Система электронного документооборота

Настройка КриптоПро на Linux

(при использовании JDK 8)

Памятка Администратора

Версия 4.x и выше

г. Самара,

2022

Оглавление

1. Настройка КриптоПро на Linux (сервер)

1.1. Лицензия КриптоПро в Системе

Перед настройкой необходимо убедиться, что в лицензии системы ТЕЗИС включена «Интеграция с КриптоПро».

Проверить лицензию можно в системе ТЕЗИС в пункте меню «Помощь» – «О программе».

При отсутствии лицензии следует обратиться в техническую поддержку.

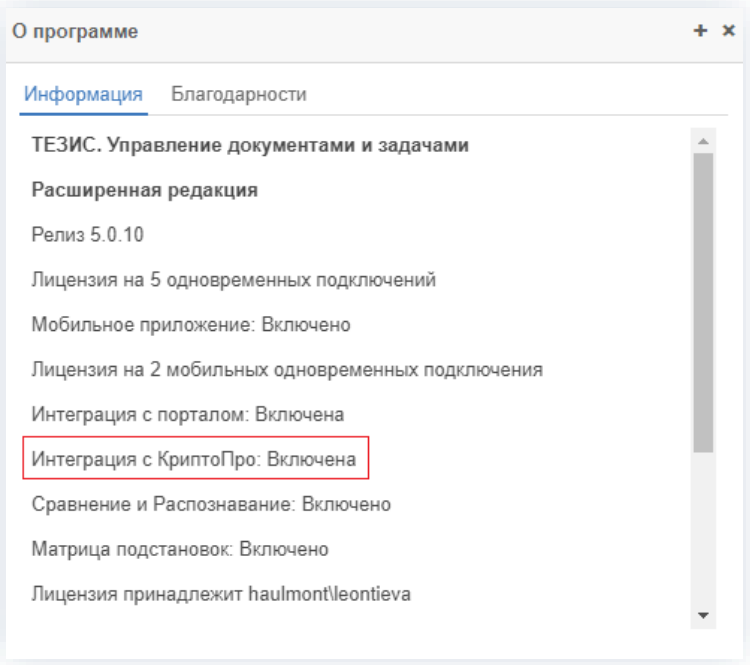


Рисунок 1. Настройка параметров на вкладке «Java»

1.2. Лицензия КриптоПро JCP

К моменту настройки на сервере должна быть приобретена лицензия КриптоПро JCP.

Серийныйномер лицензии и имя компании потребуется при установке JCP.

Срок использования демонстрационной версии КриптоПро JCP ограничен 90 днями с момента установки.

Существует возможность добавления лицензии после установки ПО.

Возможно использовать серверную или клиентскую лицензии.

Серверная лицензия КриптоПро JCP используется в случаях, если:

- используется Java TLS (данное ПО используется для поддержки защищённого обмена данными в Internet);
- JCP устанавливается на серверную платформу (Windows Server, Solaris, AIX и прочие платформы, которые позиционируются, как серверные).

Клиентская лицензия КриптоПро JCP используется в случаях, если:

- Java TLS не используется (система ТЕЗИС не использует Java TLS);
- сама ОС позволяет поставить клиентскую лицензию JCP.

Проверка требуемой лицензии может быть выполнена следующей командой (при установленном КриптоПро JCP):

```
java ru.CryptoPro.JCP.tools.License -required
```

Результат выполнения выдаст строки вида:

```
OS type: Server OS
Required license: not less than 4 cores
Или
OS type: Клиентская ОС
Required license: лицензия на право использования на одном рабочем месте
```

1.3. Настройка в интерфейсе

Для работы с электронной подписью в Системе в пункте меню «Администрирование» – «Системные параметры» – «Общие» должен быть отмечен чек-бокс «Использовать ЭЦП».

