УТВЕРЖДЕН
МКЕЮ.00630.ИЭ-ЛУ

«Аппаратно-программный комплекс
«VPN/FW «ЗАСТАВА-150», версия 6»

(«АПК «ЗАСТАВА-150», версия 6»)

Правила пользования

МКЕЮ.00630.ИЭ

2021

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
7446				

СОДЕРЖАНИЕ

1 Аннотация

Настоящий документ представляет собой Правила пользования аппаратно-программным средством криптографической защиты информации (СКЗИ) МКЕЮ.00630 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» (далее – АПК «ЗАСТАВА-150», версия 6, АПК).

Инструктивные документы, регламентирующие порядок использования АПК в корпоративных информационных истемах и инофрмационно-телекоммуникационных сетях (ИТКС), а также для Администраторов АПК должны разрабатываться с учетом требований настоящего Документа.

2 НАЗНАЧЕНИЕ АПК. УСЛОВИЯ ЭКСПЛУАТАЦИИ

2.1 АПК «ЗАСТАВА-150», версия 6 предназначен для работы в качестве VPN (СКЗИ), обеспечивающего контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами, а также защиту передаваемой по каналам связи информацию открытого и конфиденциального характера криптографическими методами.

2.2 Реализация криптографических функций шифрования, контроля целостности данных, имитозащиты, аутентификации абонентов, осуществляется в АПК с использованием сертифицированного СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base).

2.3 Эксплуатация АПК, а также входящего в него сертифицированных СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base) и RU.63793390.00009 СКЗИ «ESMART Token ГОСТ», должна проводиться согласно разделу V документа «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005)».

2.4 В целях обеспечения равнопрочной защиты информации конфиденциального характера в корпоративной информационной системе (информационно-телекоммуникационной сети (ИТКС)) рекомендуется использовать программные и аппаратно-программные комплексы, сертифицированные по тому же классу защищенности, что и АПК.

2.5 Для включения в информационную систему (ИТКС), укомплектованную СКЗИ (в том числе и АПК «ЗАСТАВА-150», версия 6), сертифицированными по классу защищенности КС3, иных СКЗИ, сертифицированных по классам защищенности КС1 и/или КС2, необходимо принятие дополнительных технических и/или организационных мер защиты, достаточность которых должно быть подтверждена организацией имеющей лицензию на разработку защищенных с использованием шифровальных (криптографических) средств информационных и/или телекоммуникационных систем.

Включение в информационную систему (ИТКС), укомплектованную АПК, сертифицированными по классу защищенности КС3, иных СКЗИ, сертифицированных по классам защищенности КС1 и/или КС2, без принятия дополнительных технических и/или организационных мер защиты, понижает класс защищенности информационой системы (ИТКС) по минимальному классу защищеенности применяемых СКЗИ КС1 или КС2.

2.6 В качестве СКЗИ АПК обеспечивает выполнение целевых криптографических функций: шифрования, контроля целостности данных, имитозащиты данных, аутентификации абонентов, что обеспечивает:

— конфиденциальность передаваемой в корпоративной 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 электронной подписи (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.

2.7 АПК «ЗАСТАВА-150», версия 6 предназначен для эксплуатации на территории Российской Федерации.

2.8 Средствами АПК НЕ ДОПУСКАЕТСЯ обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

2.9 Эксплуатация АПК без действующих сертификатов ФСБ России на версию СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP» Версия 4.0 (исполнение 2-Base) и СКЗИ RU.63793390.00009-01 «ESMART Token ГОСТ» в варианте исполнения 3 ЗАПРЕЩАЕТСЯ!

3 Состав АПК

3.1 АПК «ЗАСТАВА-150», версия 6 состоит из следующих компонентов:

- аппаратная платформа x86 ТОНК 1800S производства ООО «Группа Компаний ТОНК»;
- операционная система (ОС) собственной сборки на базе Linux, 64-битная версия;
- СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base);
- программное обеспечение (ПО) «ЗАСТАВА-Офис», версия 6;
- СКЗИ ESMART Token ГОСТ, выполненное на базе микросхемы MIK51SC72Dv6 RU.63793390.00009, в составе:
    1) электронный идентификатор, аппаратный модуль (АМ) ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01) который содержит компоненты: микросхема ДВУК.431295.011-001[1], ПО АМ, состоящее из загрузчика и функциональной части[2];
    2) программный компонент «ESMART Firmware Checker» RU.63793390.00018-01, предназначенный для контроля целостности ПО аппаратного модуля и ОС Trust 2.05 микросхемы MIK51SC72Dv6;
    3) программный компонент «ESMART PKCS11» RU.63793390.00001-01 – ПО для ОС, обеспечивающее прикладной программный интерфейс СКЗИ (исполнения 1, 2, 3).

3.2 АПК использует электронные идентификаторы ESMART Token ГОСТ ET1020 следующих типов и предназначенных для:

- внешний – для идентификации и аутентификации Администратора АПК;
- внутренний – как аппаратный датчик случайных чисел (ДСЧ).

3.3 Аппаратная платформа x64 ТОНК 1800S, производства ООО «Группа Компаний ТОНК» (процессор Intel Baytrail J1900 QuadCore) оборудована датчиком контроля вскрытия корпуса и электронным идентификатором ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01), установленным под кожух.

[1] Изделие «Отечественная микросхема MIK51SC72Dv6 с ОС Trust 2.05, предназначенная для использования в качестве средства криптографической защиты информации».

