УДК 654.151.2:65.012.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ СВЯЗИ

Конограй Наталья Алексеевна
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, romawka_nataliya@mail.ru

Современная информационно-телекоммуникационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Появление на отечественном рынке и внедрение в эксплуатацию современных импортных цифровых АТС приводят к повышению уязвимости телефонных сетей связи и информационных ресурсов организаций.

Ключевые слова – цифровая АТС, угроза, безопасность, методы защиты.

ВВЕДЕНИЕ

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, можно обеспечить целостность сети и ее элементов.

КЛАССИФИКАЦИЯ УГРОЗ В ЦИФРОВЫХ АТС

Незащищенная ЦАТС, являющаяся в повседневных условиях основным средством управления, а в ряде случаев базовым средством при создании телекоммуникационных сетей, может подвергаться определенным угрозам, таким как:

- атаки через АРМ-администратора;
- несанкционированного входа в АРМ-администратора;
- модификации системного или программного обеспечения администрирования узла связи.
- заражения файлов компьютерными вирусами.
- прослушивания и модификации трафика.
- модификации аппаратной части АРМ, АТС и линейной аппаратуры (вставка постороннего устройства).
- отказа в обслуживании.
- атаки через систему удаленного программирования и диагностики.
- атаки через систему сигнализации и управления.
- атаки наведенным сигналом.
- атаки по абонентским линиям.
- атаки через сеть электропитания.
- атаки через системы тарификации и записи переговоров.

В соответствии с законодательством, информационные системы органов государственной власти, организации, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем, подлежат обязательной сертификации по требованиям безопасности информации.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

МЕТОДЫ ЗАЩИТЫ ЦИФРОВЫХ АТС

Для обеспечения безопасной эксплуатации цифровых АТС проводится следующий комплекс работ:

- сертификация систем разграничения доступа к средствам администрирования цифровых АТС.
- аудит технологии эксплуатации ЦАТС, по результатам которого разрабатываются заключение и рекомендации по блокированию потенциальных угроз.
- проверка правильности и корректности настроек программного обеспечения и конфигурации цифровой АТС на объекте.
- определение и установка необходимых технических и программно-аппаратных средств защиты, разработка и реализация организационно-распорядительных мероприятий по защите.
- аттестация цифровых АТС, как объектов информатизации, на соответствие требованиям по безопасности информации с оформлением аттестатов соответствия по установленной форме.
- гарантийное и сервисное обслуживание СЗИ на предприятии.

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

Возможны три метода защиты ПО АТС:

1. Радикальный метод предполагает полную замену импортного фирменного ПО матобеспечением собственной разработки на основе защищенной операционной системы. Наиболее трудоемок, но в достаточной степени гарантирует устойчивость ПО при нападении.

2. Консервативный метод заключается в исследовании фирменного ПО на предмет недокументированных возможностей (закладок) и устранение их. Требует получения исходных текстов от разработчика ПО, что практически невозможно.

Любая замена версии ПО потребует дополнительного исследования.

3. Прагматический метод является комбинацией указанных выше методов и состоит в разработке защищающей оболочки (shell) для фирменного ПО. Для его реализации требуется разработка специальных аппаратно-программных средств защиты: конвертеров и фильтров сигнализации, фильтров программирования АТС, кодировщиков (шифраторов) Е1, использования технологии виртуальных частных сетей для туннелирования трафика управления и сигнализации.

ВЫВОД

Для устранения или сведения к минимуму возможного ущерба от действий потенциальных нарушителей информационной безопасности операторы сетей связи должны предпринять упреждающие меры предотвращения нарушений информационной безопасности, уделив достаточное внимание защите используемого ПО на цифровых АТС.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Радиоэлектроника и телекоммуникации (Электрон. ресурс) / Способ доступа: URL: http://masters.donntu.edu.ua/2011/fkita/zagumenjyk/library/article9.htm.

2. Информационная безопасность систем и сетей связи (Электрон. ресурс) / Способ доступа: URL: http://www.rnt.ru/to_content/action_desc/id_40/lang_ru/