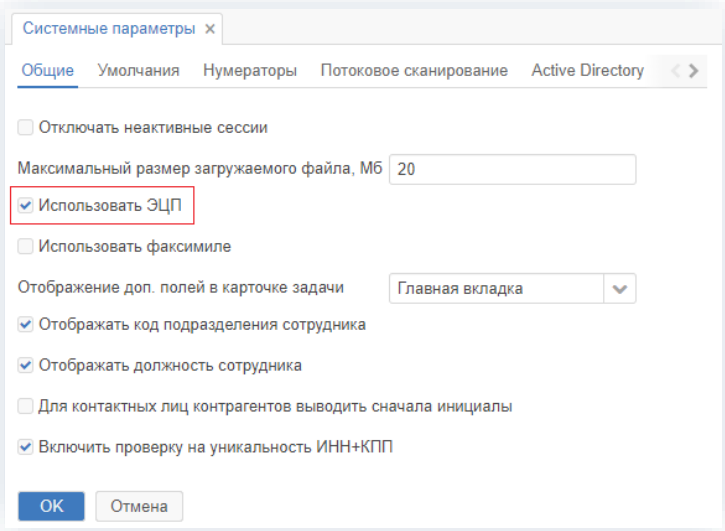


Рисунок 2. Чек-бокс «Использовать ЭЦП»

1.4. Настройка в конфигурационных файлах

Прописать настройки в конфигурационные файлы «\tomcat\conf\app\local.web-app.properties» и «\tomcat\conf\app-core\local.app.properties»:

- thesis.userSignatureTypeDefault=CryptoPro – для версии СЭД ТЕЗИС 4.2 и выше;
- thesis.signatureSupport=CryptoPro – для версии СЭД ТЕЗИС 4.1.

1.5. Проверка установленной JDK

Перед настройкой нужно проверить значение переменной «JAVA_HOME».

Для этого необходимо на сервере выполнить команду:

```
java -version
```

```
vob@vob-vb:~$ java -version
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.191-b12, mixed mode)
```

Рисунок 3. Проверка JDK

Путь до указанной JDK можно определить в Системе через пункт меню «Администрирование» – «Консоль JMX» – «java.lang:type=Runtime» атрибут «BootClassPath».

Рисунок 4. Проверка JDK

Таким образом путь к установленной JDK может иметь следующий вид: «\usr\lib\jvm\jdk1.8.0_191».

> ***Примечание:***
>
> *Установка JCP должна обязательно осуществляться в JRE, которая используется для СЭД ТЕЗИС.*

1.6. Установка КриптоПро JCP

Установка JCP (https://www.cryptopro.ru) должна осуществляться в JRE, которая используется для СЭД ТЕЗИС.

Например, в случае использования системой ТЕЗИС «JAVA_HOME» пути вида «\usr\lib\jvm\jdk1.8.0_191» приустановке КриптоПро JCP необходимо выбрать путь вида «\usr\lib\jvm\jdk1.8.0_191\jre».

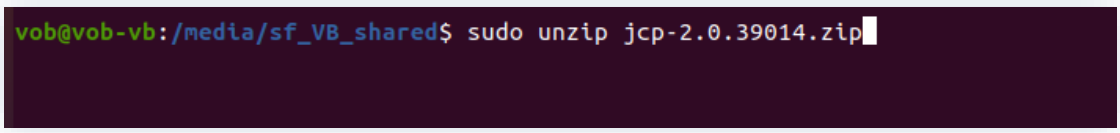


Рисунок 5. Распаковка архива

Необходимые действия:

1. Распаковать архив дистрибутива JCP командой:

   sudo unzip jcp-2.0.38481.zip

2. Перенести папку «jcp-2.0.38481» в папку «opt\haulmont» и сделать в ней файлы формата *.sh исполняемыми командой:

*sudo chmod +x *.sh.*

```
vob@vob-vb:/opt/haulmont$ cd /opt/haulmont/jcp-2.0.39014
vob@vob-vb:/opt/haulmont/jcp-2.0.39014$ sudo chmod +x *.sh
```

Рисунок 6. Добавление команды на исполняемые файлы

3. Выполнить установку в папке «\jcp opt\haulmont -2.0.38481» командой:

sudo ./ setup_console.sh /usr/lib/jvm/jdk1.8.0_191/jre [<серийный_номер> <имя_компании>]

