УТВЕРЖДАЮ:
Генеральный директор
ЗАО «Оборонпромкомплекс»
_____ Г.И. Тарусин
«17» октября 2011г.

ПОЛОЖЕНИЕ

ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАО «ОБОРОНПРОМКОМПЛЕКС»

Г.Иркутск
2011 г.

СОДЕРЖАНИЕ

ВВОДНЫЕ ПОЛОЖЕНИЯ

ВВЕДЕНИЕ

Положение об обработке и защите персональных данных в Закрытом акционерном обществе «Оборонпромкомплекс» (далее - ПОЛОЖЕНИЕ) разработано в соответствии с:

- Конституцией Российской Федерации от 12.12.1993;
- Гражданским кодексом Российской Федерации;
- Кодексом Российской Федерации об административных правонарушениях от 30.12.2001 № 195 – ФЗ;
- Трудовым кодексом Российской Федерации от 30 декабря 2001 года № 197-ФЗ;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Совместным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;

ЗАДАЧИ

Настоящее ПОЛОЖЕНИЕ устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников ЗАО «Оборонпромкомплекс» (далее - Общество) и лиц обращающихся в Общество. ПОЛОЖЕНИЕ призвано исключить возможность утечки и несанкционированного доступа к персональным данным в процессе их накопления, хранения, обработки, передачи и использования за счет:

- установления перечня персональных данных;
- определения порядка обращения информации содержащей персональные данные;

- определения порядка взаимодействия сотрудников Общества при обеспечении сохранности персональных, а также установления ответственности за разглашение персональных данных.

ЦЕЛИ

ПОЛОЖЕНИЕ определяет порядок обработки персональных данных, относящихся к специальным категориям персональных данных, персональных данных сотрудников Общества и иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Общества, обеспечивает защиту прав и свобод человека и гражданина, при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

ОБЛАСТЬ ДЕЙСТВИЯ

Настоящее ПОЛОЖЕНИЕ обязательно для исполнения всеми сотрудниками Общества.

Организационные, распорядительные и локальные нормативные документы администрации в части работы с персональными данными и защиты информации о персональных данных, не должны противоречить настоящему ПОЛОЖЕНИЮ.

ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

Настоящее ПОЛОЖЕНИЕ является локальным нормативным документом постоянного действия.

Настоящее ПОЛОЖЕНИЕ вводится в действие приказом Генерального директора Общества.

ПОЛОЖЕНИЕ признается утратившим силу на основании приказа Генерального директора Общества.

Изменения в ПОЛОЖЕНИЕ вносятся приказом Генерального директора Общества.

Изменения в ПОЛОЖЕНИЕ вносятся, в случаях: изменения законодательства Российской Федерации, изменения организационной структуры или полномочий руководителей структурных подразделений Общества, совершенствования системы информационной безопасности и т.п.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем ПОЛОЖЕНИИ используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная система в защищенном исполнении (АСЗИ) – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации[1].

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз[2].

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения

[1] ГОСТ Р 51624-2000.
[2] Закон Российской Федерации "О безопасности".

персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Держатель персональных данных является администрация, которой собственник (субъект) добровольно (на основании согласия на обработку персональных данных) передает во владение свои персональные данные. Держатель персональных данных выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства**.**

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Инсталляция – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствие с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной

системе и готовым решать определенный класс задач в определенном режиме работы[3].

Информация – сведения независимо от формы их представления.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – 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.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[4].

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Канал атаки – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

---

[3] В. Дорот, Ф. Новиков «Толковый словарь современной компьютерной лексики», СПб., БХВ-Петербург, 2004.

[4] Федеральный закон «Об информации, информационных технологиях и о защите информации».

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения[5].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя[6].

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Криптографически опасная информация (КОИ) – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну[7].

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности».

Локальные нормативные документы – внутренние регламентирующие документы структурных подразделений администрации, в данном случае в части работы с персональными данными и защиты информации о персональных данных

Модель угроз – перечень возможных угроз.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

---

[5] ГОСТ Р 51624-2000.

[6] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[7] «Положение о разработке, производстве, реализации и шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрировано Минюстом России (регистрационный № 6382 от 3 марта 2005 года)

Неавтоматизированная обработка персональных данных – 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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Негативные функциональные возможности – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

- модифицировать или искажать алгоритм работы криптосредств в процессе их использования;
- модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;
- получать доступ нарушителям к хранящейся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

Недокументированные (недекларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение характеристик безопасности защищаемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

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

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.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Опубликованные возможности ПО или ТС – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.).

Специальная защита – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

Среда функционирования криптосредства (СФК) – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации[8].

Средство вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[9].

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

[8] ГОСТ Р 50922-96.
[9] ГОСТ Р 50739-95.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Работодатель – Генеральный директор ЗАО «Оборонпромкомплекс».

