Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент» версия 8 КС3» (исполнение ZC8-AS64-VF-03)

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

2025

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ 3

1.1. Наименование и условное обозначение 3

1.2. Варианты исполнения 3

1.3. Разработчик 3

1.4. Поставщик 3

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ 4

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ 6

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование и условное обозначение

Наименование – Программно-аппаратный комплекс «VPN/FW «ЗАСТАВА-Клиент» версия 8 КС3» (исполнение ZC8-AS64-VF-03).

Условное обозначение – ПО «ЗАСТАВА-Клиент» версия 8 КС3» (далее – ПО «ЗАСТАВА-Клиент»).

1.2. Варианты исполнения

Варианты исполнений ПО «ЗАСТАВА-Клиент», поддерживаемые операционные системы (ОС), соответствие исполнений классам защиты СКЗИ, а также типам и классам защиты межсетевых экранов приведены в таблице (см. Таблица 1).

Таблица 1 - Варианты исполнений ПО «ЗАСТАВА-Клиент»

Исполнение	Поддерживаемые ОС	Класс защиты СКЗИ	Тип и класс защиты МЭ
ZC8-WX64-VF-01	ОС Microsoft Windows 10, ОС Microsoft Windows 11	КС1	В4
ZC8-RD64-VF-01	РЕД ОС 7.3	КС1	В4
ZC8-AL64-VF-01	ОС Альт 8 СП	КС1	В4
ZC8-AS64-VF-01	ОС Astra Linux Special Edition 1.7	КС1	В4
	ОС Astra Linux Special Edition 1.8		
	ОС Astra Linux Common Edition x64		
ZC8-AS64-VF-03	ОС Astra Linux Special Edition 1.7	КС3	В4

1.3. Разработчик

Акционерное общество «ЭЛВИС-ПЛЮС».

124527, Москва, Зеленоград, Солнечная аллея, д. 6, помещение VI, офис 7.

Тел. (495) 276-0211.

1.4. Поставщик

Акционерное общество «ЭЛВИС-ПЛЮС».

124527, Москва, Зеленоград, Солнечная аллея, д. 6, помещение VI, офис 7.

Тел. (495) 276-0211.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

ПО «ЗАСТАВА-Клиент» предназначено для реализации защищённого взаимодействия на сетевом уровне модели OSI/ISO (на уровне TCP/IP-протокола) с использованием технологий VPN и на основе интернет-протоколов семейства IP Security (Internet Protocol Security, далее – IPSec) и осуществления функций межсетевого экрана с целью защиты рабочего места конечного пользователя.

ПО «ЗАСТАВА-Клиент» предназначено для применения в государственных информационных системах, информационных системах обработки персональных данных, системах обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры и обеспечивает защиту информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну.

ПО «ЗАСТАВА-Клиент» обеспечивает выполнение криптографических функций шифрования, контроля целостности данных, имитозащиты данных, аутентификации.

ПО «ЗАСТАВА-Клиент» обеспечивает защиту на сетевом уровне модели взаимодействия OSI/ISO с использованием технологий VPN и межсетевого экранирования за счёт использования протоколов двухсторонней криптографической аутентификации при установлении соединений (ESP, IKEv2), описываемых рекомендациями и стандартами:

- Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2)»;
- Р 1323565.1.035–2021 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP»;
- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры («Магма» и «Кузнечик» в режиме MGM)»;
- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»;
- Р 1323565.1.023-2018 «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в

сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509»;

- Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»;
- Р 1323556.1.024-2019 «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов».

Для совместимости с другими программными и аппаратно-программными изделиями линейки «ЗАСТАВА» производства АО «ЭЛВИС-ПЛЮС» ПО «ЗАСТАВА-Клиент» обеспечивает:

- конфиденциальность передаваемой в корпоративной информационно-телекоммуникационной сети информации за счет её шифрования согласно ГОСТ 28147-89;
- защиту при осуществлении доступа к корпоративным вычислительным ресурсам за счёт использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2 с использованием алгоритмов подписи в соответствии с ГОСТ Р 34.10-2012;
- контроль целостности данных на основе применения ГОСТ Р 34.11-2012;
- имитозащиту данных на основе применения ГОСТ 28147-89 в режиме имитовставки;
- поддержку схемы открытого распределения ключей Диффи-Хеллмана на основе алгоритма ГОСТ Р 34.10-2012 VKO в 256-битном режиме.

ПО «ЗАСТАВА-Клиент» реализует пакетную фильтрацию по IP-адресу (диапазон IP) источника и назначения, номера портов и тип протокола, типы и коды сообщений ICMP, по направлению пакетов.

