УТВЕРЖДЕН

МКЕЮ.00631-01 91 01-ЛУ

«Программный комплекс
«VPN/FW «ЗАСТАВА-Управление», версия 6 КС3»

(«VPN/FW «ЗАСТАВА-Управление», версия 6 КС3»)
(исполнение ZM-WS64-VO-03)

Правила пользования

МКЕЮ.00631-01 91 01

Листов 31

Инв.№	Подп. и дата	Взам. инв.	Инв.№	Подп. и дата
7488				

2021

СОДЕРЖАНИЕ

1. АННОТАЦИЯ

Настоящий документ представляет собой Правила пользования на «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03) (далее – ПК) МКЕЮ.00631-01.

Инструкции Администраторам безопасности ПК и пользователям различных автоматизированных систем, использующих средство криптографической защиты информации (СКЗИ) ПК, должны разрабатываться с учетом требований настоящего документа.

2. НАЗНАЧЕНИЕ ПК. УСЛОВИЯ ЭКСПЛУАТАЦИИ

2.1. ПК является центром управления и предназначен для удаленного администрирования программных и аппаратно-программных СКЗИ до класса защиты КС3 и межсетевых экранов (МЭ), производимых АО «ЭЛВИС-ПЛЮС».

2.2. В качестве центра управления политиками – ПК обеспечивает:

— задание глобальной политики безопасности (ГПБ) с описанием топологии информационной телекоммуникационной системы и заданием правил шифрования/фильтрации (правил разграничения доступа);

— формирование локальных политик безопасности (ЛПБ) для управляемых СКЗИ и МЭ;

— доставку политики безопасности до управляемых СКЗИ и МЭ по защищенному каналу;

— мониторинг состояния управляемых СКЗИ и МЭ;

— удаленное обновление программного обеспечения (ПО) управляемых СКЗИ и МЭ.

2.3. В состав ПК входит агент безопасности – ПО «ЗАСТАВА-Офис», версия 6» (далее – «ЗАСТАВА-Офис»).

2.4. ПК обеспечивает криптографическую защиту служебной информации (ЛПБ, команд мониторинга и управления) при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны.

2.5. ПК обеспечивает контроль и фильтрацию сетевых пакетов в соответствии с заданными правилами, а также защиту служебной информации (ЛПБ, команд мониторинга и управления), передаваемой по каналам связи, криптографическими методами.

2.6. В состав ПК входит СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 производства ООО «КРИПТО-ПРО» (г. Москва).

2.7. В состав ПК входит средство защиты информации (СЗИ) «Secure Pack Rus» Версия 3.0 ЖТЯИ.00106.

2.8. Реализация криптографических функций шифрования, контроля целостности данных, имитозащиты данных, аутентификации абонентов на основе процедуры Диффи-Хеллмана осуществляется в ПК применением СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089.

2.9. Эксплуатация ПК с входящим в его состав СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 должна осуществляться в соответствии с требованиями технической и эксплуатационной документации на указанное СКЗИ.

2.10. Эксплуатация ПК, а также входящего в его состав сертифицированного СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, должна проводиться согласно разделу V документа

«Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005)».

Эксплуатация ПК, не укомплектованных СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, или укомплектованных иными СКЗИ, ЗАПРЕЩАЕТСЯ !

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

2.12. Для включения в информационную систему (ИТКС), укомплектованную СКЗИ (в том числе и ПК), сертифицированными по классу защищенности КС3, иных СКЗИ, сертифицированных по классам защищенности КС1 и/или КС2, необходимо принятие дополнительных технических и/или организационных мер защиты, достаточность которых должна быть подтверждена организацией имеющей лицензию на разработку защищенных с использованием шифровальных (криптографических) средств информационных и/или телекоммуникационных систем[1].

2.13. 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 организационных мер, понижает класс защищенности информационной системы (ИТКС) по минимальному классу защищенности применяемых СКЗИ КС1 или КС2.

Включение ПК в ИТКС, укомплектованную программными и аппаратно-программными СКЗИ, производимыми АО «ЭЛВИС-ПЛЮС», сертифицированными по классу защищенности КС1 и КС2, без принятия дополнительных мер защиты НЕ ДОПУСКАЕТСЯ !

