УДК 621.37/39

Габиден Айнур – магистрант (г. Алматы, Казахская академия транспорта и коммуникаций им. М. Тынышпаева)

ЭВОЛЮЦИЯ МЕХАНИЗМОВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, РЕАЛИЗОВАННЫХ В ЛИНИЯХ СОТОВОЙ СВЯЗИ

При развитии сетей сотовой линии связи, присутствует принцип преемственности в процессах развития и конвергенции сетей. Особое внимание стоит уделить вопросам тарификации и оплаты услуг, безопасности передачи данных. Аналитические исследования в области информационной безопасности (ИБ) сетей показали, что в этих сетях существует ряд уязвимостей и рисков нарушения ИБ. Уязвимости, угрозы и риски ИБ носят специфический характер, все зависит от среды передачи данных, структуры сети связи, передаваемых данных, назначения сети и т.д. Однако очевидно, что в рамках процесса объединения различных сетей и расширения области их взаимодействия растет и риск преемственности одной сетью уязвимостей другой. При этом в объединенной сети будут присутствовать одновременно все специфические угрозы ИБ для каждой сети в отдельности, входящей в общую инфраструктуру.

В ракурсе этого вопроса немаловажной становится проблема изучения и исследования направления «информационная безопасность при интеграционных процессах сетей сотовых линий связи». О безопасности в сетях можно говорить как об определенном процессе, непосредственно связанном с функционированием сети связи. Эволюционные процессы, протекающие в рамках общего развития сетей, отразились и на механизмах и принципах реализации ИБ в сетях сотовой линии связи.

В таблице 1 представлены результаты анализа эволюции развития механизмов ИБ, реализуемых в сетях сотовой линии связи с момента появления, и перспективы их развития

Таблица 1–Развитие механизмов ИБ в линиях сотовой связи

	Развитие механизмов ИБ в линиях сотовой связи
Аналоговые сети 1-го поколения	• Идентификация абонента; • Механизмы аутентификации абонента
Сети стандарта GSM 2-го поколения	• Идентификация абонента; • Идентификация оборудования в сети; • Механизм аутентификации абонента; • Шифрование в каналах связи(алгоритм А5); • Шифрование в мобильном устройстве абонента (алгоритмы А3, А8)
Сети стандарта GSM/GPRS/EDGE поколения 2,5	• Идентификация абонента; • Идентификация оборудования в сети; • Механизм аутентификации абонента; • Новые алгоритмы шифрования в каналах связи(алгоритм GEA5); • Шифрование в мобильном устройстве абонента(алгоритмы А3, А8); • Универсальный протокол передачи данных, использующий принцип туннелирования (протокол GTP); • Механизмы защищенного взаимодействия между сетевыми компонентами, такими как SGSN и GGSN; • Механизмы управления межсетевым взаимодействием(использование пограничных шлюзов и межсетевых экранов)

Сети UMTS 3-го поколения	• Идентификация абонента; • Идентификация оборудования в сети; • Взаимную аутентификацию абонента и сети доступа; • Новые алгоритмы шифрования в каналах связи; • Шифрование в мобильном устройстве абонента; • Универсальный протокол передачи данных; • Механизмы защищенного взаимодействия сетевых компонентов; • Механизмы управления межсетевым взаимодействием (использование пограничных шлюзов и межсетевых экранов, оборудование Softwitch); • Широкополосные каналы передачи с кодовым разделением (W-CDMA); • Механизмы контроля за нарушениями использования ресурсов сети(механизмы антифрода); • Механизмы согласования прохождения аутентификации пользователем в домашней и гостевой сетях; • Механизмы регистрации событий с учетом наложенных на них ограничений; • Механизмы дополнительного управления аутентификацией при взаимодействии с интеллектуальной сетью

Как видно из таблицы, вопросы обеспечения ИБ в сетях сотовых линий связи с каждым новым этапом развития расширяются и включают в себя все больше механизмов обеспечения ИБ. При этом стоит отметить, что механизмы, зарекомендовавшие себя в предыдущих поколениях, учитываются при развитии сетей последующих поколений. Эти механизмы могут реализовываться в сетях нового поколения без изменений, а могут модернизироваться с учетом новых угроз ИБ.

Рассмотрим технические каналы утечки информации, передаваемой по каналам сотовой связи.

Большинство пользователей сотовой связи доверяют своему мобильному телефону самое сокровенное, не задумываясь об опасности прослушки. Специалисты в области безопасности признают, что мобильный телефон - это потенциальный шпионский «жучок», обладающий возможностью выдать секреты.

Принцип передачи информации мобильными телефонами основан на излучении в эфир радиосигнала. Согласно законодательству каждый оператор системы сотовой связи должен использовать определенный диапазон частот. Наиболее распространенные сотовые системы используют диапазоны 450, 800 и 900 МГц (стандарты NMT, AMPS и GSM) [1].