где «usr\lib\jvm\jdk1.8.0_191\jre» – путь к JRE, используемой СЭД ТЕЗИС.

```
vob@vob-vb:/opt/haulmont/jcp-2.0.39014$ sudo ./setup_console.sh /usr/lib/jvm/jdk1.8.0_191/jre
Params: /usr/lib/jvm/jdk1.8.0_191/jre
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.191-b12, mixed mode)
Current distributive directory: /opt/haulmont/jcp-2.0.39014
Current executable JRE: /usr/lib/jvm/jdk1.8.0_191/jre
** Crypto-Pro Installer, 2005-2020 **
** Expected actions: -install or -uninstall or press enter **
Enter operation type [-install - press Enter]:-install
------ Installation ------
Choose JRE[current JRE - press Enter]:/usr/lib/jvm/jdk1.8.0_191/jre
------
Java Cryptographic Provider[yes - press Enter]:yes
Encryption module[yes - press Enter]:yes
Card module for cards and tokens, requires OCF (deprecated)[no - press Enter]:no
Card module for cards and tokens[no - press Enter]:no
Java TLS Provider[no - press Enter]:no
CAdES, XAdES modules (acquire bouncycastle: bc*-jdk15on-1.50)[no - press Enter]:yes
```

Рисунок 7. Установка JCP

4. Выбрать в мастере установки JCP только опции: «Криптопровайдер JCP», «Модули CAdES, XAdES, требуют bouncycastle: bc*-jdk15on-1.50».

Остальные параметры – по умолчанию.

Включать усиленный контроль использования ключей не следует.

5. Проверить корректность выставленных настроек и завершить установкуКриптоПро JCP.

Рисунок 8. Завершение установки JCP

Необходимые действия выполнены.

1.7. Работа с библиотеками приложения

Из папки с дистрибутивом КриптоПро «…\jcp-2.0.38481\dependencies» в папку «$JRE_HOME\lib\ext» необходимо скопировать следующие библиотеки:

- bcpkix-jdk15on-1.50.jar,
- bcprov-jdk15on-1.50.jar.

В случае использования «JAVA_HOME» по пути вида «\usr\lib\jvm\jdk1.8.0_191» требуемый каталог (куда следует положить библиотеки) будет иметь путь вида «\usr\lib\jvm\jdk1.8.0_191\jre\lib\ext».

Из папки «\tomcat\shared\lib» удалить все библиотеки, начинающиеся на «bcmail-» и «bcprov-».

1.8. Импорт корневого сертификата в хранилище доверенных сертификатов

Необходимо импортировать корневой сертификат цепочки сертификатов (той, что используется для подписи) в DER-кодировке в хранилище доверенных сертификатов JRE «cacerts».

Для импорта сертификата используется команда:

```
keytool.exe -importcert -file "<PATH_TO_CA_CERT>" -alias -keystore "<PATH_TO_JRE>/lib/security/cacerts"
```

где:

- keytool – утилита в папке «$JAVA_HOME\bin»;
- PATH_TO_CA_CERT – путь к корневому сертификату;
- CERT_ALIAS –- алиас сертификата для установки в хранилище;
- PATH_TO_ JRE – место установки JRE.

Пароль для хранилища по умолчанию: changeit.

Команда выполняется из папки «\jdk...\jre\bin».

Необходимо добавить корневой и промежуточные сертификаты.

Для каждого сертификата, используется свой уникальный алиас.

Пример выполнения:

1. Перейти в папку «\usr\lib\jvm\jdk1.8.0_191\jre\bin».
2. Сертификат положить в эту же папку.
3. Выполнить команду:

keytool -importcert -file "certnew.cer" -alias GOST2012 -keystore "/usr/lib/jvm/jdk1.8.0_191/jre/lib/security/cacerts"

где:

- certnew.cer – корневой сертификат;
- GOST2012 – алиас сертификата для установки в хранилище (любой текст);
- /usr/lib/jvm/jdk1.8.0_191/jre/lib/security/cacerts – путь до cacerts необходимой JRE.

