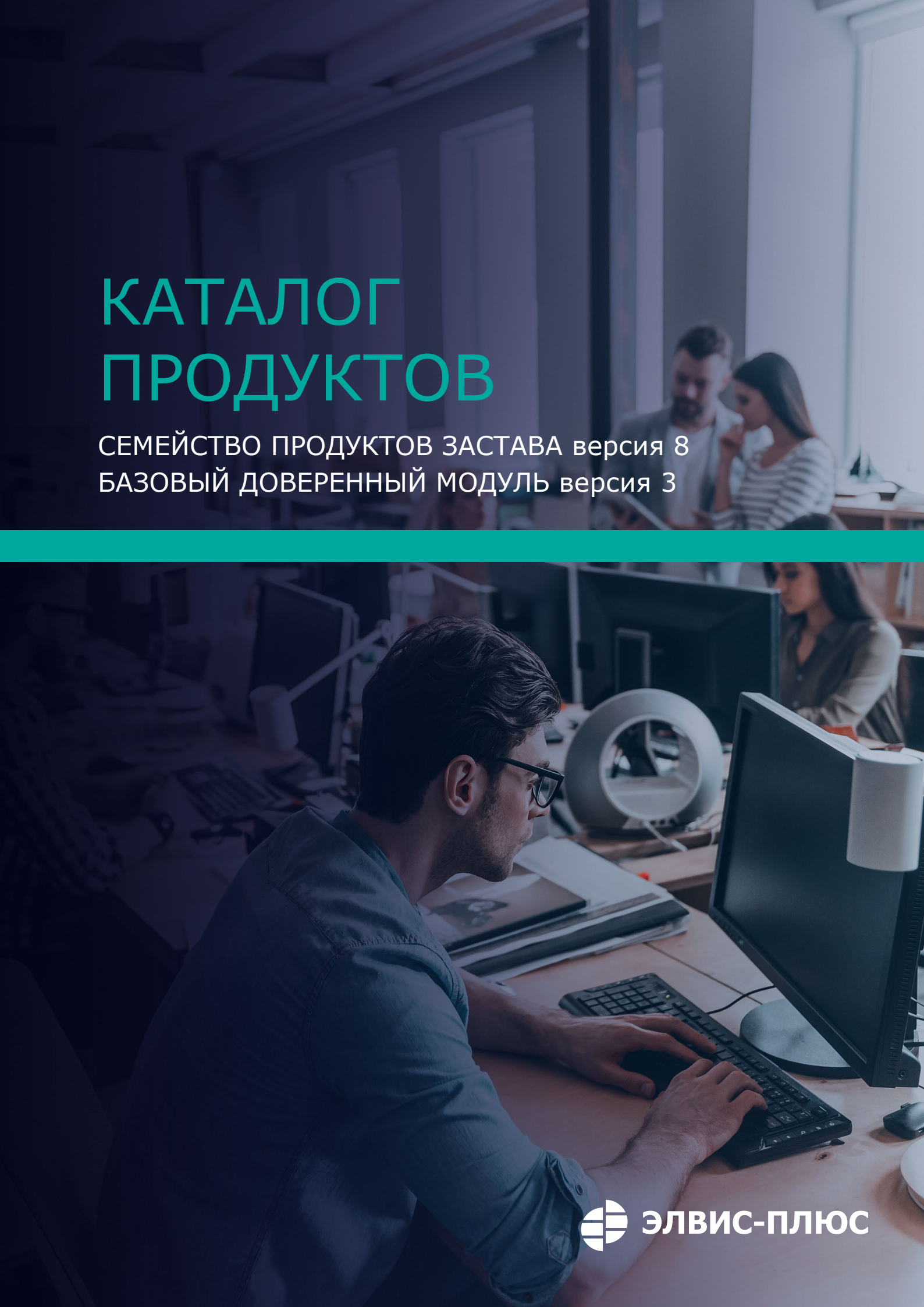


КАТАЛОГ ПРОДУКТОВ

СЕМЕЙСТВО ПРОДУКТОВ ЗАСТАВА версия 8
БАЗОВЫЙ ДОВЕРЕННЫЙ МОДУЛЬ версия 3

ЭЛВИС-ПЛЮС

О компании

Компания ЭЛВИС-ПЛЮС была основана в 1991 году с целью разработки новых компьютерных и информационных технологий, реализации проектов в области вычислительных сетей и телекоммуникаций.

Богатый опыт по созданию высокотехнологичных систем для оборонной промышленности, накопленный основателями и сотрудниками компании, позволил ЭЛВИС-ПЛЮС быстро достичь значимого уровня в создании новых технологий и впоследствии занять ведущие позиции на российском рынке системной интеграции в сфере информационной безопасности.

На сегодняшний день ЭЛВИС-ПЛЮС реализует проекты по построению защищённых информационных сетей и предлагает комплексные решения по защите информации, обеспечивающие совместимость различных систем и технологий. Такой подход позволяет выработать единую концепцию развития информационных сетей наших заказчиков, определить оптимальный порядок и этапы внедрения решений, интегрировать их в существующую инфраструктуру. Всё это способствует оптимизации затрат на реализацию проектов по защите информации.

Наша компания продолжает разрабатывать и успешно внедрять продукты на основе общепризнанных технологий информационной безопасности и национальных стандартов — семейства протоколов сетевой безопасности IPsec, стандартов Trusted Computing Group (TCG) и криптографических алгоритмов ГОСТ, реализуя их в собственных продуктах сетевой безопасности ЗАСТАВА, а также в линейке средств доверенной загрузки «Мобильное защищённое автоматизированное рабочее место «Базовый Доверенный Модуль» (МЗ АРМ «БДМ»).

