

ЗАО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, проезд 4806, д.5, стр.20
Телефон: +7 (499) 720-6928
Факс: +7 (499) 720-6928
Эл.почта: information@s-terra.com
Сайт: <http://www.s-terra.com>



Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.1”

Руководство администратора

Введение

РЛКЕ.00005-01 90 03

28.06.2010

Содержание

Введение	3
Комплекты поставки Программных комплексов	3
Назначение и функции Продукта	6
Требования на аппаратные платформы	8
Архитектура CSP VPN Gate	9
Способы создания политики безопасности	11
Требования по организационным и административным мерам обеспечения безопасности эксплуатации ПАК	12

Введение

Комплекты поставки Программных комплексов

Программный комплекс “Шлюз безопасности CSP VPN Gate. Версия 3.1” (далее – продукт CSP VPN Gate 3.1 или Продукт) предназначен для использования на:

- аппаратных платформах, работающих под управлением ОС Sun Solaris 10 x86
- аппаратных платформах, работающих под управлением ОС Red Hat Enterprise Linux 5
- аппаратных платформах, работающих под управлением ОС CentOS 5
- сетевом модуле Cisco NME-RVPN в исполнении MCM (модуль сетевой модернизированный), устанавливаемом в маршрутизаторы Cisco серий 2800, 3800, 2900, 3900 и работающем под управлением ОС Red Hat Enterprise Linux 5 или CentOS 5. В дальнейшем везде будет использоваться наименование – модуль NME-RVPN (MCM).

Комплекты поставки Программного комплекса “Шлюз безопасности CSP VPN Gate. Версия 3.1” различны в зависимости от того, установлен Программный комплекс на модуле NME-RVPN (MCM) или на аппаратной платформе.

Комплект поставки для модуля NME-RVPN (MCM)

Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1» на модуле NME-RVPN (MCM) поставляется в следующей комплектации:

сетевой модуль NME-RVPN в исполнении MCM с установленной в нем компакт-флеш картой, которая содержит:

- установленную ОС на базе свободно опубликованных исходных текстов Red Hat Enterprise Linux 5 или CentOS 5, в которую входит OpenSSH и Apache Web-Server версии 2.2.3
- подготовленный к инициализации CSP VPN Gate 3.1 со встроенным криптодром СКЗИ "Крипто-КОМ 3.2"
- либо подготовленные к инициализации CSP VPN Gate 3.1 и СКЗИ "КриптоПро CSP 3.6"

в комплект поставки входят 3 диска:

- CSP VPN Gate. Версия 3.1. Build 3.1.10330
- NME-RVPN (MCM) Recovery CD (вспомогательное ПО для восстановления образа, образ компакт-флеш карты (CF), скрипты)
- S-Terra CSP Product Line Documentation (пользовательская документация, Правила пользования (если используется СКЗИ "КриптоПро CSP 3.6"))

в бумажном виде поставляются:

- Копия сертификата соответствия ФСБ России
- Копия сертификата соответствия ФСТЭК России
- Голографический специальный защитный знак ФСТЭК России
- Лицензия на использование программного комплекса CSP VPN Gate версии 3.1
- Лицензия на использование программного продукта КриптоПро CSP Driver версии 3.6 (если используется СКЗИ "КриптоПро CSP 3.6")
- Лицензия на использование программного продукта компании «Сигнал-КОМ» (если используется СКЗИ "Крипто-КОМ 3.2")
- Формуляр. РЛКЕ.00005-01 30 02. Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1», функционирующий на аппаратных платформах в архитектуре Intel x86 под управлением операционных систем Solaris 10, Red Hat Enterprise Linux 5 и на аппаратной платформе Cisco NME-RVPN в исполнении MCM под управлением операционной системы Red Hat Enterprise Linux 5. (ФСТЭК России)
- Формуляр. РЛКЕ.00005-01 30 01. Программный комплекс CSP VPN Gate. Версия 3.1. (ФСБ России).

