

ООО «КСК ТЕХНОЛОГИИ»

наименование организации — разработчика АИС

Система управления бизнес-процессами
«Платформа КСК.Интеллектуальный конвейер»

наименование вида АИС

Платформа КСК.ИК, КСК.ИК

сокращенное наименование АИС

РУКОВОДСТВО АДМИНИСТРАТОРА

(УСТАНОВКА СИСТЕМЫ)

На 38 листах

г. Москва, 2019

АННОТАЦИЯ

Настоящий документ является руководством администратора по установке системы управления бизнес-процессами «Платформа КСК.Интеллектуальный конвейер» (далее по тексту – Платформа КСК.ИК, Система).

Настоящий документ содержит описание действий администратора в части установки Системы.

Настоящий документ разработан в соответствии с РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов».

СОДЕРЖАНИЕ

Аннотация	2
СОДЕРЖАНИЕ	3
Перечень терминов и сокращений	5
1 Введение.....	9
1.1 Область применения.....	9
1.2 Краткое описание возможностей	9
1.3 Требования к уровню подготовки пользователей	10
1.4 Перечень эксплуатационной документации	10
2 Назначение и условия применения	11
2.1 Назначение системы	11
2.2 Требования к аппаратному и программному обеспечению (Условия применения Системы)	11
2.2.1 Состав инсталляционного комплекта	11
2.2.2 Системные требования Платформы КСК.ИК.....	12
2.2.3 Программные и аппаратные требования к рабочей станции пользователя	12
2.2.4 Требования к квалификации персонала, порядку его подготовки и контролю знаний и навыков	13
3 Установка системы	14
3.1 Перечень пакетов Системы.....	14
3.2 Установка PostgreSQL	15
3.3 Установка OpenLdap.....	17
3.4 Установка Nginx на портал	17
3.5 Установка Liferay и общих компонентов	17
3.6 Установка модулей на портал.....	22
3.7 Перезапуск компонентов системы	22
4 Настройки в системе.....	24
4.1 Настройка модуля ЭЦП (КриптоПро CSP) на ПК оператора	24
4.1.1 Установка модуля КриптоПРО и плагинов для браузеров	24

4.1.2	Получение сертификата	25
4.1.3	Установка сертификата	29
4.1.4	Настройка плагина	35
5	Аварийные ситуации	37
5.1	Действия в случаях несоблюдения технологического процесса	37
5.2	Действия по восстановлению программ при сбойных ситуациях и ошибках в данных	37
5.3	Действия в случаях несанкционированного доступа к данным	37
6	Рекомендации по освоению	38

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Аббревиатура	Пояснение
API	<p>Интерфейс программирования приложений (Application Programming Interface)</p> <p>Набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах. Используется программистами при написании всевозможных приложений.</p>
BPMN	<p>англ. Business Process Model and Notation, нотация и модель бизнес-процессов — система условных обозначений (нотация) для моделирования бизнес-процессов.</p>
CD	<p>Компакт-диск (Compact Disc)</p> <p>Оптический носитель информации в виде пластикового диска.</p>
HTTP	<p>Протокол передачи гипертекста (HyperText Transfer Protocol)</p> <p>Протокол прикладного уровня передачи данных</p>
ISO	<p>Международная организация по стандартизации (International Organization for Standardization)</p>
LDAP	<p>Облегченный протокол доступа к каталогам (Lightweight Directory Access Protocol)</p> <p>Протокол прикладного уровня для доступа к службе каталогов</p>

OSGI-модули	Модули технологии OSGI, которые расширяют основной функционал.
TCP/IP	<p>Протокол управления передачей (Transmission Control Protocol) и межсетевой протокол (Internet Protocol)</p> <p>Набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет</p>
XML	Расширяемый язык разметки (eXtensible Markup Language)
БД	База данных
Бизнес-процесс	Совокупность взаимосвязанных этапов; состоит из основного процесса и подпроцессов
Диалоговое окно	Диалоговое окно предназначено для вывода информации и (или) получения ответа/подтверждения от пользователя.
Маршрут	Последовательность шагов, описанная в нотации BPM (англ. Business Process Management, управление бизнес-процессами — концепция процессного управления организацией) и предоставленная в системе в виде файла маршрута
ОС	Операционная система
Печатная форма	Заполненная форма — заявление, опись и т. п., установленная регламентом, в виде файла с данными, выгруженного из системы
Плагин CryptoPro	Стороннее ПО, обеспечивающее работу с электронной подписью (далее — ЭП)
ПО	Программное обеспечение

Подпроцесс	Набор этапов, объединенных одной темой; является отдельной веткой и запускается с этапа основного процесса. Обязательность прохождения подпроцесса для завершения этапа основного процесса регламентируется процедурой
Пользователь	Человек, использующий Систему для решения поставленных целей и выполнения задач; имеет учетную запись в Системе
Портлет	Подключаемый, сменный компонент пользовательского интерфейса веб-портала (элемент веб-страницы)
Проект	Процесс, разбитый по ключевым стадиям; реализован в виде иерархической структуры работ с возможностью привязки бизнес-процессов к работе(-ам) или проекту в целом
Роль	Совокупность прав доступа на объекты Системы
Система	Система управления бизнес-процессами «Платформа КСК.Интеллектуальный конвейер»
Скриплет	Простой сценарий, подготовленный с помощью интерпретируемого макроязыка (XML), обрабатываемый браузером совместно с кодом HTML
Спойлер	Панель с заголовком блока, по нажатию на которую открывается содержимое блока. По повторному нажатию на заголовок содержимое скрывается. Закрытый блок помечается символом «◆». Раскрытый блок — символом «▼»

СУБД	Система управления базами данных
ФИАС	Федеральная информационная адресная система
Шаблон	Форма шаблона документа — договор, акт, заключение и т.п., установленная регламентом, в виде файла с данными, выгруженного из системы и доступного для редактирования
ЭД	Электронный документ
ЭП	Электронная подпись

1 ВВЕДЕНИЕ

1.1 Область применения

Настоящий документ является руководством администратора Платформы КСК.Интеллектуальный конвейер и определяет общие принципы по установке системы.

Платформа КСК.ИК – это комплексный инструмент моделирования, исполнения и управления бизнес-процессами и проектами.

Бизнес-процесс – это совокупность взаимосвязанных этапов, направленных на достижение определенной цели.

Проект предназначен для автоматизации сквозных бизнес-процессов.

1.2 Краткое описание возможностей

Платформа КСК.ИК обеспечивает:

- моделирование бизнес-процессов в дизайн-студии: маршрут, интерактивные формы, исполнители и сроки;
- исполнение бизнес-процессов, визуализацию схемы исполнения в графическом виде с выделением пройденных этапов;
- автоматическое формирование реестров с данными, получаемыми в ходе исполнения бизнес-процессов;
- контроль сроков исполнения бизнес-процессов, в том числе контроль сроков исполнения каждого этапа процесса;
- хранение электронных документов, формируемых в ходе исполнения бизнес-процессов и проектов;
- поддержку электронной подписи документов;
- мониторинг и статистику по проектам и бизнес-процессам;
- интеграцию с другими информационными системами с целью приема-передачи данных.

