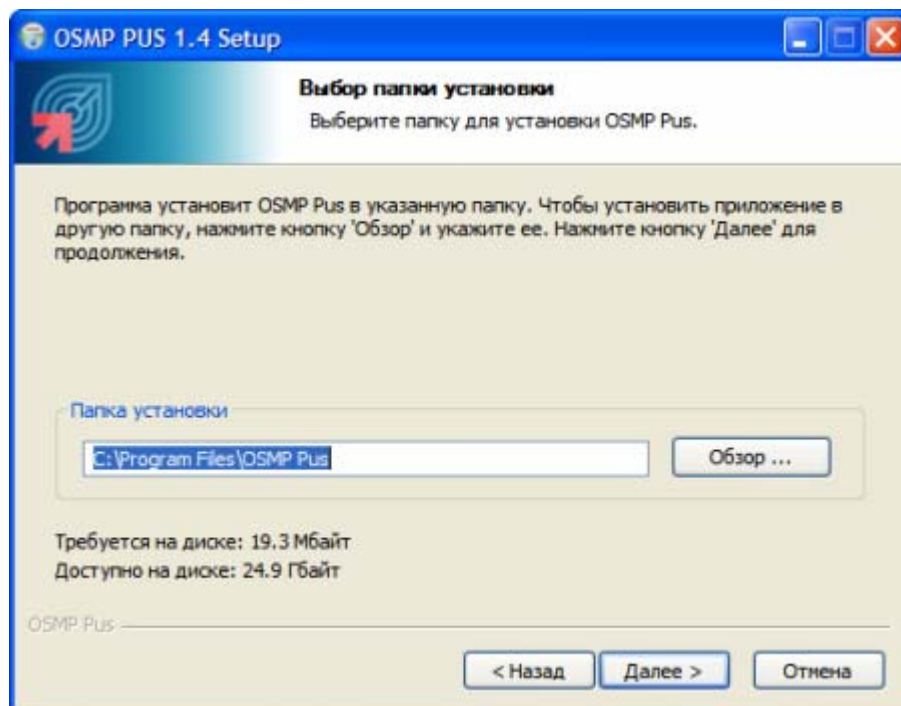
3. Для начала установки, нажмите кнопку **Далее >**. При этом вы попадете на второй шаг **Мастера установки** (Рис. 3).

Рис. 3. Второй шаг установки



4. Прочитайте условия лицензионного соглашения, которое вам предлагается на втором шаге. Если вы согласны, нажмите кнопку **Принимаю**. Если вы не согласны с условиями соглашения, то вы можете отказаться от установки, нажав кнопку **< Назад** или **Отмена**.
5. После принятия условий лицензионного соглашения нажатием кнопки **Принимаю** вы переходите на следующий шаг (Рис. 4).

Рис. 4. Третий шаг установки



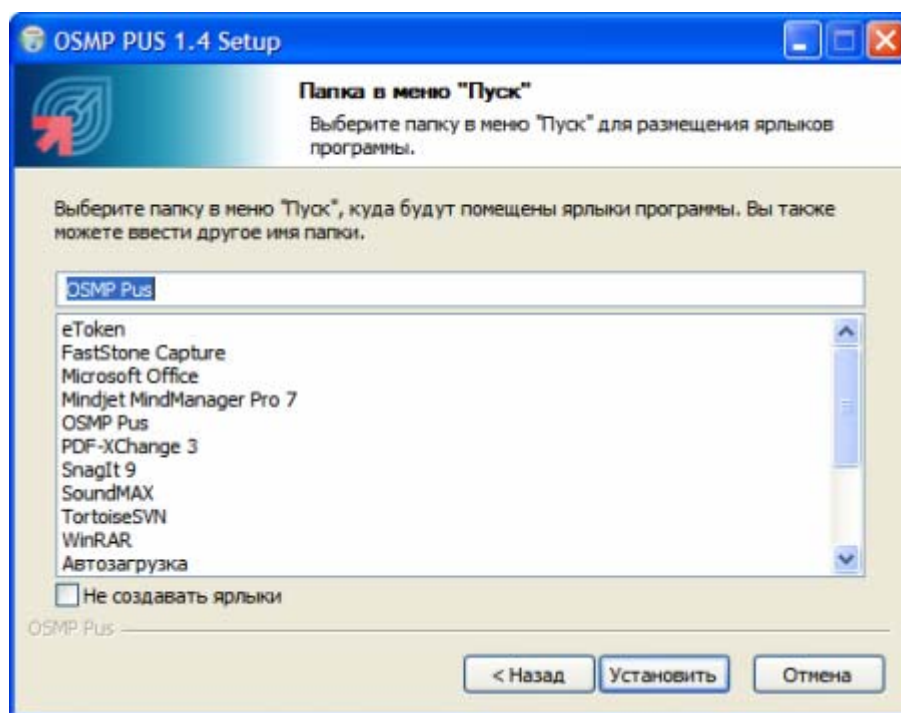
6. Укажите папку, в которую должно быть установлено приложение. По умолчанию предлагается папка `C:\Program Files\OSMP Pus`, но вы можете выбрать другую удобную вам папку.

ПРИМЕЧАНИЕ Вы можете указать путь к папке установки вручную, или выбрать в стандартном диалоге, открываемом по кнопке **Обзор...**

При этом в нижней части окна отображается требуемое и доступное пространство на диске.

7. Нажмите **Далее >** для перехода к следующему шагу (Рис. 5). Для возврата к лицензионному соглашению, нажмите **< Назад**.

Рис. 5. Четвертый шаг установки

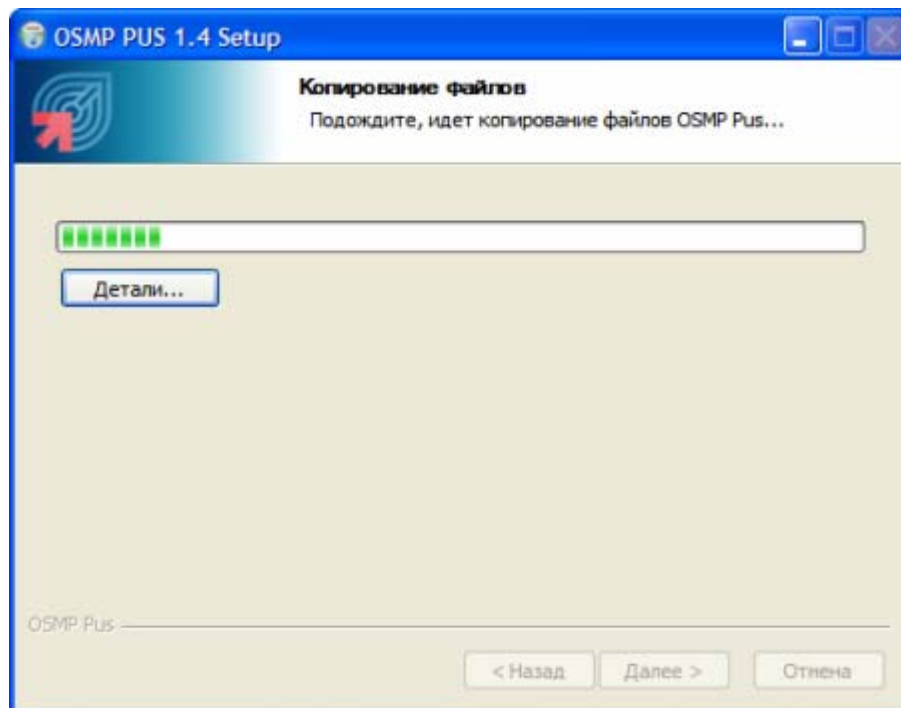


8. На данном шаге вам необходимо выбрать пункт меню **Пуск**, в котором будет размещен ярлык для приложения *OSMP Pus*. По умолчанию предлагается отдельный пункт **OSMP Pus**, однако вы можете выбрать любой из имеющихся пунктов, чтобы разместить ярлык внутри него, а также изменить название ярлыка.

