Эссе по курсу «Защита информации»

На тему:

«ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ МОБИЛЬНОЙСВЯЗИ»

(THE REVIEW OF PROBLEMS OF SAFETY MOBILE COMMUNICATION)

студента 014 гр. Химаныча С.Ю.

С момента появления первых мобильных телефонов прошло немногим более двух десятилетий. Несмотря на столь короткий период своего существования, технологии мобильной связи успели пройти в своем развитии три поколения.

Связь – одна из наиболее динамично развивающихся отраслей инфраструктуры современного общества. Этому способствует постоянный рост спроса на услуги связи и информацию, а также достижения научно-технического прогресса в области электроники, волоконной оптики и вычислительной техники. В активно разрабатываемой Международным союзом электросвязи концепции универсальной персональной связи большое место отводится сетям подвижной связи (СПС).

Преимущества СПС состоят в следующем: подвижная связь позволяет абоненту получать услуги связи в любой точке в пределах зон действия наземных или спутниковых сетей; благодаря научно-техническому прогрессу в технологии производства средств связи созданы малогабаритные универсальные абонентские терминалы, сопрягаемые с персональными компьютерами и имеющие интерфейсы для подключения к СПС всех действующих стандартов.

Сети подвижной связи можно разделить на следующие классы:

- сети сотовой подвижной связи (ССПС);
- сети транкинговой связи (СТС);
- сети персонального радиовызова (СПР);
- сети персональной спутниковой связи.

Все перечисленные классы представляют значительный интерес для научных исследований, однако в данной статье мы остановимся на рассмотрении класса сетей сотовой подвижной связи ввиду того, что эволюция ССПС в последние годы набирает стремительные темпы, возрастает масштаб применения услуг подобного рода сетей, экономическая значимость сотовой связи на мировом телекоммуникационном рынке становится первостепенной. Ожидается, что к 2010 году мобильная связь превзойдет фиксированную телефонию как по общему объему абонентской базы, так и по разнообразности и общедоступности услуг связи и информации [4].

В рамках данной статьи мы планируем исследовать эволюцию ССПС поколение за поколением, попытаемся проанализировать недостатки каждого из них, прежде всего с точки зрения информационной безопасности применяемых технологий, приведшие к смене данного поколения на следующее, а также понять, как эти недостатки нивелируются технологиями последующих поколений.

Появлению сетей сотовой связи предшествовал долгий период эволюционного развития радиотелефонной системы связи (РСС), в течение которой осваивались различные частотные диапазоны и совершенствовалась техника связи. Идея сотовой связи была предложена в ответ на необходимость развития широкой сети подвижной РСС в условиях ограничений на доступные полосы частот.

В эволюционном развитии ССПС можно выделить три поколения: первое – аналоговые системы; второе – цифровые системы; третье – универсальные системы мобильной связи недалекого будущего.

Все первые системы, или, как их еще называют, стандарты, сотовой связи были аналоговыми. Рассмотрим основные из них.

AMPS (Advanced Mobile Phone System) – известен также как «североамериканский стандарт». Был разработан в исследовательском центре Bell Laboratories, США. В 1983 году вступил в коммерческую эксплуатацию на территории США.

NMT-450 (Nordic Mobile Telephone) – используется в Скандинавии и во многих других странах, известен также как «скандинавский стандарт». Работы по его созданию начались в 70-х годах учеными 5 стран: Швеции, Финляндии, Исландии, Дании и Норвегии. Эксплуатация первых коммерческих систем сотовой связи этого стандарта началась в 1981 году. На базе этого стандарта в 1985 году был разработан стандарт NMT-900, который позволил расширить функциональные возможности и значительно увеличил абонентскую емкость системы.

В 1985 году в Великобритании был принят в качестве национального стандарта TACS (Total Access Communication System), разработанный на основе американского AMPS. Во Франции также в 1985 году был принят стандарт Radiocom-2000.

