Требования к автоматизированному рабочему месту и установленному программному обеспечению

Руководство пользователя

Оглавление

1 Требования к автоматизированному рабочему месту

Глава содержит перечень требований к автоматизированному рабочему месту.

Для обеспечения работы на электронной площадке автоматизированное рабочее место (АРМ) пользователя должно иметь следующую конфигурацию:

- IBM-совместимый персональный компьютер, по характеристикам аналогичный Pentium 2, RAM 32 Mb, HD 2 Gb;
- монитор с разрешающей способностью 1280x800.

Программное обеспечение АРМ:

- операционная система MS Windows 2000, XP, Vista или Windows 7;
- один из современных браузеров (Internet Explorer версии 8 и выше, Mozilla Firefox версии 3.6 и выше, Opera версии 11.x, Google Chrome) с поддержкой сценариев JavaScript;
- средство электронной подписи КриптоПро CSP версии 3.6 и выше;
- сертификат электронной подписи, установленный в операционной системе (со ссылкой на закрытый ключ);
- установленный плагин для браузера «КриптоПро ЭЦП Browser plug-in»;
- программные пакеты для работы с документами (например, MS Office либо аналоги, Adobe Reader);
- средства сжатия (упаковки) файлов (RAR, ZIP, WINZIP).

2 Установка средства электронной подписи КриптоПро CSP и сертификата электронной подписи

Глава содержит основные требования к установке средств электронной подписи КриптоПро CSP и сертификата электронной подписи.

Для приобретения средства электронной подписи КриптоПро CSP и сертификата электронной подписи необходимо обратиться в один из доверенных Удостоверяющих центров, аккредитованных ЭТП. Список аккредитованных Удостоверяющих центров можно найти на соответствующем разделе сайта ЭТП, или обратившись по телефону технической поддержки ЭТП. Для установки и настройки КриптоПро CSP и сертификата электронной подписи необходимо следовать инструкциям Удостоверяющего центра.

Необходимо обратить внимание на то, что использовать можно только действующий сертификат, т.е. сертификат, срок действия которого не истек, и который не был отозван. Также на рабочем месте пользователя должен быть установлен корневой сертификат Удостоверяющего центра, выдавшего сертификат. При невыполнении какого-либо из данных условий сертификат пользователя не будет отображаться в списке выбора сертификата на электронной торговой площадке, и его использование для работы будет невозможно. Для проверки срока действия сертификата и установки корневого сертификата Удостоверяющего центра необходимо выполнить шаги, описанные в ответе на вопрос в главе 5 «Вопросы и ответы» данного руководства.

3 Установка КриптоПро ЭЦП Browser plug-in

В главе представлено описание процесса установки КриптоПро ЭЦП Browser plug-in.

Для установки КриптоПро ЭЦП Browser plug-in загрузите и запустите установочный файл плагина с сайта разработчика данного плагина - компании "Крипто-Про".

ВНИМАНИЕ! Для корректной работы КриптоПро ЭЦП Browser plug-in в браузере Google Chrome необходимо произвести дополнительную настройку данного плагина. Для этого выполните следующие действия:

1. Запустите «Настройки КриптоПро ЭЦП Browser Plug-in», для этого перейдите в главное меню Windows Пуск → КРИПТО-ПРО → Настройки ЭЦП Browser Plug-in. Если при открытии данного окна появится сообщении о блокировании всплывающего окна, необходимо разблокировать всплывающее окно.
2. В открывшемся окне в список доверенных узлов добавьте узел **с вашим именем URL площадки** (например, http://companyzakupki.ru) и нажмите кнопку **«Сохранить»** (Рис. 3 .1).

