МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

“Криптографические алгоритмы и протоколы для защиты информации в виртуальных частных сетях”

Доросев Егор Алексеевич

Научный руководитель – кандидат физико-математических наук, доцент кафедры ММАД, заведующий НИЛ проблем безопасности информационных технологий Агиевич С. В.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 70 страниц, 3 главы, 22 рисунка, 12 использованных источников, 3 приложения.

Ключевые слова: ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ (VPN), ПРОКСИ-СЕРВЕР, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ, ПРОТОКОЛЫ, КОНФИДЕНЦИАЛЬНОСТЬ.

Объект исследования: виртуальные частные сети и другие решения защиты информации в сети, их применение и стандартизация в РБ.

Цель работы: изучение протоколов, применяемых в виртуальных частных сетях, изучение и сравнение безопасности этих протоколов, разработка VPN-решения с использованием белорусских криптографических стандартов.

Методы исследования: а) теоретические методы: изучение литературы и электронных источников, посвящённых протоколам информационной безопасности; всесторонний анализ протоколов и методов, применяемых для защиты данных;

б) практические методы: написание собственного протокола; разработка VPN-решения, использующего методы защиты данных, описанные в белорусских криптографических стандартах.

Результат: сравнительный анализ протоколов и описание их принципа работы; сравнение безопасности выбранных протоколов; реализация алгоритмов аутентифицированного шифрования и хэширования из белорусских криптографических стандартов на языке программирования C; модификация протокола путем внедрения алгоритмов в решение с открытым исходным кодом Wireguard.

Область применения: сфера информационной безопасности в сети.

ABSTRACT

Diploma thesis: 70 pages, 3 chapters, 22 figures, 12 sources, 3 attachments.

Keywords: VIRTUAL PRIVATE NETWORK (VPN), PROXY SERVER, CRYPTOGRAPHIC DATA PROTECTION, PROTOCOLS, PRIVACY.

Object of study: virtual private networks and other solutions for protecting information on the network, their application and standardization in the Republic of Belarus.

Purpose of work: studying the protocols used in virtual private networks, studying and comparing the security of these protocols, developing a VPN solution using Belarusian cryptographic standards.

Research methods: a) theoretical methods: study of literature and electronic sources devoted to information security protocols; comprehensive analysis of protocols and methods used to protect data;

b) practical methods: writing your own protocol; development of a VPN solution using data protection methods described in Belarusian cryptographic standards.

Result: comparative analysis of protocols and description of their operating principle; comparison of the security of selected protocols; implementation of authenticated encryption and hashing algorithms from Belarusian cryptographic standards in the C programming language; modification of the protocol by implementing algorithms into the open source Wireguard solution.

Scope: the field of information security on the network.