|  |  |
| --- | --- |
|  |  |
|  | |
| Единая информационная система в сфере закупок | |
| Инструкция по настройке рабочего места | |
|  | |
|  | |
| Листов: | |
|  | |
|  | |

Аннотация

Настоящий документ представляет собой Инструкцию по настройке рабочего места пользователя Единой информационной системы в сфере закупок для работы в личном кабинете.

Содержание

[1 Подготовка к работе 4](#_Toc517799742)

[1.1 Подготовка к работе для всех пользователей Официального сайта ЕИС 4](#_Toc517799743)

[1.2 Подготовка к работе для пользователей, использующих ЭП в личном кабинете Официального сайта ЕИС 10](#_Toc517799744)

[1.2.1 Добавление Официального сайта ЕИС в список доверенных узлов и настройка браузера 10](#_Toc517799745)

[1.2.2 Настройка параметров безопасности 12](#_Toc517799746)

[1.2.3 Настройка всплывающих окон 15](#_Toc517799747)

[1.2.4 Переопределение автоматической обработки куки-файлов 17](#_Toc517799748)

[1.2.5 Установка параметров обозревателя по умолчанию 19](#_Toc517799749)

[1.2.6 Удаление временных файлов Интернета, истории обзора и файлов cookie 21](#_Toc517799750)

[1.2.7 Добавление узла «zakupki.gov.ru» для просмотра в режиме совместимости 23](#_Toc517799751)

[1.2.8 Установка ПО CryptoPro CSP 24](#_Toc517799752)

[1.2.9 Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP» 32](#_Toc517799753)

[1.2.10 Требования к эксплуатации ПО CryptoPro CSP 33](#_Toc517799754)

[1.2.11 Проверка совместимости версии Internet Explorer 11 с версией 10 36](#_Toc517799755)

[1.2.12 Установка и настройка компонента «КриптоПро ЭЦП Browser plug-in» 36](#_Toc517799824)

[1.2.13 Настройка считывателей в CryptoPro CSP 41](#_Toc517799826)

[1.2.14 Установка сертификата в CryptoPro CSP 47](#_Toc517799827)

[1.2.15 Перерегистрация сертификата 57](#_Toc517799828)

[Лист регистрации изменений 60](#_Toc517799829)

# Подготовка к работе

## Подготовка к работе для всех пользователей Официального сайта ЕИС

Для работы с Официальным сайтом ЕИС в информационно-телекоммуникационной сети «Интернет», обеспечивающий размещение информации в публичном доступе (далее, Официальный сайт ЕИС, Система), установочный дистрибутив не требуется. На рабочих местах пользователи используют Интернет-браузер[[1]](#footnote-1).

В Интернет-браузере должен быть включен протокол шифрования TLS 1.0. Для включения протокола выберите в меню браузера пункт «Инструменты» (Tools), подпункт «Свойства обозревателя» (Internet options) и в открывшемся окне выбрать закладку «Дополнительно» (Advanced) (). В открывшемся окне активируйте кнопку с независимой фиксацией напротив пункта «TLS 1.0» (Use TLS 1.0).

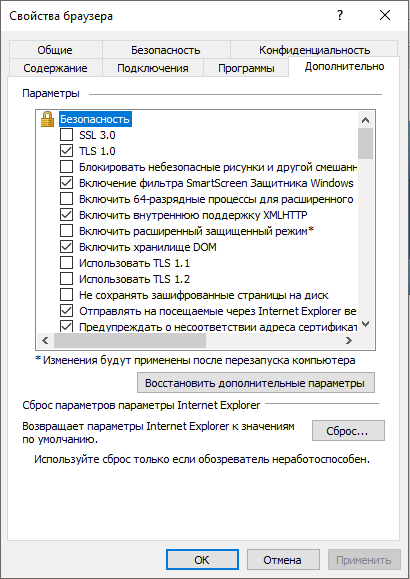


Рисунок 1 Настройка протокола шифрования TLS 1.0

Для подтверждения подлинности электронных цифровых подписей документов на Официальном сайте ЕИС следует установить сертификаты удостоверяющего центра.

Для загрузки сертификата удостоверяющего центра на главной странице Системы выберите пункт меню «Документы» в блоке «Дополнительно». На странице «Документы» выберите пункт меню «Файлы для настройки рабочего места». Отобразится страница со списком сертификатов ().

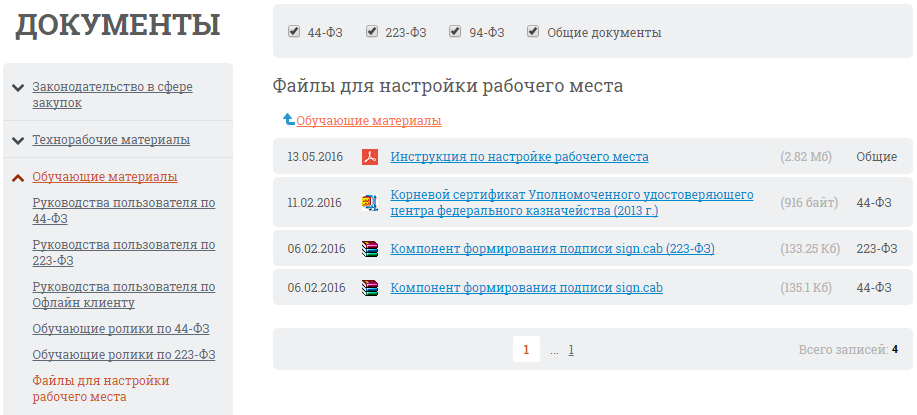


Рисунок 2 Страница со списком сертификатов

Загрузите необходимый сертификат (Корневой сертификат Уполномоченного удостоверяющего центра федерального казначейства нового формата (2013г.), нажав на его наименование.

При наличии сертификата типа PKCS #7 (данный файл выдается удостоверяющим центром) необходимо установить сертификат удостоверяющего центра, расположенный в файле с расширением \*.p7b. Для установки сертификата откройте файл \*.p7b, двойным нажатием откройте сертификат удостоверяющего центра.

Для установки промежуточного сертификата в его сведениях () нажмите на кнопку «Установить сертификат» (сертификатом является файл с расширением \*.cer).

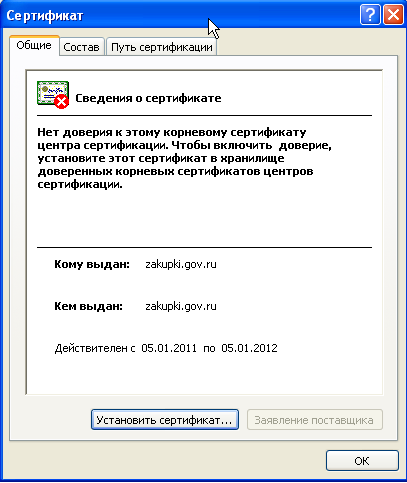


Рисунок 3 Сведения сертификата

Нажмите правой кнопкой мыши на файл сертификата, в меню выберите команду «Открыть». В открывшемся окне установки нажмите на кнопку «Установить сертификат», затем «Далее». По умолчанию выбран пункт «Автоматически выбрать хранилище на основе типа сертификата», выберите пункт «Поместить все сертификаты в следующее хранилище» ().

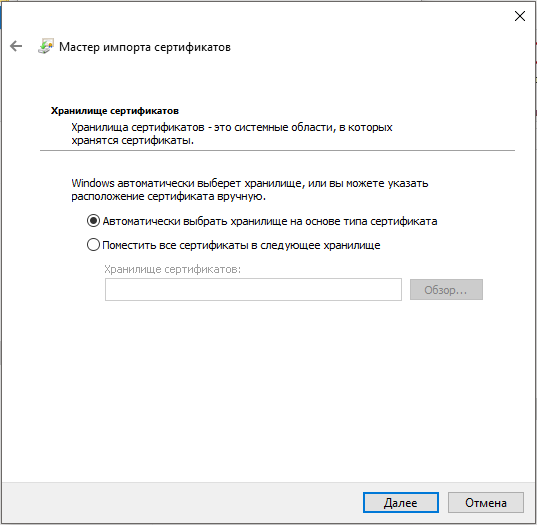


Рисунок 4 Выбор хранилища сертификата

Нажмите на кнопку «Далее» и затем кнопку «Готово» для завершения установки.

Для установки корневого сертификата в его сведениях (см. Рисунок 3) нажмите на кнопку «Установить сертификат» (сертификатом является файл с расширением \*.cer). Нажмите правой кнопкой мыши на файл сертификата, в меню выберите команду «Открыть». В открывшемся окне установки нажмите на кнопку «Установить сертификат», затем «Далее», выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите на кнопку «Обзор» (см. Рисунок 4).

В открывшемся списке хранилищ () выберите хранилище «Доверенные корневые центры сертификации» и нажмите на кнопку «ОК». В окне установки нажмите на кнопку «Далее» и затем кнопку «Готово» для завершения установки.

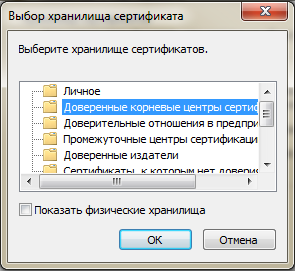


Рисунок 5 Список хранилищ

Для корректного отображения печатных форм (при выводе их на печать) необходимо убрать отображение информации в колонтитулах. Для этого выберите в меню браузера пункт «Печать», подпункт «Параметры страницы» и для всех параметров колонтитулов установите значение «-Пусто-» ().

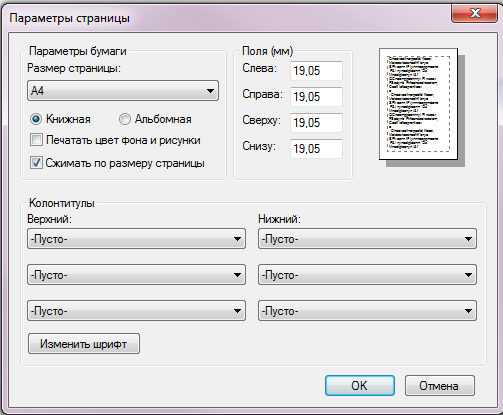


Рисунок 6 Настройка параметров страницы для печати

Для того, чтобы запустить стартовую страницу Официального сайта ЕИС, откройте Интернет-браузер и в адресной строке введите Интернет-адрес Системы.

## Подготовка к работе для пользователей, использующих ЭП в личном кабинете Официального сайта ЕИС

Пользователям, использующим ЭП для подписи документов в личном кабинете Официального сайта ЕИС, помимо настроек, указанных в разделе , требуется также выполнить дополнительные настройки, указанные в данном разделе.

Для работы с электронной цифровой подписью пользователям Личного кабинета требуется выполнить следующие действия:

* добавить адрес Официального сайта ЕИС в список доверенных узлов и настройка браузера;
* установить ПО CryptoPro CSP;
* установить компонент «КриптоПро ЭЦП Browser plug-in»;
* настроить считыватели в CryptoPro CSP;
* установить сертификат в CryptoPro CSP.

