ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ (ВЕДОМСТВЕННЫХ) СЕТЕЙ СВЯЗИ

Ярмухаметов А.У.,
директор
по телекоммуникациям
ОАО "ICL КПО ВС",
г. Казань

ОБ АВТОРЕ:

Ярмухаметов Азат Усманович - директор по телекоммуникациям ОАО "ICL КПО ВС", г. Казань, Россия. Окончил Казанский авиационный институт в 1968 г. Работал на Казанском заводе ЭВМ, в НИИ вычислительных систем, Ассоциации производителей телекоммуникационной аппаратуры. Участвовал в разработке ЭВМ М-220М, М-222, ЕС 1033, главный конструктор ЭВМ ЕС1007. В области связи - руководитель разработки комплекса УСЛ-2 по проекту "Алмаз" (обитаемые космические станции), образующего сеть из ЦВМ НИПов и КВЦ и закладку на бортовую ЭВМ КС программ непосредственно из ЦВМ через командные радиолинии в реальном времени.

В ОАО "ICL - КПО ВС" с 1995 года. Имеет 35 авторских свидетельств СССР на изобретения и 96 зарубежных патентов, является автором 1 монографии и более 25 статей в специализированных изданиях.

Введение

В начале 90-х гг. прошлого века возникла новая угроза национальной безопасности. Появились такие понятия, как "информационное противоборство", "информационная война", "информационное оружие". В США, в Европе, а позже и в России стали проводиться НИОКР в области информационной безопасности (ИБ) и защиты информации, разрабатываться нормативные и руководящие документы, приниматься стандарты*.

В настоящее время вопросу информационной безопасности уделяется повышенное внимание на правительственном уровне Большой восьмерки. Президент США в начале 2000 г. принял "Национальный план защиты информационных систем", координирующий национальную программу ИБ на период до 2003 г. План состоит из десяти программ по принятию законов, определению угроз и критических точек, внедрению средств защиты, подготовки кадров, выполнению НИОКР. Отметим, что план предусматривает решение не только военных проблем, но и направлен на консолидацию усилий правительства, федеральных ведомств и частных компаний.

В промышленных группах США, наряду с Федеральным центром защиты инфраструктуры при ФБР США и Главным федеральным центром, предусмотрена организация собственных корпоративных центров анализа информации. Таким образом, в США создается многоступенчатая система информационной

* Обширная библиография приведена в журнале "ИНФОРМОСТ", № 2, 2002, стр. 11-12.*

защиты. После событий 11-го сентября вопросы информационной безопасности находятся под пристальным вниманием также и частных лиц.

Европейские страны приняли документ под названием "Общие критерии" (оформленный позже в виде стандарта ISO 15408:1999-1-3), упорядочивающий критерии безопасности.

В сентябре 2000 г. Президентом РФ утверждена "Доктрина информационной безопасности Российской Федерации". В развитии Доктрины Министерством связи и информатизации РФ разрабатывается "Концепция информационной безопасности сетей связи общего пользования ВСС РФ".

Некоторые наиболее "продвинутые" российские корпорации (Газпром, МПС) уже приняли собственные Концепции ИБ, в которых отражены также и проблемы безопасности принадлежащих им ведомственных сетей связи и передачи данных.

Внутренние водные пути (ВВП) России являются стратегическим объектом, и вопросы информационной безопасности инфраструктуры ведомственных сетей связи на ВВП также весьма актуальны.

Ключевые положения концепции

К сожалению, нередко проблемы информационной безопасности понимаются только как проблемы защиты информации. Применительно к ИБ сетей связи - это суть разные понятия. Остановимся на этом моменте подробнее.

Ключевой момент концепции ИБ - разделение понятий "информация абонента" и "сообщение". Абонент порождает "сообщение", которое содержит посылаемую информацию и служебную информацию (например, адрес получателя). **Сеть связи переносит сообщения**, представленные в виде электрических сигналов, **а не информацию абонентов.**

