ГОРОДСКОЙ ОКРУГ УРАЙ
Ханты-Мансийского автономного округа - Югры

АДМИНИСТРАЦИЯ ГОРОДА УРАЙ
РАСПОРЯЖЕНИЕ

от 20.04.2022 № 238-р

Об обработке персональных данных

В соответствии с требованиями Федеральных законов от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 №152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 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 и муниципальными органами»:

1. Назначить заместителя главы города Урай, курирующего направление информационных технологий и связи, ответственным за организацию обработки персональных данных в администрации города Урай, возложив обязанности по:

1) осуществлению внутреннего контроля за соблюдением администрацией города Урай как оператором обработки персональных данных и ее сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доведению до сведения сотрудников администрации города Урай положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) осуществлению контроля за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей.

2. Назначить ответственным за выполнение работ по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных администрации города Урай (далее - ИСПДн), начальника отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай, возложив обязанности по обеспечению:

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

2) своевременного обнаружения фактов несанкционированного доступа к персональным данным и принятия действенных мер по защите от несанкционированного доступа в соответствии с организационно-распорядительными документами;

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

4) восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянного контроля за обеспечением уровня защищенности персональных данных;

6) обучения лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

7) учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

8) учета лиц, допущенных к работе с персональными данными в ИСПДн, установления правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечения регистрации и учёта всех действий, совершаемых с персональными данными в ИСПДн;

9) контроля за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

10) администрирования средств и систем защиты персональных данных в ИСПДн;

11) взаимодействия с лицензиатами ФСТЭК России и ФСБ России в целях приведения ИСПДн в соответствие требованиям законодательства;

12) разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработки и принятия мер по предотвращению возможных опасных последствий подобных нарушений;

13) разработки и представления руководству предложений по обеспечению безопасности персональных данных.

3. Назначить администратором безопасности информационных систем персональных данных в администрации города Урай специалиста-эксперта отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай Ю.А.Овечкина.

4. Установить, что ответственность за соблюдение сотрудниками администрации города Урай организационно-распорядительных документов по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, а так же обрабатываемых без использования средств автоматизации, несут их непосредственные руководители, которые обязаны:

1) взаимодействовать с отделом по защите информации и связи управления по информационным технологиям и связи администрации города Урай в порядке, предусмотренном организационно-распорядительными документами в области защиты информации, в том числе в части ремонта и обслуживания технических средств ИСПДн, организации доступа сотрудников к работе в ИСПДн и других вопросов, находящихся в компетенции отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай;

2) осуществлять контроль за соблюдением требований законодательной базы в области обеспечения безопасности персональных данных, а также инструкций, предписаний и иных документов, утверждённых руководством и другими уполномоченными лицами в части, предусмотренной организационно-распорядительными документами;

3) совместно с ответственным за выполнение работ по обеспечению безопасности персональных данных проводить разбирательства по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

5. Утвердить:

1) Положение о порядке обработки персональных данных в администрации города Урай согласно приложению 1;

2) Правила рассмотрения запросов субъектов персональных данных или их представителей согласно приложению 2;

3) Правила осуществления внутреннего контроля соответствия обработки персональных данных в администрации города Урай требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора, согласно приложению 3;

4) Правила работы с обезличенными данными в случае обезличивания персональных данных согласно приложению 4;

5) Перечень информационных систем персональных данных согласно приложению 5;

6) Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, согласно приложению 6;

7) Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных согласно приложению 7;

8) Перечень персональных данных, обрабатываемых в администрации города Урай, согласно приложению 8;

9) Инструкцию администратора информационной безопасности администрации города Урай согласно приложению 9;

10) Инструкцию пользователя информационной системы персональных данных согласно приложению 10;

11) Инструкцию по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств на аттестованных ИСПДн согласно приложению 11.

12) Политику в отношении обработки персональных данных согласно приложению 12;

6. Утвердить согласно приложению 13:

1) форму Журнала учета машинных носителей;

2) форму Журнала учета лиц допущенных к работе с персональными данными в информационных системах персональных данных администрации города Урай;

3) форму Журнала учета средств защиты информации;

4) форму Журнала учета выдачи персональных идентификаторов и электронных ключей (для администратора информационной безопасности);

5) форму Журнала учета обращений субъектов персональных данных по вопросам обработки персональных данных;

6) форму Акта определения уровня защищенности персональных данных при их обработке в ИСПДн и класса защищенности информационной системы;

7) форму Акта об уничтожении персональных данных субъектов персональных данных.

7. Проведение классификации ИСПДн в администрации города Урай возложить на Координационный совет по информатизации при администрации города Урай.

8. Считать утратившими силу распоряжения администрации города Урай:

1) от 25.07.2016 №386-р «Об обработке персональных данных»;

2) от 09.10.2019 №476-р «О внесении изменений в распоряжение администрации города Урай от 25.07.2016 №386-р «Об обработке персональных данных».

9. Службе обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай (Н.П.Ануфриева) обеспечить ознакомление с распоряжением работников администрации города Урай.

10. Контроль за выполнением распоряжения возложить на первого заместителя главы города Урай А.Ю. Ашихмина, заместителей главы города Урай О.Н.Хотинецкого, С.П.Новосёлову, Е.Н.Подбуцкую.

Глава города Урай Т.Р.Закирзянов

Приложение 1 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Положение о порядке обработки персональных данных в администрации города Урай

1. Общие положения

1.1. Положение о порядке обработки персональных данных в администрации города Урай (далее - Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в администрации города Урай.

1.2. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральными законами от 27.07.2006 №152-ФЗ «О персональных данных», от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации», 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 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», решением Думы города Урай 20.12.2010 №123 «О порядке материально-технического и организационного обеспечения деятельности органов местного самоуправления».

1.3. Администрация города Урай является оператором персональных данных.

2. Состав персональных данных

2.1. К персональным данным, обрабатываемым в администрации города Урай, относятся:

1) персональные данные работников администрации города Урай;
2) персональные данные уволенных работников;
3) персональные данные граждан, обращающихся в администрацию города Урай;
4) персональные данные физических и юридических лиц, заключающих (расторгающих) имущественные сделки;
5) персональные данные лиц, выполняющих поставки товаров, работы, оказывающих услуги по договорам;
6) персональные данные, обрабатываемые в целях предоставления государственных, муниципальных услуг.

2.2. Персональные данные работников администрации города Урай, обрабатываемые без использования средств автоматизации (неавтоматизированная обработка), содержатся в:

1) личных делах работников;
2) личных делах уволенных работников;
3) трудовых книжках работников;
4) медицинских справках;
5) документах, подтверждающих право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;
6) документах о возрасте детей или беременности женщины для предоставления установленных законом условий труда, гарантий и компенсаций;
7) иных документах, связанных с осуществлением трудовых отношений.

2.3. Персональные данные, обрабатываемые с использованием средств автоматизации, содержатся в информационных системах персональных данных администрации города Урай.

3. Обработка персональных данных

3.1. Обработка персональных данных осуществляется в соответствии принципами и условиями, установленными Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», а также в соответствии с общими требованиями, установленными Трудовым кодексом Российской Федерации.

3.2. Обработка персональных данных в органах администрации города Урай ведется работниками в объеме, необходимом для выполнения должностных обязанностей.

3.3. Перечень информационных систем обработки персональных данных (далее – ИСПДн), перечень должностей, замещение которых предусматривает осуществление обработки персональных данных, утверждается распоряжением администрации города Урай.

3.4. Обработка персональных данных ведется работниками на рабочих местах, выделенных для исполнения ими должностных обязанностей.

3.5. Допуск работников администрации города Урай к ИСПДн осуществляется с соблюдением порядков по информационной безопасности, действующих в администрации города Урай.