За более чем 30 лет существования ЭЛВИС-ПЛЮС нашими клиентами стали крупнейшие российские компании, государственные структуры и предприятия: Банк России, ФСТЭК России, ФНС России, СО ЕЭС, Россети ФСК ЕЭС, Росреестр, Лукойл, Газпром нефть, Транснефть, Сургутнефтегаз, Татнефть, Ростелеком, Газпромбанк, СОГАЗ, Российский Союз Автостраховщиков и многие другие.

ЗАСТАВА

ЗАСТАВА — линейка программных продуктов и аппаратно-программных комплексов (АПК), обеспечивающих защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей (Virtual Private Networks, VPN) и распределённого межсетевого экранирования (МЭ, FW).

Семейство продуктов информационной безопасности ЗАСТАВА успешно применяется для защиты информации с 1997 года. За это время сменилось несколько версий, расширились функциональные возможности, возросли надёжность и производительность.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА ПРОДУКТОВ СЕМЕЙСТВА ЗАСТАВА

- Полное соответствие новейшим стандартам и рекомендациям по стандартизации ТК26
- Высокопроизводительный драйвер для шифрования трафика
- Использование криптопровайдера «ЭЛВИС-Крипто» собственной разработки
- Совместимость с продуктами ЗАСТАВА версии 6
- Высокий уровень защиты, обеспечиваемый продуктами ЗАСТАВА
- Возможность гибкого масштабирования системы
- Централизованное управление в режиме реального времени
- Быстрота развёртывания распределённой системы защиты без участия квалифицированного персонала на местах
- Возможность оперативного управления из ЦУП «ЗАСТАВА-Управление» десятками тысяч FW/VPN-шлюзов и агентов ЗАСТАВА одновременно
- Удалённое централизованное обновление программного обеспечения
- Разделение полномочий по управлению системой
- Высокая производительность и надёжность системы
- Использование наряду с российскими криптоалгоритмами международных стандартов и протоколов сетевой защиты
- Поддержка механизмов приоритизации информационных потоков
- Гибкость поставки системы
- Сертификаты ФСБ России, ФСТЭК России
- Низкие эксплуатационные затраты

БАЗОВЫЙ ДОВЕРЕННЫЙ МОДУЛЬ (БДМ)

Продуктовая линейка на основе технологии **БДМ** предназначена для построения доверенной вычислительной среды на мобильных компьютерах, ноутбуках и планшетах, базирующихся на архитектуре Intel x64.

ПРЕИМУЩЕСТВА ТЕХНОЛОГИИ БДМ

- Сертифицированное решение для ультрабуков, планшетов и смартфонов
- Обычный внешний вид мобильного устройства, не требует установки дополнительного оборудования
- Высокая производительность шифрования
- Прозрачная доверенная среда
- Лёгкость интеграции в существующие информационные системы
- Аттестованное рабочее место
- Сертификат ФСБ России

АПК «ЗАСТАВА-150» — программно-аппаратный комплекс межсетевого экранирования и VPN, сертифицированный по классу КС3 (ФСБ России) и МЭ тип «А» класс 4 (ФСТЭК России). АПК «ЗАСТАВА-150» предназначен для защиты локальной вычислительной сети (ЛВС) предприятия на сетевом уровне с использованием криптоалгоритмов ГОСТ и технологий VPN на основе интернет-протоколов семейства IPSec.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Скорость шифрования: до 300 Мб/с
- СКЗИ VPN/FW ЗАСТАВА-Офис с криптоядром «ЭЛВИС-Крипто»
- Кол-во сетевых интерфейсов: 6 x 1 GbE
- Пассивное (безвентиляторное) охлаждение
- Аппаратный контроль вскрытия корпуса с сигнализацией
- Компактный форм-фактор: можно установить два устройства рядом в стойку 1U
- Размеры: 202 x 205 x 42 мм
- Условия эксплуатации: температура окружающей среды от 0°C до 60°C при влажности 20-80%
- Внешний блок питания
- Вес: не более 1,5 кг

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Неограниченное количество защищаемых узлов, подключаемых криптошлюзов и клиентов
- Интегрированный аппаратный ДСЧ
- Возможность использования ключей шифрования и сертификатов до 3-х лет
- Возможность восстановления ПО криптошлюза с заводского образа
- Удалённое обновление ПО АПК
- Удалённое обновление ключей и сертификатов
- Возможность организации отказоустойчивого решения (active/passive)
- Полноценная поддержка VLAN (802.1q)
- Шифрование на уровне L2
- Шифрование на уровне L3
- Поддержка динамических протоколов маршрутизации
- Поддержка PBR (Policy Based Routing)
- Возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel и т.д.)
- Возможность приоритизации трафика (ToS, DiffServ)
- Двухфакторная аутентификация
- Возможность назначения DNS и любых виртуальных IP-адресов для клиентов ЗАСТАВА, подключённых к криптошлюзу, в т. ч. функция DHCP Relay
- Возможность доступа к клиентам ЗАСТАВА по виртуальному IP-адресу (VPN-маршрутизация)
- Возможность автоматической конфигурации маршрутизации при множественных интерфейсах доступа для клиента ЗАСТАВА с помощью технологии Reverse Routing Injection (RRI)
- Возможность работы через NAT (технология NAT-T)
- Поддержка протокола IKEv2, обеспечивающего повышенный уровень безопасности
- Антиспуфинг
- Возможность интеграции с системой мониторинга ZABBIX

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа с мобильных устройств
- Подключение средних и малых офисов (Small Office Home Office)
- Защита каналов передачи данных в ГИС

АПК «ЗАСТАВА-1500» — программно-аппаратный комплекс ЗАСТАВА-1500 предназначен для защиты высоконагруженных каналов, организации удалённого доступа для большого количества сотрудников и защиты каналов между ЦОД на сетевом уровне с использованием криптоалгоритмов ГОСТ и технологий VPN на основе интернет-протоколов семейства IP-Sec.