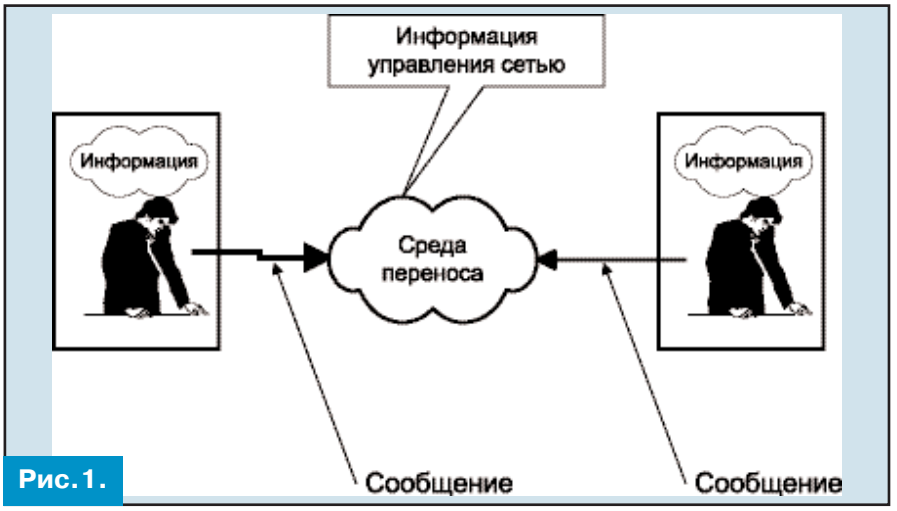

Рис.1.

Сообщения абонентов содержат некоторые данные (маршрут, сроки доставки, характер и состояние груза и судна, финансовые и отчетные документы), которые могут быть открытыми и закрытыми. Передача речи рассматривается как один из видов передачи данных.

При определении методов и средств защиты следует провести грань между защитой ***среды передачи данных (среды переноса)*** и защитой ***информации абонентов***, передаваемой этой средой.

В каком виде представлена информация абонента - кодированная, шифрованная, скремблированная, открытая - для сети связи ***(среды переноса)*** безразлично. ***Цель информационной безопасности сети связи*** - сохранить целостность циркулирующих данных. Введенные абонентом в сеть сообщения должны поступить адресату или его доверенному лицу без искажений, задержек и подмены. ***Защита же информации абонента - проблема самого абонента сети.***

Это не означает, что в сети не передается информация. Но ***это собственная, сетевая, служебная*** информация, предназначенная для управления работой сети или служб сети, которую, в свою очередь, также необходимо защищать от информационного оружия в целях обеспечения функционирования сети. Поэтому абонент со своей информацией отделяется от среды переноса. Принцип разделения формулируется так: ***абонент не является элементом службы переноса.*** Под абонентом понимается любой объект, порождающий или потребляющий информацию, например персональный компьютер, терминал позиционирования Инмарсат, транспондер АИС, система сигнализации и телеметрии, телефонный аппарат. В то же время абонент является элементом ***службы электросвязи***, так как порождает кроме данных также и ***управляющую*** информацию для сети, посылая сообщение. Иными словами, ***защита информации абонента и информационная безопасность сети связи - суть разные понятия.***

Такое разделение концептуально, так как позволяет четко установить границы ответственности, не возлагать несвойственные функции защиты абонента на аппаратуру и специалистов сети связи (экранирование кабинетов абонента, установка зашумителей, шифраторов, абонентских скремблеров, сетевых экранов и т.п.).

Объекты информационного нападения на сеть связи

Национальная сеть электросвязи состоит из:

- первичной сети, включаю-

щей международные и междугородние АТС и магистральные связи между ними;
- зоновых сетей, охватывающих региональные АТС;
- местных сетей (городские сети, ГТС);
- ведомственных сетей, подключенных к вышеуказанным сетям общего пользования.

АТС, стоящие на указанных сетях, взаимодействуют между собой посредством системы сигнализации. В настоящее время повсеместно вводится система сигнализации ОКС № 7, которая есть не что иное, как специализированная цифровая сеть пакетной передачи данных.

Объектами информационного нападения могут быть:
- цифровые АТС различного уровня;
- сеть сигнализации.

При введении в сеть связи "интеллектуальных сетей" (ИС), основной концепцией которых является динамическое управление программным обеспечением АТС из единого центра управления с целью оперативного внедрения новых услуг, объектом нападения будет также центр управления ИС и сеть управления ИС.

Поскольку наихудший результат нападения - это разрушение системы связи, то в цифровых АТС и системах цифровой передачи данных SDH, PDH (радиорелейных, кабельных, оптоволоконных) наиболее уязвимым элементом является программное обеспечение (ПО), которое и подвергнется нападению в первую очередь. Защитив ПО от несанкционированного вмешательства, мы с достаточной долей вероятности обеспечим целостность сети и ее элементов.

Очевидно также, что поскольку современное оборудование цифровой связи базируется на компьютерных технологиях, вопросы обеспечения информационной безопасности наиболее эффективно могут быть решены специалистами по вычислительной технике, имеющими соответствующий опыт и наработки.

