КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

Клиент-серверное программное средство обмена шифрованными сообщениями с iOS-клиентом

Студент группы 413801 ХАРЧЕНКО Антон Кириллович

Научный руководитель – магистр технических наук,
ассистент кафедры ПИКС МИГАЛЕВИЧ Сергей Александрович

Минск 2018

КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

АКТУАЛЬНОСТЬ ТЕМЫ ДИПЛОМНОГО ПРОЕКТА

– вопрос безопасности пользовательских данных является одним из самых важных для современного интернета;
– разрабатываемое программное средство является универсальным и подходит для использования практически на любом предприятии;
– отсутствие качественного аналогичного устройства с открытым исходным кодом и возможностью использования собственной инфраструктуры;
– желание пользователей сохранить свои секреты в тайне и получить чувство безопасности при передаче документов и иной информации.

КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

ЦЕЛЬ ДИПЛОМНОГО ПРОЕКТА

Разработка программного средства для обмена шифрованными сообщениями

КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

ЗАДАЧИ ДИПЛОМНОГО ПРОЕКТА

– провести анализ литературно-патентных исследований;
– провести анализ аналогов проектируемого продукта;
– разработать архитектуру клиент-серверного решения;
– разработать протокол зашифрованной клиент-серверной коммуникации, работающей по принципу сквозного шифрования;

АНАЛИЗ ИСХОДНЫХ ДАННЫХ

Программное средство должно обеспечивать выполнение следующих функций:

– авторизация пользователей;
– чтение и отправка сообщений;
– синхронизация списка контактов;
– работа приложения без доступа к сети;
– защищённое хранение и обмен сообщениями.

ПРИНЦИП РАБОТЫ РАЗРАБАТЫВАЕМОГО ПРОГРАММНОГО СРЕДСТВА

Программное средство является комплексом из серверной части, являющейся брокером сообщений и временным хранилищем и клиентом, на котором выполняется основная часть работы, связанной с криптографией.

Принцип работы заключается в ассоциации пары RSA ключей за каждым устройством, рассылке необходимых публичных ключей сервером на все пользовательские клиенты и формировании копий сообщений, каждая из которых зашифрована под конкретное устройство получателя.

ТЕХНОЛОГИИ, ИСПОЛЬЗОВАННЫЕ НА КЛИЕНТЕ

– UIKit, PinCache
– Starscream, Moya, ObjectMapper
– SwCrypt, CryptoSwift, KeychainAccess
– Realm
– RxSwift, RxCocoa, RxRealm, RxDataSources

ПОДХОДЫ, ИСПОЛЬЗОВАННЫЕ ПРИ ПРОЕКТИРОВАНИИ АРХИТЕКТУРЫ ПРОГРАММНОГО СРЕДСТВА

– сокращение глобального состояния;

– модульность;

– аккуратное использование изменяемого состояния и полный отказ от общего изменяемого состояния, где это возможно;

– ответственный дизайн и использование типов;

– использование реактивных подходов;

– предпочтение использования чистых функций и функций высшего порядка вместо итераций.

ЗАКЛЮЧЕНИЕ

В результате работы над дипломным проектом было разработано программное средство, позволяющее безопасно обмениваться шифрованными сообщениями, которое отвечает современным требованиям к средствам обмена информации, функциональным требованиям, а также другим требованиям технического задания.

Данное программное средство разработано с учетом современных требований к пользовательским интерфейсам и пользовательскому опыту. Основными требованиями выступали следующие условия:

– обеспечение комфортной работы без сети;
– бесшовная работа на нескольких устройствах;
– безопасность при хранении и передачи информации;
– сохранность приватности данных даже в случае кражи устройства.

СПАСИБО ЗА ВНИМАНИЕ