СОГЛАСОВАНО
на заседании педагогического совета
протокол № ____ от 03.09.2018 г.

УТВЕРЖДЕНО
Заведующий _____ Алефиренко Н.Н.
Приказ от 03.09.2018 г. № 51-ах

ПОЛОЖЕНИЕ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. Общие положения

1. Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных муниципальном бюджетном дошкольном образовательном учреждении «Центр развития ребенка – детский сад № 67» г. Уссурийска Уссурийского городского округа (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информатизации и защите информации", Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановлением Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами", Постановлением Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности", приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных" и в целях совершенствования работы по обеспечению защиты персональных данных в управлении образования и молодежной политики администрации Уссурийского городского округа

2. Настоящее Положение определяет:

а) правовое основание обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Центр развития ребенка – детский сад № 67» г. Уссурийска Уссурийского городского округа (далее - учреждение);

б) принципы обработки персональных данных в учреждении;

в) оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона:

г) основные условия проведения обработки персональных данных;

д) правила рассмотрения запросов субъектов персональных данных или их представителей;

е) правила обработки и защиты персональных данных;

ж) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом, принятыми в соответствии с федеральным законом нормативными правовыми актами учреждения;

з) соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона, и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом.

3. Настоящее Положение подлежит размещению на официальном сайте учреждения в целях исполнения требования части 2 статьи 18.1 Федерального закона.

4. В настоящем Положении используются термины и определения в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных".

5. Субъектами персональных данных в учреждении являются:

а) физические лица, состоящие с учреждением в отношениях, регулируемых трудовым законодательством;

б) физические лица, обратившиеся в учреждение в связи с предоставлением услуги «Постановка на очередь детей, в предоставлении места в ДОУ»

в) родители (законные представители) обучающихся и воспитанников образовательного учреждения) обучающиеся и воспитанники образовательных учреждений, находящихся в функциональном подчинении Управления;

6. Объектами системы безопасности персональных данных в учреждении являются:

а) информационные ресурсы с ограниченным доступом, содержащие персональные данные;

б) процессы обработки персональных данных в информационной системе персональных данных (далее - ИСПДн) учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, пользователи системы и ее обслуживающий персонал;

в) информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

7. Учреждение, в пределах своих полномочий, установленных в соответствии с нормативными правовыми актами, имеет право создавать информационные системы (в том числе ИСПДн) необходимые для обеспечения своей деятельности.

8. Для каждой создаваемой информационной системы определяется цели обработки персональных данных, перечень обрабатываемых персональных данных.

9. Перечни персональных данных обрабатываемых в учреждении в связи с реализацией трудовых отношений утверждаются приказом заведующего.

II. Определение законности целей обработки персональных данных

10. Определение законностей целей обработки персональных данных в учреждении является правовым основанием обработки персональных данных в учреждении.

11. Обработка персональных данных в учреждении осуществляется в целях реализации трудовых отношений, а также в связи с оказанием образовательных услуг, возложенных на учреждение.

12. Цели обработки персональных данных в учреждении соответствуют:

а) федеральным законам, а также иным подзаконным актам и документам органов государственной власти, которые требуют обработку персональных данных или иным документам, являющимся такими основаниями;

б) перечням задач или функций учреждения.

13. Цели обработки персональных данных определяют:

а) содержание и объем обрабатываемых персональных данных;

б) категории субъектов, персональные данные которых обрабатываются;

в) сроки их обработки и хранения;

г) порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

III. Принципы обработки персональных данных в учреждении

14. Обработка персональных данных в учреждении осуществляется на основе принципов:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

в) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

г) обработке подлежат только персональные данные, которые отвечают целям их обработки;

д) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;

е) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

ж) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

IV. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных

15. Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения правил обработки и защиты персональных данных.

16. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающие его права, свободы и законные интересы.

17. При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения правил обработки и защиты персональных данных при выполнении заявленных в рамках перечня задач или функций управления, с учетом особых правил и способов обработки персональных данных.

18. Определение юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и

обеспечению безопасности персональных данных и принимаемых мер.

