УТВЕРЖДЕН

МКЕЮ.00627-01 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 КС1»

(«VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»)

(исполнения: ZO6-L32-VF-01, ZO6-L64-VF-01)

Правила пользования

МКЕЮ.00627-01 91 01

Листов 29

2021

СОДЕРЖАНИЕ

1. АННОТАЦИЯ

Настоящий документ представляет собой Правила пользования средством криптографической защиты информации (СКЗИ) «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 КС1» (далее – ПК) МКЕЮ.00627-01.

Инструкции администраторам (офицерам) безопасности и пользователям автоматизированных систем, использующих ПК, должны разрабатываться с учетом требований настоящего Документа.

2. НАЗНАЧЕНИЕ

2.1. ПК предназначен для защиты корпоративных вычислительных ресурсов на сетевом уровне модели взаимодействия OSI/ISO (на уровне TCP/IP-протокола) с использованием технологий VPN и распределенного межсетевого экранирования на основе Интернет-протоколов семейства IPSec.

2.2. В состав ПК входит программное обеспечение (ПО) «ЗАСТАВА-Офис, версия 6» производства АО «ЭЛВИС-ПЛЮС».

2.3. В состав ПК входит СКЗИ «ЖТЯИ.00087-01 «КриптоПро CSP», версия 4.0 1-Base»[1] производства ООО «КРИПТО-ПРО» (г. Москва) (далее – СКЗИ «КриптоПро CSP» 4.0 КС1).

2.4. Реализация целевых криптографических функций шифрования, контроля целостности данных, имитозащиты данных, открытого распределения криптографических ключей осуществляется в ПК применением СКЗИ «КриптоПро CSP» 4.0 КС1.

2.5. Эксплуатация ПК с входящим в его состав СКЗИ «КриптоПро CSP» 4.0 КС1 должна осуществляться в соответствии с требованиями технической и эксплуатационной документации на соответствующее СКЗИ.

2.6. Эксплуатация ПК, а также входящего в него сертифицированного СКЗИ «КриптоПро CSP» 4.0 КС1 должна проводиться согласно с разделом V документа «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005)».

ЗАПРЕЩАЕТСЯ эксплуатация ПК без действующего сертификата ФСБ России на версию СКЗИ «КриптоПро CSP» 4.0 КС1, входящую в состав комплекта поставки, согласно Формуляру МКЕЮ.00627-01 30 02 ФО!

ЗАПРЕЩАЕТСЯ эксплуатация ПК, укомплектованных иными версиями СКЗИ «КриптоПро CSP», кроме входящих в состав комплекта поставки, согласно Формуляру МКЕЮ.00627-01 30 02 ФО, а также иными СКЗИ!

2.7. В целях обеспечения равнопрочной защиты информации конфиденциального характера в корпоративной информационной системе (информационно-телекоммуникационной сети) рекомендуется использовать ПК с другими программными и аппаратно-программными комплексами «ЗАСТАВА» производства АО «ЭЛВИС-ПЛЮС», сертифицированные по одному и

[1] с учетом извещений об изменениях ЖТЯИ.00087-01.1-2016

тому же классу защищенности и укомплектованные СКЗИ «КриптоПро CSP» одного и того же класса защищенности.

Включение в информационную систему (информационно-телекоммуникационную сеть), укомплектованную программными и программно-аппаратными комплексами «ЗАСТАВА» производства АО «ЭЛВИС-ПЛЮС», сертифицированными по классу защищенности КСЗ, ПК без принятия дополнительных мер защиты НЕ ДОПУСКАЕТСЯ!

2.8. В качестве СКЗИ ПК обеспечивает дополнительно к функциям межсетевого экранирования 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 с использованием режима гаммирования (CTR) и зацепления блоков (CBC), 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 в соответствии с ГОСТ Р 34.10-2012;
- контроль целостности данных посредством вычисления значения их хэш-функции в соответствии с 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.

