Инструкция по работе с FTPS сервером Московской Биржи в тестовой среде

Оглавление

Подключение для автоматизированной загрузки отчётов

Адреса промышленного FTPS сервера

Доменное имя: ftps.moex.com

IP-адрес сервера в сети Интернет: 85.118.181.25

IP-адрес сервера для подключения через выделенную сеть: 91.203.252.70

Порт: 21, а также диапазон 49152–65534

В качестве данных аутентификации и авторизации используются имя пользователя и пароль для личного кабинета участника (ЛКУ).

Адрес сервера FTPS в сети Интернет для тестового подключения

IP-адрес тестового сервера: 91.208.232.211

Порт: 21, а также диапазон 49152–65534

Имя пользователя: ftps_for_test1

Пароль: t3E@4mYjE7

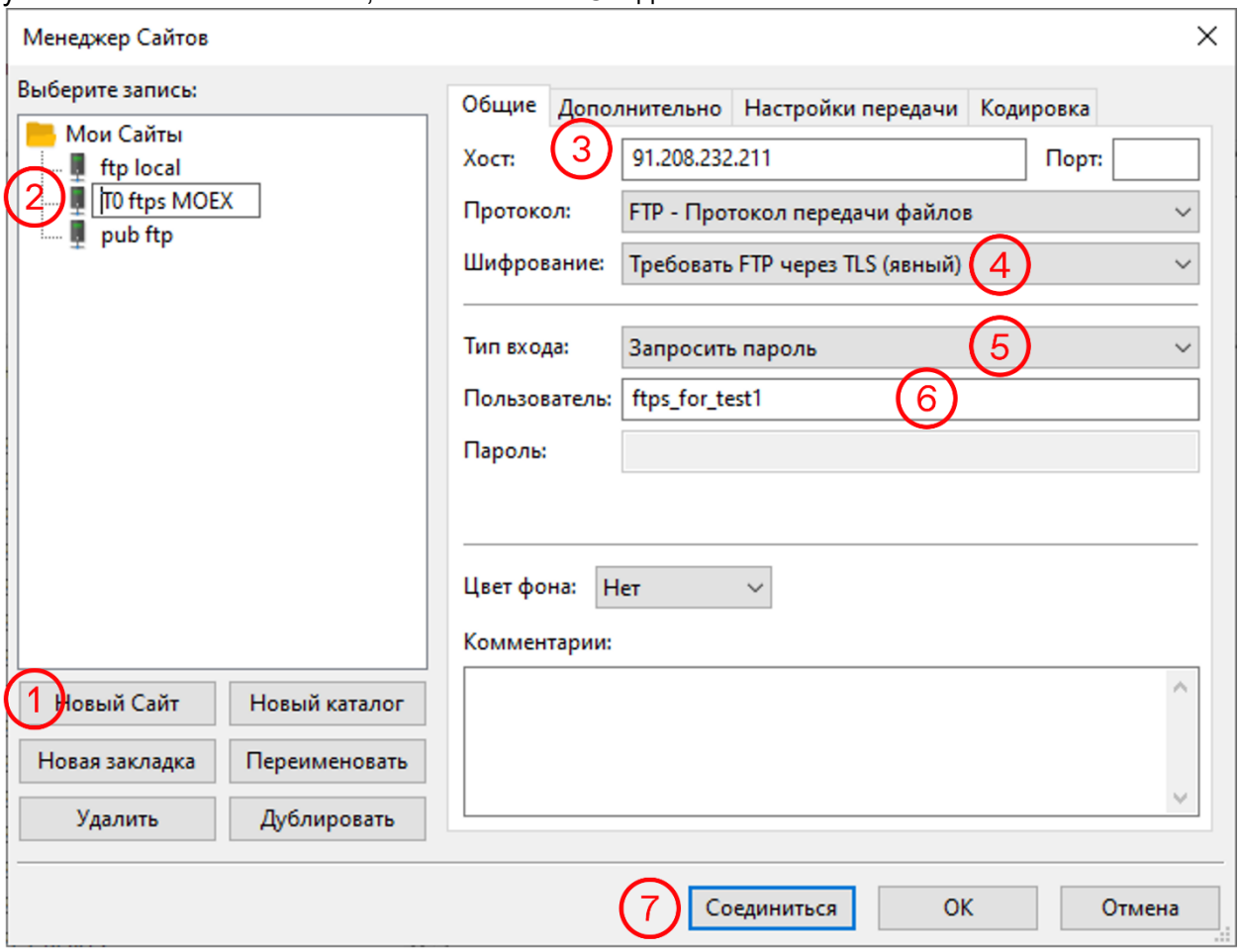
Для автоматизированной загрузки файлов отчётов используются стандартные команды протокола FTP. Потребуется установить защищённое соединение через TLS для передачи данных.

