ПРИЛОЖЕНИЕ №4

УТВЕРЖДЕНО
приказом
от 28.12.2018 № 265-ОД

ПОЛОЖЕНИЕ
о порядке обеспечения безопасности персональных данных с использованием средств криптографической защиты информации

1 Общие положения

1.1 Положение о порядке обеспечения безопасности персональных данных с использованием средств криптографической защиты информации (далее - Положение) разработано в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152 «О персональных данных», определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты персональных данных при их обработке в информационной системе комитета физической культуры и спорта администрации города Ставрополя (далее - комитет).

1.2 В документе используются положения следующих нормативных актов:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Приказ ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13.06.2001 № 152;

– «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

1.3 Требования Положения обязательны к исполнению всеми уполномоченными на работу со средствами криптографической защиты информации работниками комитета физической культуры и спорта администрации города Ставрополя (далее – Пользователи криптосредств).

1.4 Используемые термины, определения и сокращения.

– Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

– Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

– Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

– Криптографический ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

– Ключевые документы – материальные носители информации, содержащие криптографические ключи.

– Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание.

– Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

– Режимные помещения – помещения, где установлены криптосредства или хранятся ключевые документы к ним.

– СКЗИ – средство криптографической защиты информации.

– ПЭВМ – персональная электронная вычислительная машина.

1.5 Настоящее Положение вступает в силу с момента его утверждения руководителем комитета и действует бессрочно до замены его новым Положением.

1.6 Пересмотр Положения производится в следующих случаях:

– при изменении процессов и технологий обработки персональных данных в комитете;

– по результатам проверок органа по защите прав субъектов персональных данных, выявившим несоответствия требованиям законодательства РФ по обеспечению безопасности персональных данных;

– при изменении требований законодательства РФ к порядку обработки и обеспечению безопасности персональных данных;

– в случае выявления существенных нарушений по результатам внутренних проверок системы защиты персональных данных.

1.7 Ответственным за пересмотр данного Положения является сотрудник комитета, назначенный Приказом руководителя комитета ответственным за организацию обработки персональных данных в комитете. Измененное Положение утверждается Приказом руководителя комитета.

2 Организация и обеспечение безопасности обработки персональных данных с использованием криптосредств

2.1 Пользователи криптосредств допускаются к работе с ними на основании приказа руководителя комитета.

2.2 Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом руководителя комитета (далее – Ответственный пользователь криптосредств).

2.3 Допускается возложение функций Ответственного пользователя криптосредств на:

– одного из пользователей криптосредств;

– на структурное подразделение или должностное лицо (работника), ответственных за защиту информации, назначаемых комитетом.

2.4 Пользователи криптосредств обязаны:

– соблюдать конфиденциальность при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

– выполнять требования по обеспечению безопасности персональных данных;

– обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

– своевременно выявлять попытки посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

– немедленно принимать меры по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.;

– строго соблюдать правила пользования криптосредств, к эксплуатации которых допущен;

– не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

– не допускать записи на ключевой носитель посторонней информации;

2.5 Пользователи криптосредств, должны быть ознакомлены с настоящим Положением и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.6 На Ответственного пользователя криптосредств возлагаются обязанности по:

– текущему контролю за организацией и обеспечением функционирования криптосредств;

– проведению разбора конфликтных ситуаций, возникающих при эксплуатации криптосредств;

– ведению учета экземпляров криптосредств, эксплуатационной и технической документации к ним, ключевых документов.

3 Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

3.1 При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается.

3.2 Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.3 Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов». (Форма журнала представлена в Приложении 1).

3.4 Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.5 Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в Журнале поэкземплярного учета

пользователям криптосредств, несущим персональную ответственность за их сохранность.

3.6 Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) Ответственным пользователем криптосредств под расписку в соответствующем Журнале поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована Ответственным пользователем криптосредств.

3.7 Пользователи криптосредств должны хранить инсталлирующие криптосредства, носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.8 Пользователи криптосредств также обязаны раздельно хранить действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих ключевых документов.

3.9 Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, должны быть опечатаны. Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.10 При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от Ответственного пользователя криптосредств.

3.11 Получение криптосредств, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено Ответственному пользователю криптосредств в соответствии с порядком, указанным в сопроводительном письме. Ответственный пользователь криптосредств обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

3.12 Указание на изготовление очередных ключевых документов для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем криптосредств только после поступления от всех заинтересованных пользователей криптосредств подтверждения о получении ими очередных ключевых документов.

3.13 Неиспользованные или выведенные из действия ключевые документы подлежат возвращению Ответственному пользователю криптосредств или по его указанию должны быть уничтожены на месте.

3.14 Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

3.15 Криптоключи (исходную ключевую информацию) необходимо уничтожать (стирать) по технологии регламентированной эксплуатационной и технической документацией к криптосредствам.