1.3 Требования к уровню подготовки пользователей

Для использования Системы необходимо иметь навыки работы с персональным компьютером в среде Microsoft Windows и навыки работы с браузерами.

1.4 Перечень эксплуатационной документации

Для работы в Системе пользователю необходимо ознакомиться с настоящим Руководством.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Назначение системы

Платформа КСК.ИК предназначена:

- для моделирования и исполнения бизнес-процессов;
- для создания единого файлового хранилища документов;
- для создания реестров, обеспечивающих учет информации по бизнес-процессам;
- для автоматизированного контроля соблюдения последовательности и сроков выполнения задач, исполняемых в бизнес-процессах.

2.2 Требования к аппаратному и программному обеспечению (Условия применения Системы)

2.2.1 Состав инсталляционного комплекта

Инсталляционный комплект поставки имеет следующую структуру:

- Oracle JDK 8.202;
- Apache Tomcat 9;
- Liferay Portal 7;
- PostgreSQL 10;
- nginx 1.14;
- Web-модули Платформы КСК.ИК 2.1.

Установка системы производится на операционную систему Ubuntu Server 16.04.5 (<http://releases.ubuntu.com/16.04/ubuntu-16.04.5-server-amd64.iso>). При использовании других linux-based операционных систем некоторые команды могут незначительно отличаться. Необходимо свериться с документацией по используемой операционной системе.

2.2.2 Системные требования Платформы КСК.ИК

Сервер портала:

- CPU: 8 ядер (не ниже 2,4 ГГц);
- RAM: 24 ГБ;
- HDD: от 120 ГБ RAID-0/5/10.

Сервер СУБД:

- CPU: 4 ядер (не ниже 2,4 ГГц).
- RAM: 16 ГБ;
- HDD: от 60 ГБ RAID-0/5/10.

2.2.2.1 Синхронизация серверов

При установке компонентов системы на разные виртуальные машины дата и время на используемых виртуальных машинах должны быть синхронизированы. Погрешность должна быть не больше 15 секунд.

2.2.3 Программные и аппаратные требования к рабочей станции

пользователя

На клиентском рабочем месте должно быть установлено следующее программное обеспечение:

- операционная система — Windows 7 и выше;
- браузеры — Mozilla Firefox 65 и выше; Google Chrome 72 и выше.

Клиентская рабочая станция должна обладать техническими характеристиками не ниже следующих:

- процессор (CPU): Intel Pentium 2 ГГц и выше;
- оперативная память (RAM): не менее 4 ГБ;
- жесткий диск: 80 ГБ;

- монитор с разрешением экрана: 1280×1024 пикселей и выше;
- сетевой интерфейс (LAN): 100 мбит/с и выше.

2.2.4 Требования к квалификации персонала, порядку его подготовки и контролю знаний и навыков

Администратор Системы должен обладать знаниями по:

- архитектуре используемых серверов;
- установке, диагностике и администрированию ОС Linux;
- диагностике и администрированию виртуальной машины Java;
- диагностике и администрированию СУБД PostgreSQL;
- диагностике и администрированию сервера приложений Tomcat;
- диагностике и администрированию портала Liferay portal и других компонентов системы;
- проведению регламентных работ, таких как запуск / остановка, перевод в другие режимы работы, резервное копирование данных и их восстановление из резервной копии, настройка прав доступа.

3 УСТАНОВКА СИСТЕМЫ

Установка системы производится на операционную систему Ubuntu Server 16.04.5. При использовании других debian-based операционных систем некоторые команды могут незначительно отличаться. Необходимо свериться с документацией по используемой операционной системе.

3.1 Перечень пакетов Системы

Ниже представлены перечень пакетов Системы, необходимых для установки (Таблица 1).

Таблица 1 — Пакеты Системы

Пакеты АИС	Русскоязычное описание
kck-liferay-7	Портал Liferay и сервер приложений Tomcat
kck-backup	Пакет резервного копирования
kck-activemq	Брокер очередей
kck-tmof-fix	Настройка операционной системы
kck-jdk-8	Oracle JDK 8
kck-plt-db-config	Конфигурация базы данных
kck-nginx-1.14	Веб-сервер Nginx
kck-plt-nginx-conf	Конфигурация веб-сервера Nginx
kck-siu-openldap	Конфигурация директории пользователей
kck-jsp-2	Модуль подписи
kck-plt-general-clients kck-plt-manage-clients kck-plt-server	Метапакеты для установки модулей КСК.Платформы
kck-oip-cas-java8-lr7	Сервер авторизации

kck-plt-sided-modules	Метапакет для установки общих модулей системы
liferay_plt.xml	Конфигурационный xml файл для портала

Подразумевается, что архив с пакетами собственной разработки компании ООО «КСК ТЕХНОЛОГИИ» имеется в распоряжении у администратора, производящего установку Системы. Пакеты сторонней разработки скачиваются из общедоступных репозиториев.

3.2 Создание локального репозитория из деб-пакетов системы:

1. Установить пакет:

```
sudo apt-get install dpkg-dev
```

2. Перейти в папку, куда были скачаны пакеты системы и выполнить:

```
sudo dpkg-scanpackages /путь/к/папке/с/пакетами /dev/null >
/путь/к/папке/с/пакетами/Packages
```

3. Скопировать файл:

```
sudo cp /путь/к/папке/с/пакетами/Packages /
```

4. Открыть файл /etc/apt/sources.list и добавить в него строку:

```
deb file:/// ./
```

5. Дать права:

```
sudo chown -Rv _apt:root /var/cache/apt/archives/partial/
sudo chmod -Rv 700 /var/cache/apt/archives/partial/
```

6. Выполнить обновление репозиториев:

```
sudo apt-get update
```

3.3 Установка PostgreSQL

Устанавливается на сервер СУБД.

1. Добавить репозиторий для PostgreSQL:

```
sudo nano /etc/apt/sources.list.d/pgdg.list
```

2. Прописать:

```
deb http://apt.postgresql.org/pub/repos/apt/ xenial-pgdg main
```

3. Добавить публичный ключ:

```
wget --quiet -O -  
https://www.postgresql.org/media/keys/ACCC4CF8.asc | \  
sudo apt-key add -
```

4. Выполнить обновление apt/aptitude

```
sudo apt-get update -o  
Dir::Etc::sourcelist="sources.list.d/pgdg.list" -o  
Dir::Etc::sourceparts="-" -o APT::Get::List-Cleanup="0"
```

5. Установить:

```
sudo apt-get install postgresql-10
```

6. Настроить доступ к БД:

Внимание

В данном примере настройка идет для всех ПК сегмента сети. На продуктиве необходимо указывать только доменные имена и IP.