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект - собственник информационных ресурсов (персональных данных), в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные. Субъект самостоятельно решает вопрос передачи своих персональных данных на основании согласия на обработку персональных данных.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уровень криптографической защиты информации – совокупность требований, предъявляемых к криптосредству.

Успешная атака – атака, достигшая своей цели.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Шифровальные (криптографические) средства:

а) средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации)[10].

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

[10] Постановление Правительства Российской Федерации от 23 сентября 2002 года № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» (Собрание законодательства Российской Федерации, 2002 г., № 39, ст. 3792).

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
СТР-К – специальные требования к сведениям конфиденциального характера
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

3. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. В состав персональных данных, обрабатываемых в администрации, входит информация, необходимая администрации в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни, как сотрудника, так и лица обратившегося в администрацию, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- все биографические сведения сотрудника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора и дополнений к нему;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии распоряжений (локальных нормативных актов) по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;
- социальное положение;
- основания к распоряжениям (локальным нормативным актам) по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- отчеты направляемые в органы статистики и их копии;
- анкета;
- сведения о награждениях и поощрениях;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные биометрические сведения;
- свидетельство о присвоении ИНН, либо данные содержащиеся в нем;
- страховое свидетельство государственного пенсионного страхования;
- связи за рубежом;
- выезды за границу;
- иные сведения относящиеся к персональным данным.

К бумажным носителям персональных данных относятся:

– журналы учета трудовых книжек;
– журнал учета командировок;
– материалы по учету рабочего времени;
– журналы сверки и учета по военнообязанным;
– выписки из книг учета содержащих персональные данные;
– копии документов содержащих персональные данные;
– входящая и исходящая корреспонденция военкомата, страховой компании, службы судебных приставов;
– журналы приема граждан по личным вопросам и материалы рассмотрения обращений;
– материалы рассмотрения протоколов об административных правонарушениях;
– лицевые счета;
– документы по обеспечению малоимущих граждан;
– материалы по формированию резерва управленческих кадров администрации;
– материалы по организации похоронного дела;
– материалы по выдаче разрешений на переустройство и перепланировку жилых помещений;
– документы по признанию жилых помещений пригодными (не пригодными) для проживания;
– свидетельства о государственной регистрации права на не движимое имущество;
– документальные материалы по выдаче разрешений на строительство;
– документальные материалы по вводу индивидуального строительства в эксплуатацию.

Указанные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено Законодательством.

Права и обязанности держателя персональных данных осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности работодатель может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных субъектов или связана с обработкой этих данных.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3.1.1. Персональные данные сотрудников администрации:

- личные данные сотрудников администрации: паспортные данные; адрес фактического проживания; семейное, социальное, имущественное положение; образование; профессия; доходы;
- условия трудовых договоров, заключенных с сотрудниками администрации;
- сведения по страхованию сотрудников администрации, в том числе суммы страхования и размер страховых премий, перечисленных в страховую организацию, определенную по результатам проведенного тендера;
- сведения по военно-учетному столу;
- сведения об уровне заработной платы сотрудников, за исключением сведений о системе оплаты труда;
- сведения о результатах тестирования, проводимых согласно методическим материалам по организации оценочных процедур при приеме на работу, замещении вакантных должностей и формировании кадрового резерва в администрации;
- телефонный справочник администрации, в том числе списки электронных адресов сотрудников.

3.1.2. Информация, представляемая сотрудником при поступлении на работу в администрацию, должна иметь документальную форму. При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у сотрудника).
- При оформлении сотрудника в администрации сотрудниками отдела муниципальной службы, заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные сотрудника:
- общие сведения (Ф.И.О. сотрудника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;

3.1.3. В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах.

3.1.4. В отделе муниципальной службы создаются и хранятся следующие группы документов, содержащие данные о сотрудниках в единичном или сводном виде:

- документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии распоряжений по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания распоряжений по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству администрации, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);
- документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции сотрудников, приказы, распоряжения, указания руководства администрации; документы по планированию, учету, анализу и отчетности в части работы с персоналом.

3.2. Персональные данные субъектов, не являющихся сотрудниками администрации, обработка которых необходима для обеспечения деятельности администрации, либо оформления документальных материалов запрашиваемых субъектом.

3.2.1. Для осуществления пропускного режима в администрации ведется журнал, содержащий персональные данные, необходимые для пропуска субъекта персональных данных в здания администрации.

3.3. Специальные категории персональных данных:

3.3.1. В состав специальных категорий персональных данных входят данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

3.3.2. Обработка специальных категорий персональных данных допускается только в случае, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта персональных данных 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 согласия субъекта персональных данных невозможно.

