РОССИЙСКАЯ ФЕДЕРАЦИЯ
КАМЧАТСКИЙ КРАЙ

ПОСТАНОВЛЕНИЕ

АДМИНИСТРАЦИИ ЕЛИЗОВСКОГО ГОРОДСКОГО ПОСЕЛЕНИЯ

От__17.06.2013_____ № _ 391-п_____

г. Елизово

Об утверждении Положения по организации обработки и ведению работ по обеспечению безопасности (защиты) персональных данных в администрации Елизовского городского поселения и ее органах

Руководствуясь положениями Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ, постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119, постановлением Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687, руководящими документами и методическими рекомендациями ФСБ России и ФСТЭК России,

ПОСТАНОВЛЯЮ:

1. Утвердить Положение по организации обработки и ведению работ по обеспечению безопасности (защите) персональных данных в администрации Елизовского городского поселения и ее органах, согласно приложению к настоящему постановлению.
2. Руководителям органов администрации Елизовского городского поселения ознакомить с настоящим постановлением подчиненных должностных лиц, в том числе вновь принимаемых на службу (работу).
3. Управлению делами (Назаренко Т.С.) опубликовать настоящее постановление и разместить на официальном сайте в сети Интернет.
4. Контроль за выполнением настоящего постановления возложить на заместителя Главы администрации Елизовского городского поселения Авдошенко В.И.

Глава администрации Елизовского
городского поселения Л.Н.Шеметова

Приложение
к постановлению администрации
Елизовского городского поселения
от _____ № _____

ПОЛОЖЕНИЕ

по организации обработки и ведению работ по обеспечению безопасности (защите) персональных данных в администрации Елизовского городского поселения и ее органах

1. Общие положения.

1.1. Положение по организации обработки и ведению работ по обеспечению безопасности (защите) персональных данных в администрации Елизовского городского поселения и ее органах (далее – Положение) разработано в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, постановлением Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687, постановлением Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119, руководящими документами и методическими рекомендациями ФСТЭК России и ФСБ России в целях организации обработки и обеспечения безопасности персональных данных и определяет политику администрации Елизовского городского поселения и ее органов по организации и защите персональных данных.

1.2. Настоящее Положение определяет: порядок работы администрации Елизовского городского поселения и ее органов (управлений) в части обеспечения безопасности (защиты) персональных данных, принадлежащих физическим лицам, при их обработке в информационной системе персональных данных; порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования технических средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений; порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления; порядок обучения должностных лиц (служащих, работников) практике работы в информационной системе персональных данных; порядок проверки электронного журнала обращений к информационной системе персональных данных; порядок соблюдения условий использования технических средств защиты информации, предусмотренные эксплуатационной и технической документацией; правила обновления общесистемного и прикладного программного обеспечения; правила организации антивирусной и парольной защиты информационной системы персональных данных; порядок охраны и контролируемый допуск лиц в защищаемые помещения.

1.3. В настоящем Положении используются следующие понятия:

а) персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту персональных данных (информация, позволяющая идентифицировать физическое лицо);

б) обработка персональных данных – получение, хранение, комбинирование, передача или любое другое использование персональных данных работника;

в) оператор персональных данных – муниципальный орган, юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных;

г) информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

д) обезличенные персональные данные – информация, по которой невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

е) общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

ж) биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность: рост, вес, особенности строения тела, отдельных органов и тканей, работа желез внутренней секреции, различные отклонения в развитии, атавизмы, психическое состояние здоровья и т.п.;

з) субъект персональных данных – владелец (обладатель) персональных данных;

и) пользователь – должностное лицо (сотрудник, служащий, работник), осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации (персональных данных), содержащейся в ее базах;

к) администратор безопасности – лицо, ответственное за защиту информационной системы от несанкционированного доступа к информации;

л) безопасность информации – состояние защищенности информации, характеризуемое способностью персонала (пользователями), технических средств и информационных технологий обеспечивать конфиденциальность, то есть сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

1.4. В администрации Елизовского городского поселения и ее органах обработка персональных данных должностных лиц (служащих, сотрудников, работников) и граждан может осуществляться исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия муниципальным служащим и работникам в трудоустройстве, обучении и продвижении по службе;

в) обеспечения личной безопасности муниципальных служащих и работников;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества;

е) предоставления муниципальному служащему (работнику) и гражданину установленных законодательством Российской Федерации, коллективным договором,

соглашениями, локальными нормативными актами, трудовым договором условий труда, гарантий и компенсаций.

1.5. В администрации Елизовского городского поселения и ее органах в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, другими нормативными правовыми актами Российской Федерации подлежат обработке следующие персональные данные, касающиеся конкретного физического лица:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения; гражданство;
- сведения об образовании, о наличии ученой степени, ученого звания, класса, классной квалификации, разряда;
- сведения о выполняемой работе с начала трудовой деятельности;
- паспортные данные;
- семейное положение;
- адрес места жительства; номер телефона или другой вид связи;
- сведения о воинском учете;
- решения аттестационных комиссий;
- награды (поощрения, почетные звания);
- содержание трудового договора и дополнительных соглашений к нему;
- данные страхового свидетельства государственного пенсионного страхования;
- данные свидетельства о постановке на учёт в налоговый орган и присвоения ИНН;
- данные трудовой книжки;
- данные автобиографии;
- доходы; социальное и имущественное положение; сведения о социальных льготах;
- биометрические данные и результаты медицинского осмотра (обследования) - на лиц, которые в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации подлежат медицинскому осмотру (обследованию);

На должностных лиц (служащих, работников), которым по характеру занимаемой (замещаемой) должности необходим допуск к государственной тайне, дополнительно к указанным персональным данным обрабатывается следующая информация:

- наличие допуска к государственной тайне, оформленного за период работы, службы, учебы;
- наличие судимостей, в том числе близких родственников;
- сведения о выездах за пределы территории Российской Федерации;
- наличие родственников, постоянно проживающих за границей;
- наличие заграничного паспорта.

1.6. Персональные данные, необходимые для обработки содержатся в следующих документах:

а) в документах, предъявляемых муниципальным служащим и работником в соответствии со статьей 65 Трудового кодекса Российской Федерации при заключении трудового договора;

б) в личных делах;

в) в трудовых книжках;

г) в документах о составе семьи, необходимых для предоставления гарантий, связанных с выполнением семейных обязанностей;

д) в документах о состоянии здоровья муниципального служащего (работника), если в соответствии с законодательством он должен пройти предварительный и периодические медицинские осмотры (обследования);

е) в документах о состоянии здоровья детей и других близких родственников (например, справки об инвалидности), когда с наличием таких документов связано предоставление каких-либо гарантий и компенсаций;

ж) в документах, подтверждающих право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (об инвалидности, донорстве, участии в боевых действиях, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.);

з) в документах о беременности и возрасте детей для предоставления матери (отцу, иным родственникам) установленных законом условий труда, гарантий и компенсаций;

и) в унифицированных формах первичной учетной документации по учету труда и его оплаты, а также в основаниях к приказам по личному составу;

к) в докладных и аналитических записках, материалах служебных проверок и расследований, анкетах, рекомендациях, характеристиках, опросных листах и т.п.