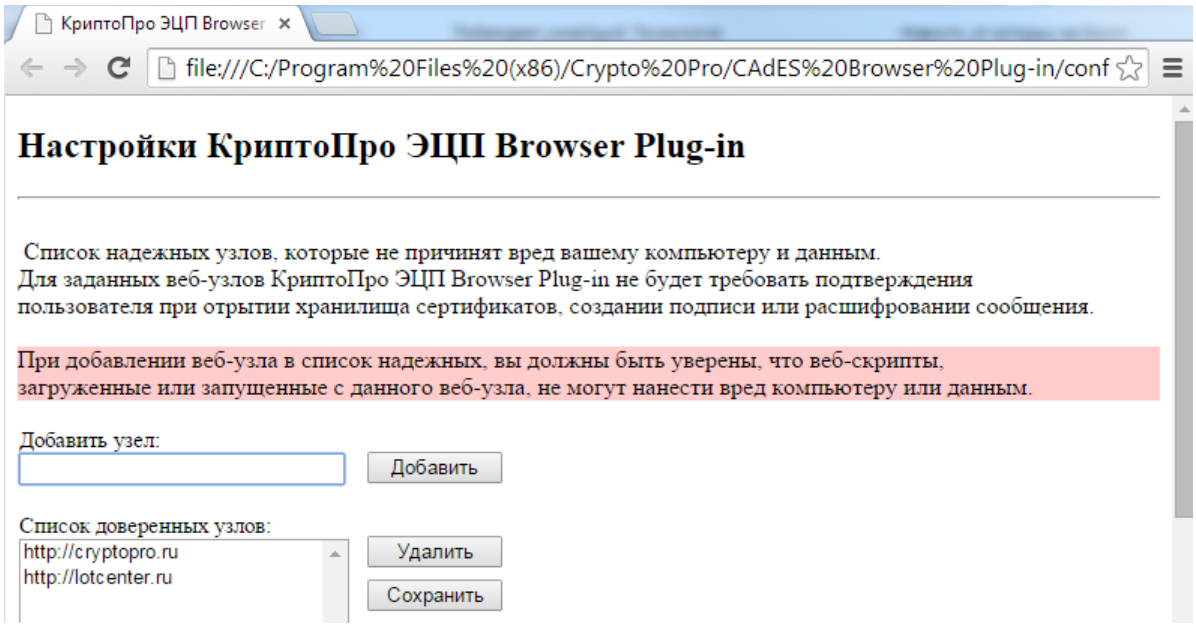

Рис. 3.1

4 Настройка обозревателя Internet Explorer

В главе представлено описание процесса настройки обозревателя Internet Explorer с целью обеспечения корректной работы на электронной площадке.

Для обеспечения корректной работы на электронной площадке выполните следующие настройки:

1. Запустите браузер Internet Explorer.
2. Перейдите в раздел «Сервис» → «Свойства обозревателя» (Рис. 4 .2).

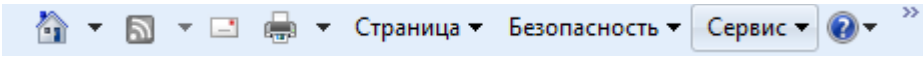

Рис. 4.2

3. В открывшемся окне «Свойства обозревателя» перейдите на вкладку «Безопасность» и выберите зону «Надёжные узлы» (Рис. 4 .3).

