БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ В КОРПОРАТИВНЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Климов Д.А.

Ширинский В.П. – к.т.н.,доцент

Изложена классификация угроз корпоративным сетям по различным аспектам, подходы к защите информационных систем, политики безопасности предприятия.

Трудности решения 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.

Существует два основных подхода к созданию защищенных операционных систем – фрагментарный и комплексный. При фрагментарном подходе вначале организуется защита от одной угрозы, затем от другой и т. д. Примером, фрагментарного подхода может служить ситуация, когда за основу берется незащищенная операционная система, на нее устанавливают антивирусный пакет, систему шифрования, систему регистрации действий пользователей и т. д.

При применении фрагментарного подхода подсистема защиты ОС представляет собой набор разрозненных программных продуктов, как правило, от разных производителей. Эти программные средства работают независимо друг, от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

Программно-аппаратные средства защиты операционной системы обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже надежная программно-аппаратная защита может давать сбои [1].

Политика безопасности подразумевает наличие множества условий, при которых пользователи системы могут получить доступ к информации и ресурсам. С одной стороны, политика безопасности предписывает пользователям, как правильно эксплуатировать систему, с другой – она определяет множество механизмов безопасности, которые должны существовать в конкретной реализации ОС. Политика безопасности ОС может быть выражена формальным и неформальным образом. Выбор и поддержание адекватной политики безопасности являются одной из наиболее важных задач администратора операционной системы.

Таким образом, политика безопасности должна учитывать два главных фактора:

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

- в то же время доступность и отзывчивость для администраторов и пользователей самой корпоративной сети [2].

Список использованных источников:

1. *Шаньгин В.Ф. Комплексная защита информации КС. Эффективные методы и средства [Электронный ресурс] : [учебное пособие] / В.Ф. Шаньгин – М : ДМК-Пресс, 2010. – 545с.*
2. *Проскурин В.Г., Защита в операционных системах: Учебное пособие для вузов / Проскурин В.Г. – М. : Горячая линия – Телеком,2014. – 192с.*