3.3.3. Выдача документов, содержащих персональные данные работников осуществляется в соответствии со ст. 62 Трудового кодекса Российской Федерации с соблюдением следующей процедуры:

- заявление сотрудника о выдаче того или иного документа на имя начальника отдела муниципальной службы;
- выдача заверенной копии (в количестве экземпляров, необходимом сотруднику) заявленного документа, либо справки о заявленном документе или сведениях, содержащихся в нем;
- внесения соответствующих записей в журнал учета выданной информации (Приложение 8)

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных – получение, хранение, комбинирование, передача или любое другое использование персональных данных физического лица. Обработка персональных данных сотрудника осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов, предусмотренных законодательством Российской Федерации и внутренними документами администрации.

4.2. Администрация не имеет права получать и обрабатывать персональные данные сотрудника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации администрация вправе получать и обрабатывать персональные данные сотрудника только с его письменного согласия (приложение 1). Администрация не имеет права получать и обрабатывать персональные данные сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации. При принятии решений, затрагивающих интересы сотрудника, администрация не имеет права основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.3. На основании статьи 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», обработка персональных данных в администрации осуществляется без письменного согласия сотрудника и субъекта, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.4. Получение персональных данных:

4.4.1. Сотрудник и субъект обязаны предоставлять администрации достоверные сведения о себе и своевременно сообщать ему об изменении своих персональных данных. Специалисты администрации проверяют достоверность предоставленных сведений, сверяя предоставленные данные с имеющимися документами.

4.4.2. В случаях, когда администрация может получить необходимые персональные данные только у третьей стороны, администрация должна уведомить об этом сотрудника или субъекта и получить от него письменное согласие по установленной форме (приложение 1). Администрация обязана сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа дать письменное согласие на их получение.

4.5. Хранение персональных данных:

4.5.1. Персональные данные сотрудников хранятся в отделе муниципальной службы администрации в сейфах (опечатываемых хранилищах). Личные дела сотрудников хранятся как в электронном, так и бумажном виде. Персональные данные субъектов хранятся в структурных подразделениях администрации в соответствии с условиями, обеспечивающими их надежную сохранность.

4.5.2. Сотрудники администрации, имеющие доступ к персональным данным в связи с исполнением трудовых обязанностей:

- обеспечивают хранение информации, содержащей персональные данные, исключающее доступ к ним третьих лиц;
- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия на своем рабочем месте, сотрудник обязан передать документы и иные носители, содержащие персональные данные лицу, на которое будет возложено исполнение его трудовых обязанностей.

4.5.3. При увольнении сотрудника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию руководителя структурного подразделения.

4.5.4. Хранение персональных данных осуществляется как в электронном, так и бумажном виде в сейфах (опечатываемых хранилищах) структурных подразделений администрации, непосредственно производящих их обработку.

4.5.5. Помещения, в которых хранятся персональные данные, по окончании рабочего дня опечатываются и сдаются под охрану.

4.6. Использование персональных данных:

4.6.1. Доступ к персональным данным имеют сотрудники администрации, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей. Перечень сотрудников, имеющих доступ к персональным данным, утверждается распоряжением администрации.

4.6.2. В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией главы администрации, доступ к персональным данным может быть предоставлен иному сотруднику, который не включен в распоряжение о назначении ответственных сотрудников для доступа к персональным данным, и которым они необходимы в связи с исполнением трудовых обязанностей.

4.6.3. В случае если администрация пользуется услугами юридических и физических лиц на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным, то соответствующие данные предоставляются только после подписания с ними обязательства о неразглашении сведений, содержащих персональные данные (приложение 3).

4.6.4. В отдельных случаях, исходя из договорных отношений с контрагентом, такие отношения могут регулироваться отдельным разделом в договоре (приложение 4), в том числе предусматривающих защиту персональных данных такие отношения могут регулироваться отдельным разделом в договоре.

4.6.5. Процедура оформления доступа сотрудника к персональным данным включает в себя:

- ознакомление сотрудника под роспись с настоящим ПОЛОЖЕНИЕМ, распоряжениями, приказами, актами и другими документами, регламентирующими работу с персональными данными в администрации;
- принятие сотрудником обязательств о неразглашении сведений конфиденциального характера и соблюдении режима конфиденциальности (приложение 2).

4.6.6. Сотрудники администрации, имеющие доступ к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения конкретных трудовых обязанностей.

4.6.7. Допуск к персональным данным сотрудникам администрации, не имеющим надлежащим образом оформленного доступа, запрещается.

4.6.8. Структурные подразделения администрации вправе передавать персональные данные в иные структурные подразделения администрации в случае необходимости исполнения сотрудниками, соответствующих структурных подразделений, своих трудовых обязанностей.

