АННОТАЦИЯ

Настоящая диломная работа посвящена вопросу безопасности реализаций протокола TLS и направлена на разработку методики тестирования реализации прокола TLS. В ходе работы были проанализированы атаки на протокол, выделены параметры, с помощью которых атаки были реализованы. Была создана методика тестирования, по которой были протестированы протоколы версий TLSv1.0, TLSv1.1, TLSv1.2. Приведены результаты тестирования и рекомендации по зпщите.