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

- конфиденциальность передаваемой в корпоративной ИТКС служебной информации (ЛПБ, команд управления), за счет ее шифрования согласно ГОСТ 28147-89;
- защиту доступа к служебной информации (ЛПБ, команд управления) за счет использования протоколов двухсторонней криптографической аутентификации при

[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.

установлении соединений на базе протоколов IKEv2 с использованием алгоритмов подписи в соответствии с ГОСТ Р 34.10-2012;

— контроль целостности данных на основе применения ГОСТ Р 34.11-2012;

— имитозащиту данных на основе применения ГОСТ 28147-89 в режиме имитовставки;

— поддержку схемы открытого распределения ключей Диффи-Хеллмана на основе алгоритмов ГОСТ Р 34.10-2012 VKO в 256-битном режиме.

2.15. ПК удовлетворяет документу «Требования к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классам защиты КС3.

2.16. 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 аппаратно-программных платформах x64 и, согласно эксплуатационной документации МКЕЮ.00631-01, функционирует в программных средах:

— Операционная система (ОС) Windows Server 2012 R2 64-бит;

— ОС Windows Server 2016 64-бит.

3.2. Консоль управления ПК функционирует в программных средах:

— ОС Windows Server 2012 R2 64-бит;

— ОС Windows Server 2016 64-бит;

— ОС Windows 8.1 64-бит;

— ОС Windows 10 64-бит.

3.3. ПО «ЗАСТАВА-Офис» функционирует в программных средах:

— ОС Windows Server 2012 R2 64-бит;

— ОС Windows Server 2016 64-бит[2].

3.4. ПК должен использоваться с СЗИ Secure Pack Rus ЖТЯИ.00106-01, совместно с СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089.

3.5. ПК, в соответствии с формулярами ЖТЯИ.00089-03 30 01 на СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, должен использовать аппаратно-программный модуль доверенной загрузки (АПМДЗ) из списка:

— Программно-аппаратный комплекс (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);

— СЗИ от НСД «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013, 4012-006-11443195-2005 ТУ;

— АПМДЗ-У М-526Б (КРИПТОН-ЗАМОК/У) КБДЖ.468243.067 ТУ, М-526Е1 (КРИПТОН-ЗАМОК/Е) КБДЖ.468243.090 ТУ;

— АПМДЗ «МАКСИМ-М1».

---

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

3.6. Эксплуатация ПК без действующего сертификата ФСБ России на средства защиты от НСД, перечисленные в подразделе 3.5, ЗАПРЕЩАЕТСЯ !

4. СОСТАВ ПК

4.1. ПК выполнено в следующем составе:

— Сервер управления;

— Консоль управления;

— Утилита командной строки;

— Агент безопасности – ПО «ЗАСТАВА-Офис»;

— СЗИ «Secure Pack Rus» Версия 3.0 ЖТЯИ.00106;

— СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089;

— АПМДЗ.

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

5.1. Общие требования

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

- по физическому размещению средств вычислительной техники (СВТ), на которые установлен ПК;
- по правильной установке и настройке системного и прикладного ПО, а также ПК и его составных частей на СВТ;
- по обеспечению защиты СВТ от НСД;
- 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 СВТ.

5.1.2. 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:

- 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.

5.2. Требования по размещению СВТ

5.2.1. Внутренняя планировка помещений, размещение в них и укомплектованность автоматизированных рабочих мест (АРМ), СВТ, на которых установлены ПК, должны обеспечивать пользователям ПК сохранность доверенных им конфиденциальных сведений, шифровальных (криптографических) средств и ключевой информации к ним.

5.2.2. Должны быть приняты организационно-технические меры, направленные на исключение 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.

5.2.3. Для хранения криптографических ключей, нормативной и эксплуатационной документации, инсталляционных дисков 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.

5.2.4. 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 вспомогательным техническим средствам и системам по защите от утечки информации по каналам побочных электромагнитных излучений и наводок, в соответствии с категорией выделенного помещения.