4.6.9. При передаче персональных данных, лица, получающие данную информацию, предупреждаются о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и с них требуется обязательство о неразглашении сведений, содержащих персональные данные (приложение 6).

4.6.10. Передача (обмен и т.д.) персональных данных между структурными подразделениями администрации осуществляется только между сотрудниками, имеющими доступ к соответствующим персональным данным.

4.7. Доступ к персональным данным третьих лиц (физических и юридических):

4.7.1. Передача персональных данных третьим лицам осуществляется только с письменного согласия (приложение 1)

4.7.2. Не допускается передача персональных данных в коммерческих целях без письменного согласия.

4.7.3. Передача сведений содержащих персональные данные контрагентам в рамках установленных договорных отношений осуществляется посредством подписания сторонами Акта приема-передачи (приложение 6). Со стороны администрации указанный Акт подписывается должностным лицом, не ниже руководителя структурного подразделения или лицом его замещающим. Акт должен содержать следующие условия:

- уведомление лица, получающего данные документы, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;
- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с законодательством Российской Федерации.

4.7.4. Передача документов (иных материальных носителей), содержащих персональные данные, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг;
- обязательства о неразглашении конфиденциальной информации (приложение 3), либо наличие в договоре с третьим лицом раздела договора о сохранности сведений содержащих персональные данные (приложение 4);
- письма-запроса от третьего лица, которое должно включать в себя указание на основании получения доступа к запрашиваемой информации, содержащей персональные данные, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

4.7.5. Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных несет руководитель структурного подразделения, осуществляющего передачу персональных данных третьим лицам.

4.7.6. Представителю персональные данные передаются в порядке, установленном действующим законодательством и настоящим ПОЛОЖЕНИЕМ.

4.7.7. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя;
- письменного заявления, написанного в присутствии сотрудника администрации (если заявление написано не в присутствии сотрудника администрации, то оно должно быть нотариально заверено).

4.7.8. Предоставление персональных данных государственным органам производится в соответствии с требованиями действующего законодательства и настоящим ПОЛОЖЕНИЕМ.

4.7.9. Персональные данные могут быть предоставлены родственникам или членам семьи только с письменного разрешения (приложение 1), за исключением случаев, когда передача персональных данных без согласия допускается действующим законодательством Российской Федерации.

4.7.10. Документы, содержащие персональные данные, могут быть отправлены через организацию Федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные, вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

4.8. Уничтожение персональных данных.

4.8.1. Персональные данные должны храниться в администрации не дольше, чем этого требуют цели их обработки, а по достижении целей обработки или утраты необходимости в их достижении персональная информация подлежит уничтожению в соответствии со ст.21 № 152-ФЗ от 27.07.2006, в течении тридцати дней, если иное не предусмотрено Законодательством Российской Федерации.

4.8.2. Номенклатурные дела временного срока хранения, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством об архивном деле в Российской Федерации, электронные носители информации, и другие документальные материалы, содержащие персональные данные находятся в администрации до истечения срока их хранения, после чего уничтожаются согласно актам (приложение 7).

4.8.3. При уничтожении персональных данных, лица производящие отбор данных материалов обязаны исключать возможность преждевременного их уничтожения.

5. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Защита персональных данных от неправомерного их использования или утраты обеспечивается системой защиты персональных данных.

5.2. Общую организацию защиты персональных данных лиц осуществляет отдел по защите информации администрации.

5.3. Отдел по защите информации совместно с руководителями структурных подразделений обеспечивает:

- ознакомление сотрудников, которые участвуют в обработке персональных данных, под роспись с настоящим ПОЛОЖЕНИЕМ, регламентирующими документами, актами и другими документами, регламентирующими работу с персональными данными в администрации;
- получение от сотрудника, обрабатывающего персональные данные, обязательства о неразглашении сведений содержащих персональные данные (приложение 2);
- общий контроль соблюдения сотрудниками администрации мер по защите персональных данных.

5.4. Организацию и контроль защиты персональных данных в структурных подразделениях администрации, осуществляют специально назначенные сотрудники структурных подразделений совместно с руководителями структурных подразделений, которые руководствуются должностным регламентом специалиста по обеспечению безопасности персональных данных (Приложение 10).

5.5. Защите подлежит:

- информация о персональных данных субъектов;
- документы, содержащие персональные данные субъектов;
- персональные данные, содержащиеся на электронных носителях.

6. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ АВТОМАТИЗАЦИИ

6.1. В соответствии с п. 1.3. Приказа ФСТЭК России № 58 от 05.02.2010, в каждой ИСПДн структурных подразделений администрации назначается ответственный за работу с персональными данными. Ответственные назначаются распоряжением администрации (локальными нормативными

актами руководителей структурных подразделений). Для функционирования информационной системы в штатном режиме и для разграничения прав пользователей, согласно созданной для каждого ИСПДн матрицы доступа, распоряжением администрации назначается администратор безопасности.