ПРИМЕЧАНИЕ Кроме меню **Пуск**, ярлык также будет размещен на рабочем столе.

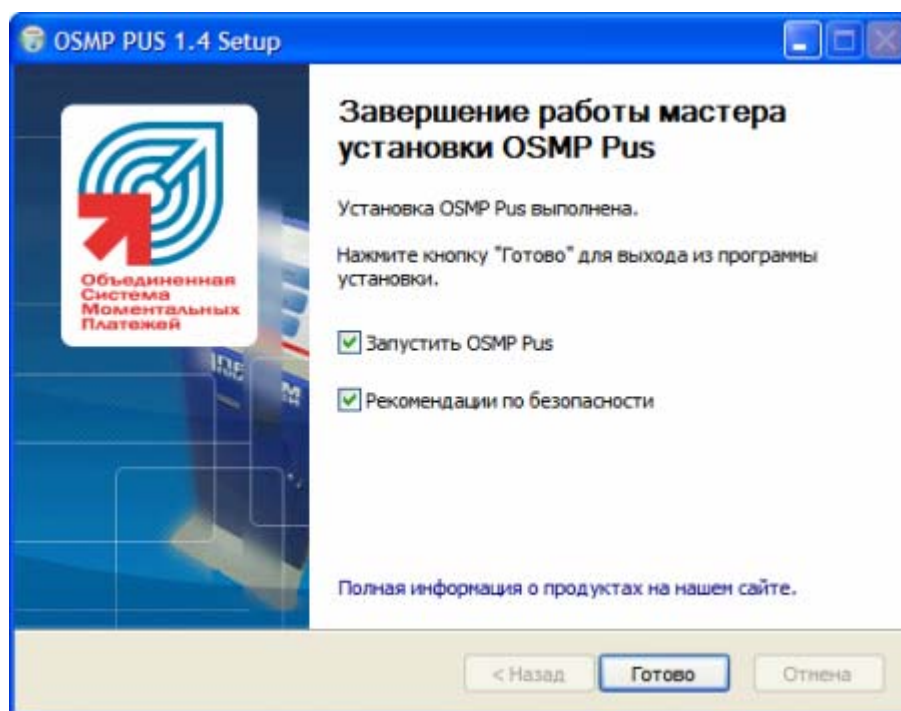
9. Отметьте флаг **Не создавать ярлыки**, если вы не хотите, чтобы ярлык на приложение был помещен в меню **Пуск**.
10. Нажмите кнопку **Установить** для запуска копирования файлов (Рис. 6). Для того чтобы вернуться на предыдущий шаг, нажмите кнопку **< Назад**.

Рис. 6. Копирование файлов



11. Процесс копирования вы можете видеть с помощью строки выполнения. Нажав кнопку **Детали...**, вы получите более детальную информацию о процессе установки.
12. По окончании копирования осуществляется переход к финальному шагу установки (Рис. 7).

Рис. 7. Финальный шаг установки



13. Если вы не хотите запускать приложение сразу после установки, снимите флаг **Запустить OSMP Pus**. Нажмите кнопку **Готово**. Для отмены установки, нажмите кнопку **Отмена**.

Совет Отметьте флаг **Рекомендации по безопасности**, чтобы ознакомиться с рекомендациями по обеспечению безопасности при работе с системой.

Примечание Также, более подробную информацию об этом или иных продуктах наших разработчиков вы можете получить, нажав ссылку **Полная информация о продуктах на нашем сайте**.

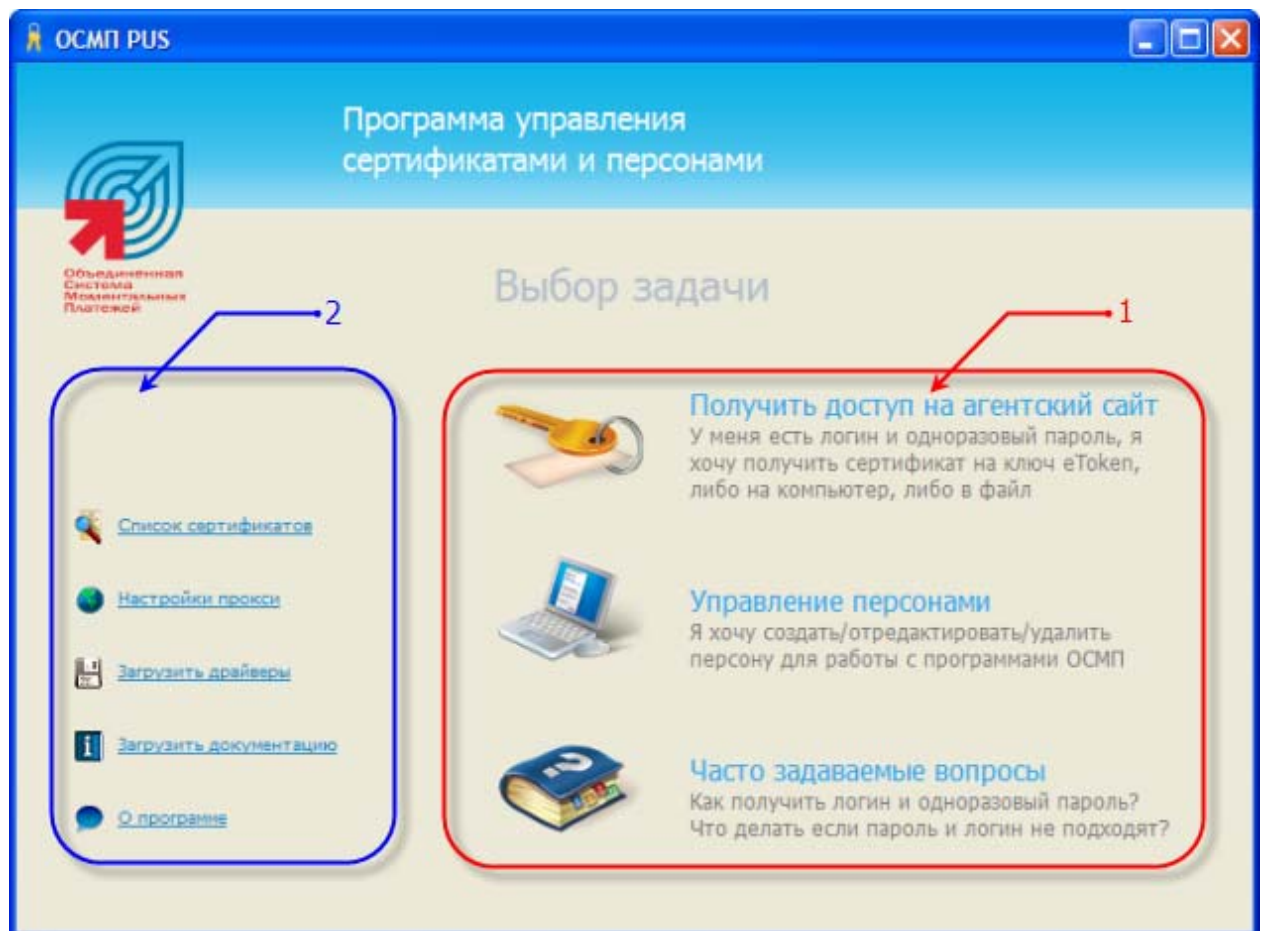
После выполнения указанных шагов программа будет установлена на ваш компьютер в указанное место (Рис. 4).