### Добавление Официального сайта ЕИС в список доверенных узлов и настройка браузера

Для добавления Официального сайта ЕИС в список доверенных узлов в Интернет-браузере выберите в меню браузера пункт «Инструменты» (Tools), подпункт «Свойства браузера» (Internet Options) и в открывшемся окне выберите вкладку «Безопасность» (Security). На экране отобразится окно настройки безопасности ().

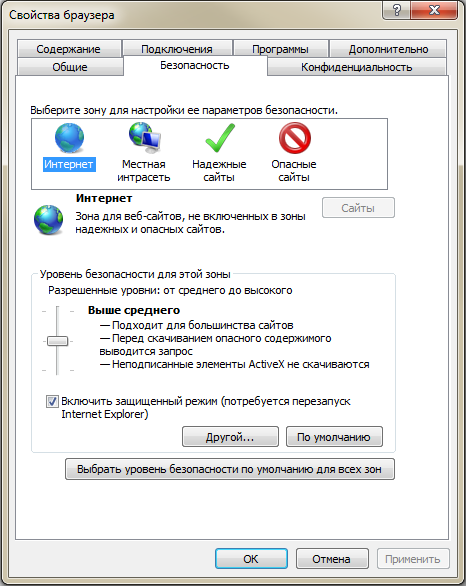


Рисунок 7 Настройка безопасности браузера

Выберите зону «Надежные сайты» (Trusted sites) и нажмите на кнопку «Сайты» (Sites). В открывшемся списке () введите адрес Официального сайта ЕИС в текстовое поле и нажмите на кнопку «Добавить» (Add). Закройте список и окно «Свойства браузера» (Internet Options).

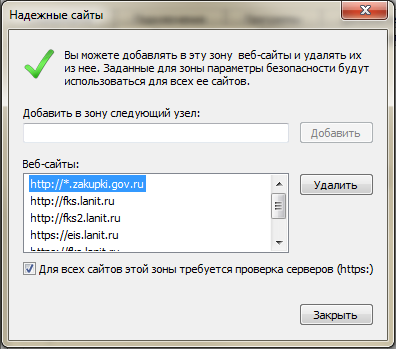


Рисунок 8 Список надежных узлов браузера

### Настройка параметров безопасности

После добавления Официального сайта ЕИС в список надежных узлов откройте закладку «Безопасность» (Security), выберите зону «Надежные сайты» (Trusted sites) и нажмите на кнопку «Другой» (Custom level). В открывшемся окне в блоке «Разное» (Miscellaneous) установите следующие значения ():

* «Доступ к источникам данных за пределами домена» (Access data sources across domains) – «Включить» (Enable);
* «Блокировать всплывающие окна» (Use Pop-up blocker) – «Отключить» (Disable).

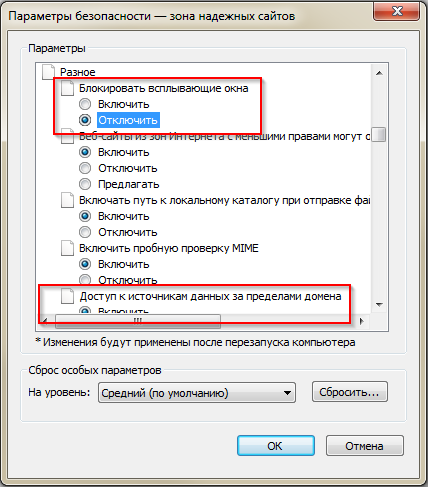


Рисунок 9 Настройка доступа, блок «Разное» (Miscellaneous)

Установите следующие значения для строк в блоке «Сценарии» (Scripting) (Рисунок 10):

* для строки «Активные сценарии» (Active scripting) – «Включить» (Enable);
* для строки «Включить фильтр XSS» (Enable XSS filter) – «Отключить» (Disable);
* для строки «Выполнять сценарии приложений Java» (Scripting of Java applets) – «Включить» (Disable).

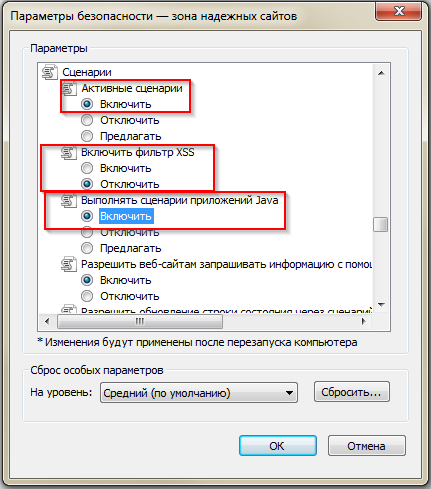


Рисунок 10 Настройка доступа, блок «Сценарии» (Scripting)

Для всех строк в блоке «Элементы ActiveX и модули подключения» (ActiveX controls and plug-ins) установите значения «Включить» (Enable) (Рисунок 11).

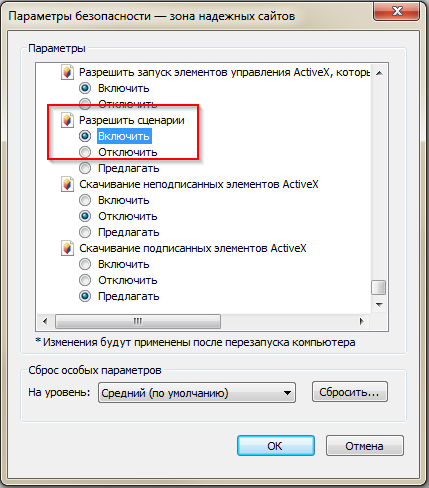


Рисунок 11 Настройка доступа, блок «Элементы ActiveX и модули подключения» (ActiveX controls and plug-ins)

Нажмите на кнопку «ОК».

### Настройка всплывающих окон

Для корректной работы Системы необходимо настроить отображение всплывающих окон браузера Internet Explorer.

В окне свойств браузера Internet Explorer перейдите на вкладку «Privacy» («Конфиденциальность») (). Снимите флажок выключателя «Turn on pop-up blocker» («Блокировать всплывающие окна») в блоке «Pop-up blocker» («Блокирование всплывающих окон»).

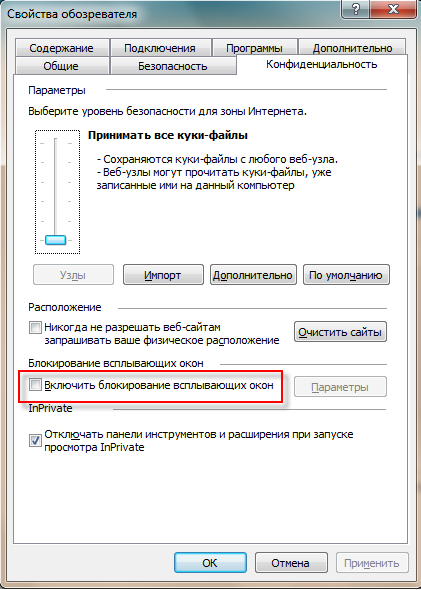


Рисунок 12 Вкладка «Конфиденциальность»

Либо добавьте адрес Официального сайта ЕИС в список исключений в настойках блокировки всплывающих окон. Для этого при установленном флажке выключателя «Turn on pop-up blocker» («Блокировать всплывающие окна») в блоке «Pop-up blocker» («Блокирование всплывающих окон») нажмите на кнопку «Settings» («Параметры»), введите адрес Официального сайта ЕИС в поле «Address of web-site to allow» («Надежные узлы») и нажмите на кнопку «Add» («Добавить») ().

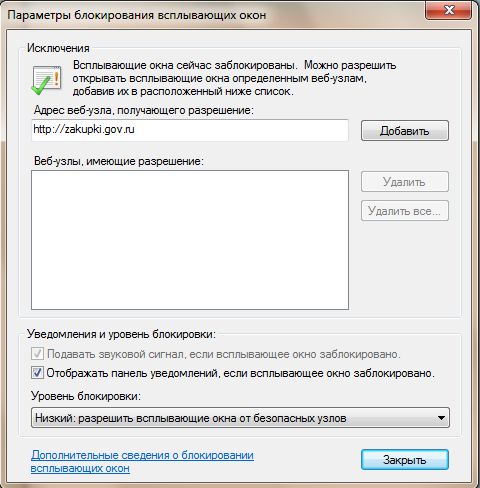


Рисунок 13 Настройка блокировки всплывающих окон

Добавленный адрес отобразится в поле «Allowed sites» («Надежные узлы»).

Либо установите уровень блокировки всплывающих окон – «Low» («низкий»), для этого следует в выпадающем списке «Blocking level» («Уровень блокировки») нажать на пункт «Low» («низкий»).

По завершению настройки блокировки всплывающих окон нажмите на кнопку «Close» («Закрыть»).

### Переопределение автоматической обработки куки-файлов

Для включения функции переопределения автоматической обработки куки-файлов в свойствах обозревателя перейдите на вкладку «Конфиденциальность» (Privacy) и нажмите на кнопку «Дополнительно» (Advansed) ().

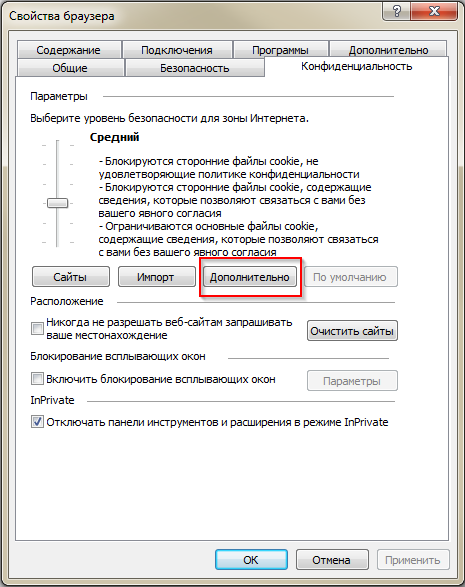


Рисунок 14 Кнопка «Дополнительно» вкладки «Конфиденциальность»

В отобразившемся окне установите флажок в поле «Переопределить автоматическую обработку файлов cookie» (Override automatic cookie handling) ().

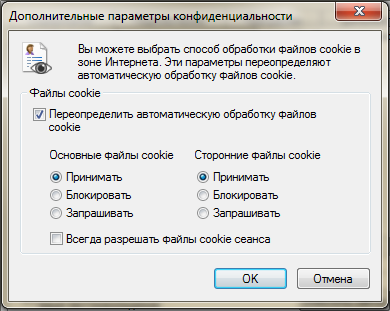


Рисунок 15 Окно «Дополнительные параметры конфиденциальности» (Advanced Privacy Settings) в русской и английской версиях браузера

Нажмите на кнопку «ОК».

### Установка параметров обозревателя по умолчанию

Для установки параметров обозревателя по умолчанию прейдите на вкладку «Дополнительно» (Advanced) и нажмите на кнопку «Сброс» (Reset) ().