[2] В соответствии со спецификацией ПО АМ присвоены децимальные номера:
RU.63793390.00003-01 12 01, RU.63793390.00003-01 12 02, RU.63793390.00006-01 12 01, RU.63793390.00006-01 12 02, RU.63793390.00007-01 12 01, RU.63793390.00007-01 12 02, RU.63793390.00008-01 12 01, RU.63793390.00008-01 12 02.
При этом индекс 01 соответствует загрузчику ПО АМ, а индекс 02 – функциональной части ПО АМ.

4 Требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации АПК

4.1 Общие требования

4.1.1 Выполнение в процессе эксплуатации АПК «ЗАСТАВА-150», версия 6 на должном уровне всех заявленных функции по защите информации возможно исключительно при соблюдении необходимых организационно-распорядительных и технических меры защиты:

— по физическому размещению АПК;

— по правильной установке и настройке АПК и его составных частей;

— по обеспечению сохранности оборудования, целостности системного и прикладного ПО, физической целостности системного блока АПК.

4.1.2 Безопасность эксплуатации АПК обеспечивается при их размещении в пределах объектов информатизации на технических средствах, для которых выполнены действующие в Российской Федерации требования по защите информации по утечке по техническим каналам, в том числе по каналам связи. При этом, если технические средства аттестованы на соответствие установленным требованиям по защите информации без учета канала связи, то для обеспечения защиты ключевой и цифровой информации конфиденциального характера достаточно, чтобы канал связи, выходящий за пределы контролируемой зоны объекта информатизации был реализован в виде:

— радиоканалов GSM, GPRS, 3G/4G, Wi-Fi, а также других современных каналов мобильной или беспроводной связи, работающих в диапазоне частот несущей свыше 800 МГц в цифровой модуляции штатного информационного сигнала;

— волоконно-оптической линии связи (ВОЛС);

— проводного канала связи с установленной в нем волоконно-оптической развязкой при условии расположения входного медиаконвертера (медь – ВОЛС) рядом с СКЗИ, а выходного медиаконвертера (ВОЛС – медь) на расстоянии не менее одного метра от СКЗИ.

4.2 Требования по размещению

4.2.1 Внутренняя планировка помещений, размещение в них АПК, должны обеспечивать Администраторам АПК сохранность доверенных им конфиденциальных сведений, шифровальных (криптографических) средств и ключевой информации к ним.

4.2.2 Должны быть приняты организационно-технические меры, направленные на исключение несанкционированного доступа (НСД) в помещения, в которых размещены АПК, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

4.2.3 В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность их негативного воздействия на АПК и(или) НСД к защищаемой информации.

4.2.4 Для хранения криптографических ключей, нормативной и эксплуатационной документации помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством предприятия.

4.2.5 В случае планирования размещения АПК в помещениях, где присутствует речевая, акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и/или установлены технические средства и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, АПК должны быть подвергнуты специальной проверке по выявлению устройств, предназначенных для негласного получения информации, а также специальным исследованиям на соответствие требованиям к вспомогательным техническим средствам и системам (ВТСС) по защите от утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) в соответствии с категорией выделенного помещения.

4.2.6 В случае применения АПК в отказоустойчивом варианте (кластер из двух узлов АПК) для обеспечения классов защищенности КС3 и КС2 должны быть приняты дополнительные организационно-технические меры:

- размещение узлов кластера в выделенном и оборудованным внутренними замками шкафу;
- опечатывание пломбами выделенного шкафа;
- запрет размещения в выделенном шкафу другого оборудования;
- соединение прямым подключением узлов кластера коммутационным кабелем;
- обеспечение доступа к содержимому выделенного шкафа только администраторам АПК.

4.2.7 В случае применения АПК в отказоустойчивом варианте в ИТКС с классом защищенности КС1 применение дополнительных организационно-технических мер не требуется.

4.3 Организационно-распорядительные меры обеспечения безопасности информации при использовании АПК

4.3.1 Порядок обращения и эксплуатации АПК должны регламентироваться нормативными документами предприятия инструктивного уровня, разрабатываемыми согласно требованиям раздела V документа «Положение о разработке, производстве, реализации и

эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005)»:

- Инструкция по обращению с сертифицированными ФСБ России шифровальными средствами (СКЗИ) на предприятии;
- Инструкция по порядку доступа в помещения, предназначенные для размещения сертифицированных ФСБ России шифровальных средств (СКЗИ);
- Журнал учета сертифицированных ФСБ России шифровальных средств (СКЗИ) и носителей ключевой информации;
- Журнал регистрации Администраторов АПК, на которых установлены сертифицированные ФСБ России шифровальные средства (СКЗИ).

4.4 Требования по обеспечению защиты АПК от НСД

4.4.1 Защита АПК, носителей ключевой информации, содержащих ключевую информацию, должна осуществляться как в процессе функционирования данных средств, так и при проведении регламентных и ремонтных работ.

Запрещается предоставление пользователям и(или) обслуживающему персоналу АПК привилегий Администратора АПК!

4.4.2 Прежде, чем приступить к работе, Администратор АПК должен ознакомиться с технической документацией на АПК в полном объеме, согласно документу МКЕЮ.00630.ФО «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Формуляр и документам, используемым в корпоративной вычислительной системе.

4.4.3 Для осуществления административных функций Администратору АПК должен быть предоставлен электронный идентификатор ESMART Token ГОСТ со специально подготовленной ключевой информацией для входа в АПК с правами Администратора.