6.2. Отдел по защите информации администрации проводит ревизию информационных систем в администрации. По результатам ревизии разрабатывается перечень информационных ресурсов.

6.3. Распоряжением администрации, в соответствии с п. 3.6 СТР-К, утверждается перечень сведений конфиденциального характера.

6.4. Защита сведений, хранящихся в электронных базах данных администрации, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается системой защиты персональных данных, включающей организационные меры, и (по мере необходимости) технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

6.5. В целях реализации требований ПОЛОЖЕНИЯ, решение вопросов в данном направлении возлагается на отдел по защите информации администрации.

6.5.1. Задачами отдела по защите информации администрации, в сфере обеспечения защиты персональных данных являются:

- классификация информационных систем персональных данных в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным совместным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20;
- определение лиц, допущенных к обработке персональных данных (либо имеющих к ним доступ) в связи с выполнением своих служебных (трудовых) обязанностей и допуск их распоряжением администрации;
- установление и утверждение перечня персональных данных, информационных систем и технических средств, используемых для их обработки в администрации, места хранения персональных данных (материальных носителей);

- установление и утверждение категорий персональных данных, обработка которых осуществляется в администрации, как с использованием, так и без использования средств автоматизации;

- утверждение правил осуществления обработки персональных данных, осуществляемой без использования средств автоматизации;

- определение условий и утверждение перечня мер, необходимых для обеспечения в администрации условий по сохранности персональных данных и исключающих несанкционированный к ним доступ, а также перечня лиц, ответственных за реализацию указанных мер;

- разработка организационных документов администрации о порядке эксплуатации информационной системы персональных данных;

- определение методов и способов защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы в администрации в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденным приказом Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58;

- разработка и принятие иных документов и мер, направленных на обеспечение информационной безопасности персональных данных в администрации.

6.6. Технические меры по защите персональных данных

6.6.1. Технические меры по защите персональных данных включают в себя:

- исключение возможности несанкционированного доступа к персональным данным в администрации лицам, не допущенным к обработке персональных данных в установленном порядке;

- установку, настройку и сопровождение технических и программных средств защиты информации (в том числе шифровальных (криптографических) средств, средств предотвращения несанкционированного доступа и утечки информации по техническим каналам.

6.6.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

- при отсутствии установленных и настроенных сертифицированных средств защиты информации;

- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

- в случаях, когда возможно визуальное считывание персональных данных с монитора посторонними лицами;

- запрещается при обработке персональных данных в слух зачитывать (диктовать) персональные данные.

6.6.3. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме (Приложение 7).

6.6.4. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых металлических шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность от повреждений при воздействии внешних факторов.

6.6.5. Доступ к персональным данным, содержащихся на электронных носителях, осуществляется только с помощью установленного пароля, либо специально установленных технических средств защиты.

6.6.6. Решение, порождающее юридические последствия в отношении лица, или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных, только при наличии его согласия в письменной форме, или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов лица.

7. ПРАВА СУБЪЕКТОВ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Субъекты обработки персональных данных имеют право:

7.1.1. Получать полную информацию об их персональных данных и обработке этих данных, свободный бесплатный доступ к своим персональным данным, и ознакомление с ними, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных законодательством Российской Федерации;

7.1.2. Требовать от администрации уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не, являющих необходимыми (для администрации) персональных данных субъекта;

7.1.3. Получать от администрации:

- сведения о лицах, которые имеют доступ к персональным данным субъекта, или которым может быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7.1.4. Определение своих представителей для защиты своих персональных данных;

7.1.5. Доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

7.1.6. Требовать от администрации извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

7.1.7. Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего ПОЛОЖЕНИЯ. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;

7.1.8. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия администрации при обработке и защите его персональных данных.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Иные права, обязанности, действия сотрудников, в трудовые обязанности, которых входит обработка персональных данных, определяются должностными инструкциями.

8.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

8.3. Разглашение персональных данных (передача их посторонним лицам, в том числе, сотрудникам администрации, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъектов, а также иные нарушения обязанностей по их

защите и обработке, установленных настоящим ПОЛОЖЕНИЕМ, локальными нормативными актами (приказами, распоряжениями) администрации, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарной ответственности.

8.4. Сотрудники администрации, имеющие доступ к персональным данным субъектов, виновные в незаконном разглашении или использовании персональных данных без согласия из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии с Уголовным Кодексом Российской Федерации. Сотрудники администрации, имеющие доступ к персональным данным и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба администрации, в соответствии с Трудовым Кодексом Российской Федерации.