2.9. В качестве шифровального (криптографического) средства ПК удовлетворяет требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу защиты КС1.

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

3. ТРЕБОВАНИЯ К ИСПОЛЬЗУЕМЫМ АППАРАТНО-ПРОГРАММНЫМ ПЛАТФОРМАМ

3.1. ПК предназначен для работы на средствах вычислительной техники (СВТ) на серверных аппаратно-программных платформах архитектур ia32, x64 и функционирует в программных средах операционных систем (ОС) ALT Linux 6/7 платформы ia32, x64, в зависимости от комплектации [2].

[2] При эксплуатации ПК необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует ПК, определяются производителями ОС. Использование ОС, поддержка которых остановлена производителем, не допускается.

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

4.1. Общие требования

4.1.1. Выполнение в процессе эксплуатации ПК на должном уровне всех заявленных функции по защите информации, возможно исключительно при соблюдении необходимых организационно-распорядительных и технических мер защиты:

- по физическому размещению СВТ, на которые установлен ПК;
- по правильной инсталляции на эти СВТ и настройке системного и прикладного программного обеспечения (ПО), а также установке и настройке ПК и его составных частей;
- по реализации мероприятий по антивирусной защите и обеспечению свободной от вирусов программной среды данных СВТ;
- по обеспечению сохранности оборудования, целостности системного и прикладного ПО, физической целостности системных блоков указанных 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 СВТ, на которых размещается и используется ПК, эксплуатация указанных объектов и СВТ должна осуществляться в соответствии с требованиями руководящих документов ФСТЭК России по технической защите конфиденциальной информации[3].

4.1.3. Размещение СВТ, на которые установлен ПК в выделенных помещениях, предназначенных для ведения секретных переговоров, и(или) защищаемых помещениях, в которых присутствует речевая, акустическая и визуальная информация и(или) которые специально предназначены для проведения конфиденциальных мероприятий должно осуществляться согласно с требованиями нормативных документов ФСТЭК России, утвержденными решением от 23.05.1997 г. № 55 и приказом от 30.08.2002 г. № 282 Гостехкомиссии России.

---

[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.

4.1.4. Безопасность эксплуатации ПК обеспечивается при его установке на технические средства, для которых выполнены действующие в Российской Федерации требования по защите информации от утечки по техническим каналам, в том числе по каналу связи. При этом, если технические средства аттестованы на соответствие установленным требованиям по защите информации без учёта канала связи, то при подключении таких технических средств к каналам связи, выходящим за пределы контролируемой территории, для обеспечения защиты ключевой и цифровой открытой информации СВТ с установленным ПК по уровню $КС_Б$ от утечки по каналу связи достаточно, чтобы канал связи был реализован в виде:

- Радиоканалов GSM, GPRS, 3G/4G, Wi-Fi, а также других современных каналов мобильной или беспроводной связи, работающих с цифровой модуляцией штатного информационного сигнала;
- ВОЛС, уходящей за пределы контролируемой зоны;
- проводного канала связи с установкой в нем волоконно-оптической развязки.

4.2. Требования по размещению СВТ, на которые установлен ПК

4.2.1. Внутренняя планировка помещений, размещение в них и укомплектованность серверных аппаратно-программных платформ, на которых установлен ПК 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 несанционированного доступа (НСД) в помещения, в которых размещены СВТ с установленным 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 СВТ, на которых установлен ПК и(или) НСД к защищаемой информации.

4.2.3. Для хранения криптографических ключей на отчуждаемых носителях, нормативной и эксплуатационной документации, инсталляционных дискет помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными двумя 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 СВТ, на которых установлен 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, технические средства, на которых функционируют программные модули 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 ПК

4.3.1. Порядок обращения и эксплуатации ПК 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)», а также с эксплуатационной документацией к СКЗИ «КриптоПро CSP» 4.0 КС1:

— 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 криптографических ключей;

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

— Журнал учета обращения эталонных CD/DVD-носителей с дистрибутивами сертифицированных ФСБ России шифровальными средствами (СКЗИ).