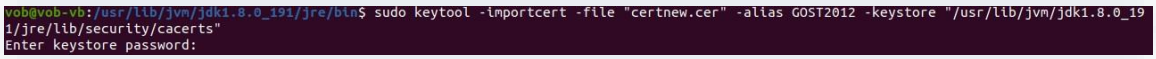


Рисунок 9. Добавление сертификата в хранилище

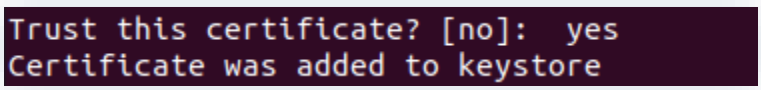


Рисунок 10. Сертификат добавлен в хранилище

1.9. Перезагрузка сервера

После внесения всех изменений выполнить полную перезагрузку сервера.

2. Настройка КриптоПро на Linux (клиент)

Для работы пользователя с электронной подписью в СЭД ТЕЗИС необходимо выполнить следующие действия:

1. Воспользоваться автоматическим инсталлятором КриптоПро для UNIX-систем по ссылке.

2. Установить КриптоПро ЭЦП Browser plug-in (версия>= 2.0.2051 с поддержкой Chrome без NPAPI).

   Информация по установке доступна по ссылке.

   Скачать актуальную версию можно по ссылке.

   Проверить работу плагина можно по ссылке.

3. Установить персональный сертификат.

   Доступные способы:

   - с помощью программы КриптоПро CSP

     Необходимые действия:

     1. Открыть КриптоПро CSP.
     2. Перейти на вкладку «Сервис» — «Установить личный сертификат».
     3. С помощью кнопки «Обзор» выбрать нужный сертификат пользователя.

        После выбора сертификата будут показаны его свойства.
     4. Нажать кнопку «Далее».
     5. Указать контейнер ключа, выбрав место хранилища «Личное».

        Установка личного сертификата пользователя завершена.

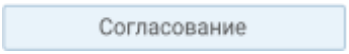
   - с помощью кнопки «Установить сертификат» в сертификате.

3. Проверка работы электронной подписи в системе ТЕЗИС

Использование электронной подписи в системе ТЕЗИС возможно в процессе согласования документов и договоров.

Пользователь при настройках внешнего вида Системы может указать тип электронной подписи.

Пользователь может согласовать документ, подписав вложения документа или договора с помощью ЭП.

Для проверки работы подписи в Системе необходимо создать карточку документа или договора, добавить вложения и запустить процесс «Согласование» (кнопка 

в карточке).

Важно!

Инициатор может определять какие из вложений должны быть подписаны. Если в документе существует иерархия вложений, то подписывается только основное вложение (или последняя версия, в зависимости от того, используется признак основного вложения или нет).

По умолчанию признак «Подписать ЭЦП» всегда устанавливается в новом вложении. Новое вложение не будет автоматически подписываться, если у него установлен соответствующий признак.

3.1. Подписание ЭП

Необходимые действия:

1. Откройте папку действий «Согласование», куда поступают все документы и договоры, направленные на согласование.
2. В открывшейся карточке в разделе действий нажмите на кнопку «Согласовать».

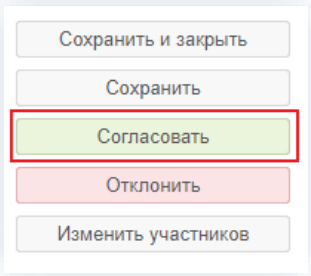


Рисунок 11. Выбор действия по документу или договору

Откроется окно добавления записи журнала действий.

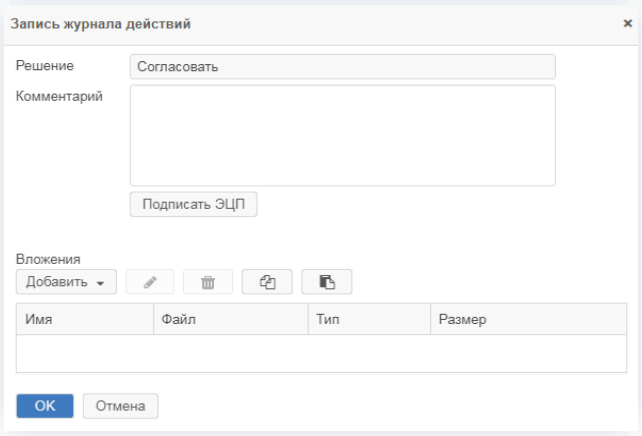


Рисунок 12. Запись журнала действий

3. В записи журнала действий в поле «Комментарий» при необходимости оставьте любые замечания или другую необходимую информацию.

