АДМИНИСТРАЦИЯ ДАЛЬНЕГОРСКОГО ГОРОДСКОГО ОКРУГА ПРИМОРСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

29 декабря 2022г. г. Дальнегорск № 379-ра

Об утверждении документов по обработке персональных данных в администрации Дальнегорского городского округа

В целях осуществления мероприятий по защите и обеспечению безопасности персональных данных при их обработке в информационных системах администрации Дальнегорского городского округа, в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21.03.2012 № 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», от 01.12.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», руководствуясь Уставом Дальнегорского городского округа:

1. Утвердить следующие документы по обработке персональных данных:

1) Политика в отношении обработки персональных данных в администрации Дальнегорского городского округа в порядке, установленном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (Приложение 1);

2) Положение об обеспечении безопасности персональных данных в администрации Дальнегорского городского округа (Приложение 2);

3) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа (Приложение 3);

4) Правила работы с обезличенными данными в случае обезличивания персональных данных в администрации Дальнегорского городского округа

(Приложение 4);

5) Перечень должностей служащих администрации Дальнегорского городского округа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных (Приложение 5);

6) Порядок доступа сотрудников администрации Дальнегорского городского округа в помещения, в которых осуществляется обработка персональных данных, и размещены информационные системы (Приложение 6);

7) Перечень помещений, в которых размещены информационные системы администрации Дальнегорского городского округа (Приложение 7);

8) Порядок учета, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа (Приложение 8);

9) Порядок реагирования на инциденты информационной безопасности в администрации Дальнегорского городского округа (Приложение 9);

10) Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации Дальнегорского городского округа (Приложение 10);

11) Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Дальнегорского городского округа (Приложение 11);

12) Порядок по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации Дальнегорского городского округа (Приложение 12);

13) Инструкция по организации антивирусной защиты в информационных системах персональных данных администрации Дальнегорского городского округа (Приложение 13);

14) Инструкция по организации парольной защиты в информационных системах персональных данных администрации Дальнегорского городского округа (Приложение 14).

2. Разместить настоящее распоряжение разместить на официальном сайте Дальнегорского городского округа.

3. Контроль за исполнением настоящего распоряжения возложить на первого заместителя главы администрации Дальнегорского городского округа.

Глава Дальнегорского
городского округа А.М. Теребилов

Приложение 1

УТВЕРЖДЕНА
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ПОЛИТИКА
в отношении обработки персональных данных в администрации Дальнегорского городского округа

1. Общие положения

1.1. Термины и определения

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

Информация – сведения (сообщения, данные) независимо от формы их представления.

Оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых оператором с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники оператора.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Уничтожение персональных данных - 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.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Трансграничная передача персональных данных – передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2. Назначение и правовая основа документа

1.2.1. Политика в отношении обработки персональных данных (далее – Политика) в администрации Дальнегорского городского округа (далее – Администрация) определяется в соответствии со следующими нормативными правовыми актами:

- Конституцией Российской Федерации;
- Трудовым, Гражданским и Уголовным кодексами Российской Федерации;
- 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»;
- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- постановлением Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных системах персональных данных»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»;

- приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- иными нормативными правовыми актами Российской Федерации и нормативными документами уполномоченных органов государственной власти.

Настоящая Политика определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и персональных данных, обрабатываемых в Администрации, функции Администрации при обработке персональных данных, права субъектов персональных данных, а также требования к защите персональных данных, реализуемые в Администрации.

Положения Политики служат основой для разработки локальных актов, регламентирующих в Администрации вопросы обработки персональных данных и других субъектов персональных данных.

2. Принципы и цели обработки персональных данных в Администрации

2.1. Администрация Дальнегорского городского округа, являясь оператором персональных данных, осуществляет обработку персональных данных Администрации и других субъектов персональных данных, не состоящих с Администрацией в трудовых отношениях.

2.2. Обработка персональных данных в Администрации осуществляется с учетом необходимости обеспечения защиты прав и свобод Администрации и других субъектов персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

- обработка персональных данных в Администрации осуществляется на законной и правовой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

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

- обработке подлежат только персональные данные, которые отвечают целям обработки;

- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям из обработки;

- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Администрацией

принимаются необходимые меры, либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того 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 уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.3. Персональные данные обрабатываются в Администрации в целях:

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Администрации;

- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Администрацию, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

- регулирования трудовых отношений с сотрудниками Администрации (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);

- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

- подготовки, заключения, исполнения и прекращения договоров с контрагентами;

- обеспечения пропускного режима в Администрации;

- осуществления прав и законных интересов Администрации в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Администрации, или третьих лиц либо достижения общественно значимых целей;

- в иных законных целях.

3. Перечень субъектов, персональные данные которых обрабатываются в Администрации

3.1. В Администрации обрабатываются персональные данные следующих категорий:

- сотрудников, бывших сотрудников, кандидатов на замещение вакантных должностей, а также родственников сотрудников;

- жителей муниципального образования (физических лиц);

- другие субъекты персональных данных (для обеспечения реализации целей обработки персональных данных в администрации Дальнегорского городского округа).

4. Перечень персональных данных, обрабатываемых в Администрации

4.1. Перечень персональных данных, обрабатываемых в Администрации, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Администрации с учетом целей обработки персональных данных, указанных в разделе 2 Политики.

4.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в администрации Дальнегорского городского округа не осуществляется.

5. Функции Администрации при осуществлении обработки персональных данных

5.1. Администрация при осуществлении обработки персональных данных:

- принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных;

- принимает правовые, организационные и технические меры 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;

- назначает лицо, ответственное за организацию обработки персональных данных в Администрации;

- издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Администрации;

- осуществляет ознакомление Администрации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных сотрудников;

- публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

- сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных

субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

- прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

- совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

6. Условия обработки персональных данных в Администрации

6.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

6.2. Обработка персональных данных в Администрации осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации.

6.3. Администрация без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено законодательством.

6.4. Администрация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

6.5. В целях внутреннего информационного обеспечения Администрация может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

6.6. Доступ к обрабатываемым в Администрации персональным данным разрешается только сотрудникам Администрации, согласно перечню должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным в Администрации.

7. Процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере персональных данных

7.1. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации

7.1.1. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, относятся:

- назначение ответственного за организацию обработки персональных данных;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиями к обеспечению безопасности персональных данных, политике и локальным актам Администрации в отношении обработки персональных данных;
- оценка вреда, который может быть причинен субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящего Положения;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных с положениями законодательства Российской Федерации о персональных данных и настоящим Положением;
- запрет на обработку персональных данных лицами, не допущенными к их обработке.

7.2. Документы, определяющие Политику Администрации в отношении обработки персональных данных, подлежат обязательному опубликованию.

8. Перечень действий с персональными данными и способы их обработки

8.1. Администрация осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

8.2. Обработка персональных данных в Администрации осуществляется следующими способами:

- неавтоматизированная обработка персональных данных – подразумевает обработку персональных данных без использования средств автоматизации, может осуществляться в виде документов на бумажных носителях. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных

данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.10.2012 № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

- смешанная обработка персональных данных.

9. Правила работы с обезличенными данными

9.1. Правила работы с обезличенными персональными данными оформляются отдельным документом и утверждаются распоряжением Администрации

9.2. Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных оформляется отдельным документом и утверждается распоряжением Администрации.

10. Правила рассмотрения запросов субъектов персональных данных

10.1. Правила рассмотрения запросов субъектов персональных данных оформляются отдельным документом и утверждаются главой Дальнегорского городского округа.

11. Сроки обработки и хранения обрабатываемых персональных данных

11.1. Сроки обработки и хранения обрабатываемых персональных данных

11.1.1. Сроки обработки и хранения персональных данных определяются:

- приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;

- сроком исковой давности;

- иными требованиями законодательства Российской Федерации и муниципальными нормативно-правовыми актами Администрации.

11.2. Особенности хранения персональных данных

11.2.1. 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.

12. Порядок уничтожения обработанных персональных данных

12.1. Уничтожение обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований

12.1.1. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

12.1.2. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

12.2. Порядок уничтожения обработанных персональных данных

12.2.1. Уничтожение обработанных персональных данных производится комиссией с составлением соответствующего акта.

13. Права субъектов персональных данных

13.1. Субъекты персональных данных имеют право на:

- полную информацию об их персональных данных, обрабатываемых в Администрации;
- доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку персональных данных;
- принятие предусмотренных законом мер по защите своих прав;
- обжалование действия или бездействия Администрации, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;
- осуществление иных прав, предусмотренных законодательством Российской Федерации.

14. Меры, принимаемые Администрацией для обеспечения выполнения обязанностей оператора при обработке персональных данных

14.1. Меры, необходимые и достаточные для обеспечения выполнения Администрацией обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

- наличие ответственного за обработку персональных данных - ответственный за организацию обработки персональных данных в Администрации назначается распоряжением Администрации из числа сотрудников Администрации. В Администрации должна быть разработана Инструкция ответственного за обработку персональных данных, которая утверждается распоряжением Администрации. Ответственный за организацию обработки персональных под роспись знакомиться с Инструкцией ответственного за организацию обработки персональных данных;

- наличие администратора информационных систем персональных данных;

- наличие утвержденных инструкций, регламентирующих работу с персональными данными и информационными системами персональных данных;

- осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

- ознакомление всех сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных под роспись;

- учет машинных носителей персональных данных;

- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- наличие правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;

- определение перечня должностей, осуществляющих обработку персональных данных - перечень должностей муниципальной службы, при замещении которых служащие допускаются к обработке персональных данных и имеют доступ к персональным данным, утверждается распоряжением Администрации. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящей Политикой и подписывают обязательство о неразглашении информации, содержащей персональные данные;

- сведения на бумажных носителях хранятся в сейфах или выделенных помещениях;

- определение места хранения персональных данных;

- определение порядка доступа в помещения, в которых ведётся обработка персональных данных - порядок оформляется в виде отдельного документа и утверждается распоряжением Администрации;

- ведение учёта всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);

- обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

14.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами Администрации, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Администрации.

15. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных

15.1. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в Администрации и локальным нормативным актам Администрации в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

15.2. Внутренний контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в Администрации.

15.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Администрации осуществляет Ответственный за организацию обработки персональных данных.

15.4. Работники Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение 2

УТВЕРЖДЕНА
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных в администрации Дальнегорского городского округа

1. Термины и определения

1.1. В настоящем Положении использованы следующие термины и определения:

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.

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.

Вредоносное программное обеспечение - программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации - возможность получения информации и ее использования.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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.

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 таковых средств.

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

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

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.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

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

Криптографическая защита - защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

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.

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.

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

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

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.

Оператор персональных данных (оператор) - муниципальный орган, организующий и (или) осуществляющий обработку ПДн, а также определяющие цели и содержание обработки ПДн.

Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Разграничение доступа (правила разграничения доступа) - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение персональных данных - действия, направленные на передачу ПДн 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.

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

Средство защиты информации - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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).

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 ИСПДн или в результате которых уничтожаются материальные носители персональных данных.

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

Шифрование - процесс преобразования открытой информации с целью сохранения ее в тайне от посторонних лиц при помощи некоторого алгоритма, называемого шифром.

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию.

2. Используемые сокращения

2.1. В настоящем Положении использованы следующие сокращения:

ИСПДн - информационная система персональных данных;

НСД - несанкционированный доступ;

ПДн - персональные данные;

СКЗИ - средство криптографической защиты информации;

СЗПДн - система защиты персональных данных.

3. Область применения

3.1. Настоящее Положение об обеспечении безопасности персональных данных в администрации Дальнегорского городского округа (далее - Положение) предназначено для применения при организации и проведении работ по обеспечению безопасности персональных данных в администрации Дальнегорского городского округа (далее по тексту - Администрация).

3.2. Требования настоящего Положения распространяются на сотрудников Администрации, принимающих участие в обеспечении безопасности персональных данных.

4. Общие положения

4.1. Настоящее Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн) Администрации, представляющей собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и

технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

4.2. Безопасность персональных данных при их обработке в ИСПДн достигается путем снижения вероятности осуществления НСД к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

4.3. При обработке персональных данных в ИСПДн Администрации должно быть обеспечено:

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

- своевременное обнаружение фактов НСД к персональным данным;

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

- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;

- непрерывный контроль и анализ уровня защищенности персональных данных.

4.4. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПДн информационные технологии.