5.3. Организационно-распорядительные меры обеспечения безопасности информации

5.3.1. Порядок обращения и эксплуатации ПК 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)», а также эксплуатационной документацией к СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089:

- Инструкция по обращению с сертифицированными ФСБ России шифровальными средствами (СКЗИ) на предприятии;
- Инструкция по порядку доступа в помещения, предназначенные для размещения сертифицированных ФСБ России шифровальных средств (СКЗИ);
- Журнал учета сертифицированных ФСБ России шифровальных средств (СКЗИ) и тестовых ключей;
- Журнал регистрации администраторов безопасности СВТ, на которых установлены сертифицированные ФСБ России шифровальные средства (СКЗИ);
- Журнал учета обращения эталонных CD-дисков с дистрибутивами СКЗИ.

5.4. Требования по обеспечению защиты СВТ от НСД

5.4.1. 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.

5.4.2. При организации защиты информации конфиденциального характера в корпоративных информационных систем и(или) ИТКС с использованием ПК должны выполняться следующие требования по защите СВТ, на которых установлен ПК, от НСД:

- функции администратора ОС СВТ, на которых установлен ПК, должны быть возложены исключительно на Администратора безопасности ПК;
- права доступа к СВТ, на которых установлены ПК, должны быть предоставлены исключительно Администратору безопасности ПК.

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

Запрещается предоставление обслуживающему персоналу защищенных СВТ, на которых установлен ПК, привилегий Администратора ОС!

5.4.4. Прежде чем приступить к работе Администратор безопасности ПК должен ознакомиться с технической документацией на ПК в полном объеме, согласно документу МКЕЮ.00631-01 30 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Формуляр», а также с технической документацией на СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, а также технической документацией на АПМДЗ, в зависимости от выбранного типа из списка подраздела 3.5. Установка и эксплуатация ПК не должна противоречить требованиям указанных документов.

5.4.5. Установка и эксплуатация ПК на СВТ должна производиться только с дистрибутивов, полученных доверенным образом.

5.4.6. Установка, настройка и эксплуатация СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, входящего в состав ПК, должны осуществляться в соответствии с требованиями технической документацией на указанное средство.

5.4.7. Установка, настройка и эксплуатация ПК должны осуществляться в соответствии с требованиями настоящих Правил пользования и документами МКЕЮ.00631-01 30 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Формуляр».

5.4.8. Настройка и конфигурирование ПК (назначение IP-адресов и интерфейсов, правил пакетной фильтрации, создание политики безопасности, импорт пользовательских сертификатов, включая управление перечнем доверенных сертификатов, другие дополнительные настройки) должны осуществлять исключительно Администратором безопасности ПК, который должен руководствоваться технической документацией на ПК, перечисленной п. 5.4.7.

5.4.9. 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. 5.4.7.

5.4.10. Аутентификация Администратора безопасности ПК осуществляется с использованием функционала АПМДЗ, в зависимости от выбранного типа из списка, см. подраздел 3.5.

Аутентификация Администратора безопасности ПК с использованием функционала АПМДЗ должна осуществляться согласно технической документации (Руководству пользователя) на средства защиты от НСД, которыми укомплектован ПК.

5.4.11. Для выбора и смены идентификаторов (имени) и пароля для входа в ОС Администратора безопасности ПК должна быть разработана политика назначения и смены паролей в соответствии со следующими правилами:

- имя Администратора безопасности ПК должно быть уникальным и не должно превышать 8 символов;
- имя Администратора безопасности ПК 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 безопасности ПК 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.

5.4.12. Администратор безопасности ПК обязан хранить пароль доступа к СВТ, а также пароль доступа к ПК в тайне, и не имеет права сообщать указанные пароли никому.

5.4.13. 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 безопасности ПК 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 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03)), закрытые криптографические ключи.**

5.4.14. В процессе эксплуатации ПК **запрещается** открытие и запуск на исполнение 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.

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

5.4.16. Для ограничения возможности влияния аппаратных компонентов СВТ на функционирование СКЗИ необходимо проведение исследований на ПО BIOS СВТ, на которых

установлено СКЗИ, в соответствии с документом «Временные требования 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.

5.5. Требования к размещению, установке и настройке ПК

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

5.5.2. В составе СВТ, предназначенного 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 безопасности ПК. 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.

5.5.3. Дистрибутив ПК должен устанавливаться на СВТ после установки и настройки СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 в соответствии с требованиями технической документации на указанное СКЗИ.

