**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский Авиационный Институт»**

**(Национальный Исследовательский Университет)**

**Институт: №8 «Информационные технологии   
и прикладная математика»   
Кафедра: 806 «Вычислительная математика   
и программирование»**

Лабораторная работа № 1  
по курсу «Основы криптографии и информационная безопасность»

Группа: М8О-307Б-22

Студент: Е. С. Кострюков

Преподаватель: А. В. Борисов

Оценка:

Дата: 20.03.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[**1** **Тема** 3](#_Toc193355599)

[**2** **Задание** 4](#_Toc193355600)

[**3** **Теория** 5](#_Toc193355601)

[**4** **Ход лабораторной работы** 8](#_Toc193355602)

[**5** **Выводы** 9](#_Toc193355603)

# **Тема**

Использование OpenPGP-ключей для шифрования и аутентификации.

# **Задание**

1. Сгенерировать пару OpenPGP-ключей, указав в сертификате свою электронную почту, с использованием почтового клиента Thunderbird, командной строки в Linux или иным способом.

2. Установить защищённую связь с преподавателем:  
2.1. Отправить преподавателю по электронной почте сообщение с вложением своего сертификата открытого ключа.  
2.2. Дождаться получения сертификата открытого ключа преподавателя.  
2.4. Отправить зашифрованное сообщение с использованием открытого ключа преподавателя.  
2.5. Получить ответное письмо.  
2.6. Расшифровать ответное письмо с помощью своего закрытого ключа.

3. Собрать подписи под своим сертификатом открытого ключа:  
3.0. Получить сертификат открытого ключа одногруппника.  
3.1. Подтвердить подлинность сертификата, сравнив отпечаток ключа по доверенному каналу связи.  
3.2. Подписать сертификат одногруппника.  
3.3. Передать подписанный сертификат обратно владельцу.  
3.4. Повторить шаги 3.0–3.3 для сбора 10 подписей под своим сертификатом.  
3.5. Отправить преподавателю свой сертификат с 10 подписями одногруппников.  
3. Подписать сертификат преподавателя и отправить ему.

# **Теория**

**OpenPGP и основы криптографии**

OpenPGP (Open Pretty Good Privacy) — это стандарт криптографической защиты данных, обеспечивающий их конфиденциальность, целостность и аутентификацию. Он используется для шифрования и подписывания сообщений, электронной почты и файлов. OpenPGP основан на асимметричной криптографии, что позволяет пользователям безопасно обмениваться зашифрованными данными без необходимости предварительного обмена секретными ключами.

**Принципы работы OpenPGP**

OpenPGP использует **гибридное шифрование**, сочетающее преимущества симметричных и асимметричных алгоритмов:

* **Асимметричное шифрование** применяется для защиты сеансового ключа, который затем используется для симметричного шифрования данных.
* **Симметричное шифрование** (например, алгоритмы AES, Twofish) применяется для непосредственно шифрования содержимого сообщения.

Каждый пользователь OpenPGP имеет **пару ключей**:

* **Открытый ключ (public key)** используется для шифрования информации и проверки цифровых подписей. Он может быть свободно распространяем среди пользователей.
* **Закрытый ключ (private key)** необходим для расшифровки сообщений и создания цифровых подписей. Он хранится в секрете и должен быть защищен от несанкционированного доступа.

**Цифровая подпись и аутентификация**

OpenPGP также обеспечивает механизм цифровой подписи, который позволяет проверять подлинность отправителя и целостность данных. Подпись создается с использованием закрытого ключа отправителя, а её проверка выполняется с помощью его открытого ключа. Если данные были изменены после подписания, проверка подписи не пройдет.

Процесс цифровой подписи включает:

1. Создание **хэша (контрольной суммы)** сообщения с использованием криптографической хеш-функции (например, SHA-256).
2. Шифрование хэша **закрытым ключом** отправителя — это и есть цифровая подпись.
3. Проверка подписи получателем, который расшифровывает хэш с помощью **открытого ключа** отправителя и сравнивает его с хэшем полученного сообщения.