4.4.4 Настройка, конфигурирование и эксплуатация компонентов АПК и его компонентов должны осуществляться в соответствии с требованиями настоящих Правил пользования, а также в соответсвии с документацией на составные части комплекса, указанные в документе МКЕЮ.00630.ФО «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Формуляр.

4.4.5 Настройка и эксплуатация СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP» версия 4.0 (исполнение 2-Base) должны осуществляться в соответствии с требованиями технической документацией на указанное средство.

4.4.6 Настройка и конфигурирование АПК должны осуществляться Администратором АПК, который должен руководствоваться технической документацией на АПК.

4.4.7 Для дистанционной настройки и конфигурирования АПК с использованием

протокола SSH должны быть предприняты меры, обеспечивающие защиту информации, циркулирующей между автоматизированным рабочим местом (АРМ) администратора АПК и АПК.

Внутренняя линия связи между АПК «ЗАСТАВА-150», версия 6 и удаленным АРМ администратора должна находиться в пределах контролируемой зоны объекта информатизации, на котором указанные средства вычислительной техники размещаются. Способ прокладки линии связи должен обеспечивать возможность ее визуального контроля и осмотра в целях защиты от несанкционированных подключений.

В случае невозможности обеспечения защиты указанной линии связи организационно-техническими мерами, информация, циркулирующая между серверной частью ПК и консолью управления, должна защищаться криптографическими методами применением программных и/или аппаратно-программных СКЗИ класса защиты не ниже КС3, производимых АО «ЭЛВИС-ПЛЮС».

4.4.8 Для обеспечения защиты от угрозы подмены времени на внутренних часах АПК при использовании протокола NTP, настройки даты и времени должны быть произведены локально или синхронизация внутренних часов АПК по протоколу NTP должна быть осуществляться только с использованием криптографическиой защиты линии связи между АПК «ЗАСТАВА-150» и NTP-сервером, применением программных и/или аппаратно-программных СКЗИ класса защиты не ниже КС3, производимых АО «ЭЛВИС-ПЛЮС».

4.4.9 Организация и осуществление мониторинга, протоколирования, аудита и анализа системных событий в компонентах АПК «ЗАСТАВА-150», версия 6 должны осуществляться в соответствии с требованиями и рекомендациями технической документации, перечисленной в п. 4.4.4.

4.4.10 Должна быть исключена возможность включения в ПО АПК «ЗАСТАВА-150» утилит, позволяющих выполнять перепрограммирование микросхем с ПО BIOS.

4.4.11 Должно быть проведено опечатывание системного блока АПК, позволяющее визуально контролировать вскрытие и исключающее возможность бесконтрольного изменения аппаратной части АПК.

4.4.12 Для эксплуатации АПК должна быть проведена установка следующих параметров BIOS Setup (Version 2.17.1246):

— в разделе «Security» установить пароль администратора с помощью пункта «Administrator Password». Пароль должен состоять из случайного набора не менее 8 буквенно-цифровых символов В составе пароля нельзя использовать: повторяющиеся комбинации; повторяющиеся символы, а также символы, расположенные на клавиатуре в закономерном порядке; данные, связанные с личностью пользователя (дата рождения, имя и т.д.). Сведения о

пароле должны быть известны только группе администраторов;

— в разделе «Advanced \\ Network Bypass Configuration» параметр Network bypass BIOS s установить в состояние «Disabled»;

— в разделе «Advanced \\ LAN Configuration» параметр LAN PXE Boot установить в состояние «Disabled»;

— в разделе «Advanced \\ CPU Configuration» параметр Intel Virtualization Technology установить в состояние «Disabled»;

— в разделе «Advanced \\ PPM Configuration» параметр EIST установить в состояние «Disabled»;

— в разделе «Advanced \\ PPM Configuration» параметр CPU C state Report установить в состояние «Disabled»;

— в разделе «Boot \\ Boot Option Properties» параметр Boot Option # 1 установить в состояние «(штатный) загрузочный диск»;

— в разделе «Boot \\ Boot Option Properties» параметры Boot Option # 2 установить в состояние «Disabled»;

— в разделе «Boot \\ USB Device BBS Priorieties» параметр Boot Option # 1 установить в состояние «(штатный) загрузочный диск»;

— в разделе «Advanced \\ USB Configuration» параметр USB Configuration XHCI Mode установить в состояние «Disabled».

4.4.13 В случае выхода из строя батареи питания CMOS на системной плате АПК должна быть проведена замена батареи, повторная установка вышеперечисленных параметров утилиты BIOS Setup и смена пароля на вход в BIOS Setup. Периодичность смены батареи – один раз в 5 (Пять) лет. Замена батареи питания CMOS в гарантийный срок производится на предприятии-поставщике (изготовителе).

4.4.14 Для выбора и смены PIN-кодов электронных идентификаторов для входа в АПК Администратора АПК должна быть разработана политика назначения и смены паролей в соответствии со следующими правилами:

— длина PIN-кодов электронных идентификаторов Администратора АПК должна быть не менее 7 символов;

— в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т. п.);

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т. д.);

— при смене пароля новое значение должно отличаться от предыдущего не менее,

чем на 4 (Четыре) символа;

— периодичность смены пароля должна определяться принятой политикой безопасности, но не должна превышать 6 (Шесть) месяцев.

4.4.15 Администратор АПК обязан хранить пароль доступа к электронному идентификаторору в тайне и не имеет права сообщать указанные пароли никому.