Если вы не указывали опцию **Не создавать ярлыки** (Рис. 5), то на рабочем столе и в меню **Пуск** будут расположены соответствующие ярлыки.

4.4. Главное окно программы

Главное окно программы показано на Рис. 8.

Рис. 8. Главное окно приложения



Главное окно приложения состоит из двух областей:

- **1** – список основных задач:

- **[Получить доступ на агентский сайт](https://portal.osmp.ru)** – позволяет создать сертификат для доступа на сайт <https://portal.osmp.ru>.
- **[Управление персонами](#)** – позволяет управлять авторизационными данными персон, используемых для работы с ПО ОСМП (например, *ОСМП Термит*).
- **Часто задаваемые вопросы** – список ответов на часто задаваемые вопросы.
- **2** – список дополнительных возможностей (см. раздел [7](#)).

5. ПОЛУЧЕНИЕ СЕРТИФИКАТА

Получения нового сертификата состоит из следующих шагов:

Шаг 1. [Получение одноразового пароля](#)

Шаг 2. [Генерация сертификата](#)

5.1. Получение одноразового пароля

Получение одноразового логина и пароля для нового пользователя осуществляется либо персонай вышестоящего агента, либо персонай текущего агента (подробнее о схеме работы читайте в [Приложении В](#)).

Для получения логина и одноразового пароля выполните следующее:

1. Зайдите в личный кабинет на сайте [ОСМП](#).

ПРИМЕЧАНИЕ Если требуется создать новую персону для нижестоящего агента, войдите под именем этого субагента.

2. Выберите пункт меню **Персоны → Создать новую**. При этом вы перейдете на форму создания новой персоны (Рис. 9).

ПРИМЕЧАНИЕ Данный этап необходим только при создании новой персоны.

В случае необходимости получения нового сертификата для существующей учетной записи, следует воспользоваться существующим логином для получения нового одноразового пароля и на основании этих данных сгенерировать сертификат.

Рис. 9. Получение одноразового пароля

СОЗДАНИЕ НОВОЙ ПЕРСОНЫ:

Фамилия персоны *	Иванов
Имя персоны	
Отчество персоны	
Login *	Login
Пароль *	<input type="password"/>
Повторить пароль *	<input type="password"/> Одноразовый пароль: <input checked="" type="checkbox"/>
Телефон	
Мобильный (в виде 79161112233 или 74959998877)	
E-Mail	
ICQ	
Принадлежит	Агенту: №1-"ОСМП"
Терминал	<input type="text"/>
Права	Claim OSMP <input type="text"/>
Подписать на рассылку:	<input type="checkbox"/> Новости
Получать рассылку по:	<input type="checkbox"/> E-mail
Введите цифры: *	4226 <input type="text"/>
Отключить персону	<input type="checkbox"/>

3. Внесите данные в обязательные поля.
4. Отметьте флаг **Одноразовый пароль**. Данная опция обозначает, что пароль не может служить для входа в систему, а только для генерации сертификата.
5. Нажмите кнопку **Записать** для сохранения данных.

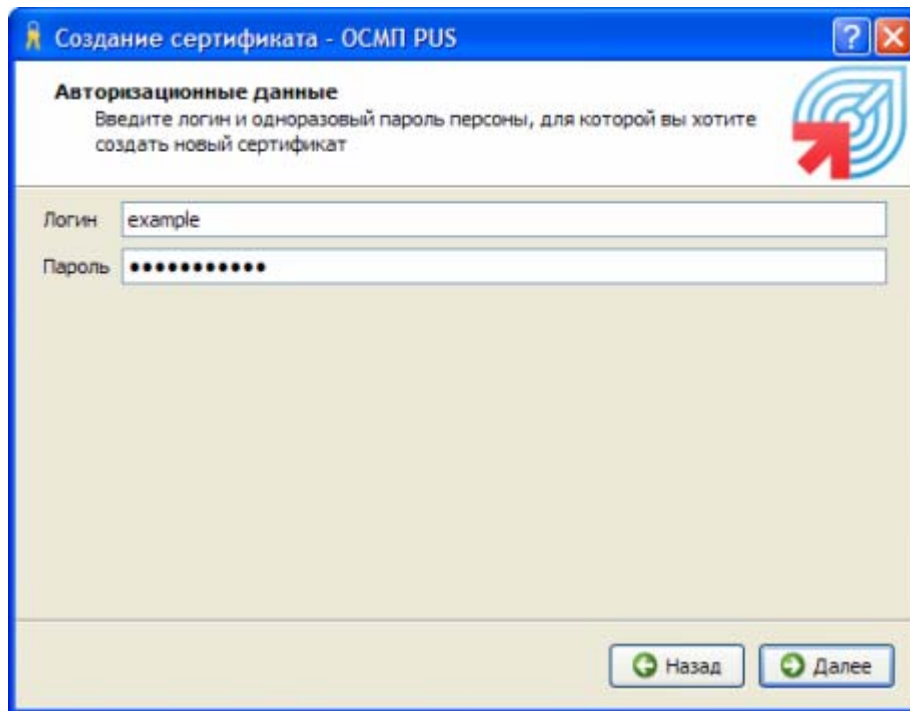
ВНИМАНИЕ! Сохраните одноразовый пароль.

5.2. Генерация сертификата

Для генерации сертификата выполните следующее:

1. Запустите *OSMP Pus* (Рис. 8).
2. Выберите действие **Получить доступ на агентский сайт**.
3. Следуйте рекомендациям **Мастера создания сертификата**.
4. Введите логин и одноразовый пароль персоны (Рис. 10). Подробнее о создании персоны см. раздел [5.1](#).

Рис. 10. Ввод авторизационных данных владельца сертификата



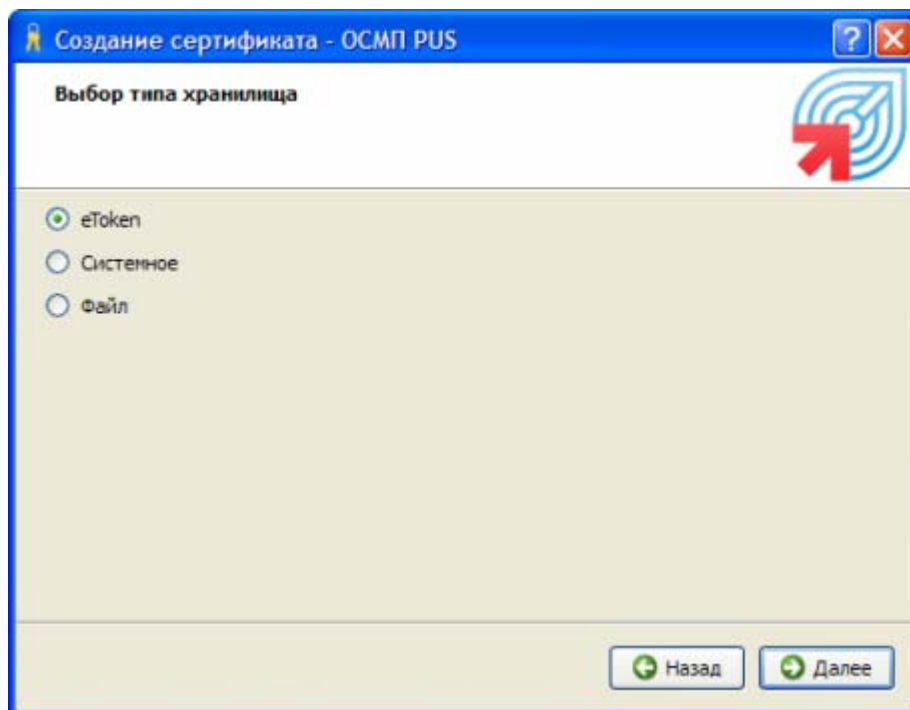
The screenshot shows a window titled "Создание сертификата - ОСМП PUS". The main heading is "Авторизационные данные" with the instruction "Введите логин и одноразовый пароль персоны, для которой вы хотите создать новый сертификат". There are two input fields: "Логин" containing the text "example" and "Пароль" containing ten dots. At the bottom right, there are two buttons: "Назад" and "Далее". A red arrow icon points towards the "Далее" button.

