Класс качества QoS LCS определяет степень выполнения требований к точности и времени задержки.

Для дополнительных услуг связи и услуг оператора PLMN справедливо следующее:

QoS LCS является несогласуемым параметром QoS. Поддержка класса QoS со стороны PLMN является опциональной. LCS-сервер может разрешить LCS-клиенту задать требуемое QoS (в контексте незамедлительного запроса местоположения) либо по предоставлению, либо по сформированному запросу. LCS-сервер будет пытаться как можно точнее удовлетворить параметрам другого качества услуги по отношению к требуемому классу QoS.

Для незамедлительного запроса на местоположение определены следующие классы QoS LCS:

А) "гарантированный": другие параметры качества должны выполняться обязательно. LSC-сервис получит текущее положение с выполнением требований, установленных к другим параметрам QoS. Если ответ на запрос на местоположение не удовлетворяет другим параметрам QoS, то этот ответ должен быть исключён.

Б) "без гарантии": другие параметры качества не обязаны выполняться строго. LSC-сервис получит текущее положение только с одной попытки с использованием только одной технологии с контролем выполнения требований к другим параметрам качества. Даже если другие параметры качества ответа на запрос местоположения не выполняются, этот ответ может быть передан на LSC-клиент.

Таким образом, требования к нормативным значениям показателей качества для услуг отслеживания местоположения мобильного телефона (украденного) и обнаружения факта клонирования могут быть разными. В случае поиска украденного телефона точность определения местоположения и время ответа должны быть минимальными, в то время как для обнаружения факта клонирования SIM-карты не требуется жесткое ограничение по времени ответа.

Подробную информацию о состоянии, тенденциях и проблемах развития рынка LBS-услуг можно найти в аналитических отчетах на сайте исследовательской компании "Современные телекоммуникации" www.modetel.ru, посвященных различным аспектам эволюционного развития услуг с добавленной стоимостью (VAS) в сетях сотовой подвижной связи: "Анализ мирового опыта внедрения сервис-функции E911/E112 для абонентов СПС с возможностью определения их местоположения" (август 2005 г.), "Анализ рынка телематических услуг на базе сетей GSM" (август 2006 г.), "Анализ рынка мобильного контента на сетях GSM России" (октябрь 2006 г.) и "Анализ состояния и тенденции развития российского рынка LBS-услуг на основе сетей СПС".

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ETCI TS 22.071 v 7.4.0 "Location Services (LCS), Service description; Stage 1, (Release 7)".

А.А. Гусаров, С.А. Таразевич, Г.Г. Хохлов
Россия, г. Санкт-Петербург, ЗАО «ТЕЛРОС»

ЗАЩИТА ИНФОРМАЦИИ В ВЕДОМСТВЕННЫХ И КОРПОРАТИВНЫХ СЕТЯХ СВЯЗИ

Опыт создания и функционирования современных ведомственных телекоммуникационных систем подтвердил экономическую и техническую целесообразность формирования их на базе арендованных магистральных линий передачи (телефонных каналов общего пользования – ТКОП) и создания на их основе систем передачи данных (СПД). Современные СПД представляют собой программно-

технические комплексы (ПТК), созданные на основе персональных компьютеров, высокоскоростных модемов и действующих каналов связи, в которых формирование и анализ сигналов выполняется как на аппаратном, так и на программном уровнях.

Характерной особенностью ПТК систем передачи данных является то, что в них интегрированы процессы ввода-вывода, защиты от ошибок, формирования и анализа сигналов. Кроме того, они выполняют и другие, не связанные с передачей данных, функции, такие как поиск и формирование файловых данных, компрессия и декомпрессия, защита от НСД и др. Следовательно, в СПД работающих по каналам ТКОП применяется аппаратура передачи данных с многовариантным набором компонентов и программно-технических средств с различными типами распределения обратного канала (частотным, временным) и с разным уровнем интеграции процессов, аппаратных и программных средств.

Однако следует отметить, что наряду с функциональной целесообразностью многообразие применяемых в СПД технических средств, функционирующих по различным алгоритмам, а также наличие значительного числа коммутируемых элементов, объективно создают предпосылки для несанкционированного доступа к конфиденциальной информации. Извлечение информации из СПД возможно посредством анализа особенностей физических процессов в элементах СПД, связанных с передаваемыми данными, сигналами синхронизации, автонабора, автовызова, автоответа, сигналами обратного канала, а также переходных процессов в цепях первичных источников питания АПД.