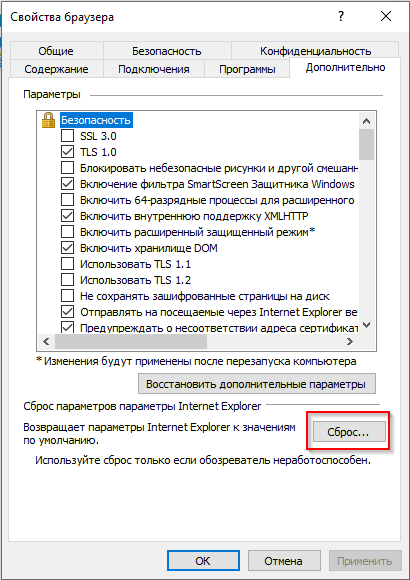


Рисунок 16 Установка параметров обозревателя по умолчанию

В случае использования версии КриптоПро CSP 4.0.9842 рекомендуется отключить использование:

* TLS 1.1 и TLS 1.2 при версии ОС Windows 7,
* TLS 1.2 для версии ОС Windows 8.1;
* TLS 1.2 для версии ОС Windows 10.

Для удаления личных настроек установите флажок в поле «Удалить личные настройки» (Delete personal settings) и нажмите на кнопку «Сброс» (Reset) ().

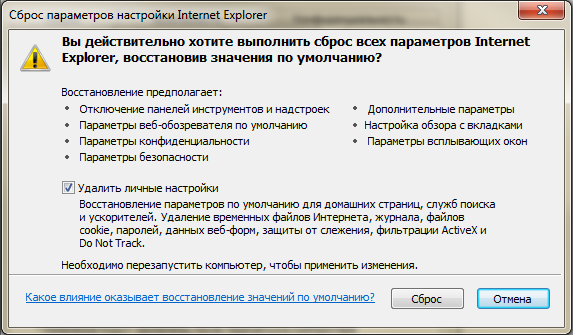


Рисунок 17 Окно сброса параметров настройки Internet Explorer

### Удаление временных файлов Интернета, истории обзора и файлов cookie

Для удаления временных файлов Интернета, истории обзора и файлов cookie перейдите на вкладку «Общие» (General) и нажмите на кнопку «Удалить» (Delete) ().

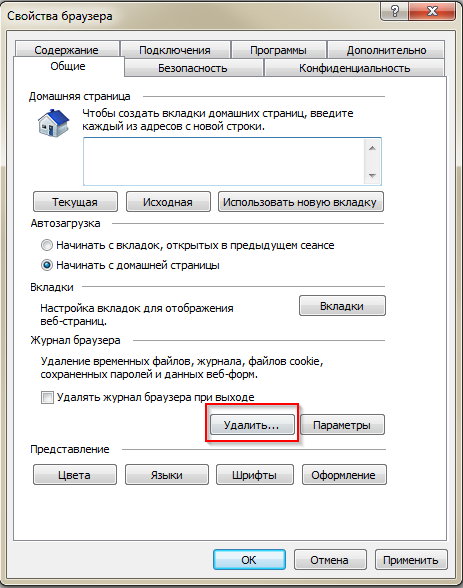


Рисунок 18 Кнопка «Удалить» вкладки «Общие»

Установите необходимые флажки и нажмите на кнопку «Удалить» (Delete) ().

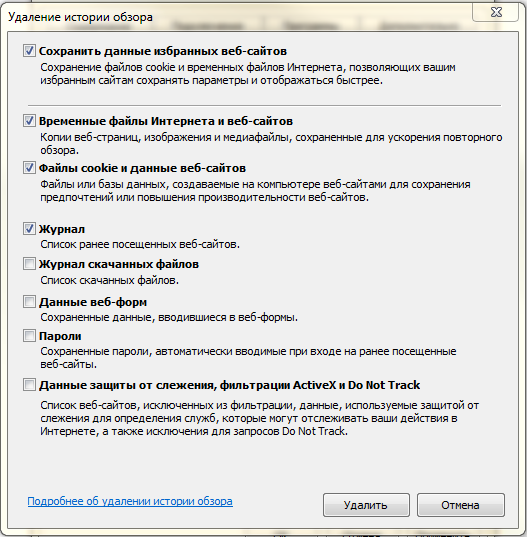


Рисунок 19 Окно сброса параметров настройки Internet Explorer

### Добавление узла «zakupki.gov.ru» для просмотра в режиме совместимости

Для предотвращения возникновения проблем совместимости Официального сайта ЕИС с Internet Explorer необходимо добавить Официальный сайт ЕИС в список просмотра в режиме совместимости.

Для добавления узла «zakupki.gov.ru» в список просмотра в режиме совместимости нажмите на пункт «Параметры режима представления совместимости» (Compatibility View settings) для браузера Internet Explorer версии 8 и 9 или «Параметры просмотра в режиме совместимости» (Compatibility View settings) (IE версии 10 и выше).

В отобразившемся окне нажмите на кнопку «Добавить» (Add) ().

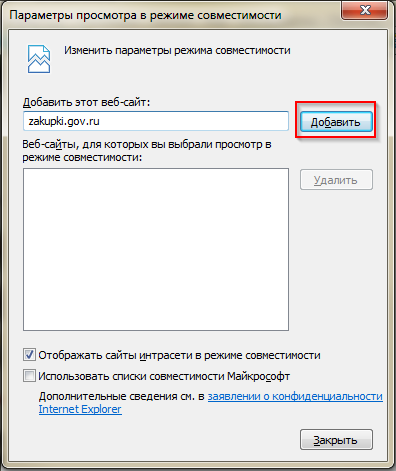


Рисунок 20 Окно параметров режима представления совместимости

После добавления узла «zakupki.gov.ru» в список просмотра в режиме совместимости нажмите на кнопку «Закрыть» (Close).

### Установка ПО CryptoPro CSP

Криптопровайдер CryptoPro CSP предназначен для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭП).

Рекомендуемая версия КриптоПро CSP – 4.0.9842 и выше.

Ниже представлен процесс установки CryptoPro CSP 4.0.9842 (информация по установке и настройке CryptoPro CSP других версий приводится в сопроводительной документации для данного ПО – см. сайт производителя[[2]](#footnote-2)).

Перед запуском мастера установки выводится диалоговое окно, в котором доступен выбор уровня защищенности ().

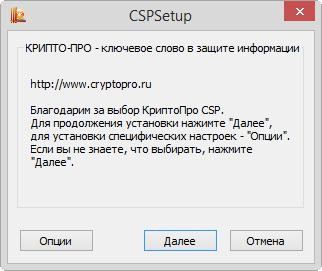


Рисунок 21 Начало установки

Для выбора уровня защищенности необходимо нажать на кнопку «Опции». В СКЗИ КриптоПро реализованы классы защиты КС1, КС2, КС3 согласно требованиям ФСБ России. Для корректной работы необходимы выбрать класс защиты КС2 ():

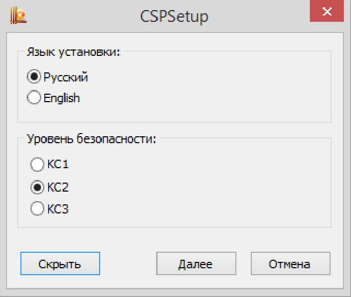


Рисунок 22 Выбор уровня безопасности

Укажите требуемый уровень безопасности, если он отличается от значения по умолчанию. После этого можно переходить к работе с мастером установки ():

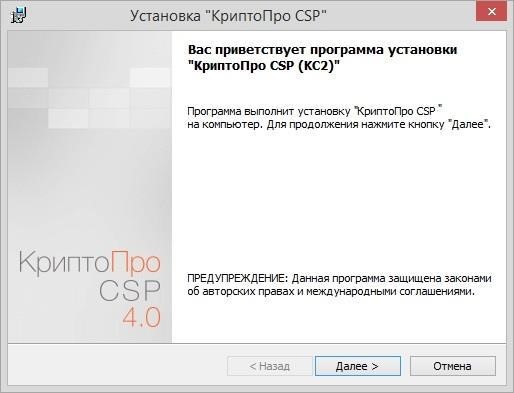


Рисунок 23 Приветственное окно мастера установки

Если на компьютере была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне появится информация об обновляемой версии ():

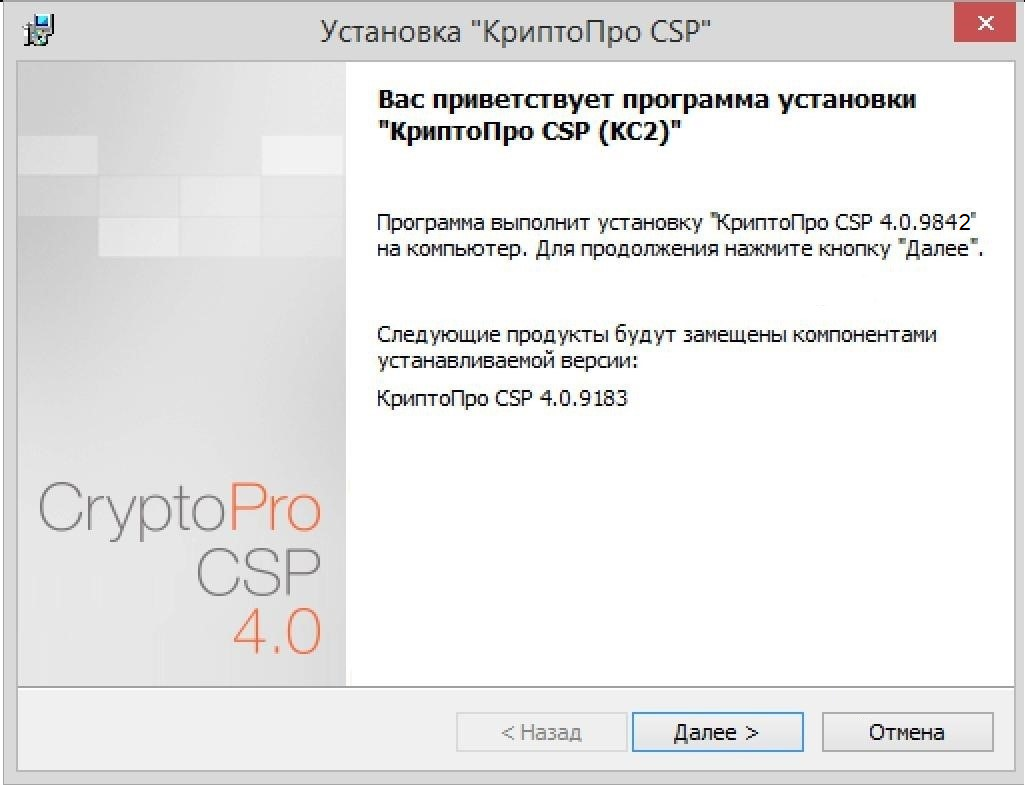


Рисунок 24 Установка с замещением компонентов

Для продолжения установки КриптоПро CSP нажмите на кнопку «Далее».

Внимательно прочитайте лицензионное соглашение, которое выводится при первой установке. Дальнейшая установка производится в соответствии с сообщениями, выдаваемыми мастером.

В процессе установки может быть предложено:

* ввести серийный номер лицензии криптопровайдера;
* зарегистрировать дополнительные считыватели ключевой информации;
* настроить дополнительные датчики случайных чисел.

Эти параметры можно изменить после завершения установки через панель свойств КриптоПро CSP.

Для корректной работы КриптоПро CSP после завершения установки необходимо перезагрузить компьютер в случае, если пользователю предлагается перезагрузка.