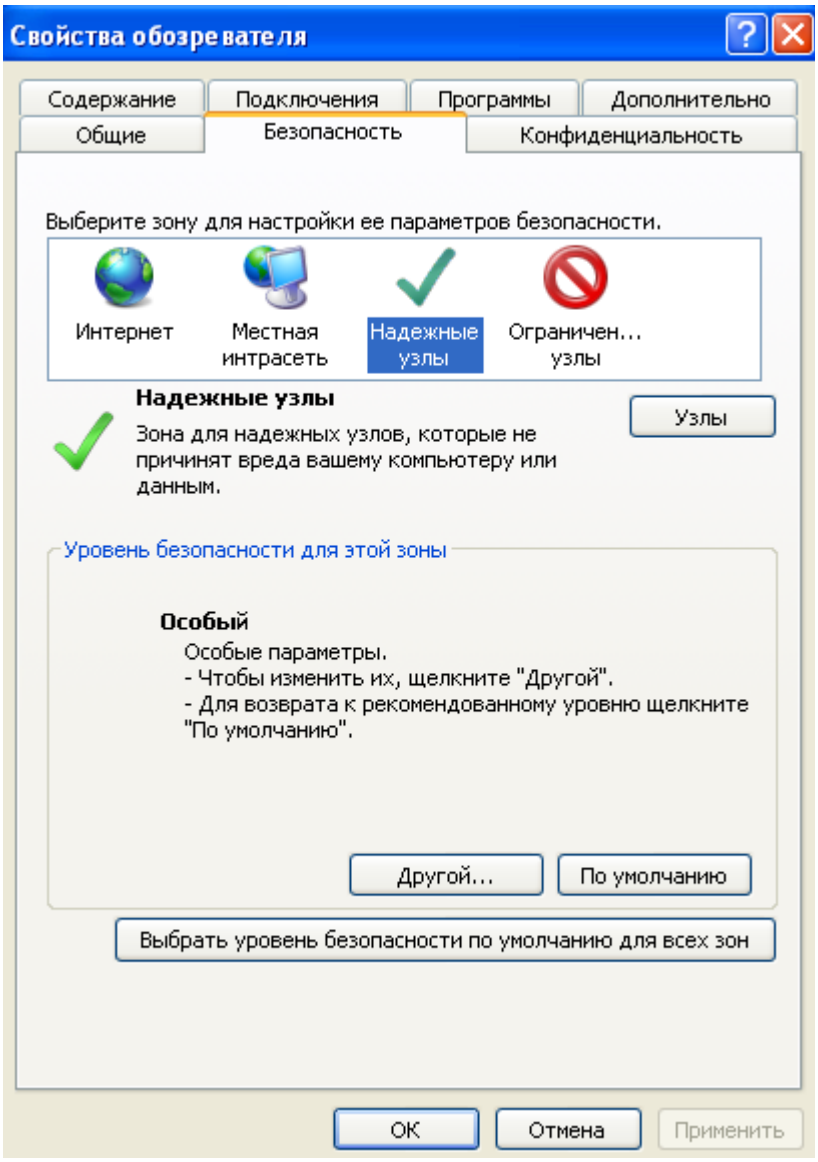

Рис. 4.3

4. В надежные узлы следует **добавить ваш URL площадки**, для этого выполните следующие действия:

- нажмите кнопку «Узлы». На экране появится форма добавления надёжных узлов (Рис. 4 .4).

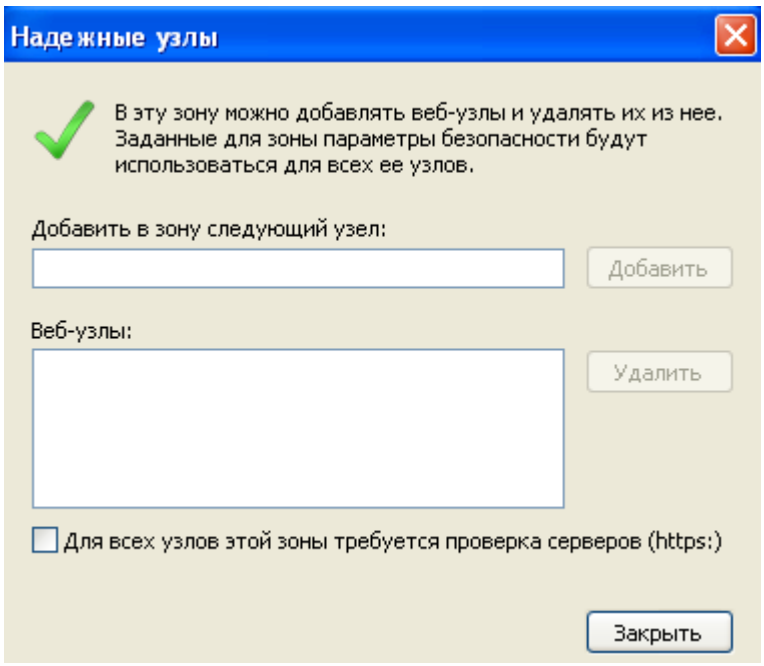

Рис. 4.4

- снимите флажок в поле «Для всех узлов этой зоны требуется проверка серверов (https:)».
- в поле «Добавить в зону следующий узел:» укажите адрес *.[адрес площадки] и нажмите кнопку **«Добавить»**. Например, *.companyzakupki.ru
- после добавления узлов нажмите кнопку **«Закрыть»**.

5. В окне обозревателя на вкладке «Безопасность» нажмите кнопку **«Другой…»** (см. Рис. 4 .3).
6. В открывшемся окне «Параметры безопасности – зона надёжных узлов»:
   - в пункте «Загрузка» включите следующие параметры:
     - Автоматические запросы на загрузку файлов;
     - Загрузка файлов;
     - Загрузка шрифта;
   - в пункте «Элементы ActiveX и модули подключения» включите все параметры данного пункта.
7. Нажмите кнопку **«ОК»**.
8. В окне обозревателя перейдите на вкладку «Конфиденциальность».
9. В блоке «Блокирование всплывающих окон» установите флажок в поле «Включить блокирование всплывающих окон» и нажмите кнопку **«Параметры»** (Рис. 4 .5).

