

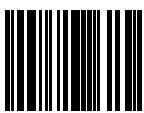
**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
ITMO University**

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
GRADUATION THESIS**

**Разработка интерактивной методики оценки эффективности систем цифровой
подписи на основе библиотеки PyCryptodome**

Обучающийся / Student Гутник Дмитрий Вячеславович
Факультет/институт/кластер/ Faculty/Institute/Cluster факультет безопасности
информационных технологий
Группа/Group N34491
Направление подготовки/ Subject area 10.03.01 Информационная безопасность
Образовательная программа / Educational program Технологии защиты информации
2019
Язык реализации ОП / Language of the educational program Русский
Статус ОП / Status of educational program
Квалификация/ Degree level Бакалавр
Руководитель ВКР/ Thesis supervisor Таранов Сергей Владимирович, кандидат
технических наук, Университет ИТМО, факультет безопасности информационных
технологий, доцент (квалификационная категория "ординарный доцент")

Обучающийся/Student

Документ подписан	
Гутник Дмитрий Вячеславович	
12.05.2023	

(эл. подпись/ signature)

Гутник
Дмитрий
Вячеславович

(Фамилия И.О./ name
and surname)

Руководитель ВКР/
Thesis supervisor

Документ подписан	
Таранов Сергей Владимирович	
12.05.2023	

(эл. подпись/ signature)

Таранов Сергей
Владимирович

(Фамилия И.О./ name
and surname)

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

**ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ /
OBJECTIVES FOR A GRADUATION THESIS**

Обучающийся / Student Гутник Дмитрий Вячеславович
Факультет/институт/кластер/ Faculty/Institute/Cluster факультет безопасности информационных технологий
Группа/Group N34491
Направление подготовки/ Subject area 10.03.01 Информационная безопасность
Образовательная программа / Educational program Технологии защиты информации 2019
Язык реализации ОП / Language of the educational program Русский
Статус ОП / Status of educational program
Квалификация/ Degree level Бакалавр
Тема ВКР/ Thesis topic Разработка интерактивной методики оценки эффективности систем цифровой подписи на основе библиотеки PyCryptodome
Руководитель ВКР/ Thesis supervisor Таранов Сергей Владимирович, кандидат технических наук, Университет ИТМО, факультет безопасности информационных технологий, доцент (квалификационная категория "ординарный доцент")

Основные вопросы, подлежащие разработке / Key issues to be analyzed

Цель работы:

Повышение эффективности применения алгоритмов цифровой подписи путём рекомендации подходящего вида ЦП в зависимости от условий применения

Задачи работы:

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 использованию методики

Исходные данные:

1. Алгоритм ECDSA
2. Алгоритм DSA
3. Алгоритм RSA (PKCS#1 v1.5 и PKCS#1 PSS)
4. Алгоритм EdDSA
5. Алгоритм SHA 256
6. Алгоритм SHA 384
7. Алгоритм SHA 512

Содержание выпускной квалификационной работы:

1. Анализ и разделение на виды актуальных алгоритмов цифровой подписи
2. Общая информация о разработанной методике
3. Описание структуры методики оценки эффективности подписей
4. Описание программной реализации методики
5. Оценка скорости работы алгоритмов

Исходные материалы и пособия:

1. TIOBE Index for April 2023 // Tiobe URL: <https://www.cryptool.org/en/ct2/> (дата обращения: 20.02.2023).
2. 3 Best Python Encryption Libraries in 2023 // TLe Apps URL: <https://tleapps.com/best-python-encryption-libraries/> (дата обращения: 20.02.2023).
3. Welcome to PyCryptodome's documentation // PyCryptodome URL: <https://www.pycryptodome.org> (дата обращения: 20.02.2023).
4. RFC 8017 // Datatracker URL: <https://datatracker.ietf.org/doc/html/rfc8017> (дата обращения: 10.03.2023).
5. 1363-2000 - IEEE Standard Specifications for Public-Key Cryptography // IEEE Xplore URL: <https://ieeexplore.ieee.org/document/891000> (дата обращения: 10.03.2023).
6. Digital Signature Standard (DSS) // NIST Technical Series Publications URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf> (дата обращения: 20.03.2023).
7. RFC 8032 // Datatracker URL: <https://datatracker.ietf.org/doc/html/rfc8032> (дата обращения: 20.03.2023).
8. Desmedt, Y., A. Odlyzko A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes // Lecture Notes in Computer Science. - Heverlee: 1985. - С. 516-522.
9. Coron, J., Naccache, D., J. Stern On the Security of RSA Padding // Lecture Notes in Computer Science. - Heverlee: 1999. - С. 1-18.
10. Coppersmith, D., Halevi, S., C. Jutla ISO 9796-1 and the new forgery strategy // Rump session of Crypto. - IBM, 1999. - С. 1-17.
11. Bellare, M., P. Rogaway The Exact Security of Digital Signatures - How to Sign with RSA and Rabin // Lecture Notes in Computer Science. - Heverlee: 1996. - С. 399-416.
12. Bernstein, D., Duif, N., Lange, T., Schwabe, P., B. Yang High-speed high-security signatures // Journal of Cryptographic Engineering. - 2012. - №2. - С. 77-89.
13. Жданов О. Методика выбора ключевой информации для алгоритма блочного шифрования. - Инфра-М, 2013. - 88 с.
14. Появилось приложение для интерактивного обучения основам криптографии // Naked science URL: <https://naked-science.ru/article/hi-tech/cryptography-is-fun> (дата обращения: 30.04.2023).
15. About CrypTool 2 // Cryptool URL: <https://www.cryptool.org/en/ct2/> (дата обращения: 01.05.2023).

Дата выдачи задания / Assignment issued on: 01.12.2022

Срок представления готовой ВКР / Deadline for final edition of the thesis 26.05.2023

Характеристика темы ВКР / Description of thesis subject (topic)

Тема в области фундаментальных исследований / Subject of fundamental research: нет / not

Тема в области прикладных исследований / Subject of applied research: да / yes

СОГЛАСОВАНО / AGREED:

Руководитель ВКР/
Thesis supervisor

Документ подписан	
Таранов Сергей Владимирович	
08.05.2023	

(эл. подпись)

Таранов Сергей
Владимирович

Задание принял к
исполнению/ Objectives
assumed BY

Документ подписан	
Гутник Дмитрий Вячеславович	
10.05.2023	

(эл. подпись)

Гутник
Дмитрий
Вячеславович

Руководитель ОП/ Head
of educational program

(эл. подпись)

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

**АННОТАЦИЯ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ
SUMMARY OF A GRADUATION THESIS**

Обучающийся / Student Гутник Дмитрий Вячеславович
Факультет/институт/кластер/ Faculty/Institute/Cluster факультет безопасности информационных технологий
Группа/Group N34491
Направление подготовки/ Subject area 10.03.01 Информационная безопасность
Образовательная программа / Educational program Технологии защиты информации 2019
Язык реализации ОП / Language of the educational program Русский
Статус ОП / Status of educational program
Квалификация/ Degree level Бакалавр
Тема ВКР/ Thesis topic Разработка интерактивной методики оценки эффективности систем цифровой подписи на основе библиотеки PyCryptodome
Руководитель ВКР/ Thesis supervisor Таранов Сергей Владимирович, кандидат технических наук, Университет ИТМО, факультет безопасности информационных технологий, доцент (квалификационная категория "ординарный доцент")

**ХАРАКТЕРИСТИКА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ
DESCRIPTION OF THE GRADUATION THESIS**

Цель исследования / Research goal

Повышение эффективности применения алгоритмов цифровой подписи путём рекомендации подходящего вида ЦП в зависимости от условий применения

Задачи, решаемые в ВКР / Research tasks

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 использованию методики

Краткая характеристика полученных результатов / Short summary of results/findings

В результате выполнения этой работы была разработана методика, которая позволяет: 1. Подписывать сообщения 2. Проверять подписи 3. Создавать ключи 4. Использовать заранее созданные ключи для подписи 5. Рекомендовать алгоритмы в зависимости от сценария использования 6. Проводить тесты производительности алгоритмов электронной подписи

Обучающийся/Student

Документ подписан	
Гутник Дмитрий Вячеславович	

Гутник
Дмитрий

Руководитель ВКР/
Thesis supervisor

12.05.2023	
------------	--

(эл. подпись/ signature)

Вячеславович

(Фамилия И.О./ name and surname)

Документ подписан	
Таранов Сергей Владимирович	
12.05.2023	

(эл. подпись/ signature)

Таранов Сергей
Владимирович

(Фамилия И.О./ name and surname)