В процессе установки мастером может быть предложен выбор наиболее подходящего вида установки ().

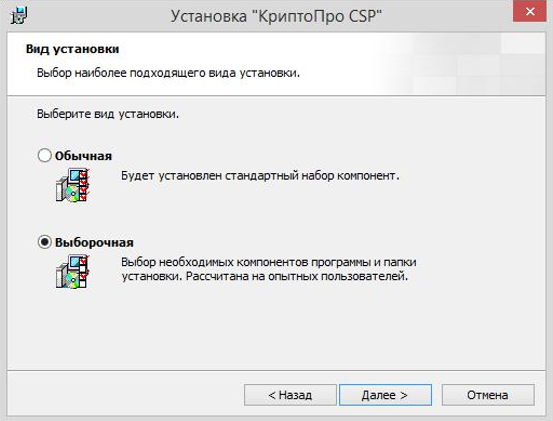


Рисунок 25 Выбор вида установки

По умолчанию (вид установки «Обычная») устанавливаются только основные файлы для работы СКЗИ (для Windows Server 2008 по умолчанию также устанавливается «Драйверная библиотека CSP»). При необходимости можно изменить набор компонентов для установки ():

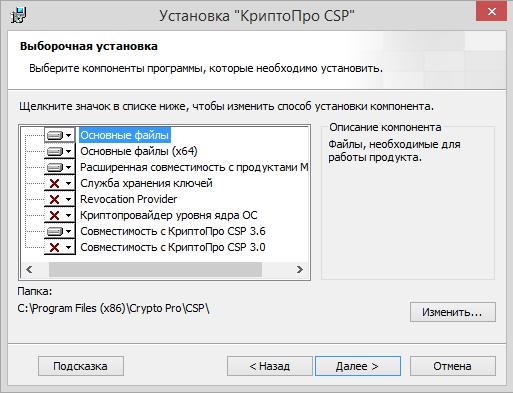


Рисунок 26 Выборочная установка

* **Расширенная совместимость с продуктами Microsoft** – Обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express. Необходима для входа в систему по смарт -картам.
* **Служба хранения ключей** – Обеспечивает хранение, использование и кэширование ключей в отдельном сервисе ОС. По умолчанию включена для уровня безопасности КС2 и КС3 (подробно описана в разделе Установка параметров безопасности).
* **Revocation Provider** – Механизм проверки текущего статуса сертификата с использованием OCSP. Является дополнением к стандартному механизму Windows проверки статуса сертификата на основе списка отозванных сертификатов (СОС, CRL). Кроме этого предоставляет возможность использования СОС, выпущенных по правилам, описанным в RFC 3280.
* **Криптопровайдер уровня ядра ОС** – Необходим для работы криптопровайдера в службах и ядре Windows (TLS-сервер, EFS, IPsec).
* **Совместимость с КриптоПро CSP 3.6** – Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.6. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.6.
* **Совместимость с КриптоПро CSP 3.0** – Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.0. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.0.

После нажатия на кнопку «Далее» мастером установки предлагается запланировать или отменить установку библиотек поддержки считывателей, а также принять решение о включении функционала накопления информации об использованных съёмных ключевых носителях. Помимо этого, также необходимо включить режим усиленного контроля использования ключей (). Данный режим осуществляет контроль срока действия долговременных ключей электронной подписи и ключевого обмена, контроль доверенности ключей проверки электронной подписи и контроль корректного использования программного датчика случайных чисел. Использование СКЗИ КриптоПро CSP 4.0.9842 без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

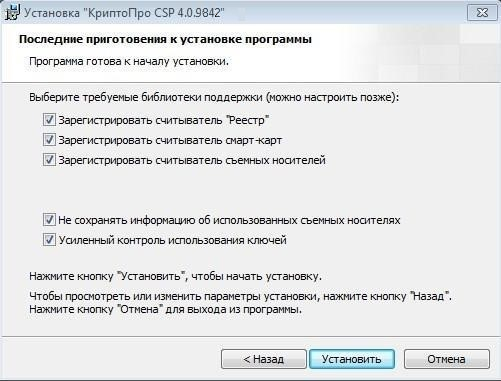


Рисунок 27 Установка усиленного контроля использования ключей

При установке СКЗИ с включением режима усиленного контроля использования ключей будут запрошены данные с датчика случайных чисел. В случае ошибки получения данных будет отображено окно, пример которого приведен на :

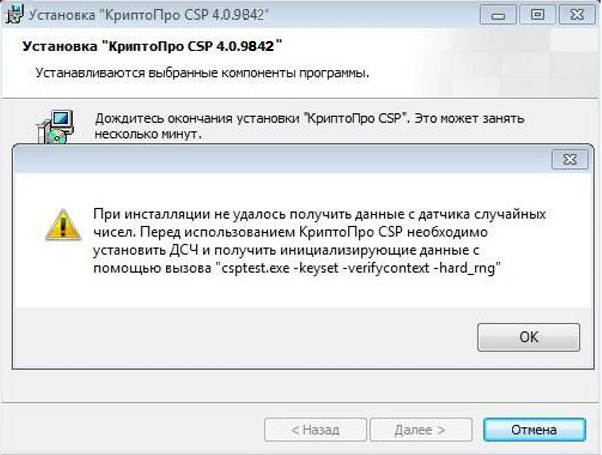


Рисунок 28 Окно ошибки получения данных с датчика случайных чисел при инсталляции СКЗИ

В этом случае при начале работы пользователя в системе с установленным СКЗИ КриптоПро CSP 4.0.9842 необходимо проверить, что зарегистрирован хотя бы один физический датчик случайных чисел (например, внешняя гамма или аппаратный ДСЧ), и выполнить команду:

csptest.exe -keyset -verifycontext -hard\_rng.

После завершения установки СКЗИ с включённым режимом усиленного контроля использования ключей необходимо в обязательном порядке установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера CryptoProTrustedStore («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки Сертификаты либо с помощью утилиты certmgr.exe:

certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer.

После этого следует осуществить перезагрузку компьютера.

### Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP»

При установке программного обеспечения КриптоПро CSP пользователю предлагается ввести данные лицензии. Без ввода лицензии пользователю предоставляется ознакомительная лицензия с ограниченным сроком действия, для использования КриптоПро CSP после окончания этого срока нужно ввести серийный номер с бланка Лицензии, полученной у организации -разработчика или организации, имеющей права распространения продукта. Если КриптоПро CSP используется на клиентской машине, то требуется лицензия клиентского типа, если на сервере, то серверная лицензия.

Для ввода лицензии после установки КриптоПро CSP воспользуйтесь кнопкой Ввод лицензии на вкладке Общие панели управления КриптоПро CSP. Откроется окно «Сведения о пользователе» (см. ).

Также можно ввести лицензию с помощью утилиты Управление лицензиями КриптоПро PKI. Для этого выполните: «Пуск» > «Программы» > «КриптоПро» > «Управление лицензиями КриптоПро PKI». В блоке «Управление лицензиями КриптоПро PKI» выберите продукт, лицензию на который Вы хотите ввести. В контекстном меню выберите «Все задачи» и далее «Ввести серийный номер» ():

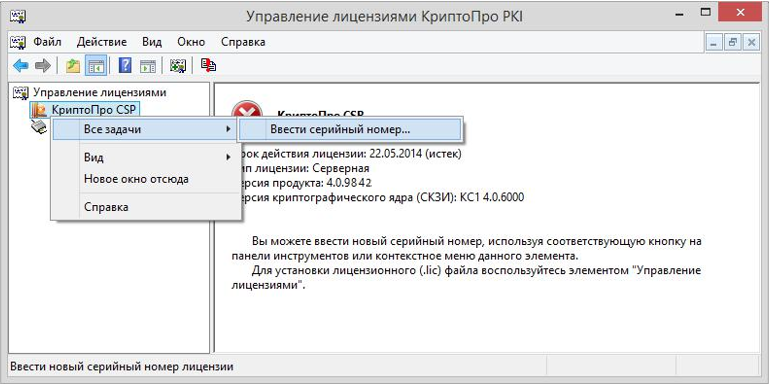


Рисунок 29 Ввод серийного номера

Откроется окно «Сведения о пользователе», в котором необходимо указать сведения о пользователе, организации, а также ввести серийный номер с бланка Лицензии в соответствующие поля ввода ():

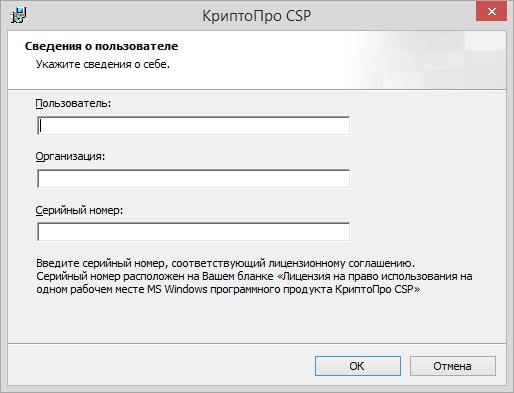


Рисунок 30 Ввод данных лицензии

После ввода и нажатия клавиши ОК данные о лицензии сохранятся или обновятся.

### Требования к эксплуатации ПО CryptoPro CSP

СКЗИ «КриптоПро CSP» версии 4.0 предназначено для защиты открытой информации в информационных системах общего пользования (вычисление и проверка ЭП) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах (шифрование и расшифрование информации, вычисление и проверка имитовставки, вычисление значения хэш-функции, вычисление и проверка ЭП).

При эксплуатации СКЗИ «КриптоПро CSP» версия 4.0 должны выполняться следующие требования:

* Средствами СКЗИ не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.
* Допускается использование СКЗИ для криптографической защиты персональных данных.
* Ключевая информация является конфиденциальной.
* Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП.
* Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является конфиденциальной.
* СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. В случае их отсутствия рекомендуется по возможности использовать существующие антивирусные средства защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.
* Размещение СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется установленным порядком.
* ПЭВМ, на которых используется СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ.
* Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.
* Встраивание СКЗИ в другие средства возможно только с использованием функций, указанных в Приложении 2. В случае использования прочих вызовов функций программных интерфейсов (уровней встраивания) СКЗИ необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).
* При эксплуатации СКЗИ должны использоваться только сертификаты открытых ключей, выпущенные доверенным органом сертификации. В качестве такого органа должен выступать сертифицированный ФСБ России Удостоверяющий центр (УЦ), выпускающий сертификаты и поддерживающий списки отозванных сертификатов в соответствии с Регламентом УЦ, а также служба корпоративной системы, обеспечивающая доверенные справочники сертификатов открытых ключей с поддержкой актуальности включаемых в справочники сертификатов.

Порядок организации и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации сведений, составляющих конфиденциальную информацию, осуществляется в соответствии с документами «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Приказ ФАПСИ № 152 от 13 июня 2001 года), «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Приказ ФСБ России № 66 от 9 февраля 2005 года) и другими руководящими документами по обеспечению безопасности информации.

