Системы межсетевого экранирования и обнаружения вторжений, используемые для защиты государственной тайны

УДК 004.056.53

О.А. БЕЗРОДНЫХ, старший инженер Главного центра информационных технологий войск национальной гвардии Российской Федерации

Системы межсетевого экранирования и обнаружения вторжений, используемые для защиты государственной тайны

Firewall and Intrusion Detection Systems Used to Protect State Secrets

В данной статье рассмотрены вопросы использования систем межсетевого экранирования и обнаружения (предотвращения) вторжений для защиты информационных систем, обрабатывающих сведения, составляющие государственную тайну. Для анализа использованы данные по производимым межсетевым экранам и средствам обнаружения (предотвращения) вторжений, прошедшим сертификацию у регуляторов на возможность применения в информационных системах, обрабатывающих сведения, составляющие государственную тайну.

This article discusses the issues of using for the protection of information systems that process information constituting a state secret of systems of firewalling and detection (prevention) of intrusions. For the analysis, we used data on manufactured firewalls and intrusion detection (prevention) tools that have been certified by regulators for the possibility of using them in information systems that process information constituting a state secret.

Ключевые слова: информационная безопасность, межсетевой экран, система обнаружения вторжений, защита информации, составляющей государственную тайну.

Keywords: *information security, firewall, intrusion detection system, protection of information constituting a state secret.*

Введение

Межсетевой экран (МЭ) — это комплекс программно-аппаратных и программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной его задачей является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.

Системы обнаружения вторжений (СОВ) также делятся на две категории. СОВ уровня сети — это программно-техническое средство, реализующее функции автоматического обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней. СОВ уровня узла являются программными средствами, выполняющими те же функции.

Для использования в информационных системах, обрабатывающих сведения, составляющие государственную тайну (ИС ССГТ), МЭ и СОВ должны соответствовать определенным требованиям [1].

Требования к МЭ и СОВ для ИС ССГТ

Основной критерий, определяющий возможность использования программных и программно-технических средств в ИС ССГТ, — наличие разрешения регуляторов, таких как ФСТЭК России, ФСБ России и Минобороны Российской Федерации, в виде выданного ими сертификата. Причем ФСБ России и Минобороны Российской Федерации производят сертификацию МЭ и СОВ для использования внутри своих ведомств. Для других государственных и негосударственных структур сертификацию проводит ФСТЭК России. Таким образом, для использования в ИС ССГТ МЭ и СОВ должны иметь сертификаты ФСТЭК [2] на соответствие требованиям:

к межсетевым экранам по 3-му классу защиты — “Профиль защиты межсетевого экрана типа “А” третьего класса защиты (ИТ.МЭ.А3.П3)” для МЭ уровня сети при обработке в ИС ССГТ сведений уровня “секретно”;

к межсетевым экранам по 2-му классу защиты — “Профиль защиты межсетевого экрана типа “А” второго класса защиты (ИТ.МЭ.А2.П3)” для МЭ уровня сети при обработке в ИС ССГТ сведений уровня “совершенно секретно”;

к межсетевым экранам по 3-му классу защиты — “Профиль защиты межсетевого экрана типа “В” третьего класса защиты (ИТ.МЭ.В3.П3)” для МЭ уровня узла при обработке в ИС ССГТ сведений уровня “секретно”;

к межсетевым экранам по 2-му классу защиты — “Профиль защиты межсетевого экрана типа “В” второго класса защиты (ИТ.МЭ.В2.П3)” для МЭ уровня узла при обработке в ИС ССГТ сведений уровня “совершенно секретно”;

Полную версию статьи читайте в бумажной версии журнала