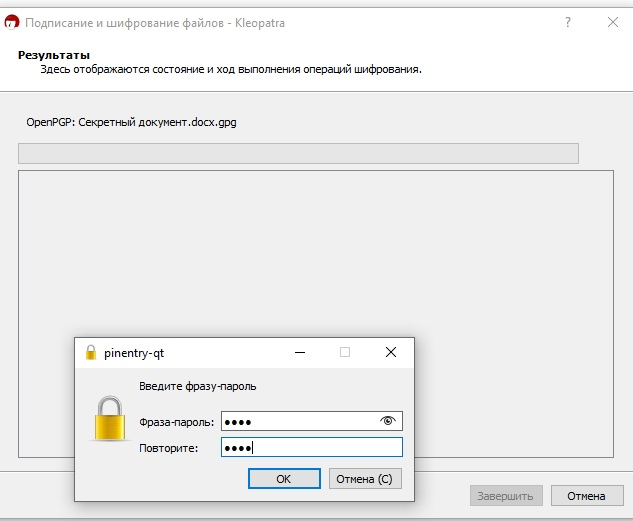
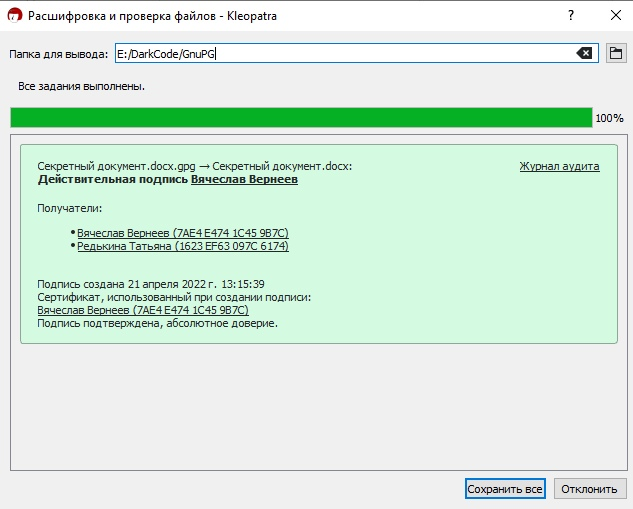
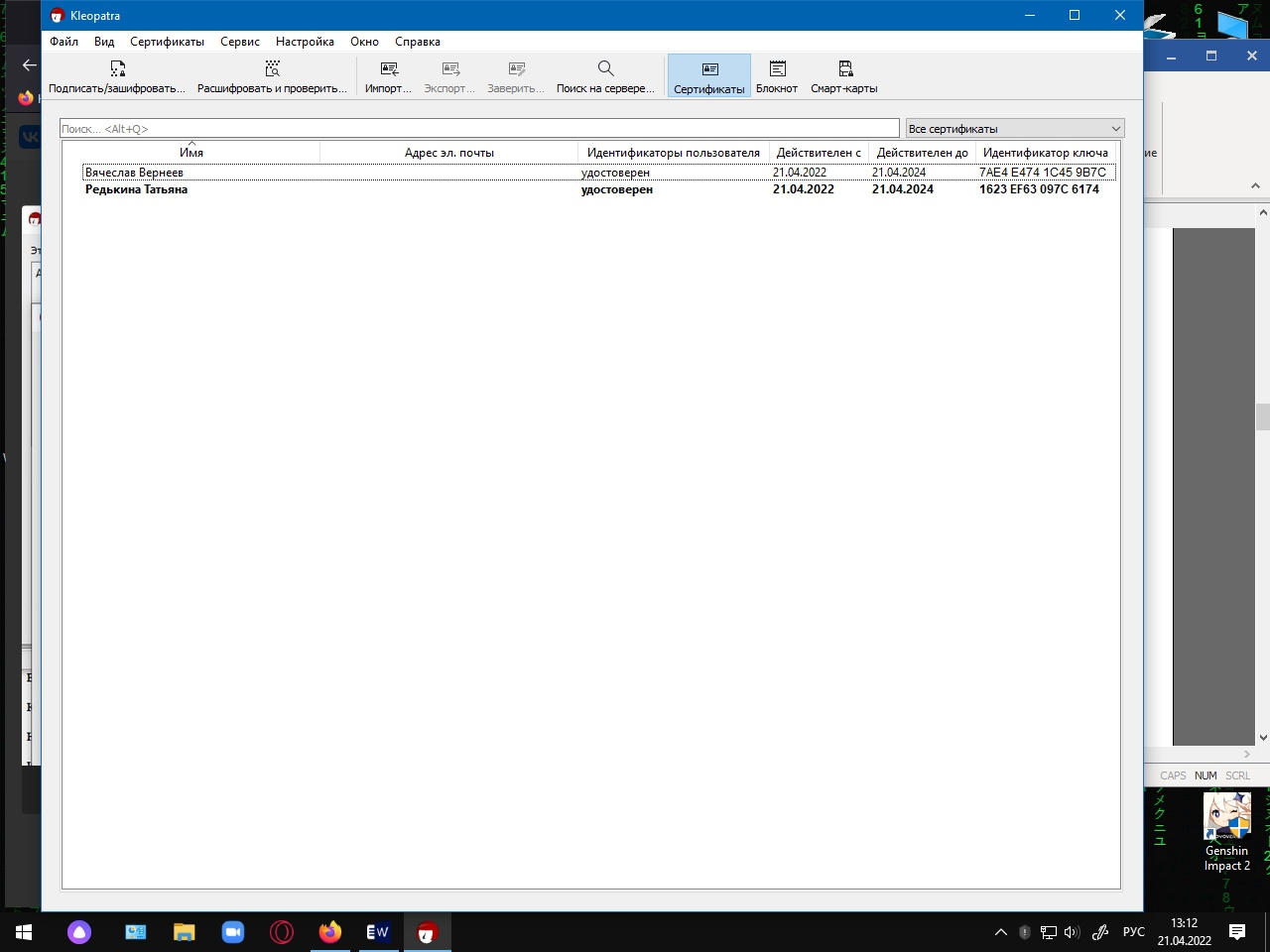
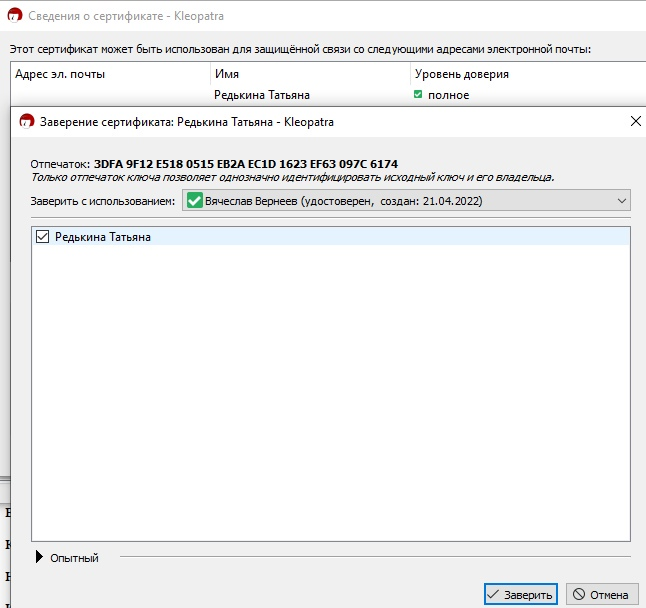
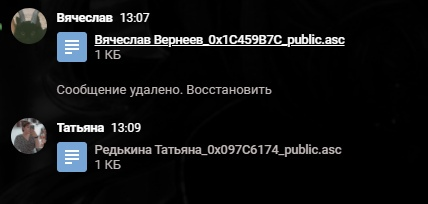
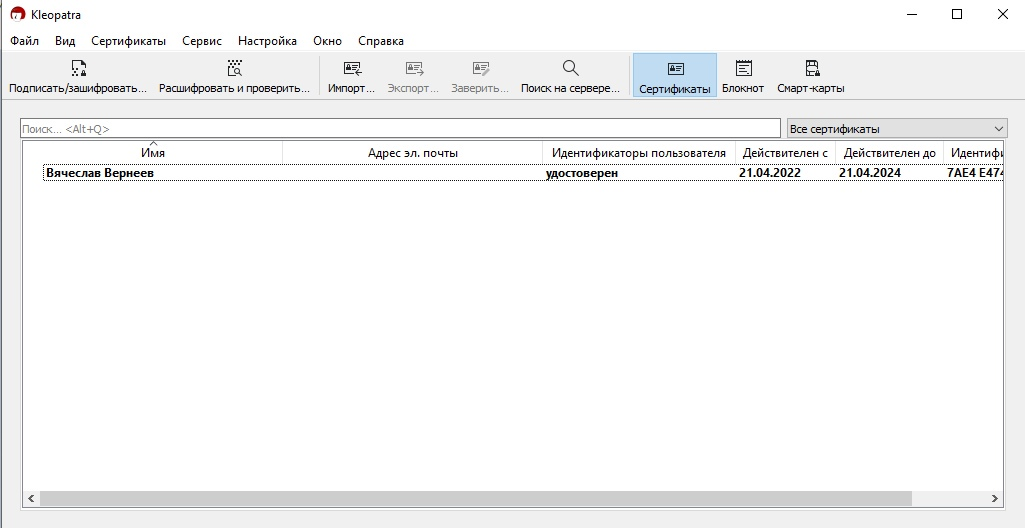
**Практическая работа № 22 (делать в парах)**

