СОЗДАНИЕ ПОДСИСТЕМЫ ЗАЩИТЫ ОТ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

А.В. Пугач

В настоящее время внутренние факторы заметно опережают внешние в рейтинге угроз безопасности информации. Наибольшие опасения специалистов вызывают утечки данных (76%) и халатность сотрудников (67%). Поэтому крайне важно минимизировать негативное влияние внутренних нарушителей на работу организации путем своевременного их обнаружения, адекватного реагирования и применения к ним дисциплинарных и правовых мер пресечения. Для решения этой задачи необходимо активизировать весь арсенал доступных средств, включая юридические, организационные и программно-технические механизмы защиты.

С юридической точки зрения необходимо в соответствии с действующим законодательством закрепление за организацией патентных и авторских прав, а также прав на защиту товарных знаков и коммерческой тайны. Договор (контракт) с работником должен содержать перечень требований по неразглашению коммерческой (служебной) тайны и ответственность работника за неправомерные действия.

Политика безопасности организации должна четко определять, что вся информация, хранимая, обрабатываемая и передаваемая по каналам связи в корпоративной сети является собственностью этой организации. Должны быть

категорически и открыто запрещены несанкционированный доступ, раскрытие, дублирование, изменение, удаление и ненадлежащее использование сведений. Служебная информация должна использоваться только в производственных целях. Границы допустимого использования этих данных должно определять руководство организации. Пользователи информационных систем должны быть предупреждены, что все программно-аппаратное обеспечение находится под наблюдением, и в случае необходимости вся последовательность их действий может быть восстановлена.

Программно-технические средства защиты могут включать контекстные анализаторы, системы статической и динамической блокировки устройств.