4. При нажатии на кнопку Подписать ЭЦП выберите сертификат из списка.

ТЕЗИС не хранит и не имеет доступа к введенным паролям. Их обработкой занимается КриптоПро CSP.

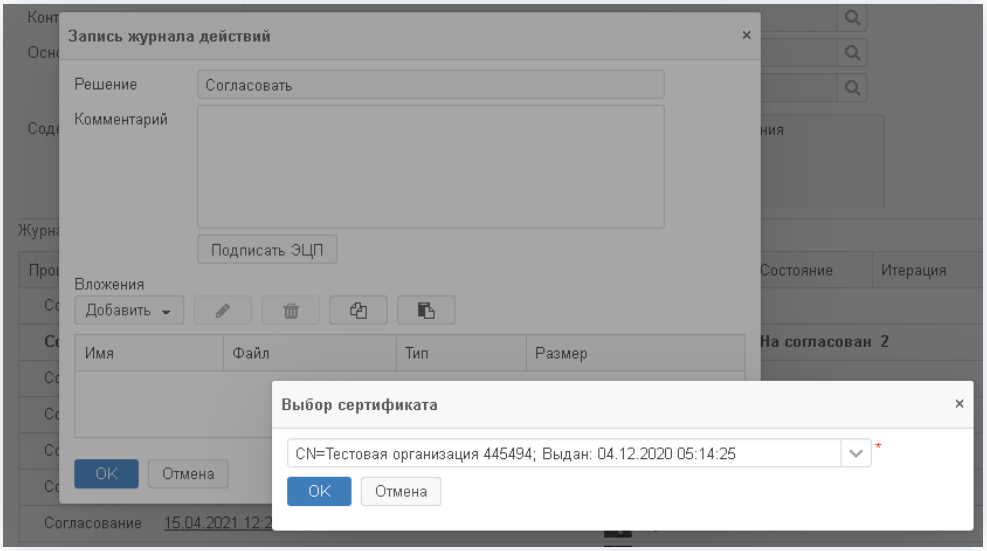


Рисунок 13. Выбор сертификата

5. Для подтверждения нажмите на кнопку OK.

При этом подписываются только вложения.

Если Инициатор не установил признак в столбце «Подписать ЭЦП», то данное вложение не будет подписываться.

Документ или договор согласован.

При возврате на доработку создается копия документа и все подписи убираются.

3.2. Просмотр ЭП

Посмотреть, какими подписями подписано вложение можно, нажав на гиперссылку «Просмотреть» в колонке «Цепочка сертификатов» таблицы вложений.

При нажатии на кнопку Просмотреть у вложения появляется информационное окно с перечислением всех подписей, сформированных для данного вложения.

