

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

“Подсчет голосов в системах электронного голосования”

Заговальский Глеб Юрьевич

Научный руководитель — кандидат физико-математических наук, доцент
кафедры математического моделирования и анализа данных Мальцев М. В.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 45 страниц, 3 главы, 6 рисунков, 28 использованных источников, 1 приложение.

Ключевые слова: ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ, КОНФИДЕНЦИАЛЬНОСТЬ, ПРОТОКОЛЫ.

Объект исследования: практическая реализация систем электронного голосования.

Цель работы: изучение решений, применяемых при конструировании систем электронного голосования, сравнение уже реализованных систем, разработка протокола электронного голосования.

Методы исследования: а) теоретические: изучение источников, посвящённых протоколам, применяемым для организации электронного голосования; изучение криптографических алгоритмов и механизмов, применяемых для защиты данных;

б) практические: разработка протокола электронного голосования.

Результат: изучение реализованных протоколов в различных странах и описание их принципа работы; изучение протоколов, которые предоставляют возможность использования в системах электронного голосования; реализация протокола электронного голосования с использованием языка программирования Python и библиотек PyRankVote, PyCryptodome, OpenSSL.

Область применения: организация безопасного электронного голосования.

ABSTRACT

Diploma thesis: 45 pages, 3 chapters, 6 figures, 28 sources, 1 attachment.

Keywords: ELECTRONIC VOTING, CRYPTOGRAPHIC DATA PROTECTION, CONFIDENTIALITY, PROTOCOLS.

Object of study: implementation of electronic voting systems.

Purpose of work: study of solutions used in the design of electronic voting systems, comparison of already implemented systems, development of an electronic voting protocol.

Research methods: a) theoretical: study of sources devoted to protocols used to organize electronic voting; study of cryptographic algorithms and mechanisms used to protect data;

b) practical: development of an electronic voting protocol.

Result: the study of implemented protocols in various countries and a description of their principle of operation; the study of protocols that make it possible to use in electronic voting systems; the implementation of the electronic voting protocol using the Python programming language and the PyRankVote, PyCryptodome, OpenSSL libraries.

Scope: organization of secure electronic voting.