Во всех аналоговых стандартах применяется частотная (ЧМ) или фазовая (ФМ) модуляция для передачи речи и ЧМ для передачи информации управления. Для передачи информации различных каналов используются различные участки спектра частот – применяется метод множественного доступа с частотным разделением каналов (Frequency Division Multiple Access – FDMA) с полосами каналов в различных стандартах от 12,5 до 30 кГц.

Подобный принцип построения связи имеет ряд существенных недостатков: отсутствие эффективных методов борьбы с замиранием сигналов под влиянием окружающего ландшафта и зданий или вследствие передвижений абонентов, относительно низкая емкость, являющаяся следствием недостаточно рационального использования выделенной полосы частот при частотном разделении каналов и, самое главное, – беспрепятственная возможность прослушивания разговоров посторонними лицами.

Согласно статистическим данным от 40 до 80 % радиообмена, ведущегося с помощью сотовых телефонов, работающих в аналоговых стандартах, случайно или преднамеренно прослушивается . Электронный перехват подобного вида сотовой связи не только легко осуществить, он к тому же не требует больших затрат на аппаратуру, и его почти невозможно обнаружить.

Принцип передачи информации в аналоговых стандартах основан на излучении в эфир радиосигнала без предварительного шифрования и, соответственно, последующего дешифрования информации, поэтому любой человек, настроив соответствующее радиоприемное устройство на ту же частоту, может услышать каждое слово. Для этого даже не нужно быть обладателем особо сложной аппаратуры. Разговор, ведущийся с аналогового сотового телефона, может быть прослушан с помощью свободно продающихся специальных программируемых сканеров с полосой приема 30 кГц, способных осуществлять поиск в диапазоне 860–890 МГц. Для этой же цели можно использовать и обычные сканеры после их небольшой модификации, которая, кстати,

весьма подробно описана в Интернете. Перехватить разговор можно даже путем медленной перестройки УКВ-тюнера в телевизорах старых моделей в верхней полосе телевизионных каналов (от 67 до 69), а иногда и с помощью обычного радиотюнера. Наконец, такой перехват можно осуществить с помощью ПК.

Таким образом, понятно, что аналоговые мобильные сотовые телефоны являются абсолютно уязвимыми с точки зрения защиты передаваемой информации. Этот недостаток в купе с остальными вышеперечисленными обусловил появление цифровых ССПС.

Переход к цифровым системам также стимулировался широким внедрением цифровой техники в отрасль связи и в значительной степени был обеспечен разработкой высокоэффективных, скоростных криптографических алгоритмов.

Основные цифровые стандарты ССПС

D-AMPS (Digital AMPS) – ввиду того что аналоговый американский стандарт AMPS получил в США столь широкое распространение, прямая замена его цифровым стандартом оказалась практически невозможной. Выход был найден в разработке двухрежимной аналого-цифровой системы, позволяющей совмещать работы аналоговой и цифровой систем в одном и том же диапазоне. Разработанный стандарт получил наименование D-AMPS – «цифровой AMPS». Работа над этим стандартом была начата в 1988 году, а первая коммерческая сеть стала функционировать в 1993 году.

GSM – наиболее широко распространенный в мире стандарт. Создан по инициативе специальной группы подвижной связи Group Special Mobile (GSM), организованной в рамках Европейского института телекоммуникационных стандартов (ETSI). Основная причина появления – сложная ситуация в Европе, обусловленная наличием множества несовместимых аналоговых систем, в результате чего в 1982 году были начаты работы по разработке единого общеевропейского стандарта GSM 900. В 1987 году были определены все основные характеристики системы, в 1988 – приняты основные документы. Первая коммерческая сеть, работающая в стандарте GSM, была развернута в Германии в 1992 году. С тех пор стандарт непрерывно развивается и совершенствуется. Он уже адаптирован для работы в частотном диапазоне 1800 МГц (GSM 1800) и 450 МГц (GSM 400) в Европе и 1900 МГц (PCS) в США.