5. Выберите хранилище сертификата (Рис. 11). Сертификат будет сохранен в выбранном хранилище.

ВНИМАНИЕ! Наиболее рекомендуемое хранилище по соображениям безопасности – **eToken**.
Наименее безопасное хранилище – **Файл**.

При сохранении сертификата в системном хранилище обязательно прочтите [Приложение В](#).

Рис. 11. Выбор хранилища сертификата



The screenshot shows the same window as Figure 10, but the heading is "Выбор типа хранилища". There are three radio button options: "eToken" (which is selected), "Системное", and "Файл". At the bottom right, there are two buttons: "Назад" and "Далее". A red arrow icon points towards the "Далее" button.

6. УПРАВЛЕНИЕ ПЕРСОНАМИ

Задача **Управления персонами** позволяет [создать](#), а также [отредактировать/удалить](#) авторизационные данные пользователей, используемые при работе с приложениями ОСМП (например, ОСМП Термит).

6.1. Создание персоны

Для создания новой персоны выполните следующее:

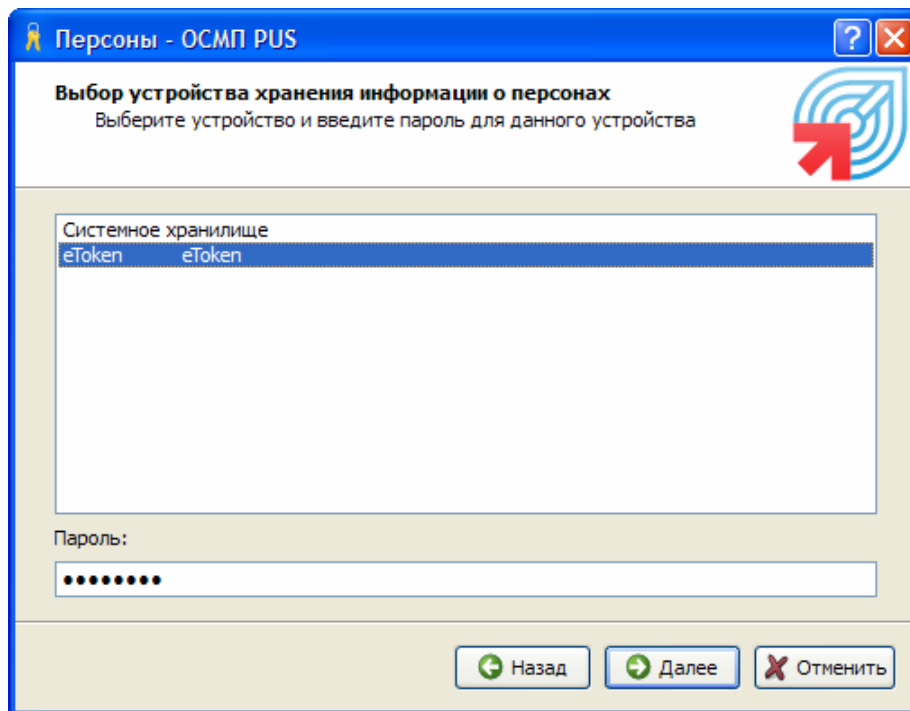
1. Выберите пункт **Управление персонами**, затем действие **Создать**.
2. Выберите тип хранилища, в которое будет записана информация о персоне (Рис. 12).

ВНИМАНИЕ! Наиболее рекомендуемое хранилище по соображениям безопасности – **eToken**.

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

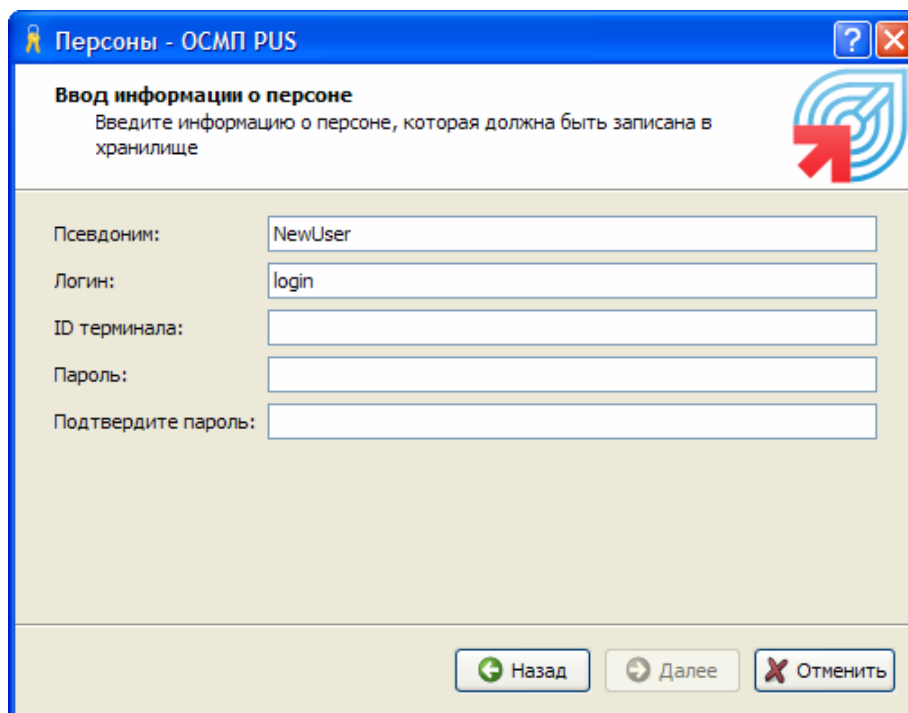
3. При выборе eToken введите пароль для доступа к нему.

Рис. 12. Выбор хранилища для записи новой персоны



4. Введите авторизационную информацию (Рис. 13):
 - *Псевдоним* – имя, отображаемое при работе в приложении.
 - *Логин* – логин персоны, созданной на сайте <https://portal.osmp.ru>.
 - *ID терминала* – номер терминала, созданного на сайте <https://portal.osmp.ru>.
 - *Пароль* – одноразовый пароль персоны.