В качестве наиболее уязвимых мест, из которых возможно извлечение информации, кроме отдельных элементов СПД, следует рассматривать абонентские линии связи, распределительные щиты, коробки, коммутационное оборудование АТС, ГТС, МТС, системы уплотнения, антенно-фидерные системы, кабели. При этом возможности по добыванию информации из СПД в значительной мере будут определяться режимами их работы и характером взаимодействия технических средств разведки, СПД и их элементами.

Обобщая вышеизложенное, следует подчеркнуть, что ведомственные сети, сформированные на базе ТКОП, обеспечивая информационный обмен, не всегда могут обеспечить его конфиденциальность без применения специальных мер защиты.

Аналогичный вывод можно сделать и в отношении корпоративных сетей связи, основу которых составляют учрежденческо-производственные АТС (УПАТС) иностранного производства. Обладая множеством полезных для успешной и комфортной работы предприятия, учреждения (организации) функций, позволяющих полностью организовать процесс коммуникации, оптимизировать управление, сократить непроизводительные затраты рабочего времени, обеспечить своевременное прохождение информации, рационально использовать городские линии связи, обеспечить эффективное общение с потребителем, УПАТС иностранного производства могут стать постоянно действующим источником разведывательной информации за счет имеющейся возможности несанкционированного доступа к программным портам станции со стороны сети общего пользования.

Динамичное развитие информационно-телекоммуникационных технологий на основе широкого применения методов цифровой обработки ставит перед разведывательными службами промышленно развитых государств в качестве одной из приоритетных задач установление контроля над использованием технических средств информационных и телекоммуникационных систем. Для разведки телекоммуникационных сетей в настоящее время разработан и используется широкий спектр средств разведки. По данным специалистов США, утечка информации по

телефонным каналам составляет от 5 до 20% от общего количества информации, получаемой разведкой [1].

Кроме съема информации с абонентских линий связи значительную угрозу представляет возможность доступа к УПАТС и магистральным кабелям.

Как указывалось выше, главной угрозой для УПАТС импортного исполнения, являющихся основой корпоративных сетей связи, является возможность несанкционированного доступа к программным портам станций со стороны сети общего пользования. Такой доступ может быть инициирован из различных центров, в том числе и расположенных на значительном удалении (зарубежных центров) от объектов наблюдения; в частности, по открытому каналу сервисного обслуживания, а наличие недекларированных возможностей в программном обеспечении («программных закладок») УПАТС обеспечивает успешную реализацию акций нарушителей. Возможность скрытного доступа к УПАТС превращает ее в мощное средство сбора статистической и другой информации (включая прослушивание разговоров и помещений), управляемое дистанционно.

По командам, скрытно передаваемым на фоне другой информации в каналах связи, УПАТС переключается в режим сбора, накопления и замаскированной передачи информации на заданные номера телефонов, становясь, таким образом, дополнительным техническим средством разведки.

Программные и аппаратные закладки, реализующие упомянутые функции, весьма сложно выявить, особенно с учетом того, что ни один иностранный производитель не передает для анализа ни принципиальных схем, ни исходных текстов программного обеспечения. В таких условиях трудоемкость поиска закладок становится соизмеримой с разработкой нового аналогичного оборудования. Кроме того, дистанционная «перезаливка» программного обеспечения фирмой-разработчиком по каналам связи, ставшая практической нормой эксплуатации, не позволяет определить, какие модули программного обеспечения (ПО) в текущий момент исполняются в оборудовании. В этих условиях органы государственной власти, предприятия ОПК, другие предприятия и учреждения, использующие УПАТС иностранного производства, рискуют стать легкодоступным источником информации для технических разведок.

Рассматривая возможность съема информации с кабельных магистралей, следует отметить, что уязвимость этого элемента телекоммуникационной сети специалистами традиционно недооценивается. В то же время известны случаи попыток установления контроля за информационными потоками кабельных магистралей на только проложенных под землей, но и на значительных глубинах. Для этих целей разработаны специальные средства, которые посредством специального индуктивного датчика, охватывающего кабель, снимают передаваемую информацию. В качестве примера можно привести американскую систему «Крот», которая позволяет записывать информацию на диск специального магнитофона. После заполнения диска выдается сигнал и агент, при удобном случае, заменяет диск. Аппарат может записывать информацию, передаваемую одновременно по 60 каналам. Длительность беспрерывной записи составляет 115 часов [2,3].