4.4.16 При эксплуатации АПК КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ:

— **оставлять АПК без контроля после прохождения аутентификации, ввода ключевой информации, либо иной конфиденциальной информации;**

— **осуществлять несанкционированное вскрытие кожухов АПК;**

— **осуществлять несанкционированное Администратором АПК копирование содержимого носителей ключевой информации;**

— **разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;**

— **использовать носители ключевой информации в режимах, не предусмотренных функционированием АПК;**

— **записывать на носители ключевой информации постороннюю информацию;**

— **передавать по каналам связи, в том числе защищенным с использованием СКЗИ (включая АПК), закрытые криптографические ключи.**

4.4.17 Эксплуатации АПК без перезагрузки в течение срока, превышающего 1 (Одни) сутки, не допускается.

4.5 Требования к размещению и настройке АПК

4.5.1 В процессе эксплуатации АПК Администратором АПК должен быть настроен механизм автоматического контроля целостности программных модулей путем запуска по расписанию утилиты icv_checker с файлом шаблона контроля целостности ПО «ЗАСТАВА-Офис», версия 6. Описание настройки механизма автоматического контроля целостности программных модулей ПО «ЗАСТАВА-Офис», версия 6 приведено в подразделе 5.11 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора.

4.5.2 В процессе эксплуатации АПК Администратор АПК не реже одного раза в месяц должен осуществлять переодический контроль целостности программных модулей путем запуска утилиты icv_checker с файлом шаблоном контроля целостности для сверки с эталонными значениями указанных контрольных сумм, поставляемых с документацией на АПК (см. МКЕЮ.00630.Д1 «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия

6»). Электронное приложение к формуляру).

4.5.3 В процессе эксплуатации АПК Администратор АПК не реже одного раза в месяц должен осуществлять проверку целостности программной и информационной части АПК (образа ОС) запуском процедуры из меню загрузчика с использованием утилиты icv_checker, входящей в его состав и предназначенной для периодического тестирования работоспособности. Эталонные контрольные суммы образа ОС АПК указаны в документе МКЕЮ.00630.ФО «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Формуляр.

4.5.4 Описание использования меню загрузчика приведено в документе МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора.

4.5.5 В процессе эксплуатации АПК запрещается несанкционированное Администратором АПК изменение среды функционирования АПК, а именно:

- модернизация ОС;
- внесение изменений в ПО АПК;
- модификация файлов, содержащих исполняемые коды АПК, при их хранении на жестком диске;
- добавление и(или) удаление аппаратных компонентов (в том числе сетевых карт, жестких дисков и т.п.) АПК.

Нарушение перечисленных ограничений рассматривается как нарушение целостности АПК, что приводит к срыву заявленной функциональности по защите информации и является основанием для отказа в сервисе технического сопровождения и поддержки АПК.

4.5.6 Инициализация ДСЧ СКЗИ «КриптоПро CSP», встроенного в АПК, осуществляется с внутреннего электронного идентификатора ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01) из состава АПК.

4.5.7 В целях защиты конфиденциальной информации от утечки по техническим каналам, в том числе по каналам связи от объектов информатизации и АПК, ввод в действие и эксплуатация указанных объектов и АПК должна осуществляться в соответствии с действующими в Российской Федерации требованиями по защите информации от утечки по техническим каналам, в том числе каналу связи (например, СТР-К).

4.5.8 Необходимость и достаточность принятых мер должна оцениваться порядком, предусмотренным упомянутыми руководящими документами с учетом целевых установок предполагаемого нарушителя и угроз безопасности информации.

4.6 Требования по криптографической защите

4.6.1 При эксплуатации АПК должны соблюдаться требования к криптографической защите, изложенные в технической документации к СКЗИ ЖТЯИ.00088 «КриптоПро CSP» 4.0 R2 2-Base и электронному идентификатору ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01).

4.7 Требования к обращению с ключевыми документами

4.7.1 В качестве ключевого носителя используется раздел HDD АПК согласно ЖТЯИ.00088-01 30 01 «КриптоПро CSP». Формуляр (основной вариант) или электронный идентификатор ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01) (дополнительный вариант).

Использование в АПК других носителей ключевой информации ЗАПРЕЩАЕТСЯ!

4.7.2 Требования по обращению с криптографическими ключами АПК (включая цифровые сертификаты ключей проверки ЭП) регламентируются настоящими правилами и технической документацией на электронный идентификатор ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01).

4.7.3 Ключевая информация, используемая АПК «ЗАСТАВА-150», версия 6, является конфиденциальной.

Использование открытых и закрытых ключей, срок действия которых закончился, ЗАПРЕЩЕНО!

4.7.4 Криптографические ключи, срок действия которых закончился, или скомпрометированные ключи подлежат обязательному уничтожению (стиранию) с ключевого носителя. Для удаления ключей Администратор АПК должен использовать утилиту vpnconfig (см. п. 3.2.2.4.4 документа МКЕЮ.00630.ИЗ «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

4.7.5 Формирование открытых и закрытых ключей и соответствующего им цифрового сертификата формата X.509 для АПК и его компонентов может выполняться исключительно:

- с использованием функционала программно-аппаратных комплексов (ПАК) удостоверяющих центров, сертифицированных ФСБ России по классу защиты не ниже класса КС3;
- на рабочих местах пользователей, с использованием функционала СКЗИ «КриптоПро CSP» версии 4.0 или СКЗИ ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01).