CDMA (Code Division Multiple Access – множественный доступ с кодовым разделением каналов). Первые научные материалы, описывающие принцип CDMA, появились в СССР еще до Великой Отечественной войны, а в последующих десятилетиях данная технология уже широко использовалась в военных системах связи как СССР, так и США. Возможности цифровой сотовой системы связи на основе кодового разделения каналов были впервые продемонстрированы американской компанией Qualcomm в ноябре 1989 года в Сан-Диего, которые подтвердили исключительно высокие характеристики системы, отличающие ее от систем других стандартов. На наш взгляд, CDMA является переходным этапом от второго к третьему поколению ССПС, так как в отличие от остальных цифровых систем второго поколения, основанных на методе множественного доступа с временным разделением каналов (Time Division Multiple Access – TDMA), этот стандарт основывается на методе множественного доступа с кодовым разделением каналов (Code Division Multiple Access – CDMA). В результате этого достигается многократное использование одного частотного канала во всех сотах, а также улучшенная защищенность передаваемых данных (CDMA использует более 4,4 триллиона кодов для

разделения индивидуальных вызовов, обеспечивая защиту и предотвращая несанкционированные подключения).

JDC (Japanese Digital Cellular) – японский стандарт цифровой сотовой связи. Новое название PDC (Personal Digital Cellular) – персональная цифровая система сотовой связи. Был утвержден в 1994 году в Японии. Развертывается в основном для национального использования и не оказывает существенного влияния на мировой рынок. В Японии сеть PDC обеспечивает покрытие практически всей территории, на которой проживает около 99 % населения страны .

Итак, каковы характерные отличия цифровых ССПС:

- временное разделение режимов приема (передачи) пакетированных сообщений;
- методы борьбы с замиранием сигналов основываются на частотном разнесении посредством применения режима передачи с медленными скачками по частоте и тестировании канала;
- эффективные виды модуляции;
- низкоскоростные речевые кодеки;
- шифрование передаваемых сообщений и закрытие данных пользователей посредством алгоритма RSA.

Однако так уж устроен мир, что любое техническое изобретение человеческого разума, расширяющее наши возможности и создающее для нас дополнительный комфорт, неизбежно содержит в себе и отрицательные стороны, которые могут представлять потенциальную опасность. Не являются исключением в этом плане и системы ССПС второго поколения. Да, они несоизмеримо расширили нашу свободу, дав нам возможность в любое время и в любом месте связаться с необходимым корреспондентом. Достаточно, на первый взгляд, защитили нас от разного рода злоумышленников. Тем не менее подводные камни и ловушки все же существуют. Попробуем с ними разобраться.

Главная забота современных сотовых операторов, помимо конкуренции друг с другом – это борьба с разными видами телефонного фрода (от англ. fraud – мошенничество). Это махинации с контрактами и счетами, хищение и клонирование сотовых телефонов, а также другие изощренные способы обмана сотовых компаний. По оценкам специалистов, общемировые потери операторов от мошенничества составляют 20–25 млрд долл. в год. Общая схема клонирования современных мобильных телефонов такова. В случае мобильных телефонов, работающих на базе аналоговых стандартов (AMPS, NMT-450 и т.д.) , мошенники с помощью сканнеров перехватывают идентифицирующий сигнал чужого телефона, которым он отвечает на запрос базовой станции по открытому радиосигналу, выделяют из него идентифицирующий номер ESN[1] и перепрограммируют этими номерами свои телефоны. В результате, стоимость разговора с этого аппарата заносится на счет того абонента, у которого эти номера были украдены. Кража номеров осуществляется, как правило, в деловых районах и в местах скопления большого количества людей: шоссе, дорожные пробки, парки, аэропорты. С помощью очень легкого, малогабаритного, автоматического оборудования, выбрав удобное место и включив аппаратуру, мошенник может за короткий промежуток времени наполнить память своего устройства большим количеством номеров. Наиболее опасным устройством является так называемый сотовый кэш-бокс, представляющий собой комбинацию сканера,

компьютера и сотового телефона. Он легко выявляет и запоминает номера ESN и автоматически перепрограммирует себя на них.

Что касается телефонов второго поколения, то здесь происходит клонирование SIM-карт. После того как в апреле 1998 года группе американских ученых удалось изготовить дубликат SIM-карты для телефона стандарта GSM, эта технология стала известна преступникам. И хотя в стандарте GSM невозможно просто сканировать и выделить серийный номер, как в устаревших стандартах, достаточно физически получить чужую SIM-карту в свое расположение на несколько часов – именно столько времени нужно, чтобы подобрать к ней код.

