

«В 1994 году мы создали одну из первых реализаций протокола SKIP для VPN-устройств, который лёг в основу широко используемого в настоящее время международного протокола IPsec. С этого и началась разработка первого отечественного межсетевое экрана, названного ЗАСТАВА.

Мы инициировали и приняли участие в разработке руководящих документов Гостехкомиссии (нынешняя ФСТЭК России) для межсетевых экранов. Первая ЗАСТАВА работала на SKIP-протоколе, поскольку была изначально ориентирована на международный рынок. А позже, когда продукт был уже представлен на международном рынке, мы сделали VPN/FW-продукт на IPsec, кстати, тоже первыми в России»

Александр Галицкий,
Президент АО «ЭЛВИС-ПЛЮС»



Семейство продуктов информационной безопасности ЗАСТАВА успешно применяется для защиты информации с 1997 года. За это время сменилось несколько версий продукта, расширилась его функциональность, возросли надёжность и производительность.

Сегодня ЗАСТАВА — это комплекс программных и программно-аппаратных продуктов, обеспечивающих защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей (Virtual Private Networks, VPN) и распределённого межсетевого экранирования (МЭ, FW).

ОБЛАСТИ ПРИМЕНЕНИЯ

Создание защищённых корпоративных и ведомственных сетей любых масштабов, уровней территориальной распределённости и связанности, вплоть до федерального уровня (объединение всех территориально распределённых подразделений компании/ведомства в единую виртуальную сеть). ЗАСТАВА поддерживает все технологии создания защищённых сетей, включая Site-to-Site VPN и Remote Access VPN, что позволяет реализовывать различные конфигурации и топологии защищённых сетей с использованием сертифицированных российских криптографических алгоритмов ГОСТ 34.12-2018, ГОСТ Р 34.12-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.

Обеспечение безопасного доступа в Интернет. Продукты ЗАСТАВА включают встроенные функции межсетевого экранирования и трансляции сетевых адресов (Network Address Translation, NAT), а также контекстный анализ протоколов прикладного уровня, что позволяет использовать их для защиты корпоративной сети при подключении к сети общего пользования.

Защищённый доступ удалённых и мобильных пользователей к корпоративной сети (предоставление защищённого доступа клиентов к сервисам компании). Для защиты соединения используются стандартные протоколы IPsec и IKE с шифрованием трафика с помощью сертифицированных российских криптографических алгоритмов ГОСТ 34.12-2018, ГОСТ Р 34.12-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.

Защита каналов связи между центрами обработки данных. Применение функций распределения нагрузки даёт возможность защищать широкополосные каналы связи (до 10 Гб/с), в том числе связывающие основной и резервный центры обработки данных федеральных и региональных органов власти, операторов, предоставляющих услуги ЦОД.

Внутреннее сегментирование корпоративной информационной системы для обработки информации

разной степени конфиденциальности. МЭ ЗАСТАВА работает на основе механизмов фильтрации пакетов с контролем соединения, что даёт необходимую гибкость в настройках политики безопасности.

Межведомственное взаимодействие (подключение сетей организаций-партнеров). Продукты ЗАСТАВА могут использоваться для подключения отдельных компьютеров или сетей других организаций к корпоративной сети. Таким образом может быть построено межсетевое взаимодействие между разными ведомствами и государственными организациями.

Обеспечение выполнения требований регуляторов в составе систем защиты персональных данных и конфиденциальной информации, в том числе в государственных информационных системах (ГИС) с учётом требований по криптографической защите информации при передаче по открытым каналам связи.

КРУПНЫЕ ПРОЕКТЫ НА ОСНОВЕ ПО ЗАСТАВА

Проекты федерального уровня

- Росреестр (Федеральная система)
- Минобороны России
- ФНС России (Федеральная система ЗАГС)
- ФСТЭК России
- Российский Союз Автостраховщиков
- ФСК ЕЭС

Проекты регионального уровня

- Сеть органов исполнительной власти г. Санкт-Петербург
- Сеть органов исполнительной власти Республики Татарстан
- Сеть органов исполнительной власти г. Москва
- МИС Тамбовской области
- МИС Республики Татарстан
- МИС Республики Калмыкия



КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

Высокий уровень масштабирования системы. Нет ограничений по масштабу, количеству и форме подчинения узлов корпоративной сети.

Централизованное иерархическое управление в режиме реального времени всей защищённой сетью из одной географической точки. Программный продукт ЗАСТАВА-Управление имеет самый удобный, функциональный и простой интерфейс администрирования среди всех сертифицированных российских продуктов криптографической защиты сетевого трафика. Графический интерфейс продукта позволяет управлять всеми наборами правил (глобальной политикой безопасности) на основе бизнес-объектов и ролей.