5.5.4. Перед установкой и настройкой СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 и ПК, на СВТ, предназначенные для их эксплуатации, необходимо проверить ПО СВТ на отсутствие вредоносного программного кода (вирусов).

ПК должен эксплуатироваться со средствами антивирусной защиты, сертифицированными ФСБ России. В случае их отсутствия рекомендуется, по возможности, использовать существующие антивирусные средства защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

Необходимо регулярно обновлять антивирусные базы.

5.5.5. Системные блоки СВТ, предназначенные для эксплуатации ПК, должны быть оборудованы средствами контроля за вскрытием и/или опечатываться специально выделенной для этой цели печатью.

Должен быть обеспечен периодический контроль целостности печати со стороны Администратора безопасности ПК.

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

5.5.7. Установка дистрибутива ПК должна производиться Администратором безопасности ПК.

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

5.5.9. После установки ПК Администратором безопасности ПК должен быть проверен шаблон контроля целостности (автоматически формируемый файл filelist.hash в рабочей директории ПК). Шаблон контроля целостности должен содержать неизменяемые программные модули, эталонные контрольные суммы которых указаны в документе МКЕЮ.00631-01 93 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Электронное приложение к формуляру МКЕЮ.00631-01 30 01 с указанием контрольных сумм исполняемых файлов». Шаблон контроля целостности может быть дополнен файлами ОС, периодический контроль целостности которых предусмотрен политикой безопасности, установленной на предприятии, где эксплуатируется ПК.

Корректировка шаблона контроля целостности проводится Администратором безопасности ПК применением утилиты *icv_writer*. Описание использования утилиты *icv_writer* находится в подразделе 5.5 документа МКЕЮ.00631-01 32 02 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). ПО «ЗАСТАВА-Офис. Руководство системного программиста».

Контрольная сумма скорректированного шаблона контроля целостности вычисленная Администратором безопасности ПК утилитой *icv_writer* вносится в раздел 14 документа МКЕЮ.00631-01 30 01 ФО Формуляр, как эталон шаблона контроля целостности ПК.

5.5.10. Шаблон контроля целостности ПК (файл filelist.hash), и файлы ОС, контроль целостности которых рекомендован технической документацией (Руководством пользователя), используемого в составе ПК АПМДЗ, должны быть включены в шаблон контроля целостности АПМДЗ.

5.5.11. Если клиентская часть (консоль управления) ПК установлена на отдельном АРМ (удаленно от серверной платформы, на которой размещен сервер управления), то должны быть предприняты меры, обеспечивающие защиту информации, циркулирующей между серверной и клиентской частями.

Внутренняя линия связи между серверной платформой и удаленной консолью ПК должна находиться в пределах контролируемой зоны объекта информатизации, на котором указанные СВТ размещаются. Способ прокладки линии связи должен обеспечивать возможность ее визуального контроля и осмотра в целях защиты от несанкционированных подключений.

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

5.5.12. В процессе установки ПК Администратором безопасности ПК должна быть проведена настройка контроля сроков действия закрытых криптографических ключей, предназначенных для взаимной аутентификации партнёров межсетевого взаимодействия и установления защищённых соединений между ними.

Настройка контроля сроков действия закрытых ключей осуществляется путем включения режима усиленного контроля использования криптографических ключей СКЗИ через вкладку «Безопасность» контрольной панели СКЗИ «КриптоПро CSP» 4.0 R4 3-Base, входящего в состав ПК, в соответствии с документацией ЖТЯИ.00089-03 95 01 и ЖТЯИ.00089-03 91 02 на указанное средство.

При этом значение параметра **ControlKeyTimeValidity**, входящего в реестр Windows **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CryptoPro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity,** должно быть задано равным числу **2**.

5.5.13. В процессе установки ПК должна быть проведена настройка СЗИ «Secure Pack Rus» Версия 3.0 ЖТЯИ.00106 в части политик управления приложениями (AppLocker) согласно таблице (см. Таблица 1).