СОСТАВ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Скорость шифрования: до 1500 Мб/с
- СКЗИ VPN/FW ЗАСТАВА-Офис с криптоядром «ЭЛВИС-Крипто»
- Количество сетевых интерфейсов зависит от комплектации:
  4 x 1 GbE, 2 x 1 Gb SFP
  8 x 1 GbE, 2 x 1 Gb SFP
  12 x 1 GbE, 2 x 1 Gb SFP
  4 x 1 GbE, 10 x 1 Gb SFP
  4 x 1 GbE, 2 x 1 Gb SFP, 4 x 10 Gb SFP+
- Возможность отказоустойчивого решения
- Балансировка нагрузки
- Форм-фактор: 1U

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Неограниченное количество защищаемых узлов, подключаемых криптошлюзов и клиентов
- Возможность реализации отказоустойчивого решения (active/passive)
- Полноценная поддержка VLAN (802.1q)
- Шифрование на уровне L2
- Шифрование на уровне L3
- Поддержка динамических протоколов маршрутизации
- Поддержка PBR (Policy Based Routing)
- Возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel и т.д.)
- Возможность приоритизации сетевого трафика (ToS, DiffServ)
- Двухфакторная аутентификация
- Возможность назначения DNS и любых виртуальных IP-адресов для клиентов ЗАСТАВА, подключённых к криптошлюзу, в т.ч. функция DHCP Relay
- Количество подключений ПО «ЗАСТАВА-Клиент» к шлюзу программно не ограничено
- Возможность доступа к клиентам ЗАСТАВА по виртуальному IP-адресу (VPN-маршрутизация)
- Возможность автоматической конфигурации маршрутизации при множественных интерфейсах доступа для клиента ЗАСТАВА с помощью технологии Reverse Routing Injection (RRI)
- Возможность работы через NAT (технология NAT-T)
- Поддержка протокола IKEv2, обеспечивающего повышенный уровень безопасности
- Антиспуфинг
- Возможность интеграции с системой мониторинга ZABBIX

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа с мобильных устройств
- Защита средненагруженных каналов (ЦОД-Офис, Офис-Офис)
- Защита каналов передачи данных в ГИС

АПК «ЗАСТАВА-6000» — программно-аппаратный комплекс ЗАСТАВА-6000 предназначен для защиты каналов между ЦОД на сетевом уровне с использованием криптоалгоритмов ГОСТ и технологий VPN на основе интернет-протоколов семейства IPSec.

СОСТАВ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Скорость шифрования: до 6000 Мб/с
- СКЗИ VPN/FW ЗАСТАВА-Офис с криптоядром «ЭЛВИС-Крипто»
- Количество сетевых интерфейсов зависит от комплектации:
  4 x 1 GbE, 4 x 1 Gb SFP, 4 x 10 Gb SFP+
  4 x 1 GbE, 8 x 10 Gb SFP+
- Возможность отказоустойчивого решения
- Балансировка нагрузки
- Форм-фактор 2U

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Неограниченное количество защищаемых узлов, подключаемых криптошлюзов и клиентов
- Возможность реализации отказоустойчивого решения (active/passive)
- Полноценная поддержка VLAN (802.1q)
- Шифрование на уровне L2
- Шифрование на уровне L3
- Поддержка динамических протоколов маршрутизации
- Поддержка PBR (Policy Based Routing)
- Возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel и т.д.)
- Возможность приоритизации сетевого трафика (ToS, DiffServ)
- Двухфакторная аутентификация
- Возможность назначения DNS и любых виртуальных IP-адресов для ПО «ЗАСТАВА-Клиент», подключённых к шлюзу, в т.ч. функция DHCP Relay
- Возможность доступа к клиентам ЗАСТАВА по виртуальному IP-адресу (VPN-маршрутизация)
- Возможность автоматической конфигурации маршрутизации при множественных интерфейсах доступа для клиента ЗАСТАВА с помощью технологии Reverse Routing Injection (RRI)
- Возможность работы через NAT (технология NAT-T)
- Поддержка протокола IKEv2, обеспечивающего повышенный уровень безопасности
- Антиспуфинг
- Возможность интеграции с системой мониторинга ZABBIX

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа для большого количества пользователей
- Защита высоконагруженных каналов (ЦОД-ЦОД)
- Защита каналов передачи данных в ГИС

АПК «ЗАСТАВА-10000» — программно-аппаратный комплекс ЗАСТАВА-10000 предназначен для защиты каналов между ЦОД на сетевом уровне с использованием криптоалгоритмов ГОСТ и технологий VPN на основе интернет-протоколов семейства IP-Sec.