Комплект поставки для аппаратной платформы

Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1» поставляется в следующей комплектации:

аппаратная платформа, жесткий диск которой содержит:

- установленную операционную систему:
 - ОС Solaris 10 x86, в которую входит SSH и Apache Web-Server версии 1.3.29
 - или ОС на базе свободно опубликованных исходных текстов Red Hat Enterprise Linux 5 или CentOS 5, в которую входит OpenSSH и Apache Web-Server версии 2.2.3.
- подготовленные к инициализации продукты:
 - CSP VPN Gate 3.1 и КриптоПро CSP 3.6
 - или CSP VPN Gate 3.1 со встроенным криптоядром СКЗИ "Крипто-КОМ 3.2"

4 компакт-диска:

- CSP VPN Gate. Версия 3.1. Build 3.1.10330
- CSP VPN Gate Disk Image (образ жесткого диска и Приложение к Инструкции по восстановлению ПАК)
- CSP VPN Gate Recovery CD (вспомогательное ПО для восстановления образа диска и Инструкция по восстановлению ПАК)
- S-Terra CSP Product Line Documentation (пользовательская документация, Правила пользования (если используется СКЗИ "КриптоПро CSP 3.6"))

в печатном виде поставляются:

- Копия сертификата соответствия ФСБ России (если используется СКЗИ "КриптоПро CSP 3.6")
- Копия сертификата соответствия ФСТЭК России
- Голографический специальный защитный знак ФСТЭК России
- Лицензия на использование программного комплекса CSP VPN Gate версии 3.1
- Лицензия на использование программного продукта КриптоПро CSP Driver версии 3.6 (если используется СКЗИ "КриптоПро CSP 3.6")
- Лицензия на использование программного продукта компании «Сигнал-КОМ» (если используется СКЗИ "Крипто-КОМ 3.2")
- Формуляр. РЛКЕ.00005-01 30 02. Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1», функционирующий на аппаратных платформах в архитектуре Intel x86 под управлением операционных систем Solaris 10, Red Hat Enterprise Linux 5 и на аппаратной платформе Cisco NME-RVPN в исполнении MCM под управлением операционной системы Red Hat Enterprise Linux 5. (ФСТЭК России)
- Формуляр. РЛКЕ.00005-01 30 01. Программный комплекс CSP VPN Gate. Версия 3.1. (ФСБ России).

Назначение и функции Продукта

Программный комплекс “Шлюз безопасности CSP VPN Gate. Версия 3.1” обеспечивает создание виртуальных защищенных сетей (VPN), защиту транзитного трафика между различными узлами сети, защиту трафика самого шлюза безопасности, а также пакетную фильтрацию трафика.

Защита трафика шлюзов безопасности осуществляется в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401
- IP Authentication Header (AH) – RFC2402
- IP Encapsulating Security Payload (ESP) – RFC2406
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
- The Internet Key Exchange (IKE) – RFC2409
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

Шлюзы безопасности обеспечивают:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней:
 - на сетевом уровне – по IPv4 адресам и/или полю 'протокол' IP-заголовка
 - на транспортном уровне – по направлению установления TCP – соединений и составу сервисов (сервисных протоколов)
- загрузку политики из внешнего файла
- различные наборы правил обработки трафика на различных интерфейсах
- получение сертификатов открытых ключей по протоколу LDAP
- событийное протоколирование
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию
- регулируемую стойкость защиты трафика
- маскировку топологии защищаемого сегмента сети (туннелирование трафика).

Управление шлюзами безопасности осуществляется:

- централизованно посредством графического интерфейса центра управления Cisco Works VPN/Security Management Solution v.2.3 – CiscoWorks Router Management Center (Router MC)
- централизованно удаленно посредством графического интерфейса Cisco Security Manager версии 3.2
- локально и удаленно по протоколу SSH с помощью интерфейса командной строки. В интерфейсе командной строки в основном используются команды Cisco, что облегчает управление администраторам, имеющим опыт конфигурирования шлюзов безопасности и межсетевых экранов Cisco Systems
- созданием политики безопасности в виде конфигурационного текстового файла и последующей его загрузки на шлюз
- удаленно с помощью Web-based графического интерфейса управления (GUI).