Таблица 1 - Правила политики управления приложениями

Действие	Пользователь	Имя	Условие	Исключение
Запретить	Office	%PROGRAMFILES%\Microsoft SQL Server*	Путь	
Запретить	Office	%PROGRAMFILES%\ELVIS+\ZASTAVA Management*	Путь	
Запретить	Manager	%PROGRAMFILES%\ELVIS+\ZASTAVA Office*	Путь	
Разрешить	Все	Все файлы в папке Windows	Путь	
Разрешить	Все	Все файлы в папке Program Files	Путь	Да, кроме папок в %PROGRAMFILES%\ELVIS+\
Разрешить	Администраторы	Все файлы	Путь	Да, кроме папок %PROGRAMFILES%\ELVIS+\
Разрешить	Office	%PROGRAMFILES%\ELVIS+\ZASTAVA Office*	Путь	
Разрешить	Office	%PROGRAMFILES%\CryptoPro\CSP*	Путь	
Разрешить	Manager	%PROGRAMFILES%\ELVIS+\ZASTAVA Management*	Путь	
Разрешить	Manager	%PROGRAMFILES%\Microsoft SQL Server*	Путь	

В свойствах AppLocker во вкладке «**Применение»** включить **«Правила исполняемых файлов»** и включить флаг «**Настроено**» и выставить значение из выпадающего списка «**Принудительное применение правил**».

Через оснастку ОС «**Службы**» стартовать службу «**Удостоверение приложений**» (Application Identity) и изменить тип запуска службы на «**Автоматически**».

5.5.14. Перед эксплуатацией ПК должно быть обеспечено выполнение следующих требований по установке и конфигурированию ПК:

- Установка политики по умолчанию на объекте ГПБ, который представляет объект ПК в топологии, равной **«Блокировать все»**;
- Запрет на создание правил фильтрации, разрешающих доступ к неиспользуемым или небезопасным сетевым службам ОС СВТ, на котором установлен ПК;
- Исключение возможности управления (настройки, администрирования) ПК по незащищенному каналу связи;
- Обновление файлов ОС СВТ (перед установкой ПК) путем использования пакетов «заплат» (Service Pack, Patches и др.), указанных в эксплуатационной документации на ПК и документации СЗИ Secure Pack Rus ЖТЯИ.00106-01 в исполнении 7, функционирующее совместно СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089.

5.5.15. В процессе эксплуатации СВТ с установленным ПК Администратор безопасности ПК не реже одного раза в месяц должен осуществлять проверку шаблона контроля целостности (файла filelist.hash) с помощью утилиты icv_checker. Эталонная контрольная сумма указана в разделе 5 документа МКЕЮ.00631-01 30 01 ФО Формуляр. Описание использования утилиты icv_writer находится в подраздела 5.5 документа МКЕЮ.00631-01 32 02 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). ПО «ЗАСТАВА-Офис». Руководство системного программиста».

5.5.16. В процессе эксплуатации СВТ с установленным ПК Администратором безопасности ПК должны осуществляться действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, а также его окружения в соответствии с документацией на него.

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

- в ПО BIOS СВТ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске;
- вход в BIOS СВТ должен быть защищен паролем с длиной не менее 6 символов;

- средствами BIOS должна быть исключена возможность работы на компьютере, если во время его начальной загрузки не проходят встроенные тесты;
- средствами BIOS должна быть исключена возможность отключения пользователями PCI-устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI-разъемах;
- должны быть отключены сетевые протоколы, которые не используются на данном СВТ, и запрещен доступ к неиспользуемым 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 системному реестру, 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;
- в СФ должна быть деактивирована системная служба Windows Error Reporting путем присвоения значение «1» параметру Disabled в следующих ключах реестра:
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting,
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting;
- в СФ, должна быть отключена функциональность стороннего ПО для отправки дампов памяти;
- в СФ, должно быть отключено удалённое управление рабочим столом;
- в настройках программно-аппаратных средств защиты от НСД должно быть установлено ограничение времени на его инициализацию;
- проведено опечатывание системного блока компьютера с установленным ПК, исключающее возможность бесконтрольного изменения аппаратной части СВТ и подключения внешних устройств.

5.5.18. В процессе эксплуатации ПК запрещается несанкционированное Администратором безопасности ПК изменение среды функционирования ПК, а именно:

- модернизация ОС компьютера, на котором установлен ПК;
- 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 по защите информации и является основанием для отказа в сервисе технического сопровождения и поддержки ПК.