3.6. Санкционированный внешний доступ к персональным данным, обрабатываемым в администрации города Урай, имеют:

1) работники контрольно-надзорных органов, при наличии служебного удостоверения и документов, на основании которых они проводят проверку;

2) работники сторонних организаций, обеспечивающих программное сопровождение информационных систем, при наличии в договоре условий о сохранении конфиденциальной информации;

3) работники страховых фондов, государственных и негосударственных пенсионных фондов, налоговых органов, в соответствии с действующим законодательством, при наличии документов, подтверждающих их полномочия.

3.7. Внутренний доступ к персональным данным, обрабатываемым в администрации города Урай, без специального разрешения имеют:

1) глава города Урай;

2) первый заместитель главы города Урай;

3) заместители главы города Урай;

4) работники службы обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай;

5) работники управления по информационным технологиям и связи администрации города Урай.

3.8. Получение (сбор) персональных данных.

3.8.1. Сбор персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности субъекта персональных данных, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.8.2. Персональные данные получаются лично у субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными.

3.8.3. В случае возникновения необходимости получения персональных данных граждан, претендующих на замещение должностей в администрации города Урай или работников, занимающих должности в администрации города Урай, у третьей стороны, следует получить письменное согласие гражданина по форме, установленной приложением 1 к Положению, и сообщить о целях, предполагаемых источниках и способах получения персональных данных.

3.8.4. При сборе персональных данных работник, осуществляющий сбор (получение) персональных данных непосредственно от работников администрации города Урай, граждан, претендующих на замещение должностей в администрации города Урай, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные по форме, установленной приложением 2 к Положению.

3.8.5. Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его национальной принадлежности, политических, религиозных и иных убеждениях, а также интимной жизни и состояния здоровья без его письменного согласия.

3.8.6. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

3.8.7. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных.

3.9. Хранение персональных данных.

3.9.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

3.9.2. Личные дела, содержащие персональные данные работников администрации города Урай, должны вестись в соответствии с требованиями действующего законодательства. Личные дела хранятся в специально отведенной секции шкафа (сейфа), обеспечивающего защиту от несанкционированного доступа.

3.9.3. Обязанности по хранению личных дел работников администрации города Урай, заполнению, хранению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, содержащих персональные данные работников администрации города Урай, возлагаются на работников службы обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай, распределяются и закрепляются в должностных инструкциях.

3.9.4. Органы администрации города Урай, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа, от копирования в порядке, установленном настоящим Положением, и обеспечивают раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.9.5. Все съемные носители (жесткие диски, flash-накопители, CD-диски, дискеты), необходимые для работы с персональными данными, учитываются в журнале учета машинных носителей персональных данных. На съемные машинные носители должны быть нанесены учетные реквизиты, отражаемые в журнале учета.

3.10. Уничтожение персональных данных.

3.10.1. Персональные данные субъектов подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в их достижении.

3.10.2. Уничтожение или обезличивание части персональных данных, производится способом, исключающим дальнейшую обработку этих персональных данных.

3.10.3. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию.

3.10.4. Уничтожение информации на съемных носителях осуществляется методом стирания (форматирования) носителя или иными методами, гарантирующими полное уничтожение конфиденциальной информации, без возможности ее восстановления. Факт уничтожения оформляется актом об уничтожении персональных данных субъектов персональных данных и отражается в журнале учета машинных носителей.

3.11. Передача персональных данных.

3.11.1. Передача персональных данных осуществляется с учетом требований, установленных статьей 88 Трудового кодекса Российской Федерации.

3.11.2. Внутри администрации города Урай без письменного согласия субъекта персональных данных разрешается передача персональных данных в органы администрации города Урай, общественные организации и комиссии, созданные для защиты прав работников и предоставления им установленных условий труда, гарантий и компенсаций в соответствии с

законодательством, необходимые им для выполнения своих функций.

3.11.3. Персональные данные передаются представителям субъектов персональных данных в порядке, установленном законодательством, и ограничиваются данными, необходимыми для выполнения указанными представителями их функций.

3.11.4. Работники администрации города Урай, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.11.5. Передача персональных данных субъектов по общедоступным каналам связи и/или по сетям международного информационного обмена разрешается только при использовании средств криптографической защиты информации.

3.11.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных по форме, установленной приложением 3 к Положению.

4. Доступ в помещения, в которых ведется обработка персональных данных

4.1. Доступ в помещения осуществляется согласно Инструкции о пропускном и внутриобъектовых режимах в здании администрации города Урай, утвержденной распоряжением администрации города Урай от 14.03.2013 №133-р.

4.2. Помещения, в которых ведется обработка персональных данных, оборудуются техническими средствами охранной и пожарной сигнализации, замками, с целью обеспечить их сохранность, исключать возможность бесконтрольного проникновения в них посторонних лиц.

4.3. Ключи от помещений сдаются ответственными работниками под охрану, с отметкой в журнале приема-сдачи служебных помещений. В течение рабочего дня ключи от шкафов (ящиков, хранилищ), в которых содержатся персональные данные, а также помещений, где находятся средства вычислительной техники, предназначенные для обработки персональных данных, находятся на хранении у ответственных сотрудников.

5. Защита персональных данных

5.1. Работники администрации города Урай обеспечивают конфиденциальность персональных данных.

5.2. Защита персональных данных осуществляется выполнением комплекса организационных, технических мер, определенных в муниципальных правовых актах.

5.3. Организация защиты персональных данных в локальной вычислительной сети администрации города Урай осуществляется в рамках действующих в администрации города Урай порядков и инструкций по защите информации.

6. Обязанности лиц, допущенных к обработке персональных данных

6.1. Каждый работник, принимаемый на работу в администрацию города Урай, должен быть ознакомлен под роспись с обязательством о неразглашении персональных данных, ставших ему известными в ходе выполнения своих служебных обязанностей по форме, установленной приложением 4 к Положению.

6.2. Работники администрации города Урай, допущенные к обработке персональных данных, обязаны:

1) знать и выполнять требования настоящего Положения;

2) не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законодательством и другими нормативными документами;

3) знакомиться только с теми персональными данными, к которым получен доступ;

4) хранить в тайне известные им сведения о персональных данных, информировать своего непосредственного начальника о фактах нарушения порядка обработки персональных данных и о попытках несанкционированного доступа к ним;

5) предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;

6) выполнять требования по защите полученных персональных данных субъекта;

7) соблюдать правила пользования документами, содержащими персональные данные, порядок их обработки и защиты;

8) соблюдать инструкции, положения, касающиеся вопроса безопасности персональных данных, обрабатываемых в ИСПДн.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

7.1. Работники администрации города Урай, которым сведения о персональных данных стали известны в силу их служебного положения, несут ответственность за их разглашение.

7.2. Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними вышеуказанных лиц.

7.3. Работники администрации города Урай, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

8. Контроль за выполнением требований настоящего Положения

8.1. Постоянный контроль за соблюдением требований в части обработки и защиты персональных данных осуществляют руководители органов администрации города Урай.

8.2. Контроль за выполнением требований по защите персональных данных, обрабатываемых в информационных системах администрации города Урай, осуществляет администратор информационной безопасности.