V. Перечень действий (операций) совершаемых с персональными данными в учреждении

19. Сбор персональных данных.

В учреждении применяются следующие способы получения персональных данных субъектов персональных данных:

а) заполнение субъектом персональных данных соответствующих форм;

б) получение персональных данных от третьих лиц;

При сборе персональных данных учреждение обязано предоставить субъекту персональных данных по его просьбе информацию, предусмотренную настоящим Положением.

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, учреждение обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные по форме согласно Приложению 3 к настоящему Положению.

Если персональные данные получены не от субъекта персональных данных, учреждение до начала обработки таких персональных данных обязана предоставить субъекту персональных данных уведомлении об обработке персональных данных по форме согласно Приложению 9 к настоящему Положению.

При сборе персональных данных управление обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона.

20. Систематизация, накопление, уточнение и использование персональных данных.

Систематизация, накопление, уточнение, использование персональных данных могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

В учреждении могут быть установлены особенности учета персональных

данных в ИСПДн, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей ИСПДн, конкретному субъекту персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в ИСПДн, конкретному субъекту персональных данных.

Уточнение персональных данных должно производиться только на основании законно полученной в установленном порядке информации.

При необходимости, уведомить об уточнении персональных данных требуемых лиц в письменном виде по форме согласно Приложению 8 к настоящему Положению.

Использование персональных данных должно осуществляться исключительно в заявленных целях. Использование персональных данных в заранее не определенных и не оформленных установленным образом целях категорически не допускается.

21. Запись и извлечение персональных данных.

Запись персональных данных в ИСПДн управления может осуществляться с любых носителей информации или из других ИСПДн.

Извлечение персональных данных из ИСПДн может осуществляться с целью:

а) вывода персональных данных на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;

б) вывода персональных данных на носители информации, предназначенные для их обработки средствами вычислительной техники.

При извлечении персональных данных должен проводиться учет носителей информации.

При осуществлении записи и извлечения персональных данных должны

соблюдаться условия обработки персональных данных, конфиденциальность персональных данных и иные требования, указанные в настоящем Положении.

22. Передача персональных данных.

Передача персональных данных в учреждении должна осуществляться с соблюдением настоящего Положения и действующего законодательства Российской Федерации.

В управлении приняты следующие способы передачи персональных данных субъектов персональных данных:

а) передача персональных данных на электронных и бумажных носителях информации нарочным способом;

б) передача персональных данных на бумажных носителях посредством почтовой связи;

в) передача персональных данных по каналам связи.

Перед осуществлением передачи персональных данных проверяется основание на осуществление такой передачи и наличие согласия на передачу персональных данных в согласии субъекта персональных данных на обработку персональных данных или наличие иных законных оснований.

Передача персональных данных должна осуществляться на основании:

а) договора с третьей стороной, которой осуществляется передача персональных данных;

б) запроса, полученного от третьей стороны, которой осуществляется передача персональных данных;

в) исполнения возложенных законодательством Российской Федерации на управление функций, полномочий и обязанностей.

Передача персональных данных без согласия или иных законных оснований категорически запрещается.

23. Хранение персональных данных.

Хранение персональных данных в управлении допускается только в форме документов - зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

а) изобразительный документ - документ, содержащий информацию, выраженную посредством изображения какого-либо объекта;

б) фотодокумент - изобразительный документ, созданный фотографическим способом;

в) текстовой документ - документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;

г) письменный документ - текстовой документ, информация которого зафиксирована любым типом письма;

д) рукописный документ - письменный документ, при создании которого знаки письма наносят от руки;

е) машинописный документ - письменный документ, при создании которого знаки письма наносят техническими средствами;

ж) документ на машинном носителе - документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение персональных данных в ИСПДн и вне таких систем управлении осуществляется 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, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

Определение сроков хранения осуществляется в соответствии с требованиями архивного законодательства Российской Федерации, в том числе в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих персональные данные, в различных целях определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку.

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящего Положения не распространяется.