1.7. Доступ к персональным данным субъектов персональных данных могут иметь только уполномоченные должностные лица администрации Елизовского городского поселения и ее органов.

В органах администрации Елизовского городского поселения соответствующими приказами определяется перечень лиц из числа специалистов структурных подразделений, уполномоченных на обработку персональных данных, в том числе на ведение и хранение личных дел и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных. Указанные структурные подразделения и должностные лица (работники) вправе обрабатывать только те персональные данные, которые необходимы для выполнения возложенных на них задач, функций и полномочий.

1.8. Защита персональных данных от неправомерного их использования или утраты обеспечивается оператором персональных данных в порядке, установленном федеральными правовыми актами и настоящим Положением.

1.9. Администрация Елизовского городского поселения и ее органы вырабатывают меры, направленные на защиту персональных данных.

Работники (а в предусмотренных законом случаях - их представители) должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных, в том числе с настоящим Положением, а также об их правах и обязанностях в этой области.

2. Принципы и условия обработки персональных данных.

2.1. Обработка персональных данных осуществляется на основе принципов:

а) законности целей и способов обработки персональных данных и добросовестности;

б) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

в) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

2.2. Все персональные данные следует получать у субъекта персональных данных. Если персональные данные, возможно, получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено на это письменное согласие. Субъекту персональных данных сообщается о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

2.3. Письменное согласие субъекта персональных данных на обработку его персональных данных оформляется в форме заявления по прилагаемой форме (Приложение 1 к настоящему Положению) и включает в себя:

а) фамилию, имя, отчество, адрес муниципального служащего (работника), номер документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

б) наименование и адрес органа администрации, получающего согласие муниципального служащего или работника;

в) цель обработки персональных данных;

г) перечень персональных данных, на обработку которых дается согласие муниципального служащего (работника);

д) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых органом администрации способов обработки персональных данных;

е) срок, в течение которого действует согласие, а также порядок его отзыва.

Для обработки персональных данных, содержащихся в оформленном в письменной форме заявлении о согласии на обработку персональных данных, дополнительного согласия в последующем не требуется.

В случае недееспособности работника, согласие на обработку его персональных данных дает в письменной форме его законный представитель. В случае смерти работника, согласие на обработку его персональных данных дают в письменной форме наследники, если такое согласие не было дано им самим при его жизни.

2.4. В соответствии со статьями 6 и 9 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей

волей и в своем интересе, за исключением случаев, если обработка персональных данных:

- осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг граждан, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

- осуществляется в целях исполнения договора, одной из сторон которого является муниципальный служащий или работник;

- осуществляется для статистических или иных целей при условии обязательного обезличивания персональных данных;

- необходима для защиты жизни, здоровья или иных жизненно важных интересов граждан, если получение согласия невозможно.

2.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, частной и интимной жизни, не допускается.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни муниципального служащего (работника), если: муниципальный служащий (работник) дал согласие в письменной форме на обработку своих персональных данных; персональные данные являются общедоступными; персональные данные относятся к состоянию здоровья муниципального служащего (работника) и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение его (их) согласия невозможно.

2.6. Орган администрации Елизовского городского поселения, с которым субъект персональных данных состоит в трудовых отношениях:

- не имеет право получать и обрабатывать персональные данные о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом РФ или иными федеральными законами;

- имеет право запрашивать информацию о состоянии здоровья, только по тем сведениям, которые относятся к вопросу о возможности выполнения субъектом персональных данных трудовой функции;

-при принятии решений, затрагивающих интересы субъекта персональных данных, не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.7. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме, за исключением случаев, предусмотренных законодательством Российской Федерации.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

3. Порядок обработки персональных данных

3.1. Обработка персональных данных осуществляется в соответствии с требованиями, установленными законодательством Российской Федерации, настоящим Положением и должна исключать их утрату или незаконное использование.

3.2. Персональные данные в наиболее полном объеме используются и хранятся в кадровой службе, в архиве, в бухгалтерии и иных структурных подразделениях - в объеме, необходимом для выполнения возложенных на них задач, функций и полномочий.

3.3. Обработка персональных данных может осуществляться с использованием средств автоматизации (технических средств) или без использования таких средств.

3.4. Обработка персональных данных, содержащихся в информационных системах органов администрации поселения осуществляется в соответствии с постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119, руководящих документов и методических рекомендаций ФСБ России и ФСТЭК России.

3.5. При обработке персональных данных должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

3.6. Ответственность за техническую эксплуатацию средств, позволяющих осуществлять обработку персональных данных, а также за осуществление контроля за выполнением мер по информационной безопасности при обработке персональных данных в информационных системах возлагается в органах администрации поселения на соответствующие структурные подразделения и должностных лиц.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения трудовых обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного Главой администрации поселения и (или) руководителем органа администрации поселения.

3.7. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из

субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с Положением «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687, руководящими документами и методическими рекомендациями ФСБ России и ФСТЭК России.

3.8. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.9. В администрации поселения и ее органах персональные данные обрабатываются с использованием технических средств: персональных компьютеров, программных продуктов бухгалтерского, кадрового учета, факсимильной связи, а также на бумажных и материальных носителях.

3.10. В кадровых службах (подразделениях) органов администрации Елизовского городского поселения основная часть документов, содержащих персональные данные, ведется и хранится:

а) в личном деле - в соответствии с Правилами оформления и ведения личных дел;

б) в трудовой книжке - в соответствии с Правилами ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденными постановлением Правительства Российской Федерации от 16.04.2003 № 225. Согласно пункту 45 указанных Правил ответственность за организацию работы по ведению, хранению, учету и выдаче трудовых книжек и вкладышей в них возлагается на работодателя (оператора персональных данных). Для этого приказом (распоряжением) работодателя (оператора персональных данных) назначается специально уполномоченное лицо (уполномоченные лица);

в) в унифицированных документах по учету кадров - в соответствии с Указаниями по применению и заполнению форм первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.2004 № 1.

3.11. В бухгалтерии ведутся и хранятся унифицированные документы по учету рабочего времени и расчетов с персоналом по оплате труда - в соответствии с Указаниями по применению и заполнению форм первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.2004 № 1.