Направления информационного нападения

Большинство проводимых работ и организационных мероприятий западных коллег сосредоточены вокруг защиты информации в сетях передачи данных и Интернета. Практически отсутствуют сведения о работах по защите собственно среды, в частности телефонной сети. Это неслучайно. Каждая страна-лидер строила свои телефонные сети на оборудовании собственной разработки и изготовленном отечественным производителем.

У нас же вся магистральная сеть телефонной связи, наиболее продвинутая часть зоновых сетей и корпоративные сети естественных монополий построены исключительно на импортном оборудовании. Это множество - S12, 5ESS, EWSD, DMS, AXE, NEAX, UT и прочие - специалисты именуют "зоопарком". Исключение составляют лишь сельские сети и некоторая часть бассейновых сетей ВВП.

Минсвязи РФ в лице начальника Управления безопасности связи В.М. Оранжереева признает: "...мы не можем знать абсолютно всего, что в этой технике заложено". Директор ЛОНИИС А.Н. Голубев еще более определенно заявил, что организовать закладку в отечественной АТС АТСЦ-90 можно в течение месяца, а искать такую же закладку (одну!) в импортной станции нужно не менее года. Таким образом, обеспечение безопасности сети телефонной связи сегодня можно считать очередной "российской национальной особенностью".

Рассмотрим возможные варианты информационного нападения на электронную АТС.

Поскольку АТС есть программируемая информационная система с множеством внешних связей, необходимо классифицировать тип связей и опасность вмешательства (рис 2).

Угрозы для цифровых АТС:

1. Угроза атаки через АРМ-администратора.
2. Угроза несанкционированного входа в АРМ-администратора.
3. Угроза модификации системного или программного обеспечения администрирования узла связи.
4. Угроза заражения файлов компьютерными вирусами.
5. Угроза прослушивания и модификации трафика.
6. Угроза модификации аппаратной части АРМ, АТС и линейной аппаратуры (вставка постороннего устройства).
7. Угроза отказа в обслуживании.
8. Угроза атаки через систему удаленного программирования и диагностики.
9. Угроза атаки через систему сигнализации и управления.
10. Угроза атаки наведенным сигналом.
11. Угроза атаки по абонентским линиям.
12. Угроза атаки через сеть электропитания.
13. Угроза атаки через системы тарификации и записи переговоров.

Входы в программное обеспечение АТС могут быть легальными и нелегальными.

К легальным входам относятся связи с системой удаленного программирования и диагностики и с локальной системой программирования и тарификации.

Остальные входы - нелегальные. При этом в современных АТС вход удаленного программирования может быть заблокирован парольной защитой или физическим отключением. В интеллектуальных сетях (ИС) указанный вход функционален и от-

