УТВЕРЖДЕН

МКЕЮ.00628-01 91 01-ЛУ

«Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3»

(«VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3»)

(исполнение ZO6-L64-FV-03)

Правила пользования

МКЕЮ.00628-01 91 01

Листов 24

2021

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
7482				

СОДЕРЖАНИЕ

1. АННОТАЦИЯ

Настоящий документ представляет собой Правила пользования программным средством криптографической защиты информации (СКЗИ) МКЕЮ.00628-01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе Интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» (исполнение ZO6-L64-FV-03) (далее – «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3», ПК).

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ ПК должны разрабатываться с учетом требований настоящего Документа.

2. СОСТАВ И НАЗНАЧЕНИЕ

2.1. «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» состоит из следующих компонентов:

— Операционная система (ОС) AltLinux СПТ 7.0, 64-битная версия производства ООО «Базальт СПО»;

— СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base) производства ООО «КРИПТО-ПРО» (г. Москва);

— Программное обеспечение (ПО) «ЗАСТАВА-Офис», версия 6 производства АО «ЭЛВИС-ПЛЮС»;

— Один из аппаратно-программных модулей доверенной загрузки (АПМДЗ):

  – программно-аппаратный комплекс (ПАК) защиты от несанкционированного доступа (НСД) «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);

  – ПАК защиты от НСД «Соболь». Версия 3.1. RU.88338853.501410.020 (исполнения 1, 2);

  – ПАК защиты от НСД «Соболь». Версия 3.2. RU.88338853.501410.021 (исполнения 1, 2).

2.2. ПК 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.

2.3. ПК представляет собой СКЗИ.

2.4. ПК обеспечивает выполнение целевых криптографических функций: шифрования, контроля целостности данных, имитозащиты данных, открытого распределения криптографических ключей, что обеспечивает:

— конфиденциальность передаваемой в корпоративной информационно-телекоммуникационной сети (ИТКС) информации, за счет ее шифрования согласно ГОСТ 28147-89;

— защиту доступа к корпоративным вычислительным ресурсам за счет использования протоколов двухсторонней криптографической аутентификации при установлении соединений на базе протокола IKEv2 с использованием алгоритмов подписи в соответствии с ГОСТ Р 34.10-2012;

— контроль целостности данных 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 алгоритма ГОСТ Р 34.10-2012 VKO в 256-битном режиме.

2.5. ПК выполняет функции шлюза безопасности и сетевого пакетного фильтра в защищаемой ИТКС.

2.6. ПК предназначен для применения в автоматизированных системах органов государственного управления и других организаций Российской Федерации, и обеспечивает защиту информации конфиденциального характера, не содержащей сведений, составляющих государственную тайну.

2.7. Реализация криптографических функций шифрования, контроля целостности данных, имитозащиты данных, аутентификации абонентов на основе процедуры Диффи-Хеллмана осуществляется в ПК применением СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base).

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

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

2.10. Для включения в информационную систему (ИТКС), укомплектованную СКЗИ (в том числе и «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3»), 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 лизензию на разработку защищенных с использованием шифровальных (криптографических) средств информационных и/или телекоммуникационных систем[1].

2.11. Включение в информационную систему (ИТКС), укомплектованную ПК, 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, понижает класс защищенности информационной системы (ИТКС) по минимальному классу защищенности применяемых СКЗИ КС1 или КС2.

2.12. Средствами ПК НЕ ДОПУСКАЕТСЯ обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

3. ТРЕБОВАНИЯ К ИСПОЛЬЗУЕМЫМ АППАРАТНО-ПРОГРАММНЫМ ПЛАТФОРМАМ

3.1. СКЗИ «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» предназначен для работы на серверных аппаратно-программных платформах x64.

3.2. ПК функционирует в программной среде ОС AltLinux СПТ 7.0, 64-битная версия.

3.3. ПК комплектуется одним из АПМДЗ:

— ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180);

— ПАК защиты от НСД «Соболь». Версия 3.1. RU.88338853.501410.020 (исполнения 1, 2);

— ПАК защиты от НСД «Соболь». Версия 3.2. RU.88338853.501410.021 (исполнения 1, 2).

Эксплуатация АПМДЗ ПАК «Соболь» без действующего сертификата ФСБ России ЗАПРЕЩАЕТСЯ !

4. ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМ И АДМИНИСТРАТИВНЫМ МЕРАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ

4.1. Общие требования

4.1.1. Выполнение в процессе эксплуатации «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» на должном уровне всех заявленных функций по защите информации, возможно исключительно при соблюдении необходимых организационно-распорядительных и технических меры защиты:

— по физическому размещению ПК;

— по правильной установке и настройке ПК 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. В целях защиты открытой конфиденциальной информации от утечки по техническим каналам, в том числе по каналам связи, отходящим от объектов информатизации и ПК, эксплуатация указанных объектов и СВТ должна осуществляться в соответствии с требованиями руководящих документов ФСТЭК России по технической защите конфиденциальной информации[2].

4.1.3. Безопасность эксплуатации ПК 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:

---

[2] «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденным 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.

— 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 «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» должны обеспечивать пользователям ПК 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 НСД в помещения, в которых размещены ПК, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

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

4.2.3. 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.

4.2.4. В случае планирования размещения ПК 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, ПК должны быть подвергнуты специальной проверке по выявлению устройств, предназначенных для негласного получения информации, а также специальным исследованиям на соответствие требованиям к ВТСС по защите от утечки информации по каналам ПЭМИН в соответствии с категорией выделенного помещения.

4.3. Организационно-распорядительные меры обеспечения безопасности информации при использовании «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3»

4.3.1. Порядок обращения и эксплуатации «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» 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 сертифицированными ФСБ России шифровальных средств (СКЗИ);

— Журнал учета сертифицированных ФСБ России шифровальных средств (СКЗИ) и тестовых ключей;

— Журнал регистрации администраторов (офицеров) безопасности СВТ, на которых установлены сертифицированные ФСБ России шифровальные средства (СКЗИ).

4.4. Требования по обеспечению защиты «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» от НСД

4.4.1. Защита «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3», носителей ключевой информации, содержащих ключевую информацию, должна осуществляться как в процессе функционирования данных средств, так и при проведении регламентных и ремонтных работ.

4.4.2. Функции Администратора ПК, должны быть возложены исключительно на Администратора (офицера) безопасности.

Запрещается предоставление обслуживающему персоналу ПК привилегий Администратора ПК!

4.4.3. Прежде, чем приступить к работе, Администратор (офицер) безопасности должен ознакомиться с технической документацией на ПК в полном объеме, согласно варианту поставки, описанному в документе МКЕЮ.00628-01 30 01 ФО «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе Интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3». Формуляр», а также с технической документацией на используемый АПМДЗ.

4.4.4. Аутентификация Администратора (офицера) безопасности должна производиться автоматически после прохождения процедуры аутентификации в АПМДЗ.

4.4.5. Установка ПК на СВТ должна производиться только с дистрибутивов, полученных по доверенному каналу.

4.4.6. Настройка и конфигурирование ПК должны осуществляться исключительно Администратором (офицера) безопасности в соответствии с требованиями настоящих Правил пользования и согласно документу МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3». Руководство системного программиста».

4.4.7. Организация и осуществление мониторинга, протоколирования, аудита и анализа системных событий в ПК должны осуществляться в соответствии с требованиями и рекомендациями документации, указанной в п. 4.4.6.

4.4.8. Аутентификация с использованием функционала АПМДЗ «ПАК защиты от НСД «Соболь» RU.40308570.501410.001 (версии кода расширения BIOS 1.0.99, 1.0.180) Администратора (офицера) безопасности должна осуществляться согласно технической документации (Руководству пользователя) на используемый АПМДЗ.

4.4.9. Для выбора и смены пароля Администратора (офицера) безопасности, используемого для входа в ОС, должна быть разработана политика назначения и смены паролей в соответствии со следующими правилами:

— длина пароля Администратора (офицера) безопасности не должна быть не менее семи 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 6 месяцев.

4.4.10. При эксплуатации ПК КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ:

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

— **осуществлять несанкционированное вскрытие кожухов СВТ, на котором эксплуатируется ПК;**

— осуществлять несанкционированное Администратором (офицером) безопасности 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 ПК;

— записывать на носители ключевой информации постороннюю информацию;

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

4.4.11. Должно быть проведено опечатывание системного блока СВТ, на котором функционирует ПК, позволяющее визуально контролировать вскрытие и исключающее возможность бесконтрольного изменения аппаратной части СВТ.

4.4.12. Эксплуатации ПК без перезагрузки в течение срока, превышающего 1 (Одни) сутки, **не допускается**.

4.4.13. Для ограничения возможности влияния аппаратных компонентов СВТ на функционирование СКЗИ необходимо проведение исследований на ПО BIOS СВТ, на которых установлено СКЗИ, в соответствии с «Временными требованиями к проведению исследований ПО BIOS».

4.5. Требования к размещению и настройке «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3»

4.5.1. В процессе эксплуатации ПК 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 5.7 документа МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста».