В бухгалтерии также хранятся копии распоряжений, приказов по личному составу, необходимые для расчетов по оплате труда. Для учета, хранения и ведения работы с указанными данными приказом (распоряжением) работодателя (оператора персональных данных) назначается специально уполномоченное лицо (уполномоченные лица).

3.12. В структурных подразделениях администрации и органах администрации поселения обрабатываются персональные данные, необходимые для выполнения возложенных на них задач, функций и полномочий, в соответствии с требованиями законодательства Российской Федерации и настоящим Положением.

3.13. В архивах документы, содержащие персональные данные хранятся в соответствии с требованиями Федерального закона от 22.11. 2004 № 125 «Об архивном деле в Российской Федерации», других федеральных законов и иных нормативных правовых актов Российской Федерации.

При учете и хранении персональных данных на бумажных и материальных носителях должны соблюдаться условия, обеспечивающие быстрый поиск и сохранность персональных данных, а также исключающие несанкционированный к ним доступ. Документы, содержащие персональные данные включаются в номенклатуру дел соответствующего органа администрации поселения с указанием сроков хранения согласно приказу Министерства культуры Российской Федерации «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» от 25.08.2010 № 558.

Указанные документы хранятся как документы строгой отчетности, в приспособленных для этой цели помещениях, оборудованных необходимым количеством сейфов или плотно закрывающихся металлических шкафов, а также охранной и пожарной сигнализацией. Сейфы (металлические шкафы) должны запираться на замок и опечатываться номерными печатями, закрепленными за ответственными должностными лицами. Личные дела, а также трудовые книжки хранятся отдельно от других документов кадровой службы.

3.14. Доступ к документам, содержащим персональные данные должны иметь только уполномоченные должностные лица, назначенные распоряжением администрации поселения либо руководителями органов администрации поселения.

В конце рабочего дня должностное лицо (работник), уполномоченный на обработку персональных данных, обязан убедиться в том, что все документы, выданные во временное пользование, возвращены, и, если необходимо, принять меры к их возвращению или розыску.

При увольнении пользователя, уполномоченного на обработку персональных данных, числящиеся за ним документы передаются другому пользователю по соответствующему акту приема-передачи.

3.15. В целях обеспечения контроля за сохранностью документов, содержащих персональные данные, ежегодно (не позднее конца первого квартала года, следующего за отчетным) на основании распоряжения администрации поселения либо приказов руководителей органов администрации поселения проводится проверка их наличия и состояния. Выявленные в ходе проверки недостатки фиксируются в акте, который после
подписания членами комиссии представляется на утверждение руководителю органа администрации Елизовского городского поселения или уполномоченному им должностному лицу.

4. Порядок передачи персональных данных

4.1. Персональные данные могут передаваться в пределах органов администрации Елизовского городского поселения (внутренние потребители), а также другим организациям (внешние потребители).

4.1.1. Внутренними потребителями являются работники администрации и ее органов - для получения лично их касающейся информации, а также для получения только тех персональных данных, которые необходимы и достаточны для выполнения возложенных на них задач, функций и полномочий.

4.1.2. Внешними потребителями являются:

а) государственные органы, внебюджетные организации и фонды, уполномоченные законодательством Российской Федерации на получение отчетов органов администрации Елизовского городского поселения, а также на проведение надзора и контроля;

б) физические и юридические лица, направившие в органы администрации поселения запрос по относящейся к ним информации;

в) представители субъекта персональных данных - для получения информации, необходимой для выполнения возложенных на них функций и полномочий.

4.2. Право на предоставление информации о персональных данных внутренним, а также внешним потребителям при наличии письменного согласия субъекта персональных данных на их передачу имеют (в пределах предоставленных им прав и полномочий) Глава администрации поселения, руководители органов администрации поселения, руководители кадровых служб (подразделений), работники архива, иные уполномоченные лица. Форма письменного заявления о согласии на передачу персональных данных третьим лицам (Приложении 2 к настоящему Положению).

4.3. Предоставление сведений о персональных данных без соответствующего согласия возможно в следующих случаях:

а) в целях предупреждения угрозы жизни и здоровья муниципальных служащих (работников) или гражданина;

б) при поступлении официальных запросов правоохранительных органов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях», Уголовно-процессуального кодекса РФ;

в) при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

4.4. По письменному заявлению субъекта персональных данных оператор персональных данных обязан не позднее трех рабочих дней со дня подачи этого заявления выдать субъекту персональных данных копии документов, связанных с работой и (или) обращением.

4.5. Персональные данные предоставляются субъектам персональных данных в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации» от 02.05.2006 № 59-ФЗ.

4.6. Юридическим лицам персональные данные предоставляются по письменным запросам, которые должны быть оформлены на бланках организации (учреждения, предприятия), иметь установленные для документа реквизиты, а также содержать предусмотренные законодательством основания (обоснование) необходимости получения запрашиваемой информации, фамилию, инициалы и телефон исполнителя.

4.7. Личные дела могут выдаваться работникам органов администрации поселения и их руководителям для ознакомления, а также передаваться в архив и другие организации в установленном законодательством Российской Федерации порядке.

4.8. Предоставление персональных данных внешним потребителям по устному или по телефонному запросу, а также по электронной почте не допускается.

4.9. При передаче персональных данных работники органов администрации поселения, наделенные правом предоставления этих данных, должны соблюдать следующие требования:

а) не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью муниципального служащего (работника) или гражданина, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами;

б) не сообщать персональные данные в коммерческих целях без письменного согласия субъекта персональных данных;

в) предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;

г) разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

д) не запрашивать информацию о состоянии здоровья, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

е) передавать персональные данные представителям в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

5. Права и обязанности субъекта персональных данных в области защиты его персональных данных

5.1. В целях обеспечения защиты персональных данных, хранящихся в органах администрации Елизовского городского поселения, субъект персональных данных имеет право на:

а) полную информацию о его персональных данных и обработке этих данных;

б) свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами;

в) определение своих представителей для защиты своих персональных данных;

г) доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

д) требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований федеральных законов. При отказе оператора персональных данных исключить или исправить персональные данные заявить в письменной форме оператору

персональных данных о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

е) требование об извещении оператором персональных данных всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

ж) обжалование в суд любых неправомерных действий или бездействия оператора персональных данных при обработке и защите его персональных данных.

5.2. Субъект персональных данных, в части обработки его персональных данных, должен:

а) предоставлять оператору персональных данных достоверные персональные данные, предусмотренные законодательством Российской Федерации;

б) в 3-дневный срок уведомлять работодателя (кадровую службу) об изменении персональных данных, указанных в пункте 1.5. Положения.

5.3. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны их персональных данных.

6. Порядок обеспечения безопасности (защиты) персональных данных при их обработке в информационной системе персональных данных.