7. Редактировать файл /etc/postgresql/10/main/postgresql.conf

```
listen_addresses = '*'  
max_connections = 800  
shared_buffers = 1024MB
```

8. Редактировать файл /etc/postgresql/10/main/pg_hba.conf

```
# IPv4 local connections:  
host      all             all             127.0.0.1/32      md5  
host      all             all             0.0.0.0/0         trust
```

9. Перезапустить Postgres

```
sudo service postgresql restart
```

10. Создать пользователя postgres:

```
sudo -u postgres psql -c "ALTER USER postgres PASSWORD 'postgres';"
```

11. Конфигурировать БД, следуя инструкциям конфигурационного пакета:


```
sudo apt-get install kck-plt-db-config
```

3.4 Установка OpenLdap

1. Установить пакет OpenLDAP:

```
sudo apt-get install kck-backup  
sudo apt-get install slapd ldap-utils netcat
```

2. Установить конфигурационный пакет:

```
sudo apt-get install kck-siu-openldap
```

Вписать в **baseDN** актуальный для клиента логин и пароль администратора.

3.5 Установка Nginx на портал

1. Установить из пакета:

```
sudo apt-get install kck-nginx-1.14
```

2. Установить конфигурационный пакет:

```
sudo apt-get install kck-plt-nginx-config
```

Во время конфигурирования Nginx будет создан самоподписанный сертификат. Все поля могут быть заполнены на усмотрение, кроме поля FQDN — в нем прописывается полное доменное имя площадки.

Создать хранилище сертификатов для последующего импорта в сервер приложений.

```
sudo openssl pkcs12 -export -in /opt/nginx/ssl/plt-cert.pem -inkey  
/opt/nginx/ssl/plt-cert.key -out /tmp/keystore -name tomcat -CAfile  
cacert
```

Примечание

Пароль на хранилище по умолчанию «changeit».

3.6 Установка брокера очередей ActiveMQ

Установить пакеты:

```
sudo apt-get install kck-tmof-fix  
sudo apt-get install kck-jdk-8
```

```
sudo apt-get install kck-activemq
```

3.7 Установка криптопровайдера

```
sudo apt-get install kck-jcp-2
```

3.8 Установка Liferay и общих компонентов

Устанавливается на сервер портала.

1. Дать шелл www-data и создать домашнюю папку:

```
sudo chsh www-data -s /bin/bash  
sudo mkdir /var/www  
sudo chown www-data:www-data /var/www
```

2. Прописать доменное имя портала в файле /etc/hosts после адреса 127.0.0.1

3. Прописать JAVA_HOME

В файл /etc/environment добавить:

```
JAVA_HOME="/opt/jdk"  
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:$JAVA_HOME/bin"
```

И выполнить:

```
source /etc/environment  
sudo ln -s /opt/jdk/jre/bin/java /usr/bin/java
```

4. Установить портал Liferay и сервер приложений Tomcat

```
sudo apt-get install kck-liferay-7
```

5. Добавить ранее созданное ключевое хранилище в хранилища tomcat'а и java.

```
sudo /opt/jdk/bin/keytool -importkeystore -deststorepass changeit -  
destkeypass changeit -destkeystore  
/opt/liferay/tomcat/conf/tomcat.jks -srckeystore /tmp/keystore -  
srcstoretype PKCS12 -srcstorepass changeit -alias tomcat
```

```
sudo /opt/jdk/bin/keytool -importkeystore -deststorepass changeit -  
destkeypass changeit -destkeystore /opt/jdk/jre/lib/security/cacerts  
-srckeystore /tmp/keystore -srcstoretype PKCS12 -srcstorepass  
changeit -alias tomcat
```

6. Запустить конфигурацию сервера приложений через пакет **kck-plt-tomcat-config**

```
sudo apt-get install kck-plt-tomcat-config
```

7. Запустить Liferay

```
sudo service kck-liferay-7 start
```

8. Авторизоваться в Liferay по адресу [http://<доменное _имя_портала>](http://<доменное_имя_портала>).
Логин / пароль: test / test.

Прописать настройки подключения в Liferay (Control Panel – Instance Settings – закладки CAS и LDAP), используя ранее заданные параметры подключений.
(Рисунок 1).

Authentication

[General](#) [OpenSSO](#) [CAS](#) [NTLM](#) [LDAP](#) [OpenID](#) [Facebook](#) [Google](#)

☒ Enabled

☒ Import from LDAP ?

Login URL ?

☐ Logout on session expiration. ?

Logout URL ?

Server Name ?

Server URL ?

Service URL ?

No Such User Redirect URL ?

Рисунок 1 — Настройка подключения

Значения по умолчанию

☐ Apache Directory Server ☐ Fedora Directory Server ☐ Microsoft Active Directory Server ☐ Novell eDirectory ☐ OpenLDAP ☐ Другая служба каталогов

Восстановить значения

Соединение

URL базового провайдера ⓘ
ldap://plt_ldap:389

Base DN ⓘ
ou=people,dc=kck,dc=ru

Доверитель
cn=admin,dc=kck,dc=ru

Верительные данные

Тестировать соединение с LDAP

Рисунок 3 – Настройка LDAP

Так же, при настройке сервера LDAP заполнить поле «Отчество» как initials и в поле «Пользовательские классы объектов по умолчанию» добавить через запятую pguPersonInfo .

Во вкладке CAS проставить галочки напротив:

- Включен;
- Импорт из LDAP.

Во вкладке LDAP проставить галочки напротив:

- Включен;
- Требуется;
- Разрешить импорт;
- Разрешить импорт на старте.

3.9 Установка модулей на портал

1. Установить базовые модули системы и провести донастройку системы:

```
sudo apt-get install kck-plt-sided-modules kck-oip-cas-java8-lr7
```

2. Установить модули Платформы:

```
sudo apt-get install kck-plt-server  
sudo apt-get install kck-plt-general-clients  
sudo apt-get install kck-plt-manage-clients
```

3. Зайти на портал и авторизоваться **test / abcd1234**:

В левом меню выбрать ваш инстанс, закладку «Навигация» и напротив закладки «Публичные страницы» нажать троеточие, выбрать «Настроить». В открывшейся странице выбрать «Внешний вид», «Изменения текущей темы», выбрать тему «platform-default-gen4-theme» и нажать «Сохранить».

Для построения меню портала необходимо:

— открыть адрес конфигулятора портала:

https://доменное_имя_портала/o/liferayconf-server/secured/preferences/api;

— загрузить файлы liferay_plt.xml и *.png на открывшейся странице .

Дождаться сообщения об успешной загрузке.

4. Вернуться на портал. Выбрать «Панель управления» - «Параметры Системы», вкладка «Фонд», строка JavaScript Loader - «Изменить». На открывшейся странице снять выбор «Expose global».

5.

6. Перезагрузить Liferay

```
sudo service kck-liferay-7 restart
```

7. Установка завершена.