СОСТАВ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Скорость шифрования: до 10000 Мб/с
- СКЗИ VPN/FW ЗАСТАВА-Офис с криптоядром «ЭЛВИС-Крипто»
- Количество сетевых интерфейсов зависит от комплектации:
  5 x 1 GbE, 4 x 10 Gb SFP+
  1 x 1 GbE, 8 x 10 Gb SFP+
  1 x 1 GbE, 4 x 10 Gb SFP+, 4 x 10 / 25 GbE SFP28
- Возможность отказоустойчивого решения
- Балансировка нагрузки
- Форм-фактор 1U

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

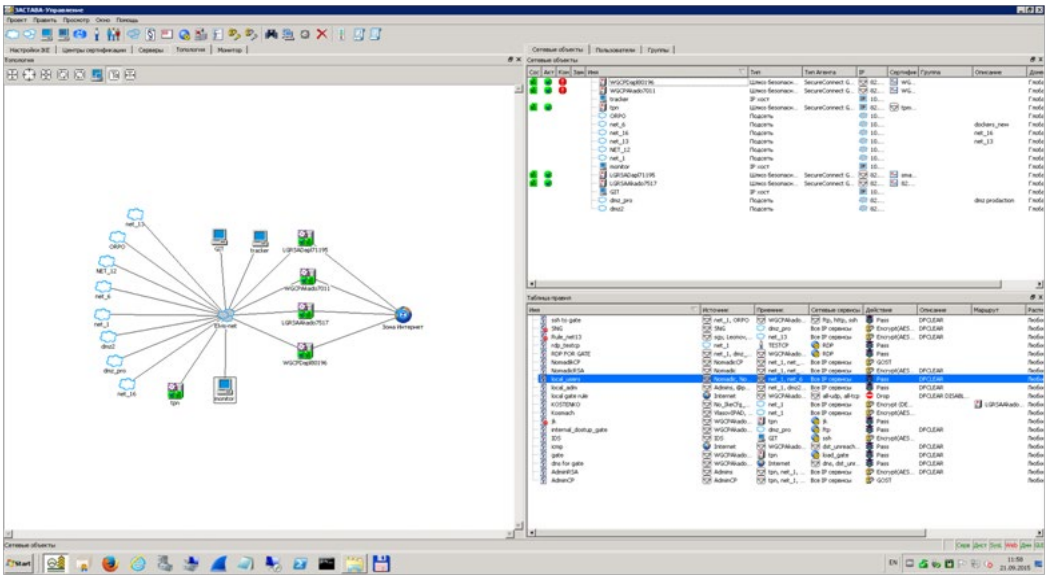
- Неограниченное количество защищаемых узлов, подключаемых криптошлюзов и клиентов
- Возможность реализации отказоустойчивого решения (active/passive)
- Полноценная поддержка VLAN (802.1q)
- Шифрование трафика L2
- Шифрование на уровне L3
- Поддержка динамических протоколов маршрутизации
- Поддержка PBR (Policy Based Routing)
- Возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel и т.д.)
- Возможность приоритизации сетевого трафика (ToS, DiffServ)
- Двухфакторная аутентификация
- Возможность назначения DNS и любых виртуальных IP-адресов для ПО «ЗАСТАВА-Клиент», подключённых к шлюзу, в т.ч. функция DHCP Relay
- Возможность доступа к клиентам ЗАСТАВА по виртуальному IP-адресу (VPN-маршрутизация)
- Возможность автоматической конфигурации маршрутизации при множественных интерфейсах доступа для клиента ЗАСТАВА с помощью технологии Reverse Routing Injection (RRI)
- Возможность работы через NAT (технология NAT-T)
- Поддержка протокола IKEv2, обеспечивающего повышенный уровень безопасности
- Антиспуфинг
- Возможность интеграции с системой мониторинга ZABBIX

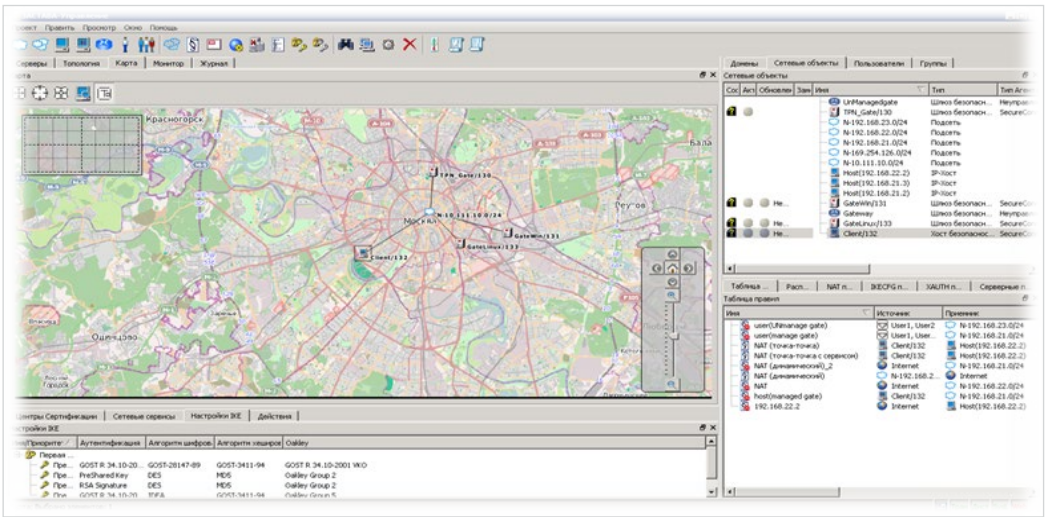
ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа для большого количества пользователей
- Защита высоконагруженных каналов (ЦОД-ЦОД)
- Защита каналов передачи данных в ГИС

ЦУП «ЗАСТАВА-Управление»

Система централизованного управления ЗАСТАВА-Управление является наиболее функциональным, удобным и эффективным инструментом управления среди всех сертифицированных российских разработок систем защиты каналов связи. ЗАСТАВА-Управление позволяет создавать единую политику безопасности — набор правил для защищаемой сети на уровне бизнес-объектов и ролей. Политика формируется в графической консоли и включает в себя сведения о топологии сети (описания объектов с их идентификационной информацией) и правила взаимодействия объектов.





ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Возможность управления десятками и сотнями тысяч агентов безопасности ЗАСТАВА из единого центра
- Интуитивно понятное средство управления безопасностью
- Высокая гибкость в возможных настройках политик безопасности
- Возможна установка на существующие аппаратные платформы заказчика
- Количество управляемых объектов ограничено только мощностью аппаратной платформы
- Отображение статусов объектов управления
- Централизованное обновление агентов безопасности ЗАСТАВА-Офис и ЗАСТАВА-Клиент
- Дистанционная смена ключей и сертификатов
- Инвентаризация устройств
- Возможно использование в режиме Standalone (ЦУП включает в себя ПО «ЗАСТАВА-Офис» для безопасной доставки политик)
- Взаимодействие с другими СЗИ
- Работа под управлением ОС Windows Server 2016
- Функционирует на ОС AstraLinux SE

ПО «ЗАСТАВА-Офис»

ПО «ЗАСТАВА-Офис», версия 8 – программные исполнения криптографических шлюзов. Программные исполнения могут быль установлены на существующие аппаратные платформы архитектуры x64. Интерфейс ПО «ЗАСТАВА-Офис», версия 8 соответствует интерфейсу линейке АПК. ПО «ЗАСТАВА-Офис», версия 8 может выполнять задачи аналогичные линейке АПК. Производительность и сетевые возможности криптографических шлюзов будет зависеть только от подобранных аппаратных платформ. Исполнение ПО «ЗАСТАВА-Офис», версия 8 КС1 может эксплуатироваться в виртуальных стендах.

СОСТАВ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Скорость шифрования: зависит от процессора подобранной аппаратной платформы
- СКЗИ VPN/FW ЗАСТАВА-Офис с криптоядром «ЭЛВИС-Крипто»
- Количество и стандарты сетевых интерфейсов: зависит от сетевых возможностей подобранной аппаратной платформы
- Возможность отказоустойчивого решения
- Балансировка нагрузки
- Для исполнения КС1 возможность развёртывания в виртуальных средах
- Для исполнения КС3 применяется АПМДЗ

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Неограниченное количество защищаемых узлов, подключаемых криптошлюзов и клиентов
- Возможность реализации отказоустойчивого решения (active/passive)
- Полноценная поддержка VLAN (802.1q)
- Шифрование трафика L2
- Шифрование на уровне L3
- Поддержка динамических протоколов маршрутизации
- Поддержка PBR (Policy Based Routing)
- Возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel и т.д.)
- Возможность приоритизации сетевого трафика (ToS, DiffServ)
- Двухфакторная аутентификация
- Возможность назначения DNS и любых виртуальных IP-адресов для ПО «ЗАСТАВАКлиент», подключённых к шлюзу, в т.ч. функция DHCP Relay
- Возможность доступа к клиентам ЗАСТАВА по виртуальному IP-адресу (VPN-маршрутизация)
- Возможность автоматической конфигурации маршрутизации при множественных интерфейсах доступа для клиента ЗАСТАВА с помощью технологии Reverse Routing Injection (RRI)
- Возможность работы через NAT (технология NAT-T)
- Поддержка протокола IKEv2, обеспечивающего повышенный уровень безопасности
- Антиспуфинг
- Функция DHCP Relay
- Возможность интеграции с системой мониторинга ZABBIX

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа с мобильных устройств
- Подключение средних и малых офисов (Small Office Home Office)
- Организация защищённого удалённого доступа с мобильных устройств
- Защита средненагруженных каналов (ЦОД-Офис, Офис-Офис)
- Защита высоконагруженных каналов (ЦОД-ЦОД)
- Защита каналов передачи данных в ГИС

ПО «ЗАСТАВА-Клиент»

Для организации защищённого доступа удалённых пользователей к корпоративным ресурсам на мобильных рабочих станциях устанавливаются программные агенты ЗАСТАВА-Клиент, которые поддерживают версии операционных систем MS Windows XP/7/8/10, а также ALTLinux, Альт 8 СП, AstraLinux 1.6 SE. ЗАСТАВА-Клиент — сертифицированный межсетевой экран 4 класса тип «В», что позволяет защитить мобильного пользователя от несанкционированного доступа и сетевых атак в сети общего пользования Интернет, а также при подключении к публичным точкам беспроводного доступа.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Работа под управлением ОС семейства Windows (10, 11)
- Работа под управлением ОС семейства Linux (Альт 8 СП, AstraLinux 1.6/1.7 SE, РЕД ОС, Android)
- VPN по уровню КС1, КС3 — для ОС Astra Linux SE (ФСБ России), МЭ тип «В» класс 4 (ФСТЭК России)
- Поддержка токенов ESMART, JaCarta, E-token, RuToken, Aladdin для хранения ключевой информации
- Установка «в один клик»
- СКЗИ: используется с криптоядром «ЭЛВИС-Крипто»
- Централизованная настройка DNS-серверов и виртуальных IP-адресов для доступа
- Возможность использования двух политик безопасности (Пользователя и Системная): одна работает до входа в ОС, другая применима индивидуально к каждому пользователю ОС после входа

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа с мобильных устройств
- Защита трафика, передаваемого по общественным сетям передачи данных (Интернет)
- Использование в качестве защищённого мобильного места сотрудника организации

АПК «ЗАСТАВА-ТК» — 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. Уникальность разработки заключается в том, что АПК «ЗАСТАВА-ТК» является продуктом с готовым набором средств защиты информации и сервисом электронной подписи, сертифицированным по классу КС3.

