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

На правах рукописи

УДК 621.396.2:004.056.53

ВОЛЧАНИН
Сергей Валерьевич

ЗАЩИТА РЕЧЕВОГО ТРАФИКА В СЕТЯХ МОБИЛЬНОЙ РАДИОСВЯЗИ

Автореферат
на соискание степени магистра техники и технологии
по специальности 1-39 81 01 Компьютерные технологии
проектирования электронных систем

Научный руководитель
канд.техн.наук, доцент
ЛИХАЧЕВСКИЙ Дмитрий Викторович

Минск 2015

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**Лихачевский Дмитрий Викторович,** кандидат технических наук, доцент, декан факультета компьютерного проектирования-учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Рецензент:	**Бондарик Василий Михайлович,** кандидат технических наук, доцент, декан факультета непрерывного и дистанционного обучения учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «23» января 2015 г. года в $9^{\underline{50}}$ часов на заседанииГосударственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г.Минск, ул. П.Бровки, 6, 1 уч.корп., ауд. 415, тел.: 293-20-88, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Создание специальных терминалов и программных обеспечений для защиты разговора по мобильным сетям диктовалось жесткой необходимостью − применяемые в стандарте мобильной связи шифры, при наличии должного оборудования, «снимаются» вместе с закрытой им 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 свободном режиме. Поэтому несколько лет назад возник вопрос «закрытия» канала сотовой связи с гарантированной конфиденциальностью на всем участке – от аппарата до аппарата абонентов. Решений этого вопроса, как водится, множество − от специальных терминалов, которые обмениваются информацией, закодированной очень надежно (даже если передачу перехватят, то «расколоть» 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

Актуальность темы исследования

Безопасность и конфиденциальность переговоров важны для любого бизнеса. Из существующих в мире стандартов сотовой связи самыми защищенными являются GSM, UMTS и CDMA. Однако «встроенной» защиты голосового трафика «силовикам» и бизнесменам уже недостаточно – перехватить их разговор можно если не с помощью специального оборудования, то с помощью электронных систем типа всемирно известного «Эшелона». Это и делает представленную тему диссертации актуальной.

Степень разработанности проблемы

Исследование криптографическихметодовзащитыинформации в телекоммуникационных системах представлены в работах Ю. Ветров, С. Макаров и других авторов. Защита информации в сетях сотовой связи пред-

ставлено в работах Б. Анин, Ю.Громаков, А. Крупнов, Л. Варакин.

Авторами российских работ, посвященных изучению информационной безопасности, концептуальных и методологических основ защиты информации, являются А. Малик, В. Мельников, С. Клейменов, А.Петраков.

Одним из недостатков защиты речевого трафика, является ненадёжность генерируемого кода алгоритма шифрования. Предложенное исследование направлено на устранение этого недостатка на основе модификации алгоритма формирования ключа шифрования.

Цель и задачи исследования

Целью диссертационной работы является исследовать методы защиты речевого трафика в сетях мобильной связи, выявить их достоинства и недостатки, и предложить меры по их усовершенствованию.

Для выполнения поставленной цели в работе были сформулированы **следующие задачи**:

− изучить литературно-патентные источники информации;

− определить существующие методы защиты речевого трафика в сетях мобильной связи;

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

− провести моделирование формирования ключа шифрования в SIM-карте;

− сделать вывод об эффективности предложенного метода.

Объектомисследования является защита речевого трафика в сетях мобильной радиосвязи.

Предметомработы выступает алгоритм формирования ключа шифрования для защиты речевого трафика в сетях мобильной радиосвязи.

Область исследования. Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем»

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, используемыев 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. Обработка статистических данных проводилась с использованием MSExcel.

Информационная базаисследования защиты речевого трафика сформированы на основе статистических данных.

Научная новизнадиссертационной работы заключается в разработке алгоритма формирования ключа шифрования.