В процессе эксплуатации ПК Администратор (офицер) безопасности, не реже одного раза в месяц, должен осуществлять периодический контроль целостности программных модулей, путем запуска утилиты *icv_checker* с файлом шаблоном контроля целостности для сверки с эталонными значениями указанных сумм, поставляемых с документацией на ПК. (См.

МКЕЮ.00628-01 92 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Электронное приложение к формуляру»).

4.5.2. В процессе эксплуатации ПК Администратор (офицер) безопасности должен настроить контроль целостности АПМДЗ для проверки целостности загрузчика ОС (/image/syslinux/alt0/full.cz) и ядра ОС (/image/syslinux/alt0/vmlinuz). Описание настроек контроля целостности АПМДЗ приведены в п. 5.1.1 документа «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста».

4.5.3. В процессе эксплуатации ПК Администратор (офицер) безопасности не реже одного раза в месяц должен осуществлять проверку целостности ПК посредством запуска процедуры из меню загрузчика с использованием утилиты *icv_checker*, входящей в его состав и предназначенной для периодического тестирования работоспособности. Эталонные КС образа ОС ПК указаны в документе МКЕЮ.000628.ФО.

4.5.4. Описание использования меню загрузчика приведено в документе МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста».

4.5.5. **В процессе эксплуатации ПК запрещается несанкционированное Администратором (офицером) безопасности изменение среды функционирования ПК**, а именно:

— модернизация ОС;

— внесение изменений в ПО ПК;

— модификация файлов, содержащих исполняемые коды ПК, при их хранении на жестком диске;

— добавление и(или) удаление аппаратных компонентов (в том числе сетевых карт, жестких дисков и т.п.) компьютера, на котором установлен ПК, по отношению к состоянию СВТ на момент установки ПК.

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

4.6. Требования к обращению с ключевыми документами

4.6.1. В качестве носителя ключевой информации в «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» должен использоваться HDD СВТ, а также возможно использование ключевых носителей, поддерживаемых СКЗИ ЖТЯИ.00088-01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base).

4.6.2. Ключевая информация, используемая ПК, является конфиденциальной

4.6.3. Срок действия открытых и закрытых ключей, используемых в составе ПК, не должен превышать 1 (один) год 3 (три) месяца.

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

4.6.4. Криптографические ключи, срок действия которых закончился, подлежат обязательному уничтожению с ключевых носителей согласно регламенту уничтожения, определенному в документации на СКЗИ «КриптоПро CSP» 4.0 2-Base ЖТЯИ.00088 (см. п. «Уничтожение ключей на ключевых носителях» документа ЖТЯИ.00088СКЗИ «КриптоПро CSP» 4.0 2-Base. Правила пользования).

4.6.5. Формирование открытых и закрытых ключей и соответствующего им цифрового сертификата формата X.509 для ПК должно выполняться:

— с использованием функционала 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 СВТ с установленным ПК, с использованием функционала сертифицированного СКЗИ ЖТЯИ.00088-01 30 01 «КриптоПро CSP», версия 4.0 (исполнение 2-Base).

Использование в ПК других носителей ключевой информации ЗАПРЕЩАЕТСЯ !

4.6.6. Механизмы аутентификации, реализованные в ПК ограничивают количество неудачных подряд совершенных попыток аутентификации для одного субъекта доступа числом, не превосходящим 10.

4.6.7. Доставка криптографических ключей и сертификатов открытых ключей должна осуществляться Администратором (офицером) безопасности на носителе ключевой информации или иным доверенным способом, соответствующим требованиям технической документации на эти СКЗИ.

4.6.8. Принятая в корпоративной ИТКС политика безопасности должна предусматривать возможность получения ПК, 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 ПК актуального списка аннулированных сертификатов CRL может привести к невозможности установления защищенных соединений с абонентами корпоративной вычислительной сети, использующими цифровые сертификаты, выпущенные УЦ, формирующим данный CRL.

4.7. Действия при компрометации ключей

4.7.1. К случаям явной компрометации закрытого ключа, используемого для организации защищенного соединения, относятся:

- потеря ключевого носителя;
- потеря ключевого носителя с последующим обнаружением;
- увольнение (смена) Администратора (офицера) безопасности, имевшего доступ к ключевой информации;
- нарушение правил уничтожения (после окончания срока действия) закрытого ключа.

Администратор (офицер) безопасности должен обеспечить запрет удаленного администрирования и доставку политик безопасности до управляемых СКЗИ по защищенному каналу на скомпрометированных ключах. Администратор (офицер) безопасности должен немедленно известить УЦ, выпустивший ключ, о факте компрометации.

