БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ В КОРПОРАТИВНЫХ СЕТЯХ

Д.А. Климов

Особенности практических задач обеспечения безопасности конкретных операционных систем связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Уязвимыми являются буквально все основные структурно-функциональные элементы современных ОС. Защищать компоненты ОС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Угрозы безопасности операционной системы существенно зависят от условий ее эксплуатации, от того, какая информация в ней хранится и обрабатывается, и т.д.

Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации:

– по цели атаки;

– по принципу воздействия на операционную систему;

– по типу используемой злоумышленником уязвимости защиты;

– по характеру воздействия на операционную систему.

Вышеперечисленные типы угроз и проникновений могут вызывать множество видов проблем различных уровней – от относительно безобидных до представляющих крайне серьезную степень опасности. Тем не менее, даже кажущиеся несерьезными нарушения могут в итоге приводить к существенному нарушению работы корпоративных сетей. Именно поэтому в современном мире необходимо осуществлять постоянный пересмотр и обновление подходов к защите операционных систем [1].

Политика безопасности должна учитывать два главных фактора:

– максимальную защиту операционных систем от внешних и внутренних, санкционированных и несанкционированных вторжений;

– доступность и отзывчивость для администраторов и пользователей самой корпоративной сети [2].

Литература

1. Шаньгин В.Ф. Комплексная защита информации КС. Эффективные методы и средства. – М: ДМК-Пресс, 2010. – 545 с.

2. Проскурин В.Г. Защита в операционных системах. – М.: Горячая линия – Телеком, 2014. – 192 с.