

«Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КСЗ»

**(«VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КСЗ»
(исполнение ZO6-L64-FV-03»)**

Функциональные характеристики

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ.....	3
1.1. Наименование изделия и условное обозначение	3
1.2. Разработчик	3
1.3. Поставщик	3
1.4. Модификация	3
2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	4
3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ	6

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование изделия и условное обозначение

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

1.1.2. Условное обозначение – ПК «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КСЗ».

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 ZO6-L64-FV-03.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. ПК «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КСЗ» (далее – ПК) предназначен для защиты открытой информации в информационных системах общего пользования и конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных и телекоммуникационных системах с выполнением следующих функций:

- защита трафика за счет шифрования IP-пакетов на основе IPsec ESP, передаваемой в корпоративных ИТКС информации, в соответствии с ГОСТ 28147-89;
- защита доступа к корпоративным вычислительным ресурсам за счет использования протоколов двухсторонней криптографической аутентификации при установлении соединений;
- пакетная фильтрация входящего и исходящего трафика;
- контроль целостности пакетов посредством вычисления значения хэш-функции.

2.2. ПК обеспечивает встречную работу с СКЗИ, производимыми АО «ЭЛВИС-ПЛЮС».

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

2.4. ПК обеспечивает контроль и фильтрацию сетевых пакетов в соответствии с заданными правилами, а также защиту криптографическими методами передаваемой по каналам связи информации конфиденциального характера.

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

2.6. В качестве СКЗИ ПК обеспечивает выполнение криптографических функций: шифрования, контроля целостности данных, имитозащиты данных, аутентификации абонентов, что 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 посредством вычисления значения их хэш-функции в соответствии с 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.

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

3.1. В ПК реализована возможность получения политики безопасности от сервера централизованного управления и последующего применения полученной политики.

3.2. ПК реализует режим защиты, используемый до загрузки операционной системы (ОС), за счет применения политики драйвера по умолчанию.

3.3. ПК реализует режим защиты, используемый перед входом и после выхода пользователя из ОС, за счет применения системной политики безопасности.

3.4. ПК реализует возможность конфигурирования IP-адреса клиентов при создании защищённых соединений (использование режима IKECFG).

3.5. ПК осуществляет контроль целостности своих файлов при каждом запуске.

3.6. В процессе функционирования ПК фиксирует в локальном журнале аудита следующий список информации:

- запуск и завершение системной службы ПК;
- результаты выполнения проверки контроля целостности;
- изменение настроек ПК;
- сведения об установленных соединениях;
- результаты обработки пакетов.

3.7. В ПК реализована возможность автоматизированного обновления по командам от сервера централизованного управления.

3.8. В ПК реализована возможность выполнения функций NAT-устройства (трансляции сетевых адресов NAT/PAT в соответствии с правилами заданной политики).

3.9. В ПК реализована возможность функционирования в кластерном режиме.

3.10. В ПК реализована возможность отправки SNMP-трапов для удаленного оповещения о событиях.

3.11. В ПК реализована поддержка SNMP MIB для получения статистики с ПК.

3.12. В ПК реализована возможность отправки syslog на удаленный компьютер.

3.13. В ПК реализована полноценная поддержка VLAN (802.1q).

3.14. В ПК реализована возможность управления качеством обслуживания (QoS): IP TOS-мапирование поверх зашифрованных IP-пакетов.

3.15. В ПК реализована возможность шифрования трафика уровня L2.

3.16. В ПК реализована поддержка динамических протоколов маршрутизации.

3.17. В ПК реализована поддержка PBR (Policy Based Routing).

3.18. В ПК реализована возможность агрегирования интерфейсов (Teaming, Bonding, EtherChannel).

- 3.19. В ПК реализована возможность назначения DNS и любых виртуальных IP-адресов для компонент «ЗАСТАВА-Клиент», подключённых к шлюзу, включая функцию DHCP Relay.
- 3.20. В ПК реализована функциональность Reverse Routing Injection (RRI).
- 3.21. В ПК реализован контроль фрагментированных пакетов, поддержка Path MTU Discovery.