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

**Факультет безопасности информационных технологий**

**Выпускная Квалификационная Работа**

**На тему:**

«Разработка методики оценки эффективности систем пороговой подписи на основе алгоритма tECDSA»

**Выполнил:**

Гутник Дмитрий Вячеславович,

студент группы N34491

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

(подпись)

**Проверил:**

Таранов Сергей Владимирович,

доцент факультета БИТ

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

(отметка о выполнении)

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

(подпись)

Санкт-Петербург

2023г.

Содержание

[Введение 3](#_Toc128228007)

[Ход работы 4](#_Toc128228008)

[1 Анализ и разделение на виды актуальных алгоритмов цифровой подписи 4](#_Toc128228009)

[2 Описание алгоритма tecdsa для схемы распределенного хранения ключей 5](#_Toc128228010)

[3 Описание критериев к методике оценки цифровых подписей 6](#_Toc128228011)

[4 Описание методики оценки эффективности пороговых подписей 7](#_Toc128228012)

[5 Описание программной реализации методики 8](#_Toc128228013)

[6 Рекомендации к практическому использования методики 9](#_Toc128228014)

[Заключение 10](#_Toc128228015)

[Список использованных источников 11](#_Toc128228016)

Введение

Цель работы – повышение эффективности применения алгоритмов цифровой подписи путём рекомендации подходящего вида ЦП в конкретных условиях

Для достижения поставленной цели необходимо решить следующие задачи:

1. Анализ и разделение на виды актуальных алгоритмов цифровой подписи

2. Разработка критериев к методике оценки цифровых подписей

3. Создание методики оценки эффективности пороговых подписей

4. Разработка программной реализации методики

5. Разработка рекомендаций к практическому использования методики

# Ход работы

# Анализ и разделение на виды актуальных алгоритмов цифровой подписи

# Описание алгоритма tecdsa для схемы распределенного хранения ключей

# Описание критериев к методике оценки цифровых подписей

# Описание методики оценки эффективности пороговых подписей

# Описание программной реализации методики

# Рекомендации к практическому использования методики

Заключение

Было выполнено то-се пятое-десятое…

Это позволили получить / закрепить навыки и т.п…

Мы все сделали, мы молодцы, поставьте нам **отлично автоматом**.

Список использованных источников

1. Васильева И. Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / Москва: Юрайт, 2016. – 349 с.
2. Крамаров С. О., Криптографическая защита информации: Учебное пособие / Крамаров С. О., Митясова О.Ю., Соколов С. В., Тищенко Е.Н., Шевчук П.С., Под ред. Крамарова С.О - Минск: РИОР, 2018. – 324 с.
3. A. Menezes, P. van Oorschot and S. Vanstone. Handbook of Applied Cryptography. CRC Press 1996. – 816с.
4. R. Gennaro, S. Goldfeder. Fast Multiparty Threshold ECDSA with Fast Trustless Setup. Conference on Computer and Communications Security 2018. – 31c.