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

УДК 004.422.81

Дударенков Анатолий Олегович

Защита голосовой информации в сетях подвижной радиосвязи

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации. Информационная безопасность»

Научный руководитель
Зельманский Олег Борисович
кандидат технических наук,
доцент

Минск 2020

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью магистерской диссертации является разработка программного модуля защиты информации в сетях мобильной передачи данных.

В соответствии с поставленной целью, в работе сформулированы и решены следующие основные задачи:

– проведен сравнительный анализ существующих средств защиты речевого трафика;

– исследованы основные компоненты, обеспечивающие защиту речевой информации, рассмотрены стандарты мобильной связи с точки зрения безопасности;

– рассмотрены методы разработки программного обеспечения;

– разработан программный модуль защиты информации в сетях мобильной передачи данных.

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует:

– п. 3.8 «Обеспечение цифрового доверия, защита информационных ресурсов и информационно-коммуникационной инфраструктуры» Стратегии развития информатизации в Республике Беларусь на 2016 – 2022 годы утверждённой на заседании Президиума Совета Министров от 03.11.2015 №26.

В диссертации поставлена и решена актуальная задача защиты речевой информации в мобильных сетях передачи.

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Основные научные и практические результаты работы получены лично автором.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились с научным руководителем, кандидатом технических наук, доцентом О.Б. Зельманским.

Апробация результатов диссертации

Основные положения и результаты, изложенные в диссертационной работе, докладывались и обсуждались на XVII Белорусско-российской научно – технической конференции «Технические средства защиты информации», Минск, 11 июня 2019 г., 55-ой юбилейной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 22 – 26 апреля 2019 г., XVIII Белорусско-российской научно – технической конференции «Технические средства защиты информации», Минск, 9 июня 2020 г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 3 печатные работы в сборниках «Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов», «ТСЗИ 2019», «ТСЗИ 2020».

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трёх разделов, заключения, списка использованных источников, списка собственных источников, двух приложений. Полный объём диссертационной работы составляет 60 страниц, включая 11 иллюстраций, список использованных источников из 27 наименований, список собственных источников из 3 наименований.

ВВЕДЕНИЕ

Широкое распространение сетей подвижной радиосвязи обуславливает необходимость обеспечения защиты передаваемой по ним информации. В настоящее время шифрование речевой информации осуществляется на основе программных средств, не позволяющих подтвердить отсутствие незадекларированных возможностей и оценить их эффективность. Также, наличие высокого спроса на персональные данные делает передачу этих данных по средствам мобильных устройств, как наиболее используемых, первоначальной целью злоумышленника. Таким образом, задача защиты речевой информации, передаваемой по сетям радиосвязи, является весьма актуальной.

Целью данной диссертации являлась разработка программного модуля для передачи зашифрованного речевого сигнала между двумя мобильными устройствами. Данное приложение необходимо чтобы избежать лавинного эффекта при ошибках передачи, и, как следствие, сделать возможным передачу предварительно зашифрованного сигнала.

Для достижения поставленной цели необходимо было решить следующие задачи:

1. Исследование технологии передачи речевой информации в сетях мобильной радиосвязи и методов защиты информации в них.

2. Разработка программного модуля защиты информации в сетях мобильной передачи данных и его тестирование.

3. Сравнительный анализ эффективности применения алгоритмов шифрования AES, RSA, Triple DES, XOR в разработанном программном модуле с точки зрения быстродействия и точности.

Актуальность работы состоит в решении перечисленных задач.

Работа выполнена самостоятельно. Пройдена проверка на плагиат.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение содержит краткое описание работы и обоснование необходимости исследований.

В первом разделе приведена краткая история развития средств защиты речевой информации и описаны средства, обеспечивающие её защиту. Проанализирована тенденция увеличения важности телефонных переговоров как в повседневной среде, так и в деловой сфере. Следствием чего является повышение цены информации, передаваемой таким путём, а значит, и увеличение интереса злоумышленников.

Второй раздел содержит основные стандарты передачи информации в мобильных сетях и принципы защиты информации в них. Показаны недостатки GSM системы, а также механизмы, которые способствуют упрощению передачи данных, но не позволяют обеспечить достаточную их защищённость. Описан принцип работы передачи данных через VoIP, который был положен в основу разработки программного модуля защиты речевой информации при передачи по сетям радиосвязи.

В третьем разделе разработана структурная схема программного модуля защиты информации в сетях мобильной передачи данных, обоснован выбор языка разработки и выбора платформы. Разработан программный модуль, позволяющий установить зашифрованный сеанс связи между двумя устройствами с установленным приложением, а также проведено его тестирование. Приведено описание функционирования программного модуля в процессе его работы. По результатам тестирования в качестве алгоритма шифрования был выбран AES по причине комбинации высокой скорости работы до 325Кб\с и низкого числа ошибок не более 4,738%. Показано, что разработанный программный модуль подходит под критерии систем передачи речевой информации с высшим классом качества.

В заключении указаны результаты исследования и сформулировано направление дальнейшего исследования.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В рамках данной работы были приведены краткая история развития средств защиты речевой информации и описаны средства, обеспечивающие её защиту. Была проанализирована тенденция увеличения важности телефонных переговоров как в повседневной среде, так и в деловой сфере, что обуславливает необходимость защиты информации в данной сфере [1-А].

Были рассмотрены основные стандарты передачи информации в мобильных сетях и принципы защиты информации в них. Было показаны недостатки GSM системы, а также механизмы, которые способствуют упрощению передачи данных, но не позволяют обеспечить достаточную их защищенность [2-А].

Был разработан программный модуль передачи речевой информации по протоколу VoIP. Было проведено его тестирование для алгоритмов шифрования AES, RSA, Triple DES, XOR, и на основании полученных данных выбран алгоритм AES, как наиболее эффективный по критерию быстродействия и точности. Скорость – до до 325Кб\с, количество ошибок – не более 4,738% [3-А].

Рекомендации по практическому использованию результатов

Целесообразным представляется применение разработанного программного модуля в сочетании с удалённой гарнитурой и ограничением доступа речевого сигнала к встроенному микрофону мобильного устройства путём использования зашумляющего чехла, звуконепроницаемой камеры или его демонтажа.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1–А. Дударенков, А. О. Программный модуль защиты голосовой информации в сетях подвижной радиосвязи / А. О. Дударенков, О. Б. Зельманский // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции, Минск, 11 июня 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2019. – С. 26.

2–А. Дударенков, А. О. Защита голосовой информации в сетях подвижной радиосвязи / А. О. Дударенков, О. Б. Зельманский // Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов, Минск, 22 – 26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2019. – С. 96.

3–А. Дударенков, А. О. Программный модуль защиты речевой информации в сетях подвижной радиосвязи / А. О. Дударенков, О. Б. Зельманский // Технические средства защиты информации : тезисы докладов XVIII Белорусско-российской научно – технической конференции, Минск, 9 июня 2020 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2020. – С. 29.