«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», версия 6»

(«ПК «VPN/FW «ЗАСТАВА», версия 6»)

Компонент «ЗАСТАВА-Управление», версия 6

Функциональные характеристики

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование изделия и условное обозначение

Наименование – «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», версия 6» («ПК «VPN/FW «ЗАСТАВА», версия 6»). «Компонент «ЗАСТАВА-Управление», версия 6». (Далее ПК «ЗАСТАВА-Управление», ПК).

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».

124498, Москва, Зеленоград, Солнечная аллея, дом 6, тел. (495) 276-0211.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. «ЗАСТАВА-Управление» является центром управления и предназначен для удаленного администрирования программных и аппаратно-программных средств криптографической защиты информации (СКЗИ) 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 (ЛПБ) для управляемых СКЗИ и МЭ;

– доставку политики безопасности до управляемых СКЗИ и МЭ по защищенному каналу;

– мониторинг состояния управляемых СКЗИ и МЭ;

– удаленное обновление программного обеспечения (ПО) управляемых СКЗИ и МЭ.

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

2.4. ПК обеспечивает контроль и фильтрацию сетевых пакетов в соответствии с заданными правилами, а также защиту передаваемой по каналам связи служебной информации (локальных политик безопасности, команд управления) криптографическими методами.

2.5. В качестве СКЗИ ПК обеспечивает выполнение криптографических функций: шифрования, контроля целостности данных, имитозащиту данных, открытого распределения криптографических ключей, что обеспечивает:

– конфиденциальность передаваемой в корпоративной ИТКС служебной информации (локальных политик безопасности, команд управления), за счет ее шифрования с использованием режима гаммирования (CTR) и зацепления блоков (CBC) на базе протокола IPsec, согласно ГОСТ 28147-89;

– защиту доступа к служебной информации (локальных политик безопасности, команд управления) за счет использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протоколов IKEv2 с использованием алгоритмов ЭП 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 алгоритмов ГОСТ Р 34.10-2012 VKO в 256-битном режиме.

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

3.1. ПК имеет графический интерфейс, который позволяет пользователю ПК наглядно описывать топологию и сетевые объекты, задавать правила фильтрации в удобной пользователю ПК нотации: источник, приемник, параметры, действие, применяемое к пакету, выполнять команды по трансляции ГПБ и доставке политик на агенты безопасности, обновлению агентов безопасности, наглядно отслеживать состояние агентов безопасности и результат выполнения команд

3.2. ПК осуществляет идентификацию и аутентификацию пользователей при доступе к управлению политиками безопасности на основании имени и пароля.

3.3. ПК обеспечивает формирование правил фильтрации трафика для управляемых с помощью ПК агентов безопасности 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.

3.4. ПК должен обеспечивает задания параметров шифрования, контроля целостности и имитозащиты данных, а также задание параметров двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2 таких как: алгоритм ЭП, алгоритм шифрования, алгоритм хеширования, алгоритм генерации ключей Диффи-Хеллмана.

3.5. ПК должен обеспечивает перевод (трансляцию) ГПБ в ЛПБ для управляемых Агентов безопасности и доставку политики безопасности до управляемых агентов безопасности в автоматическом режиме с применением криптографических методов защиты информации.

3.6. ПК обеспечивает задание параметров обновления для каждого из управляемых агентов безопасности и запуск команды на удаленное обновление.

3.7. ПК обеспечивает мониторинг состояния управляемых им Агентов безопасности, отображая состояния и результаты выполнения команд по доставке политики (статус активации политики) и обновления.

3.8. ПК обеспечивает генерацию, просмотр, сортировку и фильтрацию данных аудита.

3.9. В ПК реализован REST дублирующий функции конфигурирования и мониторинга доступные в графическом пользовательском интерфейсе.