4.4. Требования по обеспечению защиты СВТ, на которых установлен ПК от НСД

4.4.1. Защита СВТ, на которых размещен ПК, ключевой информации к нему, 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. При организации защиты информации конфиденциального характера в корпоративных информационных системах и(или) ИТКС с использованием ПК должны выполняться следующие требования по защите СВТ, на которых установлен ПК, от НСД:

— функции администратора СВТ, на которых установлен ПК, должны быть возложены исключительно на администраторов (офицеров) безопасности ПК;

— права доступа к СВТ, на которых установлен ПК, должны быть предоставлены исключительно администраторам (офицерам) безопасности ПК.

Запрещается предоставление штатным пользователям и(или) обслуживающему персоналу СВТ, на которых установлен ПК, привилегий администратора СВТ !

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.00627-01 30 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Формуляр, а также с технической документацией на СКЗИ «КриптоПро CSP» 4.0 КС1. Установка и эксплуатация ПК не должна противоречить требованиям указанных документов.

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

4.4.5. Установка, настройка и эксплуатация СКЗИ «КриптоПро CSP» 4.0 КС1, входящего в состав ПК, должна осуществляться в соответствии с требованиями технической документацией на указанное средство, перечисленной в документе «Средство криптографической защиты информации «КриптоПро CSP». Версия 4.0 1-Base. Формуляр. ЖТЯИ.00087-01 30 01, ООО «КРИПТО-ПРО», Москва, 2016 г».

4.4.6. Установка, настройка и эксплуатация ПК должны осуществляться в соответствии с требованиями настоящих Правил пользования и технической документацией:

— МКЕЮ.00627-01 30 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). формуляр.

— МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Электронное приложение к формуляру МКЕЮ.00627-01 30 01 ФО с указанием контрольных сумм исполняемых файлов.

— МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста;.

4.4.7. Настройка и конфигурирование ПК (назначение IP-адресов и портов интерфейсам, правил пакетной фильтрации, создание политики безопасности, выпуск пользовательских сертификатов, включая управление перечнем доверенных сертификатов, другие дополнительные настройки) должны осуществляться исключительно администратором (офицером) безопасности, который должен руководствоваться технической документацией на ПК, перечисленной в п. 4.4.5 и п. 4.4.6..

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

4.4.9. Аутентификация администратора (офицера) безопасности при осуществлении доступа к BIOS и/или ОС СВТ, на котором установлен ПК, основана на идентификаторе (имени) и пароле. Аутентификация штатного пользователя при осуществлении доступа к ОС СВТ, на котором установлен ПК основана на идентификаторе (имени) и пароле.

4.4.10. Идентификатор и пароль должны вводиться администратором (офицером) безопасности и(или) штатным пользователем собственноручно с использованием клавиатуры указанного СВТ. Ввод знаков пароля должен осуществляться методом, исключающим его отображение на экране монитора СВТ. Приступая к работе, Администратор (офицер) безопасности и(или) штатный пользователь обязан заменить идентификатор (имя) и пароль, установленные при инсталляции ПК на СВТ, на свои собственные, выработанные согласно рекомендациям настоящих Правил пользования.

4.4.11. Для выбора и смены идентификаторов (имени) и пароля для входа в ОС администратора (офицера) безопасности и(или) штатного пользователя СВТ, на котором установлен ПК, должна быть разработана политика назначения и смены паролей в соответствии со следующими правилами:

— имя администратора (офицера) безопасности и(или) штатного пользователя должно быть уникальным и не должно превышать 8 символов;

— имя администратора (офицера) безопасности и(или) штатного пользователя должно начинаться с буквы латинского алфавита (строчной или прописной), далее могут идти буквы латинского алфавита (строчные или прописные), цифры, символ «_» (подчеркивание) и символ «-» (дефис);

— длина пароля администратора (офицера) безопасности 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 4 символа;

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

4.4.12. Администратор (офицер) безопасности и(или) штатный пользователь СВТ, на котором установлен ПК, обязан хранить пароль доступа к СВТ, а также пароль доступа к ПК в тайне, и не имеет права сообщать указанные пароли никому.