При появлении проблем с доступом к серверу обратитесь на help@moex.com

Подключение и загрузка файлов отчётов с помощью FTP-клиента

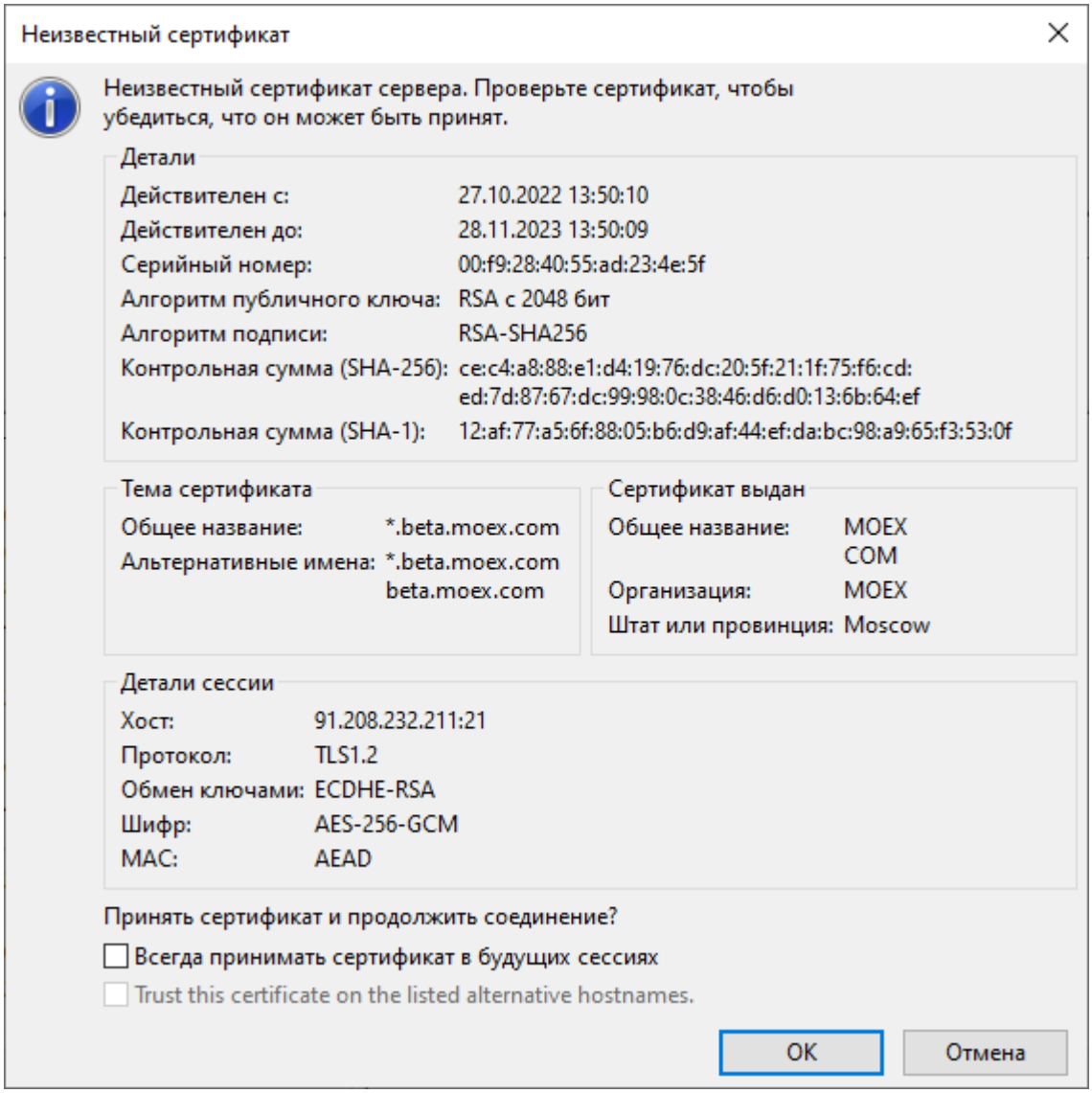
Для работы с сервером FTPS может использоваться любой FTP-клиент. Ниже на скриншотах приведён пример использования бесплатного клиента FileZilla для создания подключения и загрузки файлов с тестового сервера FTPS Московской биржи.