6.1. Допуск пользователей для работы на компьютерах информационной системы персональных данных осуществляется на основании приказа, который издается руководителем органа администрации поселения, в соответствии со списком лиц, допущенных к работе в информационной системе персональных данных. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в информационной системе персональных данных руководителем органа администрации поселения назначается администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности – ответственные за защиту информации.

6.2. Пользователь информационной системы персональных данных имеет право во время, установленное регламентом рабочего времени Управления, решать поставленные задачи в соответствии с полномочиями доступа к ресурсам информационной системы персональных данных. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, утверждаемой руководителем органа администрации поселения. При этом для хранения информации, содержащей персональные данные, разрешается использовать внешние (съемные) носители информации, учтенные в Журнале учета внешних (съемных) носителей (Приложение 3 к настоящему Положению).

6.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в информационной системе персональных данных.

6.4. Вход пользователя в систему должен осуществляться по персональному электронному идентификатору и по персональному паролю.

6.5. При необходимости записи информации, содержащей персональные данные, на внешние (съемные) носители информации, она может осуществляться пользователем только на внешние (съемные) носители информации, учтенные в

Журнале учета внешних (съемных) носителей или разрешенные руководителем органа администрации поселения в целях исполнения функциональных обязанностей.

6.6. При работе с внешними (съемными) носителями пользователь, перед началом работы, обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах информационной системы персональных данных. В случае обнаружения вирусов, пользователь обязан немедленно прекратить использование внешнего (съемного) носителя и действовать в соответствии с требованиями настоящего Положения.

6.7. Пользователь, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы персональных данных , несет персональную ответственность за свои действия (бездействия).

6.8. Пользователь обязан:

- строго соблюдать установленные правила обеспечения безопасности (защиты) информации при работе с программными и техническими средствами информационной системы персональных данных;

- знать и неукоснительно выполнять правила работы со средствами защиты информации, установленными на компьютерах информационной системы персональных данных;

- хранить в тайне свой пароль (пароли);

- хранить вне досягаемости посторонних лиц свое индивидуальное устройство идентификации (ключ) в сейфе (хранилище, металлическом шкафе и т.п.);

- немедленно извещать ответственного за защиту информации (организацию обработки персональных данных) и (или) администратора информационной безопасности в случае: утраты (хищения) индивидуального устройства идентификации (ключа) или при подозрении на компрометацию личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей, иных средств наложения обеспечения на хранилища) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к данным защищаемым СВТ; несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств информационной системы персональных данных; отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ; выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения; некорректного функционирования установленных на компьютеры технических средств защиты; выявлении непредусмотренных отводов кабелей и подключенных устройств.

6.9. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств информационной системы персональных данных или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить персональные данные на неучтенных внешних (съемных) носителях информации (гибких магнитных дисках, CD-, DVD-дисках, USB-накопителях и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации.

6.10. Администратор безопасности (а при его отсутствии – ответственный за защиту информации) обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в информационной системы персональных данных, перечень используемого программного обеспечения в информационной системы персональных данных;

- вести «Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним» (Приложение 4 к настоящему Положению);

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в информационной системы персональных данных средств защиты информации от несанкционированного доступа и сопровождать их в процессе эксплуатации, при этом:

а) реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

б) вводить описания пользователей информационной системы персональных данных в информационную базу средств защиты информации от несанкционированного доступа;

в) своевременно удалять описания пользователей из базы данных средств защиты информации при изменении списка допущенных к работе лиц;

- периодически контролировать доступ лиц в помещение в соответствии со списком работников, допущенных к работе в информационной системе персональных данных и зарегистрированных в «Журнале учета пользователей, допущенных к информационной системе персональных данных» (Приложение 5 к настоящему Положению);

- проводить инструктаж пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- контролировать своевременное (не реже чем 2 раза в течение года) проведение смены паролей для доступа пользователей к компьютерам и ресурсам информационной системы персональных данных;

- обеспечивать постоянный контроль выполнения пользователями установленного комплекса мероприятий по обеспечению безопасности информации в информационной системе персональных данных;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в информационной системы персональных данных;

- вводить в базу данных средств защиты информации от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

- периодически тестировать функции средств защиты информации от несанкционированного доступа, особенно при изменении программной среды и полномочий исполнителей с отметкой в «Журнале периодического тестирования средств защиты информации» (Приложение 6 к настоящему Положению);

- восстанавливать программную среду средств защиты информации от несанкционированного доступа, программные средства и настройки средств защиты информации при сбоях;

- вести две копии программных средств и контролировать их работоспособность;

- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования информационной системы персональных данных и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

- периодически контролировать соответствие документально утвержденного состава аппаратной и программной части информационной системы персональных данных реальным конфигурациям информационной системы персональных данных , вести учет изменений аппаратно-программной конфигурации;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания информационной системы персональных данных и отправке его в ремонт (контролировать затирание персональных данных на магнитных носителях с составлением соответствующего акта);

- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию информационной системы персональных данных;

- вести «Журнал учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств на автоматизированных рабочих местах информационной системы персональных данных» (Приложение 7 к настоящему Положению);

- поддерживать установленный порядок проведения антивирусного контроля, согласно требованию настоящего Положения в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- по «Журналу учета хранилищ» (Приложение 8 к настоящему Положению) вести учет шкафов, сейфов, металлических шкафов и т.п., предназначенных для хранения носителей, содержащих персональные данные

- докладывать ответственному за защиту информации, ответственному за эксплуатацию информационной системы персональных данных о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

- вести документацию на информационной систему персональных данных в соответствии с требованиями нормативных документов.

6.11. Администратор безопасности и ответственный за защиту информации имеют право:

- требовать от пользователей информационной системы персональных данных соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в информационной системе персональных данных;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов информационной системы персональных данных;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

7. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.

7.1. К использованию, для создания резервной копии в информационной системе персональных данных, допускаются только зарегистрированные в журнале учета внешние (съемные) носители информации.

7.2. Администратор безопасности обязан осуществлять периодическое резервное копирование информационной системы персональных данных.

7.3. Еженедельно, по окончанию работы с документами, содержащими персональные данные на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию документов на зарегистрированный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный электронный архив.

7.4. Носители информации (ЖМД, ГМД, CD, DVD, USB накопитель, другие), предназначенные для создания резервной копии и хранения персональных данных выдаются установленным порядком администратором безопасности. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности.

7.5. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, ГМД, CD, DVD, USB накопитель) на отсутствие вирусов.

7.6. Файлы, помещаемые в электронный архив должны в обязательном

порядке проходить антивирусный контроль в соответствии с п. 7 настоящего Положения.

7.7. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD, DVD, USB накопитель и другие) резервной копии.

