**Лабораторная работа № 10.2**

# **Шифрование передаваемых данных программным средством PGP**

**Цель работы: изучить умение шифрования исходящей почты программным средством PGP**

**Теоретические сведенья:**

## **Основные понятия**

Что такое PGP?

Прикладная криптосистема PGP (Pretty Good Privacy, Довольно хорошая секретность) была разработана и опубликована в интернете в 1991 году программистом и математиком Массачусетского Политеха Филиппом Циммерманом, по сути, оказавшись первым продуктом подобного уровня, представленным для свободного доступа всему миру (за что впоследствии Циммерман поплатился несколькими годами уголовного преследования со стороны Таможенной службы США — в то время экспорт стойких криптотехнологий за пределы Штатов был запрещён). Изначальной целью разработки была защита гражданских прав пользователей глобальной сети, а главной задачей программы стала криптографическая защита электронной почты — шифрование.

Программа основана на так называемой асимметричной криптографии, использующей взаимосвязные пары ключей: закрытый, хранящийся только у владельца для цели расшифрования данных и их цифрового подписания, и открытый, который не нуждается в защите, может быть широко распространен и используется для зашифрования и сличения цифровых подписей (все эти уникальные возможности достигаются засчёт особого математического аппарата). Это идеальное решение для людей, не имеющих существующего согласованного тайного ключа. Вы можете взять открытый ключ адресата из любого открытого источника, с его Интернет-сайта, например, зашифровать сообщение и отправить. Никто, кроме получателя с соответствующим закрытым ключом, не сумеет прочитать ваше письмо.

С тех пор PGP претерпел значительные изменения и преобразился, как согласно духу времени и новых угроз, так и вследствие того, что теперь значительную часть пользователей программы составляют не только обычные люди, но и крупные организации и бизнесы. Сегодня PGP — этонесколько линеек приложений, различающихся назначением и перечнем решаемых задач, функциональностью, принципами работы и средой исполнения, но объединённых полной совместимостью благодаря стандарту OpenPGP, а также своей исключительной надёжностью в обеспечении защиты информации.

**Задание №1**

1. Установите почтовый клиент, например, Mozilla Thunderbird.
2. Настройте этот почтовый клиент для своего почтового ящика.
3. Установите дополнение которое позволяет шифровать данные Enigmail.
4. При установке дополнения предложит установить ядро шифрования Gpg4win.
5. Сгенерируйте пару ключей.
6. Отправьте открытый ключ на почту \*\*\*\*,ФИО и номер группы укажите в теме письма.

**Открыть файл Thunderbird**