5.6. Требования по криптографической защите

5.6.1. При эксплуатации ПК должны соблюдаться требования по криптографической защите, изложенные в технической документации к СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089.

5.7. Требования к обращению с криптографическими ключами

5.7.1. Требования по обращению с криптографическими ключами ПК регламентируются технической документацией к СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 и регламентом используемого Удостоверяющего Центра (УЦ).

5.7.2. 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 УЦ в формате X.509v3.

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

5.7.4. Ключевая информация, используемая ПК является конфиденциальной.

5.7.5. Срок действия криптографических ключей **не должен превышать 1 год 3 месяца.**

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

5.7.6. В процессе эксплуатации СВТ с установленным ПК, Администратором безопасности ПК должна быть проведена настройка контроля сроков действия долговременных ключей в ПО СКЗИ ЖТЯИ.00089 «КриптоПро CSP» 4.0 R4 3-Base, согласно требованиям п. 5.5.12.

5.7.7. В качестве носителей ключевой информации могут использоваться ключевые носители, поддерживаемые СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, согласно технической документации на указанные средства или функциональные ключевые носители (далее – ФКН), выполненные в соответствии со спецификацией PKCS#11 не ниже v2.10, и, прошедшие сертификацию установленным образом.

Использование в ПК носителей ключевой информации, не рекомендованных технической документацией к СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, и/или, **не имеющих действующего сертификата ФСБ России, ЗАПРЕЩЕНО !**

5.7.8. Формирование открытых и закрытых ключей для ПК может выполняться:

— с использованием УЦ «КриптоПро УЦ» класс защиты КС3;

— на СВТ ПК, с использованием функционала СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089, входящего в ПК;

— на ФКН, с использованием PKCS#11 библиотек производителей ФКН.

5.7.9. Формирование открытых и закрытых ключей на СВТ ПК и на ФКН, создание PKCS#10 запросов на издание сертификатов открытых ключей в ПК должны производиться Администратором безопасности ПК в соответствии с подразделом 4.4 «Регистрация сертификатов» документа МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста».

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

5.7.11. Добавление и удаление сертификатов открытых ключей в ПК должны производиться Администратором безопасности ПК в соответствии с подразделом 4.4 «Регистрация сертификатов» документа МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста».

5.7.12. Аутентификация Администратора 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.

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

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

5.7.15. Уничтожение ключей производится путем переформатирования (очистки) ключевых носителей средствами СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 или

Администратор безопасности ПК должен использовать процедуру удаления сертификатов (см. п. 3.4.4.2 «Удаление сертификата» документа МКЕЮ.00631-01 32 02 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). ПО «ЗАСТАВА-Офис». Руководство системного программиста», после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

5.7.16. Принятая в корпоративной ИТКС политика безопасности должна предусматривать возможность получения агентом безопасности ПО «ЗАСТАВА-Офис», из состава 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.

5.8. Действия при компрометации ключей

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

— потеря ключевого носителя;

— потеря ключевого носителя с последующим обнаружением;

— увольнение (смена) Администратора безопасности ПК, имевшего доступ к ключевой информации;

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

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

5.8.2. 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).

По факту компрометации должно быть проведено служебное расследование.

5.8.1. Скомпрометированные ключи, используемые для организации защищенного соединения, выводятся из действия и уничтожаются согласно регламенту уничтожения,

определенному в документации на СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 (см. п. «Уничтожение ключей на ключевых носителях» документа ЖТЯИ.00089-01 95 01 СКЗИ «КриптоПро CSP» 4.0 R4 3-Base. Правила пользования).

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

5.8.3. Для организации защищенного соединения необходимо выпустить новую ключевую информацию и импортировать ее (см. подраздел 4.4 документа МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста» и подраздел 3.4 документа МКЕЮ.00631-01 32 02 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). ПО «ЗАСТАВА-Офис». Руководство системного программиста»).

5.9. Требования к политике безопасности СКЗИ

5.9.1. Для эксплуатации ПК должны быть настроены Администратором безопасности ПК в соответствии требованиями технической документации, перечисленной в п. 5.4.6 и п. 5.4.7.