4.4.13. При эксплуатации СВТ, на котором установлен ПК, КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ:

— оставлять без контроля СВТ, на котором эксплуатируется ПК, 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 т.п. 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.

4.4.14. В процессе эксплуатации ПК запрещается открытие и запуск исполнения полученных из общедоступных каналов связи файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX и т.д.) без проведения соответствующей проверки на предмет содержания в них программных закладок и вирусов.

4.4.15. Эксплуатации СВТ, на котором установлен ПК без перезагрузки в течение срока, превышающего 1 (Одни) сутки, не допускается.

4.4.16. 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».

Если СВТ, на котором установлен ПК, используется для хранения обработки и(или) передачи данных, не подлежащих обязательной защите в соответствии с законодательством Российской Федерации, то требования данного пункта носят рекомендательный характер.

4.5. Требования к размещению, установке и настройке ПК

4.5.1. На СВТ, предназначенном для размещения ПК, допускается размещение только одной ОС, предназначенной для функционирования устанавливаемого на данное СВТ ПК в соответствии с разделом 3.

4.5.2. В составе СВТ (ПЭВМ), предназначенном для эксплуатации ПК, должно использоваться только лицензионно «чистое» ПО, приобретенное либо у организации – производителя этого ПО, либо у ее официальных дилеров.

Любые изменения ПО, используемого в составе СВТ, на котором эксплуатируется ПК, должно осуществляться администратором (офицером) безопасности. Обновления безопасности используемого ПО, выпускаемые организациями – производителями, должны устанавливаться своевременно.

Примечание. При эксплуатации ПК необходимо учитывать, что порядок и сроки эксплуатации ОС, в среде которых они функционируют, определяются производителями ОС.

4.5.3. Установка ПК должна производиться на СВТ после установки и настройки СКЗИ «КриптоПро CSP» 4.0 КС1, проведенных в соответствии с требованиями технической документации на указанные шифровальные средства.

4.5.4. Для корректной работы СКЗИ «КриптоПро CSP» 4.0 КС1 требуется инициализация встроенного датчика случайных чисел (ДСЧ), для этого необходимо провести процедуру инициализации встроенного ДСЧ, использующего внешнюю гамму.

4.5.5. Процедура инициализации встроенного ДСЧ описана в Приложении 5 документа МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста. Перед установкой и настройкой СКЗИ «КриптоПро CSP» 4.0 КС1, и ПК, на средства СВТ (ПЭВМ), предназначенные для их эксплуатации, необходимо проверить ПО СВТ на отсутствие вредоносного программного кода (вирусов).

Должна быть организована постоянная антивирусная защита СВТ, на которые установлены и используются ПК. Рекомендуется использовать для указанных целей сертифицированное в Российской Федерации антивирусное ПО. Антивирусные базы данных должны регулярно обновляться.

4.5.6. На средствах СВТ, предназначенных для установки и эксплуатации ПК, должно быть **запрещено** размещение и(или) наличие средств разработки и отладки ПО.

4.5.7. Перед установкой ПК необходимо осуществить контроль целостности дистрибутива ПК при помощи утилиты cpverify.exe, входящей в состав СКЗИ «КриптоПро CSP».

4.5.8. В процессе установки ПК Администратором (офицером) безопасности должен осуществляться контроль целостности программных модулей, путем сравнения вычисляемых утилитой *icv_checker* хэш-сумм устанавливаемого ПО с эталонными значениями указанных сумм, поставляемых с инсталляционными комплектами ПК.