Для формирования открытых и закрытых ключей и соответствующего им цифрового

сертификата формата X.509 Администратор АПК должен использовать утилиту vpnconfig (см. п.3.2.2.4.2 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

4.7.6 Срок действия открытых и закрытых ключей используемых в АПК:

— 1 (Один) год 3 (Три) месяца для ключевого носителя – раздел HDD АПК согласно ЖТЯИ.00088-01 30 01 «КриптоПро CSP». Формуляр;

— 3 (Три) года для ключевого носителя – электронный идентификатор ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01).

4.7.7 При формировании открытых и закрытых ключей, соответсвующего им цифрового сертификата формата X.509 для АПК и его компонентов, а также в процессе эксплуатации АПК ЗАПРЕЩАЕТСЯ использование в АПК открытых и закрытых ключей и соответствующих им цифровых сертификатов формата X.509, сформированных способами, отличными от описанных в п. 4.7.5!

4.7.8 Аутентификация Администратора АПК при доступе к ключевой информации, содержащейся на СКЗИ ESMART Token ГОСТ, осуществляется на основе ввода паролей (PIN-кода).

4.7.9 Срок действия PIN-кода до смены не должен превышать 6 месяцев. Необходимость и периодичность смены PIN-кода, а также требования к сложности PIN-кода, должны быть определены на предприятии политикой назначения и смены паролей.

Администратор АПК обязан хранить пароль (PIN-код) доступа своему носителю ключевой информации в тайне и не имеет права сообщать указанный пароль никому.

Ответственность за несоблюдение требований по хранению PIN-кода доступа к административному ключевому носителю лежит на Администраторе АПК.

4.7.10 АПК осуществляет ограничение попыток входа на базе функционала USB-токена. После того, как предварительно заданное число раз (10) был введен неверный PIN-код, устройство блокируется. Получить доступ к хранящимся на заблокированном устройстве закрытым объектам (ключам) невозможно. Разблокировать устройство может Администратор АПК, которому известен PIN-код Администратора (SO-PIN). Если превышено количество допустимых попыток неверного ввода PIN-кода Администратора (SO-PIN), носитель ключевой информации не подлежит дальнейшему использованию и должен быть утилизирован посредством процедуры удаления единичного экземпляра ключевого документа путем удаления соответствующего объекта в энергонезависимой памяти аппаратного модул в соответствии с эксплуатационной документацией (ЭД) на СКЗИ «ESMART Token ГОСТ», либо процедурой полного очищения энергонезависимой памяти аппаратного модуля в соответствии

с ЭД на СКЗИ «ESMART Token ГОСТ». Факт утилизации USB-токена как носителя криптоключей должен фиксироваться в журнале поэкземплярного учёта СКЗИ.

4.7.11 Доставка криптографических ключей и сертификатов открытых ключей должна осуществляться Администратором АПК на носителе ключевой информации или иным доверенным способом, соответствующим требованиям технической документации на эти СКЗИ.

4.7.12 Принятая в корпоративной ИТКС политика безопасности должна предусматривать возможность получения АПК, эксплуатируемыми в указанной ИТКС, актуальных списков аннулированных (отозванных) сертификатов CRL формата CRLv2, выпущенных с использованием ПАК Удостоверяющего Центра и подписанных с использованием СКЗИ, класс сертификации которых не должен быть ниже класса КС3.

Примечание - Несвоевременное получение АПК актуального списка аннулированных сертификатов CRL может привести к невозможности установления защищенных соединений с абонентами корпоративной вычислительной сети, использующими цифровые сертификаты, выпущенные Удостоверяющим Центром, формирующим данный CRL.

4.7.13 Срок действия закрытых ключей, используемых в АПК, принимается равным сроку действия открытого ключа, указанному в соответствующем сертификате открытого ключа (поле Validity). АПК не допускает использование закрытого и открытого ключа до начала и после окончания срока действия. Для отслеживания срока действия ключа Администратор АПК должен использовать утилиту vpnconfig (см. п. 3.2.2.4.1 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

4.8 Действия при компрометации ключей

4.8.1 К случаям явной компрометации закрытого ключа Администратора АПК относятся:

- потеря ключевого носителя;
- потеря ключевого носителя с последующим обнаружением;
- увольнение (смена) Администратора АПК;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.

Администратор АПК должен провести процедуру возврата к эталонной версии программной части АПК и провести повторную настройку АПК с заменой ключей для организации защищённых соединений.

Пароль доступа к ОС после восстановления системы должен быть задан отличным от пароля, заданного на момент явной компрометации ключей. Для смены пароля надо провести

процудуру (см. подраздел 5.5 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

При потере ключевого носителя Администратор АПК должен заказать получение нового ключевого носителя у предприятия-поставщика (изготовителя). Потерянный и впоследствии обнаруженный ключевой носитель может быть передан предприятию-поставщику (изготовителю) для замены ключевой информации.

4.8.2 В случае неявной компрометации закрытого ключа Администратора АПК, к которым относятся случаи:

— возникновение подозрений на утечку информации или ее искажение в ИТКС;

— нарушение печати на сейфе с ключевыми носителями;

— случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Администратор АПК должен провести внеочередную процедуру контроля целостности программных модулей АПК и в случае нарушения целостности осуществить возврат к эталонной версии программной части АПК и провести повторную настройку АПК с заменой ключей для организации защищённых соединений.

При выходе из строя ключевого носителя Администратор АПК должен заказать получение нового ключевого носителя у предприятия-поставщика (изготовителя). Вышедший из строя ключевой носитель может быть передан предприятию-поставщику (изготовителю) для уничтожения или уничтожен самостоятельно, путём физического уничтожения.