СКЗИ «КриптоПро CSP» версии 4.0 можно эксплуатировать со следующими программными продуктами без проведения дополнительных тематических исследований и/или оценки влияния:

* приложения, входящие в состав ОС;
* MS Outlook (Office 2003, Office 2007, Office 2010, Office 2013);
* сервер IIS;

Следующие программные компоненты СКЗИ «КриптоПро CSP» версии 4.0 можно использовать без проведения дополнительных тематических исследований:

* приложение командной строки для подписи и шифрования файлов cryptcp;
* приложение командной строки для работы с сертификатами certmgr;
* приложение для создания TLS-туннеля stunnel.

Использование СКЗИ «КриптоПро CSP» версии 4.0 с выключенным режимом усиленного контроля использования ключей не допускается.

### Проверка совместимости версии Internet Explorer 11 с версией 10

Для корректной работы пользователю необходимо использовать режим совместимости с версией Internet Explorer 10. Для этого в меню браузера выберите пункт «Средства разработчика F12» ().

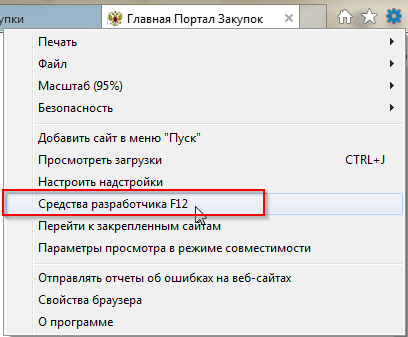


Рисунок 31 Пункт меню браузера «Средства разработчика F12»

На вкладке «Эмуляция» в поле «Режим документов» из выпадающего списка выберите пункт «10» ().

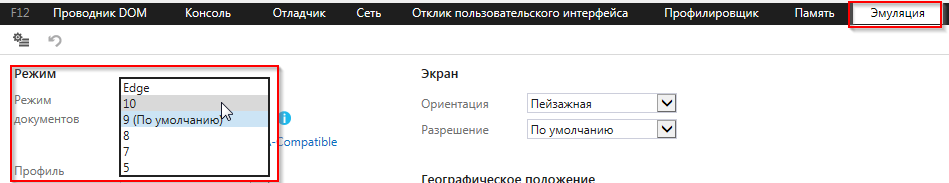


Рисунок 32 Вкладка «Эмуляция», выпадающий список поля «Режим документов»

### Установка и настройка компонента «КриптоПро ЭЦП Browser plug-in»

Компонент «КриптоПро ЭЦП Browser plug-in» предназначен для создания и проверки электронной подписи документов и информации с использованием СКЗИ «КриптоПро CSP» при работе пользователей ЕИС.

Для установки плагина «КриптоПро ЭЦП Browser plug-in» сохраните на рабочее место пользователя дистрибутив плагина, ссылка на скачивание которого доступна на странице по адресу: <https://www.cryptopro.ru/products/cades/plugin/> ().

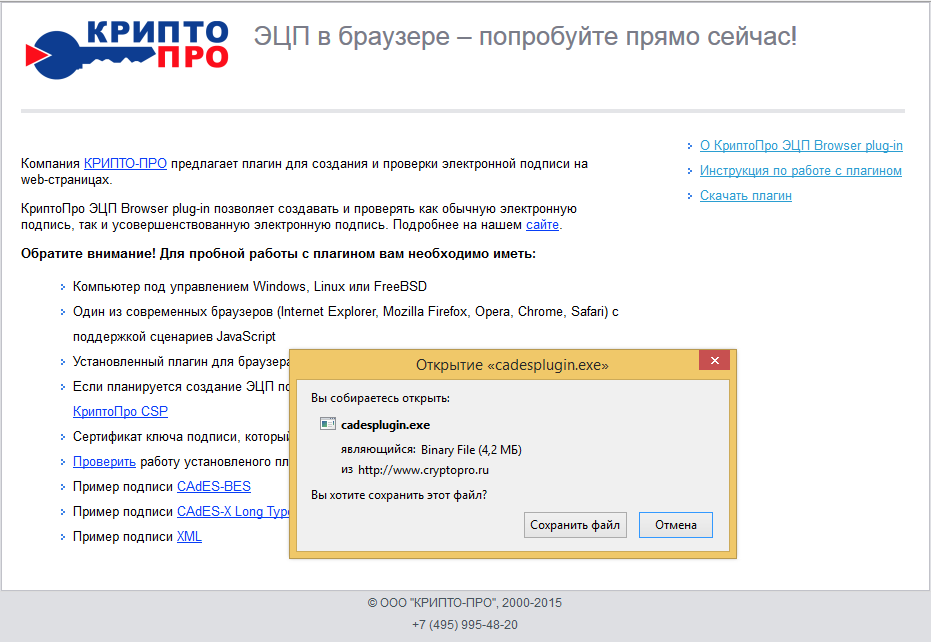


Рисунок Сохранение дистрибутива «КриптоПро ЭЦП Browser plug-in»

Запустите от имени администратора исполняемый файл «CadesPlugIn.exe». Для этого нажмите правой кнопкой мышки на иконку исполняемого файла «CadesPlugIn.exe» и в контекстном меню выберите пункт «Запуск от имени администратора».

Далее в открывшемся окне для продолжения процесса установки укажите необходимые данные и нажмите на кнопку «Да», для отмены действия – «Нет» ().

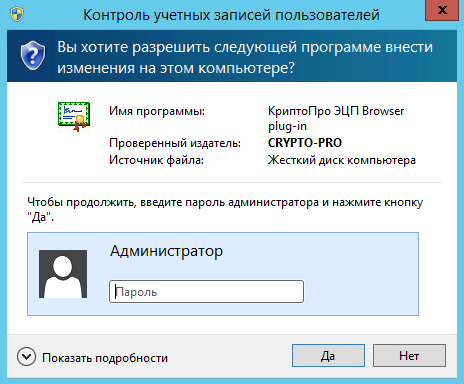


Рисунок Установка плагина «КриптоПро ЭЦП Browser plug-in». Шаг 1

Далее в открывшемся окне для продолжения процесса установки нажмите на кнопку «Да», для отмены действия – «Нет» ().

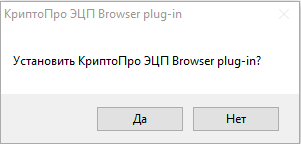


Рисунок Установка плагина «КриптоПро ЭЦП Browser plug-in». Шаг 2

После успешной установки плагина «КриптоПро ЭЦП Browser plug-in» отобразится окно с соответствующим уведомлением. Для закрытия окна нажмите кнопку «Ок» ().

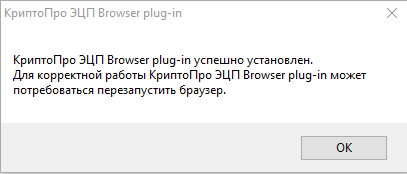


Рисунок Установка плагина «КриптоПро ЭЦП Browser plug-in». Шаг 3

После успешной установки плагина «КриптоПро ЭЦП Browser plug-in» он автоматически устанавливается в Интернет-браузеры.

Процесс проверки работы плагина подробно описан в документе «Инструкция по установке и настройке компонента «КриптоПро ЭЦП Browser plug-in», который размещен на Официальном сайте ЕИС в разделе «Документы»/«Обучающие материалы»/«Файлы для настройки рабочего места».

Для корректной работы пользователя в ЕИС в Интернет-браузере «Internet Explorer» с использованием плагина «КриптоПро ЭЦП Browser plug-in» необходимо:

* Добавить адрес Официального сайта ЕИС в список исключений и надежные узлы в настойках браузера.
* Попробовать работу в режиме совместимости (для «Internet Explorer» 10 версии и выше).

Для всех браузеров необходимо добавить адрес Официального сайта ЕИС в список надёжных узлов плагина «КриптоПро ЭЦП Browser plug-in».

Чтобы проверить, что Официальный сайт ЕИС добавлен в список надежных узлов плагина, или добавить его в надежные узлы, откройте ярлык «Настройки КриптоПро ЭЦП Browser plug-in» с помощью необходимого Интернет-браузера.

Для этого нажмите правой кнопкой мышки ярлык «Настройки КриптоПро ЭЦП Browser plug-in» и в контекстном меню выберите пункт «Открыть с помощью», далее выберите наименование необходимого браузера ().

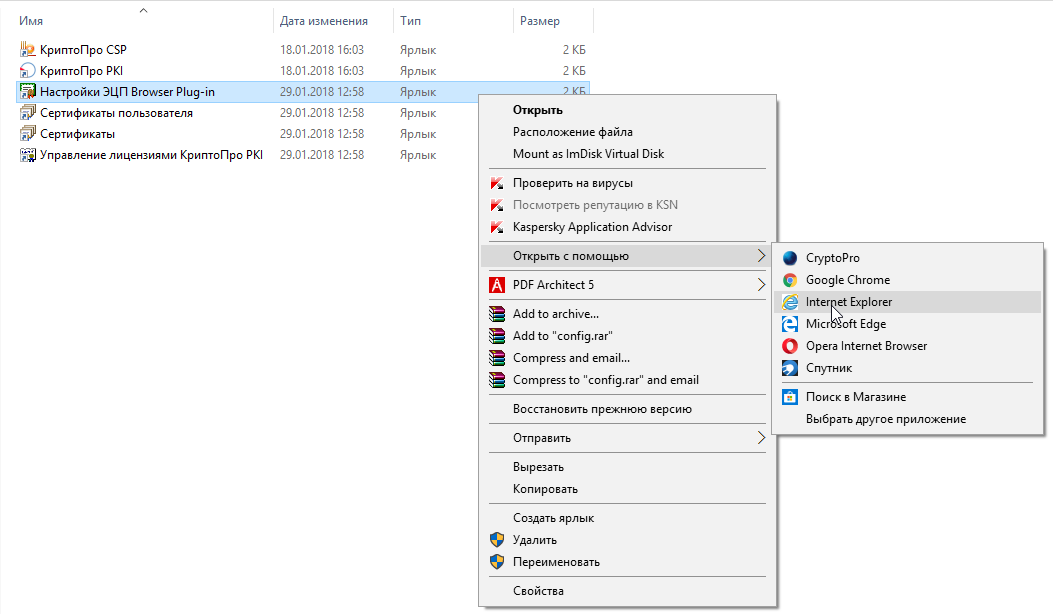


Рисунок Выбор Интернет-браузера в пункте контекстного меню «Открыть с помощью»

В открывшемся окне Интернет-браузера отобразится страница «Настройки КриптоПро ЭЦП Browser Plug-in» ().

