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

УДК 004.056.5:621.396.62

Абишев
Мевсюм Мухаметович

Защита речевой информации при передаче по сетям мобильной 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 2016

ВВЕДЕНИЕ

Создание специальных терминалов и программного обеспечения для защиты разговора по мобильным сетям диктовалось жесткой необходимостью – применяемые в стандарте мобильной связи шифры, при наличии должного оборудования, перехватываются вместе с закрытой ими информацией. Вдобавок, производители и операторы связи забывают сказать, что шифрование обеспечивается, в большинстве случаев, только на эфирной части канала сотовой связи – по проводным каналам трафик может идти и в открытом виде. Поэтому несколько лет назад возник вопрос защиты канала сотовой связи с гарантированной конфиденциальностью на всем участке – от аппарата до аппарата абонентов. Решений этого вопроса множество – от специальных терминалов, которые обмениваются информацией, закодированной очень надежно (даже если передачу перехватят, то расшифровать этот шифр не представляется возможным) до всевозможных программных решений сомнительной стойкости.

Но абсолютно надежных систем не существует, а с развитием технических средств и их доступностью это утверждение становится реальностью. Можно уже сейчас говорить о реализации следующих действий злоумышленниками в сетях сотовой связи: массовая рассылка рекламной или иной информации, не запрашиваемой пользователями сети сотовой связи, адресованная на серверы соответствующих служб оператора связи или на абонентские терминалы, с использованием средств самого оператора или Интернета; клонирование модулей SIM; хакерский взлом систем автоматизированного расчета с абонентами (биллинга); мошенничество с картами предоплаты.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование методов защиты голосового трафика в сетях мобильной связи, выявление их достоинств и недостатков, и предложение мер по их усовершенствованию.

Задачи, решаемые в диссертационной работе:

− провести анализ литературно-патентных источников информации;

− описать существующие методы защиты голосового трафика в сетях мобильной связи;

− на основе существующих методов предложить метод повышения эффективности защиты голосового трафика в сетях мобильной связи;

− оценить эффективность предложенного метода.

Объектом исследования выступают способы передачи информации в сетях мобильной радиосвязи. Предметом исследования являются методы защиты передаваемой по средствам радиосвязи речевой информации.

Тема диссертационной работы соответствует приоритетным научным направлениям фундаментальных и прикладных исследований в сфере информации и инженерно-технической безопасности создания современных систем защиты информации.

Положения, выносимые на защиту

1. Предложенный алгоритм обработки сигнальных сообщений, сигнальной сети SS7 в Core Network.

2. Предложенный алгоритм увеличения ключа шифрования в SIM-карте.

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует:

– п. 13. «Безопасность человека, общества и государства» Приоритетных направлений научных исследований Республики Беларусь на 2016–2020 годы утвержденных Постановлением Совета Министров Республики Беларусь № 190 от 12 марта 2015 г.

В диссертации поставлена и решена актуальная задача по исследованию алгоритмов обеспечения безопасности на сетях мобильной связи. Научную новизну представляет разработанные механизм обеспечения безопасности на радиоинфтерфейсе, путем увеличения ключа шифрования и обеспечение защиты сигнальной сети, которая в свою очередь служит основным протоколом в современных сетях мобильной связи. Практическая ценность работы состоит в том, что предложенные алгоритмы могут быть применены

на сетях мобильной связи Республики Беларусь для формирования комплексной системы обеспечения информационной безопасности мобильных сетей.

Личный вклад магистранта

Содержание диссертации демонстрируют личный вклад автора. Основные научные и практические результаты были получены лично автором.

В работах, опубликованных совместно, автор фокусируется на алгоритме формирования ключа шифрования в SIM-карте, а также алгоритме обработки сигнальных сообщений сети сотового оператора.

Научный руководитель Зельманский О.Б., кандидат технических наук, доцент, является соавтором основных публикаций. Он сформулировал цели и задачи исследования, выбрал методы исследования, участвовал в планировании работы и обсуждении результатов, интерпретировал и обобщал полученные результаты.

Теоретическая и методологическая основа исследования

В основу диссертации легли результаты известных исследований российских и зарубежных учёных в области информационной безопасности, концептуальных и методологических основ защиты информации. Для получения теоретических результатов исследования применялись методы защиты, используемые протоколах при передаче речевого трафика. Математическая модель формирования ключа шифрования осуществлялась на основе анализа метода проведения алгоритма формирования ключа шифрования в SIM-карте. Построения математической модели алгоритма формирования ключа шифрования осуществлены в программе LabVIEW.