1. Запустите клиент FileZilla.
2. Нажмите иконку «Открыть менеджер сайтов». Откроется окно «Менеджер сайтов», где нужно заполнить данными поля для подключения к серверу, которые вы получили от службы технической поддержки.
3. 1 — добавьте новый сайт, 2 — введите имя для сайта, 3 — В поле Хост введите IP-адрес. 4 — выберите способ шифрования «Требовать FTP через TLS (явный)», чтобы устанавливать защищенное соединение, 5 — укажите тип входа «Запросить пароль», чтобы обеспечить неприкосновенность пароля и не сохранять его вместе с данными о подключении, 6 — укажите имя пользователя, 7 — нажмите «Соединиться».

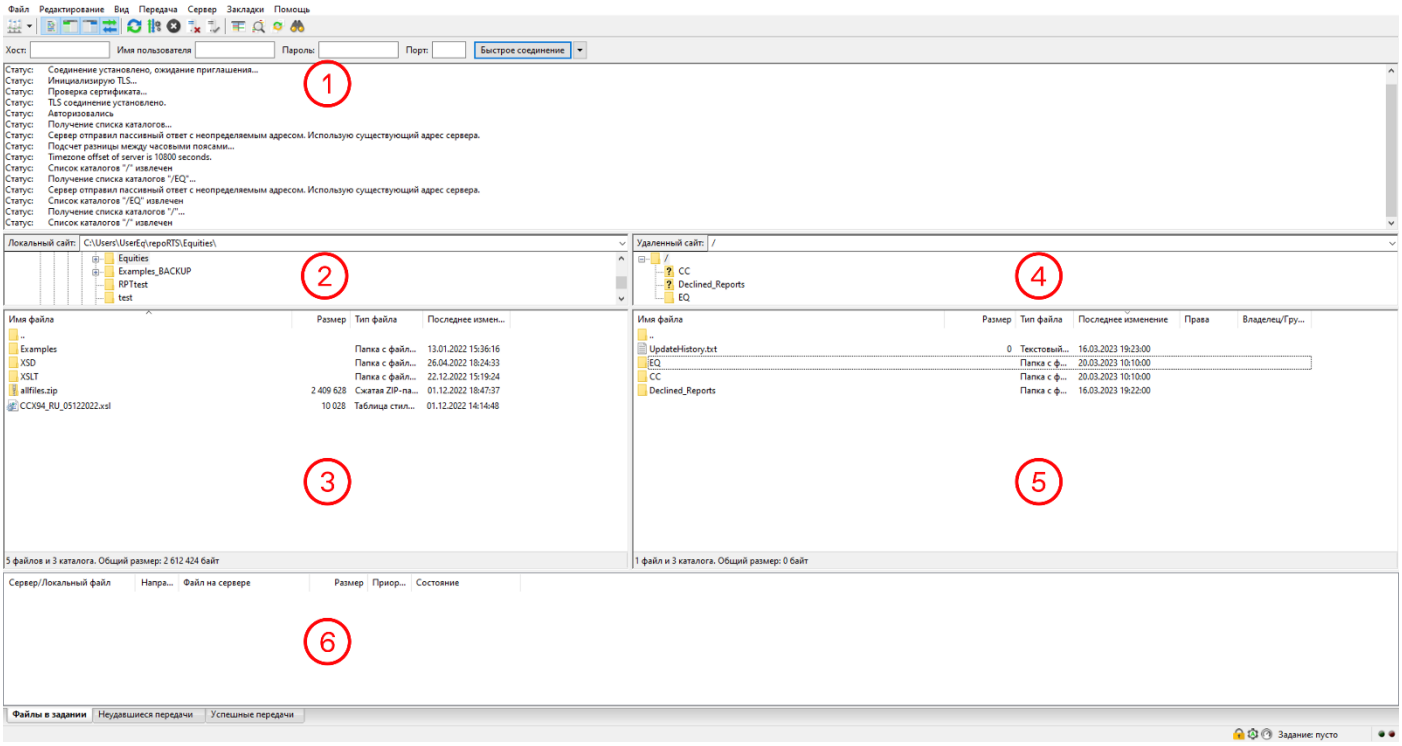


Используется стандартный порт для создания FTPS подключения: 21. Специально заполнять поле «Порт» не требуется. Тип сервера, Режим передачи, и Кодировка могут быть определены по умолчанию.

4. После того, как вы нажали «Соединиться», появится поле для ввода пароля при соединении.
5. Далее появится запрос на сохранение ключей и паролей по вашем усмотрению.
6. Если появится окно «Неизвестный сертификат», установите флажок рядом с «Всегда принимать сертификат в будущих сессиях» и нажмите «OK».



7. Подключитесь к серверу.



1 — область ведения журнала соединения. При возникновении ошибок во время работы с FTPS соединением, вы можете обратиться на help@moex.com и скопировать из этой области журнальные данные.

В правой области окна (2, 3) будет отображаться структура каталогов и файлы FTPS сервера. В левой части окна (4, 5) — папки и файлы вашего рабочего места. В правой части окна выберите папку, в которую вы хотите скопировать файл отчёта. Перейдите в нужную директорию на сервере и выберите файл отчёта, затем перетащите файл с помощью мыши в выбранную папку в левой половине окна.

6 — журнал процессов передачи файлов.