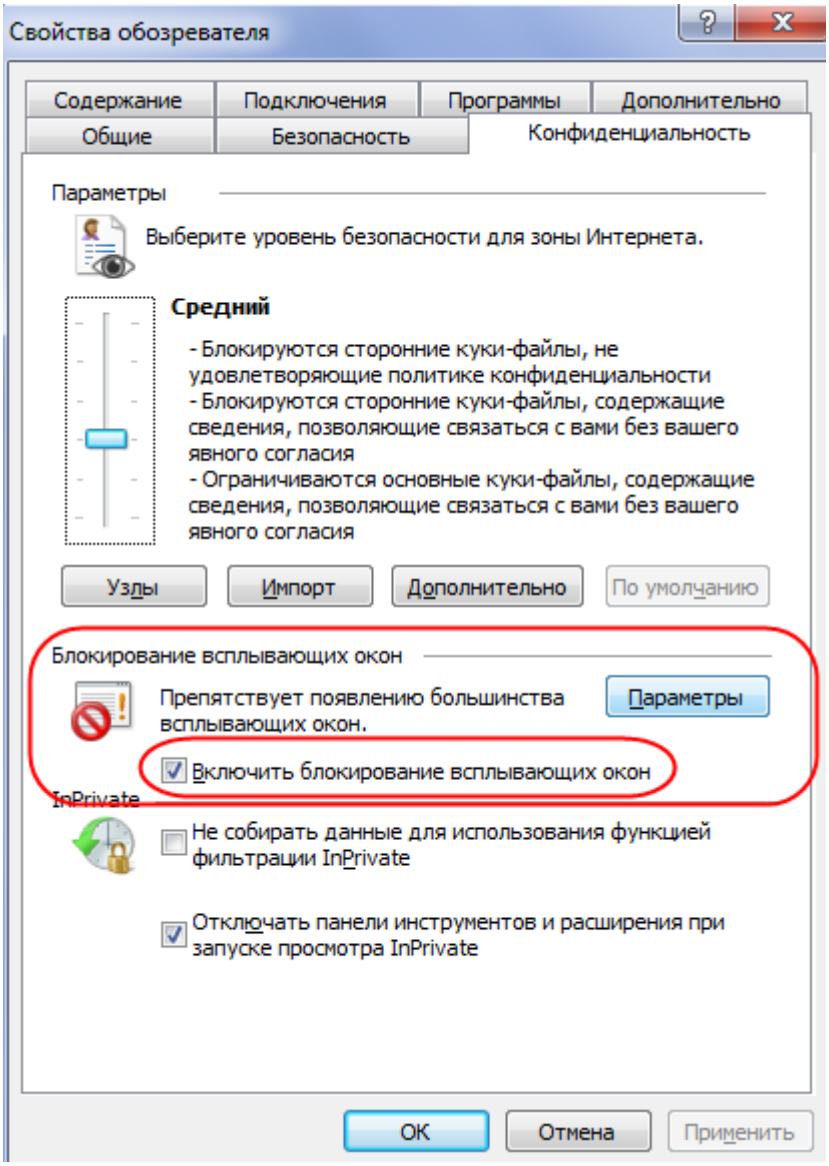

Рис. 4.5

10. В открывшемся окне «Параметры блокирования всплывающих окон» (Рис. 4 . 6):
    - В поле «Адрес веб-узла, получающего разрешение:» укажите перечень URL тех веб-узлов, для которых будет разрешено открытие в виде всплывающих окон. Например, – company.ru
        - нажмите кнопку **«Добавить»**.
        - нажмите кнопку **«Закрыть»**.