Приложение 1 к Положению о порядке обработки персональных данных в администрации города Урай

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество)

_____ серия _____ № _____, выдан

_____

_____,
наименование и реквизиты документа, удостоверяющего личность: серия, номер, дата выдачи

_____,
наименование органа и код подразделения органа (при его наличии), выдавшего документ

зарегистрированный(ая) по месту жительства по адресу:

_____,

проживающий(ая) по адресу:

_____,

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам администрации города Урай (далее- Оператор), расположенной по адресу: *Тюменская область, Ханты-Мансийский автономный округ-Югра, г.Урай, мкр.2, дом 60*, на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор (получение), запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

1) фамилия, имя, отчество (в том числе прежние фамилии, имена и (или) отчества (при их наличии) в случае их изменения, сведения о том, когда, где и по какой причине они изменялись);

2) личная фотография;

3) дата рождения (число, месяц и год рождения);

4) место рождения;

5) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при его наличии), выдавшего его, дата выдачи;

6) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, по которому граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию, наименование органа и код подразделения органа (при его наличии), выдавшего его, дата выдачи;

7) сведения о гражданстве: об имеющемся гражданстве (гражданствах); об имевшихся ранее (прежних) гражданствах;

8) адрес места жительства (места пребывания);

9) адрес и дата регистрации по месту жительства (места пребывания);

10) адреса прежних мест жительства;

11) сведения о семейном положении, о составе семьи, в том числе о гражданах, находящихся (находившихся) на иждивении, о родителях (усыновителях), детях, включая

усыновленных (удочеренных), братьях, сестрах и других близких родственниках, о супруге (бывшем или бывшей супруге), детях, включая усыновленных (удочеренных), братьях и сестрах (дата рождения, место рождения, места работы (службы), домашний адрес);

12) реквизиты свидетельств государственной регистрации актов гражданского состояния и содержащиеся в них сведения;

13) сведения об образовании, в том числе о послевузовском профессиональном образовании (когда, какие образовательные и (или) иные организации окончил, наименование указанных организаций, реквизиты документов об образовании, направление подготовки, квалификация и специальность по документам об образовании);

14) сведения о дополнительном профессиональном образовании: профессиональной переподготовке и (или) повышении квалификации (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке или о повышении квалификации, квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения);

15) сведения об ученой степени, ученом звании;

16) сведения о владении государственным языком, иностранными языками и языками народов Российской Федерации, уровне владения;

17) сведения из заключения (справок) медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на муниципальную службу (работу) и ее прохождению, а для граждан, привлекаемых к муниципальной службе (работе) в районы Крайнего Севера и приравненные к ним местности, - об отсутствии противопоказаний для муниципальной службы (работы) и проживания в данных районах и местностях;

18) сведения о трудовой деятельности до поступления на муниципальной службу (работу) в администрацию города Урай, в том числе сведения, содержащиеся в трудовой книжке (трудовых книжках) и вкладыше к трудовой книжке (вкладышах к трудовым книжкам), в том числе о прежних местах службы (работы, обучения), периодах службы (работы, обучения);

19) сведения о поступлении, прохождении и увольнении со службы (работы), завершении (прекращении) обучения, в том числе сведения о дате, основании поступления на муниципальную службу (работу), о дате, основании назначения на должность, перевода, перемещения на иную должность, о наименовании замещаемой (занимаемой) должности, номере личного дела, о календарной и льготной выслуге лет, о районных коэффициентах в целях определения надбавок при оплате труда и назначении пенсий, об общем трудовом стаже и общей выслуге лет, о периодах обучения, о денежном содержании муниципальных служащих, о заработной плате работников, руководителей муниципальных организаций, об изменениях размера денежного содержания (заработной платы), ежемесячных доплатах, о денежных удержаниях, о датах и основаниях прекращения выплат, о предоставленных государственных гарантиях (льготах, компенсациях, пособиях, в том числе о льготных пенсиях, назначенных с учетом общего трудового стажа и общей выслуги лет), об участии в обеспечении режима чрезвычайного положения, правового режима контртеррористической операции, в ликвидации чрезвычайных ситуаций, о дате и причине увольнения, а также завершения (прекращения) обучения, содержащиеся в распоряжении (приказе) об увольнении (о номере, дате издания, основании увольнения, в том числе в связи с достижением предельного возраста пребывания на муниципальной службе или работе);

20) сведения, содержащиеся в трудовом договоре (контракте), дополнительных соглашениях к трудовому договору (контракту);

21) сведения о замещаемой (занимаемой) должности, ранее замещаемой (занимаемой) должности, об имеющемся (ранее имевшемся) специальном звании, воинском звании, классном чине, дипломатическом ранге, о наличии специальных знаний, об имеющейся (имевшейся) квалификации, в том числе о квалификационном разряде федерального государственного гражданского (муниципального) служащего, квалификационном классе военнослужащего, квалификационном разряде рабочего, виде выполняемой работы;

22) сведения о форме, номере и дате оформления допуска к государственной тайне, ранее имевшемся и (или) имеющемся, в том числе, оформленном за период службы или работы,

а также к иным конфиденциальным сведениям;

23) сведения о государственных наградах, иных наградах и знаках отличия (в том числе кем и когда награжден), о применении иных видов поощрений, привлечении к дисциплинарной и (или) иным видам юридической ответственности;

24) реквизиты страхового свидетельства обязательного пенсионного страхования, содержащиеся в нем сведения;

25) страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

26) реквизиты удостоверений (документов), подтверждающих имеющиеся государственные и иные льготы (гарантии, компенсации, пособия), содержащиеся в них сведения;

27) идентификационный номер налогоплательщика;

28) реквизиты страхового медицинского полиса обязательного медицинского страхования, содержащиеся в нем сведения;

29) сведения о воинском учете, реквизиты документов воинского учета, а также сведения, содержащиеся в документах воинского учета;

30) сведения о наличии либо отсутствии судимости, в том числе у лиц, состоящих с субъектом персональных данных в родстве или свойстве;

31) сведения о пребывании за границей (когда, где и с какой целью);

32) сведения о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках без сохранения денежного содержания;

33) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также сведения о доходах, расходах, об имуществе и обязательствах имущественного характера своих супруга (супруги) и несовершеннолетних детей;

34) сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых муниципальным служащим, гражданином Российской Федерации, претендующим на замещение должности муниципальной службы, размещались общедоступная информация, а также данные, позволяющие его идентифицировать.

35) номера контактных телефонов (домашнего, служебного, мобильного), сведения об иных способах связи с субъектом персональных данных, в том числе сведения об адресе электронной почты в информационно-телекоммуникационной сети «Интернет»;

36) сведения о состоянии здоровья, о травматизме (болезнях), инвалидности, полученных в период прохождения муниципальной службы (осуществления работы) или обучения, в том числе о группе инвалидности, степени инвалидности, о причине наступления болезни или инвалидности, о сроке действия установленной инвалидности, о назначенных (выплаченных) страховых и компенсационных выплатах, о прохождении диспансеризации;

37) сведения о близких родственниках (родителях, братьях, сестрах, детях), а также супругах, в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество (при его наличии), с какого времени проживают за границей);

38) сведения о назначенной (получаемой, ранее назначенной) пенсии муниципальному служащему (работнику, руководителю муниципального учреждения, субъекту), в том числе о дате назначения пенсии, виде назначенной пенсии, наименовании организации, назначившей пенсию, сроках назначения пенсии, номере пенсионного удостоверения, номере пенсионного дела, о последнем месте прохождения муниципальной службы (работы), дате и причине прекращения (приостановления) выплаты пенсии;

39) наименования банков и (или) кредитных организаций, с которыми субъект персональных данных состоит в правоотношениях;

40) номер банковского расчетного счета;

41) номер банковской карты.

42) иные сведения, которые я пожелал(а) сообщить о себе.

Цели обработки персональных данных:

- для обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением и прохождением муниципальной службы, исполнения трудового договора, с правом передачи персональных данных третьим лицам и (или) направления запросов третьим лицам о предоставлении персональных данных в установленном порядке и составе, а также получения от указанных лиц результатов такой обработки либо запрошенных персональных данных;

- для ведения финансово-хозяйственной деятельности Оператора;

- иное (указать) _____

_____

Разрешаю поручать обработку третьим лицам на основании заключаемого с этими лицом договора (муниципального контракта), либо путем принятия Оператором соответствующего акта (далее - поручение оператора) в соответствии со статьей 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

Разрешаю размещать сведения, предусмотренные законодательством Российской Федерации, на официальном сайте органов местного самоуправления города Урай в информационно-телекоммуникационной сети «Интернет».

