Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК004.056.5

Карпук Максим Николаевич

Обеспечение безопасности программного средства, осуществляющего передачу речевой информации

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01Методы и системы защиты информации, информационная безопасность

Научный руководитель
к.т.н., доцент Таболич Т.Г.

Минск 2018

ВВЕДЕНИЕ

В наше время жизнь каждого отдельного человека и всего социума целом тесно связана с использованием компьютера, смартфона или планшета. Электронно-вычислительная техника всё шире входит во все сферы нашей жизни. Компьютер стал привычным не только в производственных целях и научных лабораториях, но и в студенческих аудиториях и школьных классах. Непрерывно растёт число специалистов, работающих с персональным компьютером, который становится их основным рабочим инструментом. Ни экономические, ни научные достижения невозможны теперь без быстрой и четкой информационной связи и без специального обученного персонала.

В связи с кардинальными переменами в образе жизни человечества, связанные с перераспределением рабочего и нерабочего времени, в результате стремительного развития технических средств, увеличения производительности труда, а также с увеличением количества свободного времени все более актуализируется вопрос проведения его вне дома, пределов города или страны. В такие моменты быть всегда на связи иногда очень необходимо, всегда можно связаться с человеком, узнать его мнение по какому-то вопросу, согласовать действия, поделиться впечатлениями. Находясь за границей появляется проблема поддержания связи с родными и близкими, либо по работе. Ведь такие частые и долгие звонки используя мобильную связь могут не только сильно «ударить» по кошельку, да и вовсе испортить всё впечатление о путешествии.

Помимо дорогих звонков из-за границы существует проблема, связанная конфиденциальностью связи. Под обеспечением конфиденциальности связи понимается защита от подслушивания передаваемых сообщений. Несмотря на сложность технической реализации сотовой связи, от подслушивания она не защищена, если для этого не принимаются специальные меры. Для подслушивания, например, информации цифровой системы сотовой связи необходимо располагать всего лишь радиоприемным устройством высокой чувствительности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований.В настоящее время популярность набирают системы, организующие передачу голосового

трафика с помощью сети Интернет. Наряду с очевидными достоинствами и популярностью таких систем, а также и их широкое применение на различных устройствах, в том числе хранящих информацию, может возникнуть целый ряд проблем, связанных с обеспечением информационной безопасности передаваемой информации организаций и лиц, использующих данную технологию.

К одному из таких методов относится шифрование, реализуемое в данном проекте путём интеграции в разрабатываемое ПС. Злоумышленники, получившие доступ SIP серверу или к устройству с поддержкой VoIP, могут детально изучить всю передаваемую речевую информацию потенциальных жертв.

Данная работа посвящена анализу подобных уязвимостей, происходит оценка и выбор наиболее оптимальных методов шифрования для обеспечения безопасности программного средства передачи речевой информации.

Поэтому **целью настоящей работы** является интеграция защиты от перехвата злоумышленником речевой информации, путём выбора и внедрения шифрования в программное средство организации голосовой системы связи.

Для достижения поставленной цели в этой диссертации **решены следующие задачи**:

1. Проведение анализа существующих средств организации голосовой системы связи.

2. Анализ программных методов шифрования систем.

3.Внедрение методов шифрования в разрабатываемое ПО.

Положения, выносимые на защиту:

1. Целесообразность использования шифрования в программном средстве, осуществляющего передачу речевой информации.

2. Обоснование выбора методов защиты.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в исследовании угроз информационной безопасности разрабатываемого программного средства и методов их парирования. Научные выводы, представленные в работе, могут быть использованы при проектировании методов защиты программного обеспечения.

Практическая значимость заключается в обеспечении программного средства, осуществляющего передачу речевой информации защитой, основанной на результатах анализа достоинств и недостатков существующих технологических решений.

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, произведено усовершенствование разрабатываемого программного средства системами защиты, предотвращающими различные виды атак.

По теме диссертации опубликованы 1 тезис доклада и 1 статья в сборнике материалов конференции.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приведён краткий исторический очерк, определено место проблемы обеспечения надёжности программного средства в современном мире. Определено место текущего исследования в области обеспечения надёжности программного средства.

В общей характеристике работы сформулированы цели и задачи исследования, показана научная и практическая значимость.

В первой главепредставлен литературный обзор по теме исследования, введение в предметную область, представлен принцип работы VoIPтехнологии, базовое знакомство с сигнальными протоколами, а также звуковыми кодеками.

Проведён анализ существующих аналогов программного средства. Выделены достоинства и недостатки каждого приложения. На основе выделенных данных были поставлены задачи следующие задачи:

- доступность;
- удобство работы с приложением;
- интуитивно-понятный интерфейс;
- высокое качество голосовых звонков;
- надежность ПС;
- наличие шифрования звонков;
- высокая скорость работы.

Во второй главе составляется функциональная модель программного средства. Определяютсябазовые функции, а также требования, которыми должно обладать программное средство.

В третьей главе ведётся разработка программного средства. Определяется платформа, под которую делается ПС. При выборе языка программирования, выбор пал на Java, благодаря его достоинствам:

– полная независимость байт-кода от операционной системы и оборудования, что позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина;

– гибкая система безопасности;

– надежность;

– многообразие типов приложений;

– стандартные библиотеки – многие задачи, встречающиеся при разработке программного обеспечения, уже решены в рамках стандартных библиотек.

Далее определялся основной сигнальный протокол для VoIP. Осуществлялся анализ существующих звуковых кодеков. Определялись достоинства и недостатки каждого, в рамках конкретно данного проекта.

И конечно же, в данной главе производился анализ существующих форм защиты, шифрования данных на различных логических уровнях в ПС.

В четвёртой главепрограммное средство уже разработано и производится окончательное тестирование, экспериментальные исследования и анализ полученных данных.Произведено 15 тестовых случаев, разработанное ПС успешно их прошло.

В заключительной **пятой главе**описывается методика работы с ПС: как создать аккаунт и совершить вызов.

ЗАКЛЮЧЕНИЕ

С целью обеспечения должного уровня защиты программного средства,выбраны и интегрированы системы защиты и шифрования, обеспечивающие безопасность от множества современных атак.

Проведен анализ существующих аналогов, выявлены их недостатки, на основании которых сформулирована постановка задачи.

Разработана функциональная и информационная модели. На основании описанных моделей описана спецификация требований.

Разработан максимально понятный и простой интерфейс для работы с программой с учетом особенностей предметной области.

Полученное программное средство протестировано на производительность, работоспособность и безопасность.

Описана методика работы пользователя с программным средством.

Программное средство обладает следующими достоинствами:

– быстрая и стабильная работа приложения;

– специально подобранные кодеки для отличной передачи звука;

– полное шифрование разговоров;

– удобный пользовательский интерфейс.

Таким образом, задачи проекта реализованы в полном объеме.

СПИСОК ОПУБЛИКОВАННЫХРАБОТ

1-А. Карпук, М.Н.Защищённое программное средство, обеспечивающее передачу речевой информации/ М. Н. Карпук // Тезисы докладов 53-й науч.-техн. конф. аспирантов, магистрантов и студентов БГУИР, Минск, 2-6 мая 2017 г. – Минск: БГУИР, 2017.

2-А. Карпук, М. Н. Информационная безопасность приложений для организации голосовой системы связи на Android / М. Н. Карпук // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В. Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 23–28.