раздела жесткого диска; обеспечение регулярного обновления; сканирование уязвимости; проверка стороннего кода; контроль физического доступа к оборудованию);

– уровень сетевого взаимодействия (защита сетевой среды платформы виртуализации; изоляция виртуальных машин, относящихся к разным зонам доверия; сетевая защита периметра платформы виртуализации.);

– уровень виртуальной машины и приложений (антивирусная защита; разделение виртуальных машин по зонам доверия; своевременное выполнение обновлений ПО; обновление средств защиты);

– уровень консоли/сервера управления (управление изменениями конфигурации; ограничение доступа по сети; обеспечение регулярного обновления; сканирование уязвимости; организация логирования и мониторинга);

– административные привилегии;

– аудит и отчетность.

К управлению защитой платформы виртуализации нужно подходить комплексно — неполная защита на одном из уровней может сделать бессмысленным использование всех остальных средств.

ВЛИЯНИЕ СПИСКОВ УПРАВЛЕНИЯ ДОСТУПОМ НА СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

О.Р. ХОДАСЕВИЧ

Локальные компьютерные и телекоммуникационные сети предприятий и организаций все больше интегрируются с глобальными общедоступными сетями. Это повышает важность вопроса безопасности передачи данных и доступа к информации. Администраторам сетей приходится балансировать между производительностью и безопасностью сети, поскольку применение различных политик безопасности отнимает ресурсы сетевого оборудования, снижая скорость обмена данными.

Важной задачей обеспечения безопасности является контроль за трафиком, который входит/покидает сеть. Чаще всего он осуществляется путем анализа адресов отправителя и получателя, используемых протоколов и приложений. Широко используемым инструментом, реализующим эти функции, являются списки управления доступом — ACL (access control list). ACL анализирует пакеты данных по ряду параметров. Чем больше параметров анализируется, тем лучше осуществляется контроль, но тем больше времени требуется на обработку пакета сетевым устройством, что приводит к задержкам трафика.

Чаще всего списки управления доступом применяются на пограничных маршрутизаторах. Поэтому для исследования была выбрана схема из четырех маршрутизаторов. Два из них являются пограничными с ЛВС, а два других — транзитными. Для имитации трафика использовались файлы различного размера: от 100 кбайт до 10 Мбайт. В качестве списков управления доступом использовались стандартные и расширенные ACL с количеством условий до 30 строк.

Исследования показали, что ACL практически не оказывают воздействия на скорость передачи трафика при подключении маршрутизаторов по линиям связи со скоростью до 10 Мбит/с. Однако, применение сложных ACL может снижать работоспособность маршрутизаторов, и на линиях связи 100 Мбит/с снижение скорости передачи трафика может достигать 25%.