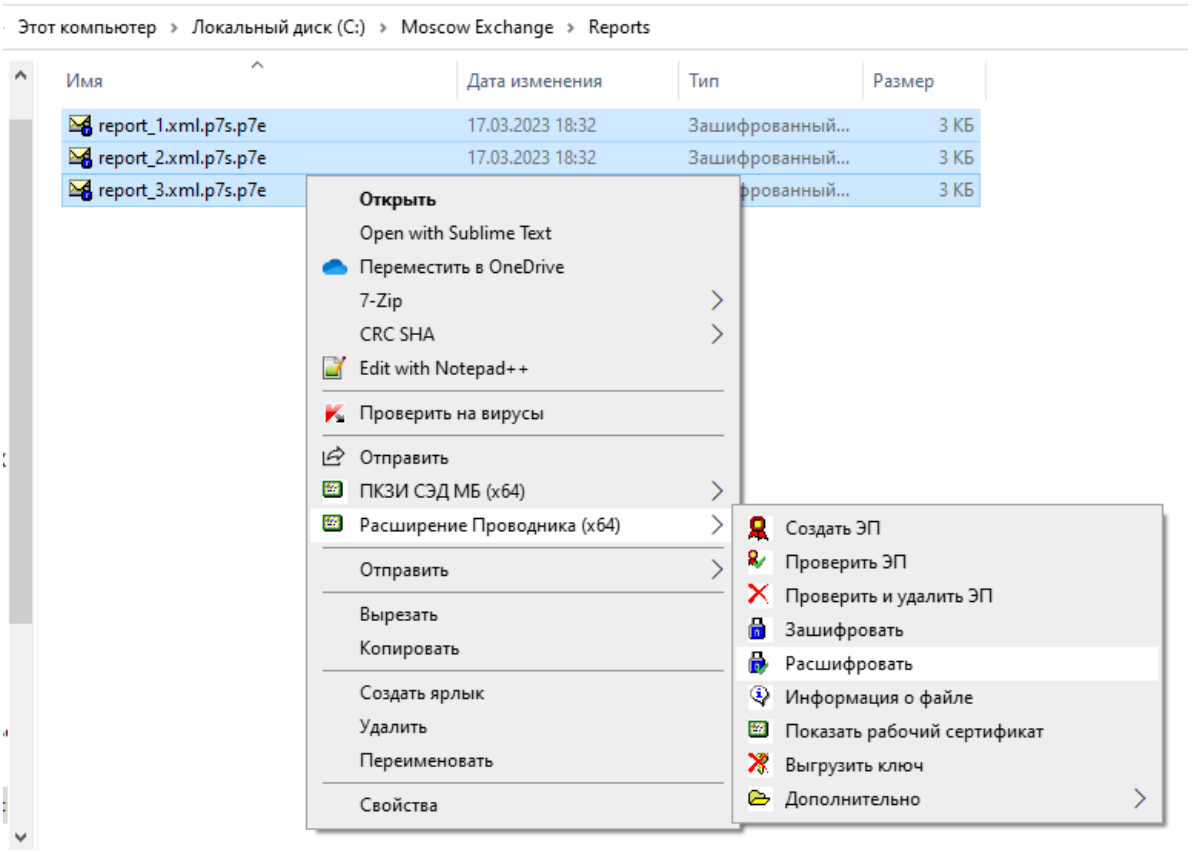
Расшифровка и снятие ЭЦП с полученного отчёта

Работа с использованием сертифицированных СКЗИ (ГОСТ криптография)