Сроки временного хранения документов, включенных в состав Архивного

фонда Российской Федерации, до их поступления в муниципальный архив, устанавливаются в соответствии с требованиями архивного законодательства Российской Федерации.

Документы Архивного фонда Российской Федерации, находящиеся в собственности управления, по истечении сроков их временного хранения передаются на постоянное хранение в муниципальный архив.

24. Блокирование персональных данных.

Блокированием персональных данных называется временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Блокирование персональных данных конкретного субъекта персональных данных должно осуществляться во всех ИСПДн управления, включая архивы баз данных, содержащих такие персональные данные.

Блокирование персональных данных в управлении осуществляется:

а) в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя по форме согласно Приложению 12 к настоящему Положению, либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;

б) в случае отсутствия возможности уничтожения персональных данных в установленные сроки до их уничтожения.

При необходимости управление направляет уведомление о блокировании персональных данных субъектам персональных данных в письменном виде по форме согласно Приложению 7 к настоящему Положению.

После устранения выявленной неправомерной обработки персональных данных управление осуществляет снятие блокирования персональных данных. При необходимости управление направляет уведомление об устранении допущенных нарушений в письменном виде по формам согласно Приложениям 5, 11 к настоящему Положению.

25. Обезличивание персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, установлены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 года N 996.

Под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки.

Решение о необходимости проведения обезличивания персональных данных принимается начальником управления.

Сотрудники управления, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, осуществляют обезличивание выбранным способом.

26. Уничтожение персональных данных.

Уничтожение персональных данных - это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Уничтожение персональных данных в управлении производится только в следующих случаях:

а) персональные данные являются незаконно полученными, или не являются необходимыми для заявленной цели обработки;

б) в случае выявления неправомерной обработки персональных данных, если обеспечить правомерность обработки персональных данных невозможно;

в) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных по форме согласно Приложению 15 к настоящему Положению.

При уничтожении персональных данных необходимо:

а) убедиться в необходимости уничтожения персональных данных;

б) убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;

в) уничтожить персональные данные подходящим способом, в соответствии с настоящим Положением или способом, указанным в соответствующем требовании или распорядительном документе;

г) проверить необходимость уведомления об уничтожении персональных данных;

д) при необходимости, уведомить об уничтожении персональных данных требуемых лиц в письменном виде по формам согласно Приложениям 4, 10 к настоящему Положению;

При уничтожении персональных данных применяются следующие способы:

а) измельчение в бумагорезательной (бумагоуничтожительной) машине - для документов, исполненных на бумаге;

б) стирание персональных данных - для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержавшем персональные данные;

в) физическое уничтожение (разрушение) носителей информации - для носителей информации на оптических дисках;

г) физическое уничтожение частей носителей информации - разрушение или сильная деформация - для носителей информации на жестком магнитном диске (уничтожению подлежат. внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

д) стирание с помощью сертифицированных средств уничтожения информации - для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении персональных данных необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части персональных данных допускается уничтожать материальный носитель одним из указанных в

настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение персональных данных производится только в присутствии лица, ответственного за организацию обработки персональных данных в управлении.

По факту уничтожения персональных данных составляется Акт уничтожения персональных данных, который подписывается лицами, производившими уничтожение.

Хранение актов уничтожения персональных данных осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

VI. Права субъектов персональных данных

27. Круг субъектов, персональные данные которых подлежат обработке в ИСПДн управления, определяется целью обработки персональных данных в каждой информационной системе персональных данных.

28. Субъект персональных данных имеет право на получение при обращении информации, касающейся обработки его персональных данных, по формам согласно Приложениям 13, 14, 16 к настоящему Положению, в том числе содержащей следующие сведения:

а) правовое основания и цель обработки персональных данных;

б) способы обработки персональных данных;

в) сведения о лицах (за исключением сотрудников управления), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с управлением или на основании федерального закона;

г) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

д) сроки обработки персональных данных, в том числе сроки их хранения;

е) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

ж) информацию об осуществленной или о предполагаемой трансграничной передаче данных.

29. Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено в соответствии с федеральным законом в случае, если:

а) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

в) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

30. Если субъект персональных данных считает, что учреждение осуществляет обработку его персональных данных с нарушением требований федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие управления в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

31. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

32. Учреждение освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 26, в случаях, если:

а) субъект персональных данных уведомлен об осуществлении обработки его персональных данных учреждением;

б) персональные данные получены учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

в) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

г) учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и

законные интересы субъекта персональных данных;

д) предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

VII. Правила рассмотрения запросов субъектов персональных данных или их представителей

33. При поступлении обращения субъекта, учреждение должно зарегистрировать его в Журнале регистрации входящих документов.

34. Учреждение обязано сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя, либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его законного представителя.

35. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных управление обязано дать в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его законного представителя, либо с даты получения запроса субъекта персональных данных или его законного представителя.

36. Учреждение обязано безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет управление, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах управление обязано уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

37. Учреждение обязано сообщить в уполномоченный орган по защите

прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

VIII. Основные условия проведения обработки персональных данных

38. Обработка персональных данных осуществляется после получения согласия субъекта персональных данных, составленного по форме согласно приложению N 1 к настоящему Положению, за исключением случаев, предусмотренных федеральным законом.

Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона.

39. Оператором ИСПДн управления, организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных является управление. Обязанности оператора возлагаются на работников управления, осуществляющих деятельность по эксплуатации ИСПДн.

40. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

41. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн оператором назначается должностное лицо, ответственное за организацию обработки персональных данных в управлении.

В учреждении назначается должностное лицо, ответственное за обеспечение безопасности персональных данных.

42. Заведующий приказом определяет должностных лиц, допущенных к обработке персональных данных.

43. Должностные лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и

подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно приложению 2 к Положению.

44. Оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Оператор или иное получившее доступ к персональным данным лицо обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

45. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

IX. Способы обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации

46. Способы обработки персональных данных в ИСПДн учреждения:

а) обработка персональных данных с использованием средств автоматизации;

б) обработка персональных данных без использования средств автоматизации;

в) исключительно автоматизированная обработка персональных данных;

г) смешанная обработка персональных данных.

X. Правила обработки и защиты персональных данных в информационных системах с использованием средств автоматизации

47. Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

48. Оператор ИСПДн определяет тип угроз безопасности персональных данных, актуальных для ИСПДн, с учетом оценки возможного вреда,

проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона, и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона.

49. Под актуальными угрозам безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

50. Угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

51. Угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

52. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

53. Оператор ИСПДн на основании типа угроз определяет уровень защищенности персональных данных в зависимости от категории обрабатываемых данных и их количества.

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

54. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся

сотрудниками оператора.

55. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более нем 100000 субъектов персональных данных, не являющихся сотрудниками оператора,

56. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и

информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

57. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

58. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение заведующим оператора документа, определяющего

перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

59. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

а) утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем, и других нормативных и методических документов;

б) настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

в) охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

XI. Правила обработки и защиты персональных данных в информационных системах без использования средств автоматизации

60. Обработка персональных данных без использования средств автоматизации (в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации) осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

61. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

а) определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

б) обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

в) соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

62. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

63. При использовании внешних электронных носителей информации с персональными данными данные электронные носители информации, учитываются в журнале учета, выдачи и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, персональных данных в управлении.

64. Все документы, содержащие персональные данные, должны храниться в служебных помещениях в недоступных для посторонних лиц местах

(запираемых шкафах, сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

XII. Правила исключительно автоматизированной обработки персональных данных

65. При исключительно автоматизированной обработке персональных данных должны выполняться правила обработки персональных данных средствами автоматизации, указанные в разделе 10 настоящего Положения.

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

67. В остальных случаях принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, запрещается.

68. При исключительно автоматизированной обработке персональных данных необходимо:

а) разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных;

б) разъяснить возможные юридические последствия такого решения;

в) предоставить возможность заявить возражение против такого решения;

г) рассмотреть возражение;

д) уведомить субъекта персональных данных о результатах рассмотрения такого возражения в течение тридцати дней со дня получения возражения.