4.7.2. К случаям неявной компрометации закрытого ключа, используемого для организации защищенного соединения, относятся:

- возникновение подозрений на утечку информации или ее искажение в ИТКС;
- 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)

4.7.3. По факту компрометации должно быть проведено служебное расследование.

4.7.4. Скомпрометированные ключи, используемые для организации защищенного соединения, выводятся из действия и уничтожаются согласно регламенту уничтожения, определенному в документации на СКЗИ «КриптоПро CSP» 4.0 2-Base ЖТЯИ.00088 (см. п. «Уничтожение ключей на ключевых носителях» документа ЖТЯИ.00088СКЗИ «КриптоПро CSP» 4.0 2-Base. Правила пользования).

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

4.7.6. Для организации защищенного соединения необходимо выпустить новую ключевую информацию и импортировать ее (см. п. 3.2.2.4 документа МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста»).

4.8. Требования к политике безопасности для «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3»

4.8.1. Для эксплуатации ПК должен быть настроен Администратором (офицером) безопасности ПК в соответствии требованиями технической документации, перечисленной в п. 4.4.6.

4.8.2. 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 «КриптоПро CSP» 4.0 2-Base ЖТЯИ.00088. Поэтому при настройке, конфигурировании и создании политики безопасности Администратор безопасности ПК 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***.

4.8.3. На объектах информатизации корпоративной ИТКС, где эксплуатируются ПК, 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[3]. При этом достаточность принятых мер должна оцениваться порядком, предусмотренным упомянутыми руководящими документами ФСТЭК России.

4.8.4. При обнаружении в процессе эксплуатации защищенной корпоративной ИТКС пользователей, локальная политика безопасности (ЛПБ) которых не соответствует действующей в корпоративной информационно-телекоммуникационной глобальной политики

---

[3] «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.

безопасности, Администратор безопасности ПК сети должен принять меры к незамедлительному принудительному восстановлению ЛПБ у указанных пользователей.

4.8.5. До начала эксплуатации ПК Администратором безопасности ПК должен быть задан пароль администратора настроек СКЗИ (см. подраздел 5.2 документа МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста»). До начала эксплуатации ПК Администратором безопасности ПК должен быть отключен режим IKEv1 в настройках ПО «ЗАСТАВА-Офис», версия 6 (см. п. 3.2.2.8 документа МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста»).

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

4.9. Требования к процедуре обновления

4.9.1. Процедура установки сертифицированных обновлений возможна в автоматическом режиме, а также локально посредством установки новой версии «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» с CD/DVD-диска или USB-носителя.

4.9.2. Для обновления ПК Заказчик (Пользователь) должен самостоятельно получить от Изготовителя (Поставщика) согласно договору на поставку и/или техническую поддержку пакет обновления на CD/DVD-диске для автоматизированного режима или USB-носитель дистрибутива с обновлением и прилагаемую к нему техническую документацию (новый формуляр или предписание на внесение изменений), содержащую новые контрольные суммы (КС) в соответствии с ГОСТ Р 34.11-2012.

4.9.3. Для установки нового сертифицированного обновления ПК 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[4].

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

4.9.4. Установка нового сертифицированного обновления в автоматизированном режиме на ПК, 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 Заказчиков (Пользователей) и установку обновленного дистрибутива.

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

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

КС пакета обновления ПК указанные в файле update.ini должны совпадать с КС в технической документации (новом формуляре или предписании на внесение изменений), сопровождающей данное обновление.

4.9.5. По завершении процедуры обновления Администратор (офицер) безопасности должен обеспечить изменение формуляра на «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» путем его корректировки согласно требованиям предписания на внесение изменений или замены на новый.

4.10. Перечень событий, при возникновении которых эксплуатация запрещена

Эксплуатация «VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3» запрещена при наступлении следующих событий:

— нарушение печати системного блока СВТ с установленным ПК;

---

[4] «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.

— нарушение целостности ПО «ЗАСТАВА-Офис», версия 6;

— сбой в работе ПО «ЗАСТАВА-Офис», версия 6;

— компрометация ключей.

При наступлении любого из перечисленных событий Администратор (офицер) безопасности должен: приостановить эксплуатацию ПК, выявить причины инцидента, а также устранить негативные последствия посредством принятия мер в соответствии с документом МКЕЮ.00628-01 32 01 «Программный комплекс защиты корпоративных вычислительных ресурсов на сетевом уровне с использованием технологий VPN и распределенного межсетевого экранирования на основе интернет-протоколов семейства IPsec/IKE «VPN/FW «ЗАСТАВА-Офис», версия 6 КС3» («VPN/FW-агент «ЗАСТАВА-Офис», версия 6 КС3») (исполнение ZO6-L64-FV-03). Руководство системного программиста» или в соответствии с подразделом 4.11.

