ГОРОДСКОЙ ОКРУГ УРАЙ
Ханты-Мансийского автономного округа - Югры

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«УПРАВЛЕНИЕ ГРАДОСТРОИТЕЛЬСТВА, ЗЕМЛЕПОЛЬЗОВАНИЯ И ПРИРОДОПОЛЬЗОВАНИЯ ГОРОДА УРАЙ»

ПРИКАЗ

от 30.12.2022 №167

Об обработке персональных данных и
защите информации

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

ПРИКАЗЫВАЮ:

1. Назначить заместителя директора Богданова С.П. ответственным за организацию обработки персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн) муниципального казенного учреждения «Управление градостроительства, землепользования и природопользования города Урай» (далее – Управление), возложив обязанности по:

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

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

2. Назначить начальника отдела информационного обеспечения градостроительной деятельности Управления Семьину И.Я. ответственным за организацию работ по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн Управления, возложив обязанности по:

1) организации мероприятий, направленных на обеспечение безопасности персональных данных;

2) доведению до сведения сотрудников Управления положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) учету лиц, допущенных к работе с персональными данными в ИСПДн;

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

5) разбирательству и составлению 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;

6) разработке и представлению руководству предложений по обеспечению безопасности персональных данных.

3. Установить, что ответственность за соблюдение сотрудниками Управления организационно-распорядительных документов по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, несут их непосредственные руководители.

4. Утвердить документы:

- Перечень информационных систем персональных данных (Приложение 1);
- Перечень персональных данных, обрабатываемых в Управлении (Приложение 2);
- Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение 3);
- Положение о порядке обработки персональных данных в Управлении (Приложение 4);
- Инструкцию пользователя информационной системы персональных данных (Приложение 5);
- Политику в отношении обработки персональных данных (приложение 6);
- Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение 7);
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 8);
- Инструкция по работе с машинными носителями информации в информационных системах (Приложение 9);
- Инструкция администратора безопасности информационных систем персональных данных (Приложение 10).

5. Утвердить формы (Приложение 11):

- журнала учета запросов субъектов персональных данных по вопросам обработки персональных данных;
- журнала учета ремонтных работ на АРМ ИСПДн Управления;
- журнала учета средств защиты информации;
- журнала учета машинных носителей персональных данных;
- журнала учета лиц, допущенных к работе с персональными данными в ИСПДн;
- журнала учета выдачи персональных идентификаторов и электронных ключей;
- акта об уничтожении персональных данных субъектов персональных данных.

6. Назначить комиссию для проведения классификации ИСПДн в Управлении в составе:

Председателя комиссии – заместитель директора Управления;

Члены комиссии:

- главный юрисконсульт службы организационно-правового обеспечения Управления;
- начальник отдела информационного обеспечения градостроительной деятельности Управления;
- эксперт службы организационно-правового обеспечения Управления.

7. Считать утратившими силу приказы от 11.09.2017 №208 «Об обработке персональных

данных и защите информации», приказ от 29.09.2020 №105 «О внесении изменений в приказ от 11.09.2017 №208».

8. Эксперту службы организационно-правового обеспечения Ельцовой Г.И. ознакомить с приказом работников Управления.

9. Контроль за выполнением приказа оставляю за собой.

Директор Л.В. Фильченко

Исполнитель:

Начальник ОИОГД _____ / _____ / 30.12.2022

Ф.И.О. подпись дата

Согласовано:

Главный юрисконсульт СОПО _____ / _____ / 30.12.22

Ф.И.О. подпись дата

Эксперт СОПО _____ / _____ / 30.12.22

Ф.И.О. подпись дата

Приложение 1 к приказу
от 30.12.22 № 167

Перечень информационных систем персональных данных

Наименование	Адрес расположения
Камин: Зарплата	г.Урай, микрорайон 2, дом 59, кабинеты 305, 312

Приложение 2 к приказу
от 30.12.22 № 167

Перечень персональных данных, обрабатываемых в Управлении

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Основание для обработки персональных данных
1. Обработка персональных данных в ИСПДн Камин Зарплата			
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, оформление трудовых договоров	Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (статьи 85-90)
Сведения о родственниках работника	Фамилия, имя, отчество, дата рождения, степень родства	Реализация кадровой политики	Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (статьи 85-90)

Приложение 3 к приказу
от 30.12.2022 № 167

Перечень должностей, замещение которых предусматривает осуществление автоматизированным или неавтоматизированным способом обработки персональных данных либо осуществление доступа к персональным данным

Должность	ИСПДн
Эксперт службы организационно-правового обеспечения	Камин: Зарплата

Приложение 4 к приказу
от 30.12.22 №167

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в Управлении

1. Общие положения

1.1. Положение о порядке обработки и защиты персональных данных в Управлении, связанных с реализацией служебных или трудовых отношений (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 Управлении.