Мне разъяснены мои права и обязанности в части обработки персональных данных, в том числе право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку ответственному сотруднику Оператора, и обязанность проинформировать Оператора в случае изменения моих персональных данных.

Срок действия данного согласия устанавливается на период: с момента подписания бессрочно.

Данные об Операторе:
Наименование: *администрация города Урай*
Адрес оператора: *628285, Тюменская область, Ханты-Мансийский автономный округ-Югра, г.Урай, мкр.2, дом 60*
Субъект персональных данных:

«____»_____ _____г. _____ _____

(подпись) *(фамилия, имя, отчество)*

Приложение 2 к Положению о порядке обработки персональных данных в администрации города Урай

Форма разъяснения
субъекту персональных данных

Мне, _____,
разъяснены юридические последствия отказа предоставить свои персональные данные в администрацию города Урай.

В соответствии со статьями 65,86 Трудового кодекса Российской Федерации, статьями 16, 29 Федерального закона от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации» определен перечень персональных данных, которые субъект персональных данных обязан предоставить в администрацию города Урай при поступлении на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	расшифровка

Приложение 3 к Положению о порядке обработки персональных данных в администрации города Урай

Согласие на обработку персональных данных,
разрешенных субъектом персональных данных для распространения

«___»_____20___.

Я, _____,

проживающий(ая) по адресу: _____,

_____,

контактный телефон _____,

адрес электронной почты (при наличии) _____,

именуемый в дальнейшем «Субъект персональных данных», в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» даю согласие администрации города Урай, далее «Оператор», на обработку моих персональных данных.

Цель обработки: размещение персональных данных на официальном сайте органов местного самоуправления города Урай в информационно-телекоммуникационной сети «Интернет» **(http://www.uray.ru)**.

Состав персональных данных:

- фамилия, имя, отчество;
- контактная информация;
- фото;
- дата и место рождения;
- биографические сведения;
- сведения об образовании (образовательное учреждение, время обучения, присвоенная квалификация);
- сведения о местах работы (город, название организации, должность, сроки работы);
- награды.

Мне разъяснены мои права и обязанности в части обработки персональных данных, в том числе право отозвать свое согласие и обязанность проинформировать Оператора в случае изменения моих персональных данных.

Срок действия данного согласия с момента подписания до «____»_____ 20_____г.

Данные об операторе персональных данных:

Наименование организации: администрация города Урай.

Адрес оператора: 628285, Ханты-Мансийский автономный округ - Югра, Урай, мкр.2, дом 60.

Субъект персональных данных:

«____»_____ _____г. _____ _____

(подпись) (фамилия, имя, отчество)

Приложение 4 к Положению о порядке обработки персональных данных в администрации города Урай

Обязательство о неразглашении персональных данных

Я,_____
_____,
(фамилия, имя, отчество, должность)

в период трудовых отношений с администрацией города Урай и после их окончания обязуюсь:

Хранить в тайне сведения о персональных данных субъектов, отнесенные к сведениям конфиденциального характера, ставшие мне известными при выполнении служебных обязанностей или иным путем.

Не сообщать персональные данные работников администрации город Урай третьей стороне без письменного согласия работников администрации города Урай, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью работников администрации города Урай, а также в случаях, установленных федеральными законами.

Знакомиться только с теми сведениями и документами, содержащими сведения о персональных данных субъектов, к которым я получил доступ в силу служебных обязанностей, знать, какие конкретные сведения подлежат защите, а также строго соблюдать правила пользования ими.

Об утрате или недостаче документов, содержащих сведения о персональных данных, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, металлических шкафов, личных печатей, а также о причинах и условиях возможной утечки таких сведений немедленно сообщить непосредственному руководителю органа администрации города Урай.

При увольнении, перед уходом в отпуск, отъездом в длительную командировку (более 1 месяца) сдать лицу, ответственному за учет и хранение, все материальные носители сведений конфиденциального характера, которые находились в распоряжении работника в связи с выполнением им служебных обязанностей.

В случае попытки посторонних лиц или организаций, получить информацию, содержащую сведения о персональных данных субъектов, сообщить об этом непосредственному руководителю органа администрации города Урай.

До моего сведения доведены с разъяснениями соответствующие положения законодательства Российской Федерации о требованиях к обработке (получение, хранение, комбинирование, передача и иное использование), обеспечению сохранности персональных данных субъектов.

Мне известно, что нарушение этих положений может повлечь уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством Российской Федерации.

_____	_____	_____
(должность)	(подпись)	(расшифровка подписи)

Экземпляр обязательств о неразглашении персональных данных получил(а):

_____	_____	_____
(должность)	(подпись)	(расшифровка подписи)

Приложение 2 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Правила
рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила)

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, предусмотренной частью 7 статьи 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и статьей 89 Трудового кодекса Российской Федерации (далее - сведения), в администрации города Урай (далее – оператор).

2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Запрос субъекта персональных данных регистрируется в журнале учета запросов.

Журнал учета запросов ведется в каждом органе администрации города Урай, допущенном к обработке персональных данных.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также

уполномоченного органа по защите прав субъектов персональных данных:

1) оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя;

2) в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;

3) оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

4) оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 3 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Правила
осуществления внутреннего контроля соответствия обработки персональных данных в администрации города Урай требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в администрации города Урай требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных организовывается проведение периодических проверок.

3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с управлением по информационным технологиям и связи администрации города Урай, ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.

4. Плановые проверки проводятся не чаще чем один раз в год.

5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

6. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

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

2) соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

3) достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

4) отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

5) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

6) порядок и условия применения средств защиты информации;

7) соблюдение правил доступа к персональным данным;

8) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

7. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

1) запрашивать у работников информацию, необходимую для реализации своих полномочий;

2) требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных

данных, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

5) вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

8. Результаты внутреннего контроля оформляются в виде акта. При выявлении в ходе внутреннего контроля нарушений в акте отражается перечень мероприятий по устранению выявленных нарушений и сроки их устранения.

9. Проверку работоспособности программного обеспечения, средств защиты информации, установленных на рабочих местах пользователей, настройку прав доступа пользователей, проведение работ по анализу защищенности информационных систем обработки персональных данных проводит администратор информационной безопасности в соответствии с инструкцией администратора информационной безопасности.

Приложение 4 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Правила
работы с обезличенными данными в случае обезличивания персональных данных

1. Общие положения

1.1. Настоящие Правила работы с обезличенными данными в случае обезличивания персональных данных (далее – Правила) разработаны с учетом Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными администрации города Урай.

1.2. Понятия, используемые в Правилах, используются в значениях, установленных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

2. Условия обезличивания персональных данных

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации города Урай и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Способы обезличивания персональных данных при условии дальнейшей обработки персональных данных:

1) уменьшение перечня обрабатываемых сведений;
2) замена части сведений идентификаторами;
3) обобщение – понижение точности некоторых сведений;
4) понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт);
5) деление сведений на части и обработка в разных информационных системах;
6) другие способы.

2.3. Способом обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3. Порядок работы с обезличенными персональными данными

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

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

3.4. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение установленных в администрации города Урай правил и инструкций по защите информации.

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

1) правил хранения бумажных носителей;
2) правил доступа к персональным данным и в помещения, где они хранятся.

Приложение 5 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Перечень информационных систем персональных данных

Наименование	Адрес расположения
МИСПДн МАИС «ЗАГС»	г.Урай, ул.Ленина, 60, каб. 302
ИСПДН «1С:Зарплата и Кадры.Доходы.Казна»	г.Урай, микрорайон Западный, 16
МИСПДн АИС «Опека»	г.Урай, ул.Ленина, 60, каб. 302
МИСПДн «Мониторинг»	г.Урай, ул.Ленина, 60, каб. 302; микрорайон Западный, 19, корп.4
ИСПДн «Административная комиссия»	г.Урай, микрорайон 2, дом 60, каб.106
МИСПДн АИС «АИСТ»	г.Урай, микрорайон 3, дом 7, каб. 14

».