4.8.3 В случае компрометации ключей для организации защищённых соединений необходимо выпустить новую ключевую информацию (см. подраздел 5.6 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора.

4.8.4 По факту компрометации ключей должно быть проведено служебное расследование.

4.8.5 Скомпрометированные ключи выводятся из действия. Выведенные из действия скомпрометированные ключевые носители уничтожаются.

4.8.6 Скомпрометированные ключи подлежат замене с отзывом соответствующих им цифровых сертификатов путем включения сведений об отзваемых цифровых сертификатах в список аннулированных (отозванных) сертификатов CRL Удостоверяющего Центра.

4.9 Требования к политике безопасности АПК «ЗАСТАВА-150», версия 6

4.9.1 Для эксплуатации АПК должен быть настроен Администратором АПК в соответствии требованиями технической документации, перечисленной в п. 4.4.4 и п. 4.4.5.

4.9.2 Для шифрования, контроля целостности, имитозащиты и взаимной аутентификации должны использоваться исключительно функции, реализующие криптографические алгоритмы, основанные на российских стандартах ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, реализованные в СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP» версия 4.0 (исполнение 2-Base). Поэтому при настройке, конфигурировании и создании политики безопасности Администратор АПК должен руководствоваться следующими требованиями:

- атрибуту ***cipher*** в структуре ***proto_ike*** должно быть присвоено значение «***G2814789CPRO1-CBC***» или «***G2814789CPRO1-CTR***»;
- атрибуту ***hash*** в структуре ***proto_ike*** должно быть присвоено значение «***GR34112012_256***»;
- атрибуту ***group*** в структуре ***proto_ike*** должно быть присвоено значение «***GR34102012_256***»;
- атрибуту ***expiry_time*** в структуре ***proto_ike*** должно быть присвоено цпфровое значение в диапазоне от ***180*** до ***28800***;
- атрибуту ***cipher*** в структуре ***proto_esp*** должно быть присвоено одно из следующих значений: «***G2814789CPRO1-CBC»***, или «***G2814789CPROD-CBC***», или «***G2814789CPRO1-CTR***», или «***G2814789CPROD-CTR***»;
- атрибут ***integrity*** в структуре ***proto_esp*** должен всегда присутствовать и ему должно быть присвоено одно из следующих значений: «***GR34112012_256-H128-HMAC***» или «***G2814789CPRO1-IMIT***»;
- атрибут ***integrity*** в структуре ***proto_esp*** со значением «***G2814789CPRO1-IMIT***» должен использоваться только в режиме туннелирования;
- атрибуту **expiry_time** в структуре ***proto_esp*** должно быть присвоено цифровое значение в диапазоне от ***180*** до ***28800***.

Примечания. 1) При установке значения ***0*** атрибуту ***expiry_time*** в структуре ***proto_ike***, атрибуту ***expiry_traffic*** должно быть присвоено цифровое значение в диапазоне от ***1*** до ***4096***.

2) При установке значения ***0*** атрибуту ***expiry_time*** в структуре ***proto_esp***, атрибуту ***expiry_traffic*** должно быть присвоено цифровое значение в диапазоне от ***1*** до ***4096***.

4.9.3 На объектах информатизации корпоративной ИТКС, где эксплуатируются

АПК, политикой безопасности которых допускается установление соединений, отличных от криптографически защищенных в соответствии с настоящими Правилами пользования, должны быть приняты предусмотренные руководящими документами ФСТЭК России организационно-технические меры защиты, исключающие возможность утечки циркулирующей на них информации конфиденциального характера с защищаемого объекта. При этом достаточность принятых мер должна оцениваться порядком, предусмотренным упомянутыми руководящими документами ФСТЭК России.

4.9.4 При обнаружении в процессе эксплуатации защищенной корпоративной ИТКС пользователей, локальная политика безопасности (ЛПБ) которых не соответствует действующей в корпоративной информационно-телекоммуникационной глобальной политике безопасности (ГПБ), Администратор АПК сети должен принять меры к незамедлительному принудительному восстановлению ЛПБ у указанных пользователей.

4.9.5 До начала эксплуатации АПК Администратором АПК должен быть сменен пароль на BIOS (см. подраздел 5.3 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора), PIN-код административного ключевого носителя (см. подраздел 5.4. документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора), пароль пользователя ОС (см. подраздел 5.5 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

4.9.6 До начала эксплуатации АПК Администратором АПК должен быть отключен режим IKEv1 в настройках ПО «ЗАСТАВА-Офис», версия 6 (см. п. 3.2.2.8 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

4.9.7 Запрещается удалять файлы-журналы работы СКЗИ без предварительного перемещения их на архивные носители. Архивные носители должны быть доступны только Администратору АПК.

4.10 Требования к процедуре обновления

4.10.1 Процедура установки сертифицированных обновлений возможна только в автоматическом режиме.

4.10.2 Для обновления АПК «ЗАСТАВА-150», версия 6 организатор корпоративной ИТКС должен самостоятельно получить у Изготовителя (Поставщика) согласно договору на поставку и/или техническую поддержку образ обновления на CD/DVD-диске или на USB-носителе для обновляемого ПО и прилагаемую к нему техническую документацию (новый

формуляр или предписание на внесение изменений), содержащую контрольные суммы этого дистрибутива в соответствии с ГОСТ Р 34.11-2012.

4.10.3 Для установки нового сертифицированного обновления АПК в автоматизированном режиме может быть использован любой http-сервер, размещение и эксплуатация которого осуществляется в соответствии с требованиями руководящих документов ФСТЭК России по технической защите конфиденциальной информации[3].