**Модель доверия OpenPGP**

OpenPGP не использует централизованные центры сертификации (CA), как в PKI (инфраструктуре открытых ключей), а вместо этого реализует **модель "веба доверия" (Web of Trust)**. В этой модели пользователи взаимно подписывают ключи друг друга, подтверждая их подлинность.

Существует три уровня доверия к подписанному ключу:

* **Полное доверие** — пользователь сам проверил личность владельца ключа и подписал его.
* **Частичное доверие** — пользователь считает подписавшего ключ достаточно надежным, но не полностью.
* **Отсутствие доверия** — пользователю неизвестна личность владельца ключа, и он не может доверять подписи.

Чем больше пользователей подписало ключ, тем выше уровень доверия к его владельцу.

**Применение OpenPGP**

OpenPGP широко используется для:

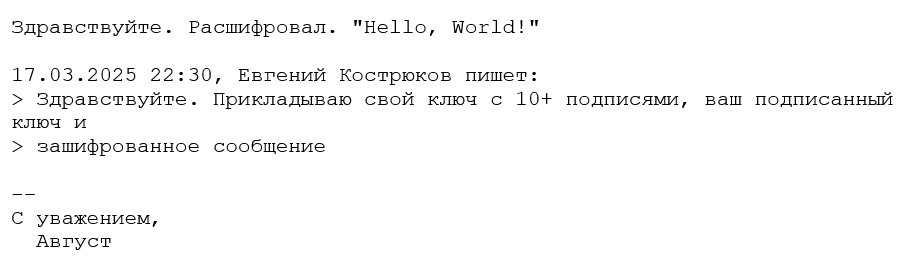
* **Шифрования электронной почты** (например, через GnuPG и почтовые клиенты с поддержкой OpenPGP).
* **Подписания и шифрования файлов** (например, с помощью PGP-клиентов).
* **Обеспечения безопасности общения в мессенджерах и на форумах**.

Стандарт OpenPGP поддерживается такими инструментами, как **GnuPG (GPG)**, PGP, Mailvelope, Enigmail и другими решениями для защиты конфиденциальности данных.

Таким образом, OpenPGP является мощным инструментом для защиты информации, основанным на криптографических принципах, цифровых подписях и модели "веба доверия".

# **Ход лабораторной работы**

1. Скачал утилиту - sudo apt update && sudo apt install gnupg
2. Создал ключ - gpg --full-generate-key
3. RSA, размер 4096, со сроком окончания в 3 года, указал имя и почту.
4. Посмотрел ключи – gpg –list-keys
5. Экспортировал ключ - gpg --export -a "kostrukov.evgeny2018@yandex.ru" > Евгений Кострюков\_0x614FBC77\_public.asc
6. Получил ключ преподавателя - gpg --import OpenPGP\_0xA67701829D9C5DE4.asc
7. Создал сообщение - echo "Hello, World!" > message.txt
8. Зашифровал - gpg --encrypt --recipient "awh@cs.msu.ru" message.txt
9. Отправил письмо преподавателю
10. Расшифровал ответ и сохранил результат - gpg --decrypt encrypted.asc > decrypted\_message.txt



Для выполнения пункта о сборе подписей я обменивался сертификатами с одногруппниками. Каждый сертификат проверял на подлинность, сравнивая отпечатки, после чего я подписывал их и отправлял обратно владельцам. Аналогично собрал 10 подписей под своим сертификатом. Завершив этот этап, подписал сертификат преподавателя и отправил ему свой сертификат с подписями одногруппников.

# **Выводы**

В ходе выполнения лабораторной работы я изучил процесс создания и управления OpenPGP-ключами, а также освоил механизмы шифрования, расшифровки и подписания данных. Практическое применение модели "веба доверия" помогло мне лучше понять принципы распределенного подтверждения подлинности ключей и формирования цепочек доверия. Работа с инструментами командной строки и проверка цифровых подписей способствовали укреплению моих навыков в области криптографии и информационной безопасности. Несмотря на необходимость внимательной настройки ключей и координации обмена сертификатами, все этапы лабораторной работы были успешно выполнены.