Приложение 6 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Должность	Название ИСПДн/МИСПДн
1	Начальник договорного отдела по оформлению прав на муниципальные земли комитета по управлению муниципальным имуществом администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна», «Мониторинг»
2	Главный специалист договорного отдела по оформлению прав на муниципальные земли комитета по управлению муниципальным имуществом администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна», «Мониторинг»
3	Ведущий специалист договорного отдела по оформлению прав на муниципальные земли комитета по управлению муниципальным имуществом администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна», «Мониторинг»
4	Консультант отдела по информационным ресурсам управления по информационным технологиям и связи администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна», «Мониторинг»,МАИС «ЗАГС»
5	Эксперт отдела по информационным ресурсам управления по информационным технологиям и связи администрации города Урай	МАИС «ЗАГС», АИС «Опека»
6	Начальник службы обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна»
7	Ведущий специалист службы обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна»
8	Начальник отдела опеки и попечительства администрации города Урай	АИС «Опека»
9	Заместитель начальника отдела опеки и попечительства администрации города Урай	АИС «Опека»
10	Главный специалист отдела опеки и попечительства администрации города Урай	АИС «Опека» АИС «АИСТ»
11	Начальник отдела записи актов гражданского состояния администрации города Урай	МАИС «ЗАГС»
12	Ведущий специалист отдела записи актов гражданского состояния администрации города Урай	МАИС «ЗАГС»
13	Главный специалист отдела записи актов гражданского состояния	МАИС «ЗАГС»

	администрации города Урай	
14	Начальник отдела национальной политики и общественной безопасности управления внутренней политики администрации города Урай	АИС «Административная комиссия»

Приложение 7 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

№ п/п	Должность	Название ИСПДн/МИСПДн
1	Начальник договорного отдела по оформлению прав на муниципальные земли комитета по управлению муниципальным имуществом администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна», «Мониторинг»
2	Консультант отдела по информационным ресурсам управления по информационным технологиям и связи администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна», «Мониторинг»,
3	Эксперт отдела по информационным ресурсам управления по информационным технологиям и связи администрации города Урай	МАИС «ЗАГС», АИС «Опека»
4	Начальник службы обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна»
5	Ведущий специалист службы обеспечения кадровой работы и противодействия коррупции управления по развитию местного самоуправления администрации города Урай	«1С:Зарплата и кадры. Доходы.Казна»
6	Начальник отдела опеки и попечительства администрации города Урай	АИС «Опека»
7	Начальник отдела записи актов гражданского состояния администрации города Урай	МАИС «ЗАГС»
8	Начальник отдела национальной политики и общественной безопасности управления внутренней политики администрации города Урай	АИС «Административная комиссия»
9	Главный специалист отдела опеки и попечительства администрации города Урай	АИС «АИСТ»

Приложение 8 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Перечень персональных данных, обрабатываемых в администрации города Урай

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Основание для обработки персональных данных
Обработка персональных данных в МИСПДн МАИС «ЗАГС»			
Общие сведения о гражданах	Фамилия, имя, отчество, Дата и место рождения, Гражданство, Национальность, Адрес проживания, Семейное положение, Образование, Паспортные данные, Данные СНИЛС, Сведения о количестве детей, Сведения о заключении/расторжении брака.	Исполнение государственных полномочий по государственной регистрации актов гражданского состояния: государственная регистрация рождения, заключения брака, расторжения брака, установления отцовства, усыновления (удочерения), перемены имени, смерти.	Федеральный закон от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния»
Обработка персональных данных в ИСПДн «1С:Зарплата и кадры. Доходы.Казна»			
Общие сведения о работниках	Фамилия, имя, отчество, Паспортные данные, Дата и место рождения, Адрес проживания, Семейное положение, Образование, Профессия, Данные ИНН, Данные Пенсионного страхового свидетельства, Данные медицинских полисов, Сведения о рождении детей, о заключении/расторжении брака, Данные о воинском учете, Место работы, Должность, Телефоны домашний и сотовый, Сведения о трудовой деятельности, Идентификационные данные пластиковых карт сотрудников.	Реализация кадровой политики и бухгалтерской политики, оформление налоговых вычетов и других льгот, предоставление сведений о доходах муниципальных служащих.	Статьи 86-90 Трудового кодекса Российской Федерации
Сведения о родственниках работника	Фамилия, имя, отчество, дата рождения, степень родства, сведения об имуществе, сведения о доходах	Реализация кадровой и бухгалтерской политики, оформление налоговых вычетов и других льгот, предоставление сведений о доходах	Федеральный закон от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации»

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Основание для обработки персональных данных
		муниципальных служащих.	
Сведения об участниках имущественных сделок	Фамилия, имя, отчество, Паспортные данные, Дата и место рождения, Адрес регистрации/проживания, Семейное положение, Данные ИНН, Сведения о рождении детей, Сведения о заключении/расторжении брака, Телефоны домашний и сотовый.	Учет движения денежных средств по договорам сделок с имущественными объектами, находящимися в собственности администрации города Урай.	Федеральный закон от 06.10.2003 №131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Устав города Урай
Обработка персональных данных в МИСПДн АИС «Опека»			
Общие сведения о гражданах	Фамилия, имя, отчество, Паспортные данные, Дата и место рождения, Адрес проживания, Семейное положение, Степень родства, Сведения о доходах, Сведения о рождении детей, о заключении/расторжении брака, Место работы, Должность, Телефоны домашний и сотовый, Сведения о совершенных правонарушениях несовершеннолетних и родителях, Сведения о проводимых индивидуальной профилактической работе, Сведения об имуществе, Сведения о доходах, степень родства.	Обеспечение учета и контроля над лицами, нуждающимися в установлении над ними опеки или попечительства, и их устройства, защита прав и законных интересов подопечных, обеспечение исполнения опекунами, попечителями и органами опеки и попечительства возложенных на них полномочий.	Федеральный закон от 24.04.2008 №48-ФЗ «Об опеке и попечительстве»
Обработка персональных данных в МИСПДн «Мониторинг»			
Общие сведения о гражданах	Фамилия, имя, отчество, паспортные данные, адрес проживания, телефон, сведения об имуществе	Обработка сделок с имущественными объектами, находящимися в собственности администрации города Урай.	Федеральный закон от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг»
Обработка персональных данных в ИСПДн АИС «Административная комиссия»			
Общие сведения о гражданах	Фамилия, имя, отчество, Паспортные данные, Дата и место рождения, Адрес проживания, Семейное положение, Степень родства, Сведения о доходах, Сведения о рождении детей, о заключении/расторжении брака, Место работы, Должность, Телефоны домашний и сотовый, Сведения о совершенных правонарушениях	Оформления постановлений о привлечении к административной ответственности и иной документации.	Кодекс Российской Федерации об административных правонарушениях; Закон Ханты-Мансийского автономного округа - Югры от 11.06.2010 № 102-оз «Об

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Основание для обработки персональных данных
	несовершеннолетних и родителях, Сведения о проводимой индивидуальной профилактической работе, Сведения об имуществе, Сведения о доходах, степень родства.		административных правонарушениях»
Обработка персональных данных в МИСПДн АИС «АИСТ»			
Общие сведения о гражданах	Сведения о детях: ФИО, дата и место рождения, информация о здоровье, информация о родителях, фотографии, особые приметы, особенности характера, информация о родственниках, внешность (рост, вес, цвет глаз и волос), пол, паспорт, свидетельство о рождении, СНИЛС, адрес регистрации и адрес проживания, гражданство. Граждане: ФИО, дата и место рождения, паспорт, семейное положение, гражданство, адрес и место проживания, номер и дата выдачи заключения, пожелания о ребенке.	Обеспечения оперативной актуализации сведений о детях, оставшихся без попечения родителей; Оказание содействия в устройстве детей, оставшихся без попечения родителей, на воспитание в семьи граждан Российской Федерации, постоянно проживающих на территории Российской Федерации; Создание условий для реализации права граждан, желающих принять детей на воспитание в свои семьи, на получение полной и достоверной информации о детях, оставшихся без попечения родителей; Осуществление учета граждан, желающих принять детей на воспитание в свои семьи.	Приказ Министерства просвещения Российской Федерации от 15.06.2020 №300 «Об утверждении Порядка формирования, ведения и использования государственного банка данных о детях, оставшихся без попечения родителей»

Приложение 9 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Инструкция администратора информационной безопасности администрации города Урай

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

1) Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

3) постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) приказа Федеральной службы по техническому и экспортному контролю 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»;

5) приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность администратора информационной безопасности администрации города Урай по обеспечению безопасности персональных данных и другой защищаемой информации, обрабатываемой во всех подлежащих в соответствии с требованиями законодательства защите информационных системах администрации города Урай (далее – Учреждения).

