ПРОГРАММНАЯ РЕАЛИЗАЦИЯ СЕТЕВОГО ПАКЕТНОГО ФИЛЬТРА НА ОСНОВЕ ДРАЙВЕРА NDIS

Е.Е. РАДИОНОВ

Защита персонального компьютера от внешних и внутренних сетевых атак является актуальной задачей. Так как аппаратные решения являются дорогостоящими, то использование программных средств безопасности позволяет существенно сэкономить, обеспечивая при этом достаточно высокий уровень защищенности. Предлагается метод реализации сетевого пакетного фильтра, основанного на использовании промежуточного драйвера NDIS (Network Driver interface specification). NDIS — стандарт, устанавливающий правила передачи сообщений между драйверами физических устройств и драйверами сетевых протоколов. Стандарт включает описание следующих компонент: NDIS упаковщика (предоставляет операционную среду для драйверов использующих NDIS), драйвера протоколов (TCP/IP), драйвера минипортов NIC (напрямую управляют NIC), промежуточных драйверов минипорта. Суть метода состоит в том, что NDIS помещается между драйвером сетевой карты и драйвером протоколов TCP/IP. Он становится виртуальным адаптером и NIC-драйвером для драйверов протоколов. Метод позволяет реализовать перехват поступивших сетевых пакетов и их предварительную фильтрацию за счет помещения драйвера NDIS на уровне ядра.