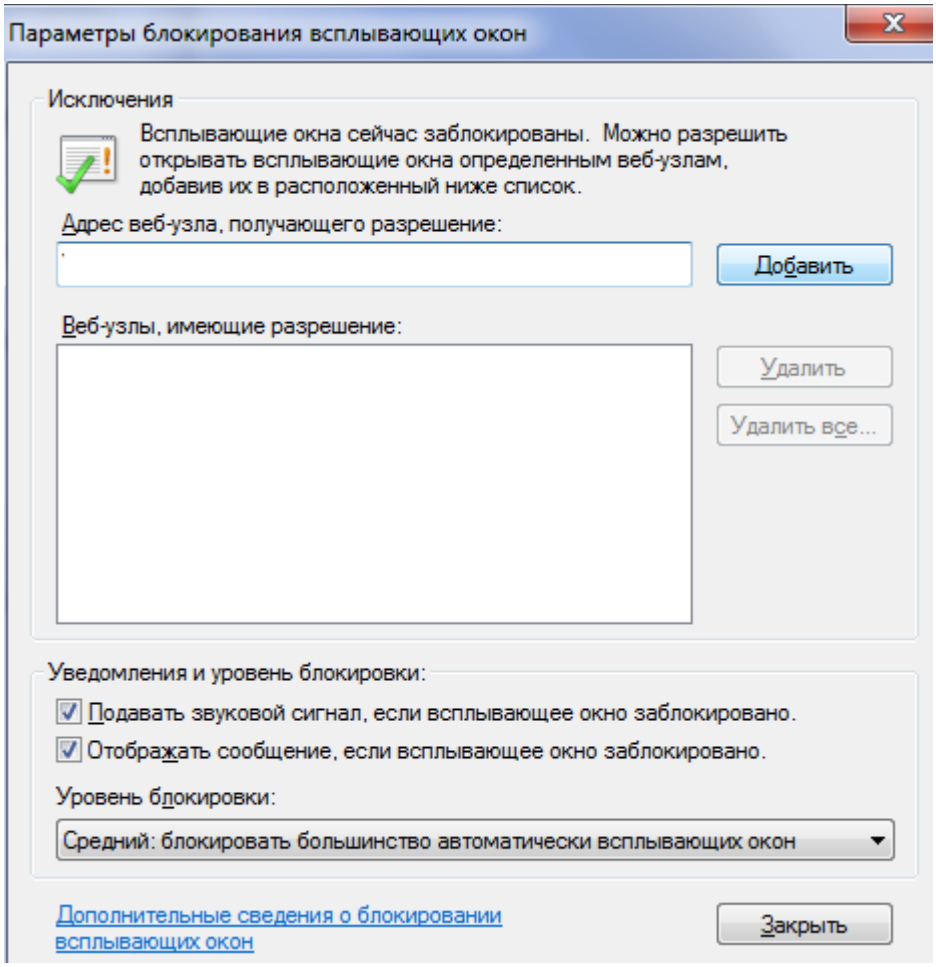

Рис. 4.6

11. Для завершения настройки свойств обозревателя нажмите кнопку **«Применить»** и **«ОК»**.

5 Вопросы и ответы

В главе представлены ответы на часто задаваемые вопросы, которые касаются настройки программного обеспечения с целью корректной работы пользователей на электронной площадке.

Вопрос: Почему установленный на рабочем месте сертификат не отображается в списке выбора сертификата?

Ответ: Использовать можно только действующий сертификат, т.е. сертификат, срок действия которого не истек, и который не был отозван. Также на рабочем месте пользователя должен быть установлен корневой сертификат Удостоверяющего центра, выдавшего сертификат. При невыполнении какого-либо из данных условий сертификат пользователя не будет отображаться в списке выбора сертификата на электронной торговой площадке, и его использование для работы будет невозможно.

Для проверки срока действия сертификата и установки корневого сертификата Удостоверяющего центра необходимо выполнить следующие действия:

1. В меню «Пуск» выберете раздел «Панель управления».
2. В открывшемся окне откройте раздел «Свойства браузера» (либо «Свойства обозревателя»).
3. В открывшемся окне (Рис. 5 .7) перейдите на вкладку «Содержание», после чего нажмите кнопку **«Сертификаты»**.

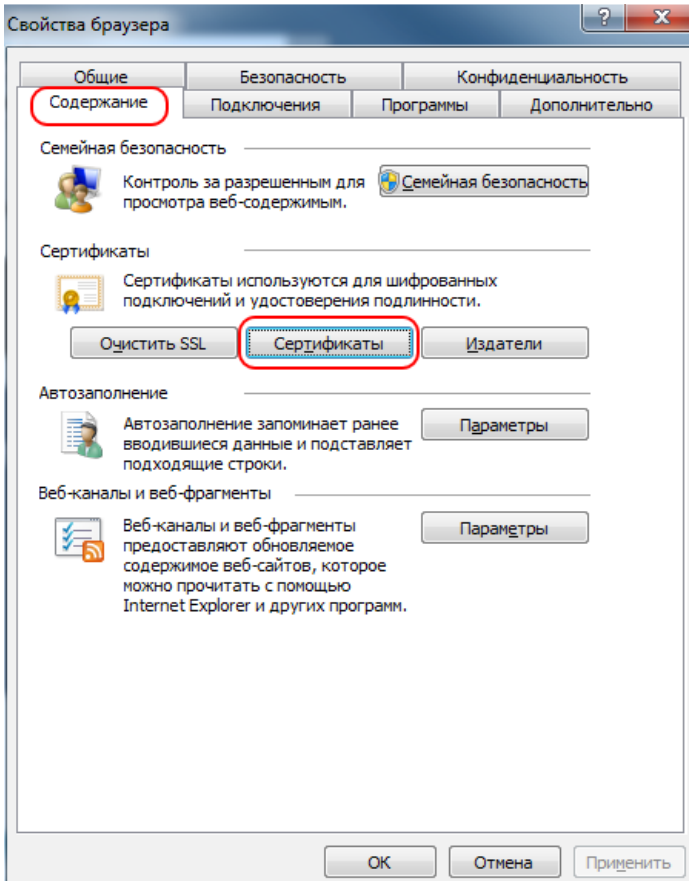

Рис. 5.7

4. В открывшемся окне «Сертификаты» (Рис. 5 .8) выберите ваш сертификат, после чего нажмите кнопку **«Просмотр»**, после чего откроется окно «Сертификат».