3.10 Перезапуск компонентов системы

1. Перезапуск портала:

```
sudo service kck-liferay-7 restart
```

2. Перезапуск СУБД:

```
sudo service postgresql restart
```

3. Перезапуск OpenLDAP:

```
sudo service slapd restart
```

4. Перезапуск ActiveMQ

```
sudo service kck-activemq restart
```

5. Перезапуск Nginx:

```
sudo service kck-nginx restart
```

4 НАСТРОЙКИ В СИСТЕМЕ

4.1 Настройка модуля ЭЦП (КриптоПро CSP) на ПК оператора

Примечание

Все действия выполняются пользователем с правами администратора.

Для работы с плагином пользователю необходимо иметь:

- персональный компьютер с установленным браузером Mozilla Firefox или Google Chrome;
- установленный плагин для браузера «КриптоПро ЭЦП Browser plug-in»;
- сертификат ключа подписи (тестовый сертификат можно получить на странице тестового центра).

4.1.1 Установка модуля КриптоПРО и плагинов для браузеров

Для настройки модуля ЭП (КриптоПро CSP) пользователю необходимо:

6. Прежде всего установить «Крипто ПРО CSP» из директории при помощи «CSPSetup.exe» (Рисунок 2).

Скачать можно с <http://www.cryptopro.ru/products/csp/downloads>.



Рисунок 2 — Установка Крипто ПРО CSP

7. Загрузить и установить плагин для браузера «КриптоПро ЭЦП Browser plug-in». Загрузить данный плагин можно с сайта <https://www.cryptopro.ru/products/cades/plugin>.

Для установки плагина подтвердите действие в диалоговом окне браузера (Рисунок 3).

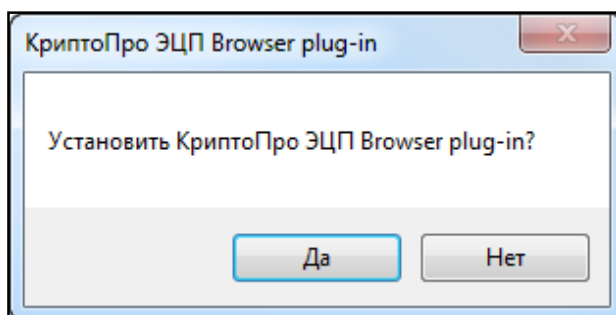


Рисунок 3 — Подтверждение установки

8. Установить модуль поддержки Криптопро CSP, скачать можно с сайта <http://www.rutoken.ru/support/download/rutoken-for-cp/>.

9. Установить драйверы Рутокен, скачать можно с сайта <http://www.rutoken.ru/support/download/drivers-for-windows/>.

4.1.2 Получение сертификата

Для получения сертификата ключа подписи необходимо выполнить шаги, описанные ниже (можно получить тестовый сертификат на странице тестового центра).

— Перейдите на страницу тестового центра <http://cryptopro.ru/certsrv/> и сформируйте ключи.

10. На указанной странице выберите пункт «Сформировать ключи и отправить запрос на сертификат» и нажмите на кнопку «Дальше».

11. В открывшемся диалоговом окне нажмите на кнопку «Да» (Рисунок 4).

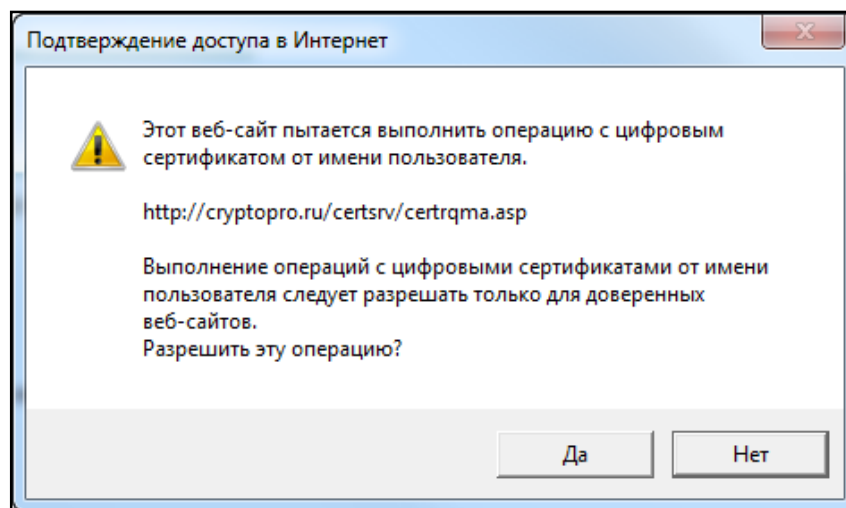


Рисунок 4 — Подтверждение выполнения операции с цифровым сертификатом

12. Заполните поля на открывшейся странице (Рисунок 5) и нажмите на кнопку «Выдать».

Идентифицирующие сведения:

Имя:

Электронная почта:

Организация:

Подразделение:

Город:

Область, штат:

Страна, регион:

Тип требуемого сертификата:

Параметры ключа:

☒ Создать новый набор ключей ☐ Использовать существующий набор ключей

CSP:

Использование ключей: ☒ Exchange ☐ Подпись ☐ Оба

Размер ключа: Минимальный: 512 Максимальный: 512 (стандартные размеры ключей: [512](#))

☒ Автоматическое имя контейнера ключа ☐ Заданное пользователем имя контейнера ключа

☒ Пометить ключ как экспортируемый

☐ Использовать локальное хранилище компьютера для сертификата
Сохраняет сертификат в локальном хранилище вместо пользовательского хранилища сертификатов. Не устанавливает корневой сертификат ЦС. Необходимо быть администратором, чтобы создать локальное хранилище.

Дополнительные параметры:

Формат запроса: ☐ CMC ☒ PKCS10

Алгоритм хеширования:
Используется только для подписания запроса.

☐ Сохранить запрос

Атрибуты:

Понятное имя:

Рисунок 5 — Форма запроса на сертификат

13. В открывшемся окне для создания хранилища ключей выберите подключенный носитель (если требуется установите сертификат на флэш-накопитель) или реестр и нажмите на кнопку «ОК» (Рисунок 6).