Продукт CSP VPN Gate использует в качестве внешней криптографической библиотеки одно из средств криптографической защиты информации (СКЗИ):

- СКЗИ "КриптоПро CSP 3.6", разработанное компанией "Крипто-Про"
- СКЗИ "Крипто-КОМ 3.2", разработанное компанией "Сигнал-КОМ".

СКЗИ "КриптоПро CSP 3.6" и СКЗИ "Крипто-КОМ 3.2" реализуют российские криптографические алгоритмы:

- ГОСТ 28147-89 – шифрование/расшифрование данных
- ГОСТ Р 34.11-94 – алгоритм хэширования
- ГОСТ Р 34.10-2001– формирование и проверка электронно-цифровой подписи (ЭЦП)
- ГОСТ Р 34.10-2001 – поддержка схемы открытого распределения ключей Диффи-Хеллмана в соответствии с RFC 4357
- генерация случайных чисел.

Требования на аппаратные платформы

Продукт CSP VPN Gate работает под управлением:

- ОС Sun Solaris 10 x86
- ОС Red Hat Enterprise Linux 5
- ОС CentOS 5.

На поставляемой аппаратной платформе ОС настраивается в соответствии с внутренними стандартами компании “С-Терра СиЭсПи” и администратору безопасности **запрещается** изменение среды функционирования, а именно:

- модернизация ОС, включая установку штатных обновлений
- добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент поставки Изделия)
- установка дополнительных приложений
- самостоятельное добавление/удаление аппаратных компонент (в том числе сетевых карт, жестких дисков и т.п.).

Архитектура CSP VPN Gate

Функциональность шлюза безопасности CSP VPN Gate состоит из следующих основных частей:

- VPN daemon (**демон**)
- VPN driver (**драйвер**)
- Cisco-like console (CLI **консоль**)
- Command Line Utilities (**утилиты**)
- Web-based Graphic User Interface (**GUI**).

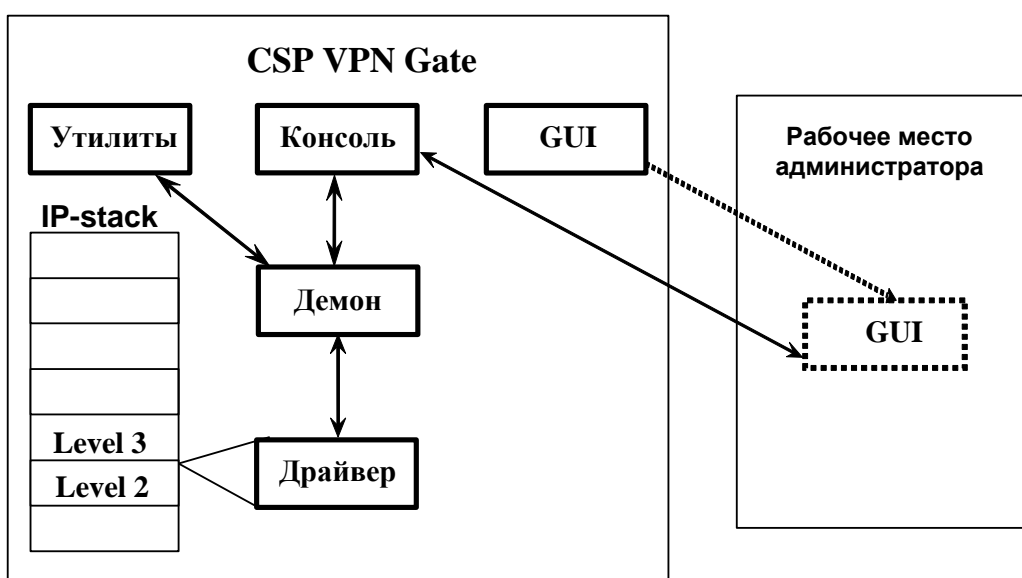


Рисунок 1

Рассмотрим основные части.