СОСТАВ

- Аппаратная платформа – компьютер в форм-факторе «тонкий клиент»
- Электронный идентификатор, аппаратно реализующий российские стандарты электронной подписи, шифрования, хэширования и являющийся ключевым носителем
- Операционная система Альт 8 СП, 64-битная версия
- Программное обеспечение на базе ЗАСТАВА-Клиент, версия 6 с СКЗИ КриптоПро CSP версия 5.0

ВЫПОЛНЯЕМЫЕ ФУНКЦИИ

- VPN по уровню КС3 (ФСБ России), МЭ тип «В» класс 4 (ФСТЭК России)
- Предоставление сервиса электронной подписи по классу КС3
- Профиль защиты ОС (А четвертого класса защиты)
- Удалённое обновление ключей и ПО «ЗАСТАВА-ТК»

Управление АПК «ЗАСТАВА-ТК» (доставка политик и обновлений) осуществляется стандартным для линейки ПО ЗАСТАВА компонентом ЗАСТАВА-Управление, исполнение КС3, который является наиболее функциональным, удобным и эффективным инструментом управления среди всех сертифицированных российских разработок систем защиты каналов связи.

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ

- Программно-аппаратный тонкий клиент, сертифицированный по классу КС3 без применения дополнительных наложенных аппаратных средств
- Высокая готовность при развёртывании (коробочный продукт)
- Инкрементное удалённое обновление всего ПО тонкого клиента
- Наличие датчика вскрытия
- Минимизация локальных настроек, централизованное удалённое управление политикой безопасности
- Хранение неизвлекаемых ключей на smart card
- Хранение всей ключевой информации на ESMART Token ГОСТ, Рутокен ЭЦП 3.0

ПРЕИМУЩЕСТВА

Комплекс программно-аппаратных средств ЗАСТАВА-ТК позволяет реализовать выполнение требований по информационной безопасности минимальным набором средств и элементов защиты, а также обеспечивает максимальную простоту и надёжность в эксплуатации с возможностью оперативного масштабирования.

- Фиксированный и достаточный набор средств защиты информации для соответствия требованиям по ИБ для ГИС до К1, для КИИ, МИС и ЕГСЗ
- Простота и надёжность в эксплуатации (наработка на отказ оборудования — 60 000 часов)
- Устойчивость к DDoS-атакам
- Гибкое масштабирование
- Централизованное обновление ПО
- Возможность отправки событий в SIEM
- Сертифицированные аппаратные средства контроля вскрытия корпуса
- Контроль целостности программной составляющей до загрузки ОС
- Все элементы АПК имеют российское происхождение и разработаны под условия применения в РФ

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Организация защищённого удалённого доступа
- Защита трафика, передаваемого по общественным сетям передачи данных (Интернет)
- Унифицированное защищённое рабочее место сотрудника ГИС

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

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Обнаружение компьютерных атак со скоростью передачи данных не менее 1 Гбит/с сигнатурным методом
- Подключение до 100 сенсоров к одному серверу
- Гибкая настройка системы:
  — задание контролируемых подсетей и IP-адресов;
  — создание и выбор сигнатур;
  — задание индивидуальных правил для каждого сенсора
- Маскирование СОА в сети и невыявление её на сетевом уровне стандартными средствами операционных систем
- Различные способы подключения к каналам связи: по схеме «Т-образие» или «в разрыв»
- Возможность передавать события в SIEM
- Обнаружение атак, описанных в базе сигнатур, с вероятностью более 99,5%
- Наличие сервера централизованного управления с веб-интерфейсом с возможностью индивидуальной работы с каждым сенсором и удобного отображения и сбора статистики

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Защита ресурсов ЦОД от атак

Технология **Базовый Доверенный Модуль (БДМ)** разработана в соответствии с требованиями российских регулирующих органов в области защиты информации и современными мировыми стандартами и предназначена для построения доверенной вычислительной среды на мобильных компьютерах, ноутбуках и планшетах, базирующихся на архитектуре Intel x64. Технология БДМ не противопоставляется реализованным в архитектуре Intel x64 мобильного устройства механизмам доверенной загрузки (PTT, Secure Boot и др.) – они могут использоваться для повышения уровня защищённости и выстраивания многоуровневой защиты от несанкционированного воздействия на доверенную вычислительную среду. Технология БДМ реализуется при помощи программного обеспечения и не требует никаких дополнительных наложенных аппаратных средств, за исключением внешнего носителя ключа.

Первым сертифицированным ФСБ России продуктом с технологией БДМ является средство криптографической защиты информации (СКЗИ) «Мобильное защищенное автоматизированное рабочее место «Базовый доверенный модуль» версии 3 в исполнении 1» (МЗ АРМ «БДМ»)

МЗ АРМ «БДМ» — это мобильный компьютер (ноутбук или планшет) со специальными функциями защиты данных, которые интегрируются в программно-аппаратную платформу и предотвращают угрозы хищения данных или раскрытия информации на потерянных, украденных или неправильно выведенных из эксплуатации компьютерах, а также при передаче данных по сети Интернет.