1.3. Администратор информационной безопасности администрации города Урай (далее – Администратор) назначается распоряжением администрации города Урай и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники Учреждения, в пределах своей зоны ответственности.

1.4. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, а также нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями информационных систем (далее – ИС).

1.5. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Обязанности Администратора

2.1. Знать нормативно-методические документы в области безопасности информации и организационно-распорядительные документы Учреждения в части его касающейся.

2.2. Знать перечень обрабатываемых в Учреждении персональных данных и другой защищаемой информации, состава, структуры, назначения и выполняемых задач ИС, а также состава информационных технологий и основных технических средств и систем (далее - ОТСС), позволяющих осуществлять обработку персональных данных и другой защищаемой информации.

2.3. Требовать от пользователей ИС и выполнять самому:

1) действующие в Учреждении порядки и инструкции по информационной безопасности;

2) Инструкцию по делопроизводству в администрации города Урай, утвержденную распоряжением администрации города Урай от 15.04.2019 №180-р;

3) инструкцию о пропускном и внутриобъектовом режимах в здании администрации города Урай, утвержденную распоряжением администрации города Урай от 14.03.2013№ 133-р;

4) распоряжения администрации города Урай по вопросам обработки персональных данных и другие организационно-распорядительные документы Учреждения в части обеспечения безопасности информации.

2.4. Контролировать соответствие ОТСС ИС техническим паспортам на ИС.

2.5. Поддерживать в актуальном состоянии организационно-распорядительные документы Учреждения (Разрешительная система доступа к ИС, Технический паспорт на ИС и иные документы), регламентирующие обработку защищаемой информации в ИС.

2.6. Выполнять работы по управлению (заведение, активация, блокирование, уничтожение) локальными учетными записями пользователей ИС:

1) назначение прав доступа пользователей к объектам доступа ИС в соответствии с задачами, решаемыми пользователями в ИС и взаимодействующими с ней ИС и Разрешительной системой доступа к ИС;

2) назначение минимально необходимых прав и привилегий пользователям и иным лицам, имеющим доступ к ИС;

3) еженедельная проверка отсутствия в ИС учетных записей уволенных (отстраненных) сотрудников;

4) своевременное удаление временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС.

2.7. Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС и контроль за действиями пользователей при работе с паролями в соответствии с Порядком использования паролей.

2.8. Контролировать неизменности настроек средств защиты информации:

1) средства защиты информации должны ограничивать доступ к ИС на 10 минут при 3 неудачных попытках входа в ИС;

2) настройки средств защиты информации должны препятствовать доступу к ИС до прохождения процедур аутентификации и идентификации;

3) средства защиты информации должны обеспечивать запрет удаленного доступа к ИС;

4) препятствие передаче защищаемой информации через сеть Интернет (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи;

5) средства доверенной загрузки должны обеспечивать:

а) блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

б) контроль доступа пользователей к процессу загрузки операционной системы;

в) контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

2.9. Контролировать запрет использования в ИС технологий беспроводного доступа и мобильных технических средств.

2.10. Контролировать отсутствие доступа к ИС со стороны пользователей информационных систем сторонних организаций.

2.11. Контролировать установки на автоматизированные рабочие места (далее - АРМ) ИС программного обеспечения (далее - ПО), отсутствующего в разрабатываемом и утверждаемом для каждой ИС перечне программного обеспечения, разрешенного к установке в ИС.

2.12. Вести учет машинных носителей защищаемой информации в соответствующем журнале по утвержденной форме.

2.13. Обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ ИС при их передаче в сторонние организации для ремонта или утилизации, либо контроль процесса уничтожения (стирания). Уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

2.14. Контролировать регистрацию в ИС следующих событий безопасности:

1) входа (выхода), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы:

а) дата (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

2) подключения машинных носителей информации и вывода информации на носители информации:

а) дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

3) запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации:

а) дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

4) попыток доступа программных средств к защищаемым объектам доступа:

а) дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип).

5) попыток удаленного доступа:

а) дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИС.

2.15. Контролировать порядок учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.16. Проводить инструктаж пользователей по правилам работы с используемыми техническими средствами и средствами защиты информации (далее – СЗИ) в соответствии с технической документацией на используемые СЗИ.

2.17. Осуществлять учет СЗИ, хранение дистрибутивов СЗИ, производство при необходимости восстановления программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИС.

2.18. Периодически (не реже 1 раза в месяц) обновлять базы признаков уязвимостей, проводить мероприятия по выявлению, анализу уязвимостей ИС, оперативно проводить работы по устранению выявленных уязвимостей. В случае невозможности устранения выявленных уязвимостей путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки СЗИ, изменение режима и порядка использования ИС), направленные на устранение возможности использования выявленных уязвимостей.

2.19. Выявлять и инициировать разбирательство инцидентов информационной безопасности в Учреждении в соответствии с Порядком управления инцидентами информационной безопасности.

2.20. Проводить мероприятия по организации антивирусной защиты в соответствии с Порядком организации антивирусной защиты.

2.21. Проводить мероприятия по организации резервного копирования информации в соответствии с Инструкцией по организации резервного копирования (восстановления) данных, обрабатываемых в ИС.

2.22. Контролировать отсутствие в составе ПО АРМ, входящих в ИС, средств разработки и отладки программ.

2.23. Реагировать на поступление в ИС спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

2.24. Знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией.

2.25. Поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом

система должна реализовывать в совокупности на каждой АРМ ИС функции, необходимые для выполнения требований по защите от НСД для ИС.

2.26. Контролировать срок действия сертификатов соответствия на СЗИ и обеспечить их продление в соответствии с порядком продления.

2.27. Выполнять контроль (мониторинг) за обеспечением уровня защищенности информации, обрабатываемой в ИС, а именно:

1) контроль за событиями безопасности и действиями пользователей в ИС;

2) анализ и оценка функционирования системы защиты информации ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС;

3) периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

4) документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

5) принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС, повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

3. Права и ответственность Администратора

3.1. Администратор имеет право:

1) получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и АРМ пользователей;

2) требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

3) участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

4) осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;

5) производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением пользователей ИСПДн;

6) вносить свои предложения по совершенствованию мер защиты в ИС.

3.2. Администратору запрещается:

1) используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;

2) использовать ставшие доступными в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий;

3) использовать в своих и в чьих-либо личных интересах ресурсы ИС, предоставлять такую возможность другим;

4) выключать СЗИ без письменной санкции руководства;

5) передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки;

6) производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИС, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей;

7) нарушать правила эксплуатации оборудования ИС и СЗИ.

8) корректировать, удалять, подменять журналы аудита.