Из всех стандартов второго поколения особая роль в процессе эволюции систем связи отведена стандарту GSM. Сейчас более 20 млн абонентов относят себя к приверженцам этого стандарта. В России сети GSM появились с 3-летним отставанием, хотя уже в начале 1994 года GSM получил официальный статус российского федерального стандарта сухопутной подвижной радиосвязи. Стандарт тесно связан со всеми современными сетевыми технологиями, в последнее время успешно интегрируется с сетями с коммутацией пакетов, обеспечивая как мобильный доступ в Интернет, так и используя IP-сети в качестве среды передачи данных.
Разработчики GSM сумели применить множество оригинальных, новых для своего времени технических решений, благодаря чему GSM является признанным лидером среди стандартов второго поколения. Тем не менее второе поколение хотя и медленно, но уходит в прошлое.
Разберем недостатки систем второго поколения на примере стандарта GSM ввиду его широкой распространенности, чтобы понять, что послужило причиной появления стандартов третьего поколения.
В технической документации на стандарт GSM упоминается об использовании трех криптографических алгоритмов :

- A3 – алгоритма аутентификации;
- A5 – алгоритма шифрования данных;
- A8 – алгоритма формирования ключей шифрования.

Алгоритмы A3 и A8 могут модифицироваться каждой конкретной компанией-оператором, предоставляющей услуги сотовой связи в стандарте GSM. Алгоритм A5 – большой секрет. Он является собственностью международной ассоциации GSM MoU Association и распространяется под ее жестким контролем. Это первый, и, на наш взгляд, достаточно весомый недостаток стандарта, ибо основное правило криптографии – правило Керкхоффа – гласит, что весь механизм шифрования, кроме значения секретного ключа, априори считается известным противнику.

Шифрование передаваемых данных производится в соответствии с алгоритмом A5. Ключ шифрования вычисляется на основании тех же случайного числа и абонентского ключа по алгоритму A8. Длина ключа предположительно равна 56 бит, так как, что собой представляет алгоритм A5, держится в тайне.

Мобильные станции (телефоны) снабжены смарт-картой, содержащей A3 и A8, а в самом телефоне имеется ASIC-чип с алгоритмом A5. Базовые станции также снабжены ASIC-чипом с A5 и "центром аутенитификации", использующим алгоритмы A3-A8 для идентификации мобильного абонента и генерации сеансового ключа.

Как известно, A5 реализует поточный шифр на основе трех линейных регистров сдвига с неравномерным движением. Такого рода схемы на языке специалистов именуются "криптографией военного уровня" и при верном выборе параметров способны обеспечивать очень высокую стойкость шифра. Однако, в A5 длины регистров выбраны очень короткими - 19, 22 и 23 бита, что в сумме и дает 64-битный сеансовый ключ шифрования в GSM. Уже одни эти укороченные длины регистров дают теоретическую возможность для хорошо известной лобовой атаки, когда перебирают заполнение двух первых регистров (сложность порядка 240), восстанавливая содержимое третьего регистра по выходной шифрующей последовательности (с общей сложностью порядка 245).

До анализа A5 дошли руки у сербского криптографа д-ра Йована Голича специалиста по поточным шифрам . С чисто теоретических позиций он описал атаку, позволяющую вскрывать начальные заполнения регистров всего по 64 битам шифропоследовательности с трудозатратами около 240. Проведенный в стенах Microsoft эксперимент действительно привел к вскрытию ключа, но понадобилось для этого около двух недель работы 32-узлового кластера машин PII-300.

Иидентификация абонентов производится идентификационным центром на основании хранящегося в модуле SIM ключа (копия этого ключа хранится также и в центре). При идентификации на мобильный телефон передается случайное число. Это число вместе с ключом используется для шифрования ответа в соответствии с алгоритмом A3. Идентификационный центр сравнивает ответ с вычисленным им на основании тех же данных результатом. При их совпадении абонент считается идентифицированным.