Демон (vpnsvc) – основная часть Продукта, которая реализует протокол IKE, обеспечивает работу с базой IPsec SA, взаимодействует с драйвером, загружая в него конфигурационную информацию и обрабатывая его запросы на создание SA. Кроме этого, в демоне выполняется вся работа с сертификатами, событийное протоколирование, сбор статистики и реализована поддержка протоколов SNMP, LDAP, SYSLOG.

Работой демона управляет специальное описание – Local Security Policy (LSP). LSP (или “native configuration”) имеет текстовое представление и может быть загружена в демон пользователем консоли или при помощи утилит. При загрузке новой LSP все существующие SA уничтожаются.

Основная задача **драйвера** – перехват, фильтрация и обработка пакетов. Перехватив пакет, драйвер сравнивает его со списком фильтров и при совпадении параметров пакета (адреса, порты, протокол) с параметрами фильтра либо выполняет обработку пакета, либо пропускает его дальше без обработки, либо уничтожает пакет.

При загрузке LSP параметры фильтров и описание действия, которое необходимо выполнить с пакетом, загружаются демоном в драйвер.

Консоль (CLI) предоставляет пользователю интерфейс в стиле командной строки Cisco IOS. Набор команд консоли является подмножеством команд IOS с некоторыми ограничениями функциональности и небольшими дополнительными возможностями. Как и у IOS, у консоли есть привилегированный и конфигурационный режимы (`configure terminal`). Однако, следует отметить, что (в отличие от IOS) изменения настроек вступают в действие не сразу, а только после выхода из конфигурационного режима. В этот момент Cisco-like конфигурация автоматически конвертируется в native-конфигурацию и загружается в `vpnsvc`. Таким образом, включает в себя:

- интерфейс командной строки для ввода команд конфигурации
- интерпретатор команд, родственных Cisco
- обработчик конфигурации. Формирует и обрабатывает конфигурацию из команд консоли и передает ее конвертору.

CLI консоль, на самом деле, является специальным shell-ом по умолчанию для предопределенного пользователя «`cscons`» и всех пользователей, которые создаются в CLI конфигурации. Остальные пользователи, например «`root`», при входе попадают в ОС.

Утилиты служат для общего управления Продуктом. Они позволяют загружать и просматривать LSP, регистрировать в Продукте сертификаты и ключи, получать различную информацию о текущем состоянии Продукта и др.

Утилиты могут быть вызваны из CLI консоли с использованием специальной команды `run`.

GUI является еще одним средством настройки шлюза безопасности. В состав ОС входит Web-сервер и SSH-сервер, а GUI представляет из себя Java-applet, который может быть загружен по протоколу HTTP администратором и запущен на его рабочем компьютере. После запуска GUI взаимодействует с консолью по протоколу SSH. Внешне GUI выполнен в стиле Cisco SDM с существенным сокращением функциональности. Он позволяет пользователю редактировать Cisco-like policy, представленную в виде набора связанных таблиц. После внесения необходимых изменений они по специальной команде пользователя в виде набора команд конфигурационного режима передаются консоли.

База Продукта – в ней хранятся сертификаты, предопределенные ключи, список интерфейсов, локальные настройки различных модулей, локальная политика безопасности и др.

Примеры взаимодействия описанных компонент

Перед созданием конфигурации с помощью интерфейса командной строки нужно зарегистрировать локальный сертификат в базе Продукта, используя утилиту. Затем запустить консоль и создать в ней конфигурацию, при выходе из конфигурационного режима консоли конфигурация конвертируется, загружается на шлюз безопасности и хранится в базе Продукта. Используя утилиту, конфигурацию можно выгрузить из шлюза безопасности и при этом загрузится политика DDP. Выгруженную конфигурацию можно опять загрузить на шлюз.