Подтверждением активного вмешательства разведывательных служб в использование телекоммуникационных сетей является крупный шпионско-политический скандал 2006 года вокруг греческой сети сотовой связи Vodafone Greece, который однозначно указал на АНБ США и его главного партнера в американской IT-индустрии, компанию SAIC, в составе дирекции которой регулярно фигурируют бывшие высокие чины из разведслужб, ФБР и Министерства обороны.

Причиной скандала стала тайная программная закладка, обеспечившая перехват и прослушивание мобильной связи всей военно-политической элиты Греции, которая была встроена в аппаратуру Vodafone Greece в процессе модернизации при подготовке к Олимпиаде-2004 в Афинах. Когда независимая греческая пресса раскрыла эту шпионскую историю и опубликовала имена сотни лиц, «стоявших на «прослушке», то в списке, помимо высшего политического руководства Греции, фигурировали также греческие партнеры SAIC по афинским контрактам и военные чины, ведающие закупками вооружений для греческой армии. После публикации списка этим военным стали совершенно понятны причины поразительной удачливости их американских партнеров по переговорам, каждый раз добивавшихся максимально выгодных для себя условий сделок.

Для контроля программного обеспечения могут использоваться как изъяны в применяемом ПО, так и специально реализуемые мероприятия.

Несовершенство операционных систем (ОС) и программного обеспечения (ПО) — едва ли не главная причина ущерба, который может быть нанесен компьютерными злоумышленниками. В сетях появляется все больше вредоносного кода, который использует их для проникновения в компьютеры, выполнения запрограммированных действий и дальнейшего своего распространения. Статистика показывает, что количество уязвимостей растет год от года. По данным британской компании mi2g, специализирующейся на проблемах компьютерной безопасности, ежегодно хакерами взламывается до 90% сетей предприятий [4].

О несовершенстве одной из наиболее широко используемой в России операционной системы может свидетельствовать тот факт, что в 2005 году в ОС Windows было выявлено 812 «дыр» (исследования US-CERT). Специалисты из McAfee отмечают, что из 124 «дыр», обнаруженных в Windows XP Professional на сайте Secunia (Security Provider), 29 так и остались не устраненными, что дало компании основание присвоить Windows статус критически опасной ОС.

В операционной системе Windows Vista, поступившей в широкую продажу 30 января 2007 года, также обнаружена одна из первых уязвимостей. «Дыру» в системе User Account Control обнаружили специалисты компании eEye. Из соображений безопасности подробная информация об уязвимости не разглашается.

Подобное положение дел касается не только ОС Windows. Британские исследователи из группы mi2g наиболее безопасными платформами считают Apple Mac OS X и открытую версию UNIX - BSD (Berkeley Software Distribution). Операционные системы Linux и Microsoft Windows, напротив, были признаны слабо защищенными. Свои выводы специалисты mi2g сделали, проанализировав 235 тыс. успешных хакерских атак, проведенных во всем мире с ноября 2003 по октябрь 2004 года. Среди компьютеров под управлением ОС Linux взломанными оказались 65%, под управлением Windows - 25%.

В последнее время появилась информация, позволяющая сделать вывод о стремлении спецслужб сотрудничать с разработчиками ОС и ПО. В частности, то, что корпорация Microsoft на протяжении многих лет сотрудничает с АНБ США, секретом, в общем-то, давно не является. Хорошо известно, в частности, что именно АНБ, когда этого требовали американские законы, всегда контролировало понижение стойкости криптографии в программных продуктах, предназначенных для экспортных продаж. А значит, и в этом отношении Microsoft поневоле имеет многолетние, но не афишируемые контакты с Агентством национальной безопасности США [5]. Приведенные в [5] примеры свидетельствуют о том, что в современных условиях под различными, в том числе и такими благовидными, как борьба с терроризмом, предлогами, разведывательными службами промышленно развитых государств и, в первую очередь США,

прилагаются серьезные усилия для установления тотального контроля над ПО информационно-телекоммуникационных сетей.