Приложение 1
к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

Главе администрации
Ленинского муниципального района
Еврейской автономной области

от _____
_____
(Ф.И.О., должность)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(фамилия, имя, отчество)
документ, удостоверяющий личность _____
(вид документа)
_____№_____выдан_____
_____
(кем и когда)
проживающий (ая) по адресу _____
_____
_____,
даю согласие администрации Ленинского муниципального района ЕАО, с. Ленинское, Ленинского района ЕАО, ул. Ленина 16, на обработку моих персональных данных, а именно:

- Фамилия;
- Имя;
- Отчество;
- Год, месяц, дата рождения, место рождения;
- Адрес;
- Паспортные данные (серия, номер, кем и когда выдан);
- Гражданство;
- ИНН;
- _____.
- _____;
- _____;
- _____;
- _____.
- _____;
- _____.
- _____;
- _____.

(указывается полный перечень персональных данных, согласие на обработку которых дается)

с целью _____
_____
_____
_____.

(указывается цель обработки персональных данных)

А также на работу с моими персональными данными: получение у третьей стороны, передачу третьей стороне, передачу в коммерческих целях, а именно:

- сотрудникам администрации, доступ которых к персональным данным, необходим для выполнения служебных обязанностей;
- архиву, для хранения;
- военному комиссариату, для организации воинского учета;
- налоговой инспекции, для _____
- пенсионному фонду, для _____
-страховой компании, для оформления медицинского полиса обязательного страхования граждан;
- банку, для открытия и ведения счета заработной платы.

_____
_____
_____
_____

(Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я уведомлен(а) о своем праве отозвать согласие путем подачи письменного заявления. Подтверждаю, что отзыв согласия производится в письменном виде в соответствии с действующим законодательством. Всю ответственность за неблагоприятные последствия отзыва согласия беру на себя.

Подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока.

_____ _____

(Ф.И.О.) *(подпись)*

«___» _____ 20____ г.

Примечание: Перечень должностных лиц, имеющих доступ к персональным данным, устанавливается распоряжением (локальными нормативными актами структурных подразделений) администрации.

Приложение № 2

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных ставших известными в период исполнения должностных обязанностей

Я,_____
(Ф.И.О. служащего администрации муниципального района)
исполняющий(ая) должностные обязанности по замещаемой должности
_____
_____
_____
(должность, наименование структурного подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностными инструкциями мне будет предоставлен допуск к информации, содержащей персональные данные сотрудников администрации и лиц обратившихся в администрацию:

- биографические сведения;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора и дополнений к нему;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии распоряжений содержащих персональные данные;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников, а также лиц обратившихся в администрацию;
- основания к распоряжениям по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;

– копии документов об образовании;
– результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
– фотографии и иные биометрические сведения;
– иные сведения относящиеся к персональным данным.

Настоящим добровольно принимаю на себя обязательства:

1. Соблюдать правительственные, и локальные нормативные акты работодателя, по работе с персональными данными, и регламентирующих вопросы защиты персональных данных;
2. В случае необходимости выполнять автоматизированную обработку и хранение персональных данных только после выполнения всех мероприятий по защите информации;
3. В случае возникновения ситуации нарушения безопасности персональных данных, или несанкционированного доступа к данной информации, попытке третьих лиц получить от меня информацию, содержащую персональные данные, немедленно сообщать о данном факте непосредственному начальнику;
4. Не осуществлять работу с персональными данными в присутствии лиц, не имеющих доступа к ним;
5. Передавать персональные данные третьим лицам (организациям) в порядке установленном регламентирующими документами;
6. Предупреждать лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они преданы, и требовать от этих лиц письменного подтверждения того, что данное правило будет соблюдено;
7. Не использовать информацию, содержащую персональные данные, с целью получения выгоды;
8. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам ставшую известной мне информацию, содержащую персональные данные.

В связи с этим за мной закрепляются права:

1. На знание требований нормативно-методических документов по защите информации и персональных данных;
2. На требование по обеспечению рабочего места средствами и материалами, необходимыми для осуществления работ с персональными данными и соблюдения режима конфиденциальности;
3. Участвовать при выработке мер защиты персональных данных, обрабатываемых в администрации муниципального района и её структурных подразделениях и вносить предложения по улучшению работы, связанной с обработкой персональных данных.

Работодатель обязан:

1. Обеспечить наличие необходимых условий в помещении и на рабочем месте сотрудника для обеспечения конфиденциальности, при которых бы исключалось бесконтрольное использование защищаемой информации;

Для проведения контрольных мероприятий Работодатель имеет право:

1. Требовать от сотрудника исполнения данного обязательства;
2. Привлекать, за нарушение норм регулирующих получение, обработку, хранение, уничтожение и защиту персональных данных, сотрудника к дисциплинарной ответственности;

Срок действия обязательства совпадает со сроком окончания трудового договора. Условия настоящего обязательства носят конфиденциальный характер и разглашению не подлежат. Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

Работодатель: глава администрации муниципального района	Сотрудник администрации:
_____ С.В. Лаврук (подпись)	_____ _____ (подпись) (фамилия, инициалы)
«___»_____ 20____г.	«___»_____ 20____г.