4.5.9. В ходе установки ПК администратором (офицером) безопасности должен быть сформирован список файлов программной части ПК, периодический контроль целостности которых должен осуществляться в процессе эксплуатации. К программной части ПК относятся неизменяемые программные модули ПК, эталонные контрольные суммы которых указаны в документе электронном приложении к документу МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1») Формуляр.и в файле *filelist.hash*. Кроме того, указанный список должен быть дополнен информационными файлами ПК, периодический контроль целостности которых предусмотрен политикой безопасности, установленной в корпоративной информационно-телекоммуникационной сети, в которой данный ПК эксплуатируется (далее – информационная часть), а файл *filelist.hash* соответствующим образом скорректирован.

Для всех программных модулей ПК, дополнительно включенных в список файлов ПК, периодический контроль целостности которых должен осуществляться в процессе его эксплуатации, а также для самого скорректированного файла *filelist.hash* Администратором (офицером) безопасности ПК в ходе установки должны быть вычислены и занесены в раздел 14 Формуляра МКЕЮ.00627-01 30 01 ФО эталонные контрольные суммы. Для вычисления эталонных контрольных сумм должна использоваться утилита *icv_writer* из состава ПК. Описание использования утилиты *icv_writer* находится в документе МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста.

4.5.10. В процессе эксплуатации СВТ с установленным ПК «Администратор (офицер) безопасности не реже одного раза в месяц должен осуществлять проверку целостности программной и информационной части ПК с помощью утилиты *icv_checker*, входящей в его состав и предназначенной для периодического тестирования работоспособности. Эталонные

контрольные суммы модулей ПК указаны в документе МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Электронное приложение к формуляру МКЕЮ.00627-01 30 01 ФО с указанием контрольных сумм исполняемых файлов», а эталонные контрольные суммы файлов, дополнительно внесенных в список контролируемых, - в разделе 14 Формуляра МКЕЮ.00627-01 30 02 ФО. Описание использования утилиты *icv_checker* находится в документе МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста.

При этом целостность скорректированного файла *filelist.hash* допустимо осуществлять только путем сравнения содержащегося в указанном файле списка контролируемых файлов ПК с эталоном, содержащемся в документе МКЕЮ.00627-01 30 01 ФО.

4.5.11. В процессе эксплуатации СВТ с установленным ПК администратором (офицером) безопасности также должна осуществляться периодическая проверка целостности программной среды функционирования СКЗИ «КриптоПро CSP» 4.0 КС1.

Проверка должна осуществляться в сроки и порядком, установленными технической документации на СКЗИ «КриптоПро CSP» 4.0 КС1.

4.5.12. Для исключения возможности влияния аппаратных и программных составляющих среды функционирования ПК на свойства и функционал СКЗИ, после установки ПК на СВТ Администратором (офицером) безопасности должны быть выполнены следующие действия:

— в BIOS СВТ должны быть определены установки, исключающие возможность загрузки ОС, отличной от инсталлированной на жестком диске, в том числе должна быть исключена возможность сетевой загрузки;

— вход в BIOS СВТ должен быть защищен паролем с длиной не менее 7 символов;

— средствами BIOS СВТ должна быть исключена возможность работы на компьютере, если во время его начальной загрузки не проходят встроенные тесты;

— должны быть отключены сетевые протоколы, которые не используются на данной СВТ, и запрещен доступ к не используемым TCP- и UDP-портам;

— должна быть исключена возможность удаленного управления ОС;

— должны быть приняты меры, максимально ограничивающие доступ пользователей к системным ресурсам используемой ОС. А именно: к системным файлам и каталогам, к временным

файлам, к системным журналам, к файлам подкачки, к кэшируемой информации (пароли и т. п.), к любой отладочной информации;

— проведено опечатывание системного блока ПЭВМ с установленным ПК, исключающее возможность бесконтрольного изменения аппаратной части СВТ и подключения внешних устройств.