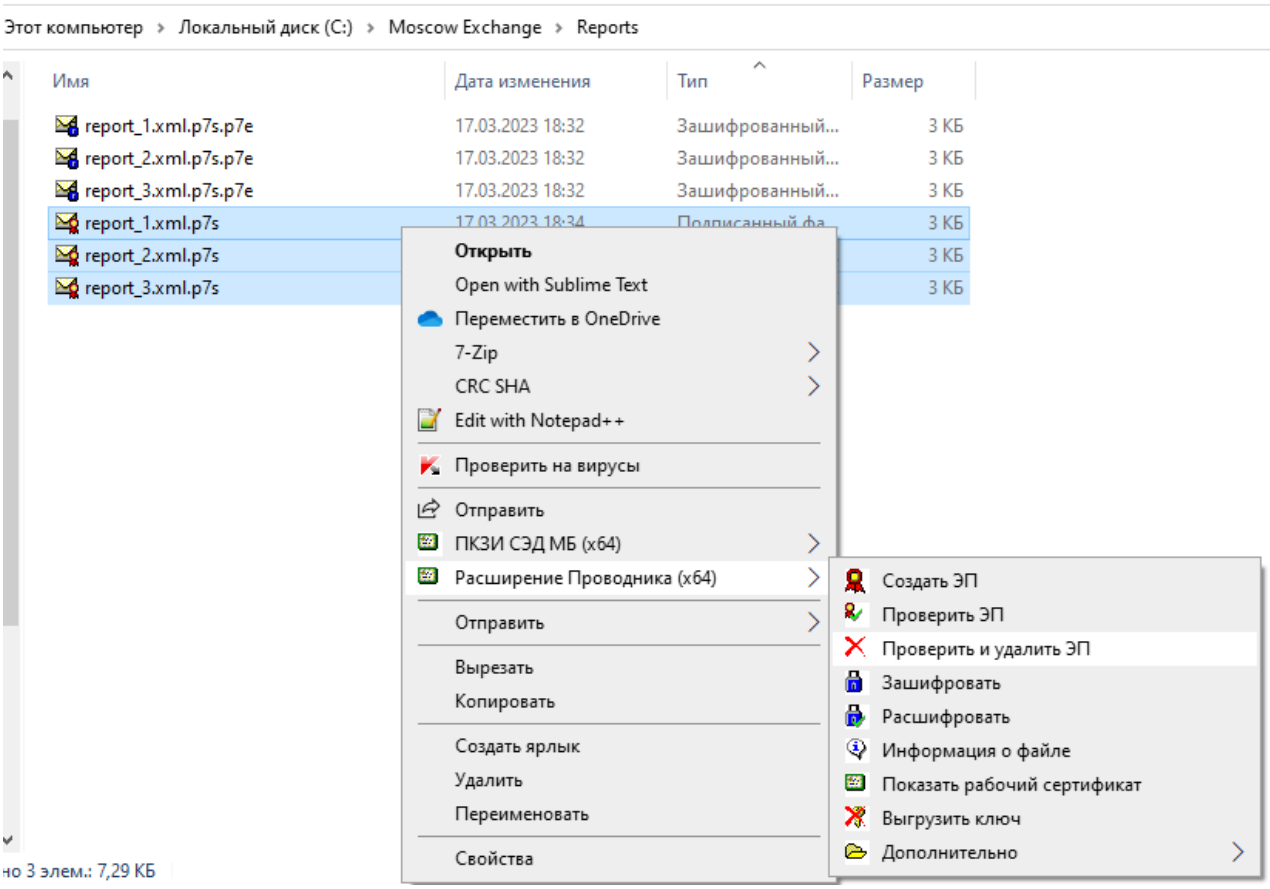
На рабочем месте должен быть установлен программный комплекс АПК «Валидата Клиент» и СКЗИ "Валидата CSP": http://moex.com/s1292