Перед созданием конфигурации с помощью графического Web-based интерфейса нужно зарегистрировать локальный сертификат в базе Продукта, используя утилиту. При запуске GUI вызывается Java-апплет, который использует консоль. В ней создается конфигурация, при доставке на шлюз безопасности она конвертируется и загружается, а также хранится в базе Продукта.

Способы создания политики безопасности

Создание политики безопасности для шлюза CSP VPN Gate возможно осуществить следующими способами:

- с помощью команд интерфейса командной строки локально или удаленно с использованием протокола SSH, описанных в документе [«Cisco-like команды»](#) (такую конфигурацию будем называть «cisco-like конфигурацией»). Написанные команды являются родственными Cisco IOS 12.4 (13a)
- создание текстового конфигурационного файла и его последующая загрузка с помощью Специализированных команд на ПАК или модуль NME-RVPN (MCM). Создание такого файла описано в документе [«Создание конфигурационного файла»](#) (такую конфигурацию будем называть «native конфигурацией»)
- создание политики безопасности удаленно с помощью Web-based графического интерфейса управления (GUI), описано в документе [«Web-based интерфейс управления: инструкция по установке и использованию»](#)
- с помощью CiscoWorks Router Management Center (далее по тексту Router MC), которое описано в документе [«Конфигурирование с помощью CiscoWorks»](#).
- удаленное создание политики безопасности с помощью графического интерфейса Cisco Security Manager (CSM), описанного в документе [«Управление CSP VPN Gate с помощью Cisco Security Manager»](#)

Перед созданием политики безопасности шлюза выполните сначала инициализацию программного комплекса CSP VPN Gate 3.1, которая описана в документах [«Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6»](#), [«Инициализация CSP VPN Gate при использовании СКЗИ «Крипто-КОМ 3.2»](#) или [«Руководство по установке и настройке NME-RVPN модуля \(MCM\)»](#).

Требования по организационным и административным мерам обеспечения безопасности эксплуатации ПАК

Общие требования

Для безопасности эксплуатации ПАК и программного обеспечения должны выполняться организационно-технические и административные требования. К ним относятся требования по физическому размещению ПАК, установке программного обеспечения на ПАК, средствам защиты от несанкционированного доступа (НСД) к ОС и управлению комплексом, обеспечению бесперебойного режима работы ПАК.

Требования по размещению ПАК

При размещении ПАК на предприятии помещения должны удовлетворять следующим требованиям физической безопасности:

- обеспечение круглосуточной охраны корпусов предприятия;
- обеспечение контроля внешнего периметра и внутренних помещений (видеонаблюдение);
- обеспечение пропускного режима;
- рядом с окнами помещений не должно быть пожарных лестниц и водосточных труб;
- двери должны быть прочными и оборудованы надежными механическими замками;
- оборудование помещений системой пожарной сигнализации;
- ведение Журнала выдачи ключей от входных дверей в офисы, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника, взявшего или сдавшего ключ дежурному вахтеру по зданию;
- принять меры по исключению несанкционированного доступа в помещения, в которых размещены ПАК с установленным СКЗИ, посторонних лиц, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях, должен быть обеспечен контроль над их действиями и обеспечена невозможность негативных действий с их стороны на ПАК
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им ПАК, конфиденциальной информации, в том числе ключевой информации.

Административные меры безопасности

Безопасная эксплуатация ПАК и обращения с СКЗИ должны регламентироваться следующими документами, которые следует разработать:

- Соглашение о неразглашении сведений, составляющих коммерческую тайну организации, которое сотрудники подписывают при приеме на работу
- Перечень сведений, составляющих коммерческую тайну организации, утвержденный Генеральным директором;

- Инструкция по обращению с сертифицированными ФСБ шифровальными средствами (средствами криптографической защиты информации) на предприятии;
- Журнал учета СКЗИ, тестовых ключей на предприятии;
- Журнал регистрации администраторов безопасности;
- Журнал учета обращения эталонных CD дисков на предприятии.