Апробация результатов диссертации

Теоретические и практические результаты диссертационных исследований докладывались и обсуждались на следующих научных конференциях: XIV Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 25-26 мая 2016 г. и 52-я научная конференция аспирантов, магистрантов и студентов БГУИР, Минск, 25-29 апреля 2016 г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 1 печатные работы в сборнике «Тезисы докладов XIV Белорусско-российской научно-технической конференции»

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех глав, заключения, библиографического

списка. Полный объем диссертационной работы составляет 77 страниц, включая 55 иллюстраций, библиографический список из 36 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформулирована цель диссертации, изложены основные положения, выносимые на защиту.

В общей характеристике работы сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В первом разделе дано описание существующих методов функционирования мобильных телекоммуникационных сетей. Также в данной главе поставлена цель и дано обоснование задач, которые необходимо решить при рассмотрении методов защиты голосового трафика в сетях мобильной связи. Рассмотрены принципы построение сетей мобильной связи в Республике Беларусь, обработка сигнальных сообщений, рассмотрены различные сценарии обслуживания вызова. Дан анализ характеристик трафика в сетях мобильной радиосвязи.

Во втором разделе рассмотрены активные способы защиты речевой информации, которые направлены на:

− создание маскирующих акустических и вибрационных шумов в целях уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения средством акустической разведки речевой информации в местах их возможной установки;

− создание маскирующих электромагнитных помех в соединительных линиях в целях уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки в возможных местах их подключения;

− подавление устройств звукозаписи (диктофонов) в режиме записи;

− подавление приемных устройств, осуществляющих прием информации с закладных устройств по радиоканалу;

− подавление приемных устройств, осуществляющих прием информации с закладных устройств по электросети 220 В.

Наиболее распространенным способом защиты речевой информации

является создание маскирующих электромагнитных помех, которые обеспечивают невозможность выделения информационного сигнала средством разведки в возможных местах их подключения.

Построена математическая модель алгоритма формирования ключа шифрования, которая представлена на рисунке 1.

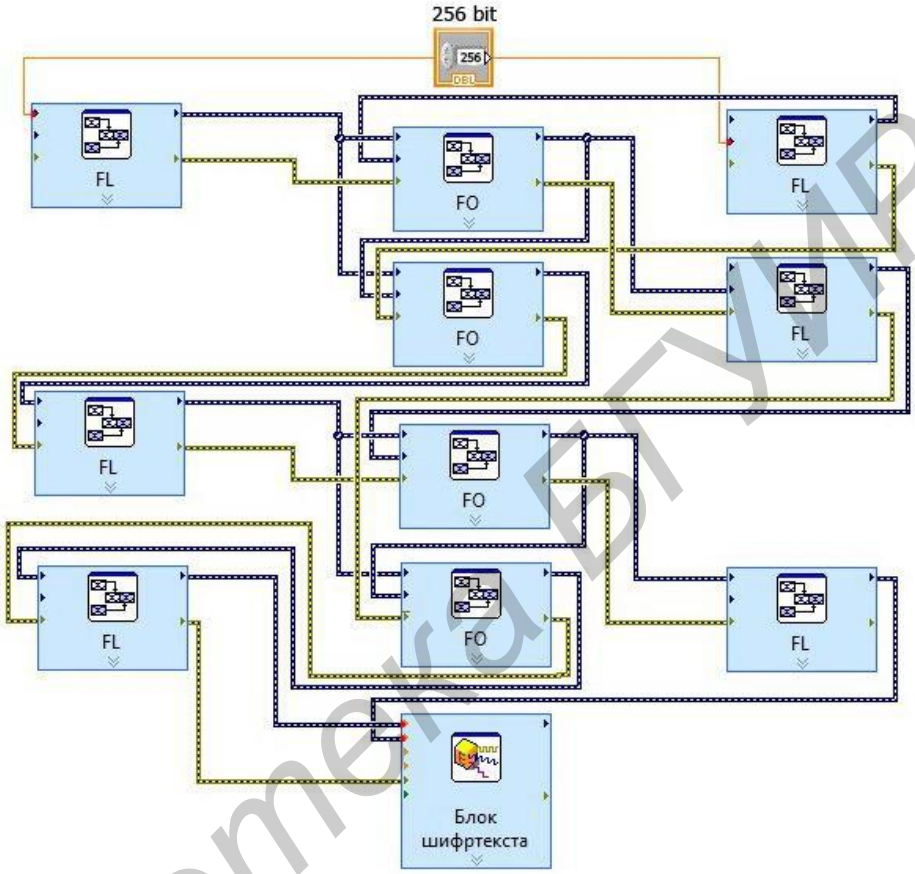

Рисунок 1 – Модель алгоритма формирования ключа шифрования

Представленная математическая модель, демонстрирующая перемещение некоторых битов ключа шифрования при сложении их друг с другом.