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

— модернизация ОС компьютера, на котором установлен ПК, включая установку штатных обновлений;

— добавление и(или) отключение отдельных сервисов ОС по отношению к состоянию ОС на момент установки ПК;

— установка дополнительных программных приложений;

— 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 ПК по защите информации и является основанием для отказа в сервисе технического сопровождения и поддержки ПК.

4.6. Требования по криптографической защите

4.6.1. При эксплуатации ПК должны соблюдаться требования к криптографической защите, изложенные в технической документации к СКЗИ «КриптоПро CSP» 4.0 КС1.

4.7. Требования к обращению с ключевыми документами

4.7.1. Требования по обращению с криптографическими ключами (включая цифровые сертификаты) к СКЗИ «КриптоПро CSP» 4.0 КС1, используемого в составе ПК, регламентируются технической документацией к указанным СКЗИ.

4.7.2. Криптографическими ключами для ПК являются:

— открытые и закрытые ключи сформированные с использованием алгоритма ГОСТ Р 34.10-2012 и соответствующий им сертификат открытого ключа в формате X.509v3;

— корневые и промежуточные сертификаты открытых ключей удостоверяющих центров (УЦ) в формате X.509v3.

4.7.3. Криптографические ключи для ПК предназначены для взаимной аутентификации партнёров межсетевого взаимодействия и установления защищённых соединений между ними.

4.7.4. Ключевая информация, используемая ПК является конфиденциальной.

4.7.5. Срок действия криптографических ключей, используемого в составе ПК, не должен превышать 1 год 3 месяца.

Использование в ПК криптографических ключей срок действия которых истек, ЗАПРЕЩЕНО !

4.7.6. В качестве носителей ключевой информации ПК должен использовать ключевые носители, поддерживаемые СКЗИ «КриптоПро CSP» 4.0 КС1, согласно технической документации на указанные средства или выполненные в соответствии со спецификацией PKCS#11 v2.10 и выше и с учетом ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и прошедшие сертификацию установленным образом.

Использование в ПК носителей ключевой информации, не рекомендованных технической документацией к СКЗИ «КриптоПро CSP» 4.0 КС1 и не имеющих действующего сертификата ФСБ России, ЗАПРЕЩАЕТСЯ !

4.7.7. Формирование открытых и закрытых ключей для ПК должно выполняется

— с использованием УЦ «КриптоПро УЦ» по классу защиты КС1 и выше;

— на СВТ ПК, с использованием функционала СКЗИ «КриптоПро CSP» 4.0 КС1;

— на функциональных ключевых носителях (ФКН), с использованием PKCS#11 библиотек производителей ФКН.

4.7.8. Формирование и управление сертификатами открытых ключей для ПК производится УЦ. В качестве УЦ может выступать УЦ «КриптоПро УЦ» или другие сертифицированные ФСБ России УЦ, обеспечивающие выполнение функций доверенного обращения с сертификатами.

4.7.9. Добавление и удаление сертификатов открытых ключей формата в ПК должны производиться Администратором (офицером) безопасности ПК в соответствии с п. 3.4.4 «регистрация и удаление Сертификата» документа МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста.

4.7.10. Аутентификация Администратора (офицера) безопасности ПК при доступе к ключевой информации на ключевых носителях, осуществляется на основе ввода паролей (PIN-кода для ФКН).

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

4.7.11. Доставка криптографических ключей должна осуществляться на носителе ключевой информации или иным доверенным способом.

4.7.12. Криптографические ключи на ключевых носителях, сроки действия которых истекли, уничтожаются.

4.7.13. Уничтожение ключей производится путем переформатирования (очистки) ключевых носителей средствами СКЗИ «КриптоПро CSP» 4.0 КС1 или Администратор (офицер) безопасности ПК должен использовать процедуру удаления сертификатов «Удаление сертификата» документа МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

4.7.14. Принятая в корпоративной ИТКС политика безопасности должна предусматривать возможность получения ПК актуальных списков аннулированных (отозванных) сертификатов CRL формата CRLv2, выпущенных УЦ.