5.9.2. 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 R4 3-Base ЖТЯИ.00089. 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***.

5.9.3. Администратор безопасности ПК должен руководствоваться следующими требованиями:

— В целях защиты управляющей информации, Агент безопасности – ПО «ЗАСТАВА-Офис» МКЕЮ.00631, входящий в состав ПК, должен быть сконфигурирован таким образом, чтобы не допускать открытых соединений для любых сетевых сервисов на внешних сетевых интрефейсах СВТ ПК подключенных к сетям общего пользования напрямую.

— Обмен информацией между клиентской и серверной частями ПК должен выполняться по каналам связи, защищенным от НСД организационно-техническими мерами.

5.9.4. На объектах информатизации корпоративной ИТКС, где эксплуатируется 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

[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;

принятых мер должна оцениваться порядком, предусмотренным упомянутыми руководящими документами ФСТЭК России.

5.9.5. При обнаружении в процессе эксплуатации защищенной корпоративной ИТКС пользователей, ЛПБ которых не соответствует действующей в корпоративной информационно-телекоммуникационной ГПБ, Администратор безопасности ПК должен принять меры к незамедлительному принудительному восстановлению ЛПБ у указанных пользователей.

5.9.6. Сразу после установки Агент безопасности – ПО «ЗАСТАВА-Офис», входящий в состав ПК, Администратором безопасности ПК должен быть задан пароль администратора настроек СКЗИ (см. п. 3.8.6 документа МКЕЮ.00631-01 32 02 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). ПО «ЗАСТАВА-Офис». Руководство системного программиста»).

5.9.7. Сразу после подключения ПК Администратором безопасности ПК должен быть отключен режим IKEv1 в настройках агента безопасности ПО «ЗАСТАВА-Офис», входящего в состав ПК (см. п. 3.8.2.2 документа МКЕЮ.00631-01 32 02 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). ПО «ЗАСТАВА-Офис». Руководство системного программиста»).

5.9.8. Запрещается удалять файлы, содержащие журналы событий ПК, без предварительного перемещения их на архивные носители. Архивные носители должны быть доступны только Администратору безопасности ПК.

5.10. Требования к процедуре обновления

5.10.1. Для обновления ПК Заказчик (Пользователь) должен самостоятельно получить у Изготовителя (Поставщика) согласно договору на поставку и/или техническую поддержку дистрибутив обновления на CD/DVD-диске 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.

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

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

5.10.4. До процедуры обновления требуется сохранить ГПБ согласно процедуре, описанной в п. 8.1.2 документа МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW

«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.

«ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста».

5.10.5. Процедура установки сертифицированных обновлений ПК производится локально путем установки эталонного образа, содержащего обновления на СВТ с установленным и настроенным ПК и соответствует процедуре установки ПК описанной в п. 2.3.2 документа МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста».

5.10.6. После процедуры обновления требуется импортировать сохранённую до обновления ГПБ согласно процедуре, описанной в п. 8.1.1 документа МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста».

5.10.7. Для завершения процедуры обновления ПК Администратор безопасности ПК должен выполнить действия по проверке и корректировке шаблона контроля целостности в соответствии с порядком, описанном в п. 5.5.9 и п. 5.5.10.

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

5.11. Перечень событий, при возникновении которых эксплуатация ПК запрещена

Эксплуатация ПК запрещена при наступлении следующих событий:

— нарушение печати системного блока СВТ с установленным ПК;

— нарушение целостности ПК;

— сбой в работе ПК;

— компрометация ключей.

При наступлении любого из перечисленных событий Администратор ПК должен: приостановить эксплуатацию ПК, выявить причины инцидента, а также устранить негативные последствия посредством принятия мер в соответствии с документом МКЕЮ.00631-01 32 01 «Программный комплекс «VPN/FW «ЗАСТАВА-Управление», версия 6 КС3» (исполнение ZM6-WS64-VO-03). Руководство системного программиста» или в соответствии с подразделом 5.12.

В случае невозможности устранения негативных последствий инцидентов Администратор ПК должен вывести из эксплуатации ПК.

