УТВЕРЖДЕН
МКЕЮ.00629.ИЭ-ЛУ

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

(«АПК «ЗАСТАВА-ТК», версия 6»)

Правила пользования

МКЕЮ.00629.ИЭ

2021

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
7430				

СОДЕРЖАНИЕ

1 Аннотация

Настоящий документ представляет собой Правила пользования аппаратно-программным средством криптографической защиты информации (СКЗИ) МКЕЮ.00629 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» (далее – АПК «ЗАСТАВА-ТК», версия 6, АПК).

Инструкции администраторам (офицерам) безопасности и пользователям различных автоматизированных систем, использующих АПК «ЗАСТАВА-ТК», версия 6, должны разрабатываться с учетом требований настоящего Документа.

2 НАЗНАЧЕНИЕ АПК. УСЛОВИЯ ЭКСПЛУАТАЦИИ

2.1 АПК «ЗАСТАВА-ТК», версия 6 предназначен для защиты корпоративных вычислительных ресурсов на сетевом уровне модели взаимодействия OSI/ISO (стек протоколов TCP/IP) с использованием технологий VPN на основе интернет-протоколов семейства IPSec.

2.2 АПК представляет собой СКЗИ.

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

2.4 Реализация криптографических функций генерации и защищеенного хранения ключевой информации и автоматического создания и проверки электронной подписи (ЭП), осуществляется в АПК применением сертифицированного СКЗИ «ESMART Token ГОСТ» RU.63793390.00009-01.

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

2.6 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.

2.7 Для включения в информационную систему (ИТКС), укомплектованную СКЗИ (в том числе и АПК «ЗАСТАВА-ТК», 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 должна быть подтверждена организацией имеющей лицензию на разработку защищенных с использованием шифровальных (криптографических) средств информационных и/или телекоммуникационных систем[1].

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

[1] Постановление Правительства РФ от 16 апреля 2012 г. N 313. Пункты 2 и 3 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

организационных мер защиты**,** понижает класс защищенности информационой системы (ИТКС) по минимальному классу защищеенности применяемых СКЗИ КС1 или КС2.

2.8 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 подписи 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.

2.9 АПК реализует функции ЭП с применением программного обеспечения (ПО) ESMART Token ГОСТ и функционала отчуждаемого ключевого носителя ESMART Token ГОСТ:

- формирование ключевых пар открытых/закрытых ключей для ЭП на основе алгоритма ГОСТ Р 34.10-2012;
- создание и проверка ЭП на основе алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р34.11-2012 в 256-битном режиме.

2.10 В качестве шифровального (криптографического) средства ЭП используемого для автоматического создания и проверки ЭП в информационной системе АПК удовлетворяет «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу защиты КС3.

2.11 В качестве средства электронной подписи класса КС3, используемого для автоматического создания и проверки ЭП в информационной системе, АПК удовлетворяет Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27.12.2011 г. № 796, в части пунктов 11-15,19-26, 28, 29, 31, 36, 38.

2.12 Для обеспечения выполнения полного функционала средства ЭП класса защищенности КС3 в состав АПК должно быть дополнительно включено прикладное программное обеспечение (ППО), реализующее функции визуализации электронных

документов (при требовании к реализации визуализации), фиксации в электронном журнале регистрации событий / разграничения доступа к журналу событий и контроля срока использования ключа ЭП в средстве ЭП и среде его функционирования, как это предусмотрено пунктами 8-9, 34-35, 37 соответственно, Требований к средствам электронной подписи, утвержденным приказом ФСБ России от 27.12.2011 г. № 796.

Указанное ППО должно использовать вызовы собственных функций (proprietary functions) программного компонента СКЗИ «ESMART PKCS11», описанные в разделе 8 документа RU.63793390.00009-01 33 «Руководство программиста ESMART PKCS11».

2.13 При включении указанного в п. 2.12 ППО в состав АПК должна быть проведена оценка влияния этого ППО на СКЗИ АПК «ЗАСТАВА-ТК», версия 6, в соответствии с требованиями Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 г. № 66.