Примечание. Несвоевременное получение актуального списка аннулированных сертификатов CRL может привести к невозможности установления защищенных соединений с абонентами корпоративной ИТКС, использующими цифровые сертификаты, выпущенных УЦ, формирующим данный CRL.

4.8. Действия при компрометации ключей

4.8.1. В случае явной компрометации закрытого ключа, используемого для организации защищенного соединения, к которым относятся случаи:

- 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 обработки информации подлежащей защите на скомпрометированных ключах. Администратор (офицер) безопасности должен немедленно известить УЦ, выпустивший ключ, о факте компрометации.

4.8.2. В случае неявной компрометации закрытого ключа, используемого для организации защищенного соединения, к которым относятся случаи:

— 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).

По факту компрометации должно быть проведено служебное расследование.

4.8.3. Скомпрометированные ключи, используемые для организации защищенного соединения, выводятся из действия и уничтожаются согласно регламенту уничтожения, определенному в документации на СКЗИ «КриптоПро CSP» 4.0 КС1 (см. п. 4.2.4 «Уничтожение ключей на ключевых носителях» документа ЖТЯИ.00087-02 95 01 «Средство Криптографической Защиты Информации КриптоПро CSP версия 4.0 КС1 1-Base. Правила пользования.»).

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

4.8.5. Для организации защищенного соединения необходимо выпустить новую ключевую информацию и импортировать ее (см. подраздел 3.4 «Регистрация сертификата» документа МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста.»).

4.9. Требования к политике безопасности для ПК

4.9.1. Для эксплуатации ПК должен быть настроен Администратором (офицером) безопасности ПК в соответствии требованиями технической документации, перечисленной в п. 4.4.5 и п. 4.4.6.

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 «КриптоПро CSP» 4.0 КС1. Поэтому при настройке, конфигурировании и создании политики безопасности Администратор (офицер) 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 цифровое 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***», или «***NULL***»;
- 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) Значение «***NULL***» атрибута ***cipher*** в структуре ***proto_esp*** может быть использовано, только в случае, когда требуется обеспечить только аутентификацию передаваемых данных без обеспечения их конфиденциальности. **При указании атрибута «NULL» шифрование информации не производится!**

2) 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***.

3) 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 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[4]. 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 факта что, локальная политика безопасности (ЛПБ) не соответствует действующей в корпоративной информационно-телекоммуникационной ГПБ, Администратор (офицер) безопасности ПК сети должен принять меры к незамедлительному принудительному восстановлению ЛПБ.

4.9.5. До начала эксплуатации ПК Администратором (офицером)безопасности ПК должен быть отключен режим IKEv1 в настройках ПК (см. Параметры протокола IKE документа МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста.»).

---

[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.

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

4.10. Требования к процедуре обновления

4.10.1. Для обновления ПО ПК Заказчик (Пользователь) должен самостоятельно получить на предприятии-поставщике (изготовителе) ПК согласно договору на поставку и/или техническую поддержку дистрибутив обновления на CD 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.

4.10.2. 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[5].

Установка нового сертифицированного обновления ПК должна производиться только с использованием дистрибутивов на CD, доставленных (полученных) по доверенному каналу.

Процедура автоматизированного обновления ПК осуществляется из центра управления политиками ПК МКЕЮ.00631-01 «Программный комплекс «VPN/FW ЗАСТАВА-Управление», версия 6 КС3» («VPN/FW ЗАСТАВА-Управление», версия 6 КС3») (исполнение ZM-WS64-VO-03) производства АО «ЭЛВИС-ПЛЮС».

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

4.10.3. Доставка нового сертифицированного обновления ПК в автоматическом режиме на СВТ, 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.

---

[5] «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденного 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.