В третьем разделе сделан анализ результатов моделирования, который показал, что увеличив 128-битный ключ авторизации Ki, на 256-битный ключ мы сделаем алгоритм более сложным. Как следствие Центр Авторизации после генерации в ответ получит не 32 бита из последовательности, а 64-битную последовательность, что незначительно бы увеличило время, но в последующем существенно улучшило бы степень защиты. Далее алгоритмом A8 на Мобильной Станции, используя полученный RAND и имеющийся Ki, вычисляется сеансовый ключ Kc. Так же, он вычисляется и Центром Авторизации. После чего радиоканал считается шифрованным. Ключ Kc имеет длину 128 бит, образуется добавлением к 118 битам, полученным

данным алгоритмом, десяти нулевых битов – это значение и является входом для алгоритма шифрования A5 разговора (рисунок 2).

	0110001011001011
	0010111001000110
	1001011000100110
	0110010111000100
0110001011001011	1101010011010011
0010111001000110	0001101110010110
1001011000100110	0100110001011001
0110010000000000	1100010000000000
а)	б)

а) 64-битный ключ; б) 128-битный ключ

Рисунок 2 – Примеры кода алгоритма

Исходя из рисунка 2 видно, что степень защиты ключа шифрования увеличилась во много раз. Так же следует заметить, что время, затраченное на данный шифр тоже увеличилось, но оно незначительно по сравнению с тем временем, которое необходимо потратить злоумышленнику на его взлом. И если это не полностью позволит защитить телефон от прослушки, то хотя бы сильно усложнит задачу взломщику.

ЗАКЛЮЧЕНИЕ

Полученные в рамках диссертационной работы теоретические и практические результаты направлены на совершенствование защиты речевого трафика в сетях мобильной радиосвязи.

1. Проанализировав особенности передачи речевого трафика в сетях мобильной радиосвязи, можно сказать, что существующие сейчас цифровые сети сотовой связи характеризуются относительно не высокими значениями скорости передачи данных, малыми размерами кадров и преобладанием режима коммутации каналов.

Изучив протоколы, используемые при передаче речевого трафика, их характеристики, выявив их достоинства и недостатки, можно сделать вывод, что наиболее лучшим протоколом при передачи речевого трафика в сетях мобильной связи является SS7. Он гарантирует безошибочную доставку данных от одного хоста к другому. Кроме того, SS7 выполняет прозрачную сегментацию и сборку пользовательских данных, а также управление потоком и предотвращение перегрузки. Так же был проведён анализ методов защиты в существующих протоколах, который позволил поставить цель и задачи

исследования, которые необходимо решить при написании магистерской диссертации.

2. Анализ возможностей управления и особенностей передачи речевого трафика в сетях связи показал, что на передачу данных по сотовым сетям и беспроводным ЛВС существенное влияние оказывают задержки и канальные ошибки. В условиях постоянного перемещения абонентов параметры потока ошибок постоянно меняются и плохо поддаются прогнозированию, также к высокому уровню ошибок приводят атмосферные явления в виде дождя, грозы и др.

Анализ алгоритма формирования ключа шифрования в SIM-карте показал, что абсолютно надёжного метода шифрования нет и при большом желании и возможности его можно взломать и извлечь ключ из SIM-карты. Поэтому с целью улучшения защиты алгоритма формирования ключа шифрования была построена математическая модель нового алгоритма, которая в свою очередь должна лучше защитить информацию от взлома.

3. Анализ результатов моделирования показал, что разработанная математическая модель алгоритма формирования ключа шифрования, а так же предложенный алгоритм обработки сигнальных сообщений по аналогии с системой firewall, не смотря на то, что получились более сложным и процесс формирования ключа шифрования проходит в два раза больше этапов и занимает немного больше времени на процесс аутентификации, он гораздо эффективнее ныне существующего алгоритма и способен более надёжно защитить передачу речевого трафика от взлома.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Абишев М.М. Защита речевой информации при передаче по сетям мобильной радиосвязи / М.М. Абишев, О.Б. Зельманский // Технические средства защиты информации: Тезисы докладов XIV Белорусско-российской научно-технической конференции, 25-26 мая 2016г., Минск. Минск: БГУИР, 2016. – с. 14