ПОДКЛЮЧЕНИЕ КЛЮЧЕВЫХ СИСТЕМ К СЕТЯМ ОБЩЕГО ПОЛЬЗОВАНИЯ

О.К. Барановский

Взаимодействие с обрабатывающими конфиденциальную информацию информационными системами (ИС), автоматизированными системами критически важных объектов (АС) должно осуществляться с использованием защищенных каналов передачи данных. Не допускается подключение одного из участников информационных отношений к сетям общего пользования. Межсетевые экраны, детекторы вторжений, VPN, средства антивирусной защиты не обеспечивают гарантированную защиту от утечки конфиденциальной информации и передачи команд деструктивного воздействия на ключевую систему (ИС или АС) в условиях применения продуктов информационных технологий импортного производства. Программные и аппаратно-программные агенты, внедренные в элементы ключевой системы (КС), могут устанавливать каналы связи с внешними субъектами, находящимися за пределами контролируемого периметра, по так называемым скрытым каналам (СК).

В этой связи при взаимодействии КС с внешними субъектами информационных отношений в создаваемых системах защиты информации предусматривают применение средств обнаружения и перекрытия (снижения до приемлемого уровня пропускной способности) СК. Для выявления СК используют статистические методы анализа пакетов в сетях передачи данных. Обнаруженные реализации СК в дальнейшем выявляют на основе сигнатурного анализа пакетов. В средствах перекрытия СК реализуют нормализацию временных интервалов между пакетами и нормализацию полей пакетов.

Расширение информационных связей между отдельными КС увеличивает вероятность реализации угроз установления СК с сетями общего пользования и недоверенными субъектами информационных отношений. Решение задачи перекрытия СК не может быть реализовано только правовыми и организационными мерами и требует обязательного применения технических средств защиты.