Для организации такого канала допускается использование ПК (в том числе, и обновляемых). При этом используемые ПК должны быть укомплектованы, установлены, настроены и эксплуатироваться согласно настоящему документу и Формуляру МКЕЮ.00627-01 30 01. Настройки используемых ПК должны соответствовать требованиям подраздела 4.9 настоящих Правил пользования и обеспечивать аутентификацию и целостность передаваемых данных.

4.10.4. Для завершения процедуры обновления ПК Администратор (офицер) безопасности должен скорректировать список файлов программной и информационной части ПК и ОС СВТ, на которой этот ПК устанавливается, периодический контроль целостности которых должен осуществляться в процессе эксплуатации в соответствии с порядком, описанном в п. 4.5.9.

4.10.5. По завершении процедуры обновления Администратор (офицер) безопасности должен обеспечить изменение формуляра ПК путем его корректировки согласно требованиям предписания на внесение изменений или замены на новый, полученный одновременно с дистрибутивом нового обновления ПК.

4.11. Перечень событий, при возникновении которых эксплуатация ПК запрещена

Эксплуатация ПК запрещена при наступлении следующих событий:

— нарушение печати системного блока компьютера с установленным ПК;

— нарушение целостности ПК;

— сбой в работе ПК;

— компрометация ключей.

При наступлении любого из перечисленных событий Администратор (офицер) ПК должен: приостановить эксплуатацию ПК, выявить причины инцидента, а также устранить негативные последствия посредством принятия мер в соответствии с п. 4.12 «Нештатные ситуации» настоящих Правил пользования используя документ МКЕЮ.00627-01 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 КС1» («VPN/FW «ЗАСТАВА-Офис», версия 6 КС1»). Руководство системного программиста.»;

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

4.12. 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 (офицера) 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 безопасности: – Останавливает СВТ. – Администратор (офицер) безопасности 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. – Администратор (офицер) безопасности 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 или пользователь уничтожает всю ключевую информацию с носителей, находящихся в контейнере.
2.	Компрометация ключей, используемых для организации защищенного соединения.	Порядок действий при компрометации ключей описан в подразделе 4.8«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 разделе 4.7 «Требования к обращению с ключевыми документами» и в документации на СКЗИ ЖТЯИ.00087-01 «КриптоПро CSP» версия 4.0 1-Base (см. п. 4.2.4 «Уничтожение ключей на ключевых носителях» документа ЖТЯИ.00087-02 95 01 Средство Криптографической Защиты Информации КриптоПро CSP версия 4.0 КС1 1-Base Правила пользования.).
4.	Отказы и сбои в работе аппаратной части ПК.	При отказах и сбоях в работе аппаратной части необходимо остановить работу, 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 безопасности должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства защиты от НСД.
6.	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в ПО.	При отказах и сбоях в работе программных средств, вследствие не выявленных ранее ошибок в ПО, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и обратиться в

№п/п	Нештатная ситуация	Действия Администратора безопасности
		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 безопасности обязан произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы ПК в установленном порядке.
8.	Нарушение печати системного блока СВТ с установленным ПК.	При нарушении целостности печати системного блока СВТ с установленным ПК, Администратор 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
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
SA	-	Security Association Защищенное соединение в контексте протоколов IPsec и IKE
TCP	-	Transmission control protocol Сетевой протокол транспортного уровня (с гарантированной доставкой) в IP-сетях
VPN	-	Virtual Private Network; Виртуальная частная сеть
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
ПК	-	Программный комплекс
ПО	-	Программное обеспечение
ПЭВМ	-	Персональная электронная вычислительная машина
ПЭМИН	-	Побочные электромагнитные излучения и наводки
СВТ	-	Средство вычислительной техники
СКЗИ	-	Средство криптографической защиты информации
УЦ	-	Удостоверяющий центр
ФКН	-	Функциональный ключевой носитель
ФСБ России	-	Федеральная служба безопасности
ФСТЭК России	-	Федеральная служба по таможенному и экспортному контролю

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	-	-	29	МКЕЮ.0077	-		21.09.2021