Дополнительная защита обеспечивается за счет идентификации не только абонента, но и телефона. Как упоминалось в начале статьи, все телефоны имеют уникальные идентификаторы. Эти идентификаторы хранятся в реестре оборудования и разбиты на три списка — белый, серый и черный. В случае, если телефон находится в черном списке, его пользователю не удастся установить соединение с сетью. Это позволяет, например, воспрепятствовать использованию украденных телефонов.

В связи с недоступностью информации об алгоритме A5 о нем имеются достаточно противоречивые данные. По одним источникам , шифрование по алгоритму A5 заключается в выполнении операции «исключающего или» между кодирующей псевдослучайной последовательностью (ПСП) и 114-ю информационными битами каждого нормального слота[2]. Параметрами кодирующей ПСП является номер слота в гиперкадре[3] и ключ, задаваемый с использованием алгоритма A8 в процессе установления соединения. Процесс дешифрования представляет собой обратную операцию.

Согласно другим источникам, шифрование передаваемых сообщений и закрытие данных пользователей системы происходит по алгоритму шифрования с открытым ключом RSA. Однако в любом случае алгоритм A5 был принят в 1987 году, а с тех пор климат в криптографии изменился значительно. В связи с этим Группой экспертов по алгоритмам безопасности (SAGE)[4] был разработан новый алгоритм безопасности для GSM – A5/3. Он основывается на технических требованиях, разработанных 3GPP[5]. Базой для A5/3 служит алгоритм Касуми, утвержденный 3GPP для использования в третьем поколении мобильных систем в качестве ядра для алгоритмов конфиденциальности и целостности информации. Касуми, в свою очередь, был получен из алгоритма MISTY, разработанного корпорацией Mitsubishi.

Потребуется немало времени, прежде чем A5/3 будет полностью интегрирован в мировую мобильную сеть, и произойдет замена алгоритма A5 на новый. Возможно, этого не произойдет никогда ввиду наступления эры третьего поколения мобильной связи и бесперспективности инвестирования средств в реанимацию проектов второго поколения.

Таким образом, самый главный недостаток стандарта GSM, а также других стандартов второго поколения заключается в использовании старых (дата разработки – 70–80-е годы XX столетия), а соответственно, уже не надежных по нынешним временам (40-разрядные ключи шифрования, применяемые в настоящий момент в стандарте GSM, опытным специалистом с помощью мощного компьютера могут быть определены в течение нескольких минут) средств криптографической защиты информации.

Теперь становится ясно, почему уже в середине 90-х годов начались работы по разработке основных принципов стандартов третьего поколения, выбору технологий радиодоступа и закрытия данных.

В настоящий момент ETSI разработало стандарт UMTS (Universal Mobile Telecommunication System), который соответствует техническим спецификациям IMT-2000[6]. Хотя начальная фаза создания стандартов третьего поколения только подходит к завершению, в некоторых европейских странах уже выданы лицензии на эксплуатацию UMTS, а в ряде других – заявки на его использование находятся в стадии рассмотрения.

В качестве основы для UMTS европейские страны выбрали W-CDMA (WideBand Code Division Multiple Access – широкополосный множественный доступ с кодовым разделением каналов) – это некоторое расширение технологии CDMA, которая рассматривалась выше. Основным конкурентом W-CDMA будет технология cdma2000 компании Qualcomm, которая, возможно, найдет применение в японских компаниях, в настоящее время использующих технологию cdmaOne.

Итак UMTS – это высокоскоростная передача данных, мобильный Интернет, различные приложения на его основе, интранет и мультимедиа. Системы W-CDMA/UMTS включают усовершенствованную базовую сеть GSM и радиоинтерфейс по технологии W-CDMA. Скорость передачи в радиоканале для мобильного абонента достигает 2 Мбит/с.

Что касается принципов обеспечения безопасности в системах третьего поколения, то в начале 2000 года SAGE разработало для 3GPP два алгоритма, которые будут использованы для обеспечения конфиденциальности и защиты целостности информации, передаваемой по сети UMTS. Они основаны на блоковом алгоритме Касуми и будут принудительно использованы во всех будущих UMTS системах.