3.16 Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к криптосредствам.

3.17 Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожают путем сжигания или с помощью любых бумагорезательных машин.

3.18 Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств.

3.19 Ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующем Журнале поэкземплярного учета. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

3.20 Ключевые документы уничтожаются либо пользователями криптосредств, либо Ответственным пользователем криптосредств под расписку в соответствующем Журнале поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) Ответственного пользователя криптосредств для списания уничтоженных документов с их Лицевых счетов.

3.21 Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается что уничтожается и в каком количестве. В

конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации (Приложение 2). Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующем Журнале поэкземплярного учета.

3.22 Криптоключи, в отношении которых, возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.23 О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать Ответственному пользователю криптосредств.

3.24 Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

3.25 В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.26 Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет Ответственный пользователь криптосредств.

3.27 Изготавливают ключевые документы пользователи криптосредств, применяя штатные криптосредства, в строгом соответствии с эксплуатационной и технической документацией к криптосредствам.

4 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

4.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

4.2 При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

4.3 Перечисленные в настоящем документе требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

4.4 Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

4.5 Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.6 Двери режимных помещений должны быть закрыты на ключ в нерабочее время и могут открываться только для санкционированного прохода сотрудников. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в «Журнале учета хранилищ СКЗИ и ключей к ним» (Приложение 3). Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе пользователя криптосредств.

4.7 Блоки ПЭВМ с установленными СКЗИ должны быть опечатаны (опломбированы) с внесением информации в Журнал опломбирования ПЭВМ (Приложение 4), кроме того, в техническом (аппаратном) журнале отражаются также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится если нет прямых указаний о его ведении Форма технического (аппаратного) журнала приведена в Приложении 5.

4.8 Для предотвращения просмотра извне режимных помещений их окна должны быть защищены (занавешены плотными шторами или жалюзи).

4.9 Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации. Результаты проверки исправности фиксируются в Журнале учета проверок сигнализации (Приложение 6).

4.10 Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания. Хранение эксплуатационной и технической документации, инсталлирующих криптосредства носителей осуществляет Ответственный пользователь криптосредств.

4.11 Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе Ответственного пользователя криптосредств.

4.12 По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты на ключ. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале Ответственному пользователю криптосредств, который хранит эти ключи в личном или специально выделенном хранилище.

4.13 Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

4.14 При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Ответственный пользователь криптосредств.

4.15 В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища, могут быть вскрыты только пользователями криптосредств, Ответственным пользователем криптосредств или Администратором ИБ ИС.

4.16 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено Ответственному пользователю криптосредств. Прибывший Ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

4.17 Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

4.18 На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

5. Организация доступа в режимные помещения, в которых размещены используемые СКЗИ, в том числе носители ключевой, аутентифицирующей и парольной информации СКЗИ

5.1. Для режимных помещениях, в которых размещены используемые СКЗИ, в том числе носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) организуется режим обеспечения безопасности, при котором обеспечивается сохранность СКЗИ, ключевой информации и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

5.2. В Помещения допускаются работники комитета, указанные в Перечне лиц, имеющих право доступа в Помещения, в которых размещены СКЗИ (далее – Перечень).

5.3. Помимо лиц, указанных в Перечне (далее – лица, имеющие право доступа в Помещение) право самостоятельного пребывания в Помещениях, для которых введен режим безопасности, имеют непосредственно ответственные за организацию обработки персональных данных, ответственный за защиту информации и обеспечение безопасности персональных данных, администратор информационной безопасности информационных систем, администраторы информационных систем, ответственный пользователь СКЗИ.

5.4. Сотрудники, не внесенные в Перечень (далее – лица, не имеющие право доступа в Помещение), являются посторонними лицами и могут находиться в Помещениях только в присутствии лиц, имеющих права доступа в Помещения.

5.5. Сторонние лица, не являющиеся работниками комитета, имеют право пребывать в Помещении только в присутствии лиц, имеющих право доступа в Помещение, и в течение ограниченного количества времени, необходимого для решения вопросов, связанных с исполнением функций и (или) осуществлением полномочий по предоставлению государственных и муниципальных услуг.

5.6. Доступ в Помещения разрешается только в рабочее время, в нерабочее время режимное помещение должно закрываться.

5.7. В течение рабочего времени лица, имеющие право доступа в Помещение:

при оставлении Помещения закрывают дверь Помещения на ключ (при этом запрещается оставлять ключ в замке Помещения);

– не покидают Помещение, если в нем находятся лица, не имеющие право доступа в Помещение;

– при обнаружении фактов нарушения режима безопасности Помещения ставят в известность ответственного пользователя СКЗИ и Администратора информационной безопасности ИС;

– при посещении Помещения сторонними лицами с целью проведения контрольных, проверочных мероприятий, а также работ по обслуживанию Помещения и его инженерно-технических средств ставят в известность об этом ответственного пользователя СКЗИ, администратора информационной безопасности ИС и руководителя подразделения.