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

Сведения о функциональных, технических и эксплуатационных характеристиках ПО «ЗАСТАВА-Клиент» приведены в таблице (см. Таблица 2).

Таблица 2 - Функциональные, технические и эксплуатационные характеристики ПО «ЗАСТАВА-Клиент»

Характеристика	Описание
Конфигурирование и мониторинг	Утилиты командной строки, реализующие функции конфигурирования и мониторинга ПО «ЗАСТАВА-Клиент»
	Мониторинг с использованием протокола SNMP v2 и v3 (поддержка SNMP-трапов для удалённого оповещения о событиях
Идентификация и аутентификация	Двухфакторная идентификация и аутентификация пользователя ПО «ЗАСТАВА-Клиент» на основании цифрового сертификата X.509, хранящегося на программном или физическом ключевом носителе, и предъявленного PIN-кода
	Идентификация партнёров межсетевого взаимодействия по сетевому адресу, порту и протоколу субъектов
Реализация политики безопасности	Применение политики драйвера по умолчанию до загрузки ПО «ЗАСТАВА-Клиент»
	Применение системной политики безопасности после загрузки ПО «ЗАСТАВА-Клиент»
	Применение политики безопасности пользователя после аутентификации в ОС
Контроль целостности	Реализован механизм контроля целостности ПО «ЗАСТАВА-Клиент» по контрольным суммам в процессе его загрузки
	Для исполнения ПО «ЗАСТАВА-Клиент» ZC8-AS64-VF-03 реализован механизм динамического контроля целостности во время его работы
Криптографическая защита	Защита трафика за счёт аутентифицированного шифрования IP-пакетов на основе протокола IPsec ESP и взаимной аутентификации с применением функций, реализующих криптографические алгоритмы, основанные на российских стандартах ГОСТ Р 34.12-2015 («Магма» и «Кузнечик» в режиме МГМ), ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
	Защита трафика за счёт шифрования IP-пакетов на основе протокола IPsec ESP, передаваемых в корпоративных информационно-телекоммуникационных системах информации, в соответствии с ГОСТ 28147-89 и имитозащиты данных на основе применения ГОСТ 28147-89 в режиме имитовставки
	Защита при доступе к корпоративным вычислительным ресурсам за счёт использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2 с использованием алгоритмов подписи в соответствии с ГОСТ Р 34.10-2012
	Контроль целостности данных на основе применения ГОСТ Р 34.11-2012
	Поддержка схемы открытого распределения ключей Диффи-Хеллмана на основе алгоритма ГОСТ Р 34.10-2012 VKO в 256-битном режиме
	Криптографическая защита передаваемой информации за счёт функционала криптопровайдера «Элвис-Крипто» производства АО «ЭЛВИС-ПЛЮС» и СКЗИ USB-токена RU.63793390.00003-01 ESMART Token ГОСТ (форм-фактор USB) и КБДЖ.01558 Рутокен ЭЦП 3.0 (форм-фактор USB)
Пакетная фильтрация	Пакетная фильтрация по IP-адресу (диапазон IP) источника и назначения, номера портов и тип протокола, типы и коды сообщений ICMP, по направлению пакетов
Защищённое подключение (использование режима IKECFG)	Возможность назначения DNS и любых виртуальных IP-адресов, а также функцию DHCP Relay для ПО «ЗАСТАВА-Клиент»
	Возможность доступа к ПО «ЗАСТАВА-Клиент» по виртуальному IP-адресу (VPN-маршрутизация)

Характеристика	Описание
Журналирование	Фиксация в локальном и системном (syslog) журнале аудита следующий список информации: — регистрация событий вход\выход пользователей в СКЗИ; — регистрация событий по контролю целостности аппаратного обеспечения и ПО; — регистрация и учет запросов на установление соединений; — регистрация событий, связанных с выполнением в ПО криптографических функций; — создание и удаление защищённых соединений
	Возможность передачи данных системного журнала на удаленный syslog-сервер
Дополнительные функции	Контроль фрагментированных пакетов, поддержка Path MTU Discovery
	Возможность работы через NAT (технология NAT-T)
	Выполнение функций трансляции сетевых адресов NAT в соответствии с правилами заданной политики
	Реализация IKEv2, повышенный уровень безопасности и защиты от DDoS-атак
	Наличие функционала антиспуфинга
Обновление	Возможность автоматизированного обновления по командам от сервера централизованного управления
Совместимость	ПО «ЗАСТАВА-Клиент» совместимо с программными и аппаратно-программными изделиями линейки «ЗАСТАВА» производства АО «ЭЛВИС-ПЛЮС»