7.8. Резервное копирование производится в следующем порядке:

- к компьютеру подключается зарегистрированный электронный носитель (ЖМД, ГМД, CD, DVD, USB накопитель, другие) для резервного копирования;
- выбирается необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных создается файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполняется процедура создания резервной копии;
- производится копирование на отчуждаемый (внешний, съемный) носитель;
- производится отключение отчуждаемого носителя, который, после внесения необходимых записей в журналах, убирается в хранилище.

7.9. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище (сейфе, шкафе), имеющем запирающие и опечатывающие устройства совместно с ключевой и аутентифицирующей информацией.

7.10. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

7.11. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

7.12. При необходимости ремонта технических средств, с них, по согласованию с администратором безопасности, ответственным за защиту информации и представителем организации, проводившей аттестацию, удаляются опечатывающие пломбы, извлекается ЖМД и оборудование передается в сервисный центр. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

7.13. При работе на компьютерах информационной системы персональных данных должны использоваться источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

7.14. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации. Настройку данных средств должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

7.15. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище (сейфе, металлическом шкафе), имеющем запирающие и опечатывающие устройства. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

7.16. Ответственность за проведение резервного копирования в информационной системе персональных данных в соответствии с требованиями настоящего Положения возлагается на администратора.

7.17. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

8. Порядок контроля защиты информации в информационной системе персональных данных и приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления.

8.1. Контроль защиты информации в информационной системе персональных данных - комплекс организационных и технических мероприятий, которые осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами персональных данных, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

8.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в органах администрации Елизовского городского поселения;
- проверка учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- уточнение зон перехвата обрабатываемой на объектах информатизации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите информационной системы персональных данных от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в информационной системе персональных данных.

8.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в информационной системе персональных данных органов администрации поселения, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

8.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных;

- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов обеспечения безопасности персональных данных;

- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- эффективность применения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии, выданные установленным порядком ФСТЭК России.

8.5. Основными видами технического контроля являются:

- визуально-оптический контроль;

- контроль эффективности защиты информации от утечки по техническим каналам;

- контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

8.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации, ответственный за защиту информации докладывает Главе администрации поселения и (или) руководителю органа администрации поселения для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

8.7. Невыполнение предписанных мероприятий по защите персональных данных, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию Главы администрации Елизовского городского поселения и (или) руководителя органа администрации Елизовского городского поселения проводится расследование.

Для проведения расследования назначается комиссия. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования Глава администрации Елизовского городского поселения и (или) руководителя органа администрации Елизовского городского поселения принимают решение о применении мер дисциплинарного воздействия к виновным лицам и необходимых мероприятиях по устранению недостатков.

8.8. Контроль защиты информации осуществляется путем проведения периодических, плановых и контрольных проверок объектов защиты. Периодические, плановые и контрольные проверки объектов проводятся, как правило, силами администратора безопасности и (или) ответственного за защиту информации, в

соответствии с утвержденным планом или по согласованию с Главой администрации поселения или руководителем органа администрации поселения.

8.9. Одной из форм контроля защиты информации является обследование объектов информационной системы персональных данных. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования информационной системы персональных данных может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

8.10. Обследование информационной системы персональных данных проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в "Аттестате соответствия" и (или) требованиям по безопасности персональных данных.

8.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта информационной системы персональных данных условиям, сложившимся на момент проверки;
- соблюдение организационно-технических требований помещений, в которых располагается информационной системы персональных данных;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- соответствие выполняемых на объекте информационной системы персональных данных мероприятий по защите информации данным, изложенным в настоящем положении;
- выполнение требований по защите информационных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите.

8.12. Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения, а также документа установленной формы на право проведения проверки.

9. Порядок обучения пользователей практике работы в информационной системе персональных данных в части обеспечения безопасности (защиты) персональных данных.

9.1. Перед началом работы в информационной системе персональных данных пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

9.2. Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности и (или) ответственный за защиту информации должны вести журнал учета проверок знаний и навыков пользователей.

9.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего Положения, к работе в информационной системе персональных данных не допускаются.

9.4. Ответственным за организацию обучения и оказание методической помощи в органах администрации поселения является администратор безопасности и (или) ответственный за защиту информации.

9.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов информационной системы персональных данных, организаций-лицензиатов ФСТЭК России.

9.6. К работе в информационной системе персональных данных допускаются только пользователи, прошедшие первичный инструктаж обеспечения безопасности (защиты) в информационной системе персональных данных и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в информационной системе персональных данных.

10. Порядок проверки электронного журнала обращений к информационной системе персональных данных.

10.1. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в информационной системе персональных данных.

10.2. Право проверки электронного журнала обращений имеют:

- администратор безопасности;
- ответственный за защиту информации;
- руководитель органа администрации поселения;
- специальная комиссия, уполномоченная Главой администрации поселения на проведение проверки.

10.3. На технических средствах информационной системы персональных данных, на которых установлены специализированные средства защиты информации проверка электронного журнала производится в соответствии с прилагаемым к средствам защиты информации Руководством с отражением проверки в «Журнале периодического тестирования средств защиты информации».

10.4. В случае выявления в ходе периодических, плановых или контрольных проверок информационной системы персональных данных случаев несанкционированного доступа к информации конфиденциального характера применяется п. 8.7. настоящего Положения.

10.5. Проверке подлежат все электронные журналы информационной системы персональных данных.

10.6. Проверка должна проводиться не реже чем один раз в квартал с целью своевременного выявления фактов нарушения требований настоящего Положения.

10.7. Проверки электронных журналов отражаются в «Журнале проверок электронных журналов» (Приложение 9 к настоящему Положению). После каждой проверки администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

11. Правила антивирусной защиты.

11.1. К использованию на компьютерах допускаются только лицензионные антивирусные средства.

11.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

11.3. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

11.4. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

11.5. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD, DVD и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной информационной системы персональных данных класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

11.6. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

11.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка информационной системы персональных данных.

11.8. На компьютеры информационной системы персональных данных запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

11.9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с администратором безопасности должен провести внеочередной антивирусный контроль компьютера.

11.10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в информационной системе персональных данных;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также других должностных лиц

(работников), использующих эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

11.11. Ответственность за организацию антивирусного контроля в информационной системе персональных данных в соответствии с требованиями настоящего Положения возлагается на администратора безопасности и (или) ответственного за защиту информации.

11.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной информационной системе персональных данных и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной информационной системы персональных данных.

12. Правила парольной защиты.

12.1. Аутентификация авторизированных субъектов доступа осуществляется с помощью парольной защиты (логин + пароль), электронных ключей, комбинированных методов аутентификации (двухфакторная аутентификация) и других программно-технических средств разграничения доступа пользователей. Способ аутентификации авторизированных пользователей определяется в соответствии с уровнем конфиденциальности информации.