Также были разработаны алгоритмы аутентификации и распределения ключей, которые могут быть использованы операторами UMTS систем. Они, проходящие под одним названием – MILENAGE, были закончены в декабре 2000 года и опубликованы в 2001 году. В качестве ядра здесь использовался известный алгоритм Rijndael, который был отобран Американским национальным институтом стандартов и технологий (NIST) в качестве национального стандарта шифрования (AES – Advanced Encryption Standard).

Таким образом, понятно, что оба недостатка второго поколения успешно решаются в технологиях третьего поколения: все алгоритмы опубликованы, и в них применяются последние достижения в криптографии. Время покажет, как UMTS в роли основы мобильных технологий ближайшего будущего оправдает возлагаемые на него ожидания.

Ожидается, что в 2003 году количество абонентов мобильной связи превысит 1 млрд человек , хотя с момента появления первых мобильных телефонов прошло немногим более двух десятилетий. За этот небольшой период времени технологии мобильной связи успели пройти в своем развитии три поколения.

Как мы смогли убедиться, системы первого поколения, основанные на аналоговом принципе, первоначально использовались исключительно для телефонной связи, и лишь впоследствии обзавелись некоторыми базовыми сервисами. Телефонная связь, основанная на их применении, была практически не защищена от прослушивания. Системы второго поколения, включая стандарт GSM, предоставляют улучшенное качество передачи и защиту сигнала, дополнительные сервисы, низкоскоростную передачу данных, однако также являются весьма уязвимыми с точки зрения закрытия данных от мошенников, так как используют устаревшие принципы шифрования и недостаточную по сегодняшним меркам длину ключа.

Оптимальным образом отвечают на запросы современного рынка телекоммуникационных услуг системы мобильной связи третьего поколения, массовый запуск которых ожидается в 2003 году. Наибольший интерес представляет собой общеевропейская система UMTS, которая, во-первых, решает все недостатки предыдущих поколений, кроме того, значительно продвигается вперед как в области защиты информации, так и во всех других сферах мобильной связи. Так, планируется ввести новые средства защиты, включая UIM-модули, методы обнаружения «двойников», средства защиты в биллинговых операциях, новые подходы к идентификации неправомочных операций (в том числе на базе экспертных систем и алгоритмов нейронных сетей). Будут разработаны новые архитектуры аутентификации, биометрические методы идентификации пользователей и др

[1] *ESN - Electronic Serial Number (электронный серийный номер) - присваивается каждому сотовому телефонному аппарату.*

[2] *Слот - промежуток времени эфирного интерфейса GSM, его длительность составляет 577 мкс или 156,25 бита. Является составной частью гиперкадра.*

[3] *Гиперкадр - основной временной промежуток эфирного интерфейса GSM длительностью 3 ч 28 мин 53,760 с. Количество слотов в гиперкадре - 19 009 536 штук.*

[4] *ETSI SAGE (Security Algorithm Group of Experts) - технический комитет в рамках ETSI, ответственный за разработку всех криптографических алгоритмов, используемых в стандартах ETSI.*

[5] *3GPP - The 3rd Generation Partnership Project - проект, организованный для разработки и поддержки полного набора глобально применимых технических спецификаций для мобильных систем третьего поколения.*

[6] *В IMT-2000 в 1996 году была переименована инициативная группа, созданная в 1985 году на базе ITU (International Telecommunication Union), основной сферой деятельности которой является проектировка стандартов мобильной связи следующего поколения на глобальном уровне.*

ЛИТЕРАТУРА.

1. Р. Калаушин, Е. Крук. Обзор проблем безопасности мобильной связи зарождения и по настоящее время.
http://www.security.strongdisk.ru/i/127&all=1/

2. Стандарт GSM // LAN: Журнал сетевых решений. 2000. 6. № 7–8.
http://www.osp.ru/lan/2000/07-08/018.htm

3. Алгоритмы шифрования GSM и взлом (без автора)
http://spreed.by.ru/algoritm_gsm.html