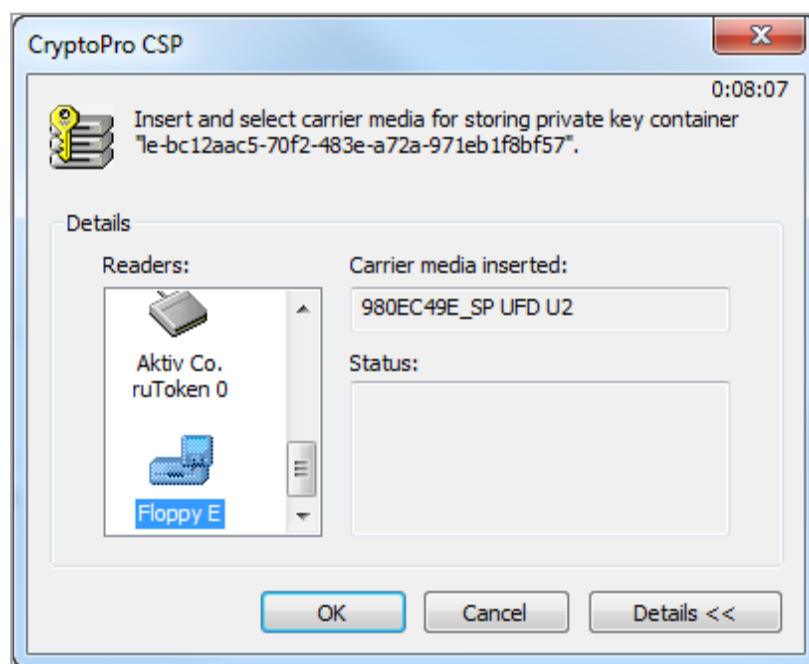


Рисунок 6 — Создание хранилища ключей

14. В диалоговом окне сгенерируйте ключ с помощью нажатия любых клавишей клавиатуры или движением курсора мыши в области окна (Рисунок 7).

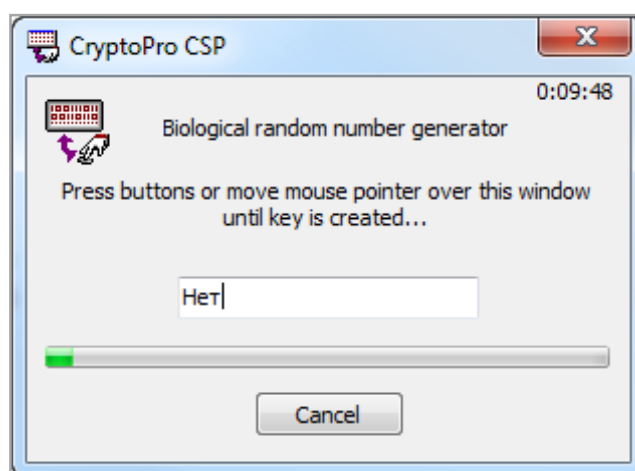


Рисунок 7 — Генерация ключа

15. Придумайте и введите пароль ЭЦП и нажмите на кнопку «ОК», если потребует Система (Рисунок 8).

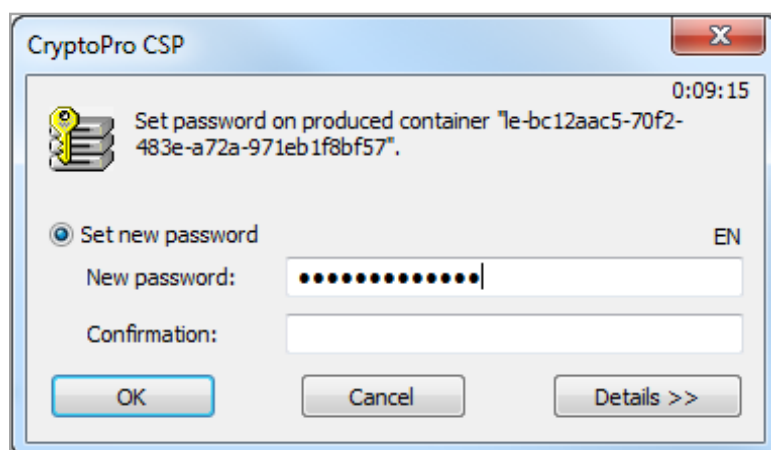


Рисунок 8 — Ввод пароля ЭЦП

16. Подтвердите действие в открывшемся окне (Рисунок 9).

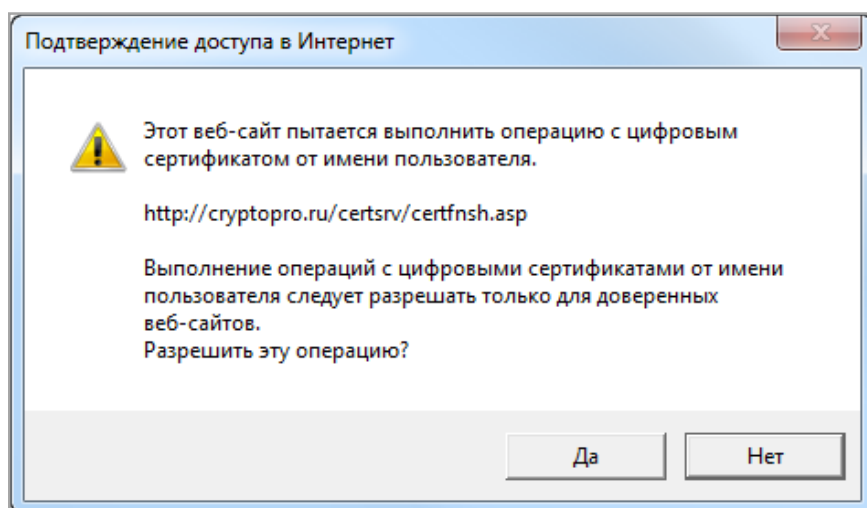


Рисунок 9 — Подтверждение действия

4.1.3 Установка сертификата

— После получения сертификата (см. пункт 4.1.2) в браузере перейдите по ссылке «Установить сертификат» (Рисунок 10).

Примечание

На данном этапе система может предложить установить сертификат от самого Test Center CRYPTO-PRO — в это случае скачайте его с расширением «*.crt» и установите.

17. Если сертификат не является доверенным, добавьте его в доверенные, перейдя по ссылке «установите этот сертификат ЦС» (Рисунок 10).

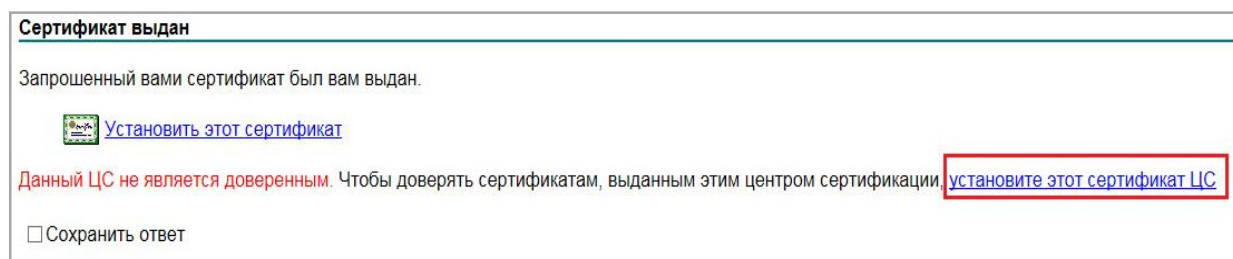


Рисунок 10 — Установка сертификата

18. В открывшемся диалоговом окне информации о сертификате нажмите на кнопку «Install Certificate...» (Рисунок 11).