4.5. Обеспечение безопасности персональных данных в Администрации осуществляется на основе следующих принципов:

- соответствие мер и средств защиты актуальным угрозам безопасности - построение и модернизация СЗПДн в Администрации производится на основе анализа угроз безопасности персональных данных с учетом специфических особенностей ИСПДн;

- соответствие мер и средств защиты требованиям нормативных документов РФ - в Администрации используются меры и средства обеспечения безопасности персональных данных в строгом соответствии с действующими нормативными правовыми актами РФ в области обработки и защиты персональных данных;

- комплексность - с целью обеспечения безопасности персональных данных в Администрации используется совокупность организационных мер и технических средств защиты;

- патентная чистота - средства защиты информации, входящие в состав СЗПДн, отвечают требованиям по обеспечению патентной чистоты согласно

действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей.

- удобство пользователей - при построении и модернизации СЗПДн учитываются и по возможности сводятся к минимуму возможные трудности пользователей в работе со средствами защиты и с основными процедурами обеспечения безопасности персональных данных;

- постоянное совершенствование - осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности персональных данных, эффективности применяемых организационных мер и технических средств защиты и уровня защищенности персональных данных, а также регулярно пересматриваются состав угроз и уровень защищенности ПДн, на основании чего принимаются меры по устранению выявленных недостатков и модернизации/совершенствованию СЗПДн.

4.6. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

4.7. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн Администрации включают в себя:

- определение уровня защищенности обрабатываемых ПДн, в том числе отслеживание изменений состояния ИСПДн, которые могут повлиять на классификационные признаки ИСПДн (уровень защищенности ПДн);

- определение угроз безопасности персональных данных при их обработке в ИСПДн;

- разработка на основании определенных угроз и поддержание в актуальном состоянии частной модели безопасности угроз безопасности персональных данных при обработке их в ИСПДн;

- разработку на основе частной модели угроз системы защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для установленного уровня защищенности ПДн;

- установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с проектными решениями по созданию СЗПДн, эксплуатационной и технической документацией к данным СЗИ;

- обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам работы с ними;

- учет применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации к ним;

- учет носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в ИСПДн;

- контроль соблюдения условий использования СЗИ, входящих в состав СЗПДн, предусмотренных эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание состава и режима функционирования компонентов СЗПДн (описание СЗПДн).

4.8. Размещение компонентов ИСПДн, охрана помещений, в которых ведется работа с персональных данных, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СЗИ, входящих в состав СЗПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.9. Настоящее Положение должно быть доведено до всех работников Администрации, участвующих в обеспечении безопасности персональных данных, под роспись.

5. Стадии создания СЗПДн

5.1. В Администрации обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках следующих стадий создания и совершенствования СЗПДн: предпроектная стадия, стадия проектирования, стадия приемки и ввода в действие, модернизация СЗПДн.

5.1.1. Проектная стадия создания СЗПДн

5.1.1.1. Целью предпроектной стадии создания СЗПДн является:

- определение категории субъектов персональных данных, чьи данные обрабатываются в Администрации, состава и объема обрабатываемых персональных данных, а также цели и правовое основание обработки этих данных;

- определение должностных лиц, участвующих в обработке персональных данных;

- определение угроз безопасности персональных данных применительно к конкретным условиям функционирования ИСПДн;

- определение уровня защищенности ПДн.

5.1.1.2. Для достижения указанных целей проводится анализ информационных систем Администрации, содержащих персональные данные, и определяются все внутренние и внешние процессы обработки персональных данных, осуществляемые как с использованием средств автоматизации, так и без использования таковых.

5.1.1.3. По результатам предпроектной стадии определяется степень выполнения требований нормативно-правовых документов в области защиты

персональных данных, а также разрабатывается план необходимых дальнейших организационных и технических мероприятий по реализации данных требований.

5.1.1.4. Должностное лицо, ответственное за проведение работ по защите персональных данных, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели предпроектной стадии.

5.1.1.5. В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в Администрации определяются состав, цели, правовое основание обработки персональных данных и сроки хранения обрабатываемых персональных данных. На основании полученных данных формируется документ *«Перечень персональных данных, обрабатываемых в администрации Дальнегорского городского округа».*

5.1.1.6. В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в Администрации определяется перечень лиц, которым необходим доступ к персональных данных для выполнения трудовых обязанностей, а также перечень лиц, которые в рамках выполнения своих трудовых обязанностей имеют право доступа к ресурсам, содержащим персональные данные, без права ознакомления с персональными данными. На основании полученных данных формируется *перечень должностных лиц, допущенных в помещения и к работе со средствами вычислительной техники из состава ИСПДн Администрации, который утверждается соответствующим распоряжением администрации.*

5.1.1.7. В ходе обследования информационных систем Администрации определяются все базы данных (хранилища) и отчуждаемые носители информации и содержащиеся в них персональных данных. Кроме того, определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, а именно *перечень серверного оборудования, автоматизированных рабочих мест, общесистемных и прикладных программных средств, задействованных при обработке персональных данных, перечень применяемых средств защиты информации, а также сетевая инфраструктура и перечень сетевого оборудования.*

5.1.1.8. С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в ИСПДн Администрации, проводится анализ и оценка вероятности реализации и величины негативных последствий вследствие реализации угроз безопасности персональных данных при их обработке в ИСПДн. В Администрации составляется частная модель угроз безопасности персональных данных, которая разрабатывается на основании:

- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения»;

- Базовой модели угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;

- Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России;

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144.

5.1.1.9. Определение уровня защищенности ПДн осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». При определении уровня защищенности ПДн используется модель угроз безопасности ПДн, в которой проведен анализ актуальных угроз безопасности ПДн.

5.1.2. Стадия проектирования СЗПДн

5.1.2.1. Цели проектирования СЗПДн:

- определить требования по обеспечению безопасности персональных данных;

- определить структуру и характеристики создаваемой СЗПДн, состав технических средств защиты информации, предполагаемых к использованию в СЗПДн, требования к настройке и эксплуатации этих средств, параметры их взаимодействия, а также план мероприятий по подготовке СЗПДн к вводу в действие;

- определить требования и регламентировать деятельность работников Администрации по организации легитимной обработки персональных данных и обеспечению безопасности персональных данных, обрабатываемых как с использованием средств автоматизации, так и без использования таковых.

5.1.2.2. Для достижения указанных целей в Администрации разрабатывается *комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.*

5.1.2.3. Должностное лицо, ответственное за проведение работ по защите персональных данных в Администрации, определяет необходимость проведения мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии проектирования СЗПДн.

5.1.2.4. По результатам предпроектной стадии, в зависимости от определенного уровня защищенности ПДн и определенного перечня актуальных угроз безопасности персональных данных, задаются конкретные требования по

обеспечению безопасности ПДн при их обработке в ИСПДн Администрации, выполнение которых обеспечивает минимизацию вероятности реализации предполагаемых угроз безопасности персональных данных.

5.1.2.5. На основании требований, указанных выше, осуществляется проектирование СЗПДн, определяется состав и характеристики средств защиты информации, которые будут входить в состав создаваемой СЗПДн. В Администрации разрабатывается *комплект организационно-распорядительной документации на СЗПДн, описывающей требования и процедуры по управлению и обеспечению безопасности персональных данных*. За разработку и, при необходимости, пересмотр организационно-распорядительной документации на СЗПДн в Администрации отвечает должностное лицо, ответственное за проведение работ по обеспечению безопасности персональных данных в Администрации.

5.1.3. Стадия ввода в действие СЗПДн

5.1.3.1. Цели стадии ввода в действие СЗПДн:

- внедрить технические средства защиты информации;
- проверить работоспособность средств защиты информации в составе ИСПДн;
- принять организационные меры по обеспечению безопасности персональных данных;
- ознакомить работников Администрации с требованиями и обучить порядку обработки и обеспечения безопасности персональных данных.

5.1.3.2. Для достижения перечисленных целей выполняются следующие мероприятия:

- осуществляется закупка, установка и настройка средств защиты информации;
- проводятся опытная эксплуатация и приемо-сдаточные испытания средств защиты информации;
- утверждается и вводится в действие комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.
- проводится обучение работников по направлению обеспечения безопасности персональных данных.

5.1.3.3. Должностное лицо, ответственное за проведение работ по защите персональных данных в Администрации, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии ввода в действие СЗПДн.

5.1.3.4. Согласно требованиям, определенным в документации, осуществляется закупка, установка и настройка программных и технических средств защиты информации с составлением соответствующих актов установки. Установка и ввод в эксплуатацию средств защиты информации осуществляется строго в соответствии с эксплуатационной и технической документацией к ним.

Перед установкой средств защиты информации проверяется их готовность к использованию, и составляются заключения о возможности их эксплуатации. В Администрации необходимо применять средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и имеющие соответствующие сертификаты ФСТЭК и ФСБ России.

5.1.3.5. В Администрации утверждается и вводится в действие *комплект организационно-распорядительной документации на СЗПДн.* Все должностные лица, допущенные к обработке персональных данных, и лица, ответственные за обеспечение безопасности персональных данных, в обязательном порядке изучают организационно-распорядительные документы на СЗПДн в части их касающейся и руководствуются ими в своей работе. Общий контроль над исполнением требований организационно-распорядительной документации на СЗПДн в Администрации возлагается на должностное лицо, ответственное за обеспечение безопасности ПДн.

5.1.3.6. В Администрации все работники, участвующие в обработке персональных данных, в обязательном порядке проходят обучение по следующим направлениям:

- общие вопросы обеспечения информационной безопасности;
- правила автоматизированной и неавтоматизированной обработки персональных данных и обеспечения безопасности персональных данных;
- правила использования прикладных систем и технических средств обработки персональных данных;
- правила использования средств защиты информации, входящих в состав СЗПДн;
- ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

5.1.3.7. Ответственным за организацию и контроль проведения обучения работников Администрации, участвующих в обработке и обеспечении безопасности персональных данных, является должностное лицо, ответственное за обеспечение безопасности персональных данных в Администрации. Обучение может проводиться как самим должностным лицом, ответственным за обеспечение безопасности персональных данных в Администрации, так и с привлечением сторонних организаций. Новые работники Администрации, принимаемые на работу, в обязательном порядке проходят *первичный инструктаж*. Ответственным за направление работника на первичный инструктаж является должностное лицо, ответственное за организацию работ по обработке персональных данных в Администрации.

5.1.3.8. Перед допуском работников Администрации к работе с ПДн должностное лицо ответственное за обеспечение безопасности ПДн проводит ознакомление с нормативной документацией, утвержденной в Администрации, в области безопасности ПДн.

5.1.4. Модернизация СЗПДн

5.1.4.1. Для определения необходимости модернизации СЗПДн не реже одного раза в год должностным лицом ответственным за обеспечение безопасности ПДн проводится проверка состава и структуры СЗПДн, состава угроз и уровня защищенности ПДн, обработка которых осуществляется в ИСПДн Администрации.

5.1.4.2. Модернизация СЗПДн в обязательном порядке проводится в случаях, если:

- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав обрабатываемых ПДн, состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и пр.);
- изменился состав угроз безопасности ПДн в ИСПДн;
- изменился уровень защищенности ПДн.

5.1.4.3. Выбор мер и СЗИ, входящих в состав СЗПДн, проводится на основании проведенного анализа угроз и проведенной классификации ИСПДн (определения уровня защищенности ПДн). Порядок проведения данных мероприятий определен в настоящем Положении.

5.1.4.4. Должностное лицо ответственное за обеспечение безопасности ПДн ежегодно разрабатывает план работ по обеспечению безопасности ПДн в Администрации, в котором определяется перечень необходимых мероприятий по обеспечению безопасности ПДн с учетом уже выполненных мероприятий. В план работ по обеспечению безопасности ПДн включаются организационные и технические мероприятия, направленные на выполнение требований нормативно-правовых документов в области безопасности ПДн и на совершенствование СЗПДн, а также контрольные мероприятия и мероприятия по проведению обучения работников Администрации. В плане указываются дата, сроки проведения мероприятий, их периодичность (разовые или регулярные) и назначаются ответственные за их организацию и выполнение лица.

5.1.4.5. Работники, участвующие в обеспечении безопасности ПДн в Администрации вправе формировать предложения по совершенствованию СЗПДн и направлять их на рассмотрение должностному лицу ответственному за защиту ПДн, которое в свою очередь формирует сводный перечень предложений по совершенствованию СЗПДн.