Рис. 13. Ввод информации о персоне



The screenshot shows a window titled "Персоны - ОСМП PUS" with a blue header bar. Below the header, the text "Ввод информации о персоне" is displayed, followed by the instruction "Введите информацию о персоне, которая должна быть записана в хранилище". To the right of this text is a red arrow icon pointing towards a target symbol. The form contains five input fields: "Псевдоним:" with the value "NewUser", "Логин:" with the value "login", "ID терминала:", "Пароль:", and "Подтвердите пароль:". At the bottom of the window, there are three buttons: "Назад" (Back), "Далее" (Next), and "Отменить" (Cancel).

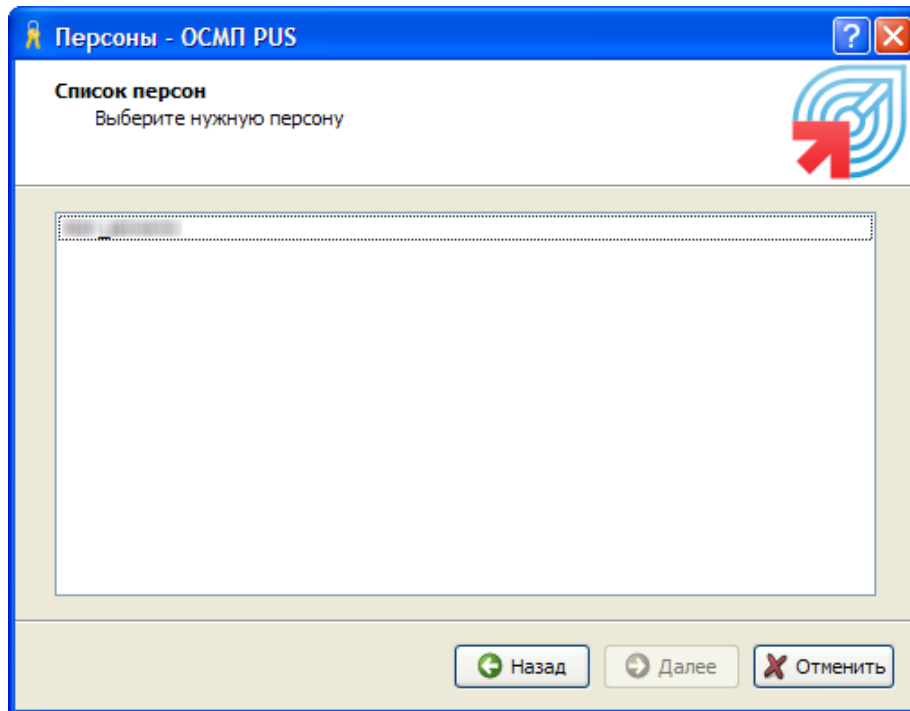
5. Нажмите кнопку **Завершить** для сохранения авторизационных данных персоны.

6.2. Редактирование/удаление персоны

Для редактирования/удаления данных персоны выполните следующее:

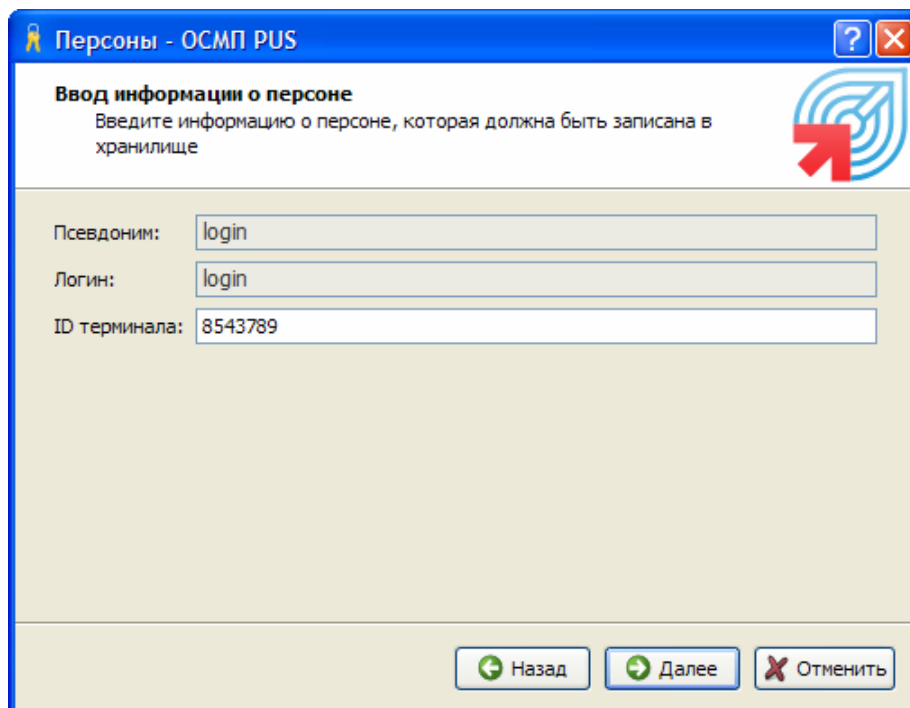
1. Выберите пункт **Управление персонами**.
2. Выберите нужное действие и нажмите кнопку **Далее**.
3. Выберите хранилище, на котором находятся авторизационные данные и введите пароль для доступа к нему.
4. Выберите нужную персону (на ключе может храниться информация о нескольких персонах) (Рис. 14).

Рис. 14. Выбор персоны



5. При редактировании – измените **ID терминала** (Рис. 15).

Рис. 15. Изменение данных персоны



6. Нажмите кнопку **Завершить**.

7. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

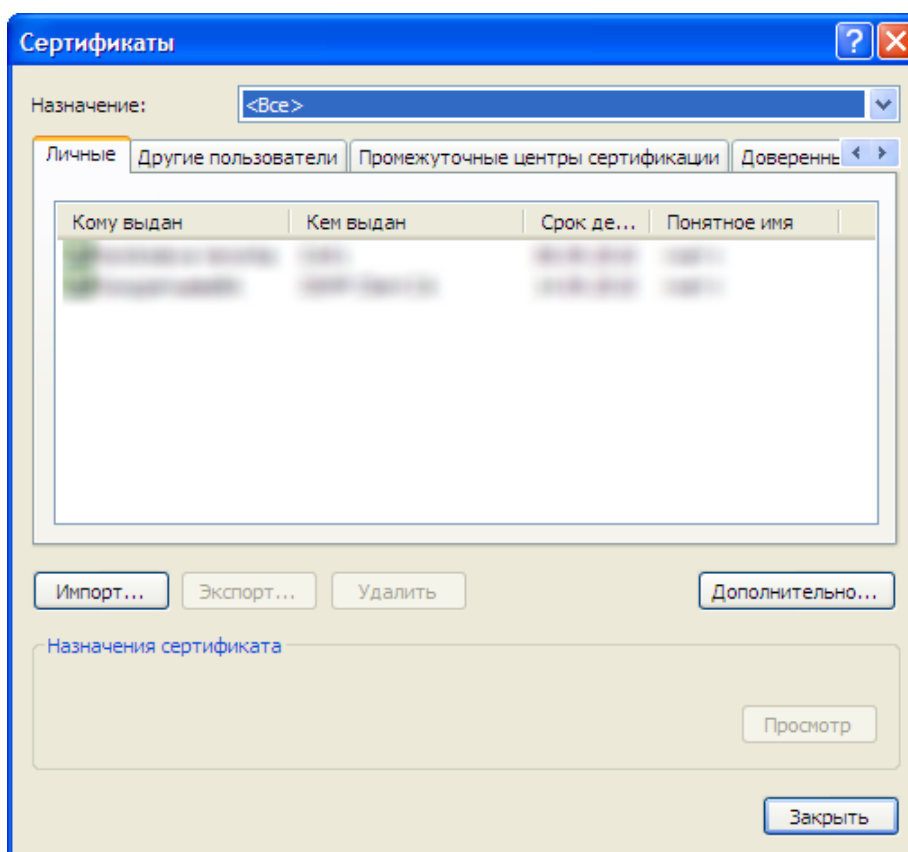
Приложение реализует следующие дополнительные возможности:

- [Список сертификатов](#) – открывает список системных сертификатов;
- [Настройки прокси](#) – позволяет задать настройки прокси-сервера для доступа к Интернету;
- [Загрузить драйверы](#) – позволяет загрузить драйвера, необходимые для работы с eToken в различных ОС;
- [Загрузить документацию](#) – открывает ссылку на руководство пользователя *OSMP Pus*;
- [О программе](#) – открывает окно с информацией о приложении.