5.8. Доступ в Помещение при возникновении нештатной ситуации в нерабочее время осуществляется в присутствии администратора информационной безопасности

5.9. При обслуживании Помещения (уборка или различный ремонт Помещения, инженерно-технического оборудования):

– обслуживающий персонал находится в Помещении только в присутствии лиц, имеющих право доступа в Помещение.

– ключи от замков дверей Помещения обслуживающему персоналу и другим лицам, не имеющим права доступа в Помещение, без согласования с Ответственным за организацию обработки персональных данных, не выдаются.

– сотрудники подразделения, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонентов информационной системы и материальных носителей информации ограниченного доступа.

– капитальный или иной ремонт может проводиться и в отсутствие лиц, имеющих право доступа в Помещение, при условии того, что компоненты информационной системы и материальные носители информации ограниченного доступа будут вынесены из ремонтируемого Помещения в другое контролируемое помещение, и по окончании ремонта будут сменены замки. Организует и контролирует исполнение Ответственный за организацию обработки персональных данных.

5.10. Лица, имеющие право доступа в Помещение, несут ответственность за нерегламентированное пребывание в Помещении работников, не имеющих права доступа в Помещение, и сторонних лиц.

6. Допуск в помещения, в которых ведётся эксплуатация СКЗИ

6.1. Доступ посторонних лиц в помещения, в которых ведётся эксплуатация СКЗИ, должен осуществляется только ввиду служебной необходимости. При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с информацией ограниченного доступа.

6.2. Допуск сотрудников в помещения, в которых ведётся эксплуатация СКЗИ, оформляется после подписания сотрудником обязательства о

неразглашении и проведении инструктажа ответственным пользователем СКЗИ, либо администратора информационной безопасности.

6.3. В нерабочее время помещения, в которых осуществляется функционирования СКЗИ, должны опечатываться или ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, ключевые документы, должны быть убраны в запираемые шкафы (сейфы), средства вычислительной техники выключены либо заблокированы.

7. Допуск в серверные помещения с СКЗИ

7.1. Доступ в серверные помещения разрешён только списку сотрудников, имеющих допуск в соответствии с приказом руководителя комитета или распоряжением руководителя филиала. Уборка серверных помещений происходит только при строгом контроле указанных лиц.

7.2. Серверное помещение в обязательном порядке оснащается опечатывающим устройством, либо охранной сигнализацией.

7.3. Доступ в серверные помещения посторонних лиц допускается строго по согласованию с вышеперечисленными лицами.

7.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего не допустимо.

ПРИЛОЖЕНИЕ 1 К ПОЛОЖЕНИЮ

ЖУРНАЛ ПОЭКЗЕМПЛЯРНОГО УЧЕТА КРИПТОСРЕДСТВ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

№ п/п	Наименование	Регистрационные номера	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Выдано		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				от кого получены	дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	подпись пользователя СКЗИ и дата	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	дата подключения (установки) и подписи лиц, произведших подключение (установку)	номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие	Номер акта или расписка об уничтожении	
1	КриптоПро 3.6	3636K-30000-0IWPR-3DTA3-5VPEE		ООО РОСИНТЕГРАЦИЯ	14.07.2014	Гостищева Г.В.		Морозов В.В.	17.07.2014	34140023				
2	КриптоПро 3.6	36366-60000-0IR71-X7OGG-1V1QQ		ООО РОСИНТЕГРАЦИЯ	14.07.2014	Чурсинова Т.Г.		Морозов В.В.	17.07.2014	041400000000006				

3	КриптоПро 3.6	3636A-70000-0IQXK-L54AE-389ZQ		ООО РОСИНТЕ ГРАЦИЯ	14.07.2014	Морозова С.А.		Морозов В.В.	17.07.2014	04140000 0001960
4	КриптоПро 3.6	3636K-30000-0IWPR-3DTA3-5VPEE		ООО РОСИНТЕ ГРАЦИЯ	14.07.2014	Шонин Е.В.		Морозов В.В.	17.07.2014	34140045
5	КриптоПро 3.6	3636W-90000-0IZEY-N8IGF-8YW1F		Россельхоз банк	19.06.2015	Морозов В.В.		Морозов В.В.	18.02.2018	04140000 0001970
6	КриптоПро 4.0	40405-Q0000-01LWH-PEWOV-D1DA5		ООО УЦ ОРБИТА	22.09.2017	Бердник Е.В.		Морозов В.В.	09.10.2017	34140200
7	КриптоПро 4.0	4040H-X0000-01MWP-695FW-YFWHB		Администр ация г. Ставрополя	30.01.2017	Морозов В.В.		Морозов В.В.	21.05.2018	34140146
8	КриптоПро 4.0	4040E-L0000-01CMN-A12D9-GLRHG		Администра ция г. Ставрополя	30.01.2017	Морозов В.В.		Морозов В.В.	21.05.2018	04140000000 0019970
9	VipNet 4.3 – VipNet CSP 4.2	782-001962		ООО РОСИНТЕГ РАЦИЯ		Гостищева Г.В.	14.07.2014	Морозов В.В.	17.07.2014	34140023