3.3. Администратор несет ответственность по действующему законодательству за ненадлежащее выполнение возложенных функций по обеспечению безопасности персональных данных и другой защищаемой информации при ее обработке в ИС Учреждения в соответствии с положениями законодательства Российской Федерации в области защиты информации

Приложение 10 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Инструкция пользователя информационной системы персональных данных (далее – инструкция)

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

1) Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

2) постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3) приказа Федеральной службы по техническому и экспортному контролю 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»;

4) приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Настоящая инструкция определяет общие обязанности, права и ответственность пользователя информационной системы персональных данных (далее – ИСПДн) администрации города Урай (далее - Учреждение) по обеспечению информационной безопасности при работе со сведениями конфиденциального характера.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Обязанности пользователя

2.1. При выполнении работ в ИСПДн Пользователь обязан:

1) знать и соблюдать:

а) порядки и инструкции по информационной безопасности, утвержденные постановлением администрации города Урай;

б) инструкцию по делопроизводству в администрации города Урай, утвержденную распоряжением администрации города Урай от 15.04.2019 №180-р;

в) инструкцию о пропускном и внутриобъектовом режимах в здании администрации города Урай, утвержденную распоряжением администрации города Урай от 14.03.2013 №133-р;

г) порядок обработки персональных данных в администрации города Урай, утвержденный настоящим распоряжением;

д) документы, утвержденные распоряжением администрации города Урай об обработке персональных данных, и другие организационно-распорядительные документы Учреждения в части обеспечения безопасности информации.

2) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн, правила работы и порядок регистрации в ИСПДн, доступа к информационным ресурсам ИСПДн;

3) знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);

4) хранить в тайне свои идентификационные данные (имена, пароли и т.д.);

5) осуществлять вход в ИСПДн только под своими идентификационными данными;

6) передавать для хранения установленным порядком свое индивидуальное устройство идентификации и другие реквизиты разграничения доступа, только своему непосредственному руководителю или администратору безопасности ИСПДн (ответственному за информационную безопасность подразделения);

7) немедленно вызывать администратора безопасности ИСПДн и поставить в известность непосредственного руководителя в случае утери индивидуального устройства идентификации или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенному АРМ;

8) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ ставить в известность администратора безопасности ИСПДн при необходимости внесения изменения в состав аппаратных и программных средств АРМ;

9) экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

10) соблюдать установленный режим разграничения доступа к информационным ресурсам;

11) немедленно выполнять предписания администраторов безопасности ИСПДн, предоставлять свое АРМ администратору безопасности для контроля;

12) ставить в известность администраторов ИСПДн в случае появления сведений или подозрений о фактах НСД к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.);

13) при работе в ИСПДн использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности;

14) осуществлять установленным порядком (сочетанием клавиш Shift+Del), уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;

15) уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;

16) сообщать непосредственному руководителю обо всех проблемах, связанных с эксплуатацией ИСПДн.

2.2. Пользователю категорически запрещается:

1) использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

2) самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИСПДн (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные паспортом АРМ;

3) осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;

4) записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.), в том числе для временного хранения;

5) оставлять включенное без присмотра свое АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);

6) передавать кому-либо свое индивидуальное устройство идентификации в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;

7) оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);

8) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИСПДн (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность администратора безопасности ИСПДн и руководителя своего подразделения;

9) подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;

10) осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;

11) фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;

12) разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;

13) вносить изменения в файлы, принадлежащие другим пользователям;

14) осуществлять передачу защищаемой информации по незащищаемым каналам сетей связи общего пользования;

15) отключать (блокировать) средства защиты информации;

16) осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;

17) производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) АРМ и серверов;

18) закрывать доступ к информации паролями без согласования с администратором информационной безопасности;

19) использовать для доступа к ИСПДн технологии беспроводного доступа;

20) выполнять какие-либо действия на АРМ до прохождения им процедуры идентификации- аудентификации.

3. Права пользователя

3.1. Пользователь имеет право:

1) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;

2) участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными;

3) своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей;

4) требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Ответственность пользователя

4.1. Пользователь несет персональную ответственность за:

1) ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуальных устройств идентификации и целостность установленного программного обеспечения;

2) разглашение сведений, отнесенных к сведениям конфиденциального характера (в том числе персональных данных), и сведений ограниченного распространения, ставших известными ему по роду работы.

4.2. Ответственность за нарушение функционирования ИСПДн, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

4.3. Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение 11 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Инструкция
по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств на аттестованных ИСПДн

1. Общие положения

1.1. Настоящей инструкцией регламентируется проведение любых модификаций и изменений в составе технических средств и программного обеспечения ИСПДн, технического обслуживания и устранения нештатных ситуаций в работе средств вычислительной техники (далее СВТ), входящих в состав ИСПДн.

1.2. Все изменения конфигурации технических и системных программных средств ИСПДн, ремонт, модификация, а также неконтролируемое со стороны сотрудников отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай (далее – отдел по защите информации и связи) техническое обслуживание основных технических средств и систем (далее – ОТСС), входящих в состав ИСПДн, должны производиться только на основании письменных заявок в управление по информационным технологиям и связи администрации города Урай с указанием необходимых действий и обоснования их необходимости. Ответственность за выполнение данного требования несёт сотрудник, эксплуатирующий данные средства информатизации.

2. Порядок проведения работ по техническому обслуживанию ОТСС

2.1. При возникновении необходимости в проведении работ у сотрудников, эксплуатирующих ОТСС ИСПДн (далее – пользователи), последние направляют в адрес начальника управления по информационным технологиям и связи администрации города Урай заявку на проведение работ. Начальник управления по информационным технологиям и связи администрации города Урай поручает исполнение заявки по существу вопроса лицам, ответственным за данные работы по компетенции, и параллельно сотрудникам отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай в части их касающейся (в части контроля за действиями в ходе ремонта, обслуживания и иных мероприятий, в части резервного копирования, удаления СЗИ и информации при необходимости). Пользователь допускает лиц, прибывших для проведения работ по заявке, только при присутствии сотрудников отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай.

2.2. При всех вышеуказанных работах на объектах информатизации сотрудниками подразделений (или сторонних организаций), занимающихся ремонтом, модификацией программных и аппаратных средств, инженерных коммуникаций, кабельных линий и систем объекта и выступающих в качестве инициаторов данных действий в соответствии с планом работ либо внепланово, пользователь допускает указанных исполнителей к данным работам только в присутствии сотрудника отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай.

2.3. Передача СВТ в другое подразделение или в распоряжение другой организации для ремонта или решения иных задач осуществляется только после того, как сотрудник отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай снимет средства защиты и предпримет необходимые меры для затирания или резервного копирования (при необходимости) защищаемой информации, которая хранилась на дисках.

2.4. О факте выполнения всех без исключения вышеуказанных работ сотрудником отдела по защите информации и связи делается соответствующая отметка в «Журнале учета ремонтных (профилактических) работ, выполненных в информационной системе персональных

данных», ведение которого контролируется начальником отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай.

Журнал ведётся отделом по защите информации и связи управления по информационным технологиям и связи администрации города Урай в отношении каждой аттестованной ИСПДн администрации города Урай.

Формат записей «Журнала учета ремонтных (профилактических) работ, выполненных в информационной системе персональных данных»:

№ п/п	Дата записи	Краткое описание выполненной работы, основание	Дата и время начала работы	Дата и время окончания работы	ФИО исполнителей работ и их подписи	Подпись администратора безопасности ИСПДн	Номер наклейки для опечатывания системного блока (если работы проводились с системным блоком)	Примечание
1	2	3	4	5	6	7	8	9

2.5. Пользователи и сотрудники отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай должны знать, что контролю и регистрации в журнале подлежат:

1) замена (модификация) средств вычислительной техники, входящих в состав ИСПДн в соответствии с техническим паспортом на ИСПДн, в том числе изменения линий локально-вычислительной сети;

2) замена, изъятие, добавление средств информатизации ИСПДн (средства электронно-вычислительной техники, комплектующие, системы и сети ИСПДн, системы и сети электросвязи, программные средства);

3) техническое обслуживание и ремонт СВТ без замены комплектующих и составных частей;

4) ремонт инженерных коммуникаций (в том числе линий силового питания, слаботочных линий), изменения в системе силового питания СВТ;

5) обновление (замена) на конкретном автоматизированном рабочем месте или сервере программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

6) изменение местоположения СВТ и вспомогательных средств и систем, указанных в схеме технического паспорта.