Всегда следует помнить, что абсолютно любой сотовый (мобильный) телефон можно прослушать. Организовать «прослушку», то есть прослушивать переговоры можно даже при "положенной" трубке сотового (мобильного) телефона.

Перехват информации происходит по электромагнитному каналу. Защита информации от утечки по электромагнитным каналам — это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Известны следующие электромагнитные каналы утечки информации:

- микрофонный эффект элементов электронных схем;
- электромагнитное излучение низкой и высокой частоты;

Для защиты информации от утечки по электромагнитным каналам применяются как общие методы защиты от утечки, так и специфические — именно для этого вида каналов. Кроме того, защитные действия можно классифицировать на конструкторско - технологические решения, ориентированные на исключение возможности возникновения

таких каналов, и эксплуатационные, связанные с обеспечением условий использования мобильных телефонов в условиях производственной и трудовой деятельности.

Защита от утечки за счет микрофонного эффекта:

Акустическая энергия, возникающая при разговоре, вызывает соответствующие колебания элементов мобильного телефона, что в свою очередь приводит к появлению электромагнитного излучения или электрического тока. Защита телефонного аппарата от утечки информации за счет микрофонного эффекта может быть обеспечена организационными или техническими мерами. Организационной мерой может быть – использование защищенного телефона, либо использование специальных технический средств, защищающих мобильный телефон.

Защита от утечки за счет электромагнитного излучения

Мобильный телефон, обладает основным электромагнитным излучением, специально вырабатываемым для передачи информации, и нежелательными излучениями, образующимися по тем или иным причинам конструкторско-технологического характера. Нежелательные излучения подразделяются на побочные электромагнитные излучения (ПЭМИ), внепобочные и шумовые. И те и другие представляют опасность. Особенно опасны ПЭМИ. Они-то и являются источниками образования электромагнитных каналов утечки информации. Каждое телефон является источником электромагнитных полей широкого частотного спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией. Известно, что характер электромагнитного поля изменяется в зависимости от дальности его приема. Это расстояние делится на две зоны: ближнюю и дальнюю. Для ближней зоны расстояние г значительно меньше длины волны (г << Х*)* и поле имеет ярко выраженный магнитный характер, а для дальней — (г >> Х) поле носит явный электромагнитный характер и распространяется в виде плоской волны, энергия которой делится поровну между электрическим и магнитным компонентами. С учетом этого можно считать возможным образование канала утечки в ближней зоне за счет магнитной составляющей, а в дальней — за счет электромагнитного излучения. В результате перекрестного влияния электромагнитных полей мобильного телефона в энергетическом помещении создается помехонесущее поле, обладающее магнитной и электрической напряженностью. Значение (величина) и фазовая направленность этой напряженности определяется числом и интенсивностью источников электромагнитных полей; размерами помещения, в котором происходит разговор; материалами, из которых изготовлены элементы телефона и помещения. Очевидно, чем ближе расположено оборудование относительно друг друга, чем меньше размеры помещения, тем больше напряженность электромагнитного поля.

Блокирование линий сотовой связи.

Блокираторы сотовой связи – это устройства, связанные с обеспечение безопасности и комфорта. Его назначение – блокировать сотовый телефон. Блокирование обусловлено двумя причинами: пресечение канала утечки информации (мобильный телефон является идеальным “радиожучком”) и соблюдение тишины, что актуально для музеев, театров, библиотек и т.д. Устройства, представленные на рынке, подавляют работу сотовых телефонов практически всех известных и распространенных сотовых стандартов.

Трезвон сотовых телефонов все сильнее раздражает людей в общественных местах. Почти во всех странах запрещено использование трубок в больницах и поликлиниках, где они могут помешать электронному оборудованию. Значки с перечеркнутыми трубками встречаются в аудиториях, где проводятся экзамены, на электростанциях, храмах и музеях. Во Франции некоторое время назад рассматривался законопроект, разрешающий установку мобильных блокираторов в библиотеках и музеях.

Убедились в необходимости устанавливать запрет на сотовые телефоны и священники. В мусульманских мечетях Саудовской Аравии он уже введен. В одной из католических церквей Испании мобильные телефоны больше не мешают проведению служб. Настоятель установил внутри храма электронное приспособление, блокирующее мобильные телефоны. Причиной, побудившей священника пойти на этот шаг, стали постоянные звонки телефонов, раздающиеся во время мессы и мешающие проявлению религиозных чувств.