7.1. Просмотр/управление установленными сертификатами

1. Для просмотра данных о выданных сертификатах нажмите ссылку **Список сертификатов** на главном окне программы (Рис. 8).
2. Откроется окно со списком сертификатов, установленных в системе (Рис. 16).

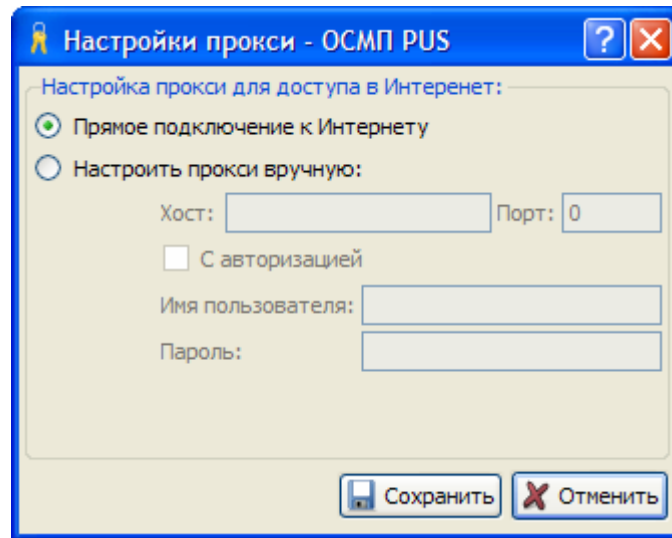
Рис. 16. Системные сертификаты



7.2. Настройка прокси-сервера

1. Для просмотра данных о настройках прокси-сервера нажмите ссылку **Настройки прокси** на главной форме (Рис. 8).
2. Откроется окно для изменения настроек подключения (Рис. 17).

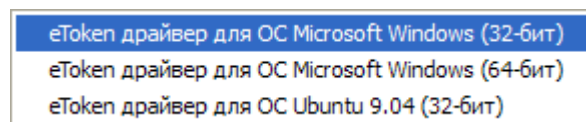
Рис. 17. Настройки прокси-сервера для доступа к Интернету



7.3. Загрузка драйверов

1. Для загрузки драйверов для работы с eToken нажмите ссылку **Загрузить драйверы**, расположенную на главном окне программы (Рис. 8).
2. Появится список драйверов для различных операционных систем (Рис. 18).

Рис. 18. Загрузка драйверов



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

7.4. Загрузка документации

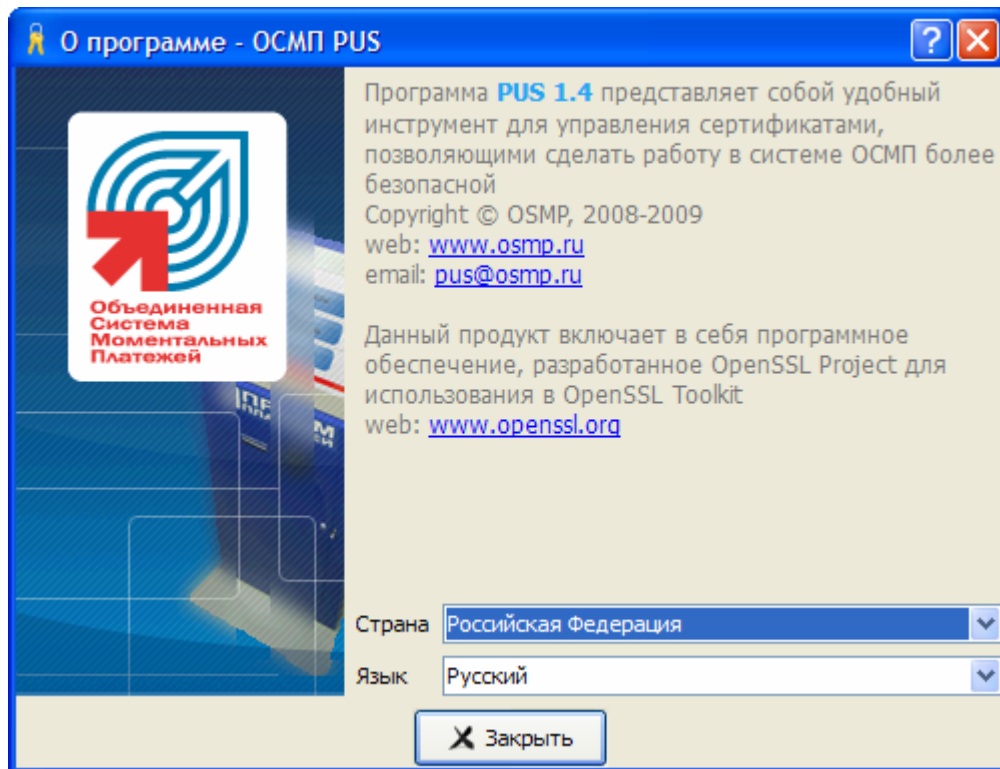
Для скачивания данное *Руководство пользователя* на локальный компьютер нажмите на ссылку **Документация**, расположенную на главном окне программы (Рис. 8).

7.5. О программе

1. Для просмотра информации о программе нажмите ссылку **О программе**, расположенную на главном окне программы (Рис. 8).

2. В появившемся окне можно изменить язык интерфейса программы (Рис. 19). Изменение будет применено после перезапуска приложения.

