



ПРОДУКТЫ КОМПАНИИ ЭЛВИС-ПЛЮС

Семейство продуктов информационной безопасности ЗАСТАВА 5.3

Продукты ЗАСТАВА 5.3 обеспечивают защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей (Virtual Private Networks - VPN) и распределенного межсетевое экранирования (МЭ). Они работают на различных аппаратных платформах, под управлением практически всех популярных операционных систем.

Семейство продуктов ЗАСТАВА 5.3 обеспечивает:

- Защиту отдельных компьютеров, в том числе мобильных, от атак из сетей общего пользования и Интернет;
- Защиту корпоративной информационной системы или ее частей от внешних атак;
- Организацию доверенных, защищенных каналов связи между сегментами территориально распределенной информационной системы, а также с мобильными пользователями;
- Ограничение доступа с рабочих станций к внешним информационным ресурсам и интернет-сайтам;
- Соответствие информационной системы Российскому законодательству и нормативным требованиям в сфере информационной безопасности и защиты персональных данных;
- Централизованное, удобное управление сетевой безопасностью в информационных системах масштабом более 5000 защищенных узлов;
- Высокую производительность и прозрачность для пользователей и приложений.

Для выполнения криптографических функций ЗАСТАВА использует внешние, сертифицированные криптомодули ведущих российских производителей, реализующие стандарты ГОСТ Р 34.11-94, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ 28147-89. Обычно это продукт КриптоПро CSP компании Крипто-Про, однако, по выбору пользователя, это могут быть Крипто-КОМ (Сигнал-КОМ), Вербa (МО ПНИЭИ). Также ЗАСТАВА может использовать криптоалгоритмы RSA, DES, 3DES, SHA1, MD5 и другие.

Продукты ЗАСТАВА 5.3 сертифицированы ФСТЭК по 2-му классу защищенности межсетевых экранов и 2-му уровню контроля отсутствия недеklarированных возможностей, а также по 3-му классу защищенности межсетевых экранов и 3-му уровню контроля отсутствия недеklarированных возможностей согласно РД Гостехкомиссии. Продукты могут быть использованы (и рекомендованы некоторыми ведомствами) для защиты персональных данных до 1 категории включительно.

Семейство ЗАСТАВА 5.3 включает программные агенты ЗАСТАВА-Клиент и Застава-Офис, которые устанавливаются, соответственно, на персональные компьютеры и шлюзы защищаемой информационной системы. Третий продукт семейства, ЗАСТАВА-Управление, в удаленном режиме обеспечивает централизованное администрирование и оперативное управление агентами, их политиками безопасности.

ЗАСТАВА-Агенты

Программные агенты ЗАСТАВА-Офис 5.3, ЗАСТАВА-Клиент 5.3 предназначены для использования в качестве межсетевых экранов с функциями расширенной пакетной фильтрации и организации

защищенных VPN-соединений в сетях связи общего пользования. На их основе строятся территориально распределенные, защищенные информационные системы, обеспечивающие конфиденциальность, целостность и аутентичность сетевого трафика на базе стандартных протоколов IPSec. Строгая аутентификация пользователей, а также взаимная аутентификация агентов, производится с использованием сертификатов цифрового ключа.

Межсетевой экран и VPN-агент ЗАСТАВА-Офис реализует функции прикладного проксирования популярных сетевых сервисов и протоколов (Telnet, FTP, SMTP, HTTP, SOCKS), а также маскирование топологии защищаемой сети в режиме VPN-туннелирования, либо с использованием встроенного централизованно управляемого NAT-сервера.

Персональный межсетевой экран и VPN-агент ЗАСТАВА-Клиент обеспечивает полный набор функций сетевой защиты для отдельных рабочих станций и мобильных пользователей – например, при работе из Интернет, включая режим выделения мобильному пользователю внутреннего локального адреса для удаленного VPN-доступа в защищенную корпоративную сеть.

ЗАСТАВА-Управление

ЗАСТАВА-Управление обеспечивает централизованное, гибкое и динамическое управление всей совокупностью агентов. Это позволяет существенно сократить расходы на содержание организационной системы информационной безопасности.

ЗАСТАВА-Управление работает не только с агентами ЗАСТАВА-Офис и ЗАСТАВА-Клиент, но и обеспечивает управление конфигурациями VPN и МЭ продуктов сетевой защиты лидеров зарубежного рынка информационной безопасности: Cisco IOS Router, МЭ Cisco PIX Firewall, шлюзов Check Point VPN-1/FireWall-1 Gateway, а также встроенных в ОС Microsoft 2000/XP/2003 агентов IPSec Agent.

Комплексы высокой готовности на основе продуктов ЗАСТАВА

Комплексы высокой готовности могут иметь в своей основе любой из описанных продуктов семейства ЗАСТАВА, но уже установленный на аппаратную платформу и в максимальной степени сконфигурированный силами производителя.

Программно-аппаратные комплексы ЗАСТАВА

Программно-Аппаратный Комплекс ЗАСТАВА (ПАК ЗАСТАВА) предназначен для тех же целей, что и продукт ЗАСТАВА-Офис, а именно для использования в качестве межсетевого экрана и VPN устройства, обеспечивающего защиту трафика по протоколам IKE/IPsec. ПАК ЗАСТАВА поставляется на нескольких, заранее выбранных аппаратных платформах. Для организации защищенных каналов до 20 Мбит/с предназначены ПАК на базе компактных с процессорами семейства Intel Atom. Более мощные компьютеры, на базе современных процессоров Intel, позволяют организовать VPN-каналы свыше 1 Гбит/с.

ПАК автоматически восстанавливает работоспособность после перезагрузки, вызванной внезапным отключением питания. При этом восстанавливается последняя загруженная конфигурация.

Кластеры ЗАСТАВА

Кластерная реализация ПАК обеспечивает высокую доступность (High Availability, HA) защищаемых информационных систем. Комплексы высокой доступности предназначены для применения в крупных информационных системах кредитно-финансового сектора, энергетики, газо- и нефтедобывающей промышленности, телекоммуникационной отрасли. Наличие сертификатов ФСТЭК на основное программное обеспечение и криптоалгоритмы позволяет применять кластеры Застава для защиты конфиденциальной информации на предприятиях оборонного комплекса, в региональных и федеральных органах власти, в государственных учреждениях и организациях.

Комплекс высокой доступности обеспечивает автоматическое восстановление работоспособности агентов Застава в случае аппаратного отказа оборудования одного из узлов кластера, отказа каналов связи с одним из узлов, отказа программного обеспечения Застава на одном из узлов.

Использование комплексов высокой доступности Застава позволяет обеспечить стабильный удаленный доступ к корпоративной информационной системе и организовать надежное разделение ее на зоны, в которых обрабатывается информация разной степени секретности.