МЗ АРМ «БДМ» обеспечивает защиту данных пользователя и предотвращает несанкционированный доступ к компьютеру путем авторизации пользователя до загрузки ОС и прозрачного шифрования всего системного раздела. При подключении к сети МЗ АРМ «БДМ» обеспечивает защиту канала передачи данных с помощью шифрования с использованием протоколов IKE/IPsec. Для защиты взаимодействия МЗ АРМ «БДМ» с корпоративной информационной сетью используется VPN-клиент ЗАСТАВА.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- Поддержка основных производителей UEFI BIOS (AMI, Phoenix, Insyde)
- Контроль целостности аппаратного и программного обеспечения, начиная с включения питания и до завершения работы с устройством
- Двухфакторная строгая аутентификация на уровне BIOS до загрузки ОС
- Поддержка в качестве ключевых носителей, JaCarta 2 ГОСТ, Рутокен ЭЦП 2.0
- На платформах с UEFI BIOS AMI работа БДМ в режиме средства доверенной загрузки по требованиям ФСТЭК России
- Шифрование всех данных на жёстком диске мобильного устройства
- Криптографическая защита информации в соответствии с ГОСТ Р 34.12–2015 с использованием режимов ГОСТ Р 34.13–2015
- Фоновое перешифрование (возможность прозрачной для пользователя замены ключей без отрыва от штатного функционирования ПЭВМ)
- Утилита ОС, отображающая пользователю статус перешифрования диска
- Расширенные функции администрирования:
  — смена ключей шифрования;
  — сохранение журнала работы на административный носитель;
  — обновление файла контроля целостности объектов доверенной ОС

ОБЛАСТИ И ОПЫТ ПРИМЕНЕНИЯ

- Защищённое мобильное рабочее место руководителя
- Защищённое мобильное рабочее место сотрудника во время командировки или дистанционной работы

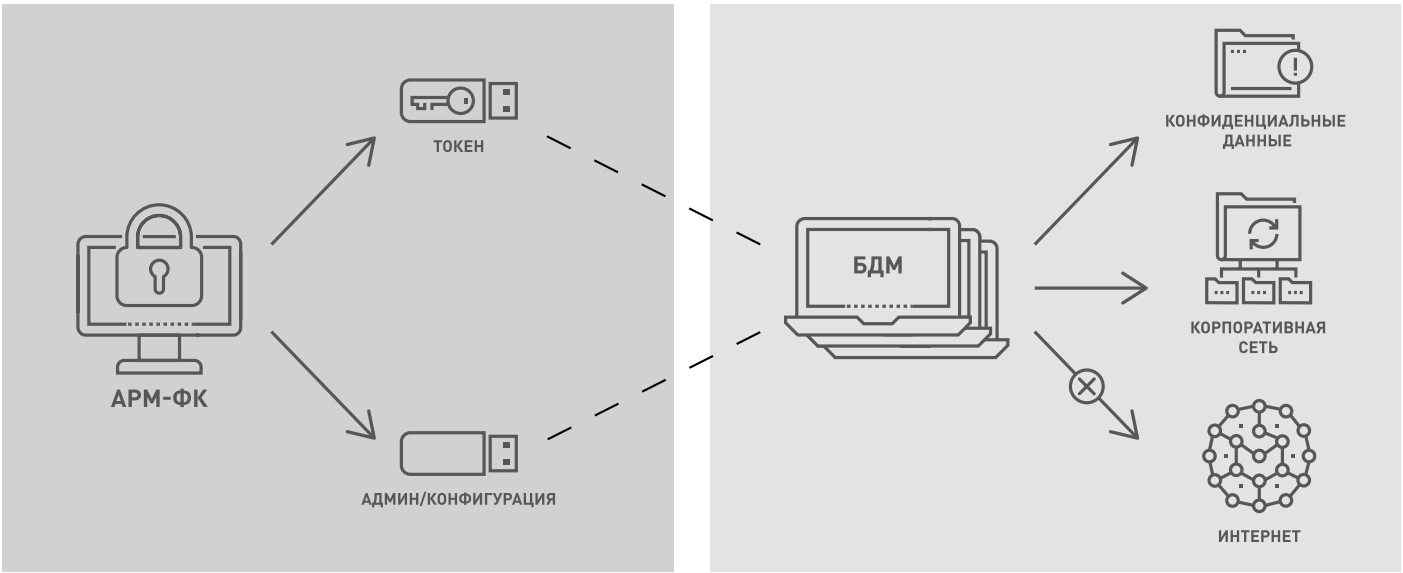
Базовый Доверенный Модуль. Автоматизированное рабочее место формирования ключей (БДМ-АРМ-ФК версия 3) — стационарный компьютер, который предназначен для администрирования МЗ АРМ «БДМ». СКЗИ сертифицировано по классу КС2 ФСБ России.

ВЫПОЛНЯЕМЫЕ ФУНКЦИИ

- Создание ключевой информации
- Хранение и каталогизация конфигурационных параметров рабочих станций МЗ АРМ «БДМ» и аутентифицирующих пользователей данных с помощью специального программного обеспечения (СПО) «БДМ-АРМ-ФК»
- Подготовка ключевых носителей для авторизации пользователей и создание USB-носителя МЗ АРМ «БДМ», предназначенного для установки и управления СКЗИ МЗ АРМ «БДМ» на рабочих станциях пользователей
- Дискреционное разграничение доступа Администратора АРМ и Администратора безопасности к информации об устройствах
- Контроль целостности ключевой и конфигурационной информации пользователей, сохраненной в базе данных СКЗИ «БДМ-АРМ-ФК»

СОСТАВ

- СПО «БДМ-АРМ-ФК»
- СКЗИ КриптоПро CSP версия 4.0 R4 2-Base
- СЗИ Secure Pack Rus версия 3.0 (исполнение 6)
- Программно-аппаратное средство защиты от несанкционированного доступа (НСД), имеющее действующий сертификат ФСБ России и соответствующее требованиям по использованию программно-аппаратных средств защиты от НСД в соответствии с эксплуатационной документацией КриптоПро CSP 4.0 R4 2-Base из состава СЗИ Secure Pack Rus версии 3.0 (исполнение 6)