Установка нового сертифицированного обновления АПК должна производиться только с использованием дистрибутивов на CD/DVD-диске или USB-носителе, доставленных (полученных) по доверенному каналу.

4.10.4 Установка нового сертифицированного обновления в автоматическом режиме на АПК, в том случае, если канал связи выходит за пределы контролируемой зоны объекта информатизации, в которой размещается http-сервер обновления, должна осуществляться с использованием защищенного сертифицированным СКЗИ канала связи, обеспечивающего доверенную аутентифицированную доставку до потребителей и установку обновленного дистрибутива.

Для организации такого канала допускается использование СКЗИ, производимые АО «ЭЛВИС-ПЛЮС».

Описание процедуры автоматизированного обновления описаны в документе МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW ЗАСТАВА-Управление», версия 6 КС3» («VPN/FW ЗАСТАВА-Управление», версия 6 КС3») (исполнение ZM-WS64-VO-03). Руководство системного программиста.

Контрольные суммы дистрибутива обновления АПК, указанные в файле update.ini, должны совпадать с контрольными суммами в технической документации (новом формуляре или предписании на внесение изменений), сопровождающей данное обновление.

4.10.5 По завершении процедуры обновления Администратор АПК должен обеспечить изменение формуляра на АПК, путем его корректировки согласно требованиям предписания на внесение изменений или замены на новый.

---

[3] «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282;

«Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным Приказом ФСТЭК России от 11.02.2013 г. № 17;

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным Приказом ФСТЭК России от 18.02.2013 г. № 21.

4.11 Перечень событий, при возникновении которых эксплуатация АПК запрещена

4.11.1 Эксплуатация АПК запрещена при наступлении следующих событий:

— обнаружение несанкционированного вскрытия корпуса (срабатывание датчика вскрытия корпуса);

— нарушение целостности пломбы выделенного шкафа для размещения узлов кластера АПК;

— нарушение целостности образа ПО АПК;

— сбой ПО АПК;

— сбой в ходе процедуры POST BIOS;

— компрометация ключей.

4.11.2 При наступлении любого из перечисленных в п. 4.11.1 событий Администратор АПК должен: приостановить эксплуатацию АПК, выявить причины инцидента, а также устранить негативные последствия посредством принятия мер в соответсвии с разделом «Нештатные ситуации» документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора.

4.11.3 В случае невозможности устранения негативных последствий инцидентов, перечисленных в п. 4.11.1, Администратор АПК должен вывести из эксплуатации АПК «ЗАСТАВА-150» и передать АПК в ремонт или утилизировать.

4.12 Нештатные ситуации при эксплуатации АПК

4.12.1 В таблице (см. Таблица 1) приведен основной перечень нештатных ситуаций и соответствующие действия Администратора АПК при их возникновении.

Таблица 1 - Действия администратора АПК в нештатных ситуациях

№п/п	Нештатная ситуация	Действия Администратора АПК
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в помещении, где размещается АПК	Администратор АПК: – останавливает АПК; – упаковывает ключевые носители в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы АПК; – оповещает по телефонным каналам общего пользования всех пользователей и администраторов программных и аппаратно-программных СКЗИ и межсетевых экранов ИТКС о приостановке работы АПК; – в случае наступления события, повлекшего за собой долговременный выход из строя АПК, Администратор АПК уничтожает всю ключевую информацию с носителей, находящихся в контейнере.

№п/п	Нештатная ситуация	Действия Администратора АПК
2.	Некорректная работа АПК после обновления ОС	В случае некорректной работы АПК после очередного обновления следует выполнить возврат к эталонной версии программной составляющей. Эталонной версией является программная составляющая, установленная при поставке АПК. Образ эталонной версии программной составляющей хранится на жестком диске АПК и может быть развернут при необходимости. Инструкция по возврату к эталоной версии приведена в подразделе 6.1 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора.
3.	Обнаружение несанкционированного вскрытия корпуса	В случае обнаружения вскрытия корпуса (срабатывание датчика вскрытия или в результате нарушения целостности наклейки при визуальном осмотре) необходимо: – отключить АПК от каналов передачи данных; – выполнить перезагрузку и сверить контрольные суммы с зафиксированными в формуляре (см. подраздел 5.2 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора); – назначить ответственного за расследование инцидента. Всю ключевую информацию считать скомпрометированной; – если в результате расследования выяснилось, что действия нарушителя не несли злого умысла, то необходимо выполнить возврат в эталон (см. подраздел 6.1 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора) и выпустить новую ключевую информацию для VPN (см. подраздел 5.6 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора); – в случае невозможности выполнить возврат к эталонной версии, необходимо отправить АПК предприятию-поставщику (изготовителю) для ремонта.