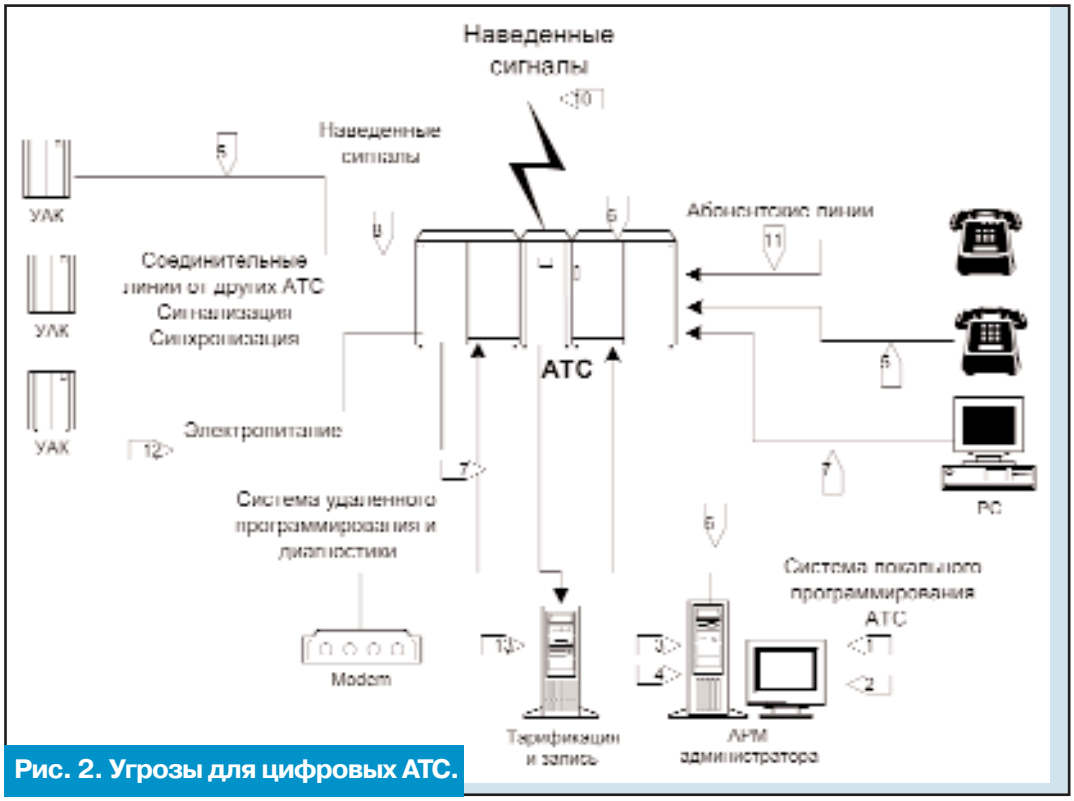

Рис. 2. Угрозы для цифровых АТС.

ключен быть не может.

а) Наибольшую опасность представляет вход удаленного программирования и диагностики АТС, функционально предназначенный для непосредственного вмешательства в ПО АТС.

б) Вход локального программирования и тарификации также очень опасен для ПО, однако, доступ к нему ограничен персоналом станции и безопасность может быть обеспечена организационными мерами.

в) Нападение по абонентским и соединительным линиям, а также со стороны системы сигнализации может быть произведено через включение в ПО "закладок", открывающих по кодовому сигналу доступ к ПО АТС с указанных направлений.

г) Нападение наведенным сигналом (например, с космического объекта) может быть осуществлено через аппаратурные закладки совместно с программными закладками.

д) Особой разновидностью может быть "внутреннее" направление, обеспеченное закладкой в ПО, срабатывающее от счетчика, даты или других внутренних факторов (на рис. не показано).

Методы защиты

Для эффективной защиты необходимо применять все возможные методы, начиная от организационно-технических мероприятий по охране объектов связи и кончая агентурно-оперативными по выявлению закладок непосредственно у разработчика и изготовителя систем коммутации. Основное же внимание следует сосредоточить на наиболее вероятном предмете нападения - программном обеспечении АТС.

Возможны три метода защиты ПО АТС:

· радикальный;
· консервативный;
· прагматический.

Радикальный метод защиты предполагает полную замену импортного фирменного ПО математическим обеспечением собственной разработки на основе защищенной операционной системы.

Консервативный метод заключается в исследовании фирменного ПО на предмет недокументированных возможностей (закладок) и устранение их.

Прагматический метод является комбинацией указанных выше методов и состоит в разработке защищающей оболочки (shell) для фирменного ПО.

Метод а) наиболее трудоемок, но в достаточной степени гарантирует устойчивость ПО при нападении. Пример: ЛОНИИС заменил фирменное ПО финской АТС DX-200 на ПО собственной разработки. Правда, на это потребовалось около 10-и лет (причем фирмой NOKIA были переданы все исходные тексты), и замена была произведена вовсе не с целью защиты.

Метод b) требует получения исходных текстов от разработчика ПО, что практически невозможно. Кроме того, всякая смена версии ПО потребует дополнительного исследования. Не исключено, что исследованию должен подвергаться каждый экземпляр поставляемой АТС. Опыт таких работ есть, но лишь применительно к офисным АТС.

Метод с) создания защитной оболочки наиболее реально осуществим, но при этом довольно трудоемок. Для его реализации требуется разработка специальных аппаратно-программных средств защиты: конвертеров и фильтров сигнализации, фильтров программирования АТС, кодировщиков (шифраторов) E1, использования технологии вир-

