### Комплекс «Рубикон»

Разработанный компанией «Эшелон» программно-аппаратный комплекс «Рубикон» успешно прошел сертификацию во ФСТЭК России. Комплекс сочетает в себе межсетевой экран и систему обнаружения вторжений. «Рубикон» может использоваться в информационных системах персональных данных (ИСПДн) 1-го класса, а также в информационных системах, в которых обрабатывается информация вплоть до грифа «Совершенно секретно».

Комплекс «Рубикон» может использоваться в качестве одностороннего шлюза для организации односторонней передачи информации в сегменты локальных вычислительных сетей, в которых обрабатывается информация, составляющая государственную тайну.

Выданный ФСТЭК России сертификат соответствия №2574 подтверждает, что комплекс «Рубикон» соответствует 2 уровню контроля отсутствия недекларированных возможностей и 2 классу защищенности РД Гостехкомиссии, а также техническим условиям. Напомним, что «Рубикон» ранее уже успешно прошел сертификацию в Минобороны России по самым жестким требованиям к средствам защиты государственной тайны.

«Рубикон» является первой системой обнаружения вторжений (СОВ), прошедшей сертификацию во ФСТЭК России. Функционал СОВ, реализованный в продукте, позволяет оперативно обнаруживать различные атаки:

* на web-службы;
* по служебным протоколам (в том числе SMTP, POP, SNMP, TELNET, FTP);
* на известные базы данных;
* класса «отказ в обслуживании (DOS и DDOS);
* и другие.

Система позволяет выявлять компьютерные атаки на основе анализа сетевого трафика вплоть до прикладного уровня и сигнализировать о произошедшей атаке администратору.

#### Преимущества

«РУБИКОН» является программно-аппаратным комплексом, что упрощает его внедрение, эксплуатацию и сопровождение.

* производительность МЭ: до 9Gb/s;
* производительность СОВ: до 3Gb/s;
* производительность маршрутизации: до 9 Gb/s;
* возможность горячего резервирования: на уровне устройств (VRRP, Enthernet Bypass), на уровне портов (VLAN bonding), на уровне каналов связи (динамическая маршрутизация OSPF);
* поддержка мандатных меток отечественных защищенных операционных систем в сетевом трафике;
* возможность интеграции с системой мониторинга событий информационной безопасности «KOMRAD Enterprise SIEM»;
* модульная структура аппаратных платформ;
* возможность конфигурации до 64 портов в одном комплексе.

#### Технические характеристики

* имеет в своем составе сертифицированную систему обнаружения вторжений (СОВ);
* администрирование межсетевого экрана выполняется по защищенному протоколу HTTPS, устойчивому к перехвату информации;
* обнаружение атак: web-службы, по служебным протоколам (в том числе SMTP, POP, SNMP, TELNET, FTP), на известные базы данных, DOS и DDOS атак, другие специфические атаки;
* обеспечивает фильтрацию сетевых пакетов и осуществляет разграничение доступа пользователей к ресурсам сети на основе заданных правил. Поддержка фильтрации пакетов с мандатными метками Astra Linux и МСВС;
* производит трансляцию сетевых адресов. Это дает возможность скрыть структуру внутренней сети от внешних субъектов и расширяет возможности использования произвольных диапазонов внутренних IP-адресов;
* обеспечивает построение однонаправленного шлюза для связи сегментов с различными уровнями секретности;
* высокая скорость работы;
* количество сетевых портов - до 64 свободно конфигурируемых интерфейсов (Ethernet 100/1000 Base-T и оптических на основе SFP модулей);
* возможность горячего резервирования;
* поддержка оптических интерфейсов;
* обновление базы правил СОВ;
* возможна поставка в пяти вариантах исполнения.