5.1.4.6. Ежегодно должностное лицо ответственное за защиту ПДн формирует отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности ПДн, обрабатываемых в Администрации, и предоставляет его главе администрации совместно со сводным перечнем предложений по совершенствованию СЗПДн. Ежегодный отчет по выполнению плана работ включает в себя:

- результаты проведенной проверки состава и структуры, состава угроз и уровня защищенности ПДн;
- результаты проведенных контрольных мероприятий по защите ПДн;
- результаты проверок регулирующими органами;

- результаты анализа инцидентов информационной безопасности;

- результаты плановых мероприятий по обеспечению безопасности ПДн;

- предложения по совершенствованию СЗПДн на основе полученных результатов.

5.1.4.7. На основании решения, принятого главой администрации, по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн должностное лицо ответственное за защиту ПДн составляет план работ по обеспечению безопасности ПДн, обрабатываемых в администрации, на следующий год.

5.2. СЗПДн включает организационные меры, технические средства защиты информации, а также используемые в ИСПДн информационные технологии, реализующие функции защиты информации.

5.3. Выполнение всех вышеуказанных стадий должно проходить по согласованию с должностным лицом, ответственным за организацию работ по обработке персональных данных.

5.4. Выполнение всех вышеуказанных стадий должно проходить под контролем должностного лица, ответственным за проведение работ по защите персональных данных.

6. Мероприятия по организации и обеспечению безопасности персональных данных

6.1. Под организацией обеспечения безопасности персональных данных при их обработке в ИСПДн Администрации понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

6.2. Организационные мероприятия по обеспечению безопасности персональных данных в Администрации включает в себя:

- мероприятия по обеспечению охраны и физической защиты помещений, в которых расположены технические средства ИСПДн, исключающие несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности;

- обучение работников Администрации правилам обработки и защиты персональных данных.

6.3. В целях осуществления технического обеспечения безопасности персональных данных при их обработке в ИСПДн Администрации реализовываются мероприятия по защите от НСД к ПДн.

Планирование мероприятий по обеспечению безопасности персональных данных осуществляется в соответствии с Разделом 8 настоящего Положения.

6.4. Мероприятия по обеспечению управления доступом

6.4.1. Для организации *системы допуска и учета должностных лиц, допущенных к работе с персональными данными в Администрации, должен быть*

определен перечень должностных лиц и утвержден соответствующим распоряжением главы администрации.

6.4.2. В Администрации должна быть реализована разрешительная система допуска пользователей и разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью функциональных возможностей операционной системы, прикладных систем обработки персональных данных либо специализированных средств защиты информации.

6.4.3. Работникам Администрации предоставляется доступ к ПДн и средствам их обработки в объеме, минимально необходимом для выполнения их трудовых обязанностей.

6.4.4. Для идентификации и аутентификации пользователей ИСПДн Администрации должны применяться пароли условно-постоянного действия. Требования к формированию пароли и периодичности их смены определены в *эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности, и Инструкция работника по правилам обработки ПДн*).

6.4.5. Своевременное предоставление работникам Администрации прав доступа к персональным данным и средствам их обработки, а также изменение их полномочий обеспечивает должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации.

6.4.6. Порядок генерации, смены и прекращения действия паролей в ИСПДн Администрации определен в эксплуатационной документации на СЗПДн).

6.5. Мероприятия по обеспечению регистрации и учета

6.5.1. В Администрации должен вестись учет как машинных, так и бумажных носителей ПДн. Также должно быть организовано хранение и использование этих носителей, исключающее их хищение, подмену и уничтожение.

6.5.2. В Администрации учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, BD и прочее);

- неотчуждаемые носители информации (жесткие магнитные диски).

6.5.3. Порядок учета, хранения, использования носителей персональных данных (машинных и бумажных), а также порядок их уничтожения определены в документе *«Порядок учета, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа».*

6.5.4. Ответственность за ведение учета машинных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо, ответственное за защиту ПДн.

6.5.5. Контроль и ответственность за ведение учета бумажных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

6.6. Мероприятия по обеспечению целостности

6.6.1. Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

6.6.2. В Администрации должен быть *определен и документально зафиксирован состав и назначение ПО*, используемого в ИСПДн. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован.

6.6.3. Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован.

6.6.4. С целью недопущения изменения состава ПО ИСПДн, из него должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения).

6.6.5. Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

6.6.6. В Администрации должны быть реализованы механизмы восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним и/или возникновения форс-мажорных ситуаций или воздействия опасных факторов окружающей среды.

6.6.7. Требования к периодичности осуществления резервного копирования и требования к носителям, предназначенным для записи на них резервных копий, определены в документе *«Порядок проведения резервного копирования персональных данных в администрации Дальнегорского городского округа»*.

6.6.8. Порядок организации резервного копирования и восстановления массивов информации в Администрации определен в документе *«Порядок проведения резервного копирования ПДн в администрации Дальнегорского городского округа»*. Ответственность за организацию своевременного резервного копирования и восстановления информации, а также за надлежащее хранение резервных носителей, содержащих резервные копии данных, возлагается на должностное лицо ответственное за защиту ПДн.

6.7. Мероприятия по обеспечению антивирусной защиты

6.7.1. Для предотвращения возможности внедрения в ИСПДн вредоносного программного обеспечения в Администрации должны применяться антивирусные средства:

6.7.2. Требования к настройке антивирусных средств защиты определены в проектной документации на СЗПДн, процедуры по управлению антивирусными средствами определены в эксплуатационной документации на СЗПДн (*Инструкция администратора информационной безопасности*).

6.7.3. Порядок использования антивирусных средств защиты определен в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности).

6.7.4. Системный администратор Администрации, осуществляет:

- установку антивирусных средств защиты в соответствии с эксплуатационной и технической документацией к ним;

- настройку параметров антивирусных средств защиты согласно требованиям по обеспечению безопасности, определенным в проектной документации на СЗПДн;

- контроль эффективности работы антивирусных средств защиты;

6.7.5. Контроль соблюдения условий использования антивирусных средств защиты, предусмотренных эксплуатационной и технической документацией, возлагается на должностное лицо ответственное за защиту ПДн.

6.8. Мероприятия по обеспечению криптографической защиты

6.8.1. В Администрации должны применяться следующие типы средств криптографической защиты информации, сертифицированные ФСБ России:

- СКЗИ для обеспечения безопасности ПДн, передаваемых по каналам связи между Администрацией и ИС сторонних организаций;

- средства электронной подписи, т.е. шифровальные (криптографические) средства, используемые для подписания передаваемых документов и проверки электронной подписи получаемых документов.

6.8.2. СКЗИ, применяемые в Администрации для защиты ПДн, должны иметь класс, определенный в Частной модели угроз безопасности ПДн при их обработке в ИСПДн Администрации. Частная модель угроз безопасности ПДн составляется на каждую ИСПДн.

6.8.3. Правила использования СКЗИ при обмене информацией со структурными подразделениями Правительства Приморского края должны быть определены в соответствующих регламентах, утвержденных уполномоченными должностными лицами Правительства Приморского края.

6.8.4. Правила использования СКЗИ при обмене информацией со сторонними организациями СКЗИ должны быть определены условиями заключаемых договоров между Администрации и данными организациями.

6.8.5. В Администрации *ведется учет всех применяемых СКЗИ*, эксплуатационной и технической документации к ним, а также учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности ПДн. Требования к эксплуатации и учету применяемых в Администрации СКЗИ определены в документе *«Порядок эксплуатации СКЗИ в администрации Дальнегорского городского округа»*.

6.8.6. Порядок организации криптографической защиты в Администрации, определен в документе *«Порядок эксплуатации СКЗИ в администрации Дальнегорского городского округа»*. На должностное лицо, ответственное за выполнение работ по защите ПДн в Администрации, возлагается ответственность за обеспечение функционирования и безопасности СКЗИ согласно требованиям руководящих документов ФСБ России.

6.9. Мероприятия по обеспечению физической защиты

6.9.1. В целях предотвращения несанкционированного входа (вскрытия) в помещения, а также исключения возможности неконтролируемого проникновения в эти помещения посторонних лиц, в Администрации организуется и обеспечивается физическая охрана и техническая защита помещений Администрации, с использованием охранной сигнализации, обеспечивающие сохранность технических средств обработки персональных данных, носителей персональных данных и средств защиты информации.

6.9.2. Защите подлежат следующие типы помещений:

- помещения, в которых осуществляется непосредственно обработка ПДн пользователями ИСПДн Администрации;
- серверные помещения, в которых установлено серверное, сетевое оборудование и технические средства защиты информации;
- архивные помещения, в которых организовано хранение бумажных документов, содержащих ПДн.

6.9.3. *Перечень лиц, которые допускаются в указанные помещения, определяется распоряжением администрации.*

6.9.4. В целях обеспечения физической защиты помещений применяться следующие средства защиты и контроля за несанкционированным вскрытием:

- система охранной сигнализации;
- двери помещений оборудуются замками для защиты от несанкционированного проникновения и местами для их опечатывания и сдачи под охрану.
- устанавливаются металлические двери для защиты от несанкционированного проникновения в серверные и архивные помещения.

6.9.5. В целях организации противопожарной безопасности в Администрации устанавливается система пожарной сигнализации

6.9.6. Контроль обеспечения безопасности помещений, в которых расположены компоненты ИСПДн, возлагается на должностное лицо ответственное за защиту ПДн.

6.9.7. Доступ в защищаемые помещения осуществляется согласно перечню утвержденного распоряжением администрации. Лица, не указанные в Перечне допущенных в защищаемые помещения, при наличии необходимости могут посещать помещения Администрации только в сопровождении допущенных лиц. Одиночное, бесконтрольное пребывание лиц, не допущенных к работе по обработке ПДн, в производственных помещениях - **СТРОГО ЗАПРЕЩЕНО**.

Пребывание посторонних лиц в серверных помещениях допускается в целях производственной необходимости, только в присутствии должностного лица, ответственного за защиту ПДн.

6.9.8. В случае утраты ключей (либо подозрении на утрату) к замкам в защищаемые помещения предпринимаются следующие меры:

- оповещаются должностные лица, ответственные за организацию работ по обработке ПДн за защиту ПДн служебной запиской;

- производится немедленная замена запираемых замков.

- назначается административная проверка всех режимных помещений с составлением акта и принятым мерам, виновные лица привлекаются к административной ответственности.

6.9.9. При возникновении форс-мажорных обстоятельств в защищаемых помещениях (возникновение пожара, затопление помещения, возгорание электропроводки и прочее) в отсутствии лиц, имеющих доступ в эти помещения, осуществляется вскрытие помещений с соблюдением следующих условий:

- оповещаются должностные лица ответственные за организацию работ по обработке и защите ПДн;

- помещения вскрываются группой в составе не менее двух человек;

- при вскрытии помещения составляется акт о вскрытии, в котором указываются должности и фамилии лиц, вскрывших помещение, дата, время и причины вскрытия.

7. Обязанности, права и ответственность должностных лиц при обеспечении безопасности ПДн

7.1. Обязанности, права и ответственность должностных лиц, участвующих в обеспечении безопасности ПДн в Администрации определены в соответствующих *инструкциях*.

8. Планирование работ по защите ПДн

8.1. Планирование работ по защите информации, требования к содержанию плана, порядок разработки, согласования, утверждения и оформления плана, порядок отчетности и контроля над его выполнением определяются действующими нормативными документами РФ.

8.2. *План определяет перечень основных проводимых организационно-технических мероприятий по защите информации* (в том числе ПДн) в Администрации с указанием:

- сроков выполнения мероприятий;

- ответственных за выполнение соответствующих пунктов Плана работников.

8.3. В План включаются:

- мероприятия по контролю состояния защищенности ПДн;

- мероприятия по своевременному устранения выявленных нарушений безопасности.

8.4. План на очередной календарный год разрабатывается должностным лицом, ответственным за защиту информации в ИС ПДн, который осуществляет общий контроль над выполнением работ по защите информации.

8.5. Утвержденный план хранится у должностного лица ответственного за организацию работ по обработке ПДн.

8.6. Отчет о результатах выполнения запланированных мероприятий по обеспечению безопасности ПДниза текущий год формируется должностным лицом, ответственным за защиту ПДн, в рамках общего отчета работы за текущей год.

9. Контроль состояния защищенности ПДн

9.1. Контроль состояния защищенности ПДн в Администрации осуществляется с целью своевременного выявления и предотвращения утечки конфиденциальной информации, отнесенной к категории ПДн, вследствие НСД к ней, преднамеренных программно-технических воздействий на персональные данные и оценки защищенности ПДн (далее по тексту - Контроль).