XIII. Правила смешанной обработки персональных данных

69. При смешанной обработке персональных данных необходимо выполнять правила объединяющие правила обработки персональных данных

с использованием средств автоматизации, указанные в разделе 10 настоящего Положения, и правила обработки персональных данных без использования средств автоматизации, указанные в разделе 11 настоящего Положения.

XIV. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных третьему лицу

70. Учреждение вправе поручить обработку персональных данных третьему лицу (поручение оператора):

а) с согласия субъекта персональных данных и если иное не предусмотрено федеральным законом;

б) на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Положением.

71. В поручении оператора:

а) должен быть определен перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;

б) должны быть определены цели обработки персональных данных;

в) должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных;

г) должна быть установлена обязанность такого лица обеспечивать безопасность персональных данных при их обработке;

д) должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с настоящим Положением и техническим заданием на создание системы защиты персональных данных;

е) установлена ответственность такого лица перед управлением, в случаях нарушений установленных требований и законодательства Российской Федерации в области персональных данных;

ж) при необходимости получения согласий на обработку персональных данных от субъектов персональных данных предусмотрен порядок сбора и передачи в управление таких согласий субъектов персональных данных.

72. В случае если управление поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет управление.

73. В случае необходимости получения согласия на обработку персональных данных от субъекта персональных данных, обязанность получения таких согласий возлагается на управление.

XV. Правила обработки обезличенных персональных данных

74. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

75. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

76. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

а) парольной политики;

б) антивирусной политики;

в) правил работы со съемными носителями;

г) правил резервного копирования;

д) правил доступа в помещения, где расположены элементы информационных систем.

77. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

а) правил хранения бумажных носителей;

б) правил доступа к ним и в помещения, где они хранятся.

XVI. Правила обработки специальных категорий персональных данных

78. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, если:

а) субъект персональных данных дал согласие в письменной форме на

обработку своих персональных данных;

б) персональные данные сделаны общедоступными субъектом персональных данных;

в) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

г) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

79. Обработка персональных данных о судимости может осуществляться управлением в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации.

80. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных пунктами 76 и 77, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

XVII. Правила обработки биометрических категорий персональных данных

81. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных, могут обрабатываться в учреждении только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных пунктом 80.

82. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской

Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

XVIII. Правила обработки общедоступных персональных данных

83. Общедоступные персональные данные физических лиц, полученные из сторонних общедоступных источников персональных данных, в управлении обрабатываются в исключительных случаях в сроки, не превышающие необходимых для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта персональных данных на включение такой информации в общедоступные источники персональных данных, так как в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на управление. По достижении целей обработки общедоступных персональных данных они подлежат немедленному уничтожению.

84. В целях информационного обеспечения в управлении могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных, по форме согласно приложению 18 к Положению, могут включаться его фамилия, имя, отчество, дата рождения, служебный номер телефона, занимаемая должность, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

85. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

XIX. Обеспечение безопасности персональных данных в учреждении

86. С целью защиты субъектов персональных данных учреждения от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи в управлении создается система безопасности персональных данных, включающая в себя организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

87. Система безопасности персональных данных учреждения

обеспечивает решение следующих задач:

а) своевременное выявление, оценка и прогнозирование источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба заинтересованным субъектам персональных данных, нарушению нормального функционирования ИСПДн управления;

б) создание механизма оперативного реагирования на угрозы безопасности персональных данных;

в) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных;

г) защиту от вмешательства в процесс функционирования ИСПДн управления посторонних лиц;

д) разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам управления, то есть защиту от несанкционированного доступа;

е) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

ж) защиту от несанкционированной модификации используемых в ИСПДн управления программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

з) защиту персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

88. В рамках реализации системы безопасности персональных данных в учреждении проводятся следующие мероприятия:

а) строгий учет всех подлежащих защите ресурсов ИСПДн управления (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

б) регистрация действий персонала, осуществляющего обслуживание и модификацию программных и технических средств ИСПДн;

в) разработка организационно-распорядительных документов по вопросам обеспечения безопасности информации;