**Тема:** Выполнение операций по обмену открытыми ключами через инфраструктуру открытых ключей, отправке и получению зашифрованных и подписанных ЭЦП документов

**Цель:** научиться выполнять операции по обмену открытыми ключами

**Ход выполнения:**



**Вопросы:**

1. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
2. **Подписи**, созданные с использованием стандартов ГОСТ 3410 или DSS, **называются** **рандомизированными**, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будут создаваться разные **подписи**, поскольку каждый раз будет использоваться новое значение.
3. Прежде чем использовать **открытый** **ключ**, абонент должен быть уверен, что **открытый** **ключ** принадлежит именно получателю. **Открытые** **ключи** хранятся на общедоступном сервере и нарушитель имеет возможность, подменив **открытый** **ключ** одного из абонентов, выступать от его имени.
4. Функции:

* удостоверить личность человека, который обратился за сертификатом электронной подписи,
* изготовить и выдать сертификат, в который включены данные о владельце сертификата и его открытый ключ проверки,
* управлять жизненным циклом сертификата (выпуск, приостановление, возобновление, окончание срока действия).

1. **Сертификат** **открытого** **ключа -** электронный или бумажный документ, содержащий **открытый** **ключ**, информацию о владельце **ключа**, области применения **ключа**, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность **открытого** **ключа** владельцу.