9.2. Контроль заключается в проверке выполнения требований действующих нормативных документов в области обработки и обеспечения безопасности ПДн, в оценке обоснованности и эффективности принятых мер по защите ПДн.

9.3. Контроль эффективности внедренных мер и СЗИ, входящих в состав СЗПДн, должеи проводиться в соответствии с требованиями эксплуатационной документации на СЗПДн в целом на конкретные СЗИ, а также требованиями других нормативных документов не реже одного раза в год.

9.4. Обязательным является контроль СЗИ, входящих в состав СЗПДн, при вводе их в эксплуатацию после проведения ремонта таких средств, а также при изменении условий и расположения их эксплуатации.

9.5. Контроль обеспечения безопасности ПДн в Администрации организовывается должностным лицом, ответственным за проведение работ по защите ПДн в Администрации.

9.6. Контроль состояния и эффективности СЗПДн может осуществляться в соответствии с планом основных мероприятий по защите информации на текущий год или носить внеплановый характер.

9.7. Результаты периодического контроля оформляются отдельными протоколами или актами.

9.8. По всем выявленным нарушениям требований по защите ПДн должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации, в пределах предоставленных ему прав и своих функциональных обязанностей обязано добиваться их немедленного устранения. Должностное лицо, ответственное за организацию работ по обработке ПДн в Администрации, обязано принять все необходимые меры по немедленному устранению выявленных нарушений. При невозможности их немедленного устранения должна быть

прекращена обработка ПДн и организованы работы по устранению выявленных нарушений.

9.9. Работники Администрации, осуществляющие обработку ПДн в ИСПДн, обязаны выполнять требования должностного лица ответственного за обеспечение безопасности ПДн, по устранению допущенных ими нарушений норм и требований по обработке и/или обеспечении безопасности ПДн. Также работники несут персональную ответственность за соблюдение требований по обеспечению безопасности ПДн в ходе проведения работ.

9.10. Учет, хранение и выдача работникам паролей и ключей для системы защиты ПДн от НСД, оперативный контроль действий работников, осуществляющих обработку ПДн, осуществляет должностное лицо ответственное за обеспечение безопасности ПДн.

10. Управление инцидентами информационной безопасности

10.1. В Администрации в целях своевременного устранения выявленных нарушений безопасности определен и задокументирован порядок действий при возникновении инцидентов информационной безопасности, связанных с нарушением требований по обработке и обеспечению безопасности ПДн.

10.2. К инцидентам информационной безопасности, связанным с нарушением требований по обработке и обеспечению безопасности ПДн, относятся любые нарушения, приводящие к снижению уровня защищенности ИСПДн, в том числе несоблюдение условий хранения носителей ПДн и использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности или доступности ПДн.

10.3. В Администрации в случаях возникновения подобных инцидентов информационной безопасности проводятся разбирательства, составляются заключения по фактам возникновения инцидентов, разрабатываются и принимаются меры по предотвращению возможных последствий инцидентов.

10.4. Организация и контроль процесса реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн, в Администрации возлагается на должностное лицо ответственное за обеспечение безопасности ПДн.

10.5. Процедура управления инцидентами информационной безопасности, связанными с нарушением требований по обработке и обеспечению безопасности ПДн, регламентирована в документе «*Порядок реагирования на инциденты информационной безопасности в администрации Дальнегорского городского округа*». Данный документ определяет порядок проведения следующих мероприятий:

- определение инцидента информационной безопасности;
- оповещение ответственного лица о возникновении инцидента;
- устранение последствий и причин инцидента;
- расследование инцидента;

- реализация необходимых корректирующих и превентивных мер.

10.6. Дополнительно порядок действий работников Администрации в случаях возникновения инцидентов информационной безопасности определен в документе *«Инструкция пользователю информационной системы ПДн в администрации Дальнегорского городского округа».*

11. Привлечение сторонних организаций для проведения мероприятий по обеспечению безопасности ПДн

11.1. В Администрации могут привлекаться сторонние организации для проведения следующих мероприятий по обеспечению безопасности ПДн:

- разработка нормативно-методических материалов по вопросам обеспечения безопасности ПДн;

- поставка СЗИ и СКЗИ;

- выполнение организационных и технических мероприятий в области защиты ПДн, на проведение которых у Администрации отсутствует соответствующее разрешение либо отсутствуют технические средства и подготовленные работники (специалисты);

- выполнение организационных и технических мероприятий в области защиты ПДн, выполнение которых силами Администрации экономически нецелесообразно;

- подтверждение соответствия мер по защите ИСПДн требованиям нормативно-правовой базы РФ в области безопасности ПДн, путем проведения аттестационных испытаний ИСПДн Администрации по требованиям безопасности информации;

- контроль и аудит эффективности проводимых мероприятий по защите ПДн.

11.2. Привлекаемые для оказания услуг в области защиты ПДн сторонние организации должны иметь лицензии на соответствующие виды деятельности.

11.3. Перечень совместно выполняемых организационных и технических мероприятий в области защиты ПДн определяется с учетом планируемых работ по созданию (реконструкции) ИСПДн и включается в План основных мероприятий по защите ПДн.

11.4. Привлечение сторонних организаций для проведения мероприятий по созданию и модернизации СЗПДн и/или проведению контрольных мероприятий

11.4.1. Привлекаемая сторонняя организация должна обладать соответствующими, проводимым работам, лицензиями и сертификатами.

11.4.2. Должностное лицо, ответственное за обеспечение безопасности ПДн, является ответственным за выбор организации, привлекаемой для проведения мероприятий по созданию или модернизации СЗПДн и проведению контрольных мероприятий. Должностное лицо, ответственное за защиту ПДн, осуществляет подбор подходящих организаций и формирует предложения для согласования с главой администрации.

11.4.3. Существенным условием договора является обязательство привлекаемой организации обеспечить конфиденциальность получаемой

информации, ставшей известной в ходе выполнения работ по обеспечению безопасности ПДн в администрации.

11.4.4. В случае привлечения сторонней организации для проведения мероприятий по созданию или модернизации СЗПДн в договоре прописываются обязательства привлекаемой организации по проведению необходимых организационно-технических мероприятий, включающих в себя:

- организацию и проведение работ по созданию СЗПДн;
- реализацию требований нормативно-правовых документов РФ в области обработки и защиты ПДн;
- своевременное совершенствование СЗПДн;
- поддержание работоспособности и сопровождение СЗПДн.

11.4.5. В случае привлечения сторонней организации для проведения контрольных мероприятий (аудит обеспечения безопасности ПДн) в договоре прописываются обязанности привлекаемой организации по выполнению необходимых работ, включающих в себя:

- проверку выполнения требований нормативно-правовых документов РФ в области обработки и защиты ПДн;
- оценку обоснованности и эффективности принятых в Администрации мер по обеспечению безопасности ПДн.

11.4.6. Должностное лицо, ответственное за обеспечение безопасности ПДн, осуществляет контроль над выполнением привлекаемой организацией взятых на себя обязательств.

11.5. Привлечение сторонних организаций для проведения обучения работников

11.5.1. К организациям, привлекаемым для проведения обучения работников Администрации по направлению обеспечения безопасности ПДн, предъявляются следующие требования:

- организация должна иметь лицензию на осуществление образовательной деятельности, выданную Министерством образования РФ, государственными органами управления образованием субъектов РФ или органами местного самоуправления, наделенными соответствующими полномочиями;
- предлагаемые организацией программы и курсы обучения должны быть согласованы с регулирующими и надзорными органами;
- по результатам проведенного обучения организация должна проводить итоговую аттестацию работников.

11.6. Привлечение сторонних организаций (подрядчиков) для ремонтно-восстановительных работ

11.6.1. Организацией обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн, в Администрации занимается системный администратор Администрации. В случае необходимости, ремонт технических средств может быть произведен с привлечением специалистов сторонних организаций на договорной основе с составлением актов выполненных работ.

11.6.2. Должностным лицом, ответственным за обеспечение безопасности ПДн, определяется порядок привлечения сторонних организаций (подрядчиков) для обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн.

11.6.3. Сопровождение и контроль сторонних организаций (подрядчиков) обеспечивается должностным лицом, ответственным за обеспечение безопасности ПДн.

11.6.4. Обязательным условием при передаче технических средств обработки ПДн и машинных носителей ПДн для осуществления ремонтных работ сторонней организацией является удаление ПДн с носителей, установленных на передаваемых устройствах, либо извлечение носителей ПДн. Контроль исполнения данного требования возлагается на должностное лицо ответственное за защиту ПДн. В случае, когда выполнить данное требование не представляется возможным, должностным лицом, ответственным за защиту ПДн, составляется двусторонний протокол, в котором указано, что сторонняя организация осведомлена о том, какие именно персональные данные содержатся на носителе и обязана принять все необходимые меры по обеспечению их безопасности.

11.6.5. После проведения ремонта средств защиты или средств обработки ПДн, при изменении условий их расположения или эксплуатации обязательно осуществляется проверка готовности этих средств к использованию с составлением заключений о возможности их эксплуатации.

12. Пересмотр и внесение изменений

Настоящее Положение должно пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;
- изменением организационной и технологической инфраструктуры, в рамках которой обрабатываются ПДн;
- выявления снижения общего уровня информационной безопасности (по результатам регулярного мониторинга или аудита);

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за обеспечение безопасности ПДн в Администрации.

Внесение изменений производится на основании соответствующего распоряжения Администрации.

Приложение 3

УТВЕРЖДЕНЫ
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 349-ра

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в администрации Дальнегорского городского округа требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила) разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Виды и периодичность внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа Приморского края (далее – Администрация) проводятся текущие и периодические проверки условий обработки персональных данных.

2.2. Текущий внутренний контроль осуществляется на постоянной основе Ответственным за обеспечение безопасности персональных данных в администрации Дальнегорского городского округа.

2.3. Периодический внутренний контроль осуществляется комиссией в соответствии с поручением главы Дальнегорского городского округа.

3. Порядок осуществления внутреннего контроля

3.1. Осуществление текущего внутреннего контроля

3.1.1. Текущий внутренний контроль заключается в проведении плановой проверки соответствия обработки персональных данных требованиям к защите персональных данных проводится ответственным за организацию обработки

защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Администрации.

3.1.2. Плановые проверки условий обработки персональных данных проводятся на основании Перечня мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных администрации Дальнегорского городского округа (Приложение № 1).

3.2. Осуществление периодического внутреннего контроля

3.2.1. Периодический внутренний контроль заключается в проведении внеплановых проверок на основании поступившей информации о нарушениях правил обработки персональных данных. Проверки осуществляются комиссией, созданной распоряжением главы администрации Дальнегорского городского округа, из числа сотрудников администрации Дальнегорского городского округа, допущенных к обработке персональных данных, так же возможно привлечение в качестве членов комиссий экспертов. **В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах**.

3.2.2. Проведение внеплановой проверки организуется в течение **трех рабочих дней** со дня поступления информации о нарушениях правил обработки персональных данных.

3.2.3. При проведении внеплановой проверки условий обработки персональных данных Комиссией должны быть полностью, объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите персональных данных;

– порядок и условия соблюдения парольной защиты;

– порядок и условия соблюдения антивирусной защиты;

– порядок и условия обеспечения резервного копирования;

– эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в информационные системы персональных данных;

– условия соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена;

– порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационной системы персональных данных;

– порядок и условия применения средств защиты информации;

– состояние учета носителей персональных данных;

– соблюдение правил доступа к персональным данным;

– соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

– мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

3.2.4. В проведении внеплановой проверки условий обработки персональных данных не могут участвовать сотрудники Администрации, прямо или косвенно заинтересованные в ее результатах.

3.3. Плановые и внеплановые проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников Администрации, участвующих в процессе обработки персональных данных.

3.4. Для каждой проверки составляется Протокол проведения внутренней проверки (далее – Протокол) (Приложении № 2 к настоящим Правилам).

3.5. При выявлении в ходе проверки нарушений в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.6. Протоколы внеплановых проверок хранятся у председателя комиссии, в протоколы плановых проверок хранятся у Ответственного за организацию обработки персональных данных в течение текущего года. Уничтожение Протоколов проводится комиссией и Ответственным самостоятельно по истечении срока хранения.

3.7. О результатах проверки и мерах, необходимых для устранения нарушений председатель комиссии и Ответственный докладывает главе Дальнегорского городского округа.