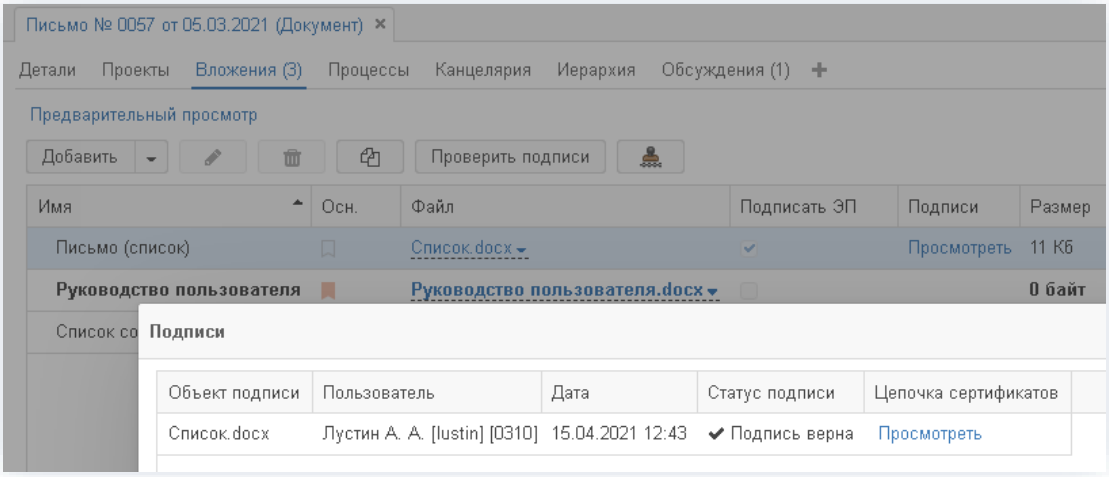


Рисунок 14. Просмотр подписи

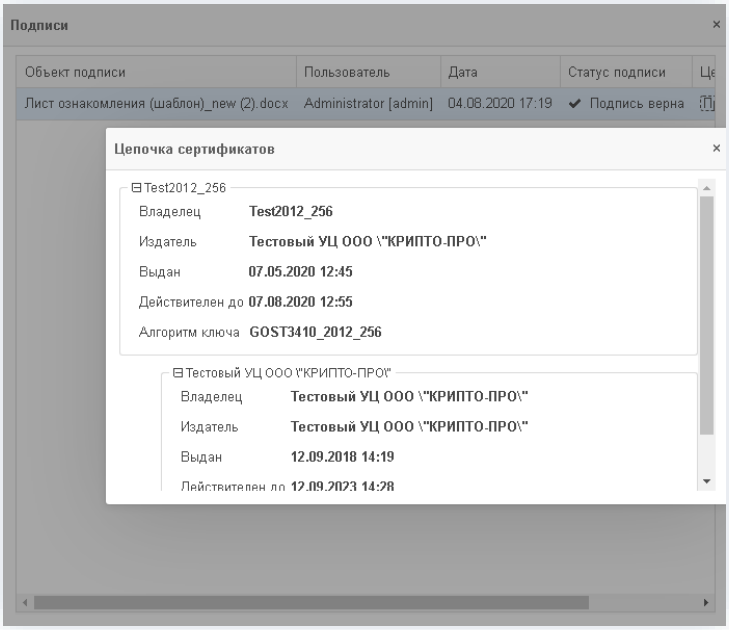


Рисунок 15. Просмотр цепочки сертификатов

Для проверки всех вложений на подлинность подписи требуется нажать на кнопку Проверить подписи на вкладке «Вложения».

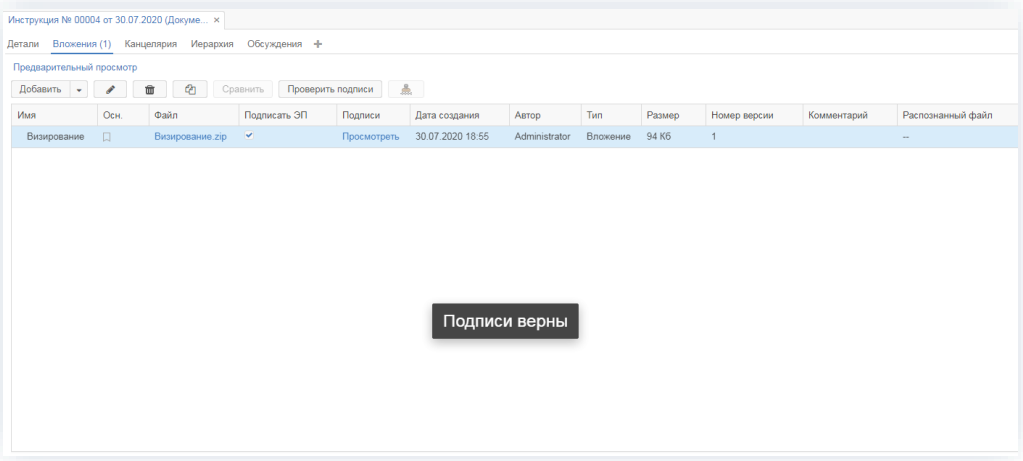


Рисунок 16. Проверка подписи

Если подпись верна, то пользователь увидит сообщение «Подписи верны».