10	VipNet 4.3 – VipNet CSP 4.2	782-001962		ООО РОСИНТЕГРАЦИЯ		Чурсинова Т.Г.		Морозов В.В.	17.07.2014	041400000000006				
11	VipNet 4.3 – VipNet CSP 4.2	782-001962		ООО РОСИНТЕГРАЦИЯ		Морозова С.А.		Морозов В.В.	17.07.2014	041400000000196				
12	VipNet 4.3 – VipNet CSP 4.2	782-001962		ООО РОСИНТЕГРАЦИЯ		Шония Е.В.		Морозов В.В.	17.07.2014	34140045				
13	VipNet 4.3 – VipNet	782-013420		ООО РОСИНТЕГРАЦИЯ		Морозов В.В.		Морозов В.В.	17.07.2014	34140143				
14	Континент АП 3.7	351E2-009995/2133/311		УЦ Федеральное казначейство по СК		Бердник Е.В.		Морозов В.В.	14.06.2018	34140200				

ПРИЛОЖЕНИЕ 2 К ПОЛОЖЕНИЮ

Акт уничтожения ключевых документов

Комиссия, в составе:

председатель комиссии:

_____

члены комиссии:

_____

_____

провела уничтожение

_____

_____

_____

цифрами и прописью о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации

путем

_____

разрезания, демонтажа, измельчения, сдачи для уничтожения предприятию по утилизации вторичного сырья

_____

Председатель комиссии:

_____ _____

(ФИО) (дата, подпись)

Члены комиссии:

_____ _____

(ФИО) (дата, подпись)

_____ _____

(ФИО) (дата, подпись)

ПРИЛОЖЕНИЕ 3 К ПОЛОЖЕНИЮ

ЖУРНАЛ УЧЕТА ХРАНИЛИЩ СКЗИ И КЛЮЧЕЙ К НИМ

№ п/п	Наименование (сейф, металл. Шкаф, кладовая, склад, спец. хранилище)	Инвентарный номер хранилища	Местонахождение (отдел, цех, лаборатория и т. д., номер комнаты и корпус здания)	Что хранится	Фамилия ответственного за шкаф, сейф, спец. хранилище	Коли. Ключей и их номера	Расписка за получение рабочего экз. ключ.	Место хранения запасного ключа	Примечание
1	2	3	4	5	6	7	8	9	10
1	сейф	6-141	Отдел автоматизации каб. 401	Ключ ЭЦП Морозов В.В., Карпенко Л.А.	Морозов В.В.	2		нет	
2	сейф	6-140	Отдле бухгалтерского учета, контроля и отчетности каб. 408	Ключи ЭЦП Карпенко Л.А., Белогай Л.А., Афисова Е.П.	Белогай Л.А.	3		нет	

ПРИЛОЖЕНИЕ 4 К ПОЛОЖЕНИЮ

ЖУРНАЛ ОПЛОМБИРОВАНИЯ ПЭВМ

№ п/п	Адрес размещения ПЭВМ, номер помещения	Серийный, инвентарный номера ПЭВМ	Опломбировал		Отметка о внесении в журнал			Номер печати, либо оттиск печати которой опечатана ПЭВМ и/или образцы подписи
			Ф.И.О.	Дата	Ф.И.О.	Дата	Подпись и № акта	
1	Отдел автоматизации, каб. 401	34140146	Морозов В.В.	01.01.2014	Морозов В.В.	01.01.2014		Для документов
2	Отдел социально-правовых гарантий каб. 109	041400000000088	Морозов В.В.	01.01.2014	Морозов В.В.	01.01.2014		Для документов
3	Отдел социальной помощи и поддержки населения каб. 102	041400000000087	Морозов В.В.	01.01.2014	Морозов В.В.	01.01.2014		Для документов
4	Отдел	041400000000006	Морозов В.В.	01.01.2014	Морозов В.В.	01.01.2014		Для

	назначения и выплаты жилищных субсидий каб. 112							документов
5	Отдел бухгалтерского учета, контроля и отчетности каб. 409	34140028	Морозов В.В.	01.01.2014	Морозов В.В.	01.01.2014		Для документов

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом «___» _________ 2018

«Об утверждении положения о порядке обеспечения безопасности персональных данных с использованием средств криптографической защиты информации»

№ пп	Ф.И.О. работника	Должность работника	Дата	Подпись об ознакомлении