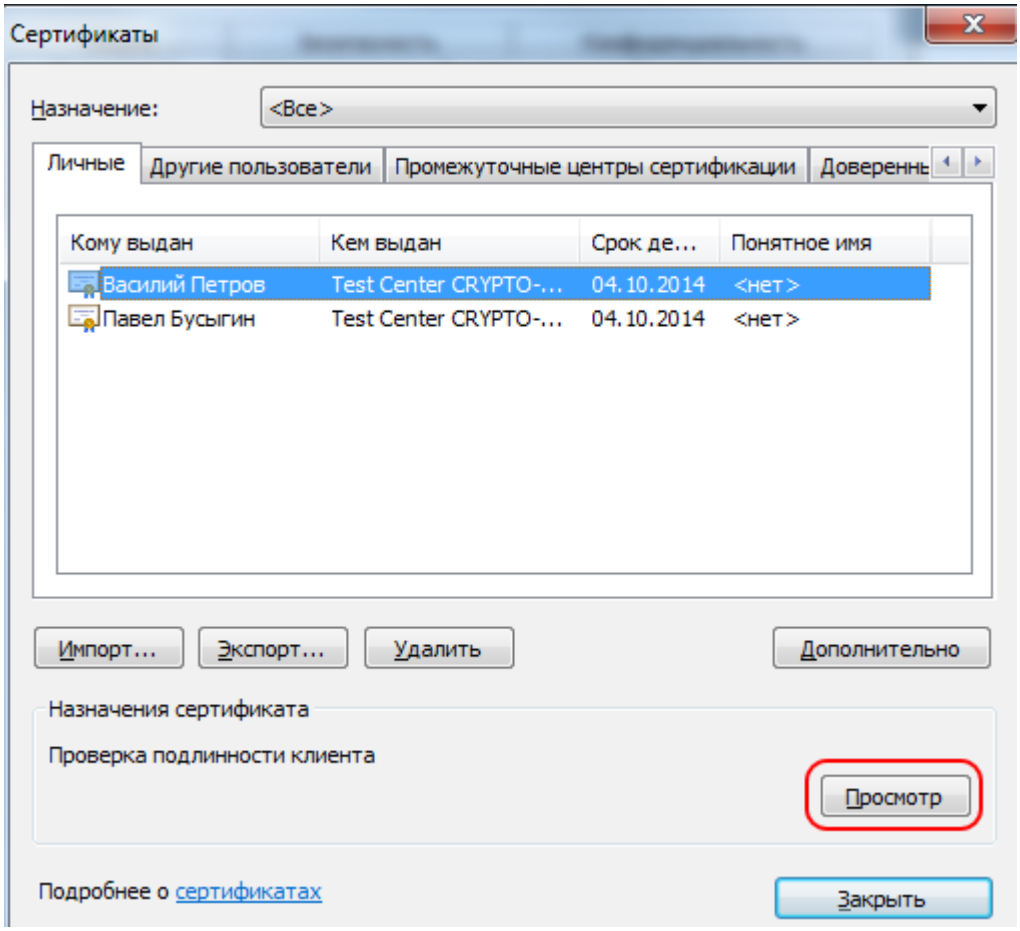

Рис. 5.8

5. Для проверки срока действия сертификата в открывшемся окне «Сертификат» (Рис. 5 .9) обратите внимание на интервал действия сертификата – надпись «**Действителен с** <начальная дата> **по** <конечная дата>» – текущая дата должна попадать в интервал действия сертификата. Если срок действия вашего сертификата истек, необходимо получить и установить на рабочее место новый сертификат.

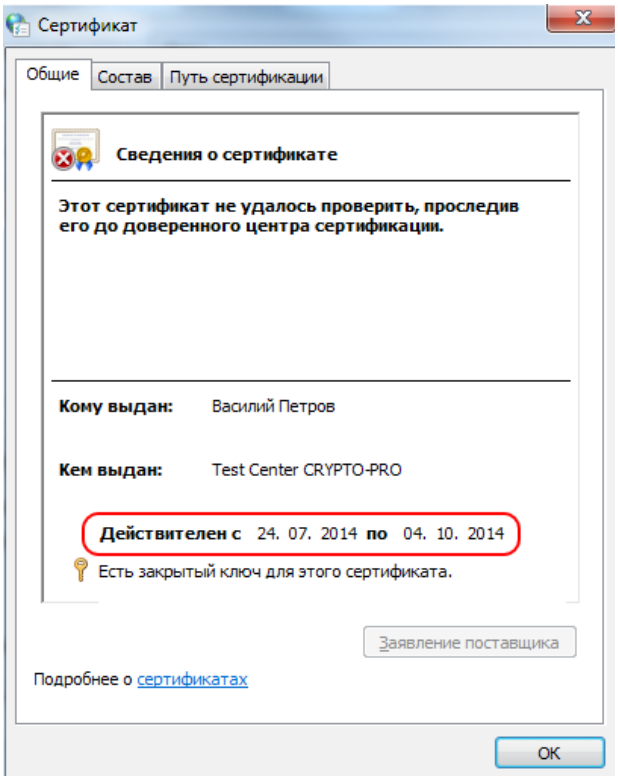

Рис. 5.9

6. Для проверки того, установлен ли корневой сертификат на рабочем месте, в окне «Сертификат» перейдите на вкладку «Путь сертификации» (Рис. 5 .10). Если в дереве сертификатов в корневом элементе, соответствующем корневому сертификату, есть данного вида пиктограмма , то корневой сертификат НЕ установлен.