5.12. Нештатные ситуации при эксплуатации ПК

В таблице (см. Таблица 2) приведен основной перечень нештатных ситуаций и соответствующие действия Администратора безопасности ПК при их возникновении.

Таблица 2 - Действия администратора ПК в нештатных ситуациях

№п/п	Нештатная ситуация	Действия Администратора безопасности ПК
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в помещении где размещается СВТ ПК.	Администратор безопасности ПК: – Сохраняет ГПБ на внешний накопитель. – Останавливает СВТ ПК. – Администратор безопасности ПК упаковывает ключевые носители и внешний накопитель с сохранённой ГПБ 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 ПК. – Администратор безопасности ПК оповещает по телефонным каналам общего пользования всех пользователей и администраторов программных и аппаратно-программных СКЗИ и МЭ ИТКС о приостановке работы ПК. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств ПК, Администратор безопасности ПК 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 5.8 «Действия при компрометации ключей».
3.	Истечение срока действия ключей, используемых для организации защищенного соединения.	Производится замена ключей. Криптографические ключи на ключевых носителях, сроки действия которых истекли, уничтожаются. Порядок уничтожения ключей описан в подразделе 5.7 «Требования к обращению с криптографическими ключами» и в документации на СКЗИ «КриптоПро CSP» 4.0 R4 3-Base ЖТЯИ.00089 (см. п. «Уничтожение ключей на ключевых носителях» документа ЖТЯИ.00089-01 95 01 СКЗИ «КриптоПро CSP» 4.0 R4 3-Base. Правила пользования).
4.	Отказы и сбои в работе аппаратной части ПК.	При отказах и сбоях в работе аппаратной части ПК 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 ПК, должен восстановить работоспособность средств защиты от 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 невыявленных ранее ошибок в ПО, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и обратиться в службу технической поддержки Изготовителя

№п/п	Нештатная ситуация	Действия Администратора безопасности ПК
		(Поставщика) 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 ПК 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 компьютера с установленным ПК Администратор безопасности ПК обязан произвести служебное расследование по данному факту с целью установления причины нарушении целостности печати и при необходимости переустановить ПК.

Все нештатные ситуации должны отражаться в «Журнале эксплуатации ПК».

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

BIOS – Basic input/output system
Базовая система ввода-вывода
FW – Firewall;
Межсетевой экран
IKE – Internet Key Exchange;
Протокол обмена ключевой информацией; используется совместно с протоколами IPsec для организации защищенного канала
IP – Internet Protocol;
Протокол сетевого уровня, являющийся базовым протоколом IP-сетей
IPsec – IP security;
группа протоколов для установления защищенных соединений в IP-сетях
PIN – Personal Identification Number
Персональный идентификационный код
PKCS – PublicKey Cryptography Standards;
Криптографические стандарты открытого ключа
VPN – Virtual Private Network;
Виртуальная частная сеть
АО – Акционерное обществ
АПМДЗ – Аппаратно-программный модуль доверенной загрузки
АРМ – Автоматизированное рабочее место
ГПБ – Глобальная политика безопасности
ИТКС – Информационно-телекоммуникационная сеть
ЛПБ – Локальная политика безопасности
МЭ – Межсетевой экран
НСД – Несанкционированный доступ
ООО – Общество с ограниченной ответственностью
ОС – Операционная система
ПАК – Программно-аппаратный комплекс
ПК – Программный комплекс
ПО – Программное обеспечение
СВТ – Средство вычислительной техники
СЗИ – Средство защиты информации
СКЗИ – Средство криптографической защиты информации
СФ – Среда функционирования
УЦ – Удостоверяющий центр
ФКН – Функциональные ключевые носители
ФСБ России – Федеральная служба безопасности
ФСТЭК России – Федеральная служба по таможенному и экспортному контролю
ЭП – Электронная подпись

СВЕДЕНИЯ О ПРОВЕРКАХ И ВНЕСЕННЫХ ИЗМЕНЕНИЯХ

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

Лист регистрации изменений

Изменение	Номера листов				Всего листов в документе	Номер документа	Вх. № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	изъятых					
1	2	3	4	5	6	7	8	9	10
1	-	Все	-	-	31	МКЕЮ.0080	-		21.09.2021