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

3 Состав АПК

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

- аппаратная платформа x64 ТОНК производства ООО «Группа Компаний ТОНК»;
- операционная система (ОС) AltLinux СПТ 7.0, 64-битная версия;
- СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base);
- ПО «ЗАСТАВА-Клиент», версия 6;
- СКЗИ ESMART Token ГОСТ, выполненное на базе микросхемы MIK51SC72Dv6 RU.63793390.00009, в составе:
  1) считыватель смарт-карт ESMART Reader ER4006 – считыватель смарт-карт формата ID-1 без корпуса RU.63793390.00007-01;
  2) программный компонент «ESMART Firmware Checker» RU.63793390.00018-01, предназначенный для контроля целостности ПО аппаратного модуля (АМ) 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);
  4) смарт-карта формата ID-1 RU.63793390.00004-01, которая содержит компоненты: микросхема ДВУК.431295.011-001[2], ПО АМ, состоящее из загрузчика и функциональной части[3].

3.2 В состав АПК входит аппаратная платформа x64 ТОНК, производства ООО «Группа Компаний ТОНК» (процессор Intel Baytrail J1900 QuadCore), оборудованная считывателем смарт-карт и датчиком контроля вскрытия корпуса.

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

[3] 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 «ЗАСТАВА-ТК», версия 6

4.1 Общие требования

4.1.1 Выполнение в процессе эксплуатации АПК «ЗАСТАВА-ТК», 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 системных блоков указанных средств вычислительной техники (СВТ).

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 АПК

4.2.1 Внутренняя планировка помещений, размещение в них АПК, должны обеспечивать пользователям 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.

4.3 Организационно-распорядительные меры обеспечения безопасности информации при использовании АПК

4.3.1 Порядок обращения и эксплуатации АПК «ЗАСТАВА-ТК», версия 6 должен 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 тестовых ключей;
- Журнал регистрации администраторов безопасности СВТ, на которых установлены сертифицированные ФСБ России шифровальные средства (СКЗИ).

4.4 Требования по обеспечению защиты АПК от НСД

4.4.1 Защита АПК «ЗАСТАВА-ТК», версия 6, 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 варианту поставки, описанному в документе МКЕЮ.00629.ФО «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Формуляр и используемому в корпоративной вычислительной системе.

4.4.3 Для осуществления административных функций Администратору АПК должен быть предоставлен электронный идентификатор (смарт-карта) ID-1 RU.63793390.00004-01 из состава СКЗИ RU.63793390.00009 ESMART Token ГОСТ со специально подготовленной ключевой информацией для входа в АПК с правами Администратора.

4.4.4 Для пользователей АПК должен быть предоставлен электронный идентификатор (смарт-карта) ID-1 RU.63793390.00004-01 из состава СКЗИ RU.63793390.00009 ESMART Token ГОСТ со специально подготовленной ключевой информацией для входа в АПК с правами пользователя.

4.4.5 Настройка и эксплуатация компонентов АПК должны осуществляться в соответствии с требованиями настоящих Правил пользования и согласно МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора.

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

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

4.4.8 Организация и осуществление мониторинга, протоколирования, аудита и анализа системных событий в компонентах АПК должны осуществляться в соответствии с требованиями и рекомендациями технической документации, перечисленной в п. 4.4.5.

4.4.9 Должна быть исключена возможность включения в ПО АПК утилит, позволяющих выполнять перепрограммирование микросхем с ПО BIOS.

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

4.4.11 Для эксплуатации АПК должна быть проведена установка следующих параметров BIOS Setup (Version 2.16.1242):

— 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 «Security» параметр «Secure Boot» установить в состояние «Disabled»;

— в разделе «Advanced \\ ACPI Settings» все параметры 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 «Advanced \\ PPM Configuration» параметр SOix установить в состояние «Disabled»;

— в разделе «Advanced \\ LPSS & SCC Configuration» параметр OS Selection установить в состояние «Android»;

— в разделе «Advanced \\ System Component» параметр PNP Setting установить в состояние «Disabled»;

— в разделе «Advanced \\ Trusted Computing» параметр Security Device Support установить в состояние «Disabled»;

— в разделе «Advanced \\ USB Configuration» параметр USB Mass Storage Driver Support установить в состояние «Disabled»;

— в разделе «Boot» параметр Boot Option#1 установить в состояние «HDD0».

4.4.12 Для эксплуатации АПК должна быть проведена установка датчика вскрытия в режим **hard mode**. Описание действий по настройке датчика вскрытия приведено в подразделе 6.3 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора.