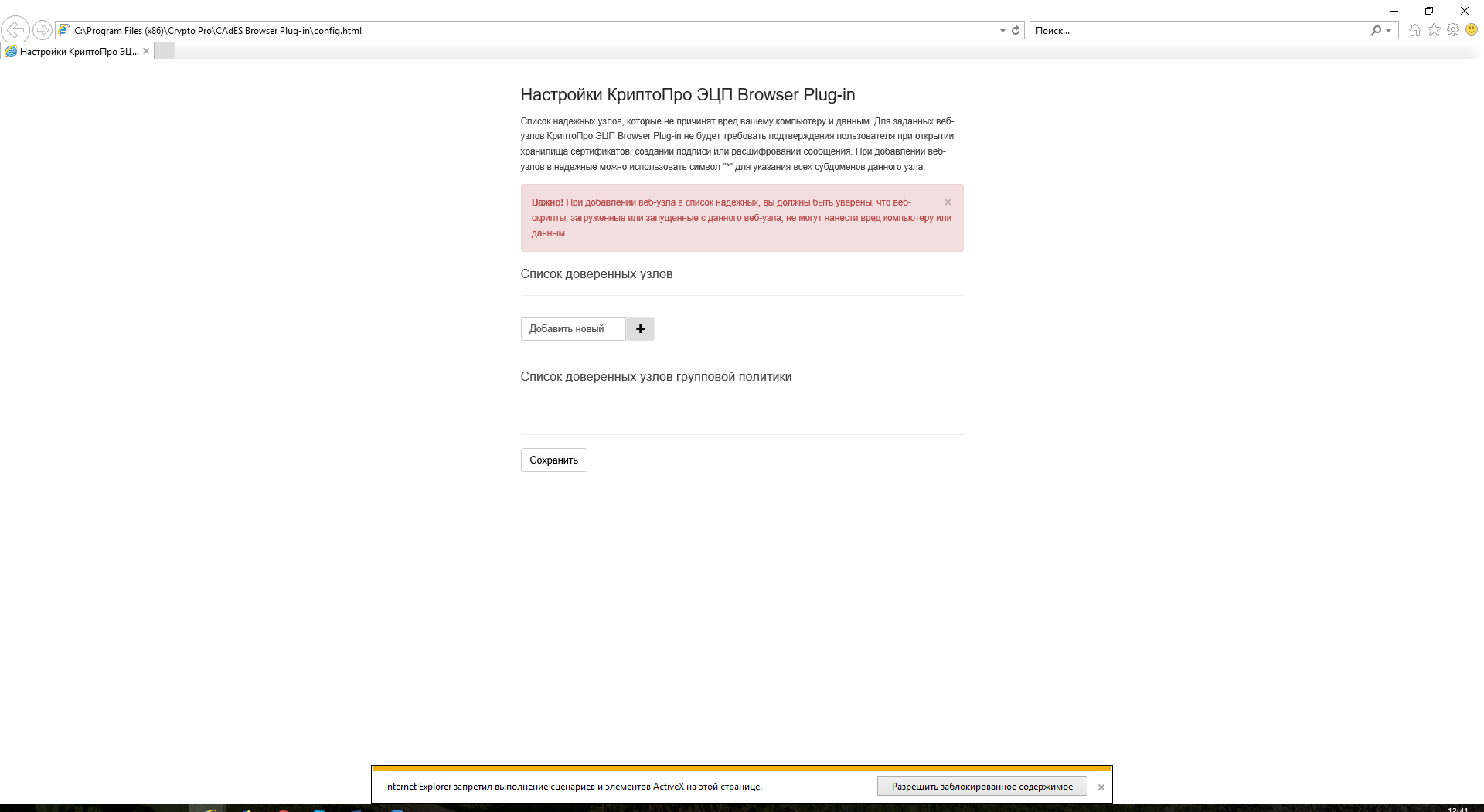


Рисунок Страница настройки плагина «КриптоПро ЭЦП Browser Plug-in»

В Интернет-браузере «Internet Explorer» в сплывающем окне разрешите выполнение сценариев и элементов ActiveX, нажав на кнопку «Разрешите заблокированное содержимое» (см. ).

На странице настройки плагина в блоке «Список доверенных узлов» укажите в поле для ввода значений адрес Официального сайта ЕИС «<http://zakupki.gov.ru>» и нажмите на пиктограмму «».

Для сохранения добавленных узлов нажмите на кнопку «Сохранить» ().

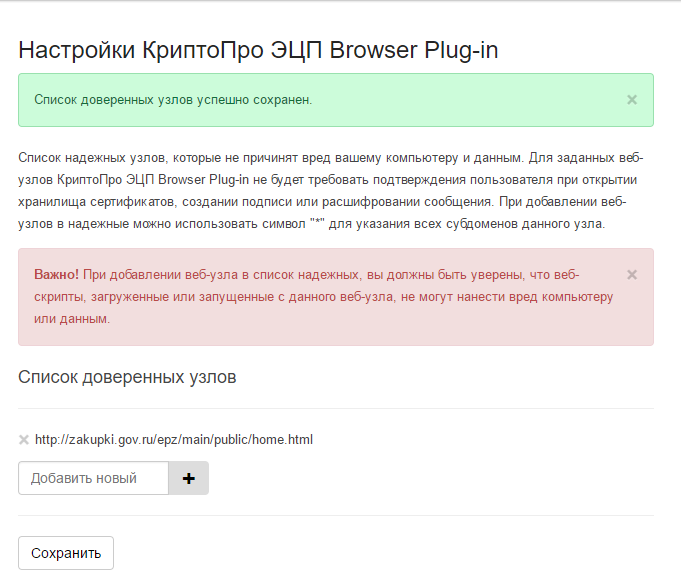


Рисунок Страница настройки плагина «КриптоПро ЭЦП Browser Plug-in» с добавленным адресом Официального сайта ЕИС в список доверенных узлов

### Настройка считывателей в CryptoPro CSP

Запустите программу из меню пуски или /Program Files/Crypto Pro/CSP/cpconfig.cpl ().

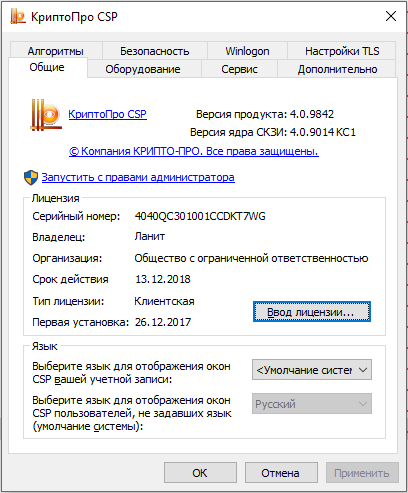


Рисунок 40 Запуск программы cpconfig.cpl

Перейдите на вкладку «Оборудование» и нажмите на кнопку «Настроить считыватели» ().

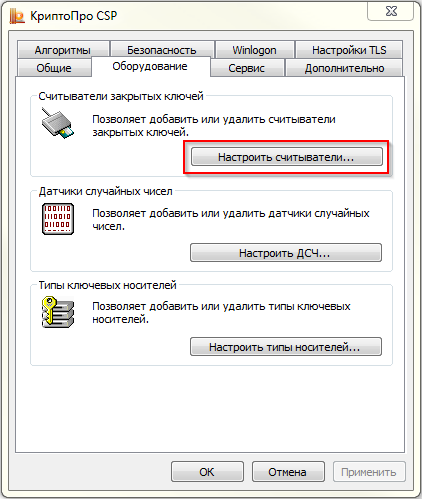


Рисунок 41 Оборудование

Вставьте физический Flash-накопитель в USB-порт. Нажмите на кнопку «Добавить» ().

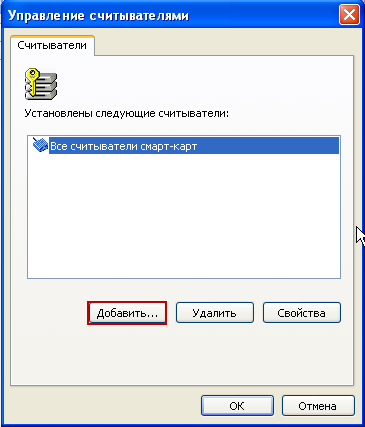


Рисунок 42 Добавление считывателя

В открывшемся окне нажмите на кнопку «Далее» ().

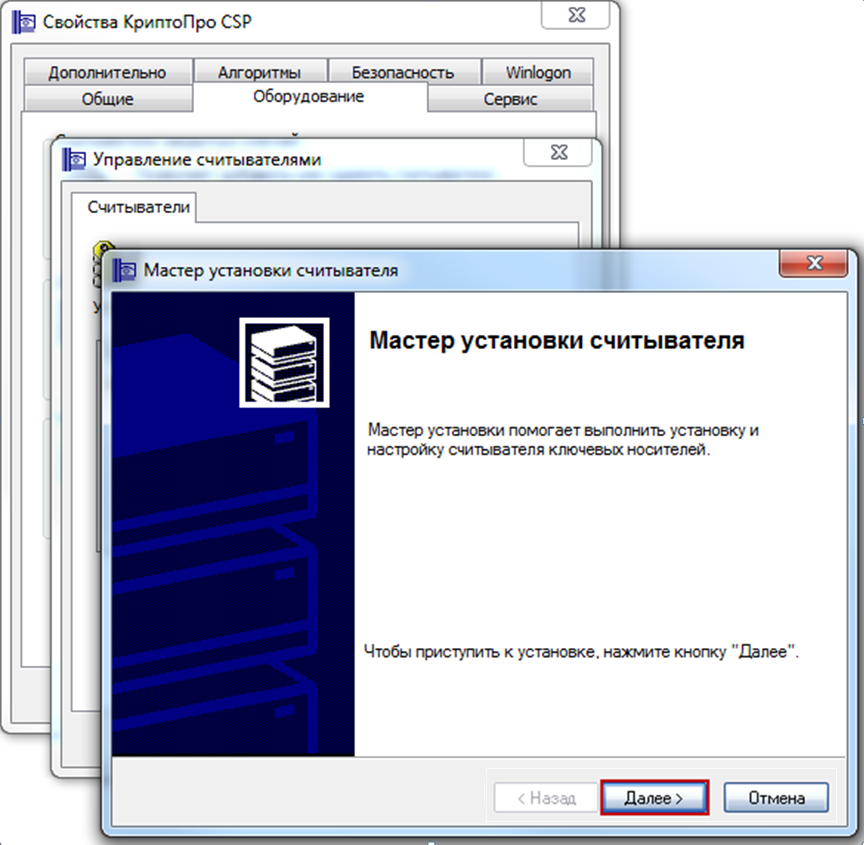


Рисунок 43 Установка считывателя

В блоке «Производители» выберите пункт «Компания Крипто-Про», в блоке «Доступные считыватели» выберите пункт Дисковод G (где G – буква вашего Flash-накопителя). Нажмите на кнопку «Далее» ().

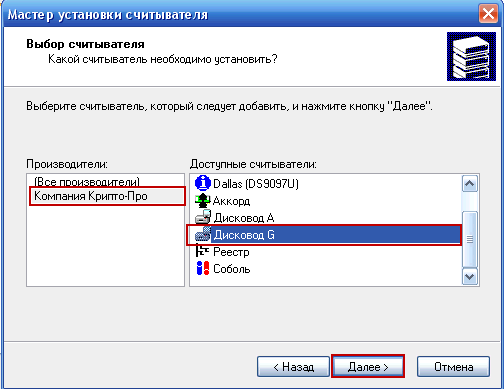


Рисунок 44 Добавление Flash-накопителя

Укажите имя считывателя и нажмите на кнопку «Далее» ().