Обязательно наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с продуктом, другой конфиденциальной информации. Для сейфа должно быть два ключа – основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат – в опечатанном его личной печатью пенале в сейфе Генерального директора.

Запрещается:

- обрабатывать на ПАК, оснащенный СКЗИ, информацию, содержащую государственную тайну
- осуществлять несанкционированное вскрытие ПАК.

Требования по защите ПАК от несанкционированного доступа (НСД)

При организации работ на ПАК должны быть выполнены следующие требования по защите ПАК от НСД:

- администратором ПАК назначается администратор безопасности
- право доступа к ПАК имеет только администратор безопасности
- администратор безопасности должен ознакомиться со всей документацией, прилагаемой к ПАК
- аутентификация администратора безопасности основана на пароле, который должен вводиться им с клавиатуры собственноручно при осуществлении доступа в ОС, не отображаясь на экране монитора в явном виде, идентификация основана на идентификаторе, который вводится с клавиатуры. При первом доступе администратор безопасности должен заменить пароль на отличный от установленного при инсталляции ПАК.
- право доступа к режиму управления ПАК (пользовательскому интерфейсу) имеет только администратор с уровнем привилегий 15. Об уровнях привилегий и их назначении см. Руководство администратора
- имя администратора с уровнем привилегий 15 должно быть уникальным и не превышать 8 символов
- имя администратора с уровнем привилегий 15 должно начинаться с буквы латинского алфавита (строчной или прописной). Далее могут идти буквы латинского алфавита (строчные или прописные), цифры, _ (подчеркивание) и - (дефис)
- настройку ПАК (назначение IP-адресов интерфейсам, создание политики безопасности, регистрацию сертификатов, другие дополнительные настройки) осуществляет только администратор безопасности в соответствии с Руководством администратора
- необходимо организовать систему протоколирования и аудита, и вести регулярный анализ результатов аудита с целью выявления нарушений несанкционированного доступа к ПАК
- администратор безопасности не имеет права сообщать никому пароль доступа к ПАК
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год.

Запрещается:

- оставлять без контроля ПАК после прохождения аутентификации, ввода ключевой информации либо иной конфиденциальной информации
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на монитор, принтер и т.п. иные средства отображения информации
- использовать ключевые носители в режимах, не предусмотренных функционированием ПАК
- записывать на ключевые носители постороннюю информацию.

Защита ПАК и ключевой информации от НСД должна обеспечиваться не только в режиме функционирования, но и при проведении ремонтных и регламентных работ.

Требования по установке ПО на ПАК

ПАК «CSP VPN Gate» поставляется с настроенной операционной системой и инсталлированным ПО. При этом администратору безопасности

запрещается несанкционированное изменение среды функционирования ПАК, а именно:

- модернизация ОС, включая установку штатных обновлений
- добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент поставки ПАК)
- установка дополнительных приложений
- внесение изменений в ПО ПАК
- модификация файлов, содержащих исполняемые коды, при их хранении на жестком диске
- добавление/удаление аппаратных компонент (в том числе сетевых карт, жестких дисков и т.п.).

Нарушение этих ограничений рассматривается как нарушение целостности ПАК и приводит к срыву заявленной функциональности ПАК, и является основанием для отказа в сервисе технического сопровождения и поддержки ПАК;

разрешается:

- при нарушении содержимого жесткого диска ПАК восстановить ПО, используя образ диска и другое дополнительное ПО, предоставляемое компанией «С-Терра СиЭсПи». Перед этим необходимо ознакомиться с Инструкцией по восстановлению ПАК
- выполнить процедуру обновления версии ПО ПАК, используя образ диска с новой версией ПО, предоставляемой компанией «С-Терра СиЭсПи». Перед этим необходимо изучить документ «Сценарий обновления версии», чтобы сохранить и не потерять созданную политику безопасности и все настройки ПАК
- после восстановления ПО жесткого диска или обновления ПО провести контроль целостности установленного ПО в соответствии с документацией.