4.4.13 В случае выхода из строя батареи питания CMOS на системной плате АПК осуществляется замена батареи, повторная установка вышеперечисленных параметров утилиты BIOS Setup и смена пароля на вход в BIOS Setup. Периодичность смены батареи – один раз в пять лет.

4.4.14 Для выбора и смены PIN-кодов электронных идентификаторов для входа в АПК Администратора АПК и(или) штатного пользователя АПК должна быть разработана

политика назначения и смены паролей в соответствии со следующими правилами:

- длина PIN-кодов электронных идентификаторов Администратора АПК и(или) штатного пользователя 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 четыре символа;
- периодичность смены пароля должна определяться принятой политикой безопасности, но не должна превышать шести месяцев.

4.4.15 Администратор и(или) штатный пользователь 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 Эксплуатация АПК «ЗАСТАВА-ТК», версия 6 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 «ЗАСТАВА-ТК», версия 6 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-Клиент», версия 6. Описание механизма автоматического контроля целостности программных модулей ПО «ЗАСТАВА-Клиент», версия 6 приведено в подразделе 6.7 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора.

4.5.2 В процессе эксплуатации АПК «ЗАСТАВА-ТК», версия 6 Администратор АПК, не реже одного раза в месяц, должен осуществлять переодический контроль целостности программных модулей путем запуска утилиты icv_checker с файлом шаблона контроля целостности для сверки с эталонными значениями указанных сумм, поставляемых с документацией на АПК «ЗАСТАВА-ТК», версия 6 (см. МКЕЮ.00629.Д1 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», 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 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.00629.ФО «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Формуляр.

4.5.4 Описание использования меню загрузчика приведено в документе МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», 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 встроенного датчика случайных чисел (ДСЧ) СКЗИ «КриптоПро CSP», встроенного в АПК, осуществляется в процессе производства АПК на

технологическом ключевом носителе производителя.

Администратором АПК при необходимости может быть произведена переинициализация указанного ДСЧ СКЗИ «КриптоПро CSP». Для этого Администратор АПК должен осуществить вход в ОС АПК с использованием собственного ключевого носителя. При этом в журнале событий с уровнем логгирования «Отладочный» ПО «ЗАСТАВА-Клиент», версия 6 должна появиться запись:

«CP_Conf_InitPluginRNG: RNG for Plugin crypto_cpro_user successfully initialized from: [имя токена-ключевого носителя] / [номер текена-ключевого носителя]».

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 должен 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», версия 4.0 (исполнение 2-Base) и СКЗИ RU.63793390.00009-01 ESMART Token ГОСТ.

4.6.2 При эксплуатации АПК для реализации функций ЭП с применением программного обеспечения (ПО) ESMART Token ГОСТ и функционала отчуждаемого ключевого носителя ESMART Token ГОСТ должны использоваться только алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р34.11-2012 в 256-битном режиме.

4.7 Требования к обращению с ключевыми документами

4.7.1 В качестве носителя ключевой информации в АПК «ЗАСТАВА-ТК», версия 6 должен использоваться только электронный идентификатор (смарт-карта) ID-1 RU.63793390.00004-01 из состава СКЗИ RU.63793390.00009 ESMART Token ГОСТ.

4.7.2 Требования по обращению с криптографическими ключами АПК (включая сертификаты) регламентируются технической документацией на СКЗИ RU.63793390.00009 ESMART Token ГОСТ.

4.7.3 Ключевая информация, используемая АПК, является конфиденциальной.

4.7.4 Срок действия открытых и закрытых ключей, используемых в составе АПК, не должен превышать 3 (три) года.

4.7.5 Срок действия ключа проверки ЭП не должен превышать срок действия ключа ЭП более чем на 15 лет.

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

4.7.6 Криптографические ключи, срок действия которых закончился, подлежат обязательному уничтожению с ключевых носителей. Уничтожение должно осуществляться форматированием (инициализацией) электронного идентификатора (смарт-карты) ID-1 RU.63793390.00004-01 из состава СКЗИ RU.63793390.00009 ESMART Token ГОСТ согласно Правилам пользования на данную смарт-карту.

4.7.7 Формирование открытых и закрытых ключей и соответствующего им цифрового сертификата формата X.509 для АПК и его компонентов должно выполняться:

— с использованием функционала программно-аппаратных комплексов (ПАК) удостоверяющих центров (УЦ), сертифицированных ФСБ России по классу защиты не ниже класса КС3;

— с использованием функционала СКЗИ, реализующих целевую криптографическую функцию изготовления ключевых документов и сертифицированных ФСБ России по классу защиты не ниже класса КС3;

— на рабочих местах пользователей, с использованием функционала СКЗИ RU.63793390.00009 ESMART Token ГОСТ.