В случае невозможности устранения негативных последствий инцидентов Администратор (офицер) безопасности должен вывести ПК из эксплуатации.

4.11. Нештатные ситуации при эксплуатации

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

Таблица 1 - Действия Администратора безопасности в нештатных ситуациях

№п/п	Нештатная ситуация	Действия Администратора безопасности
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в помещении где размещается СВТ.	Администратор (офицер) безопасности: – Останавливает СВТ; – 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 аппаратных и программных средств; – оповещает по телефонным каналам общего пользования всех пользователей и администраторов программных и аппаратно-программных СКЗИ о приостановке работы ПК. – В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств ПК, Администратор (офицер) безопасности уничтожает всю ключевую информацию с ключевых носителей.
2.	Компрометация ключей, используемых для организации защищенного соединения.	Порядок действий при компрометации ключей описан в подразделе 4.7 «Действия при компрометации ключей».
3.	Истечение срока действия закрытых криптографических ключей.	Производится замена ключей. Криптографические ключи на ключевых носителях, сроки действия которых истекли, уничтожаются. Порядок уничтожения ключей описан в подразделе 4.6 и в документации на СКЗИ «КриптоПро CSP» 4.0 2-Base ЖТЯИ.00088 (см. п. «Уничтожение

№п/п	Нештатная ситуация	Действия Администратора безопасности
		ключей на ключевых носителях» документа ЖТЯИ.00088 СКЗИ «КриптоПро CSP» 4.0 2-Base. Правила пользования).
4.	Отказы и сбои в работе аппаратной части ПК.	При отказах и сбоях в работе аппаратной части необходимо остановить работу ПК, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку ПК.
5.	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, Администратор (офицер) безопасности должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства защиты от НСД.
6.	Отказы и сбои в работе программных средств вследствие невыявленных ранее ошибок в ПО.	При отказах и сбоях в работе программных средств, вследствие невыявленных ранее ошибок в ПО, необходимо остановить работу ПК, локализовать по возможности причину отказов и сбоев и обратиться в службу технической поддержки производителя ПК для устранения причин, вызывающих отказы и сбои.
7.	Отказы в работе программных средств ПК вследствие случайного или умышленного их повреждения. Нарушение целостности ПО.	При отказах в работе программных средств, вследствие случайного или умышленного их повреждения или нарушения целостности ПО, Администратор (офицер) безопасности обязан произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы ПК, комплектация ZO6-L64-FV-03 в установленном порядке.
8.	Нарушение печати системного блока СВТ с установленным ПК.	При нарушении целостности печати системного блока СВТ с установленным ПК, Администратор (офицер) безопасности, обязан произвести служебное расследование по данному факту с целью установления причины нарушении целостности печати и при необходимости переустановить ПК.

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

BIOS	–	Basic input/output system Базовая система ввода-вывода
CRL	–	Certificate Revocation List, Список отозванных сертификатов
ESP	–	Encapsulating Security Payload Инкапсуляция защищенных данных IP-протокол шифрования сетевого трафика
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
ISAKMP	–	Internet Security Association and Key Management Protocol; Протокол защищенного соединения и управления ключами в сети Интернет
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
АПМДЗ	–	Аппаратно-программный модуль доверенной загрузки
АО		Акционерное общество
ВОЛС		Волоконно оптические линии связи
ВТСС	–	Вспомогательные технические средства и системы
ИТКС	–	Информационно-телекоммуникационная сеть
КС		Контрольная сумма
ЛПБ	–	Локальная политика безопасности
НСД	–	Несанкционированный доступ
ООО		Общество с ограниченной ответсвенностью
ОС	–	Операционная система
ПАК	–	Программно-аппаратный комплекс
ПК	–	Программный комплекс
ПО	–	Программное обеспечение
ПЭМИН	–	Побочные электромагнитные излучения и наводки
СВТ	–	Средство вычислительной техники
СКЗИ	–	Средство криптографической защиты информации
ФСБ России	–	Федеральная служба безопасности
ФСТЭК России	–	Федеральная служба по таможенному и экспортному контролю
УЦ		Удостоверяющий центр

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					
1	-	Все	-	-	24	МКЕЮ.0079	-		21.09.2021