Приложение 3

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ОБРАЗЕЦ ОБЯЗАТЕЛЬСТВА О НЕРАЗГЛАШЕНИИ СВЕДЕНИЙ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, КОНТРАГЕНТОМ

ОБЯЗАТЕЛЬСТВО
о неразглашении сведений, содержащих персональные данные

Я, _____,
(фамилия, имя, отчество)
в период действия договора №____ от __.__.20__ г. между администрацией и _____, и в течение _____ после его окончания в соответствии с «Положением об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений» обязуюсь:

1) Не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны в результате выполнения работ по договору №____ от __.__.20__ г. между администрацией и _____, кроме случаев, предусмотренных законодательством Российской Федерации;

2) В случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, немедленно сообщить об этом лицу заключившему со мной договор и начальнику отдела по защите информации администрации.

До моего сведения доведены требования «Положения об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений», в части касающейся передачи персональных данных третьим лицам.

Мне известно, что нарушение этого обязательства может повлечь гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

_____ _____
(Ф.И.О.) *(подпись)*

«___» _____ 20____ г.

Приложение 4

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

РАЗДЕЛ ДОГОВОРА О СОХРАННОСТИ СВЕДЕНИЙ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

11. Сохранность персональных данных

11.1. Получатель обязуется:

обеспечить конфиденциальность получаемых персональных данных в соответствии с действующим законодательством Российской Федерации;

не предоставлять третьим лицам полученные персональные данные, кроме случаев, прямо предусмотренных действующим законодательством Российской Федерации.

11.2. Получатель обязуется использовать персональные данные только в целях _____

(указывается цель обработки персональных данных получателем)

Приложение 5

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ОБРАЗЕЦ АКТА УНИЧТОЖЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

_____
(степень конфиденциальности акта)
Экз. №___

РАЗРЕШАЮ УНИЧТОЖИТЬ
Глава администрации
Ленинского муниципального района
С.В.Лаврук
«___» _____2010 г.

А К Т № ___

Комиссия в составе: - _____
Члены комиссии: _____
_____
отобрала на уничтожение утратившие практическое значение и не имеющие научной и исторической ценности следующие материалы с персональными данными:

№	Рег №, дата документа	Наименование документа	Количество экземпляров	№ экз	Листов
1	2	3	4	5	6
1.					

Всего подлежит уничтожению ___ (_____) наименований документальных материалов в ___ (_____) экземплярах.

Члены комиссии:
_____
_____
_____
«___»_____20___ г.

Правильность произведенных записей в акте с данными учета сверил
_____
«___»_____20___ г.

Документальные материалы перед уничтожением с записями в акте сверили и уничтожили полностью путем _____ «___»_____20___ г.

Члены комиссии:

_____

_____

_____

Отметки об уничтожении документальных материалов произвел.

_____

«___»_____20___ г.

Приложение 6

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ОБРАЗЕЦ АКТА ПРИЕМА-ПЕРЕДАЧИ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Акт приема-передачи документов (иных материальных носителей), содержащих персональные данные

Во исполнение договора на оказание услуг №_____ от _____20___года, заключенного между администрации Ленинского муниципального района ЕАО, с. Ленинское Ленинского района ЕАО, ул. Ленина 16 и _____

_____

_____,

(наименование организации, принимающей документы (иные материальные носители), содержащие персональные данные)

администрация в лице _____

_____

(Ф.И.О., должность работника администрации, осуществляющего передачу персональных данных)

передает, а _____

_____

(наименование организации, принимающей документы (иные материальные носители), содержащие персональные данные)

в лице _____

_____

_____

(Ф.И.О., должность представителя организации, принимающей документы (иные материальные носители), содержащие персональные данные, данные документа удостоверяющего личность)

принимает документы (иные материальные носители), содержащие персональные данные на срок _____ и в целях:

_____

_____

_____

(указывается цель использования)

Перечень документов (иных материальных носителей), содержащих персональные данные

№ п/п	Документ (носитель)	Кол-во
Всего:		

Полученные персональные данные могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения и другими способами, установленными федеральными законами, может повлечь

соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.