2.6. После внесения изменений в состав ИСПДн сотрудником отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай делается пометка в техническом паспорте на ИСПДн.

3. Порядок установки и обновления программного обеспечения

3.1. Установка или обновление подсистем ИСПДн должны проводиться уполномоченными сотрудниками (администраторы сети (серверов) и администраторы баз данных) обязательно в присутствии сотрудника отдела по защите информации и связи.

3.2. После установки модифицированных модулей на сервер (рабочую станцию) сотрудник отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай производит пересчет контрольных сумм с помощью установленных средств защиты информации и проводит антивирусный контроль.

3.3. Установка и обновление общего программного обеспечения (в том числе системного, тестового) на рабочие станции и сервера производится с оригинальных лицензионных

дистрибутивных носителей (дискет, компакт дисков и иных носителей), полученных в установленном порядке.

3.4. Факты установки или обновления фиксируются в «Журнале учета ремонтных (профилактических) работ, выполненных в информационной системе персональных данных».

4. Нештатные ситуации и форс-мажор

4.1. В условиях необходимого немедленного реагирования на нештатные ситуации разрешается модификация, замена, ремонт и иные мероприятия без согласования с отделом по защите информации и связи управления по информационным технологиям и связи администрации города Урай.

К нештатным ситуациям относятся:

1) выход из строя или неустойчивое функционирование узлов СВТ, периферийных устройств, средств защиты информации по различным причинам;

2) выход из строя системы электроснабжения.

4.2. При возникновении необходимости оперативной модификации, замены, ремонта пользователь немедленно обращается в отдел по защите информации и связи управления по информационным технологиям и связи администрации города Урай посредством телефонной связи. Необходимые работы выполняются под контролем пользователя и последующим написанием служебной (докладной) записки на имя заместителя главы администрации города Урай, ответственного за организацию работ по обеспечению безопасности персональных данных, с обоснованием экстренных изменений и описанием произведенных действий.

По результатам рассмотрения объяснительной записки сотрудник отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай выполняет все действия, предусмотренные настоящей инструкцией.

4.3. В случае выявления сотрудником отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай факта модификации, замены, ремонта и других действий, предусмотренных настоящей инструкцией, пользователями без согласования с отделом по защите информации и связи управления по информационным технологиям и связи администрации города Урай или без последующего написания служебной (докладной) записки на имя заместителя главы администрации города Урай, сотрудники отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай обязаны доложить о фактах грубого нарушения настоящего распоряжения заместителю главы администрации города Урай и инициировать проведение служебной проверки по факту нарушения.

5. Ответственность

5.1. Ответственность за ведение журнала и ознакомление пользователей аттестованных ИСПДн с данной инструкцией несёт начальник отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай.

5.2. Ответственность за соблюдение пользователями требований инструкции несут их непосредственные руководители согласно действующему законодательству.

Приложение 12 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

ПОЛИТИКА
в отношении обработки персональных данных

1. Общие положения

1.1. Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Конституцией Российской Федерации, Трудовым кодексом Российской Федерации.

1.2. Политика определяет порядок и условия обработки персональных данных в администрации города Урай (далее – Оператор) с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных осуществляется в целях приема и регистрации обращений (или запросов) граждан, организаций и общественных объединений, поступивших в адрес Оператора, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности муниципального имущества и исполнения полномочий, возложенных на администрацию города Урай.

2. Основные понятия, используемые в настоящей Политике

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

2.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых 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.

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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

2.7. 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.

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

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

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

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной и справедливой основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

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

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:

4.1.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

4.1.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

4.1.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4.1.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.1.6. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4.1.7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

4.1.8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

5. Конфиденциальность персональных данных

5.1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. Право субъекта персональных данных на доступ к его персональным данным

6.1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения, указанные в пункте 6.7 настоящей Политики, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.3. Сведения, указанные в пункте 6.7 настоящей Политики, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и сведения о выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.4. В случае, если сведения, указанные в пункте 6.7 настоящей Политики, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в пункте 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 6.3 настоящей Политики, должен содержать основание направления повторного запроса.

6.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным пунктом 6.3 и пунктом 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

6.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

6.7.1. Подтверждение факта обработки персональных данных Оператором;

6.7.2. Правовые основания и цели обработки персональных данных;

6.7.3. Цели и применяемые Оператором способы обработки персональных данных;

6.7.4. Наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

6.7.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

6.7.6. Сроки обработки персональных данных, в том числе сроки их хранения;

6.7.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

6.7.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.7.9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

6.7.10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7. Право на обжалование действий или бездействий Оператора

7.1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

8. Обязанности Оператора при сборе персональных данных

8.1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную пунктом 6.7 настоящей Политики.

8.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

8.3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных пунктом 8.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

8.3.1. Наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;

8.3.2. Цель обработки персональных данных и ее правовое основание;

8.3.3. Предполагаемые пользователи персональных данных;

8.3.4. Установленные Федеральным законом «О персональных данных» права субъекта персональных данных;

8.3.5. Источник получения персональных данных.

8.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 8.3 настоящего Положения, в случаях, если:

8.4.1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;

8.4.2. Персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

8.4.3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

8.4.4. Предоставление субъекту персональных данных сведений, предусмотренных пунктом 8.3 настоящей Политики, нарушает права и законные интересы третьих лиц.

9. Меры, направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом «О персональных данных»

9.1. Назначение ответственного за организацию обработки персональных данных.

9.2. Издание документов, определяющих политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.3. Утверждение правил проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, настоящей Политике, локальным актам.

9.4. Проведение оценки вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых Оператором мер.

9.5. Проведение ознакомления работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

10. Меры по обеспечению безопасности персональных данных при их обработке

10.1. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

10.2. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

10.3. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

10.4. Проведение оценки соответствия принимаемых мер по обеспечению безопасности персональных данных, получение аттестата соответствия требованиям по безопасности информации.

10.5. Ведение учета машинных носителей персональных данных.

10.6. Выполнение мер по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

10.7. Определение комплекса мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

10.8. Установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

10.9. Осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

Приложение 13 к распоряжению
администрации города Урай
от 20.04.2022 № 238-р

Форма журнала
учета машинных носителей персональных данных

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Место установки (использования)/ дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)

Форма журнала
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№	Наименование информационной системы персональных данных/способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер документа о допуске	Дата и подпись допускаемого лица	Дата и номер документа о прекращении допуска

Форма журнала
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

Форма журнала

учета выдачи персональных идентификаторов и электронных ключей
(для администратора информационной безопасности)

№ п/п	Ф.И.О.	№ идентификатора	Получил	Дата	Сдал	Отметка о возврате

Форма журнала

учета запросов субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

Форма акта

определения уровня защищенности ПДн при их обработке в ИСПДн и класса защищенности ИС администрации города Урай

Председатель комиссии _____ ФИО

Члены комиссии

_____ ФИО

_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются специальные категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии _____ ФИО

Члены комиссии

_____ ФИО

_____ ФИО

«__»_____20__ г.

Форма акта

об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Статус	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (п.7 ст. 5), подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем _____

_____

(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии:

_____ _____

подпись расшифровка

Члены комиссии:

_____ _____

подпись расшифровка

_____ _____

подпись расшифровка