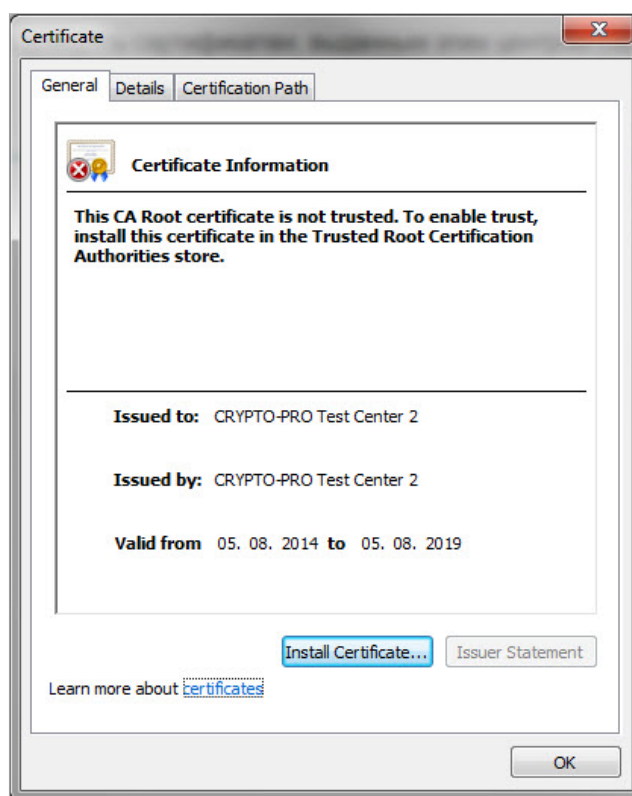


Рисунок 11 — Сведения о сертификате

19. В диалоговом окне импорта сертификата на первом шаге импорта нажмите на кнопку «Next» (Рисунок 12).



Рисунок 12 — Импорт сертификата. Шаг 1

20. На втором шаге укажите путь установки с помощью кнопки «Browse...» (Рисунок 13) и проводника (Рисунок 14) и снова нажмите на кнопку «Next».

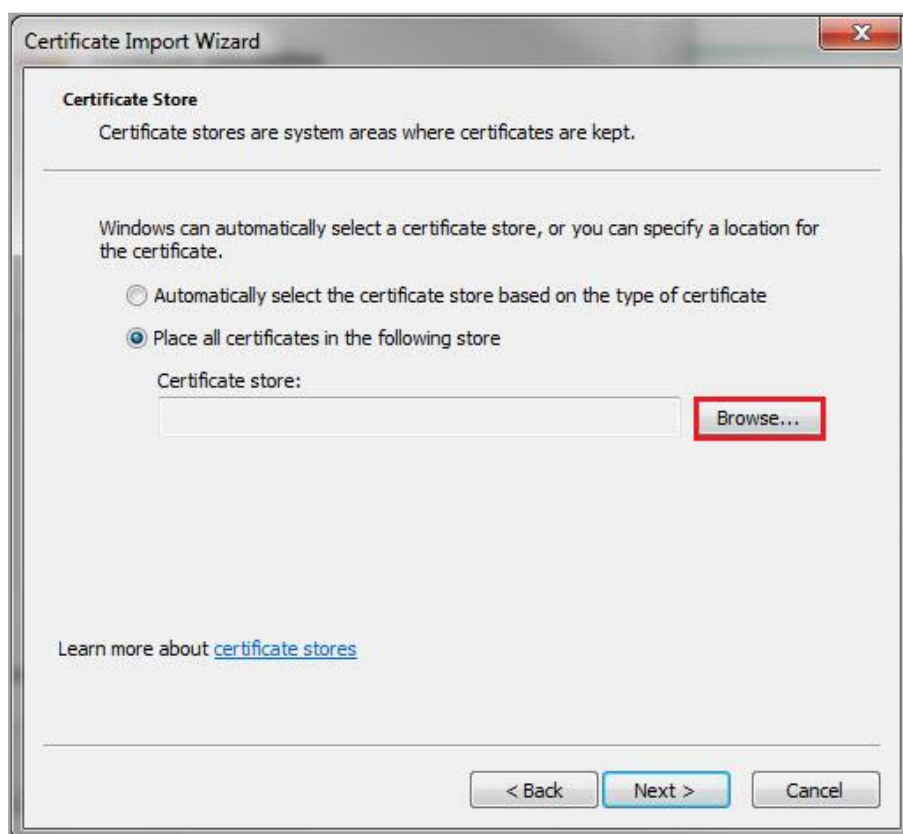


Рисунок 13 — Импорт сертификата. Шаг 2

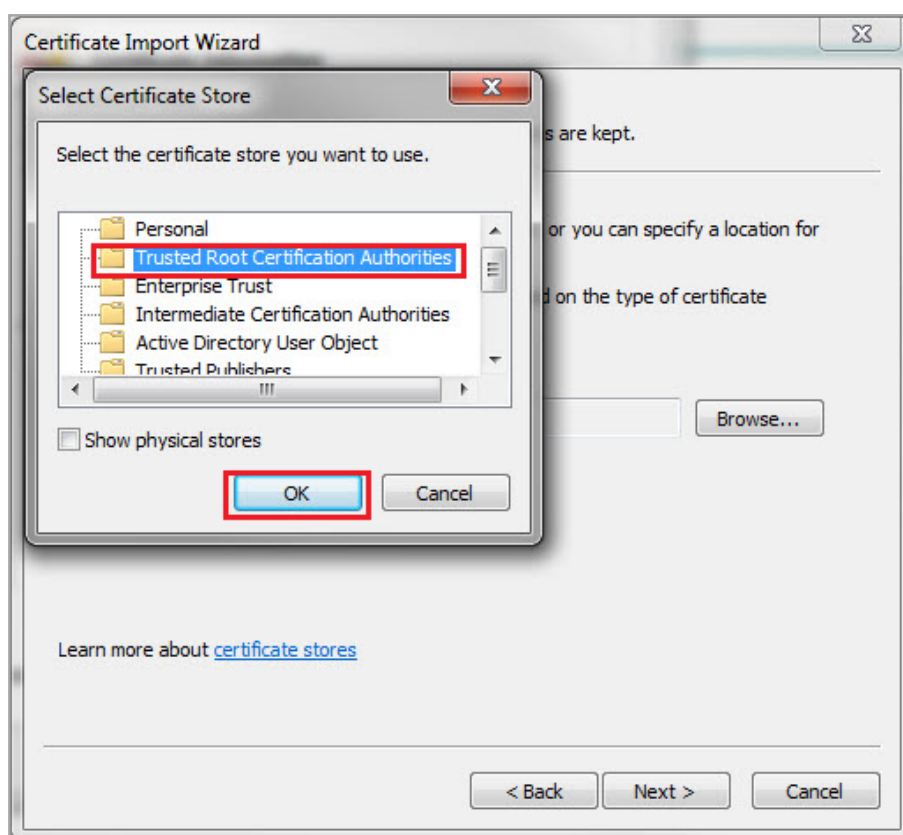


Рисунок 14 — Импорт сертификата. Выбор папки

21. На шаге 3 кнопкой «Finish» завершите импорт (Рисунок 15).

