**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 ПРАКТИЧЕСКОЙ РАБОТЕ №5**

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

**Выполнил:**

Изображение выглядит как зарисовка, Штриховая графика, Шрифт, рукописный текст

Автоматически созданное описаниеПолевцов Артем Сергеевич, студент группы N34511

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

(подпись)

**Проверил:**

Волков Александр Григорьевич, инженер ФБИТ

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

(отметка о выполнении)

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

(подпись)

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc154059498)

[1 ЦИФРОВЫЕ ПОДПИСИ И СЕРТИФИКАТЫ В GNU PRIVACY GUARD. СИСТЕМА УПРАВЛЕНИЯ КЛЮЧЕЙ KLEOPATRA 4](#_Toc154059499)

[1.1 Ход работы 4](#_Toc154059500)

[1.1.1 Установка и генерация ключей при помощи утилиты gnupg 4](#_Toc154059501)

[ЗАКЛЮЧЕНИЕ 9](#_Toc154059502)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 10](#_Toc154059503)

# ВВЕДЕНИЕ

Цель работы **-** изучение основных функций программного средства шифрования информации, создание цифровых подписей GnuPG, получение навыков работы с данным программным средством.

Для достижения цели необходимо выполнить следующие задачи:

* + Установить GnuPG вместе с менеджером ключей Kleopatra на компьютер;
  + Сгенерировать новую пару ключей (создать новый сертификат), следуя инструкциям, данным в Теоретической части данной лабораторной работы;
  + Экспортировать открытую часть сгенерированной пары ключей в файл ***key.asc*** и приложить к отчету;
  + Составить небольшой файл с названием notion.doc, содержащий краткое определение термина (3-4 предложения), в зависимости от выбранного варианта;
  + Создать цифровую подпись для файла notion.doc, используя сгенерованную пару ключей, и приложить файл цифровой подписи notion.doc.sig к отчету;
  + Осуществить проверку созданной цифровой подписи и отразить результат в отчете;
  + Зашифровать файл notion.doc, используя импортированный открытый ключ (файл crypto.asc), который находится в приложении к тексту данной лабораторной работы, и приложить к отчету результат шифрования notion.doc.gpg;

# ЦИФРОВЫЕ ПОДПИСИ И СЕРТИФИКАТЫ В GNU PRIVACY GUARD. СИСТЕМА УПРАВЛЕНИЯ КЛЮЧЕЙ KLEOPATRA

## Ход работы

### Установка и генерация ключей при помощи утилиты gnupg

В установленной утилите GnuPG сгенерировали новую пару ключей (новый сертификат)

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 1 - Создание сертификата OpenPGP

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

Автоматически созданное описание

Рисунок 2 – Дополнительные параметры - Kleopatra

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

Автоматически созданное описание

Рисунок 3 – Сообщение об успешном создании сертификата

Далее экспортировали открытую часть сгенерированной пары ключей в файл ***key.asc*:**

Изображение выглядит как текст, линия, Мультимедийное программное обеспечение, Шрифт

Автоматически созданное описание

Рисунок 4 – Экспорт открытой части ключа в файл

Составили небольшой файл с названием ***notion.doc***, содержащий краткое определение термина Дискретное логарифмирование:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 5 – Файл notion.doc

Создали цифровую подпись для файла ***notion.doc***, используя сгенерированную мной пару ключей:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 6 – Создание подписи

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

Автоматически созданное описание

Рисунок 7 – Результаты создания подписи

Осуществили проверку созданной мной цифровой подписи:

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Рисунок 8 – Итог подтверждения подписи

Зашифровал файл ***notion.doc***, используя импортированный открытый ключ:

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

Автоматически созданное описание

Рисунок 9 – Создание подписи и шифрование файла

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

Автоматически созданное описание

Рисунок 10 – Результаты создания подписи и шифрования файла

Осуществили проверку зашифрованного файла:

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Рисунок 11 – Итог подтверждения подписи и дешифрование файла

Видим, что файл успешно дешифрован и подпись подтверждена.

# ЗАКЛЮЧЕНИЕ

В ходе данной лабораторной работы были изучены основные функций программного средства шифрования информации, создание цифровых подписей GnuPG, а также были получены навыки работы с данным программным средством.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 c.
2. Бабенко, Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 c.
3. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. - М.: КомКнига, 2012. - 306 c.
4. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - 186 c.