Сатанин Д.Н., ФСБ России
(войсковая часть 43753)

О СЕРТИФИЦИРОВАННЫХ ФСБ РОССИИ КОММЕРЧЕСКИХ СРЕДСТВАХ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Требования ФСБ России к средствам обнаружения компьютерных атак (СОА)

- Действуют с 2002 года, новая редакция – от 2012 года.
- Имеют ограничительную пометку «для служебного пользования».
- Выделено 4 класса устройств (от Г до А). Подход к классификации: функциональные возможности – СОА более высокого класса обладает всеми функциональными возможностями СОА предыдущего класса.

Требования ФСБ России к СОА (продолжение)

- **Выделено 4 класса устройств (от Г до А).**
- **Основным условием успешной сертификации является выполнение испытуемым устройством требований к СОА ФСБ России по количественным характеристикам обнаружения компьютерных атак.**
- **Подход к классификации: функциональные возможности – СОА более высокого класса обладает всеми функциональными возможностями СОА предыдущего класса.**
- **На данный момент:**
  - С 2002 года проведено порядка 7 сертификаций;
  - сертификат выдан 5 СОА (перечень прилагается).

СОА «Аргус»

- Разработчик, собственник и производитель – ООО «Центр Специальной Системотехники» (г. Москва).
- Действующие сертификаты имеют версии 1.0 и 1.5 (по классам Г и В соответственно).
- Предназначено для обнаружения компьютерных атак в сетевом трафике стека протоколов TCP/IP в каналах со скоростью передачи данных до 1 Гбит/с включительно с использованием сигнатурного метода.
- Функционирует под управлением модифицированной операционной системы OpenBSD версии 4.7.
- Управление осуществляется локально при помощи Web-интерфейса.

СОА «Форпост»

- Разработчик, собственник и производитель – ЗАО «РНТ» (г. Москва).
- Действующий сертификат имеет версия 2.0 (по классу Б с ограничениями).
- Предназначено для обнаружения компьютерных атак в сетевом трафике стека протоколов TCP/IP в каналах со скоростью передачи данных до 1 Гбит/с включительно с использованием сигнатурного метода и контроля СВТ, на которых установлены компоненты СОА «Форпост».
- Функционирует под управлением операционных систем Microsoft Windows 2000/XP и Server 2003/2008.
- Управление осуществляется удалённо при помощи Web-интерфейса с использованием СКЗИ «КриптоПро CSP» версии 3.6.

СОА «Тор»

- Разработчик, собственник и производитель – ФГУП «НТЦ «Атлас» (г. Москва).
- Действующий сертификат –по классу Б с ограничениями.
- Предназначено для обнаружения компьютерных атак в сетевом трафике стека протоколов TCP/IP в каналах со скоростью передачи данных до 100 Мбит/с включительно с использованием сигнатурного метода.
- Функционирует под управлением операционной системы Атликс-2И (ядро Linux версии 2.6.32, на базе CentOS Linux).
- Управление осуществляется удалённо при помощи Web-интерфейса с использованием СКЗИ AtlixGCL из состава ОС Атликс-2И.

Программно-аппаратный комплекс «Ручей-М»

- Разработчик, собственник и производитель – ООО «Удостоверяющий центр ИнформПро» (г. Санкт-Петербург).
- Действующий сертификат имеет версия 1.02 по классу Г.
- Предназначено для обнаружения компьютерных вирусов в сетевом трафике стека протоколов TCP/IP со скоростью передачи данных до 10 Мбит/с (в типовой комплектации) включительно с использованием сигнатурного метода.
- Функционирует под управлением операционной системы Slackware версии 12.0.
- Управление осуществляется локально в режиме командной строки.

СПАСИБО ЗА ВНИМАНИЕ!