Использование в АПК других носителей ключевой информации ЗАПРЕЩАЕТСЯ !

4.7.8 Аутентификация Администратора АПК и(или) штатного пользователя АПК при доступе к ключевой информации, содержащейся на СКЗИ RU.63793390.00009 ESMART Token ГОСТ, осуществляется на основе ввода паролей (PIN-кода).

4.7.9 Срок действия PIN-кода до смены не должен превышать шести месяцев. Необходимость и периодичность смены PIN-кода, а также требования к сложности PIN-кода следует отразить во внутреннем регламенте использования СКЗИ.

Администратор и(или) штатный пользователь 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 пользователя лежит на Пользователе СКЗИ.

4.7.10 Носитель ключевой информации защищен от подбора PIN-кода методом перебора. После того, как предварительно заданное число раз (10 по умолчанию), был введен неверный PIN-код, устройство блокируется. Получить доступ к хранящимся на заблокированном устройстве закрытым объектам (ключам) невозможно. Разблокировать устройство может Администратор СКЗИ RU.63793390.00009 ESMART Token ГОСТ, которому известен PIN-код Администратора (SO-PIN). Если превышено количество допустимых попыток

неверного ввода PIN-кода Администратора, 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 модуля в соответствии с эксплуатационной документацией (ЭД) на СКЗИ RU.63793390.00009 ESMART Token ГОСТ, либо процедурой полного очищения энергонезависимой памяти АМ в соответствии с ЭД на СКЗИ RU.63793390.00009 ESMART Token ГОСТ. Факт утилизации смарт-карты, как носителя криптоключей, должен фиксироваться в журнале поэкземплярного учета 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 Для автоматического выбора сертификата в АПК для входа в ОС персональный сертификат пользователя формата X.509 должен содержать расширенное назначение ключа: Smart Card Logon (OID 1.3.6.1.4.1.311.20.2.2).

4.7.13 Для реализации ролевого доступа расширенное назначение ключа Smart Card Logon в АПК для входа в ОС, персональный сертификат пользователя формата X.509 должен содержать Дополнительное имя субъекта: UserPrincipalName (OID 1.3.6.1.4.1.311.20.2.3) со значениями:

— user@localhost - для пользователей АПК;

— admin@localhost – для администраторов АПК.

4.7.14 Для возможности автоматического выбора сертификата в АПК, для установления езащищенного соединения персональный сертификат пользователя формата X.509 должен содержать расширенное назначение ключа: id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17).

Примечание - Для установления защищенного соединения АПК не требует обязательного наличия в цифровом сертификате партнера по взаимодействию формата X.509 расширенное назначение ключа: id-kp-ipsecIKE.

4.7.15 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 УЦ 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 входа в АПК и/или установления защищенных соединений с абонентами ИТКС, использующими цифровые сертификаты, выпущенные УЦ, формирующим данный CRL.

4.8 Действия при компрометации ключей

4.8.1 К случаям явной компрометации закрытого ключа Администратора АПК и/или Пользователя АПК относятся:

— потеря ключевого носителя;

— потеря ключевого носителя с последующим обнаружением;

— увольнение (смена) Администратора АПК и/или Пользователя АПК;

— нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.

4.8.2 Пользователь АПК, в случае потери ключевого носителя (в т.ч. с последующим обнаружением), должен сообщить об этом Администратору АПК. Администратор АПК должен немедленно известить УЦ о факте компрометации.

При потере ключевого носителя Администратора АПК и/или Пользователя АПК требуется заказать получение нового ключевого носителя. Потерянный, и впоследствии обнаруженный, ключевой носитель может быть использован для замены ключевой информации.

4.8.3 К случаям неявной компрометации закрытого ключа Администратора АПК относятся:

— 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.

При выходе из строя ключевого носителя Администратор АПК должен заказать получение нового ключевого носителя. Вышедший из строя ключевой носитель может быть уничтожен самостоятельно, путем физического уничтожения.

4.8.4 По факту компрометации ключей должно быть проведено служебное расследование.