12.2. Активное сетевое оборудование (маршрутизаторы и сетевые принтеры) не должно допускать возможности несанкционированной переконфигурации, в связи с чем, каждое активное сетевое устройство должно быть защищено уникальным паролем.

12.3. Локальная и сетевая политики авторизации в информационной системе администрации поселения и ее органов должны быть настроены следующим образом:

- количество неудачных попыток авторизации до временной блокировки пользователя - не более 3;

- длительность временной блокировки доступа – не менее 15 минут;

- учетная запись «Гость» или «Guest» должна быть заблокирована;

- встроенная учетная запись «Администратор» («Administrator») должна быть переименована.

12.4. Личные пароли должны генерироваться и распределяться централизованно администратором парольной защиты с учетом следующих требований:

- длина пароля должна быть не менее 9 символов;

- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места (далее – АРМ) и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

12.5. При введении нового пользователя администратор парольной защиты должен назначить для него пароль, персональный код либо другую уникальную информацию для доступа к информационным ресурсам компьютерной сети.

12.6. Пользователь обязан хранить в тайне пароль, код и другие средства доступа к информационным ресурсам.

12.7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже двух раз в год или незамедлительно при создании предпосылок к его утрате (хищению) и (или) разглашению.

12.8. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться администратором парольной защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

12.9. В случае утраты надежности (компрометации) личного пароля пользователя должны быть немедленно предприняты меры в соответствии с пунктами 2.4, 2.5 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

12.10. При установке и переустановке автоматизированного рабочего места производится смена (установка) пароля администратора BIOS ПЭВМ с целью ограничения доступа к изменению параметров загрузки и системных характеристик.

12.11. Период действия паролей для сетевых компьютеров и для не сетевых компьютеров не должен превышать шести месяцев.

12.12. При окончании срока действия пароля администратор парольной защиты обязан сгенерировать и заменить его на новый, не применявшийся ранее.

12.13. Период действия паролей для входа в домен или локальную учетную запись автоматизированной системы не должен превышать шести месяцев.

12.14. Период действия паролей на изменение настроек антивирусной защиты не должен превышать шести месяцев.

12.15. Информация о паролях пользователей является конфиденциальной информацией.

12.16. Операционные системы серверов и рабочих станций должны быть настроены таким образом, чтобы исключить возможность ознакомления пользователей с действующими и истекшими паролями.

12.17. Информация о персональных кодах, электронных ключах и других средств доступа пользователей к информационному ресурсу является конфиденциальной информацией и разглашению не подлежит, должна содержать защиту от доступа посторонних лиц.

12.18. Опечатанный конверт с паролями исполнителей должен храниться в сейфе Управления делами. Для опечатывания конверта должна применяться печать учреждения. Пароли могут быть выданы только владельцу. В случае нарушения оттиска печати на конверте или утери конверта, пароли считаются скомпрометированными и подлежат немедленной смене.

12.19. Если пользователь уверен в правильности ввода названия учетной записи и пароля, но ему не удается войти в систему, пользователь обязан незамедлительно сообщить об этом администратору парольной защиты для получения нового пароля.

12.20. Если пользователь заметит несанкционированное появление, изменение или удаление информации, он должен немедленно сообщить об обнаруженных изменениях руководителю структурного подразделения, администратору парольной защиты и администратору безопасности.

12.21. Набор личного пароля следует проводить, в отсутствии лиц, которые потенциально могут увидеть процесс набора.

12.22. При оставлении рабочего места необходимо завершить открытую пользовательскую сессию либо использовать функцию «временной блокировки» рабочей станции (сочетание клавиш Windows + L).

12.23. Для предотвращения случайного оставления рабочего места с открытой пользовательской сессией рекомендуется использовать Screen Saver с автоматической блокировкой, включающийся автоматически, если компьютер не используется в течение определенного времени (5-10 минут).

12.24. Запрещается:

- передача личного пароля посторонним лицам, в том числе должностным лицам органов администрации поселения.
- запись личного пароля доступа на материальные носители (напр. бумагу, дискеты) в открытом виде.
- вход в компьютерную сеть и информационную систему с использованием чужих идентификаторов и паролей доступа.
- оставлять без присмотра рабочее место с открытой пользовательской сессией.

12.25. В случае подозрения о компрометации пароля, пользователь обязан незамедлительно поставить об этом в известность администратора парольной защиты и администратора безопасности для исключения возможности утечки информации.

12.26. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора парольной защиты и администратора безопасности.

12.27. Любые действия пользователей и посторонних лиц нарушающие требования настоящего Положения, категорируемые как значимые нарушения и нарушения, имеющие признаки компьютерного преступления, должны анализироваться через процедуру служебного расследования.

13. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн.

13.1. Все изменения конфигураций технических и программных средств информационной системы персональных данных должны производиться только на основании письменных заявок ответственного за эксплуатацию информационной системы персональных данных по согласованию с администратором безопасности и (или ответственным за защиту информации, а также (при проведении аттестационных мероприятий) с организацией, имеющей лицензию ФСТЭК России.

13.2. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных информационной системы персональных данных предоставляется:

- в отношении системных и прикладных программных средств, аппаратных средств, а также в отношении программно-аппаратных средств защиты - администратору безопасности по согласованию с органом по аттестации, проводившим аттестацию данной информационной системы персональных данных.

13.3. Изменение конфигурации аппаратно-программных средств информационной системы персональных данных кем-либо, кроме вышеперечисленных уполномоченных лиц и организаций, запрещено.

13.4. Процедура внесения изменений в конфигурацию системных и прикладных программных средств информационной системы персональных данных инициируется письменной заявкой ответственного за эксплуатацию информационной системы персональных данных.

13.5. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств информационной системы персональных данных:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной информационной системе персональных данных;
- обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

13.6. Также в заявке указывается наименование информационной системы персональных данных. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

13.7. Заявку ответственного за эксплуатацию информационной системы персональных данных, в которой требуется произвести изменения конфигурации, рассматривает руководитель органа администрации поселения, визирует ее, утверждая тем самым производственную необходимость и целесообразность проведения указанных в заявке изменений.

После чего заявка передается администратору безопасности и (или) ответственному за техническую защиту информации для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке информационной системы персональных данных.

13.8. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения информационной системы персональных данных тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от несанкционированного доступа и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации, проводившим аттестацию данной информационной системы персональных данных. Работы производятся в присутствии ответственного за эксплуатацию данной информационной системы персональных данных.