Основные положения, выносимые на защиту

1. Анализ методов защиты в существующих протоколах: криптографическая защита информационных ресурсов систем сотовой связи с использованием алгоритмов A3, A5 и A8, носителем которых, за исключением A5, является SIM-карта абонента.

2. Анализ метода проведения алгоритма формирования ключа шифрования в SIM-карте и построение математической модели алгоритма формирования ключа шифрования.

3. Реализация разработанной математической модели алгоритма формирования ключа шифрования и результаты моделирования работы этого алгоритма показали, что разработанный алгоритм формирования ключа шифрования способен лучше защитить передачу речевого трафика.

Теоретическая значимостьдиссертации заключается в том, что в ней предложен алгоритм формирования ключа шифрования, позволяющий более надёжно защитить передачу речевого трафика. Представлена математическая модель, демонстрирующая перемещение некоторых битов ключа шифрования при сложении их друг с другом.

Практическая значимостьдиссертации состоит в том, что на основе предложенногоалгоритма формирования ключа шифрования возможна защита речевого трафика в сетях мобильной радиосвязи от взлома и прослушивания.

Апробация и внедрение результатов исследования

Результаты исследования были неоднократно представлены на XVIII Всероссийской научно-технической конференции студентов, молодых учёных и специалистов «Новые информационные технологии в научных исследованиях» (Рязань, 13-15ноября 2013 года), 7-й Международной студенческой научно-технической конференции «Новые направления развития приборостроения» (Минск, 23-25 апреля 2014 года), Международной научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности» (Минск, 19 июня 2014 года), 50-ой Научной конференции аспирантов, магистрантов и студентов БГУИР «Проектирование информационно-компьютерных систем» (Минск, 24-28 марта 2014 года).

Публикации

Основные положения работы и результаты диссертации изложены в четырёх опубликованных работах общим объемом 5,0 стр. (авторский объем5,0 стр.).

Структура и объем работы.Структура диссертационной работы

обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх разделов, заключения ибиблиографического списка. Общий объем диссертации −69 страниц. Работа содержит 1 таблицу, 17 рисунков. Библиографический список включает 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** рассматриваются основные особенности передачи трафика в сотовых сетяхс учетом специфики стека TCP/IP применительно к канальному и транспортному уровням эталонной модели взаимодействия открытых систем (OSI). Можно выделить как общие, так и специфические характеристики названных сетей, влияющие на эффективность передачи трафика.

Современные цифровые сети сотовой связи второго поколения характеризуются относительно невысокими значениями скорости передачи данных, малыми размерами кадров и преобладанием режима коммутации каналов. В них реализован временной TDMA (GSM и D-AMPS) или кодовый множественный доступ CDMA (IS-95).

При передаче речевого трафика используются следующие протоколы:

1. Протокол TCPявляется самым популярным транспортным протоколом, который гарантирует безошибочную доставку данных от одного хоста к другому;

2. Протокол маршрутизации RIPпредназначен для сравнительно небольших и относительно однородных сетей, маршрут которого характеризуется вектором расстояния до места назначения.

3. Протокол маршрутизации IGRP предназначен для определения маршрутов, которые расположены внутри автономных систем и относится, поэтому, к классу протоколов InteriorGatewayProtocol. По способу сбора информации о маршрутах внутри автономной системе этот протокол относится к типу distant–vector.

4. Протокол маршрутизации Enhanced IGRP был разработан специалистами компании Cisco, и представляет собой дальнейшее развитие принципов, которые были заложены в IGRP. В частности, по отношению к протоко-

лу IGRP обеспечиваются следующие дополнительные возможности:

− поддержка внеклассовых IP сетей;

− передача частичных обновлений таблицы маршрутов;

− поддержка различных протоколов сетевого уровня.

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 ВТСС 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.