Операции расшифрования файлов и снятия ЭЦП можно производить помощью Расширения проводника:

Для расшифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Расшифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа.



Для того, чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Проверить и удалить ЭП»



Доступен также способ дешифрования через командную строку Windows:

1. Перейти в командную строку Windows: сочетание клавиш Win+R, затем в поле «Открыть» ввести cmd.
2. Произвести дешифрование файла с командой:

```
zpki1utl.exe -profile CLTEST1 -registry -decrypt -ldap -in
MC90000_CCX99_EQ1_16082022.p7f -out MC90000_CCX99_EQ1_16082022.p7s -recsubj
INN=009107775356
```

3. Произвести снятие электронной цифровой подписи с командой:

```
zpki1utl.exe -profile CLTEST1 -registry -verify -in
MC90000_CCX99_EQ1_16082022.p7s -delete 1 -out MC90000_CCX99_EQ1_16082022.xml
```

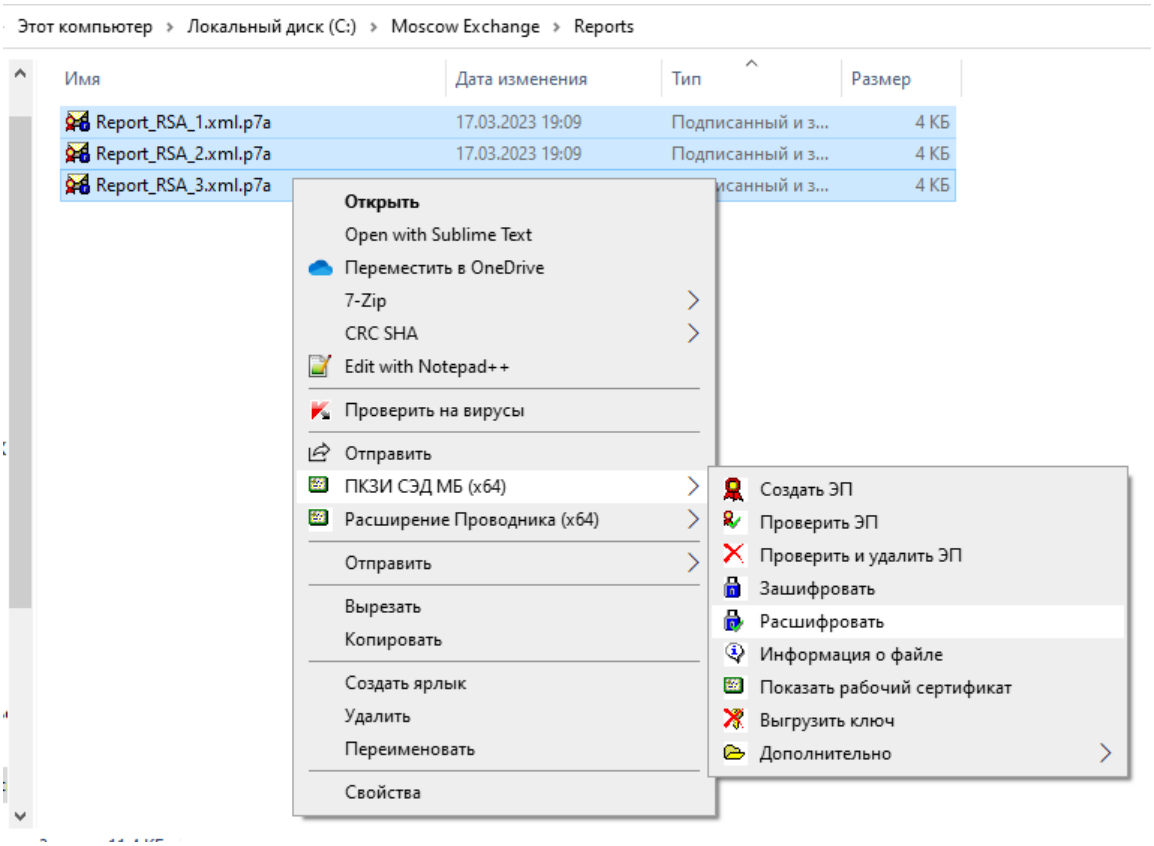
В указанных командах:
zpki1utl.exe – исполняемый файл утилиты, поставляемой с ПО «Справочник сертификатов», располагается по умолчанию в C:\Program Files\Validata\zpki
MC90000_CCX99_EQ1_16082022.p7f – зашифрованный файл отчёта полученный с FTPS сервера.
CLTEST1 – название профиля клиента в Справочнике сертификатов.
INN=009107775356 – указатель на сертификат специалиста Московской биржи, с помощью которого зашифрован файл, в сетевом справочнике сертификатов.

Обратите внимание, что в Справочнике сертификатов должен быть подключен сетевой справочник сертификатов:
ldap://simple/vcert.pki.moex.com:50005/C=RU