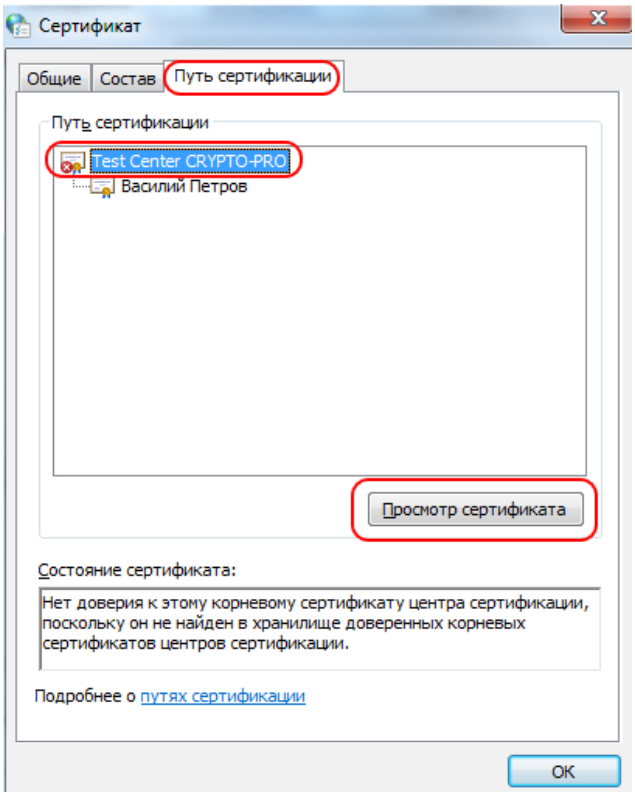

Рис. 5.10

Для установки корневого сертификата выполните следующие действия:

1. В окне «Сертификат» на вкладке «Путь сертификации» (Рис. 5 .10) в дереве сертификатов выберите корневой сертификат, после чего нажмите кнопку **«Просмотр сертификата»**.
2. В открывшемся окне «Сертификат», соответствующем корневому сертификату, перейдите на вкладку «Состав», после чего нажмите кнопку **«Копировать в файл»** (Рис. 5 .11).