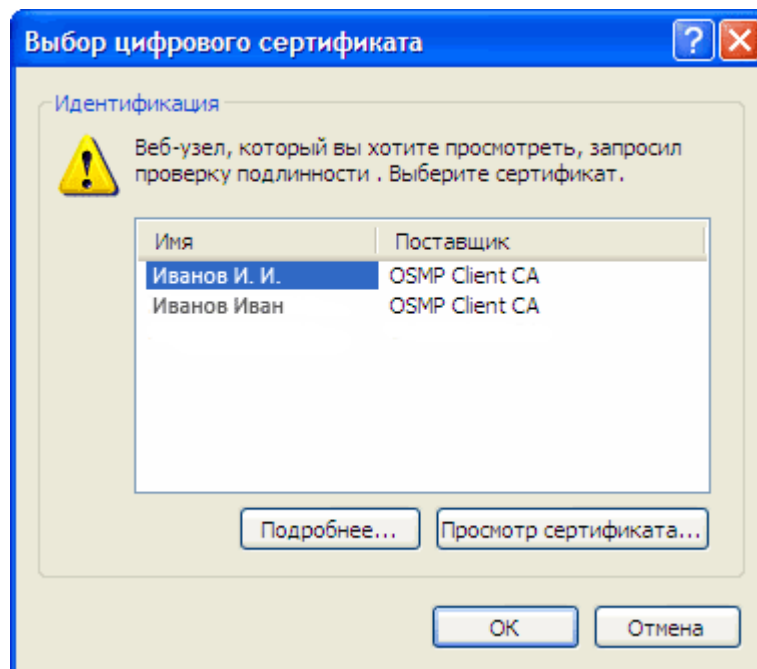
Рис. 19. Информация о программе



8. ВХОД НА САЙТ

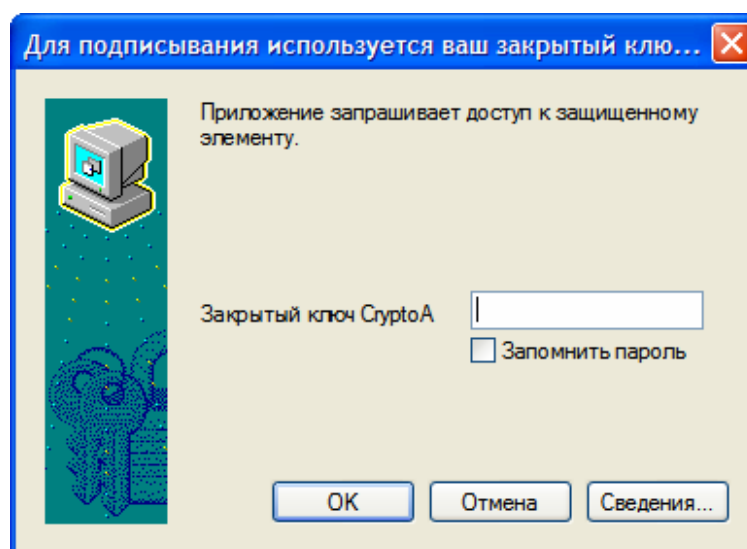
1. При попытке входа в личный кабинет вам будет предложено выбрать сертификат (Рис. 20).

Рис. 20. Выбор сертификата при входе на сайт



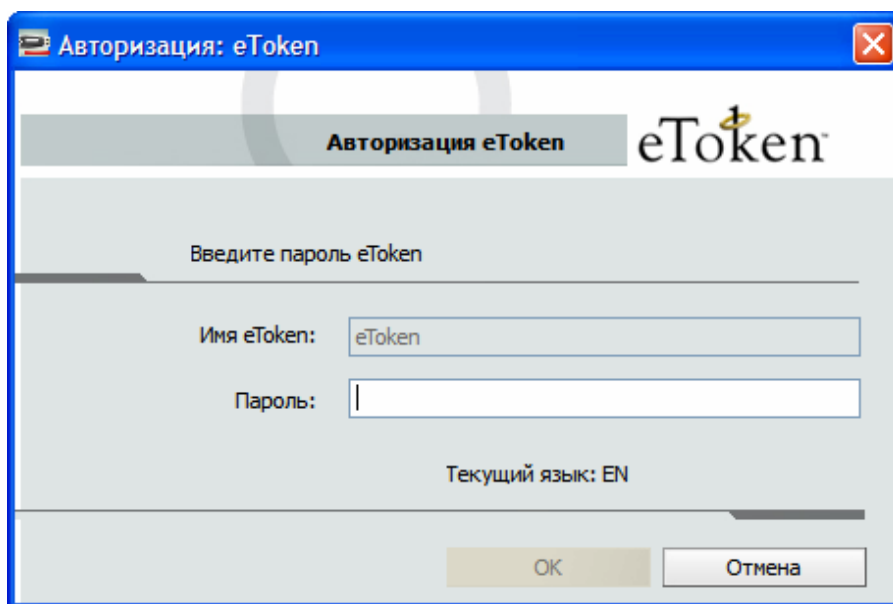
2. Выберите нужный сертификат (сертификаты различаются по имени владельца, которое вы устанавливаете при получении сертификата (Рис. 10)).
3. Введите пароль:
 - 3.1. В случае если при сохранении сертификата в системное хранилище вы выбрали высокий уровень безопасности (см. [Приложение В](#)), при входе на сайт вам будет предложено указать пароль для доступа к закрытому ключу (Рис. 21).

Рис. 21. Ввод пароля для закрытого ключа в системном хранилище



- 3.2. Если сертификат был сохранен на eToken, введите пароль для доступа к закрытому ключу ([Рис. 22](#)).

Рис. 22. Ввод пароля eToken



После этого вы попадете в личный кабинет на сайте ОСМП и получите доступ ко всем функциям в соответствии с ролью персоны.

Пояснение Вход на сайт осуществляется по протоколу HTTPS с запросом сервером клиентского сертификата.

Схема аутентификации следующая:

1. Запрос сертификата сервером осуществляется при установке SSL подключения (процесс SSL handshake).
2. После выбора нужного сертификата пользователем в диалоговом окне браузера, сервер проверяет свою подпись сертификата пользователя и ищет его в списке отозванных.
3. Если сертификата нет в числе отозванных, сервер устанавливает защищенное соединение.

ПРИЛОЖЕНИЕ А: РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

1. Для предотвращения несанкционированного проведения платежей от имени *терминалов агента* с другого оборудования необходимо осуществить «привязку» каждого *терминала*, используемого *агентом*, к серийному номеру оборудования.

Определить серийный номер конкретного типа *терминала* агент может на личной странице сайта следующим образом:

- **Win-терминал (Dealer)** – в меню программы **Dealer** выбрать закладку **Справка → 0 программе**.
- **POS-терминал (Nurit)** – **Меню → Сервис → Серийный номер**.
- **Автомат самообслуживания** – в **Монитор терминалов**, далее серийный номер (указан в поле **Инфо** после версии программного обеспечения (ПО)).

Для осуществления «привязки» необходимо прописать серийный номер в поле **Привязан к SN** (Раздел **Редактирование терминала**).

2. Для снижения ущерба и локализации источника в случае кражи учетных данных *персоны* (под «*Персоной*» понимается учетная запись с определенным набором прав доступа к Системе, зарегистрированная Агентом для пользователей), Агенту необходимо при проведении Платежей использовать учетные записи с минимальным необходимым набором прав («продавец»). Кроме того, Агенту следует произвести привязку Персон к Терминалам, с которых эти Персоны проводят Платежи.
3. Для защиты от кражи компьютерными вирусами авторизационных данных персон *агенту* необходимо защищать периодически обновляемыми антивирусными средствами компьютеры, с которых ведется работа с *Системой*. Оператор *Системы* рекомендует *агентам* также использовать криптоключи eToken Pro.

Оператор *Системы* настоятельно не рекомендует *агенту* (пользователям *агента*) заходить в *Систему* с общедоступных компьютеров (например, с компьютеров в интернет-кафе).