г) подготовка должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

д) наделение каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ИСПДн управления;

е) соблюдение всеми пользователями ИСПДн управления требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

ж) несение персональной ответственности за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к ИСПДн управления;

з) поддержание необходимого уровня защищенности элементов ИСПДн управления;

и) применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

к) контроль над соблюдением пользователями ИСПДн управления требований по обеспечению безопасности информации;

л) защита интересов управления при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

XX. Контроль и надзор за соблюдением правил по обработке и защите персональных данных

89. Контроль и надзор за соблюдением правил по обработке и защите персональных данных в управлении состоит из следующих направлений:

а) внешний контроль и надзор за соблюдением правил по обработке и защите персональных данных;

б) внутренний контроль и надзор за соблюдением правил по обработке и защите персональных данных.

90. Внутренний контроль и надзор за соблюдением правил по обработке и защите персональных данных в управлении состоит из:

а) контроля и надзора за исполнением правил по обработке и защите персональных данных;

б) оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

91. Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи, федеральным органом исполнительной власти; уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

92. Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации в области защиты прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, подзаконных нормативных актов Правительства Российской Федерации, ведомственных нормативных актов и административных регламентов.

93. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

94. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

а) запрашивать у управления информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

б) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных управления, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

в) требовать от управления уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

г) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства в области персональных данных;

д) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

е) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, необходимые сведения;

ж) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

з) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

95. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

96. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

97. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

XXI. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в учреждении

98. В целях осуществления внутреннего контроля соответствия обработки

персональных данных установленным требованиям в учреждении организуется проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в управлении, на основании утвержденного Плана внутренних проверок условий обработки персональных данных в управлении.

99. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в учреждении производится проверка:

а) соблюдения принципов обработки персональных данных;

б) соответствия нормативных правовых актов управления в области персональных данных действующему законодательству Российской Федерации;

в) выполнения сотрудниками управления требований и правил обработки персональных данных в ИСПДн управлении;

г) перечней персональных данных, используемых для решения задач и функций управлением, и необходимости обработки персональных данных в ИСПДн управлении;

д) актуальности информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;

е) правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой ИСПДн управления;

ж) актуальности перечня должностей сотрудников управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

з) соблюдения прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных управления;

и) соблюдения обязанностей управления, предусмотренных

действующим законодательством в области персональных данных;

к) порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных управления, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

л) наличия необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных управления;

м) актуальности сведений, содержащихся в уведомлении управления об обработке персональных данных;

н) актуальности перечня информационных систем персональных данных в управлении;

о) знаний и соблюдения сотрудниками управления положений действующего законодательства Российской Федерации, нормативных правовых актов администрации Уссурийского городского округа и управления в области обработки и обеспечения безопасности персональных данных;

п) знаний и соблюдения сотрудниками управления инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

р) соблюдения сотрудниками управления конфиденциальности персональных данных;

с) актуальности нормативных правовых актов управления в области обеспечения безопасности персональных данных;

т) соблюдения сотрудниками управления требований по обеспечению безопасности персональных данных;

у) наличия нормативных правовых актов управления, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных управления;

ф) иных вопросов.

100. По результатам проведенной проверки оформляется Акт внутренней проверки состояния защиты персональных данных в управлении.

XXII. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных

101. Во время осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в управлении производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в управлении.

102. При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, для каждой ИСПДн управления производится экспертное сравнение заявленной управлением оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения правил обработки и защиты персональных данных и применяемых управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и изложенных в настоящем Положении.

103. По итогам сравнений принимается решение о достаточности применяемых управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных, и возможности или необходимости принятия дополнительных мер или изменения установленного в управлении порядка обработки и обеспечения безопасности персональных данных.

104. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в управлении оформляется в виде отдельного документа.

105. По результатам принятых решений лицом, ответственным за организацию обработки персональных данных в управлении организуется

работа по их реализации.

XXIII. Ответственность должностных лиц

106. Сотрудники учреждения, допущенные к персональным. данным, 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.

107. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.