Если подпись не верна, то в открывшемся окне «Подписи» будут указаны результаты проверки.

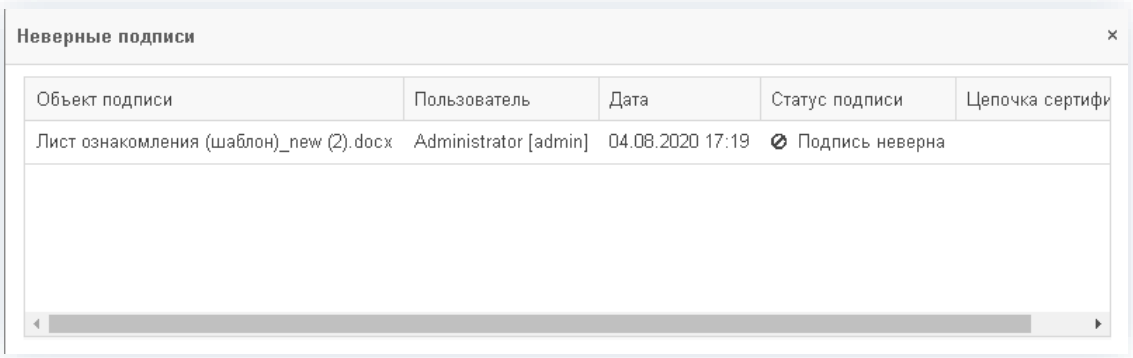


Рисунок 17. Проверка подписи

3.3. Сохранение ЭП

Пользователь может скачать контейнер, содержащий документ и подпись на вкладке «Вложения», нажав правой кнопкой мыши на вложении и выбрав пункт меню «Сохранить подписанное вложение».

При этом на сервере формируется множественная «attached CADES BASE» подпись из списка всех созданных detached-подписей. Таким образом подпись и сам документ объединяются в один контейнер, который может быть выслан, например, контрагенту.

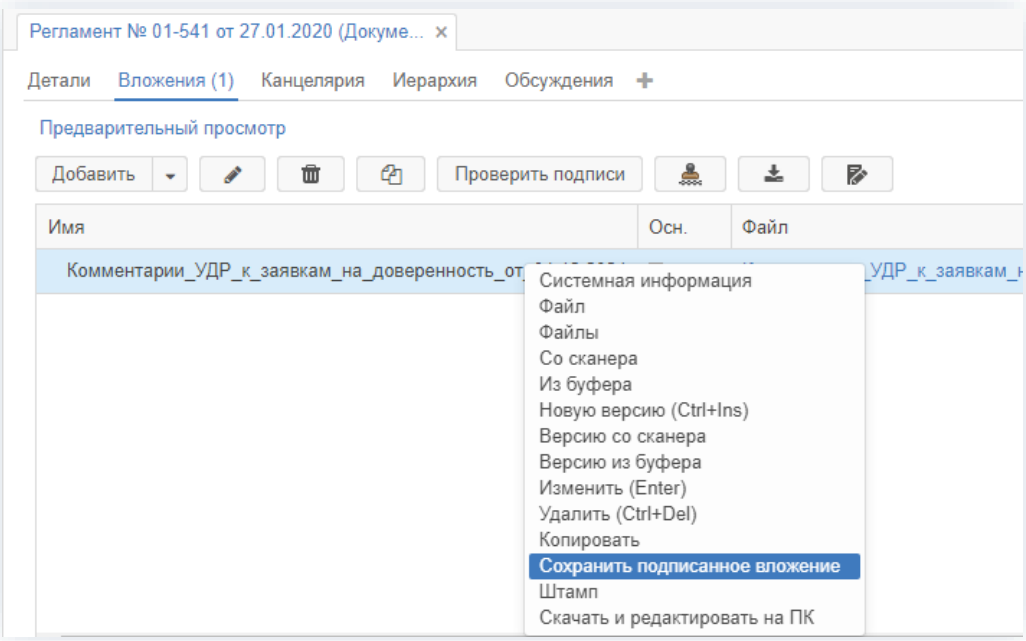


Рисунок 18. Сохранение подписанного вложения