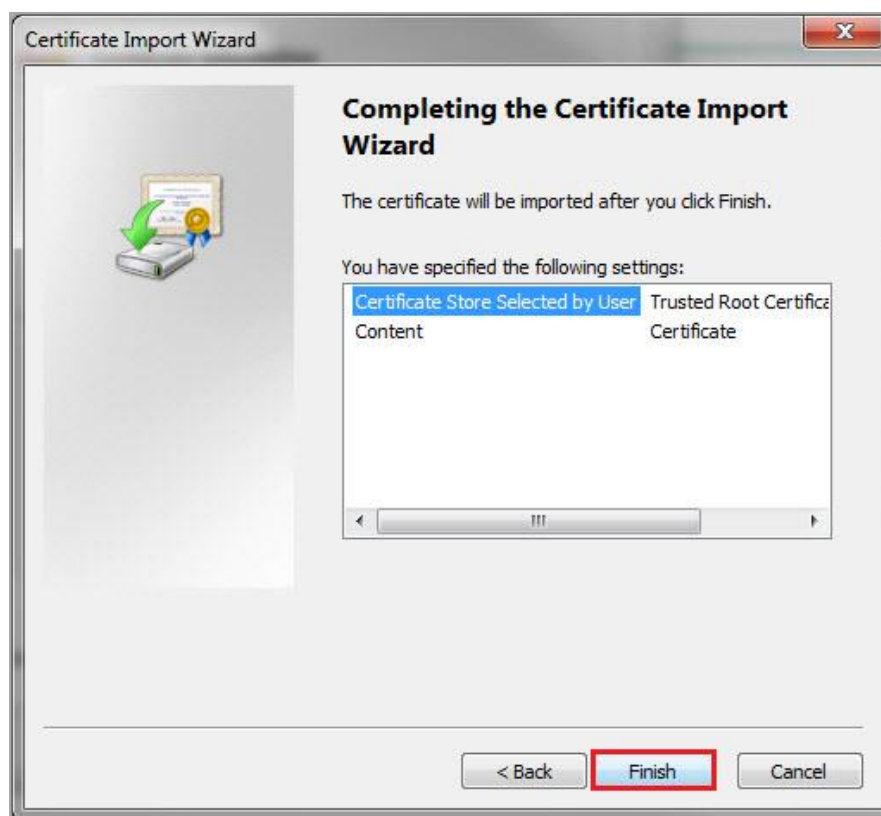


Рисунок 15 — Импорт сертификата. Шаг 3

22. В диалоговом окне предупреждения подтвердите установку данного сертификата (Рисунок 16).

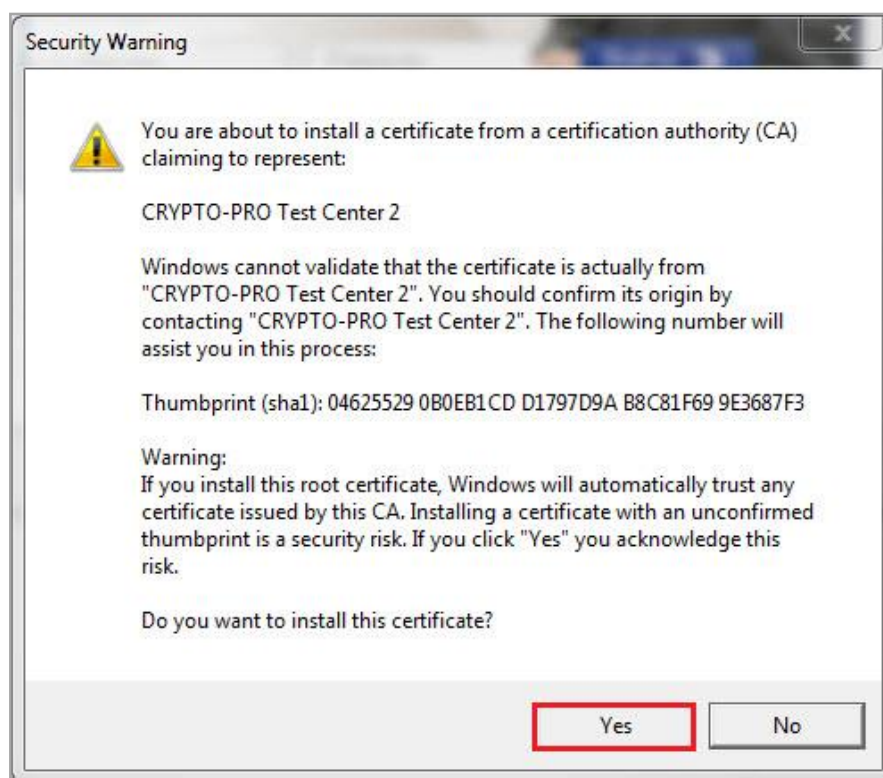


Рисунок 16 — Подтверждение установки сертификата

23. После успешного импорта отобразится соответствующее сообщение (Рисунок 17).



Рисунок 17 — Информация об успешном импорте

24. При успешном импорте сертификата установите его: в браузере отобразится ссылка «Установить этот сертификат», по которой необходимо перейти для установки (Рисунок 18).

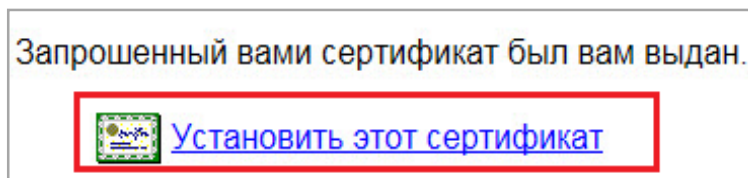


Рисунок 18 — Ссылка «Установить этот сертификат»

25. В открывшемся диалоговом окне введите ранее придуманный пароль (Рисунок 19). Он же будет использоваться и при подписании файлов на портале.

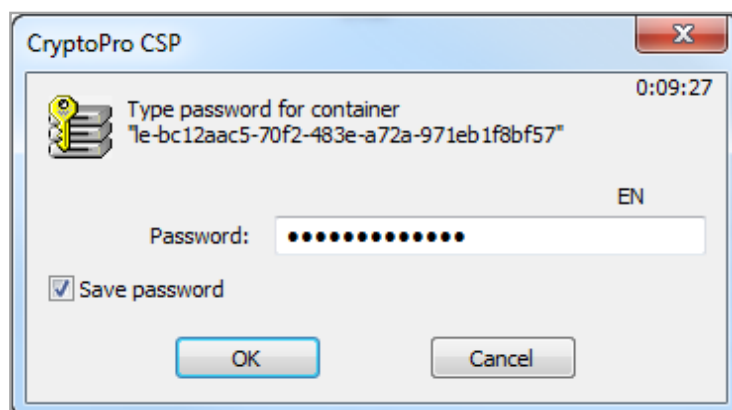


Рисунок 19 — Окно ввода пароля

26. В результате в браузере отобразится сообщение об успешной установке сертификата (Рисунок 20).