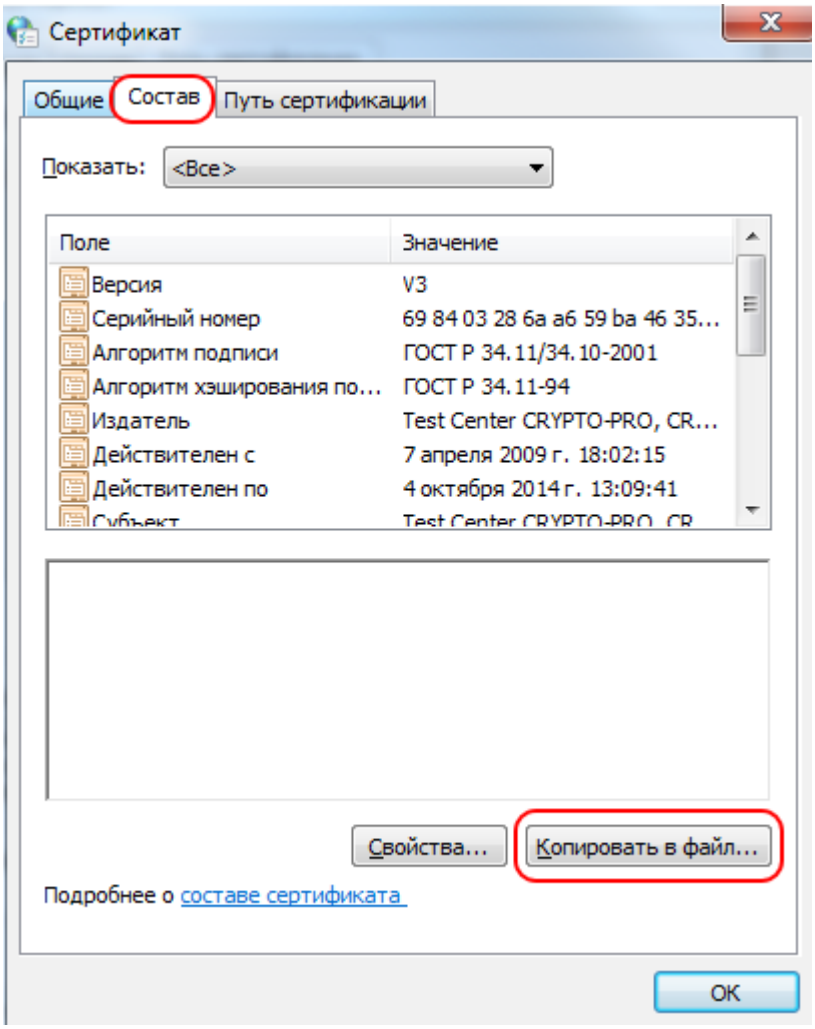

Рис. 5.11

3. Откроется мастер экспорта сертификатов. Выполните все шаги мастера, нажимая кнопку **«Далее»**, при этом на шаге «Имя экспортируемого файла» укажите путь к файлу и имя файла, в который будет экспортирован корневой сертификат. Запомните путь и имя файла, в который вы экспортируете корневой сертификат – это вам пригодится при выполнении следующих шагов.
4. После выполнения мастера экспорта сертификатов закройте окна «Сертификат», соответствующие корневому сертификату и сертификату пользователя, после чего в окне «Сертификаты» перейдите на вкладку «Доверенные корневые центры сертификации» и нажмите кнопку **«Импорт...»** (Рис. 5 .12).

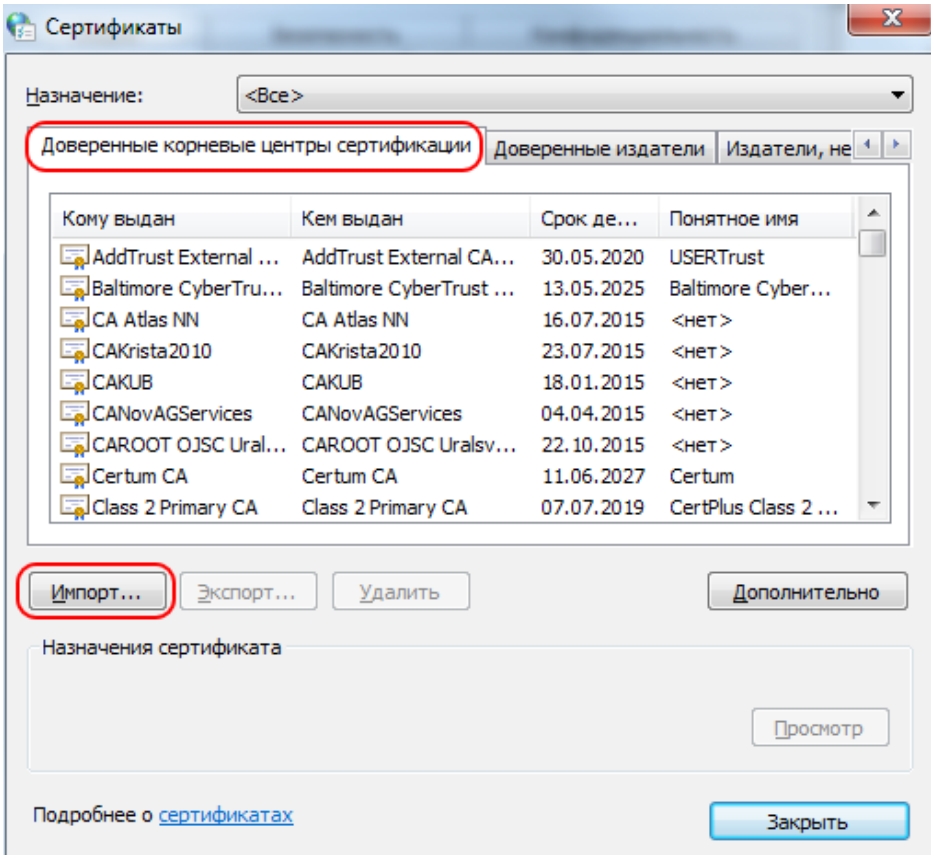

Рис. 5.12

5. Откроется мастер импорта сертификатов. Выполните все шаги мастера, нажимая кнопку **«Далее»**, при этом на шаге «Импортируемый файл» укажите путь и имя к файлу, в который вами был экспортирован корневой сертификат.
6. После выполнения мастера импорта сертификатов корневой сертификат будет установлен на рабочем месте.