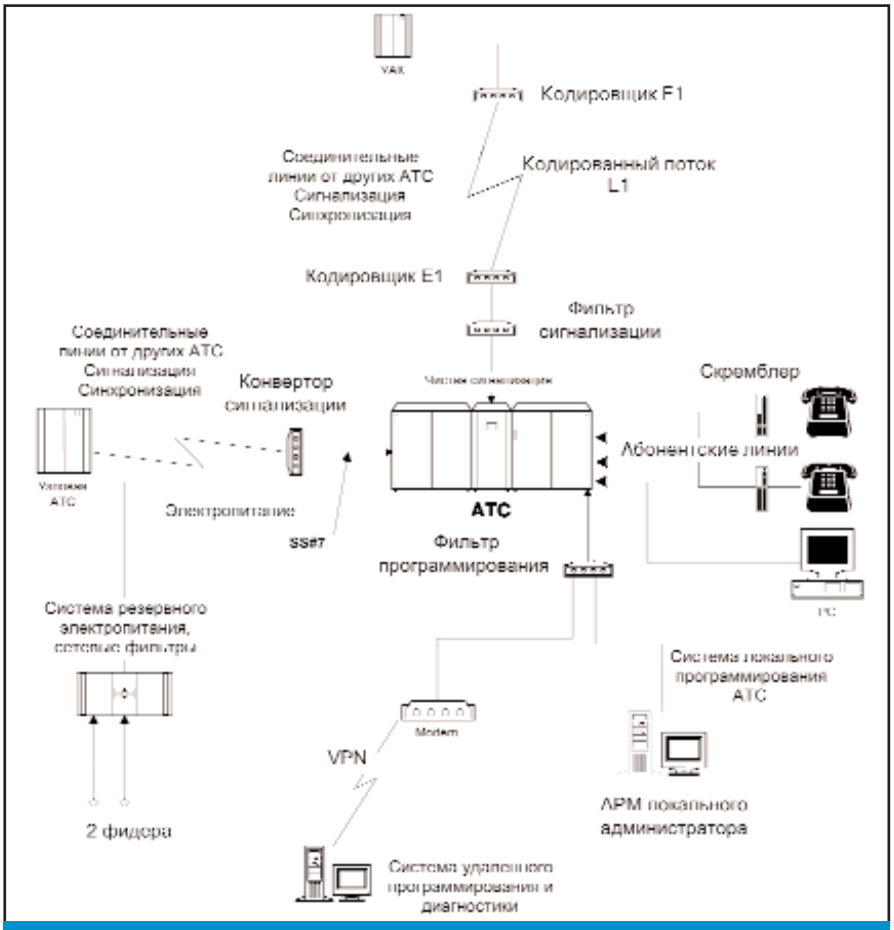

Рис. 3. Методы защиты ПО АТС и аппаратура защитной оболочки.

туальных частных сетей для туннелирования трафика управления и сигнализации (рис. 3). Первые попытки практической реализации такого подхода уже сделаны. Так, Гостехкомиссией в марте 2001 г. сертифицирована система разграничения доступа к функциям администрирования АТС Difinity G3siV8 для ЦДУ Министерства энергетики.

Все вышеизложенное об АТС в равной мере относится к выделенным сетям передачи данных и системам АИС.

Методика создания системы информационной безопасности сети связи

Смысл методики заключается в определенной последовательности действий по обеспечению безопасности ведомственной сети связи. Работы целесообразно поручить организации - системному интегратору, имеющему опыт выполнения таких работ и соответствующие лицензии. Последовательность работ следующая:

- обследование сети связи;
- разработка концепции защиты сети связи;
- выбор методов и оборудования защиты;
- разработка методики оценки эффективности защиты;
- обоснование инвестиций в защиту (расчет экономического эффекта в результате предлагаемых мер);
- разработка нормативно-методических документов (профилей защиты и заданий);
- создание центра информационной безопасности (Центра реагирования);
- создание испытательного (сертификационного) полигона;
- создание фрагмента (опытной зоны) защищенной сети и проведение натурных испытаний разработанных методов и аппаратуры;
- внедрение системы безопасности сети поэтапно в соответствии с концепцией по "мягкому" и "жесткому" сценариям.

Под "мягким" сценарием понимается защита сети в точках ее сопряжения с другими сетями (построение защитной оболочки самой сети) в предположении, что угроза сети вероятна извне, а собственные средства являются дружественными.

Согласно "жесткому" сценарию, угроза может исходить из всех направлений, в том числе от сопрягаемых элементов собственной сети в предположении, что вероятен "прорыв" ранее построенной защитной оболочки по "мягкому" сценарию и проведение атаки на узлы сети, не имеющие точек сопряжения с внешними сетями.

Заключение

Вопросы обеспечения информационной безопасности ведомственных сетей связи требуют глубокой научной проработки, а также проведения опытно-конструкторских работ по созданию аппаратно-программных средств защиты.

Владельцам (операторам) сетей следует преодолеть психологический барьер "возрастания стоимости" сети в связи с применением средств защиты и начать инвестировать разработки. Стимулом послужит осознание высокой вероятности понести ощутимый ущерб от простоя сети в случае доказанного (выявленного) нападения или удовлетворенного иска клиента от потери или утечки передаваемого оператором сообщения.

С автором статьи можно связаться по:
Тел.: (8432) 760432
E-mail: azat9@yandex.ru