3.8. Проверка условий обработки персональных данных должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

3.9. Плановые и внеплановые проверки Ответственный за организацию обработки персональных данных фиксирует в Журнале учёта внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа (Приложение № 3)

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа

Перечень
мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных

№ п/п	Краткое описание мероприятий
1	Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны
2	Проверка выполнения требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в помещениях, в которых размещены средства информационных систем персональных данных (далее - ИСПДн)
3	Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки персональных данных
4	Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных данных
5	Проверка соответствия реального уровня полномочий по доступу к персональным данным различных пользователей, установленному в списке лиц, допущенных к обработке персональных данных, уровню полномочий
6	Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн
7	Проверка правильности применения средств защиты информации
8	Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей
9	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн
10	Проверка соблюдения правил парольной защиты
11	Проверка работоспособности системы резервного копирования
12	Проведение мероприятий по проверке организации учета и условий хранения

	съемных носителей персональных данных
13	Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети "Интернет"
14	Проверка знаний работниками руководящих документов, технологических инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях
15	Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн
16	Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов)

Приложение 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа

Протокол
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен в том, что «___»._____.20__ комиссией по внутреннему контролю проведена проверка:_____

(место проведения проверки)

Проверка осуществлялась в соответствии с требованиями _____

_____

(название документа)

В ходе проверки проверено: _____

_____

_____

Выявленные нарушения: _____

_____

_____

_____

Меры по устранению нарушений: _____

_____

_____

Срок устранения нарушений: _____.

Должность Ответственного _____ И.О. Фамилия

либо

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность
Фамилия

_____ И.О.

Приложение 3
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа

Журнал учёта внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Дальнегорского городского округа

№ п/п	Дата проведения проверки, вид внутренней проверки (плановая/внеплановая)	Место проведения проверки	Выявленные нарушения	Срок устранения	Номер и дата Протокола	Примечание

Приложение 4

УТВЕРЖДЕНА
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

Правила работы с обезличенными данными в случае обезличивания персональных данных в администрации Дальнегорского городского округа

1. Общие положения

1.1. Правила работы с обезличенными данными в случае обезличивания персональных данных в администрации Дальнегорского городского округа Приморского края (далее – Правила) разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 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», приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и определяют условия обезличивания персональных данных, методы обезличивания персональных данных и порядок работы с обезличенными данными.

2. Условия обезличивания персональных данных

2.1. В соответствии с Федеральным законом «О персональных данных» обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.2. Обезличивание персональных данных может быть проведено в статистических целях, в целях предупреждения ущерба от разглашения персональных данных, по достижении целей или в случае утраты необходимости в достижении этих целей, а также в иных целях, предусмотренных законодательством Российской Федерации.

2.3. Обезличивание персональных данных должно обеспечивать следующие свойства информации:

- полноту (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);
- структурированность (сохранение структурных связей между обезличенными персональными данными конкретного субъекта или группы

субъектов, соответствующих связям, имеющимся до обезличивания);

- релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме);

- семантическую целостность (сохранение семантики (сути и смысла) персональных данных при их обезличивании);

- применимость (возможность решения задач обработки персональных данных, стоящих перед администрацией Дальнегорского городского округа (далее – Администрация) осуществляет обезличивание персональных данных, обрабатываемых в информационных системах персональных данных без предварительного деобезличивания всего объема записей о субъектах);

- анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

2.4. Методы обезличивания персональных данных должны обладать следующими характеристиками:

- обратимостью (возможностью преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность);

- вариативностью (возможностью внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

- изменяемостью (возможностью внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

- стойкостью (стойкостью метода к атакам на идентификацию субъекта персональных данных);

- возможностью косвенного деобезличивания (возможностью проведения деобезличивания с использованием информации других операторов);

- совместимостью (возможностью интеграции персональных данных, обезличенных различными методами);

- параметрическим объемом (возможностью определения объема дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);

- возможностью оценки качества данных (возможностью проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

2.5. Методы обезличивания персональных данных должны обладать следующими свойствами:

- обратимостью (возможность проведения деобезличивания);

- возможностью обеспечения заданного уровня анонимности;

- увеличением стойкости при увеличении объема обезличиваемых персональных данных.

2.6. Получаемые обезличенные данные должны обладать следующими свойствами:

- сохранением полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);

- сохранением структурированности обезличиваемых персональных данных;

- сохранением семантической целостности обезличиваемых персональных данных;

- анонимностью отдельных данных не ниже заданного уровня.

2.7. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.

2.8. В Администрации могут быть использованы следующие методы обезличивания:

- метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

- метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

2.9. Описание методов обезличивания, обеспечиваемых ими свойств обезличенных данных, оценка свойств методов, требования к реализации методов приведены в приложении к настоящим Правилам.

2.10. Предложения о методах обезличивания вносит ответственный за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Администрации. Решение о методах обезличивания персональных данных принимает глава Дальнегорского городского округа.

2.11. Ответственность за обезличивание персональных данных несут лица, замещающие должности, вошедшие в Перечень должностей служащих Администрации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных.

3. Порядок работы с обезличенными данными

3.1. Обезличенные персональные данные конфиденциальны и не подлежат

разглашению.

3.2. Обезличенные персональные данные могут обрабатываться как с использованием, так и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение парольной политики, антивирусной политики, правил работы со съемными носителями (если они применяются в Администрации), правил резервного копирования, правил доступа в помещения, где расположены элементы информационных систем.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение: правил хранения бумажных носителей, правил доступа к бумажным носителям и в помещения, где они хранятся.

3.5. При обработке обезличенных персональных данных сотрудники Администрации руководствуются настоящими Правилами.

Приложение
к Правилам работы с обезличенными данными в случае обезличивания персональных данных в администрации Дальнегорского городского округа

ОПИСАНИЕ МЕТОДОВ ОБЕЗЛИЧИВАНИЯ

1. Метод введения идентификаторов

1.1. Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

1.2. Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- семантическая целостность;
- применимость.

1.3. Оценка свойств метода:

- обратимость (метод позволяет провести процедуру деобезличивания);
- вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);
- изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);
- стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
- возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
- совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);
- параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах персональных данных, подлежащих обезличиванию);
- возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

1.4. Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.

2. Метод изменения состава или семантики

2.1. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.

2.2. Метод обеспечивает следующие свойства обезличенных данных:

- структурированность;
- релевантность;
- применимость;
- анонимность.

2.3. Оценка свойств метода:

- обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);
- вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);
- изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
- стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
- возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
- совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);
- параметрический объем (параметры метода определяются набором правил изменения состава или семантики персональных данных);
- возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения персональных данных).

2.4. Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта. При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

3. Метод декомпозиции

3.1. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

3.2. Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- релевантность;
- семантическая целостность;
- применимость.

3.3. Оценка свойств метода:

- обратимость (метод позволяет провести процедуру деобезличивания);
- вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);
- изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
- стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);
- возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
- совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);
- параметрический объем (определяется числом подмножеств и числом субъектов персональных данных, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц связывания записей, находящихся в различных хранилищах);
- возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

3.4. Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

4. Метод перемешивания

4.1. Метод перемешивания реализуется путем перемешивания отдельных записей, а также групп записей между собой.

4.2. Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- релевантность;
- семантическая целостность;
- применимость;
- анонимность.

4.3. Оценка свойств метода:

- обратимость (метод позволяет провести процедуру деобезличивания);

- вариативность (метод позволяет изменять параметры перемешивания без проведения процедуры деобезличивания);

- изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

- стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);

- возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием персональных данных, имеющихся у других операторов);

- совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами);

- параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);

- возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

4.4. Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.

4.5. Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

Приложение 5

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

Перечень должностей служащих администрации Дальнегорского городского округа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных

№ п/п	Структурное подразделение	Должность
1	**Управление делами**	Начальник управления
2		Главный специалист 1 разряда
3		Ведущий специалист 1 разряда
4		Старший специалист 1 разряда
5	Отдел кадров и муниципальной службы управления делами	Начальник отдела в управлении
6		Ведущий специалист 1 разряда
7	**Управление экономики**	Начальник управления
8		Заместитель начальника управления
9	Отдел экономики и проектной деятельности управления экономики	Главный специалист 1 разряда
10		Главный специалист 2 разряда
11	Отдел предпринимательства и потребительского рынка управления экономики	Начальник отдела в управлении
12		Главный специалист 1 разряда
13		Ведущий специалист 1 разряда
14	**Юридический отдел**	Начальник отдела
15		Главный специалист 1 разряда
16	**Отдел бухгалтерского учета и отчетности**	Начальник отдела
17		Заместитель начальника отдела
18		Главный специалист 1 разряда
19		Главный специалист 2 разряда
20		Ведущий специалист 3 разряда
21	**Отдел по делам ГО и ЧС и мобилизационной работе**	Начальник отдела
22		Главный специалист 2 разряда
23	**Отдел жизнеобеспечения**	Начальник отдела
24		Главный специалист 1 разряда
25		Главный специалист 2 разряда
26		Ведущий специалист 1 разряда
27		Ведущий специалист 3 разряда
28		Старший специалист 1 разряда
29		Старший специалист 2 разряда

30	**Отдел архитектуры и строительства**	Начальник отдела
31		Главный специалист 1 разряда
32		Ведущий специалист 2 разряда
33		Ведущий специалист 3 разряда
34		Старший специалист 1 разряда
35	**Архивный отдел**	Начальник отдела
36		Главный специалист 2 разряда
37		Ведущий специалист 1 разряда
38	**Отдел ЗАГС**	Начальник отдела
39		Главный специалист 1 разряда
40		Ведущий специалист 1 разряда
41	**Отдел по исполнению административного законодательства**	Начальник отдела
42	**Комиссия по делам несовершеннолетних и защите их прав**	Главный специалист 1 разряда
43		Ведущий специалист 1 разряда
44	**Отдел опеки и попечительства**	Начальник отдела
45		Главный специалист 1 разряда
46		Ведущий специалист 3 разряда

Приложение 6

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

Порядок доступа сотрудников администрации Дальнегорского городского округа в помещения, в которых осуществляется обработка персональных данных, и размещены информационные системы

1. Настоящий Порядок разработан в соответствии с требованиями:

- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановления Правительства Российской Федерации от 21 марта 2012 г. № 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»;

- приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Настоящий Порядок регламентирует условия и порядок осуществления доступа сотрудников администрации Дальнегорского городского округа (далее – Администрация) в помещения, в которых осуществляется обработка персональных данных, и размещены информационные системы (далее – Помещения), в целях организации контролируемой зоны и режима обеспечения безопасности персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа с целью уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных.

3. Персональные данные относятся к конфиденциальной информации. Должностные лица администрации Дальнегорского городского округа (далее – Администрация), получившие доступ к персональным данным, обязаны не

раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством.

4. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в отдельных кабинетах Администрации.

5. В помещения, где размещены информационные системы, позволяющие осуществлять обработку персональных данных, также хранятся носители персональных данных и средств защиты информации, допускаются только сотрудники Администрации, уполномоченные на обработку персональных данных и имеющие доступ к персональным данным. Перечень сотрудников, уполномоченных на обработку персональных данных и имеющих доступ к персональным данным (далее – Сотрудники), утверждается нормативным актом Администрации. При обработке персональных данных, защищаемой информации в информационных системах должна обеспечиваться сохранность носителей персональных данных.

6. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств, позволяющих осуществлять обработку персональных данных, средств защиты информации и носителей защищаемой информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц.

7. Нахождение в Помещениях посторонних лиц допускается только в сопровождении Сотрудников Администрации.

8. Уборка и техническое обслуживание Помещений допускаются только в присутствии Сотрудников Администрации.

9. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать первому заместителю главы Дальнегорского городского округа.

10. Двери Помещений должны быть оборудованы механическими замками.

11. Перед началом рабочего (служебного) времени Сотрудники Администрации берут ключи от Помещений без внесения записи в журнал.

12. В течение рабочего (служебного) времени ключи от Помещений хранятся у Сотрудников Администрации.

13. По окончании рабочего (служебного) времени Сотрудники Администрации закрывают Помещения и сдают ключи без внесения записи в журнал.

14. Внутренний контроль за соблюдением порядка доступа в Помещения проводится лицом, ответственным за организацию обработки персональных данных в администрации Дальнегорского городского округа.