4.8.5 Все скомпрометированные ключи подлежат замене и отзыву сертификатов в УЦ. Все скомпрометированные ключи (при доступности ключевого носителя) выводятся из действия посредством процедуры последовательного удаления каждого экземпляра ключевого документа путем удаления соответствующего объекта в энергонезависимой памяти АМ в соответствии с ЭД на СКЗИ RU.63793390.00009 ESMART Token ГОСТ, либо процедуры полного очищения энергонезависимой памяти АМ в соответствии с ЭД на СКЗИ RU.63793390.00009 ESMART Token ГОСТ.

4.8.6 Администратор безопасности АПК, в случае невозможности выполения п. 4.8.5 на парке обслуживаемых им АПК, должен включить режим обработки CRL для блокирования возможности входа в АПК и/или установления защищенных соединений на скомпрометированных ключах.

Для включения режима обработки CRL Администратор АПК должен выполнить настройку обработки CRL (см. п. 3.7.7, подраздел 6.6 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора.

4.9 Перечень событий, при возникновении которых эксплуатация АПК запрещена

4.9.1 Эксплуатация АПК запрещена при наступлении следующих событий:

— обнаружение несанкционированного вскрытия корпуса;

— нарушение целостности образа ПО АПК;

— сбой ПО АПК;

— компрометация ключей.

4.9.2 При наступлении любого из перечисленных в п. 4.9.1 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.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора.

4.9.3 В случае невозможности устранения негативных последствий инцидентов, перечисленных в п. 4.9.1, Администратор АПК должен вывести из эксплуатации АПК и передать АПК в ремонт или утилизировать.

4.10 Требования к политике безопасности

4.10.1 АПК должен быть настроен для эксплуатации Администратором АПК в соответствии с требованиями технической документации, перечисленной в п. 4.4.5 - 4.4.7.

4.10.2 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***.

4.10.3 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[4]. При этом достаточность принятых мер должна оцениваться порядком, предусмотренным упомянутыми руководящими документами ФСТЭК России.

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

4.10.5 До начала эксплуатации АПК Администратором АПК должен быть сменен PIN-код ключевого носителя администратора (см. подраздел 6.4 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора).

4.10.6 До начала эксплуатации Администратором безопасности АПК должен быть отключен режим IKEv1 в настройках ПО «ЗАСТАВА-Клиент», версия 6 (см. п. 3.11.2.1 и 3.11.2.2 или п. 4.3.6 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора).

4.10.7 Запрещается удалять файлы-журналы работы СКЗИ без предварительного перемещения их в архив.

4.11 Требования к процедуре обновления

4.11.1 Процедура установки сертифицированных обновлений возможна только в автоматическом режиме.

4.11.2 Для обновления АПК Заказчик (Пользователь) должен самостоятельно получить у Изготовителя (Поставщика) согласно договору на поставку и/или техническую поддержку образ обновления на CD/DVD-диске или USB-носителе 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.

4.11.3 Для установки нового сертифицированного обновления АПК в автоматизированном режиме может быть использован любой http-сервер, размещение и

---

[4] «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282;
«Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными Приказом ФСТЭК России от 11.02.2013 г. № 17;
«Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом ФСТЭК России от 18.02.2013 г. № 21.

эксплуатация которого осуществляется в соответствии с требованиями руководящих документов ФСТЭК России по технической защите конфиденциальной информации[5].

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

4.11.4 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 производства 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.

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

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.

[5] «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.

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.
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 7.1 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», 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 6.2 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», 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 7.2 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора); – в случае невозможности выполнить возврат к эталонной версии, необходимо отправить АПК Изготовителю (Поставщику) для ремонта.

№п/п	Нештатная ситуация	Действия Администратора АПК
4.	Компрометация ключей	В случае компрометации ключей необходимо действовать в соответсвии с подразделом 4.8.
5.	Истечение срока действия закрытых криптографических ключей	Производится замена ключей. Криптографические ключи на ключевых носителях, сроки действия которых истекли, уничтожаются. Порядок уничтожения ключей описан в п. 3.9.2 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора. После уничтожения (стирания) криптоключей на смарт-карте в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним делается соответствующая отметка об уничтожении криптоключей.
6.	Не проходит локальный вход Пользователей и Администраторов АПК при предъявлении зарегистрированного ключевого носителя и корректного PIN-кода к нему.	Администратор безопасности АПК: – остановливает 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. 4.4.11, и, при необходимости, установить в корректные значения. Сохранить настройки BIOS; – пройти повтороно аутентификацию. В случае отрицательного результата произвести замену батареи питания CMOS согласно п. 4.4.12.

