Заборовский В.С.,
ЦНИИ РТК, Санкт-Петербург

Защита данных в ИПИ-системах: новое направление создания систем информационной безопасности

Всего несколько лет назад информационная безопасность в компьютерных сетях являлась, в основном, проблемой государственных организаций и крупных монополий, предоставляющих специализированные услуги связи. Однако ситуация кардинально изменилась, когда информационные технологии стали основой развития сетевой экономики и внедрения средств электронной торговли и построения ИПИ систем.

Внимание к безопасности информационных систем нарастает параллельно быстрому росту числа пользователей и важности информации, которая передается через такие сети. Эффективное решение проблемы защиты данных при использовании компьютерных телекоммуникаций становится необходимым условием ускоренного развития и эффективного функционирования всех современных крупных предприятий и корпораций, которые ориентированы на использование ИПИ систем.

В этих условиях под безопасностью компьютерных сетей стали понимать сопротивление любым действиям, которые могут поставить под угрозу доступность, аутентичность, целостность и конфиденциальность передаваемой информации. При использовании ИПИ систем требуется, чтобы все защитные действия не снижали общую сетевую производительность и скорость информационного обмена. Такая расширенная формулировка требований к сетевой безопасности приводит к необходимости разработки новых подходов и применения таких технических средств, которые с одной стороны позволяют обеспечить высокий уровень защиты данных, а с другой не требует существенной перестройки сетевой инфраструктуры или модификации протоколов межсетевого взаимодействия, которые традиционно используются для ИПИ приложений.

Важными требованиями, непосредственно влияющими на состав аппаратно-программных компонент систем защиты информации в ИПИ системах, становятся их надежность, скрытность и управляемость. Практическая реализация этих требований приводит к тому, что все активные компоненты системы безопасности должны функционировать в двух сетевых подпространствах, которые объединяют: 1) устройства защиты и управления, 2) устройства хранения и передачи данных.

Такая организация сетевой инфраструктуры позволяет обеспечить эффективную защиту информации как извне (передача и прием данных по внешним каналам связи), так и изнутри сети (защита от злонамеренных и/или ошибочных действий пользователей и операторов).

В ЦНИИ РТК ведется разработка новых подходов к построению систем информационной безопасности для ИПИ приложений, как с теоретической, так и практической точек зрения. Установлено, что эффективной может быть и весьма простая система безопасности, сам факт и характер функционирования которой скрыт от участников информационного обмена. В компьютерных сетях реализация различных методов сокрытия источников сообщений хорошо разработана и основана на использовании специальной или альтернативной системы адресации. Однако эти методы пока не нашли широкого применения в системах защиты для ИПИ систем. В ЦНИИ РТК принцип сокрытия адресов нашел свое применение при создании сетевых систем управления и по аналогии с известными примерами из области авиационной техники получил название «стелс» технологии.

С точки зрения практического использования это означает, что все интерфейсы сетевых устройств разделяются на две группы. Первая группа интерфейсов, которая связана с

открытыми сетевыми сегментами, не имеет ни физических, ни логических адресов. Поэтому сами эти интерфейсы не могут являться ни источником, ни приемником пакетов, однако они могут использоваться для обработки пакетного трафика с помощью специальных программно-аппаратных средств контроля и управления. Вторая группа интерфейсов имеет «ортогональную» систему адресации, т.е. эти интерфейсы связаны с каналами, которые физически отделены от открытого сетевого сегмента или Интернет. Описанный выше подход к построению систем информационной безопасности защищен патентом № 2000133391 от 29.12.2000г. и на его основе создан и сертифицирован Гостехкомиссией межсетевой экран ССПТ.

Применение межсетевого экрана ССПТ со «стелс» интерфейсами позволяет в полном объеме реализовать требования Гостехкомиссии к устройствам защиты 3 класса, а также обеспечить возможность координированного управления межсетевыми экранами по физически отделенным от открытого сегмента интернет сети каналам связи. Применение устройств со «стелс» интерфейсов не требует внесения изменений в сложившуюся систему маршрутизации. Последнее обстоятельство повышает уровень защищенности всей системы и позволяет объединять ССПТ в кластеры. При этом на рабочей станции оператора сетевой безопасности не требуется устанавливать дополнительного программного обеспечения, так как все транзакции осуществляются с использованием WEB интерфейса и стандартных протоколов межсетевого обмена. Это позволяет учитывать особенности изменяющейся структуры интернет сети и эффективно реализовывать корпоративную политику информационной безопасности при использовании нового класса ИПИ систем.