Приложение 7

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-па

Перечень помещений, в которых обрабатываются персональные данные и размещены информационные системы администрации Дальнегорского городского округа

Настоящий документ содержит список помещений администрации Дальнегорского городского округа, в которых осуществляется обработка персональных данных, и размещены информационные системы которых осуществляется обработка персональных данных, и размещены информационные системы

№ п/п	Адрес места расположения	Наименование структурного подразделения, наименование помещения
1. Хранение бумажных носителей персональных данных		
1.1	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 125	– кабинет № 3 – отдел бухгалтерского учета и отчетности – кабинет № 7 - отдел жизнеобеспечения – кабинет № 9 – отдел ГО и ЧС и мобильной работы – кабинеты 13, 14а, 20 – Управление делами – кабинеты № 16, 19 – отдел экономики и предпринимательства
1.2	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 129	– кабинет № б/н - административная комиссия – кабинет № б/н - комиссия по делам несовершеннолетних – кабинет № 3 – отдел архитектуры и строительства
1.3	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 49	– кабинеты № б/н – Архивный отдел
1.4	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 71	– кабинеты б/н – Отдел опеки и попечительства
1.5	692446, Приморский край, г. Дальнегорск, ул. Набережная, д. 29	– кабинеты б/н – Отдел ЗАГС
2.Размещение автоматизированных рабочих мест информационных систем персональных данных		
2.1	692446, Приморский край,	- кабинет № 3 – отдел бухгалтерского учета и отчетности

№ п/п	Адрес места расположения	Наименование структурного подразделения, наименование помещения
	г. Дальнегорск, проспект 50 лет Октября, д. 125	- кабинет № 7 - отдел жизнеобеспечения - кабинеты 13, 14а, 20 – Управление делами - кабинеты № 16, 19 – отдел экономики и предпринимательства
2.2	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 129	– кабинет № б/н - административная комиссия кабинет № б/н - комиссия по делам несовершеннолетних - кабинет № 3 – отдел архитектуры и строительства
2.3	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 49	– кабинеты № б/н – Архивный отдел
2.4	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 71	– кабинеты б/н – Отдел опеки и попечительства
2.5	692446, Приморский край, г. Дальнегорск, ул. Набережная, д. 29	– кабинеты б/н – Отдел ЗАГС
3. Перечень помещений, в которых осуществляется обработка и хранение персональных данных		
3.1	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 125	- кабинет № 3 – отдел бухгалтерского учета и отчетности - кабинет № 7 – отдел жизнеобеспечения - кабинеты 13, 14а, 20 – Управление делами – - кабинеты № 16, 19 – отдел экономики и предпринимательства
3.2	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 129	– кабинет № б/н – административная комиссия кабинет № б/н – комиссия по делам несовершеннолетних - кабинет № 3 – отдел архитектуры и строительства
3.3	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 49	– кабинеты № б/н – Архивный отдел
3.4	692446, Приморский край, г. Дальнегорск, проспект 50 лет Октября, д. 71	– кабинеты б/н – Отдел опеки и попечительства
3.5	692446, Приморский край, г. Дальнегорск, ул. Набережная, д. 29	– кабинеты б/н – Отдел ЗАГС

Приложение 8

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ПОРЯДОК
учета, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа

1. Термины и определения

1.1. В настоящем Порядке использованы следующие термины и определения:

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

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

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

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 ПДн.

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

Пользователь персональных данных - лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных - процесс, в котором присутствует обработка персональных данных.

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

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

2. Используемые сокращения

2.1. В настоящем Порядке использованы следующие сокращения:

- ИСПДн – информационная система персональных данных;
- ОС – операционная система;
- ПДн – персональные данные;
- СВТ – средства вычислительной техники;
- СЗПДн – система защиты персональных данных.

3. Область применения

3.1. Настоящий Порядок учета, хранения и уничтожения носителей ПДн (далее - Порядок) предназначен для определения единого порядка обращения с машинными (электронными) и бумажными носителями персональных данных в администрации Дальнегорского городского округа (далее - Администрация).

4. Общие положения

4.1. Настоящий Порядок устанавливает порядок учета, хранения, использования и уничтожения носителей ПДн в процессах обработки ПДн.

4.2. Настоящий Порядок разработан в соответствии с Положением об обеспечении безопасности персональных данных в администрации Дальнегорского городского округа.

5. Порядок работы с бумажными носителями

5.1. Порядок учета бумажных носителей, содержащих ПДн

5.1.1. Любой документ, содержащий ПДн, является конфиденциальным и подлежит обязательному учету. Учет документов, содержащих ПДн, осуществляется в соответствии с положениями настоящего Порядка.

5.1.2. Ответственность за организацию ведения учета документов возлагается на должностное лиц, ответственное за организацию работ по обработке ПДн.

5.2. Порядок хранения бумажных носителей, содержащих ПДн

5.2.1. С целью обеспечения физической сохранности документов, содержащих ПДн, предотвращения хищения документов, а также с целью недопущения разглашения содержащихся в них сведений документы должны храниться в местах, исключающих доступ к ним посторонних лиц.

5.2.2. Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

5.2.3. Рабочее место работника Администрация должно быть организовано таким образом, чтобы исключить возможность просмотра документов с ПДн лицами, которые не допущены к ПДн.

5.2.4. Во время работы на столе должны находиться только те документы, непосредственно с которыми ведется работа, все остальные должны быть убраны в места, предназначенные для хранения.

5.3. Порядок уничтожения бумажных носителей, содержащих ПДн

5.3.1. Основанием для уничтожения документов, содержащих ПДн, является достижение целей обработки.

5.3.2. Локальные документы, содержащие ПДн, уничтожаются по мере необходимости.

5.3.3. Ответственность за своевременное уничтожение документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

5.3.4. Уничтожение документов производится с помощью специальных бумагорезательных технических средств (шредеров) или сжиганием.

5.3.5. Уничтожение массивов документов.

5.3.6. Массивы документов (архивы, библиотеки и т.п.) уничтожаются под контролем должностного лица ответственного за защиту ПДн.

5.3.7. Экспертиза документа проводится раз в год. Экспертиза охватывает все документы, содержащие ПДн, за соответствующий период времени.

5.3.8. Экспертиза проводится путем изучения содержания документов. Цель проведения экспертизы - определить возможность уничтожения документов либо дальнейшие сроки их хранения.

5.3.8. После проведения экспертизы составляется Акт о выделении дел и документов, подлежащих уничтожению (Приложение 1 к Порядку). В Акт включаются отобранные дела для уничтожения, отдельные документы из дел и документы выделенного хранения.

5.3.9. Уничтожение массивов документов производится с помощью бумагорезательных технических средств или сжиганием.

5.3.10. Если уничтожение массивов документов производит третья сторона, с которой заключен соответствующий договор, то документы, выделенные для уничтожения, помещаются в короба, после чего короба запечатываются передаются третьей стороне.

5.3.11. После уничтожения массива документов должностными лицами, ответственными за организацию работ по обработке ПД и за защиту ПДн, а также работниками, производившими уничтожение документов, подписывается Акт об уничтожении документов, содержащих ПДн (Приложение 2 к Порядку).

6. Порядок работы с машинными носителями

6.1. Учету подлежат следующие типы машинных носителей ПДн:

6.1.1. отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее);

6.1.2. неотчуждаемые носители информации (жесткие магнитные диски).

6.2. Порядок учета машинных носителей, содержащих ПДн

6.2.1. Все отчуждаемые машинные носители данных, используемые при работе со средствами вычислительной техники (далее - СВТ) для обработки и хранения ПДн, обязательно регистрируются и учитываются в Журнале учета выдачи машинных носителей ПДн (Приложение 3 к Порядку).

6.2.2. Неотчуждаемые носители информации подлежат учету в составе системных блоков СВТ, которые в свою очередь учитываются в Техническом паспорте ИСПДн.

6.2.3. Ответственность за ведение Журнала учеты выдачи машинных носителей ПДн и контроль учета носителей ПДн возлагается на ответственного за организацию обработки персональных данных Администрации.

6.2.4. Каждому машинному носителю, содержащему ПДн, присваивается учетный номер согласно Журналу.

6.2.5. В качестве учетного номера допускается использование серийного (заводского) номера носителя. В случае отсутствия серийного номера, учетный номер наносится на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

6.3. Порядок использования машинных носителей ПДн

6.3.1. Машинные носители ПДн выдаются пользователям или другим лицам, участвующим в обработке ПДн, для работы под подпись в Журнале. По завершении работы машинные носители ПДн сдаются обратно.

6.3.2. В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся должностному лицу ответственному за защиту ПДн.

6.3.3. Передача носителя, содержащего ПДн, третьим сторонам производится в соответствии с требованиями договора между Администрация и третьим лицом.

6.3.4. Машинные носители ПДн пересылаются в том же порядке, что и документы.

6.3.5. При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

6.3.6. Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны Администрация запрещается без соответствующего разрешения должностного лица ответственного за защиту ПДн.

6.4. Порядок хранения машинных носителей ПДн

6.4.1. Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, нарушения целостности или уничтожения содержащейся на них информации.

6.4.2. Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или металлические шкафы, запираемые на ключ.

6.4.3. Не допускается оставлять без присмотра на рабочем столе или в СВТ машинные носители, содержащие ПДн.

6.4.4. Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них ПДн несет работник, за которым закреплен носитель.

6.5. Порядок уничтожения машинных носителей ПДн

6.5.1. Основанием для уничтожения машинных носителей ПДн, является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает должностное лицо ответственное за защиту ПДн.

6.5.2. Списанные машинные носители, подлежащие уничтожению, хранятся в сейфе должностного лица ответственного за защиту ПДн. Уничтожение таких носителей производится раз в год.

6.5.3. Уничтожение носителей производится путем их физического разрушения с предварительным затиранием (форматированием, уничтожением) содержащихся на них ПДн, если это позволяют физические принципы работы носителя.

6.5.4. Уничтожение машинных носителей производится Комиссией по уничтожению персональных данных на машинных (бумажных) носителях (далее – Комиссия) в составе не менее 3 человек. В состав Комиссии должно обязательно входить должностное лицо ответственное за защиту ПДн. После уничтожения всех машинных носителей составляется Акт на списание и уничтожение машинных(бумажных) носителей персональных данных (Приложение 4 к Порядку).

6.5.5. При уничтожении, машинные носители снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале.

6.6. Порядок уничтожения (стирания) ПДн с машинного носителя

6.6.1. Основанием для уничтожения (стирания) записей или части записей с электронного носителя являются следующие случаи:

- возврат носителя сотрудником;
- передача носителя в ремонт;
- списание носителя.

6.6.2. Хранящаяся на электронных носителях и потерявшая актуальность информация, содержащая ПДн, своевременно стирается (уничтожается). Работник, совместно с системным администратором Администрации, принимает окончательное решение о необходимости уничтожения (стирания) с него записей.

6.6.3. Работник осуществляет уничтожение информации с носителя самостоятельно, с использованием встроенных средств ОС.

6.6.4. При невозможности самостоятельного уничтожения информации с носителя, работник передает электронный носитель должностному лицу ответственному за защиту ПДн. Совместно с носителем передается служебная записка, в которой указывается причины передачи (возврата) и основание для уничтожения содержащейся на нем информации.

6.6.5. Должностное лицо ответственное за защиту ПДн, ответственное за уничтожение (стирание) информации с электронных носителей, при получении носителя должно обеспечить уничтожение (стирание) информации с носителя, способом, исключающим ее дальнейшее восстановление и подготовить Акт на списание и уничтожение машинных(бумажных) носителей персональных данных.

6.6.6. В Акт заносится дата, учетный номер носителя и способ уничтожения (стирания) информации, а также используемые для этого программные средства.

6.6.7. Носители, пригодные к повторной эксплуатации, после уничтожения записанной на них информации могут быть использованы для повторной записи информации.

7. Пересмотр и внесение изменений

7.1. Пересмотр положений настоящего документа проводится в следующих случаях:

- при появлении новых требований к обработке и обеспечению безопасности ПДн со стороны законодательства РФ и контролирующих органов исполнительной власти Российской Федерации;
- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;
- не реже одного раза в год.

7.2. Ответственным за пересмотр настоящего Порядка и составление рекомендаций по изменению является должностное лицо ответственное за организацию обработки ПДн.

7.3. Внесение изменений производится на основании соответствующего распоряжения администрации Дальнегорского городского округа.

Приложение 1
к Порядку учёта, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа

А К Т № _____
о выделении дел и документов, подлежащих уничтожению

от «_____»_____202_ г.

Комиссия в составе:
<Фамилия И.О. – должность;>
<Фамилия И.О. – должность.>
<Фамилия И.О. – должность.>

составила настоящий акт о том, что на основании проведенной экспертизы, отобрала к уничтожению, следующие документы и дела, утратившие практическую ценность:

№ п\п	Заголовок документа\дела	Основание для уничтожения

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Приложение 2
к Порядку учёта, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа

А К Т № _____
уничтожения бумажных носителей, содержащих персональные данные

от «_____»_____202_ г.