Существенное значение для решения проблемы защиты информации вообще и в ведомственных и корпоративных сетях связи в частности имеет сам факт понимания важности этой проблемы. В этой связи весьма показательными являются результаты исследования "Средства защиты информации от несанкционированного доступа", проведенного журналом "Информационная безопасность/Information Security" (компания "Гротек) [4]. Большая часть опрошенных (39,8%) считают, что отечественные компании и организации весьма неохотно идут на увеличение расходов на информационную безопасность и выделяют на эти цели менее 5% от бюджета информационных технологий.

В то же время мировая статистика свидетельствует о том, что в большинстве зарубежных компаний, затраты на информационную безопасность составляют в среднем около 15% от бюджета информационных технологий компаний.

Отсутствие понимания важности и необходимости квалифицированного решения проблемы защиты информации приводит к тому, что во многих случаях в качестве панацеи от всех бед принимаются декларации фирм – разработчиков ОС и ПО. В качестве примера можно привести подход к позиционированию возможности применения сертифицированной по требованиям безопасности ОС Windows XP Professional, который используют некоторые поставщики услуг в области защиты информации. Они заявляют, что применение сертифицированной ОС Microsoft позволяет легально обрабатывать на клиентских рабочих местах конфиденциальную информацию, защищаемую в соответствии с законодательством Российской Федерации. При этом среди прочих преимуществ использования указанной сертифицированной ОС особо отмечается отсутствие необходимости установки дополнительных сертифицированных «наложенных» средств защиты информации. В порядке замечания отметим, что указанный тезис даже по формальным признакам в части «выполнения требований нормативных документов» не совсем корректен.

Изложенный выше подход, подкупающий простотой реализации и относительной дешевизной, не только не решает проблемы защиты информации с ограниченным доступом, но и вводит в заблуждение пользователей ПЭВМ и сетей связи.

Реальная безопасность информационной и телекоммуникационной инфраструктуры, в особенности критически важных объектов, может быть обеспечена только при условии развития современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, а также защиты информационных ресурсов от несанкционированного доступа, обеспечения безопасности информационных и телекоммуникационных систем [6].

Одним из значимых шагов в реализации указанных направлений следует рассматривать принятие Государственной Думой Федерального закона от 09 февраля 2007 года №14-ФЗ, основные положения которого направлены на обеспечение целостности, устойчивости функционирования и безопасности сетей связи общего пользования посредством их регистрации и оценки соответствия установленным требованиям проектной документации путем проведения экспертизы.

Заслуживает внимания также инициатива депутата Государственной Думы ФС РФ Ю.Г. Медведева по внесению на рассмотрение Правительства проекта закона «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры».

Предлагается реализацию мер по обеспечению информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры, включая функционирующие в их составе ключевые информационно-телекоммуникационные системы, возложить на субъекты информационной и телекоммуникационной инфраструктуры. Такие меры должны осуществляться ими как самостоятельно, с обязательным привлечением специализированных организаций в области обеспечения безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры, так и с участием федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, в области внутренних дел, по контролю и надзору в сфере государственной охраны, в области обеспечения безопасности, в области обороны.

Только при условии государственного подхода к решению проблемы защиты информации в телекоммуникационных сетях в РФ могут быть созданы условия для адекватного противодействия возросшим угрозам в информационной сфере.

Основываясь на изложенном, компания «ТЕЛРОС» строит свою деятельность по разработке и производству оборудования, проектированию и строительству телекоммуникационных сетей с учетом необходимости реализации организационных и технических решений по защите информации. В частности, специалистами ЗАО «ТЕЛРОС» разработана учрежденческо-производственная АТС (УПАТС) Т7, на которую получен Сертификат ФСТЭК России от 20 марта 2007 года №1359, который удостоверяет, что комплекс средств защиты информации указанной УПАТС разработан и изготовляемый является программно-техническим средством защиты информации и соответствует требованиям руководящих документов ФСТЭК России по 4 уровню контроля отсутствия недекларированных возможностей и 5 классу защищенности от НСД. УПАТС Т7 рекомендована к использованию в автоматизированных системах до класса защищенности 1Г включительно.

УПАТС Т7 - современная телефонная станция с расширенными функциональными возможностями. Аппаратная и программная части Т7 являются полностью универсальными, что позволяет путем простого конфигурирования программного обеспечения УПАТС создавать различные системы с множеством функций, удовлетворяющие самым разнообразным требованиям.