№п/п	Нештатная ситуация	Действия Администратора АПК
4.	Нарушение целостности образа	В случае нарушения целостности образа необходимо: – назначить ответственного за расследование инцидента. Всю ключевую информацию считать скомпрометированной; – необходимо выполнить возврат к эталонной версии (см. подраздел 6.1 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора) и выпустить новую ключевую информацию для VPN (см. подраздел 5.6 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора); – в случае невозможности выполнить возврат к эталонной версии, необходимо отправить АПК предприятию-поставщику (изготовителю) для ремонта.
5.	Компрометация ключей	В случае компрометации ключей необходимо действовать в соответсвии с подразделом 4.8.
6.	Истечение срока действия закрытых криптографических ключей	Производится замена ключей. Сертификаты, сроки действия которых истекли, должны быть удалены. Процедура удаления сертификатов описана в п. 3.2.2.4.4 документа МКЕЮ.00630.И3 ««Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).
7.	Истечение срока действия закрытых криптографических ключей	Производится замена ключей. Сертификаты, сроки действия которых истекли, должны быть удалены. Процедура удаления сертификатов описана в п. 3.2.2.4.4 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).
8.	Не проходит локальный вход Администратора АПК при предъявлении корректных учётных данных и паролей к АПК и ключевому носителю	Администратор безопасности АПК: – останавливает АПК; – проверяет целостности наклейки; – если целостность наклейки не нарушена, включает АПК и входит в BIOS для контроля системных часов; – если системные часы сброшены на дату по-умолчанию, требуется установить корректную дату и время. Перепроверить настройки, описанные в п. 4.4.12, и при необходимости установить в корректные значения. Сохранить настройки BIOS; – пройти повторно аутентификацию. В случае отрицательного результата произвести замену батареи питания CMOS согласно п. 4.4.13.

5 Порядок ремонта и утилизации АПК

5.1.1 Ремонт АПК «ЗАСТАВА-150», верия 6 должен осуществляться Изготовителем (Поставщиком) СКЗИ или организацией, осуществляющей требуемую лицензируемую деятельность в отношении шифровальных (криптографических) средств и которой Изготовитель (Поставщик) делегировал право осуществлять ремонт АПК.

5.1.2 Перед передачей в ремонт или утилизацией АПК все закрытые ключи и соответствующие им открытые ключи подлежат обязательному уничтожению (стиранию) с внутренних ключевых носителей. Для удаления ключей Администратор АПК должен использовать утилиту vpnconfig (см. п. 3.2.2.4.4 документа МКЕЮ.00630.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-150», версия 6» («АПК «ЗАСТАВА-150», версия 6»). Руководство администратора).

5.1.3 Перед передачей в ремонт или утилизацией АПК должен быть выполнен отзыв цифровых сертификатов x.509, соответствующих удалённым закрытым и открытым ключам.

5.1.4 При передаче в ремонт и в случае невозможности отзыва сертификатов x.509, хранящихся на внутреннем твердотельном накопителе, потребитель должен согласовать с производителем СКЗИ или организацией, осуществляющей ремонт АПК, дополнительные меры по обеспечению невозможности доступа нарушителей во время ремонта АПК к внутреннему твердотельному накопителю.

5.1.5 Утилизация АПК должа производиться с физическим уничтожением накопителя информации и электронного идентификатора ESMART Token ГОСТ ET1020 в виде USB-токена (RU.63793390.00003-01), установленного под кожух системного блока.

5.1.6 Допускается повторное использование аппаратных компонентов АПК в новых сертифицированных модификациях АПК «ЗАСТАВА», производимых АО «ЭЛВИС-ПЛЮС», путём полной замены программной и информационной части АПК, и при условии что эксплуатация вновь созданного СКЗИ на базе аппаратных компонентов АПК будет осуществляться той же организацией – владельцем АПК. К аппаратным компонентам АПК относятся:

— аппаратная платформа ТОНК 1800S;
— электронный идентификатор ESMART Token ГОСТ, аппаратно-реализующий российские стандарты ЭП, шифрования, хэширования.

Перечень принятых терминов и сокращений

CD/DVD – Compact Disk / Digital Versatile Disc
Компакт диск / цифровой многоцелевой диск

BIOS – Basic input/output system
Базовая система ввода-вывода

CBC – Cipher Block Chaining
Один из режимов шифрования для симметричного блочного шифра с использованием механизма обратной связи

CMOS – Complementary metal oxide semiconductor
Энергонезависимая память BIOS

CRL – Certificate Revocation List
Список отозванных сертификатов

CTR – Counter mode
Один из режимов шифрования для симметричного шифра, при котором зашифрованный блок текста представляет собой побитное сложение блока открытого текста с зашифрованным значением счетчика

IKE – Internet Key Exchange
Протокол обмена ключевой информацией; используется совместно с протоколами IPsec для организации первичного защищенного канала ISAKMP SA

NTP – Network Time Protocol
Протокол сетевого времени

PIN – Personal Identification Number
Персональный идентификационный код

VPN – Virtual Private Network
Виртуальная частная сеть

АПК – Аппаратно-программный комплекс

АРМ – Автоматизированное рабочее место

ВОЛС Волоконно-оптические линии связи

ВТСС – Вспомогательные технические средства и системы

ГПБ – Глобальная политика безопасности

ДСЧ – Датчик случайных чисел

ИТКС – Информационно-телекоммуникационная сеть

ЛПБ – Локальная политика безопасности

НСД – Несанкционированный доступ

ОС – Операционная система

ПАК – Программно-аппаратный комплекс

ПО – Программное обеспечение

ПЭМИН – Побочные электромагнитные излучения и наводки

СКЗИ – Средство криптографической защиты информации

ФСБ России – Федеральная служба безопасности

ФСТЭК России – Федеральная служба по таможенному и экспортному контролю

ЭП – Электронная подпись

Сведения о проверках и внесенных изменениях

Основание (входящий номер сопроводительного документа и дата)	Дата проведения проверки (изменения)	Содержание проверки (изменения)	Должность, фамилия и подпись ответственного лица за проведение проверки (изменения)	Подпись администратора службы безопасности информации

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	изъятых					