Область применения	Продукт из линейки	Примеры использования
Государственные информационные системы	ЗАСТАВА-150 ЗАСТАВА-1500 ЗАСТАВА-6000 ЗАСТАВА-10000 ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ ЗАСТАВА-IDS	Организация защищённого подключения к ресурсам ЦОД множества региональных объектов (L2, L3 шифрование) Шифрование канала между ЦОД и РЦОД Организация защищённого рабочего места мобильного сотрудника для выездной работы
Межведомственное взаимодействие	ЗАСТАВА-1500 ЗАСТАВА-6000 ЗАСТАВА-10000 ЗАСТАВА-Управление ЗАСТАВА-IDS	Организация защищённого обмена между различными ведомствами (L2, L3 шифрование) Шифрование канала между ЦОД различных ведомств
Медицина	ЗАСТАВА-150 ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ	Организация защищённого канала между терминалами ЕМИАС в поликлиниках и ЦОД Защита каналов передачи данных между рабочим местом врача и БД в ЦОД
Транспорт	ЗАСТАВА-Клиент	Защита трафика, передаваемого между информационными табло на остановках и ЦОД
Многофункциональные центры по оказанию государственных услуг	ЗАСТАВА-150 ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ	Организация защищённого доступа к информационным системам множества ГИС, ФОИВ и ГОИВ Организация защищённого рабочего места мобильного сотрудника для выездной работы
Образовательные учреждения	ЗАСТАВА-150 ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ	Проведение ЕГЭ, мобильное защищённое рабочее место организатора Получение и отправка данных по защищённому каналу Защищённое рабочее место бухгалтера Защита информации, передаваемой между системой прохода и ЦОД
Нефтегазовая промышленность	ЗАСТАВА-150 ЗАСТАВА-1500 ЗАСТАВА-6000 ЗАСТАВА-10000 ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ ЗАСТАВА-IDS	Защита трафика, передаваемого между компонентами АСУ ТП Шифрование канала между площадками Организация защищённого рабочего места мобильного сотрудника во время командировки
Энергетика	ЗАСТАВА-150 ЗАСТАВА-Клиент ЗАСТАВА-Управление	Объединение подстанций/филиалов в единую защищённую информационную сеть (L2, L3 шифрование)
Строительство	ЗАСТАВА-150 ЗАСТАВА-Клиент ЗАСТАВА-Управление БДМ	Организация защищённого удаленного доступа со строительных площадок при использовании радиорелейных станций или спутниковой связи (L2, L3 шифрование) Организация защищённого удаленного доступа со строительных площадок при использовании кабельных каналов (L2, L3 шифрование)
Защита АСУ ТП	ЗАСТАВА-150 ЗАСТАВА-1500 ЗАСТАВА-6000 ЗАСТАВА-10000 ЗАСТАВА-Управление ЗАСТАВА-IDS	Защита трафика, передаваемого между компонентами АСУ ТП
Защита каналов связи между центрами обработками данных	ЗАСТАВА-6000 ЗАСТАВА-10000 ЗАСТАВА-Управление ЗАСТАВА-IDS	Шифрование канала между ЦОД и РЦОД (L2 или L3 шифрование)
Малый и средний бизнес (создание приватной сети между офисами)	ЗАСТАВА-150 ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ	Объединение офисов в единую защищённую информационную сеть (L2, L3 шифрование) Организация защищённого рабочего места мобильного сотрудника
Защищённое мобильное рабочее место	ЗАСТАВА-Клиент ЗАСТАВА-ТК ЗАСТАВА-Управление БДМ	ММЗ АРМ для сотрудников ГИБДД на посту, проверки штрафов и правонарушений Для мобильных сотрудников МФЦ, оказывающих услуги в районах, где здание МФЦ находится в процессе строительства Для сотрудников, находящихся в командировке

Основные характеристики	ЗАСТАВА-150	ЗАСТАВА-1500	ЗАСТАВА-6000	ЗАСТАВА-10000
Сетевые интерфейсы, Мб	• 6x10/100/1000 GbE	• 4x1 GbE, 2x1 Gb SFP • 8x1 GbE, 2x1 Gb SFP • 12x1 GbE, 2x1 Gb SFP • 4x1 GbE, 10x1 Gb SFP • 4x1 GbE, 2x1 Gb SFP, 4x10 Gb SFP+	• 4x1 GbE, 4x1 Gb SFP, 4x10 Gb SFP+ • 4x1 GbE, 8x10 Gb SFP+	• 5x1 GbE, 4x10 Gb SFP+ • 1x1 GbE, 8x10 Gb SFP+ • 1x1 GbE, 4x10 Gb SFP+, 4x10/25 GbE SFP28
Скорость шифрования, Мб/с	до 300	до 1500	до 6000	до 10000
Тип ОС	ZASTAVA OS	ZASTAVA OS	ZASTAVA OS	ZASTAVA OS
Требование к наличию АПМДЗ	нет	да	да	да
Класс сертификации по ФСБ России	ФСБ России КС3 ФСТЭК России МЭ 4А	ФСБ России КС3	ФСБ России КС3	ФСБ России КС3

Компания ЭЛВИС-ПЛЮС является разработчиком средств защиты информации и одним из ведущих системных интеграторов в области информационной безопасности. Компания оказывает широкий спектр консалтинговых и интеграционных услуг в области построения государственных и корпоративных информационных систем, компьютерных сетей и систем информационной безопасности.

presale@elvis.ru | elvis.ru