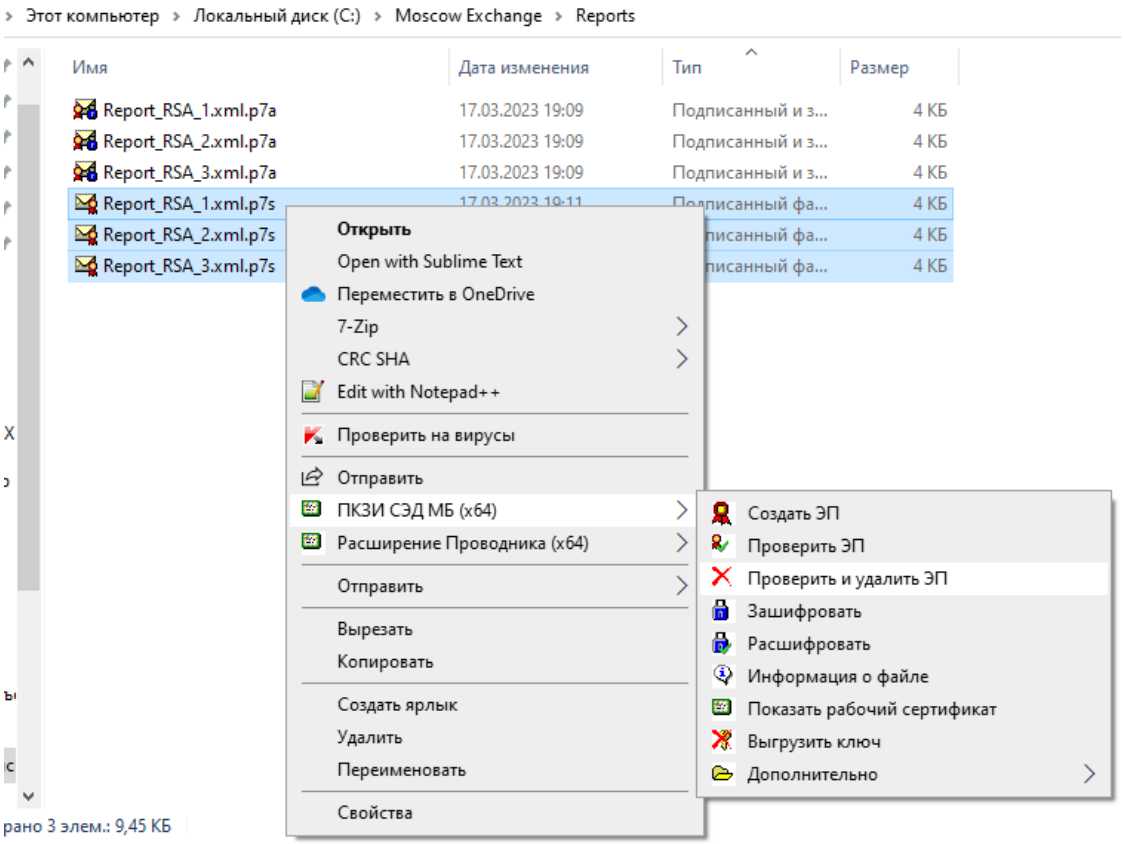
Работа с использованием несертифицированных СКЗИ (RSA криптография)
На рабочем месте должен быть установлен программный комплекс "ПКЗИ СЭД МБ": https://www.moex.com/s1293

Операции расшифрования файлов и снятия ЭЦП можно производить помощью Расширения проводника:

Для расшифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПКЗИ СЭД МБ пункт «Расшифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа.



Для того, чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПКЗИ СЭД МБ пункт «Проверить и удалить ЭП»



Доступен также способ дешифрования через командную строку Windows:

1. Распаковать архив xCertUtil.zip, полученный с сайта Московской Биржи: http://fs.moex.com/cdp/po/xCertUtil.zip
2. Перейти в командную строку Windows: сочетание клавиш Win+R, затем в поле «Открыть» ввести cmd.
3. Произвести дешифрование файла с командой:

```
rpki1utl.exe -profile CLTEST1 -registry -decrypt -ldap -in
MC90000_CCX99_EQ1_16082022.p7f -out MC90000_CCX99_EQ1_16082022.p7s -recsubj
INN=009107775356
```

4. Произвести снятие электронной цифровой подписи с командой:

```
rpki1utl.exe -profile CLTEST1 -registry -verify -in
MC90000_CCX99_EQ1_16082022.p7s -delete 1 -out MC90000_CCX99_EQ1_16082022.xml
```

В указанных командах:
rpki1utl.exe – исполняемый файл утилиты из пакета xCertUtil/pki1util.
CLTEST1 – название профиля клиента в Справочнике сертификатов.
MC90000_CCX99_EQ1_16082022.p7f – зашифрованный файл отчёта полученный с FTPS сервера.
INN=009107775356 – указатель на сертификат специалиста Московской биржи, с помощью которого зашифрован файл, в сетевом справочнике сертификатов.

Обратите внимание, что, в Справочнике сертификатов должен быть подключен сетевой справочник сертификатов:
ldap://simple/vcert.pki.moex.com:50007/C=RU