Программное обеспечение
«VPN/FW «ЗАСТАВА-Офис», версия 8»

Функциональные характеристики

2024

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование изделия и условное обозначение

1.1.1. Наименование изделия – Программное обеспечение «VPN/FW «ЗАСТАВА-Офис», версия 8».

1.1.2. Условное обозначение – ПО «VPN/FW «ЗАСТАВА-Офис», версия 8» (далее – ПО).

1.2. Варианты использования

1.2.1. В зависимости от требований по уровню защиты СКЗИ (КС1 или КС3), ПО «VPN/FW «ЗАСТАВА-Офис», версия 8» может применяться в качестве:

- Программного обеспечения «VPN/FW «ЗАСТАВА-Офис», версия 8 КС1;
- Программного обеспечения «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3.

1.2.2. В случае применения «VPN/FW «ЗАСТАВА-Офис», версия 8» в системах, где необходимо обеспечить уровень защиты СКЗИ класса КС3 («Программное обеспечение «VPN/FW «ЗАСТАВА-Офис», версия 8 КС3»), СВТ, на котором устанавливается ПО, должно быть укомплектовано аппаратно-программным модулем доверенной загрузки (АПМДЗ), прошедшим оценку соответствия ФСБ России.

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

2.1. ПО «VPN/FW «ЗАСТАВА-Офис», версия 8» предназначено для защиты корпоративных вычислительных ресурсов на сетевом уровне модели взаимодействия OSI/ISO (на уровне TCP/IP-протокола) с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IP Security (Internet Protocol Security, далее – IPSec).

2.2. ПО предназначено для применения в государственных информационных системах, информационных системах обработки персональных данных, системах обеспечения информационной безопасности значимых объектов КИИ и обеспечивает защиту информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну.

2.3. ПО обеспечивает выполнение криптографических функций: шифрования, контроля целостности данных, имитозащиты данных, аутентификации абонентов.

2.4. ПО обеспечивает защиту на сетевом уровне модели взаимодействия OSI/ISO с использованием технологий VPN и распределенного межсетевого экранирования за счет 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.

2.5. Для совместимости с другими программными и аппаратно-программными исполнениями «ЗАСТАВА» производства АО «ЭЛВИС-ПЛЮС» ПО обеспечивает:

— конфиденциальность передаваемой в корпоративной информационно-телекоммуникационной сети (ИТКС) информации за счет ее шифрования согласно ГОСТ 28147-89;

— защиту доступа к корпоративным вычислительным ресурсам за счет 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.

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

2.7. ПО может эксплуатироваться без перезагрузки в течение 7 (семи) суток.

2.8. Скоростные характеристики ПО зависят от выбранной аппаратной платформы. Перечень поддерживаемых аппаратных платформ приведён в документе «Программное обеспечение «VPN/FW «ЗАСТАВА-Офис», версия 8». Руководство администратора».

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

Сведения о функциональных, технических и эксплуатационных характеристиках ПО приведены в таблице:

Таблица 1 - Функциональные, технических и эксплуатационных характеристиках ПК

№ п.п.	Сведения о функциональных, технических и эксплуатационных характеристиках ПО
1.	***Конфигурирование и мониторинг***
1.1.	Утилиты командной строки, реализующие функции конфигурирования и мониторинга ПО
1.2.	Мониторинг с использованием протокола SNMP v2 и v3: – поддерживает SNMP trap для удаленного оповещения о событиях; – поддерживает SNMP MIB для получения статистики ПО
1.3.	Возможность интеграции с по мониторинга zabbix
2.	***Идентификация и аутентификация***
2.1.	Двухфакторная идентификация и аутентификация пользователя ПО на основании цифрового сертификата X.509, хранящегося на ключевом носителе (ФКН) и предъявленного PIN-кода
2.2.	Идентификация партнеров межсетевого взаимодействия по сетевому адресу, порту и протоколу субъектов
3.	***Реализация политики безопасности***
3.1.	Поддержка централизованного управления VPN из единого центра управления на основе сформированных единых политик безопасности
3.2.	Применение политики драйвера по умолчанию до загрузки ПО
3.3.	Применение системной политики безопасности после загрузки ПО
4.	***Контроль целостности***
4.1.	Реализован механизм контроля целостности ПО по КС в процессе загрузки
5.	***Криптографическая защита***
5.1.	Защита трафика за счет 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
5.2.	Защита трафика за счет 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
5.3.	Защита доступа к корпоративным вычислительным ресурсам за счет использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2 с использованием алгоритмов подписи в соответствии с ГОСТ Р 34.10-2012
5.4.	Контроль целостности данных на основе применения ГОСТ Р 34.11-2012
5.5.	Поддержка схемы открытого распределения ключей Диффи-Хеллмана на основе алгоритма ГОСТ Р 34.10-2012 VKO в 256-битном режиме
5.6.	Криптографическая защита передаваемой информации за счет функционала криптопровайдера «Элвис-Крипто» производства АО «ЭЛВИС-ПЛЮС» и СКЗИ USB-