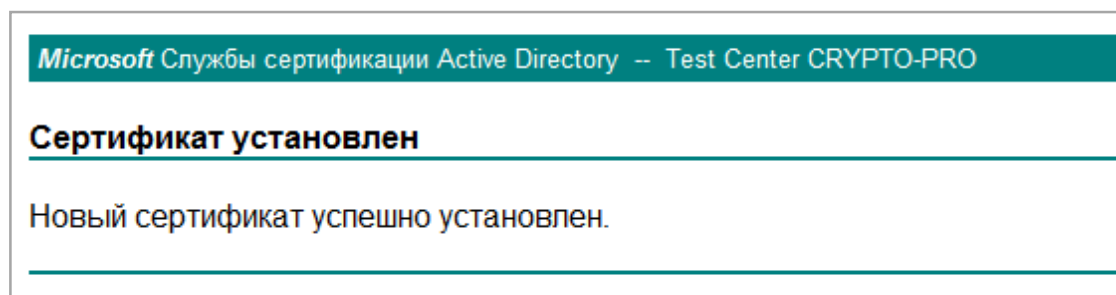


Рисунок 20 — Подтверждение установки сертификата

4.1.4 Настройка плагина

При необходимости для корректной работы следует настроить ЭЦП Browser Plug-in.

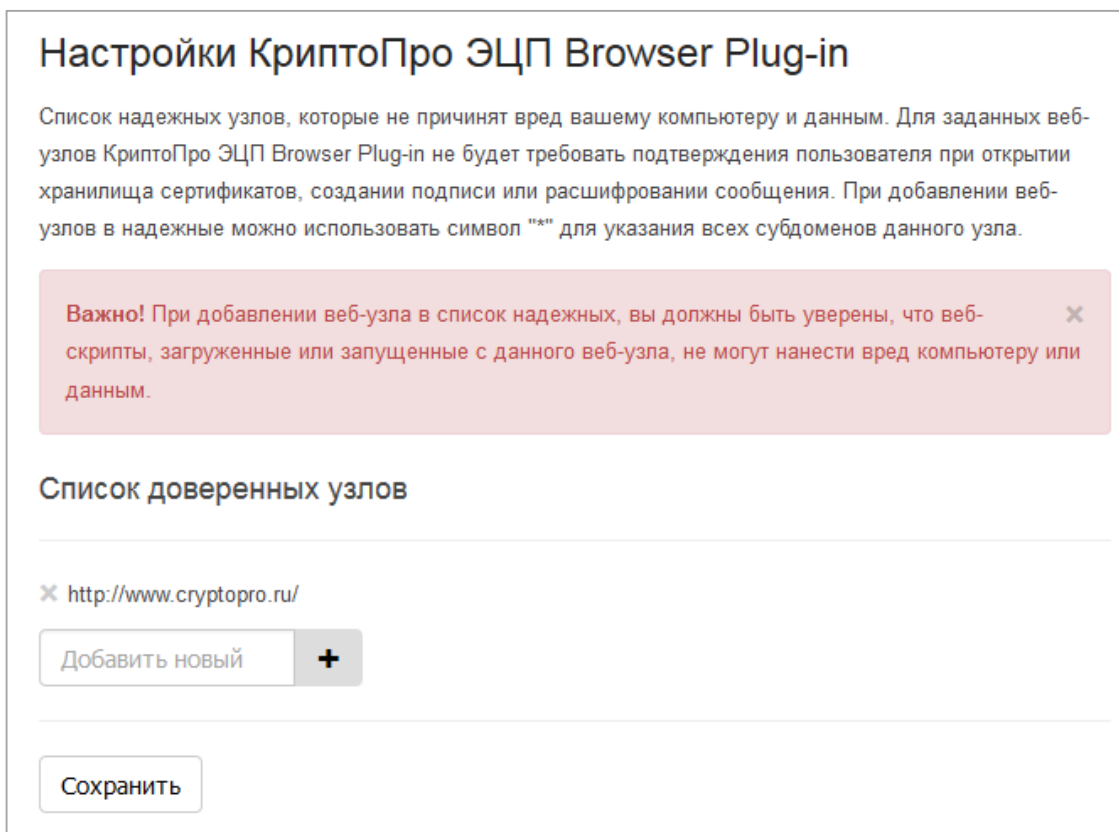
Настройка плагина:

1. Откройте меню «Пуск» → «Все программы» → «КРИПТО-ПРО» → «Настройки ЭЦП Browser Plug-in».

27. Введите URL в поле «Добавить новый» (Рисунок 24).

28. Нажмите на кнопку «+».

4. После добавления всех узлов нажмите на кнопку «Сохранить».



Настройки КриптоПро ЭЦП Browser Plug-in

Список надежных узлов, которые не причинят вред вашему компьютеру и данным. Для заданных веб-узлов КриптоПро ЭЦП Browser Plug-in не будет требовать подтверждения пользователя при открытии хранилища сертификатов, создании подписи или расшифровании сообщения. При добавлении веб-узлов в надежные можно использовать символ "*" для указания всех субдоменов данного узла.

Важно! При добавлении веб-узла в список надежных, вы должны быть уверены, что веб-скрипты, загруженные или запущенные с данного веб-узла, не могут нанести вред компьютеру или данным. ✕

Список доверенных узлов

✕ http://www.cryptopro.ru/

Добавить новый **+**

Сохранить

Рисунок 21 — Настройки плагина КриптоПро

5 АВАРИЙНЫЕ СИТУАЦИИ

5.1 Действия в случаях несоблюдения технологического процесса

При неверных действиях пользователей, неверных форматах или недопустимых значениях входных данных для пользователя отображаются соответствующие сообщения, после чего возвращается в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

5.2 Действия по восстановлению программ при сбойных ситуациях и ошибках в данных

При ошибках в работе аппаратных средств (кроме носителей, данных и программ), а также при продолжительных обрывах связи восстановление функции системы возлагается на ОС. Для восстановления работоспособности клиентской части системы достаточно войти в систему заново.

При ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на ОС. При невозможности восстановления работы системы следует действовать в соответствии с должностной и иными инструкциями.

5.3 Действия в случаях несанкционированного доступа к данным

В случае обнаружения фактов несанкционированного доступа к данным, утери либо компрометации пароля для доступа к системе необходимо действовать в соответствии с должностной и иными инструкциями, регламентирующими действия по соблюдению информационной безопасности.

6 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Для работы с системой необходимо ознакомиться с настоящим руководством («Руководство администратора. Установка системы»).