13.9. Установка или обновление подсистем информационной системы персональных данных должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

13.10. Установка и обновление программного обеспечения (системного, тестового и т.п.) на компьютерах информационной системы персональных данных производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного

программного обеспечения – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

13.11. Все добавляемые программные и аппаратные компоненты на компьютеры информационной системы персональных данных должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

13.12. После установки (обновления) программного обеспечения на компьютерах информационной системы персональных данных, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность программного обеспечения и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в информационной системе персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационной системы персональных данных», делает отметку о выполнении (на обратной стороне заявки).

13.13. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа по аттестации и в дальнейшем действует согласно их инструкций. В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с документацией на информационной системе персональных данных и «Журналом учета нештатных ситуаций информационной системы персональных данных, выполнения профилактических работ, установки и модификации программных средств на автоматизированных рабочих местах информационной системы персональных данных» у ответственного за защиту информации.

13.14. Копии заявок могут храниться у администратора безопасности:

- для восстановления конфигурации информационной системы персональных данных после аварий;
- для контроля правомерности установки на информационной системе персональных данных средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты информационной системы персональных данных.

13.15. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и пользователя, ответственного за эксплуатацию данной информационной системы персональных данных.

13.16. С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю, допущенному к работе на автоматизированном рабочем месте информационной системы персональных данных, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном автоматизированном рабочем месте.

13.17. Использование несколькими пользователями при работе в информационной системе персональных данных одного и того же имени пользователя («группового имени») запрещено.

13.18. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам информационной системы персональных данных инициируется заявкой ответственного за эксплуатацию данной информационной системы персональных данных.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя информационной системы персональных данных, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам информационной системы персональных данных ранее зарегистрированного пользователя);
- должность (с полным наименованием структурного подразделения), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного должностного лица (работника);
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в информационной системе персональных данных).

13.19. Заявку рассматривает руководитель органа администрации Елизовскогогородского поселения, визируя её, подтверждая тем самым производственную необходимость допуска (изменения прав доступа) конкретного пользователя к необходимым для решения им указанных в заявке задач ресурсам информационной системы персональных данных. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем информационной системы персональных данных.

13.20. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального пароля (регистрацию персонального идентификатора), заявленных прав доступа к ресурсам информационной системы персональных данных и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение шести месяцев.

13.21. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной информационной системы персональных данных. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор безопасности.

13.22. Пользователю, зарегистрированному в качестве нового пользователя информационной системы персональных данных, сообщается имя соответствующего ему пользователя, выдается персональный идентификатор и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

13.23. Исполненные заявка и задание (за подписью администратора безопасности) передаются ответственному за обеспечение безопасности информационной системы персональных данных.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий информационной системы персональных данных;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам информационной системы персональных данных при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам информационной системы персональных данных.

14. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических.

14.2. Порядок работы с техническими средствами защиты информации определен в соответствующих руководствах по настройке и использованию средств защиты информации обязательных для исполнения, как пользователи, обрабатывающими персональные данные, так и администратором безопасности информационной системы персональных данных.

14.3. Право проверки соблюдения условий использования средств защиты информации имеют:

- администратор безопасности;
- ответственный за защиту информации;
- руководитель органа администрации поселения;
- специальная комиссия, уполномоченная Главой администрации поселения на проведение проверки.

14.4. Пользователю информационной системы персональных данных категорически запрещается:

- обрабатывать персональные данные с отключенными средствами защиты информации;
- менять настройки средств защиты информации.

14.5. Администратору безопасности запрещается менять настройки программно-аппаратных средств защиты информации, предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

14.6. Если в ходе периодических, плановых или внезапных проверок информационной системы персональных данных выявлено нарушение требования п. 14.4. то вступает в силу п. 8.7. настоящего Положения.

15. Порядок охраны и допуска посторонних лиц в служебные помещения.

15.1. Сдача под охрану (вскрытие) служебных помещений, в которых происходит обработка персональных данных (далее – служебные помещения), сдача (получение) ключей от них и выдача разрешения на отключение охранной сигнализации (при ее наличии) данных помещений производится только работниками, которые осуществляют служебную деятельность (работают) в этих помещениях (далее – ответственные лица), на основании списка, подписанного руководителем органа администрации поселения.

15.2. Список ответственных за вскрытие (сдачу) служебных помещений передается на пост охраны.

15.3. Ответственные лица после окончания работы в служебных помещениях обязаны:

- закрыть окна и форточки;
- закрыть жалюзи;
- сообщить дежурному поста охраны о подготовке к сдаче помещения;
- закрыть и опечатать помещение;
- предъявить дежурному поста охраны оттиск печати на входной двери в помещение;
- дать разрешение на включение охранной сигнализации (при ее наличии в служебном помещении) и убеждаются в ее исправности;
- передать дежурному поста охраны ключи от помещения;
- сделать запись о сдаче помещения под охрану и поставить свою подпись в журнале приема-сдачи служебных помещений.

15.4. Ответственные лица перед началом работы в служебных помещениях обязаны:

- убедиться в исправности охранной сигнализации (при ее наличии) вскрываемого служебного помещения;
- вскрыть служебное помещение;
- убедиться в срабатывании охранной сигнализации вскрываемого помещения;
- сделать запись о вскрытии помещения и поставить подпись в журнале приема-сдачи служебных помещений.

15.5. Журнал приема-сдачи служебных помещений должен быть учтен в делопроизводстве. Листы данного журнала должны быть пронумерованы, прошнурованы, скреплены наклейкой с оттиском печати «Для пакетов», о чем делается заверительная запись.

15.6. Ответственное лицо, допустившее утрату ключей от служебного помещения, обязано немедленно доложить об этом непосредственному руководителю, проинформировать дежурного поста охраны и руководителя органа администрации поселения.

15.7. Принятые под охрану служебные помещения при срабатывании охранной или пожарной сигнализации, при обнаружении протечек и других технологических аварий, а также при возникновении чрезвычайных и других ситуаций, требующих вскрытия служебных помещений, вскрываются:

- комиссией в составе: дежурного поста охраны, ответственного лица за служебное помещение и руководителя органа администрации поселения;
- дежурным поста охраны для беспрепятственного доступа аварийно-спасательной, эвакуационной команды соответствующих дежурных служб.

При отсутствии ответственного лица, дежурный поста самостоятельно вскрывает служебное помещение для локализации последствий, указанных выше. О данном факте делается контрольная запись в Журнале приема-сдачи дежурства и Журнале приема-сдачи служебных помещений, с последующим докладом по команде руководителям соответствующих служб и руководителю органа администрации Елизовского городского поселения.

15.8. Принятые под охрану служебные помещения в рабочее время во время отсутствия ответственных лиц, вскрываются комиссионно на основании приказа руководителя органа администрации поселения.