Передал: _____

_____

(Ф.И.О., должность работника администрации, осуществляющего передачу персональных данных)

Принял: _____

_____

(Ф.И.О., должность представителя организации, принимающей документы (иные материальные носители), содержащие персональные данные)

Приложение 7

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ФОРМА ЖУРНАЛА УЧЕТА
ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

АДМИНИСТРАЦИЯ ЛЕНИНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

(наименование структурного подразделения)

ЖУРНАЛ
учета электронных носителей персональных данных

Начат «___» _____ ____ г.
Окончен «___» _____ ____ г.
На _____ листах

Учетный номер	Дата постановки на учет	Вид электронного носителя, место его хранения (размещения)	Ответственный за использование и хранение			Опись файлов, содержащихся на носителе, с указанием цели обработки и категории персональных данных.
			Ф.И.О.	подпись	дата	
1	2	3	4	5	6	7.

Приложение 8

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ФОРМА ЖУРНАЛА УЧЕТА ЗАПРОСОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБРАБОТКИ ИНФОРМАЦИИ

АДМИНИСТРАЦИЯ ЛЕНИНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

(наименование структурного подразделения)

ЖУРНАЛ
учета запросов персональных данных и обработки информации

Начат «___» _____ ____ г.
Окончен «___» _____ ____ г.
На _____ листах

№ п\п	Реквизиты запроса	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника	Место хранения запроса (дело, страница)

Приложение 9

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

ОТЗЫВ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

В администрацию
Ленинского муниципального района
Еврейской автономной области
с. Ленинское ЕАО ул. Ленина 16
от _____
_____
_____
(Ф.И.О. субъекта персональных данных)
_____
_____
_____
(Адрес, где зарегистрирован субъект персональных данных)
_____
_____
_____
_____
_____
(Номер документа, удостоверяющего личность, дата выдачи указанного документа, наименование органа, выдавшего документ)

ЗАЯВЛЕНИЕ

Прошу Вас прекратить обработку моих персональных данных в связи с
_____
_____
_____
_____
(указать причину)

_____ _____
(подпись) (расшифровка подписи)

"__" _____ 20__ г.

Приложение 10

к Положению об обработке и защите персональных данных в администрации Ленинского муниципального района и её структурных подразделений

Должностной регламент специалиста
по обеспечению безопасности персональных данных

I. Общие положения

1.1. Настоящий должностной регламент специалиста по обеспечению безопасности персональных данных (далее - Регламент) определяет основные цели, функции и права специалиста по обеспечению безопасности персональных данных (далее - Специалист) в администрации.

1.2. Специалист назначается распоряжением (локальным нормативным актом структурного подразделения) администрации, на основании Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51, во исполнение Федерального Закона «О персональных данных» №152-ФЗ от 27.07.2006г.

1.3. Специалист проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

1.4. Непосредственное руководство работой специалиста осуществляет начальник отдела по защите информации администрации.

Назначение и освобождение от должности специалиста производится Руководителем организации.

1.5. Специалист назначается из числа сотрудников соответствующей организации, имеющих опыт работы по основной деятельности соответствующей организации или в области защиты.

1.6. Специалист приравнивается по оплате труда, льготам и премированию к соответствующим категориям работников основных подразделений соответствующей организации.

1.7. Работа специалиста проводится в соответствии с планами работ, утверждаемыми непосредственным руководителем или руководителем организации.

1.8. В своей работе специалист руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами и указаниям Руководителя организации и другими руководящими документами по обеспечению безопасности персональных данных.

II. Основные функции специалиста

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в соответствующей организации.

2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию информационных систем персональных данных.

2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе

- мероприятия по размещению, охране, организации режима допуска в помещения, где ведется обработка персональных данных;
- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;
- мероприятия по защите от несанкционированного доступа к персональным данным
- мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Постоянный контроль обеспечения уровня защищенности персональных данных.

2.9. Участие в подготовке объектов соответствующей организации к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.10. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в соответствующей организации.

2.11. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля устранения этих нарушений.

2.12. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в соответствующей организации.

2.13. Проведение периодического контроля эффективности мер защиты персональных данных в соответствующей организации. Учет и анализ результатов контроля.

2.14. Организация повышения осведомленности руководства и сотрудников в соответствующей организации по вопросам обеспечения безопасности персональных данных, сотрудников подведомственных предприятий, учреждений и организаций.

2.15. Подготовка отчетов о состоянии работ по обеспечения безопасности персональных данных в соответствующей организации.

III. Права специалиста

Специалист имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность структурных подразделений соответствующей организации в части выполнения ими требований по обеспечению безопасности персональных данных.

3.5. Вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.6. Привлекать в установленном порядке необходимых специалистов из числа сотрудников соответствующей организации для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

IV. Ответственность специалиста

4.1. Специалист несет персональную ответственность за:

правильность и объективность принимаемых решений;

правильное и своевременное выполнение приказов, распоряжений, указаний руководства соответствующей организации по вопросам, входящим в возложенные на него функции;

выполнение возложенных на него обязанностей, предусмотренных настоящим Регламентом;

соблюдение трудовой дисциплины, охраны труда;

качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.

согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.