№ п.п.	Сведения о функциональных, технических и эксплуатационных характеристиках ПО
	токена RU.63793390.00003-01 ESMART Token ГОСТ (форм-фактор USB) и КБДЖ.01558 Рутокен ЭЦП 3.0 (форм-фактор USB)
5.7.	Возможность использования конфигурируемых исходных туннельных адресов
5.8.	Возможность шифрования трафика уровня L2
6.	***Пакетная фильтрация***
6.1.	Пакетная фильтрация по IP-адресу (диапазон IP) источника и назначения, номера портов и тип протокола, типы и коды сообщений ICMP, по направлению пакетов
6.2.	Возможность создания правил защиты трафика для каждого сетевого интерфейса индивидуально
7.	***Подключение клиентов (использование режима IKECFG)***
7.1.	Возможность назначения DNS и любых виртуальных IP-адресов для компоненты ПО «ЗАСТАВА-Клиент», подключённых к шлюзу, включая функцию DHCP Relay
7.2.	Количество подключений к шлюзу программно не ограничено
7.3.	Возможность доступа к ПО «ЗАСТАВА-Клиент» по виртуальному IP-адресу (VPN-маршрутизация)
8.	***Журналирование***
8.1.	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 виртуальных соединений; – регистрация событий, связанных с выполнением в ПО криптографических функций; – создание и удаление защищённых соединений
8.2.	Возможность передачи данных системного журнала на удаленный syslog-сервер
9.	***Отказоустойчивость***
9.1.	Функция «горячего» резервирования функций межсетевого экранирования и VPN
9.2.	Возможность реализации сценария отказоустойчивого решения в режиме распределения нагрузки для ПО «ЗАСТАВА-Клиент»
9.3.	Возможность функционирования в отказоустойчивом исполнении (кластер active/passive)
10.	***Маршрутизация***
10.1.	Поддержка динамической маршрутизации с применением протоколов BGP и OSPF
10.2.	Поддержка PBR (Policy Based Routing)
10.3.	Наличие Reverse Routing Injection (RRI)
11.	***Дополнительные функции***
11.1.	Поддержка QoS: IP TOS-мапирование поверх зашифрованных IP-пакетов
11.2.	Возможность приоритезации трафика (ToS, DiffServ)
11.3.	Контроль фрагментированных пакетов, поддержка Path MTU Discovery
11.4.	Возможность работы через NAT (технология NAT-T)

№ п.п.	Сведения о функциональных, технических и эксплуатационных характеристиках ПО
11.5.	Выполнение функций NAT-устройства (трансляции сетевых адресов NAT/PAT в соответствии с правилами заданной политики)
11.6.	Реализация IKEv2, повышенный уровень безопасности и защиты от DDoS-атак
11.7.	Наличие функционала антиспуфинга
11.8.	Наличие функции DHCP Relay
11.9.	Возможно выполнение функций DHCP-сервера, NTP-сервера
11.10	Возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel)
12.	***Обновление***
12.1.	Возможность автоматизированного обновления по командам от сервера централизованного управления
13.	***Совместимость***
13.1.	Изделие совместимо с программными и аппаратно-программными исполнениями «ЗАСТАВА» производства АО «ЭЛВИС-ПЛЮС»