МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

“Широковещательное шифрование для видеоконференций”

Станюль Глеб Валерьевич

Научный руководитель – кандидат физико-математических наук, доцент кафедры математического моделирования и анализа данных Агиевич С. В.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 49 страниц, 4 главы, 8 рисунков, 2 таблицы, 9 использованных источников, 1 приложение.

Ключевые слова: ШИРОКОВЕЩАТЕЛЬНОЕ ШИФРОВАНИЕ, СИСТЕМЫ ВИДЕОКОНФЕРЕНЦИЙ, ЗАЩИТА ДАННЫХ, ПРОТОКОЛЫ, КРИПТОНАБОРЫ.

Объект исследования: системы широковещательного шифрования, системы видеоконференций.

Цель работы: изучение схем выработки общего ключа в системах видеоконференций, изучение протоколов потоковой передачи аудио- и видео-данных, изучение протоколов транспортного уровня защиты данных, разработка криптонабора с использованием широковещательного шифрования.

Методы исследования: а) теоретические: изучение источников, посвящённых архитектурам безопасности некоторых систем видеоконференций; изучение протоколов, используемых в этих системах, их особенностей; изучение возможности использования схемы широковещательного шифрования в системах видеоконференций.

б) практические: разработка криптонабора для протокола SSL/TLS на основе широковещательного шифрования, использующего методы защиты данных, описанные в белорусских криптографических стандартах.

Результат: анализ архитектур безопасности систем видеоконференций: схем выработки общего ключа, протоколов потоковой передачи аудио- и видео-данных, протоколов установки безопасного соединения между узлами сети; реализация криптонабора на основе широковещательного шифрования на языке программирования C (Си) для установки безопасного TLS соединения.

Область применения: сфера информационной безопасности в сети.

ABSTRACT

Diploma thesis: 49 pages, 4 chapters, 8 figures, 2 tables, 9 sources, 1 attachments.

Keywords: BROADCAST ENCRYPTION, VIDEO CONFERENCE SYSTEMS, DATA PROTECTION, PROTOCOLS, CRYPTO KITS.

Object of study: broadcast encryption systems, video conferencing systems.

Purpose of work: studying schemes for generating a shared key in video conferencing systems, studying protocols for streaming audio and video data, studying protocols for the transport layer of data protection, developing a cryptographic suite using broadcast encryption.

Research methods: a) theoretical: study of sources,related to the security architectures of some video conferencing systems;studying the protocols used in these systems and their features; exploring the possibility of using a broadcast encryption schemein video conferencing systems.

b) practical: development of a cryptographic suite for the SSL/TLS protocol based on broadcast encryption using data protection methods, described in Belarusian cryptographic standards.

Result: analysis of security architectures of video conferencing systems: public key generation schemes, audio streaming protocols and video data, protocols for establishing a secure connection between nodes networks; implementation of cryptographic dialing based on broadcast encryption in the C programming language to establish a secure TLS connection.

Scope: the field of information security on the network.