Определенный задел у компании «ТЕЛРОС» имеется и в изготовлении технических средств защиты информации в информационно-телекоммуникационных сетях - разработана автоматизированная система управления телекоммуникационным трафиком (АСУТТ), выполняющая функции телекоммуникационного экрана, обеспечивающего защиту УПАТС от несанкционированных действий. АСУТТ осуществляет непрерывный контроль всех каналов пользователей и служебных каналов на фазах установления и окончания соединений, а также в режиме разговора и фиксирует нарушения политики безопасности, принятой в организации, с определением вида сообщения в канале (голосовым, факсимильным, модемным). Помимо указанных функций, система обеспечивает автоматизированный сбор и анализ информации, циркулирующей в сети, что позволяет создавать портрет телекоммуникационного общения для каждого абонента, накапливать статистическую информацию и отслеживать динамику изменений, создавать базы данных атрибутивной информации по каждому соединению.

О возможностях компании «ТЕЛРОС» свидетельствует успешная реализация ряда крупных проектов. В частности, специалистами компании был разработан проект, осуществлено строительство и произведен монтаж оборудования телекоммуникационной сети Северо-Западного управления Федеральной пограничной

службы ФСБ России. По итогам выполненной работы Заказчик получил фрагмент современной цифровой телекоммуникационной сети, объединяющей в единое информационное пространство около 20 объектов управления. В проекте использованы системы коммутации, каналообразования и мультиплексирования российского производства. Аналогичные работы проводятся в настоящее время на Северо-Кавказском участке государственной границы России, где компания «ТЕЛРОС» приступила к реализации второго этапа строительства телекоммуникационной сети Пограничной службы в районе г. Сочи.

В целом же, обобщая вышеизложенное, следует подчеркнуть необходимость консолидации усилий всех заинтересованных ведомств и организаций для эффективного решения рассмотренных проблем информационной безопасности ведомственных и корпоративных сетей связи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Конахович Г.Ф.* Защита информации в телекоммуникационных системах. – Киев, МК-Пресс, 2005.

2. *Андрианов В.И., Бородин В.А., Соколов А.В.* «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие. - СПб: Лань, 1996.

3.. *Байков Е.А*. Разведывательные операции американского подводного флота (рассекреченные страницы). – СПб, Галея Принт. 2002.

4. *Щеглов А.Ю.* Почему мы не готовы к угрозам ИТ-безопасности? http://www.morepc.ru/security/sec220320071.html.

5. *Киви Берд*. Секретное оружие АСБ. //Компьютера, январь 2007.

6. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ 9 сентября 2000 г.

И.М. Исмаилов, Ф.Д. Касимов
Азербайджан, г. Баку, Национальная академия авиации

ОПТИМАЛЬНАЯ ДИНАМИЧЕСКАЯ ФИЛЬТРАЦИЯ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ПОМЕХ И АПРИОРНОЙ НЕОПРЕДЕЛЕННОСТИ ИЗУЧАЕМОГО ЯВЛЕНИЯ

Рост сложности объектов контроля в авиационной технике, увеличение источников информации, учет динамических свойств объектов и систем (большинство бортовых систем управления относятся к динамическим системам), возросшие требования к точности и объективности принимаемых решений поставили вопрос об автоматизации процесса диагностирования и прогнозирования. Вследствие этого появилась необходимость в автоматизации процесса контроля систем и комплексов авиационной техники в процессе эксплуатации на основе точной и достоверной измерительной информации, получаемой с помощью высокоэффективных информационно-измерительных систем (ИИС).

Необходимо отметить, что для объектов авиационной техники, находящихся в режиме полета, детерминированная связь между векторами пространства параметров и пространства наблюдений (результаты измерения) нарушается из-за действия помех и влияния различных случайных факторов как на объект, так и на систему регистрации записей полета, являющуюся основным источником информации. Такое положение свойственно, в частности, динамическим бортовым системам с их флюктуациями параметров за счет внешних и внутренних возмущений [1].

Из-за динамического характера контролируемых процессов в авиационно-вычислительном комплексе, протекающих под воздействием случайных влияющих факторов и стохастической природы помех и шумов, которые сопровождают