Комиссия в составе:
<Фамилия И.О. – должность;>
<Фамилия И.О. – должность.>
<Фамилия И.О. – должность.>

составила настоящий акт о том, что произведено плановое уничтожение бумажных носителей, содержащих персональные данные, с истекшим сроком использования и/или утративших практическое значение.

- «тип носителя, учётный номер носителя»
- «тип носителя, учётный номер носителя»
- …

Бумажные носители уничтожены путём сжигания/шредирования/химической обработки и т.п. *(нужное отметить)*.

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Приложение 3
к Порядку учёта, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа

Журнал учета носителей информации, содержащих персональные данные

№ п/п	Учетный № носителя	Дата	Тип носителя	Содержимое носителя	Ф.И.О. отв. лица	Подпись отв. лица	Отметка о возврате (с указанием причины)	Ф.И.О. отв. лица	Подпись отв. лица	Дата уничтожения носителя	Ф.И.О. отв. за уничтожение
1	2	3	4	5	6	7	8	9	10	11	12

Приложение 4
к Порядку учёта, хранения и уничтожения носителей персональных данных в администрации Дальнегорского городского округа

УТВЕРЖДАЮ
Глава Дальнегорского городского округа
ФИО _____
«__»_____202__г.

Акт на списание и уничтожение
машинных (бумажных) носителей персональных данных

Комиссия в составе:

Председатель комиссии:	
Члены комиссии:	

составила настоящий акт в том, что перечисленные в нем машинные (бумажные) носители персональных данных, подлежат уничтожению как утратившие практическое значение и непригодные для перезаписи.

№ п/п	Вид носителя	Учетный номер носителя	Дата поступления	Краткое содержание информации

Всего подлежит списанию и уничтожению _____ наименований машинных (бумажных) носителей защищаемой информации (количество числом и прописью)
Правильность произведенных записей в акте проверил:

_____
(подпись)
Машинные (бумажные) носители защищаемой информации перед уничтожением сверили с записями в акте и полностью уничтожили путем
_____
_____

«_____»_____20__г.

Председатель комиссии: _____

Члены комиссии: _____
_____
_____

Приложение 9

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-па

ПОРЯДОК
реагирования на инциденты информационной безопасности в администрации Дальнегорского городского округа

1. Термины и определения

1.1. В настоящем Порядке использованы следующие термины и определения:

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.

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

Вредоносное программное обеспечение - программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации - возможность получения информации и ее использования.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

Информационная система персональных данных - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таковых средств.

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

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

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

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

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 ПДн.

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

Пользователь персональных данных - лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных - процесс, в котором присутствует обработка персональных данных.

Средство защиты информации - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

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

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

Доступность информации - свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

2. Используемые сокращения

В настоящем Порядке использованы следующие сокращения:

- ИБ – информационная безопасность;
- ИСПДн – информационная система персональных данных;
- НСД - несанкционированный допуск;
- ПДн – персональные данные.

3. Область применения

3.1. Настоящий Порядок реагирования на инциденты информационной безопасности (далее - Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в администрации Дальнегорского городского округа (далее - Администрация).

3.2. Требования настоящего Порядка распространяются на должностных лиц Администрации, отвечающие за обеспечение безопасности ПДн.

4. Общие положения

4.1. Настоящий Порядок разработан в соответствии с Политикой администрации Дальнегорского городского округа в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

4.2. В соответствии с настоящим Порядком к инцидентам ИБ в Администрации относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;
- отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;
- несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);
- заражение программных компонентов ИСПДн вредоносным программным обеспечением.

4.3. К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн, срок действия полномочий, которых истек, либо в состав полномочий, которых не входят выявленные действия с ПДн;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.
- совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и

идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав ИСПДн.

4.4. Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения, описанных выше инцидентов.

5. Оповещение об инциденте информационной безопасности

5.1. В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников Администрации:

5.1.1. прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

5.1.2. оповестить своего непосредственного руководителя о факте выявления инцидента ИБ;

5.1.3. руководитель должен оповестить должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн;

5.1.4. после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

5.2. Должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется главе Администрации для принятия решения о проведении расследования инцидента ИБ.

5.3. Порядок проведения расследования инцидента ИБ описан в разделе 7 настоящего Порядка.

5.4. Мероприятия по устранению причин и недопущению повторного возникновения инцидента ИБ описаны в разделе 8 настоящего Порядка.

6. Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

6.1. В случае если инцидент ИБ может стать (или уже стал) причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин, повлекших за собой возникновение инцидента ИБ. Решение о блокировании ПДн принимает должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн.

6.2. ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

7. Проведение расследования инцидента информационной безопасности

7.1. Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

- нарушения конфиденциальности, целостности или доступности ПДн;
- халатности и несоблюдения требований по обеспечению безопасности ПДн;
- несоблюдения условий хранения носителей ПДн;
- использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

7.2. Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

7.3. Проведение внутреннего расследования проводится по решению главы муниципального образования. С целью проведения расследования в обязательном порядке формируется Комиссия, в состав которой входят должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн, юрист и иные должностные лица Администрации, участие которых может потребоваться.

7.4. Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

7.5. Общая продолжительность внутреннего расследования не должна превышать одного месяца.

7.6. В рамках проведения расследования инцидента ИБ Комиссия уполномочена:

- проводить опрос сотрудников Администрации, по вине которых предположительно произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;
- проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ;

7.7. По решению главы Администрации на Комиссию могут быть возложены дополнительные обязанности и права.

7.8. Работник, в отношении которого проводится расследование, должен быть ознакомлен с распоряжением о проведении расследования.

7.9. Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки и т.п.).

7.10. Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии в виде протокола.

7.11. В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения главой администрации Дальнегорского городского округа.

7.12. Для оперативного проведения внутреннего расследования должностное лицо ответственного за защиту ПДн составляет План проведения расследования.

7.13. Одновременно с проведением внутреннего расследования, глава Администрации может поручить Комиссии определить ущерб для Администрации и (или) для субъекта ПДн от произошедшего инцидента ИБ. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

7.14. По окончании внутреннего расследования Комиссия представляет главе Администрации отчет по результатам расследования, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

7.15. К отчету прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

7.16. Отчет должен быть подписан всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

7.17. Отчет подлежит утверждению главой Администрации.

7.18. Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами

расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

7.19. Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с отчетом по результатам расследования.

7.20. Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

7.21. При наличии в действиях работника признаков административного правонарушения или уголовного преступления глава Администрации обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

7.22. В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

7.23. При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

7.24. Первый экземпляр отчета с резолюцией главы Администрации, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у главы Администрации.

8. Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

8.1. Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе ПДн;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе ПДн;
- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;
- ознакомление пользователей с мерами ответственности, установленными нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

9. Пересмотр и внесение изменений

9.1. Настоящий Порядок должен пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;

- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;

- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

9.2. Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн в Администрации.

9.3. Внесение изменений производится на основании соответствующего распоряжения Администрации.

Приложение 10

УТВЕРЖДЕНЫ
распоряжением администрации
Дальнегорского городского округа
от 29.11.2022 № 379-ра

ПРАВИЛА
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации Дальнегорского городского округа

1. Общие положения

1.1. Настоящие Правила определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Правила), и отражают соотношение указанного возможного вреда и принимаемых администрацией Дальнегорского городского округа (далее – Администрация) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. В настоящих Правила используются следующие основные понятия:

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.

Доступность информации – состояние информации (ресурсов информационной системы), при которой субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система персональных данных - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таковых средств.

Конфиденциальность информации/персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Моральный вред – физические или нравственные страдания, причиняемые действиями (бездействием), нарушающими личные неимущественные права субъекта персональных данных либо посягающими на принадлежащие ему нематериальные блага, а также в других случаях, предусмотренных законодательством Российской Федерации.

Оценка возможного вреда – определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

Убытки – расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утраты ил повреждения его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условия гражданского оборота, если бы его право не было нарушено.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

2. Методика оценки возможного вреда субъектам персональных данных

2.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных (далее – ПДн).

2.2. Неправомерные действия в отношении персональных данных определяются как следующие нарушения безопасности информации:

- неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности ПДн;
- неправомерное уничтожение и блокирование ПДн является нарушением доступности ПДн;
- неправомерное изменение ПДн является нарушением целостности ПДн;
- нарушение прав субъекта требовать от оператора уточнения его ПДн, их блокирования или уничтожения является нарушением целостности информации;
- нарушение прав субъекта на получение информации, касающейся обработки его ПДн, является нарушением доступности ПДн;
- обработка ПДн, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности ПДН;
- неправомерное получение ПДн от лица, не являющегося субъектом ПДн, является нарушением конфиденциальности ПДН;
- принятие решения, порождающего юридические последствия в отношении субъекта ПДн или иным образом затрагивающего его права и законные интересы, на основании исключительно автоматизированной обработки его ПДн без согласия

на то в письменной форме субъекта ПДн или не предусмотренное федеральными законами, является нарушением конфиденциальности ПДН.

2.3. Субъекту ПДн может быть причинен вред в форме:

- убытков;

- морального вреда;

- распространения информации, порочащей честь и достоинство, деловую репутацию;

2.4. Уровни возможного вреда определяются на основании последствий допущенного нарушения принципов обработки ПДн:

- низкий уровень возможного вреда (1) – последствия нарушения принципов обработки ПДн, включающие только нарушение целостности ПДн либо только нарушение доступности ПДн;

- средний уровень возможного вреда (2) – последствия нарушения принципов обработки ПДн, включающие только нарушение целостности ПДн, повлекшее убытки и моральный вред, либо только нарушение доступности ПДн, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности ПДН;

- высокий уровень возможного вреда (3) – последствия нарушения принципов обработки ПДн, включающие только нарушение конфиденциальности ПДН, повлекшие убытки и моральный вред.

3. Порядок проведения оценки возможного вреда, а также соответствия возможного вреда и реализуемых мер защиты

3.1. Оценка возможного вреда субъектам ПДн, а также соотнесение возможного вреда и реализуемых в Администрации мер защиты (далее – оценка вреда субъекту ПДн) осуществляется в отношении каждой информационной системы ПДн (далее – ИСПДн) Администрации.

3.2. Оценка вреда субъектам ПДн осуществляется для ИСПДн органов Администрации – лицом, ответственным за организацию обработки ПДн в Администрации.

3.3. Для проведения оценки вреда субъектам ПДн распоряжением Администрации создается комиссия не менее чем из трех человек из числа работников органов Администрации, в чьем ведении находится ИСПДн. В обязательном порядке в состав комиссии включаются сотрудники, отвечающие за информационную безопасность и за профилактику коррупции.

3.4. Оценка вреда субъектам ПДн проводится следующим образом: *каждым членом комиссии, в соответствии с показателями, указанными в разделе 2 настоящих Правил, выставляется одна из оценок уровней возможного вреда субъекту в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и реализации актуальных угроз безопасности ПДн из-за несанкционированного, в том числе случайного, доступа к ПДн при их обработке в конкретной ИСПДн.*

3.4.1. Оценка возможного вреда субъекту ПДн определяется как среднее значение оценок возможного вреда субъекту, выставленных членами комиссии, и принимается равным:

- низкой – в случае, если среднее значение равно от 1 до 1,5;
- средней – в случае, если среднее значение равно от 1,6 до 2,5;
- высокой – в случае, если среднее значение равно от 2,6 до 3.

3.5. По результатам проведения оценки вреда субъектам персональных данных составляется Акт оценки вреда субъектам персональных данных, обрабатываемых в информационной системе персональных данных администрации Дальнегорского городского округа, по форме согласно приложению к настоящим Правилам.

3.6. Состав реализуемых Администрацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законов от 27.07.2006 № 152-ФЗ «О персональных данных», определяется лицом, ответственным за организацию обработки ПДн, исходя из правомерности и разумной достаточности указанных мер.