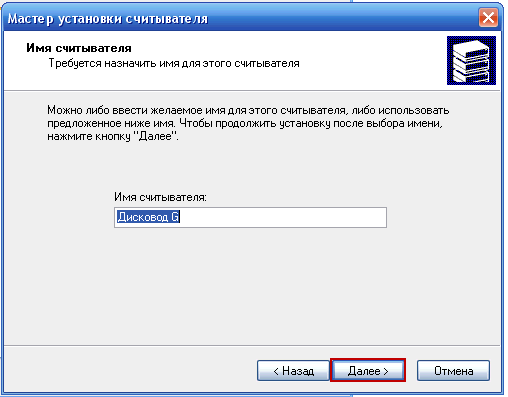


Рисунок 45 Имя считывателя

Нажмите на кнопку «Готово» (). Перезагрузите компьютер.

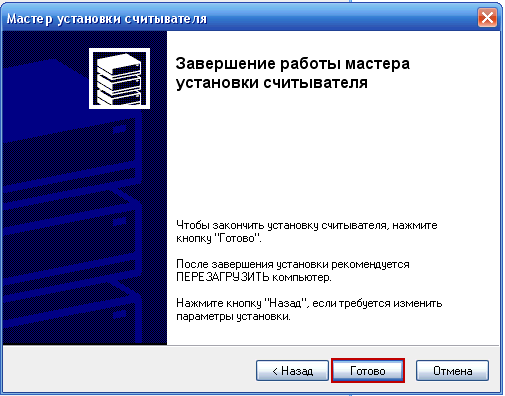


Рисунок 46 Окончание установки

### Установка сертификата в CryptoPro CSP

Вставьте установленный ранее Flash-накопитель с контейнерами сертификатов.

При наличии сертификата типа PKCS #7 (данный файл выдается удостоверяющим центром) необходимо предварительно экспортировать личный сертификат, расположенный в файле с расширением \*.p7b. Для экспорта сертификата выполните следующие действия:

1. Откройте файл \*.p7b.
2. В левой части открывшегося окна разверните иерархию, нажмите на пункт «Certificates».
3. В правой части окна для личного сертификата нажмите на пункт контекстного меню «All task», далее нажмите на пункт «Export» ().

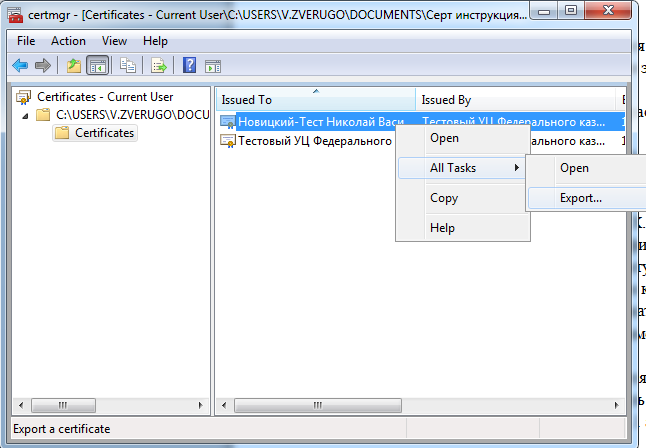


Рисунок 47 Экспорт сертификата

1. В открывшемся окне нажмите на кнопку «Далее».
2. Выберите формат файла для сохранения экспортируемого сертификата «Base-64 encoded X.509 (.CER)», нажмите на кнопку «Далее».
3. Укажите место для сохранения экспортированного сертификата (например, флэш-накопитель с сертификатами) и введите имя файла сертификата. Рекомендуется, чтобы введенное имя совпадало с названием контейнера.
4. Нажмите на кнопку «Далее», в окне подтверждения нажмите на кнопку «Завершить».

Система осуществляет экспорт сертификата и сохраняет его по указанному пути с присвоением введенного имени.

Для установки личного сертификата загрузите CryptoPro (/Program Files/Crypto Pro/CSP/cpconfig.cpl).

Выберите вкладку «Сервис» и нажмите на кнопку «Установить личный сертификат» ().

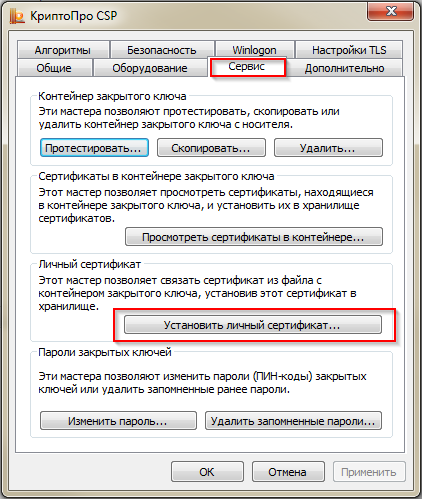


Рисунок 48 Установка личного сертификата

Отображается окно выбора устанавливаемого личного сертификата.

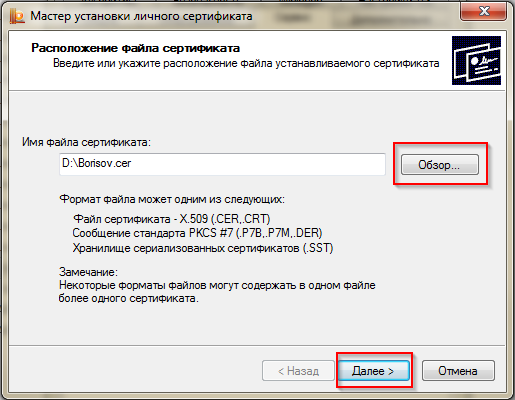


Рисунок 49 Выбор личного сертификата

Нажмите на кнопку «Обзор» и выберите личный сертификат в формате \*.cer. Нажмите на кнопку «Далее». Отображается окно просмотра и выбора сертификата для продолжения установки ().

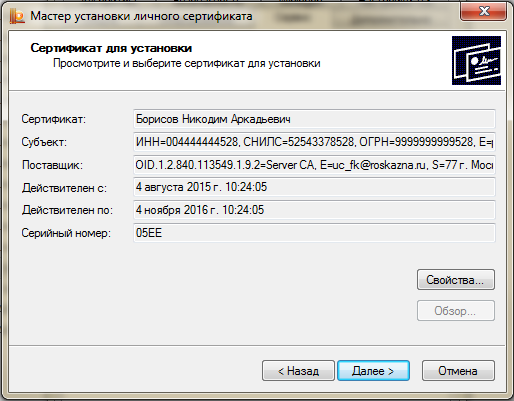


Рисунок 50 Данные сертификата

Проверьте наличие необходимых данных и нажмите на кнопку «Далее». Отображается окно для выбора ключевого контейнера ().

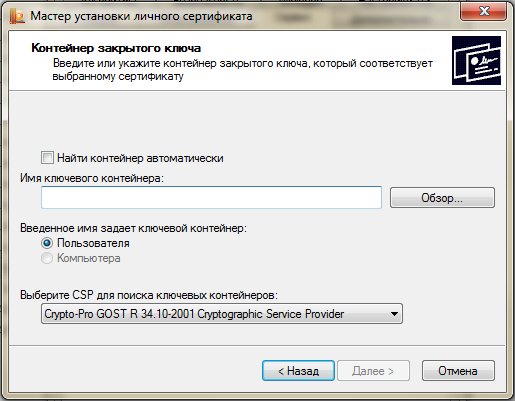


Рисунок 51 Выбор контейнера

Нажмите на кнопку «Обзор». Выберите необходимый ключевой контейнер ().

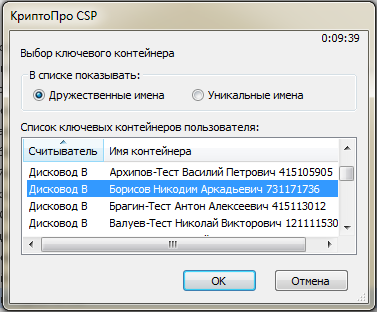


Рисунок 52 Выбор ключевого контейнера

Нажмите на кнопку «ОК». В отобразившемся окне нажмите на кнопку «Далее» ().

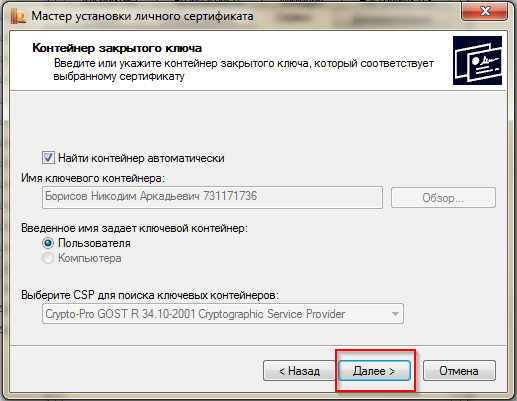


Рисунок 53 Выбор ключевого контейнера

Нажмите на кнопку «Обзор». Отображается окно выбора хранилища сертификатов ().

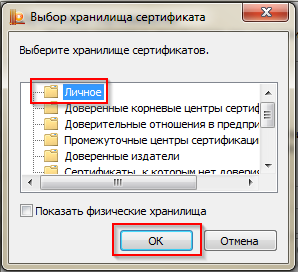


Рисунок 54 Выбор хранилища

Выберите пункт «Личное» и нажмите на кнопку «ОК». После этого нажмите на кнопку «Далее» (см. ). На открывшейся странице нажмите на кнопку «Готово» (). Система произведет установку сертификата.

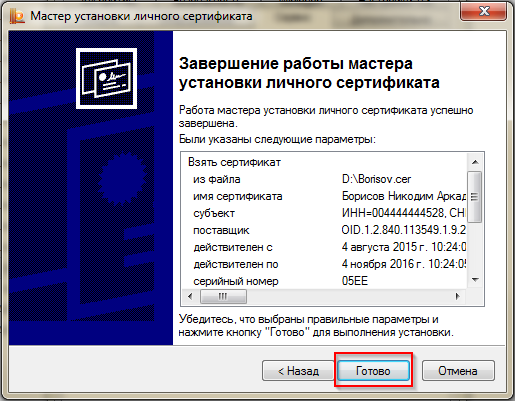


Рисунок 55 Окончание установки

В системе предусмотрено автоматическое оповещение об окончании срока действия сертификата ЭП. При входе в ЛК пользователя отображается модальное окно о скором окончании срока действия сертификата ЭП ().

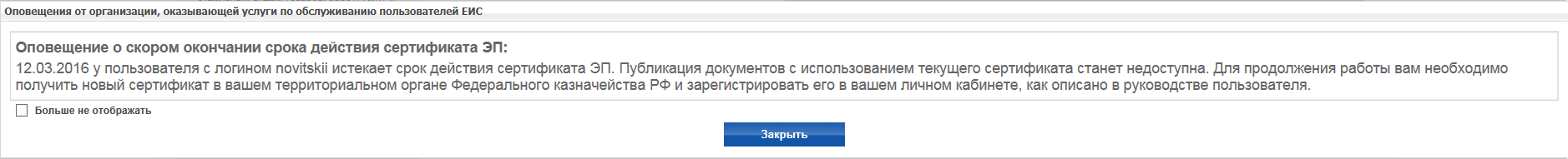


Рисунок 56 Оповещение о скором окончании срока действия сертификата ЭП

При установке флажка в поле «Больше не отображать» это оповещение перестает отображаться только для пользователя, установившего флажок в ЛК.