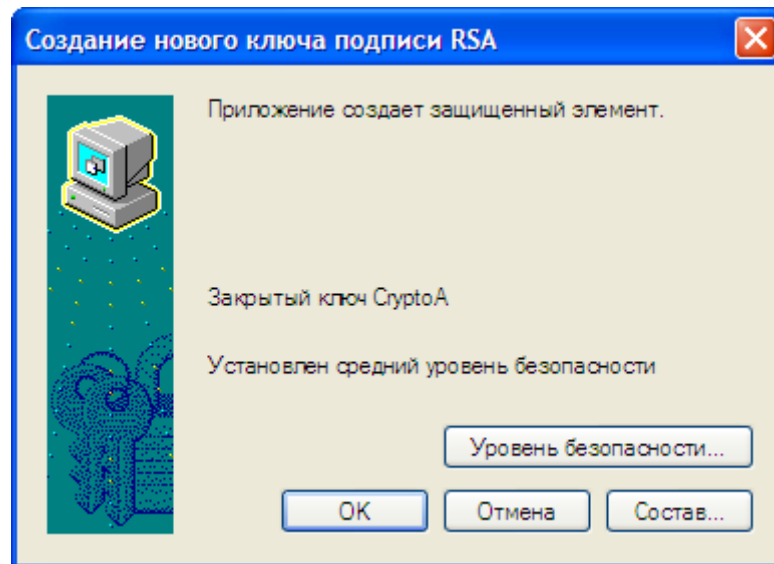
4. На компьютерах, используемых для работы с *Системой*, *агенту* рекомендуется ограничить доступ в сеть Интернет, а также воздержаться от открытия подозрительных писем с вложениями. При получении письма, содержащего вложения, от имени *оператора Системы* *агенту* рекомендуется такое письмо переслать в адрес sb@osmp.ru для его проверки и, в случае обнаружения вируса, внесения вируса в антивирусные базы.

ПРИЛОЖЕНИЕ Б: СОХРАНЕНИЕ СЕРТИФИКАТА В СИСТЕМНОМ ХРАНИЛИЩЕ

Для сохранения сертификата в системном хранилище выполните следующее:

1. Выберите уровень безопасности по кнопке **Уровень безопасности...** в диалоге **Импорт нового закрытого ключа обмена** (Рис. 23).

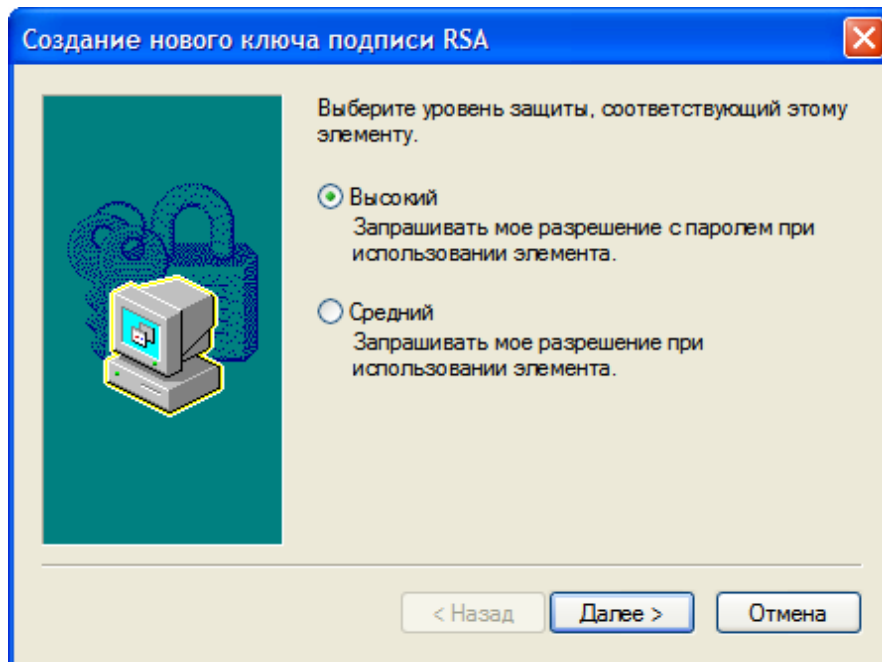
Рис. 23. Импорт закрытого ключа в системное хранилище



РЕКОМЕНДАЦИИ

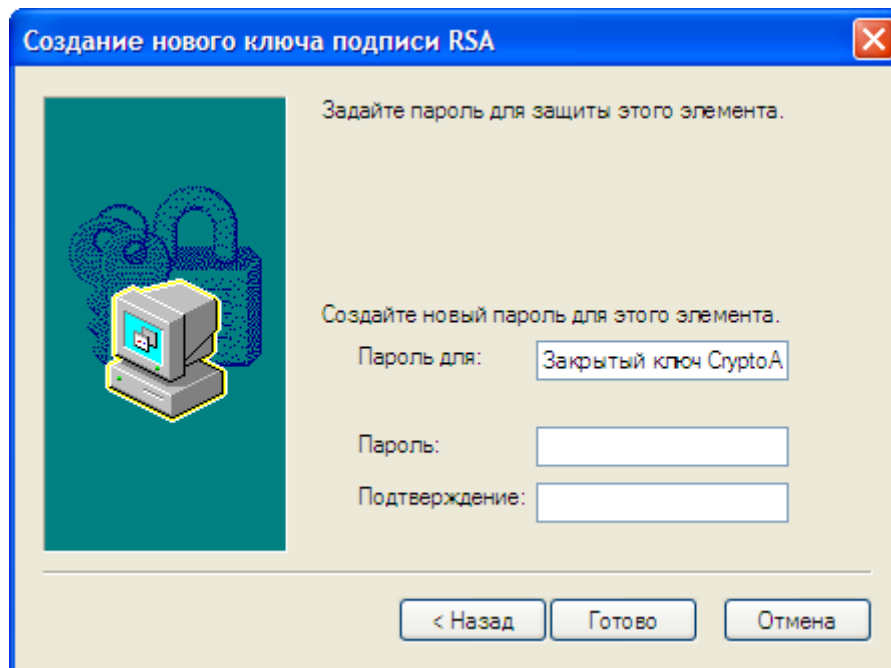
В целях повышения уровня защиты установите **Высокий** уровень (Рис. 24) и используйте безопасный **пароль** (Рис. 25).

Рис. 24. Установка высокого уровня безопасности



Для высокого уровня безопасности также укажите **пароль** (Рис. 25).

Рис. 25. Пароль для защиты закрытого ключа в системном хранилище



СПИСОК РИСУНКОВ

Рис. 1. Установка пароля администратора	6
Рис. 2. Первый шаг установки	7
Рис. 3. Второй шаг установки	8
Рис. 4. Третий шаг установки	8
Рис. 5. Четвертый шаг установки	9
Рис. 6. Копирование файлов	10
Рис. 7. Финальный шаг установки	10
Рис. 8. Главное окно приложения	11
Рис. 9. Получение одноразового пароля	14
Рис. 10. Ввод авторизационных данных владельца сертификата	15
Рис. 11. Выбор хранилища сертификата	15
Рис. 12. Выбор хранилища для записи новой персоны	16
Рис. 13. Ввод информации о персоне	17
Рис. 14. Выбор персоны	18
Рис. 15. Изменение данных персоны	18
Рис. 16. Системные сертификаты	19
Рис. 17. Настройки прокси-сервера для доступа к Интернету	20
Рис. 18. Загрузка драйверов	20
Рис. 19. Информация о программе	21
Рис. 20. Выбор сертификата при входе на сайт	22
Рис. 21. Ввод пароля для закрытого ключа в системном хранилище	22
Рис. 22. Ввод пароля eToken	23
Рис. 23. Импорт закрытого ключа в системное хранилище	25
Рис. 24. Установка высокого уровня безопасности	26
Рис. 25. Пароль для защиты закрытого ключа в системном хранилище	26