3.7. Обеспечение безопасности ПДн достигается:

- определением угроз безопасности ПДн при из обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн.;
- применение прошедших в установленном порядке процедур оценки состояния средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПД;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Приложение
к Правилам оценки вреда, который может быть причинен субъекта персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации Дальнегорского городского округа

АКТ
оценки вреда субъектам персональных данных, обрабатываемых в информационных системах персональных данных

_____

_(наименование информационной системы персональных данных)

«____»_____20__г. №

_____

Комиссия в составе:

Председателя: _____

членов комиссии: _____

_____

_____

в целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами провела оценку возможного вреда субъектами персональных данных, а также соотнесение возможного вреда и реализуемых мер защиты на основании правил оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

№ п/п	Требования Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»/тип актуальных угроз безопасности персональных данных	Член комиссии № 1			Член комиссии № …			Реализуемые меры защиты	Оценка возможного вреда
		Возможные нарушения безопасности информации и причиненный субъекту вред (+/-)		Уровень возможного вреда	Возможные нарушения безопасности информации и причиненный субъекту вред (+/-)		Уровень возможного вреда		
1		убытки и моральный вред			убытки и моральный вред				
		целостность			целостность				
		доступность			доступность				
		конфиденциальность			конфиденциальность				
2		убытки и моральный вред			убытки и моральный вред				
		целостность			целостность				
		доступность			доступность				
		конфиденциальность			конфиденциальность				
…		убытки и моральный вред			убытки и моральный вред				
		целостность			целостность				
		доступность			доступность				
		конфиденциальность			конфиденциальность				

На основании экспертных оценок, выставленных членами комиссии, комиссия определила, что в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и реализации активных угроз безопасности персональных данных из-за несанкционированного доступа, в том числе случайного доступа к персональным

данных при их обработке в информационных системах персональных данных _____, субъектам персональных данных может быть причинен вред, который оценивается как _____.

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

_____ _____

Приложение 11

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ПОРЯДОК
резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Дальнегорского городского округа

1. Общие положения

1.1. Настоящая инструкция разработана на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» с целью организации порядка резервирования и восстановления работоспособности технических средств (далее — ТС) и программного обеспечения (далее - ПО), баз данных (далее - БД) и средств защиты информации (далее — СЗИ) в информационных системах персональных данных администрации Дальнегорского городского округа (далее - ИСПДн).

1.2. Настоящий Порядок определяет порядок резервирования и восстановления работоспособности ТС и ПО, БД и СЗИ, и определяет порядок действий ответственных лиц, связанных с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.3. Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.4. Задачами данной инструкции являются:

- определение мер защиты от потери информации;
- определение действий по восстановлению в случае потери информации.

1.5. Действие настоящего Порядка распространяется на всех пользователей администрации Дальнегорского городского округа, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.6. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

1.7. Сотрудником ответственным, за реагирование на инциденты безопасности и контроль мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, назначается Администратор безопасности ИСПДн.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в Журнале учета нештатных ситуаций и выполнения профилактических работ, установки, модификации программных средств на рабочих станциях и серверах, составленном по форме (Приложение № 1 к Порядку).

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники администрации Дальнегорского городского округа, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством.

3. Технические меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа; системы жизнеобеспечения ИС.

3.2. Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все помещения администрации Дальнегорского городского округа, в которых размещаются элементы ИСПДн, материальные носители ПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных рабочих станций и серверов;

- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

3.6. Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИС должны использоваться территориально удаленные системы кластеров.

3.7. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на съемный носитель (ленту, жесткий диск и т. п.).

4. Организационные меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

4.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных - не реже раза в день инкрементальным способом, и не реже одного раза в неделю полный объем данных;

- для технологической информации - не реже одного раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС - не реже одного раза в

месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале резервного копирования информации (Приложение № 2 к Порядку).

4.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя, датой проведения резервного копирования.

4.4. Носители должны храниться в несгораемом шкафу или в помещении, оборудованном системой пожаротушения.

4.5. Носители должны храниться не менее года для возможности восстановления данных.

5. Ответственность за поддержание установленного в настоящем Порядке проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности информации ИСПДн

Приложение 1
к Порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Дальнегорского городского округа

ЖУРНАЛ УЧЕТА

нештатных ситуаций и выполнения профилактических работ, установки, модификации программных средств на рабочих станциях и серверах ИСПДн

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО ответственного за эксплуатацию	Специалист/организация, выполнявшая работы
1	2	3	4	5

Приложение 2
к Порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Дальнегорского городского округа

ЖУРНАЛ
резервного копирования информации

№ п/п	Дата	Наименование объекта резервного копирования	Место хранения	Примечание
1	2	3	4	5

Приложение 12

УТВЕРЖДЕН
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ПОРЯДОК
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации Дальнегорского городского округа

1. Общие положения

1.1. Порядок по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (далее - ИСПДн) администрации Дальнегорского городского округа (далее - Администрация), регламентирует действия при проведении работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн.

1.2. Требования настоящего Порядка распространяются на всех должностных лиц и сотрудников органов Администрации, использующих в работе ИСПДн, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

1.3. Сотрудники Администрации, задействованные в обеспечении функционирования ИСПДн, знакомятся с основными положениями и приложениями Порядка в части, их касающейся, по мере необходимости.

1.4. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например: в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний, злоумышленных действий, практическая «глубина» исполнения настоящего Порядка определяется Администратором безопасности ИСПДн (далее - Администратор), по согласованию с первым заместителем главы Дальнегорского городского округа.

2. Порядок проведения работ

2.1. Все изменения конфигурации технических и программных средств рабочих станций Администрации должны производиться только на основании заявок руководителей органов Администрации, составленных согласно форме (приложение №1), согласованных с главой Дальнегорского городского округа. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя органа Администрации.

2.2. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИСПДн Администрации, должны производиться только на

основании заявок руководителей структурных подразделений Администрации (приложение № 1 к Порядку), согласованных с главой Дальнегорского городского округа. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя органа Администрации. При этом необходимо уведомить об осуществленных изменениях организацию, производившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

2.3. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИСПДн Администрации, отражаются в Техническом паспорте объекта информатизации. Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации.

2.4. В заявке указываются наименование ПЭВМ и ответственный за нее сотрудник. После чего заявка передается Администратору ИСПДн для выполнения работ по внесению изменений в конфигурацию ПЭВМ ИСПДн Администрации.

2.5. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИСПДн Администрации предоставляется Администратору.

2.6. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме Администратора, запрещено.

2.7. Установка и настройка программного средства осуществляется администратором согласно эксплуатационной документации.

2.8. Запрещается установка и использование на ПЭВМ (серверах) программного обеспечения (ПО), не входящего в перечень программного обеспечения, разрешенного к использованию в Администрации.

2 2.9. Руководители органов Администрации осуществляют контроль за отсутствием на ПЭВМ сотрудников подразделения программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.10. Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у Администратора. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

2.11. После установки (обновления) ПО Администратор должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем ПЭВМ, проверить правильность настройки средств защиты.

2.12. В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают руководителю своего подразделения и Администратору.

Использование программного средства до получения специальных указаний запрещается.

2.13. После завершения работ по внесению изменений в состав аппаратных средств, защищенных ПЭВМ, системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) Администратором.

2.14. При изъятии ПЭВМ из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью Администратора (приложении № 2 к Порядку).

2.15. Оригиналы заявок (документов) и актов должны храниться у Администратора.

Приложение 1
к Порядку по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн администрации Дальнегорского городского округа

Главе Дальнегорского городского округа

ЗАЯВКА

На внесение изменений в состав программного (аппаратного) обеспечения
(ненужное зачеркнуть)

_____
(наименование ПЭВМ)

Прошу дать указание ответственным сотрудникам Администрации для установления (изменения настроек)
(ненужное зачеркнуть)

_____

_____
(перечень ПО (аппаратных средств) и необходимых настроек)

для решения задач:

_____

_____

_____

_____

следующим пользователям:

_____

_____

_____
(Фамилия, Имя, Отчество)

Руководитель _____
(наименование структурного подразделения)

«____»_____20___г._____

_____
(подпись) (Фамилия, инициалы)

Обратная сторона заявка

Изменения на ПЭВМ ИСПДн произведены (не произведены) по следующей причине:

(ненужное зачеркнуть)

_____

_____

_____

_____

Выполнены следующие работы:

_____

_____

_____

_____

_____

_____

Выполнены следующие изменения в настройках средств защиты:

_____

_____

_____

_____

_____

Администратор безопасности ИСПДн

«____»_____20___г._____

_____

(подпись) (Фамилия, инициалы)

Приложение 2
к Порядку по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн администрации Дальнегорского городского округа

АКТ
о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД _____
(модель, серийный номер)
передаваемого _____
(с какой целью)
_____
_____
(кому: должность, Ф.И.О.)

ПЭВМ: _____
(наименование ПЭВМ)
уничтожены (затерты) посредством программы _____
_____

Администратор безопасности ИСПДн

«____»_____20___г._____
_____
(подпись) (Фамилия, инициалы)

Приложение 13

УТВЕРЖДЕНА
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных администрации Дальнегорского городского округа

1. Общие положения

1.1. Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее –ИСПДн) и устанавливает ответственность за их выполнение.

2. Основные определения

2.1. Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

- дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);
- модификации или уничтожению программ, или данных;
- приведению в негодность носителей информации и других технических средств;
- нарушению функционирования средств защиты информации.

3. Инструкция по применению средств антивирусной защиты

3.1. Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

3.2. К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.

3.3. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на системного администратора администрации Дальнегорского городского округа.

3.4. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

3.5. Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.

3.6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места системного администратора администрации Дальнегорского городского округа.

3.7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.

3.8. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.

3.9. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

3.10. Контроль входящей информации необходимо проводить непосредственно после ее приема.

3.11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

3.12. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3.13. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к системному администратору администрации Дальнегорского городского округа.

3.14. При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

3.15. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения вируса системного администратора администрации Дальнегорского городского округа;

- провести лечение зараженных файлов;

- в случае невозможности лечения обратиться к администратору безопасности ИСПДн.

3.16. По факту обнаружения зараженных вирусом файлов системный администратор администрации Дальнегорского городского округа должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3.17. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

3.18. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

3.19. Ответственный за организацию обработки ПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

3.20. С данной инструкцией Пользователи должны быть ознакомлены под роспись в листе ознакомления с данной инструкцией.

3.21. Проводить периодическое тестирование функций средств антивирусной защиты.

3.22. Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

Приложение 14

УТВЕРЖДЕНА
распоряжением администрации
Дальнегорского городского округа
от 29.12.2022 № 379-ра

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах персональных данных администрации Дальнегорского городского округа

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационных системах персональных данных администрации Дальнегорского городского округа (далее – Инструкция) является документов, устанавливающим основные принципы и правила организационно-технического обеспечения процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в администрации Дальнегорского городского округа (далее – Администрация), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с идентификаторами и личными паролями.

1.2. Целью настоящей Инструкции является обеспечение оптимальной работы пользователей информационной системы персональных данных (далее – ИСПДн), уменьшение угрозы безопасности ИСПДн и минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее – ПДн).

1.3. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 152 «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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».

1.3. Требования настоящей Инструкции распространяются на всех сотрудников Администрации (штатных, временных, работающих по контракту и др.) и должны выполняться при всех режимах функционирования ИСПДн.

2. Организационное и техническое обеспечение процессов генерации

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за действиями пользователей при работе с паролями в ИСПДн возлагается на ответственного за организацию обработки персональных данных (далее – Ответственный).

2.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) Пользователей осуществляет администратор ИСПДн в Администрации.

3. Организация парольной защиты

3.1. Личные пароли должны создаваться Пользователями самостоятельно.

3.2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.

3.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.4. Внеплановая смена пароля Пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность и др.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и ИСПДн соответственно.

3.5. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

3.6. Разблокирование учетной записи осуществляется Администратором и Ответственным для учетных записей Пользователя для АРМ и ИСПДн соответственно.

3.7. После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

4. Требования к формированию паролей

4.1. Пользователи при формировании паролей должны руководствоваться следующими требованиями:

- длина пароля должна быть не мене 8 символов;

- в пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих: *буквы в верхнем регистре, буквы в нижнем регистре, цифры, специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $ и др.);*

- пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.);

- пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть;

- пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.п., из нескольких символов (например, «1111111111», «wwwww» и т.п.);

- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «asdfgh» и т.п.).

4.2. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

5. Правила ввода паролей

5.1. Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и ИСПДн должны руководствоваться следующими правилами:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.);

5.2. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ и ИСПДн, Пользователю необходимо уведомить Администратора или Ответственного соответственно для проведения процедуры генерации нового пароля.

6. Обязанности

6.1. Пользователи ИСПДн обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов администрации Дальнегорского городского округа по парольной защите;

- своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно;

- ознакомиться под роспись с перечисленными в настоящей Инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

7. Ответственность

7.1. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ и ИСПДН в администрации Дальнегорского городского округа.