Низкая стоимость приобретения, внедрения и владения. Благодаря применению ЗАСТАВА-Управление снижаются расходы на эксплуатацию системы: удалённое администрирование отменяет необходимость содержания в штате территориально распределённой организации системных администраторов в региональных подразделениях.

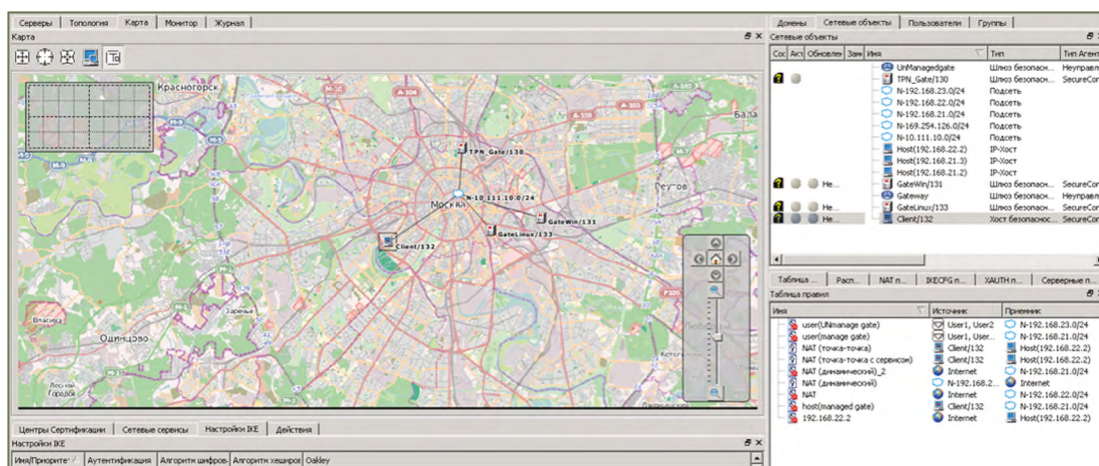
Разделение полномочий по управлению системой. ЗАСТАВА-Управление имеет функцию доменного управления. Для каждого домена можно задать собственные параметры и политики безопасности, а также передать полномочия по управлению в региональные подразделения компании или межрегиональные центры компетенции.

Высокая надёжность системы. ПАК ЗАСТАВА могут объединяться в кластеры, которые работают как единый логический шлюз. При возникновении сбоя происходит автоматическое переключение на резервный узел кластера. Процесс смены активного узла полностью прозрачен для пользователей и приложений корпоративной сети.

Высокая производительность. ЗАСТАВА функционирует на различных аппаратных платформах и поддерживает несколько типов операционных систем, что позволяет выбрать оптимальное техническое решение с учётом требований к производительности и стоимости.

Использование международных стандартов и протоколов сетевой защиты. Решение ЗАСТАВА использует международные протоколы и стандарты IPsec и IKE, что позволяет реализовать интеграцию с другими продуктами как в части создания защищённых туннелей, так и в управлении устройствами. ЗАСТАВА на сегодняшний день является единственным российским решением, в котором реализован протокол IKEv2.

Поддержка механизмов качества обслуживания (QoS). Продукты ЗАСТАВА обеспечивают возможность обработки параметров качества обслуживания на основе значений кодов DSCP, содержащихся в заголовке IP-пакета. Это позволяет эффективно использовать продукты ЗАСТАВА для защиты приложений, чувствительных к пропускной способности канала связи, задержкам, джиттеру (например, IP-телефонии и видеоконференций).



Уникальный режим представления топологии сети — наложение на географическую карту.

Этот режим будет особенно удобен администраторам системы в территориально распределённых организациях.

СИСТЕМА ОБНАРУЖЕНИЯ АТАК ЗАСТАВА-IDS

ЗАСТАВА-IDS — это комплекс программного обеспечения, предназначенный для обнаружения компьютерных атак на систему или сеть на основе анализа сетевого трафика стека протоколов TCP/IP со скоростью передачи данных не менее 1 Гбит/с сигнатурным методом.

ЗАСТАВА-IDS надёжно защищает сеть, устойчива к различным техникам обхода сетевой защиты и имеет широкие возможности настройки.

АПК «ЗАСТАВА-ТК»

ЗАСТАВА-ТК — это первый аппаратный тонкий клиент российского производства, реализующий концепцию универсального рабочего места для использования в государственных и корпоративных территориально распределённых информационных системах и компьютерных сетях, в которых требуется обеспечить централизованную обработку, хранение и доступ к данным с использованием облачных технологий и VDI с высокой степенью защищённости, до класса К1 ИСПДн и ГИС включительно, а также в медицинских ИС.

Первый на рынке программно-аппаратный тонкий клиент, сертифицированный по классу КСЗ без применения налоговых аппаратных средств.

Сертификаты: ФСБ России — КС1, КС2, КС3
ФСТЭК России — МЭ класс 4 тип А, В