5 Порядок ремонта и утилизации АПК

5.1.1 Ремонт АПК 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 Утилизация АПК обеспечивается отсоединением модуля памяти DOM от аппаратной платформы АПК и последующей его утизизацией. Рекомендуемые способы утилизации – физическое уничтожения модуля памяти DOM (например, разбитие молотком).

5.1.3 Пригодные для дальнейшего использования узлы и детали аппаратной платформы x64 ТОНК, не предназначенные для реализации криптографических алгоритмов или иных функций СКЗИ, разрешается использовать после уничтожения СКЗИ в других целях, по усмотрению владельца АПК.

5.1.4 Уничтожение (стирание) криптоключей, содержащихся на электронном идентификаторе (смарт-карте) ID-1 RU.63793390.00004-01 из состава СКЗИ RU.63793390.00009 ESMART Token ГОСТ, может производиться либо путем форматирования смарт-карты – стирания (разрушения) криптоключей без повреждения электронного идентификатора (для обеспечения возможности ее многократного использования), либо путем физического уничтожения электронного дентификатора.

5.1.5 Форматирование электронного идентификатора производится Администратором АПК. Описание процедуры уничтожения криптографических ключей приведено в п. 3.9.2 документа МКЕЮ.00629.И3 «Аппаратно-программный комплекс «VPN/FW «ЗАСТАВА-ТК», версия 6» («АПК «ЗАСТАВА-ТК», версия 6»). Руководство администратора.

5.1.6 В случае, если при обращении к электронному идентификатору в целях уничтожения (стирания) криптоключей превышено количество допустимых попыток неверного ввода PIN-кода (10 попыток по умолчанию), электронный идентификатор не подлежит дальнейшему использованию и должен быть утилизирован.

5.1.7 Утилизация выполняется путем нанесения неустранимого физического повреждения, исключающего возможность повторного использования и восстановления ключевой информации. Рекомендуемые способы утилизации электронного идентификатора – разрезание карты ножницами по середине микросхемы.

5.1.8 Пригодные для дальнейшего использования узлы и детали аппаратной платформы x64 ТОНК, не предназначенные для реализации криптографических алгоритмов или иных функций СКЗИ, разрешается использовать после уничтожения СКЗИ в других целях, по усмотрению владельца АПК.

5.1.9 Допускается повторное использование аппаратных компонентов АПК в новых

сертифицированных модификациях АПК «ЗАСТАВА», производимых АО «ЭЛВИС-ПЛЮС», путем 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[6]. К аппаратным компонентам АПК относятся:

- аппаратная платформа x64 ТОНК производства ООО «Группа Компаний ТОНК»;
- электронный идентификатор ESMART Token ГОСТ, аппаратно-реализующий российские стандарты ЭП, шифрования, хэширования.

[6] В организации должна быть регламентирована процедура передачи в администрирование модифицированных АПК другим лицам без процедуры физического уничтожения модуля памяти в целях предупреждения возможности получения доступа к остаточной информации после процедуры разметки и форматирования внутреннего накопителя АПК.

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

DOM – Disk on Module
Устройство, выполняющее функции жесткого диска, но реализованное на модуле памяти

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

IP – Internet Protocol
Протокол сетевого уровня, являющийся базовым протоколом IP-сетей

IPsec – IP security
группа протоколов для установления защищенных соединений в IP-сетях

PIN – Personal Identification Number
Персональный идентификационный код

PKCS – PublicKey Cryptography Standards
Криптографические стандарты открытого ключа

TCP – Transmission control protocol
Сетевой протокол транспортного уровня (с гарантированной доставкой) в IP-сетях

VPN – Virtual Private Network
Виртуальная частная сеть

АМ – Аппаратный модуль

АПК – Аппаратно-программный комплекс

ВТСС – Вспомогательные технические средства и системы

ВОЛС – Волоконно-оптические линии связи

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

СВТ – Средство вычислительной техники

СКЗИ – Средство криптографической защиты информации

ФСБ – Федеральная служба безопасности России

ФСТЭК – Федеральная служба по таможенному и экспортному контролю России
УЦ – Удостоверяющий центр
ЭД – Эксплуатационная документация
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					