**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Криптографические методы обеспечения информационной безопасности»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

«Цифровые подписи и сертификаты в GNU Privacy Guard. Система управления ключей Kleopatra»

**Выполнил:**

Молитвин Илья Алексеевич, студент группы N3Изображение выглядит как текст, соединитель

Контент, сгенерированный ИИ, может содержать ошибки.345

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Таранов Сергей Владимирович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Содержание

[Введение 3](#_Toc152996465)

[1 Ход работы 4](#_Toc152996466)

[1.1 Cоздание нового сертификата 4](#_Toc152996467)

[1.2 Экспорт открытой части сертификата 6](#_Toc152996468)

[1.3 Подпись файла 8](#_Toc152996469)

[1.4 Проверка подлинности подписи 10](#_Toc152996470)

[1.5 Шифрование файла 11](#_Toc152996471)

[Заключение 13](#_Toc152996472)

Введение

Цель работы – целью лабораторной работы является изучение основных функций программного средства шифрования информации, создание цифровых подписей GnuPG, получение навыков работы с данным программным средством.

Для достижения поставленной цели необходимо решить следующие задачи:

* Генерация новой пары ключей (нового сертификата), по инструкциям, данным в Теоретической части данной лабораторной работы, и экспорт открытой части;
* Создание цифровой подписи для файла notion.doc с использованием сгенерированной пары ключей и ее проверка;
* Шифрование файла notion.doc с использованием импортированного открытого ключа.
* Результаты выполнения работы оформить в виде отчета.

# Ход работы

Для выполнения лабораторной работы необходимо установить

GnuPG и менеджер ключей Kleopatra на свою операционную систему.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

1. Установка GnuPG и менеджера ключей Kleopatra

## Cоздание нового сертификата

Создадим новый сертификат (пару ключей). Для этого в разделе

Файл выбираем Новая пара ключей OpenPGP.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Переход к созданию новой пары ключей

Заполняем данные о владельце сертификата:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Заполнение данных для новой пары ключей

Далее перейдём во вкладку Дополнительные параметры - там указываются технические сведения о нашем сертификате (алгоритм, длина) и параметры его использования:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Дополнительные параметры для новой пары ключей

По окончании настройки происходит непосредственно создание пары ключей.

Изображение выглядит как снимок экрана, текст, Мультимедийное программное обеспечение, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

1. Процесс создания сертификата

После его завершения получаем сообщение о том, что все выполнено успешно. Наш сертификат появился во вкладке Все сертификаты:

Изображение выглядит как Мультимедийное программное обеспечение, программное обеспечение, Графическое программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

1. Сообщение об успешном создании сертификата

## Экспорт открытой части сертификата

Экспортируем открытую часть сгенерированной в предыдущем пункте пары ключей. Для этого в разделе Файл выбираем Экспорт.

При этом также должен быть выбран нужный сертификат.

Изображение выглядит как программное обеспечение, Мультимедийное программное обеспечение, Графическое программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

1. Переход к экспорту открытой части сертификата

Сохраняем открытую часть в файле key.asc (файл см в приложении к ЛР).

При открытии файла видим следующее:

Изображение выглядит как Мультимедийное программное обеспечение, программное обеспечение, Графическое программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

1. Отчет об открытой части сертификата

## Подпись файла

Создадим файл notion.doc, где в соответствии с выбранным вариантом(9) поместим определение указанного термина.

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

1. Содержание файла notion.doc

Для создания подписи в разделе Файл выбираем Подписать/­зашифровать.

Изображение выглядит как программное обеспечение, Мультимедийное программное обеспечение, Графическое программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

1. Переход к подписи файла

Формируем подпись: выбираем файл, который подписываем, и сертификат, которым это делается.

Изображение выглядит как снимок экрана, программное обеспечение, Мультимедийное программное обеспечение, текст

Автоматически созданное описание

1. Формирование подписи файла notion.doc

Получаем сообщение о том, что файл успешно подписан:

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Сообщение об успешном подписании файла notion.doc

По завершении подписания появляется файл notion.doc.sig.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Появление файла

## Проверка подлинности подписи

Проверим подлинность подписи нашего файла из предыдущего пункта. Для этого в разделе Файл выбираем Расшифровать и проверить:

Изображение выглядит как программное обеспечение, Мультимедийное программное обеспечение, Графическое программное обеспечение, Редактирование

Контент, сгенерированный ИИ, может содержать ошибки.

1. Переход к проверке подписи файла

Выбрав нужный файл notion.doc.sig получаем сообщение о корректности (действительности) подписи и информацию о сертификате.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Результат проверки подписи

Аналогичное сообщение можно получить, просто дважды щелкнув по файлу на Рабочем столе.

## Шифрование файла

Проведем шифрование файла notion.doc сгенерированной ранее парой ключей. Для этого в разделе Файл снова выбираем Подписать/зашифровать. Также выбираем нужный файл, выбираем, что необходимо только шифрование, и выбираем сертификат.

Изображение выглядит как снимок экрана, программное обеспечение, Мультимедийное программное обеспечение, текст

Автоматически созданное описание

1. Настройка шифрования файла notion.doc

По окончании шифрования получаем сообщение об успешном завершении. Там же указан зашифрованный файл - notion.doc.gpg

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Сообщение об успешном шифровании файла notion.doc

Для дешифрования файла можно либо в разделе Файл выбрать Расшифровать и проверить, либо дважды щелкнуть по файлу notion.doc.gpg на Рабочем столе.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Результат дешифрования файла notion.doc.gpg

Заключение

В данной лабораторной работе я поработал с GNU Privacy Guard, а именно с системой управления ключей Kleopatra. В ходе работы был сгенерирован сертификат (пара ключей), открытая часть которого была экспортирована в отдельный файл. С помощью данного сертификата был подписан (подпись проверена) и зашифрован текстовый файл (также созданный в рамках работы).