Для установки корневого сертификата пользователя откройте файл сертификата и нажмите на кнопку «Установить сертификат» (Рисунок 57).

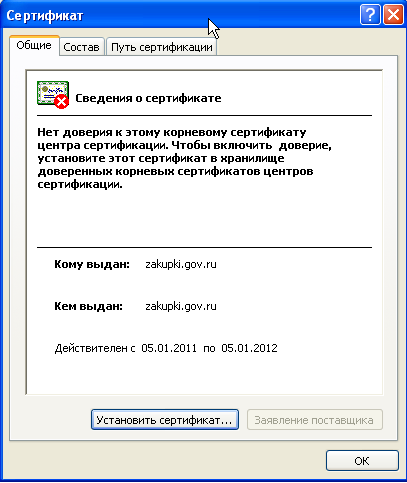


Рисунок 57 Сведения о сертификате

В открывшемся окне установки нажмите «Далее», выберите пункт «Поместить сертификат в следующие хранилища» и нажмите кнопку «Обзор» (Рисунок 58).

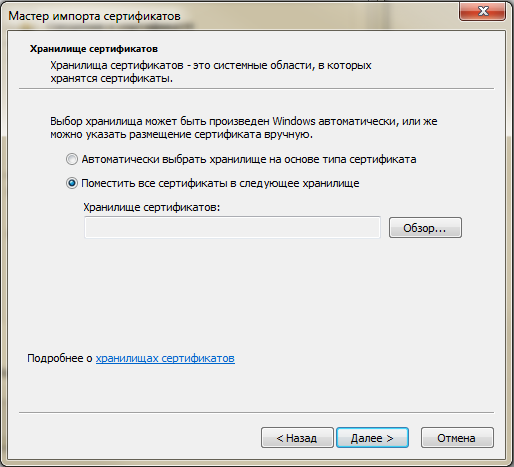


Рисунок 58 Выбор хранилища сертификата

В открывшемся списке хранилищ (Рисунок 59) выберите хранилище «Доверенные корневые центры сертификации» и нажмите «ОК». В окне установки нажмите кнопку «Далее» и затем кнопку «Готово» для завершения установки.

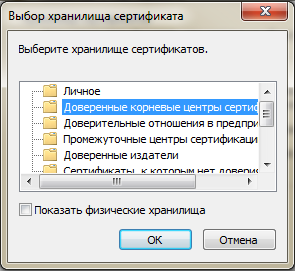


Рисунок 59 Список хранилищ

В появившемся окне нажмите на кнопку «Да» (Рисунок 60).

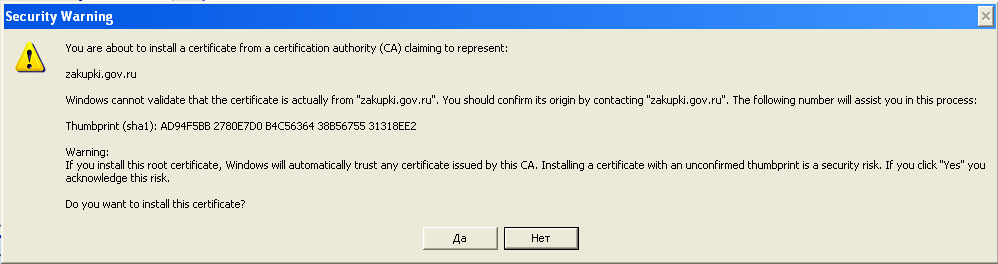


Рисунок 60 Подтверждение установки

### Перерегистрация сертификата

Для осуществления перерегистрации сертификата необходимо авторизоваться в личном кабинете пользователя, у которого истек срок действия ранее полученного сертификата.

Выберите пункт вертикального меню «Редактировать», в блоке «Пользователь» ().

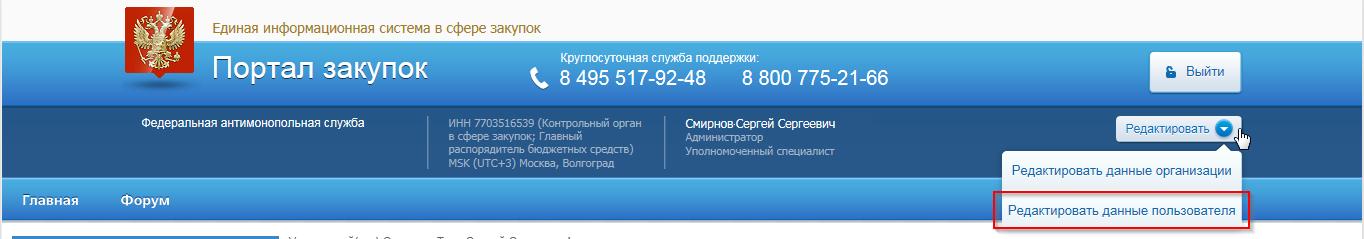


Рисунок 61 Пункт меню «Редактировать данные пользователя»

Отображается страница «Регистрационные данные пользователя».

Страница содержит следующие элементы:

* гиперссылку «Зарегистрировать сертификат ЭП»;
* поле «Полномочия пользователя»;
* поле «Фамилия»;
* поле «Отчество»;
* поле «Логин»;
* поле «Пароль»;
* поле «Подтверждения пароля»;
* поле «Кодовая фраза»;
* поле «Должность»;
* поле «Контактный телефон»;
* поле «Адрес электронной почты»;
* кнопка «Сохранить»;
* кнопка «Отмена».

Для регистрации сертификата ЭП, нажмите на гиперссылку «Зарегистрировать сертификат ЭП» ().

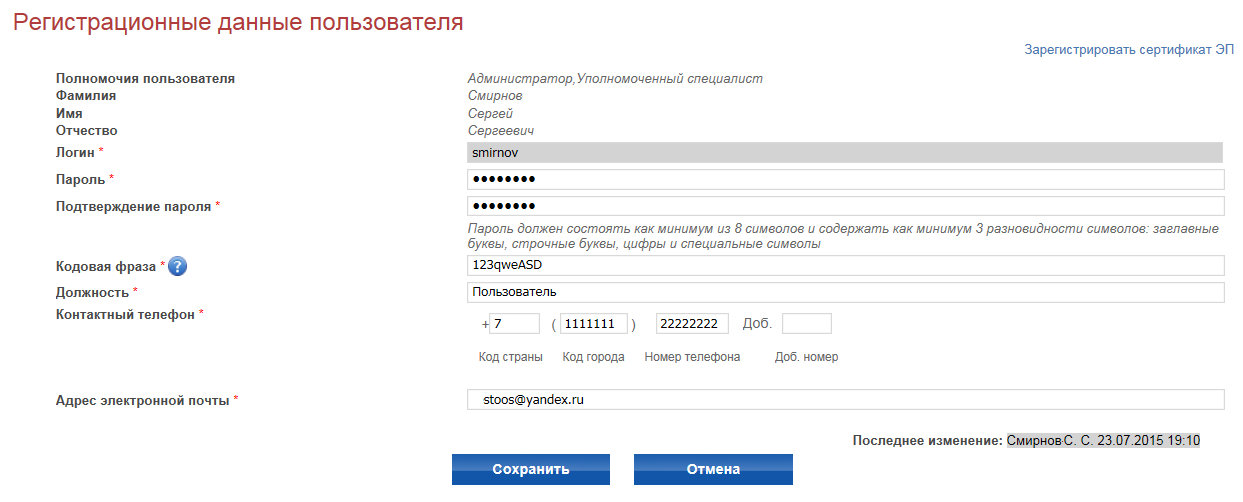


Рисунок 62 Гиперссылка «Зарегистрировать сертификат ЭП»

Отображается страница «Регистрационные данные пользователя». Страница содержит поле для указания пути к файлу ().

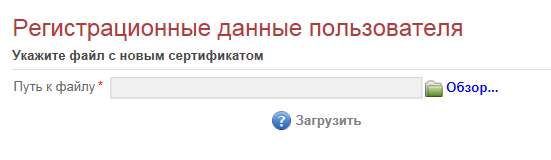


Рисунок 63 Страница «Регистрационные данные пользователя»

Нажмите на гиперссылку «Обзор».

Отображается окно выбора файла. Укажите путь к файлу с расширением \*.crl для нового сертификата, нажмите на кнопку «Загрузить».

Отображается окно с регистрационными данными пользователя. Введите пароль и подтвердите его в соответствующих полях. Нажмите на кнопку «Сохранить».

Для проверки корректности выполнения перерегистрации, необходимо выйти из личного кабинета пользователя и заново авторизоваться под сертификатом.

Лист регистрации изменений

| Версия док-та | Дата изменения | Изменение |
| --- | --- | --- |
| 1.0 | 08.01.2014 | Исходная версия документа |
| 1.1 | 18.02.2014 | В п. добавлено описание компонента sign.cab |
| 1.2 | 19.01.2015 | Актуализированы п. , , |
| 1.3 | 23.01.2015 | В пп. , добавлено описание работы с квалифицированными сертификатами при установке сертификата удостоверяющего центра и личного сертификата |
| 1.4 | 06.04.2015 | В пп. добавлено уточнение названия актуального корневого сертификата.  В пп. добавлены изображения для настройки английской версии браузера и добавления адреса <http://zakupki.gov.ru>.  В пп. добавлена полная настройка параметров безопасности в зоне надежных узлов.  В пп. добавлено описание процесса включения параметра «.Net Framework 3.5 (включает .Net 2.0 и 3.0)».  Добавлено описание следующих процессов:  включение пункта «Переопределить автоматическую обработку куки-файлов» (пп. );  сброс параметров браузера по умолчанию (пп. );  удаление временных файлов Интернета, истории обзора, куки-файлов (пп. );  добавление узла «zakupki.gov.ru» для просмотра в режиме совместимости (пп. ). |
| 1.5 | 30.07.2015 | В пп. , удалена информация об альтернативном варианте входа.  Добавлена нумерация страниц. |
| 1.6 | 24.09.2015 | Отредактирован п. 2.1.1. |
| 1.7 | 29.01.2016 | Документ обновлен для версии браузера Internet Explorer 11.0. |
| 1.8 | 13.05.2016 | Добавлены п. 1.2.3, 1.2.10. |
| 1.9 | 02.05.2017 | Обновлены п. 1.2.8, 1.2.10, 1 2 12. Добавлен п. 1.2.9. |
| 2.0 | 22.12.2017 | Обновлен п. 1.1 в части установки Корневого сертификата Уполномоченного удостоверяющего центра Федерального казначейства. |
| 2.1 | 02.03.2018 | Добавлен п. 1.2.12. |
| 2.2 | 23.05.2018 | Обновлены требования по использованию ПО CryptoPro CSP – п. 1.2.8, а также рекомендации по установке параметров обозревателя по умолчанию в части использования TLS – п. 1.2.5. |

1. В данном документе настройки описываются на примере Интернет-браузера Internet Explorer 11.0. Для осуществления аналогичных настроек в других Интернет-браузерах см. документацию на данное ПО. [↑](#footnote-ref-1)
2. Федеральное казначейство бесплатно предоставляет Криптопровайдер CryptoPro CSP Заказчикам [↑](#footnote-ref-2)