«Программный комплекс

«VPN/FW «ЗАСТАВА-Управление», версия 6 КС3»

(«VPN/FW «ЗАСТАВА-Управление», версия 6 КС3»)
(исполнение ZM-WS64-VO-03)

Функциональные характеристики

2022

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование изделия и условное обозначение

1.1.1. Наименование изделия – Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (далее ПК «ЗАСТАВА-Управление», ПК).

1.1.2. Условное обозначение – ПК «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3».

1.2. Разработчик

Акционерное общество «ЭЛВИС-ПЛЮС».

124527, Москва, Зеленоград, Солнечная аллея, д. 6, помещение VI, офис 7, тел. (495) 276-0211.

1.3. Поставщик

Акционерное общество «ЭЛВИС-ПЛЮС».

124527, Москва, Зеленоград, Солнечная аллея, дом 6, тел. (495) 276-0211.

1.4. Модификация

Исполнение ZM-WS64-VO-03.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. ПК является центром управления и предназначен для удаленного администрирования программных и аппаратно-программных СКЗИ до класса защиты КС3 и межсетевых экранов (МЭ), производимых АО «ЭЛВИС-ПЛЮС».

2.2. В качестве центра управления политиками ПК обеспечивает:

- задание глобальной политики безопасности (ГПБ) с описанием топологии информационной телекоммуникационной системы и заданием правил шифрования/фильтрации (правил разграничения доступа);
- формирование локальных политик безопасности для управляемых СКЗИ и МЭ;
- доставку политики безопасности до управляемых СКЗИ и МЭ по защищенному каналу;
- мониторинг состояния управляемых СКЗИ и МЭ;
- удаленное обновление ПО управляемых СКЗИ и МЭ.

2.3. ПК обеспечивает криптографическую защиту служебной информации (локальных политик безопасности (ЛПБ), команд управления) при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны.

2.4. ПК обеспечивает выполнение криптографических функций: шифрования, контроля целостности данных, имитозащиты данных, аутентификации абонентов, что обеспечивает:

- конфиденциальность передаваемой в корпоративной информационно-телекоммуникационной сети (ИТКС) служебной информации (ЛПБ, команд управления), за счет ее шифрования согласно ГОСТ 28147-89;
- защиту доступа к служебной информации (ЛПБ, команд управления) за счет использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протоколов IKEv2 с использованием алгоритмов подписи в соответствии 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 алгоритмов ГОСТ Р 34.10-2012 VKO в 256-битном режиме.

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

3.1. В ПК реализован графический пользовательский интерфейс.

3.2. ПК обеспечивает возможность задания топологии объектов и правил фильтрации трафика с помощью графического интерфейса или веб-службы (создание ГПБ).

3.3. В ПК реализована ролевая модель и разграничение доступа на основании принадлежности к домену (здесь и далее домен – термин ПК «ЗАСТАВА-Управление»).

3.4. Создание Администратора ПК с максимальными привилегиями в Глобальном домене (Глобальный администратор).

3.5. Блокирование учетной записи пользователя ПК на 60 (шестьдесят) сек. по умолчанию после 5 (пяти) неудачных попыток подключения.

3.6. Запрет доступа неаутентифицированного пользователя ПК (Администратора ПК).

3.7. ПК формирует правила фильтрации трафика с заданием следующих атрибутов:

- сетевой адрес узла отправителя/отправителей;
- сетевой адрес узла отправителя/получателей;
- порт и протокол;
- направление трафика;
- действие, выполняемое над пакетом (пропускать/отбрасывать/шифровать);
- идентификатор сетевого интерфейса, через который проходит пакет;
- правила для переназначения IP-адресов (NAT правила);
- уровень протоколирования, который будет применен на МЭ при обработке пакета в соответствии с правилом фильтрации;
- список SNMP-трапов;
- параметры для отправки syslog-сообщений.

3.8. ПК обеспечивает возможность задания параметров шифрования, контроля целостности и имитозащиты данных.

3.9. ПК обеспечивает возможность задания параметров двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2, таких как: алгоритм ЭП, алгоритм шифрования, алгоритм хеширования, алгоритм генерации ключей Диффи-Хеллмана.

3.10. ПК обеспечивает запуск команды на удаленное обновление управляемых агентов безопасности с сервера обновления.