15.9. При вскрытии служебных помещений, комиссия проверяет целостность оттисков печатей и исправность запоров на входных дверях.

При обнаружении нарушения целостности оттисков печатей, повреждения запоров или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, председатель комиссии:

- немедленно доводит о случившемся дежурному поста охраны и докладывает руководителю органа администрации;

- организует дополнительную охрану служебного помещения.

До прибытия ответственного лица:

- доступ в служебное помещение должностных лиц осуществляется по указанию руководителя органа администрации поселения.

По данному факту составляется акт.

15.10. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличии других признаков, указывающих на проникновение в служебное помещение посторонних лиц, ответственным должностным лицом (служащим, работником) проводятся действия, указанные в п. 15.9. настоящего Положения.

15.11. При возникновении пожара и (или) иных чрезвычайных ситуаций дежурный поста охраны немедленно вызывает аварийно-спасательные службы, оповещает должностных лиц и граждан, находящихся в здании, принимают меры к организации ликвидации очага возгорания, вредных последствий чрезвычайной ситуации и по эвакуации имущества, в том числе защищаемой информации.

15.12. Уборка, другие необходимые хозяйственные и ремонтные работы в служебных помещениях производятся только в присутствии ответственных лиц в рабочее время.

16. Порядок удаления защищаемой информации и уничтожения носителей защищаемой информации.

16.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Удалению подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе информационной системы персональных данных. Не допускается удаление неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

16.2. Удаление должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

16.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантированное стирание информации

на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

16.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

16.5. По факту уничтожения носителей составляется акт, в журналах учета делаются соответствующие записи.

16.6. Процедуры удаления и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию информационной системы персональных данных, ответственный за защиту информации, администратор безопасности.

17. Заключительные положения.

17.1. В соответствии со статьей 90 Трудового кодекса Российской Федерации и статьей 24 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных муниципального служащего (работника), привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение № 4
к Положению, утвержденному
постановлением администрации
Елизовского городского поселения
от _____ № _____

Журнал
поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

№ п.п.	Наименование средства защиты информации, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СЗИ, эксплуатационной и технической документации к ним	Отметка о получении		Отметка о выдаче	
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя	Дата и расписка в получении
1	2	3	4	5	6	7

Отметка о подключении (установке) СЗИ			Отметка об изъятии СЗИ из аппаратных средств			Примечание
Ф.И.О. пользователя, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
8	9	10	11	12	13	14

Приложение № 3
к Положению, утвержденному
постановлением администрации
Елизовского городского поселения
от _____ № _____

Журнал
учета внешних (съемных) носителей информации

№ п/п	Регистрационный (учетный) номер носителя	Вид носителя	Тип носителя и его емкость	Дата поступления
1	2	3	4	5

Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
6	7	8	9	10

Приложение № 8
к Положению, утвержденному
постановлением администрации
Елизовского городского поселения
от _____№ _____

Журнал
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата
1	2	3	4	5

Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
6	7	8

Приложение № 6
к Положению, утверждённому
постановлением администрации
Елизовского городского поселения
от _____ № _____

Журнал
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование
1	2	3	4	5

Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
6	7	8

Приложение № 7
к Положению, утвержденному
постановлением администрации
Елизовского городского поселения
от _____ № _____

Журнал

учета нештатных ситуаций информационной системы персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационной системы персональных данных

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи
1	2	3	4

ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
5	6	7

Приложение № 5
к Положению, утвержденному
постановлением администрации
Елизовского городского поселения
от _____№ _____

Журнал
учета пользователей, допущенных к информационным системам персональных данных

№ п/п	Дата	Фамилия, имя, отчество пользователя	Наименование информационной системы персональных данных
1	2	3	4

Подпись пользователя об ознакомлении с Положением и требованиями по безопасности	Подпись администратора безопасности о готовности пользователя к работе в информационной системе персональных данных	Примечание
5	6	7

Приложение № 9
к Положению, утвержденному
постановлением администрации
Елизовского городского поселения
от _____ № _____

Журнал
проверок электронных журналов

№ п/п	Дата проверки	Наименование информационной системы персональных данных, компьютера, технического средства	Наименование проверяемого журнал
1	2	3	4

Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора безопасности	Примечание
5	6	7

Приложение № 1
к Положению, утвержденному
постановлением Администрации
Елизовского муниципального района
от _____ № _____

Согласие на обработку персональных данных

г. Елизово « » _____ 20__ года

Я, _____,
серия_____номер_____выдан_____
(вид документа, удостоверяющего личность)
_____
проживающий(ая) по
адресу:_____
_____
в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 г. № 152-ФЗ "О персональных данных", подтверждаю свое согласие на обработку моих персональных данных
_____(далее Оператор),
(наименование организации)
расположенного по адресу:
_____,
включающих:
_____
_____
_____
(перечень персональных данных)
в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества, иных целях:
_____
_____

Предоставляю Оператору право осуществлять все действия, которые необходимы или желаемы для достижения указанных выше целей (операций) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов).

Обработка персональных данных осуществляется Оператором с применением следующих основных способов (но, не ограничиваясь ими): хранение, запись на электронные носители и их хранение, составление перечней, маркировка.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дается до истечения сроков хранения соответствующей информации или документов, содержащих вышеуказанную информацию, определяемых в соответствии с законодательством Российской Федерации, а также может быть отозвано путем направления мною соответствующего письменного уведомления, которые может быть направлено в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручено лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует до _____
_____
(Ф.И.О., подпись лица, давшего согласие)

Приложение № 2
к Положению, утвержденному
постановлением Администрации
Елизовского муниципального района
от _____№_____

Оператор:
_____
_____

Субъект персональных данных:
_____,
зарегистрированный по адресу:
_____
_____,
паспорт серии: _____№_____
выдан «___»_____,_____
_____

Третья сторона:
_____
(наименование, адрес)
_____

ЗАЯВЛЕНИЕ
о согласии на передачу персональных данных третьим лицам

Даю согласие на передачу оператором третьей стороне: _____
_____
_____ следующих
персональных данных: _____
_____
_____
_____
(перечень персональных данных для передачи)

с целью исполнения служебных обязанностей связанных с занимаемой должностью:
_____
_____

В случае неправомерного использования предоставленных персональных данных соглашение отзывается письменным заявлением субъекта персональных данных.

Данное согласие действует с «___»_____20 г. по «___»_____20 г. включительно.

Субъект персональных данных: _____/_____/
подпись расшифровка подписи

«_____»_____20 ___ г.

Третья сторона предупреждена:
- об использовании полученных персональных данных субъекта персональных данных, лишь в целях, для которых они сообщены предоставлении по требованию оператора подтверждения о соблюдении этого правила;
-о соблюдении режима конфиденциальности полученных персональных данных.