Но отдельный и главный вопрос – это безопасность. Поскольку мобильный телефон может выступить в качестве взрывателя для различного рода бомб, глушение активно используется силовыми структурами. Особенно богатый опыт в этом отношении у израильских, американских и российских спецслужб – сказывается напряженная борьба с терроризмом. К примеру, при проезде высокопоставленных чиновников по правительственной трассе еще за пару минут до появления их автомобилей на дисплее мобильного телефона пропадает сотовая сеть и восстанавливается только через пару минут после удалившегося кортежа. Раньше в арсенале у сотрудников спецслужб были устройства, подавляющие активность радиовзрывателей с помощью излучения по широкому спектру радиочастот. Теперь же перешли на более современное оборудование.

В Казахстане применение блокираторов сотовой связи распространено гораздо меньше, чем на Западе. В основном в государственных учреждениях, при подавлении важных совещаний специальными службами.

Блокираторы можно порекомендовать и для защиты комнат переговоров, кабинетов руководителей компаний. Ведь лишняя перестраховка никогда не бывает лишней, особенно в век промышленного шпионажа.

Однако блокираторы сотовой связи могут быть использованы и злоумышленниками. Явный тому пример – подавление сигнала тревоги, идущего от системы охраны, оснащенного GSM передатчиком, к абоненту. Следует отметить, что не существует нормативно-правовых документов, регламентирующих продажу и использование блокираторов сотовой связи [2].

Использование сотового телефона в качестве радиозакладного устройства

Один из самых распространенных способов съема акустической информации - использование различных радиозакладных устройств, т.е. устройств, передающих акустическую информацию и/или сигналы с телефонной линии по радиоканалу. Принципиального различия между акустическими и телефонными радиозакладками нет. Средний радиус действия радиоканала - 200-300 метров, типовое время работы при использовании автономного питания - 2-3 дня, но может быть и значительно больше. При питании от внешних источников время работы практически неограниченно. Устройства с автономным питанием работают недолго, но проблем с их установкой значительно меньше. По степени разреженности источника питания можно приблизительно определить период времени, когда устройство было установлено. Например, нет смысла вспоминать, кто заходил в ваш офис неделю назад, если обнаруженная радиозакладка еще работает, а применяемый источник питания обеспечивает время автономной работы около 3-х дней. В качестве внешнего питания может быть использовано силовое питание 220В. Установка устройств с внешними источниками питания требует более сложной в организационном плане подготовки и исполнения. Как правило, необходимо проникновение в офис под видом ремонта чего-либо или тайное посещение в ваше отсутствие. Вопреки распространенному мнению о возможности подавления радиозакладок с помощью широкополосных генераторов радиошума, радиопередающие прослушивающие устройства плохо поддаются различным средствам радиопротиводействия. Несмотря на это, некоторые фирмы продолжают продавать генераторы широкополосных радиопомех для этих целей, которые именно из-за широкого спектра излучения не могут эффективно противостоять радиозакладкам средней

и даже малой мощности. Исключения составляют генераторы прицельной помехи, но для их работы необходимо сначала определить частоту излучения радиозакладки. Поэтому генераторы прицельной помехи работают в комплексе с приемной аппаратурой или в составе автоматизированных комплексов и стоят значительно дороже широкополосных генераторов.

В последнее время очень часто, в качестве радиозакладного устройства для съема информации используют сотовый телефон. Он не является техническим средством для негласного получения информации, т.е. риск при его применении для шпионских целей минимальный. Стоит значительно дешевле, чем большинство профессиональных радиозакладок, так что разницу в цене вполне можно отдать на оплату трафика. Наиболее часто его могут использовать непосредственно в процессе переговоров, но были случаи, когда его забывали или подбрасывали в офис.

Вывод. В статье проведен обзор угроз информационной безопасности линий сотовой связи организации. Была представлена эволюция механизмов защиты от НСД. Были рассмотрены технические каналы утечки информации, передаваемой по каналам сотовой связи, представлена схема утечки и перехвата информации, дана информация по блокированию линий сотовой связи в мирных целях, а также злоумышленниками, и было подмечено, что сотовый телефон можно использовать в качестве радиозакладного устройства. Любая компания в наши дни может быть подвержена угрозе в создании каналов несанкционированного доступа.

По результатам проведенного анализа можно сделать вывод, что линии сотовой связи представляют собой интегрированную структуру и включают в себя механизмы обеспечения информационной безопасности (ИБ) информации абонентов сети. При этом технологии связи, применяемые в сетях, продолжают развиваться, в том числе и механизмы обеспечения ИБ.

ЛИТЕРАТУРА

1.Романец Ю. В. Защита информации в компьютерных системах и сетях. /Под ред. В.Ф. Шаньгина. – М: Радио и связь 2009

2.Петраков А.В. Основы практической защиты информации. 2-е издание Учебное. Пособие. – М: Радио и связь 2010