Цель работы: ознакомится с составом основного пакета GNU Privacy Guard, назначением утилит. Получить навыки работы с сертификатами PGP. Освоить понятия сертификата и ЭЦП.

Необходимые средства: доступ к сайту <https://www.gnupg.org>, общая сетевая папка.

Порядок выполнения:

1. С сайта <https://www.gnupg.org/download/index.html> скачайте и установите пакет GnuPG stable. При установке убедитесь, что будет установлен компонент GNU Privacy Assistant
2. Создайте сертификат. Установите на него срок годности до 01.01.2016.
3. Осуществите шифрованный обмен:
   1. В вашей студенческой группе договоритесь с одним коллегой об осуществлении шифрованного обмена
   2. обменяйтесь сертификатами через общую папку
   3. импортируйте проверьте подлинность сертификата доступным способом
   4. установите достаточный для шифрованного обмена уровень доверия
   5. создайте текстовый файл с произвольным текстом и обменяйтесь шифрограммами с вашим коллегой через общую сетевую папку или электронную почту,
   6. расшифруйте шифрограмму.
4. подпишите своей подписью файлы task0-1.txt и task0-2.txt из каталога task0 (создавайте открепленные (detached) подписи). Сравните объемы подписей и текстов.
5. В каталоге task1 содержатся три исходных файла, три ЭЦП к ним и сертификат, которым они подписаны. Проверьте ЭЦП. Сравните результаты.
6. Осуществите шифрованный обмен с удостоверением подлинности:
   1. Получите подпись на ваш сертификат у преподавателя и его сертификат по защищенному каналу обмена, гарантирующему достаточный уровень доверия.
   2. Обновите ваш сертификат в локальном хранилище.
   3. Установите сертификат преподавателя и необходимый уровень доверия.
   4. Экспортируйте ваш сертификат в общую сетевую папку.
   5. После того, как ваш коллега сделает тоже самое, импортируйте его (её) сертификат.
   6. Создайте текстовый файл, зашифруйте его для вашего коллеги и подпишите файл.
   7. Осуществите обмен шифрограммами через общую сетевую папку.

В отчет включите:

1. Свой сертификат (экспортируемую часть)
2. Таблицу свойств сертификата с пояснениями назначения полей

Ответы на вопросы:

1. Можно ли полностью доверять сертификатам, полученным в п. 3.b-3.c? Почему?
2. Как осуществлялась проверка подлинности сертификата абонента в п. 3.с?
3. Какие уровни доверия сертификата бывают? В чем их отличие? В чем разница между достоверностью и доверием владельцу?
4. Почему объемы ЭЦП в п. 4 оказались одинаковыми?
5. Какие выводы о подлинности ЭЦП и (или) файлов можно сделать на основании результатов проверки ЭЦП в п.5?
6. Чем существенно отличается шифрообмен в п. 3.e и 6.g