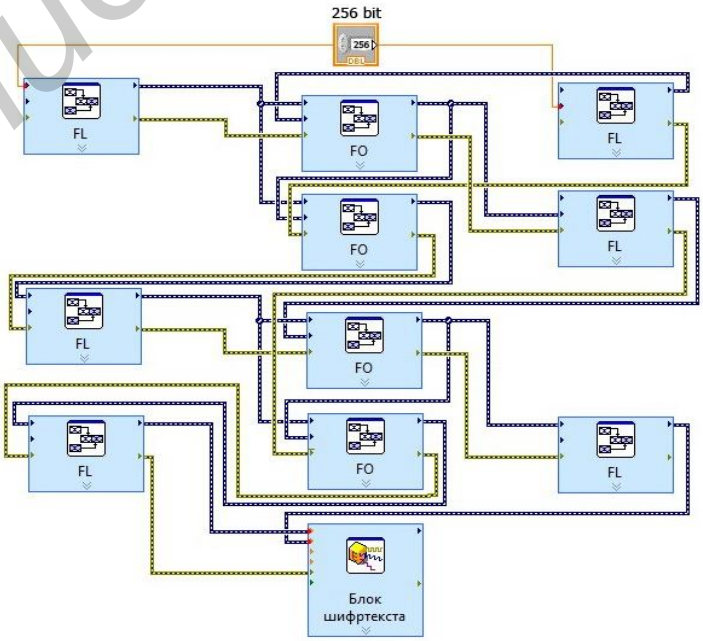

Рисунок 1 – Модель алгоритма формирования ключа шифрования

Представленная математическая модель, демонстрирующая перемеще-

ние 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
01100100000000001100010000000000
        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 отпрослушки, то хотя бы сильно усложнит задачу взломщику.

ЗАКЛЮЧЕНИЕ

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.

2. Изучив протоколы, используемые при передаче речевого трафика, такие как: TCP, RIP, IGRP, EIGRP, BGP, иххарактеристики, выявив их досто-

инства и недостатки, можно сделать вывод, что наиболее лучшим протоколом при передачи речевого трафика в сетях мобильной связи является TCP. Он гарантирует безошибочную доставку данных от одного хоста к другому. Кроме того, TCP 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.

3. 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.

4. Анализ метода проведения 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.

5. Приведена реализация разработанной математической модели алгоритма формирования ключа шифрования, приведены результаты моделирования работы этого алгоритма, которые показали, что разработанный алгоритм формирования ключа шифрования способен лучше защитить передачу речевого трафика. Сделаны выводы о его применимости и даны практические рекомендации по применению в существующих сетях мобильной радиосвязи.

Список опубликованных работ

[1–А]. Волчанин, С.В. Методы защиты речевого трафика в сетях мобильной радиосвязи / С.В. Волчанин / Новые информационные технологии в научных исследованиях : материалы XVIII Всероссийской научно-технической конференции студентов, молодых учёных и специалистов (Рязань, 13-15 ноября 2013 года) – Рязань : РГРТУ, 2013. – с. 260−261.

[2–А]. Волчанин, С.В. Алгоритм формирования ключа шифрования в SIM-карте / С.В. Волчанин / Новые направления развития приборостроения : материалы 7-й Международной студенческой научно-технической конференции (Минск, 23-25 апреля 2014 года) – Минск : БНТУ, 2014. – с. 6.

[3–А]. Волчанин, С.В. Увеличение степени защиты речевого трафика, посредством изменения алгоритма COM128 / С.В. Волчанин / Теоретические и прикладные проблемы информационной безопасности : материалы Международной научно-практической конференции (Минск, 19 июня 2014 года) – Минск : АМВДРБ, 2014. – с. 13.

[4−А]. Волчанин, С.В. Изменение регистра сдвига с линейной обратной связью в алгоритме А5 / С.В. Волчанин / Международная научно-техническая конференция, приуроченная к 50-летию БГУИР (Минск, 18-19 марта 2014 года) : материалы конференции в 2 ч.− Ч. 2. – Минск, 2014. –с. – в печати.