Аннотация дипломной работы

Тема: протоколы формирования общего ключа на основе паролей

ФИО студента: Чибисов Олег Олегович

Научный руководитель: Бодягин Игорь Александрович**,** кандидат физико-математических наук

Кафедра (специальность, специализация): кафедра математического моделирования и анализа данных (компьютерная безопасность).

Объем дипломной работы, количество рисунков, количество использованных источников литературы, структура дипломной работы: 45 с., 2 табл., 14 рис., 8 источников.

Ключевые слова: ПРОТОКОЛ, ФОРМИРОВАНИЕ КЛЮЧА, СЕАНСОВЫЙ КЛЮЧ

Цель работы: рассмотрение протоколов формирования общего ключа на основе паролей, его программная реализация.

Результатом является реализация протокола формирования общего ключа на основе пароля, рассмотрены алгоритмы формирования общего ключа на основе пароля, и модификации алгоритма Диффи-Хеллмана.

Областью применения являются криптографические системы.