1.2. Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановлением Правительства Российской Федерации от 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», Постановлением правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3.Управление является оператором персональных данных.

2. Состав персональных данных

2.1. К персональным данным, обрабатываемым в Управлении, относятся:

персональные данные работников;

персональные данные уволенных работников;

персональные данные родственников работников;

персональные данные граждан, обращающихся в Управление;

персональные данные физических и юридических лиц, заключающих (расторгающих) имущественные сделки;

персональные данные лиц, выполняющих поставки, работы, услуги по договорам;

персональные данные, обрабатываемые в целях предоставления государственных и муниципальных услуг.

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

личных делах работников;

личных делах уволенных работников;

трудовой книжке работника;

медицинских справках;

документах, подтверждающих право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;

документах о возрасте детей или беременности женщины для предоставления установленных законом условий труда, гарантий и компенсаций;

иных документах, необходимых для определения трудовых отношений.

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

3. Обработка персональных данных

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

3.2. Обработка персональных данных в Управлении 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 приказом директора Управления.

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

3.5. Допуск работников управления к ИСПДн осуществляется с соблюдением порядков по информационной безопасности, действующих в Управлении.

3.6. Санкционированный внешний доступ к персональным данным, обрабатываемым в Управлении, имеют:

- работники контрольно-надзорных органов, при наличии служебного удостоверения и документов, на основании которых они проводят проверку;
- работники сторонних организаций, обеспечивающих программное сопровождение информационных систем, при наличии в договоре условий о сохранении конфиденциальной информации;
- 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 Управлении, без специального разрешения имеют:

- директор Управления;
- заместитель директора Управления;
- работники, осуществляющие кадровую работу в Управлении;
- работники бухгалтерии, в чьи обязанности входит работа с персональными данными работников Управления согласно должностным инструкциям.

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 Управлении или работников, занимающих должности в Управлении, у третьей стороны, следует получить письменное согласие гражданина и сообщить о целях, предполагаемых источниках и способах получения персональных данных (Приложение 1 – Форма согласия).

3.8.4. При сборе персональных данных работник, осуществляющий сбор (получение) персональных данных непосредственно от работников Управления, граждан, претендующих на замещение должностей Управления, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные (Приложение 2 – Форма разъяснения).

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 Управления, должны вестись в соответствии с требованиями действующего законодательства. Личные дела хранятся в специально отведенной секции шкафа (сейфа), обеспечивающей защиту от несанкционированного доступа.

3.9.3. Обязанности по хранению личных дел работников Управления, заполнению, хранению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, содержащих персональные данные работников Управления, возлагаются на работника, исполняющего кадровую работу в Управлении, что закреплено в должностной инструкции.

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

3.9.5. Все съемные носители (винчестеры, flash-накопители, CD-диски), 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 РФ.

3.11.2. 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 Управления, 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.

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

4.1. 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.

4.2. Ключи от помещений, сдаются ответственными работниками под охрану. 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 работников, которые назначаются приказом.

5. Защита персональных данных

5.1. Работники Управления 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 Управления осуществляется в рамках действующих порядков и инструкций по защите информации Управления.

6. Обязанности лиц, допущенных к обработке персональных данных

6.1. Каждый работник, принимаемый на работу в Управление, должен быть ознакомлен под личную подпись с обязательством о неразглашении персональных данных, ставших ему известными в ходе выполнения своих служебных обязанностей по форме, утвержденной приложением №3 к настоящему Положению.

6.2. Работники Управления, допущенные к обработке персональных данных, обязаны:

- знать и выполнять требования настоящего Положения;
- 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;
- знакомиться только с теми персональными данными, к которым получен доступ;
- хранить в тайне известные им сведения о персональных данных, информировать своего непосредственного начальника о фактах нарушения порядка обработки персональных данных и попытках несанкционированного доступа к ним;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
- выполнять требования по защите полученных персональных данных субъекта;
- соблюдать правила пользования документами, содержащими персональные данные, порядок их обработки и защиты;
- 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 Управления, 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 Управления, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с действующим законодательством.

8. Контроль за выполнением требований настоящего Положения

8.1. Повседневный контроль соблюдения требований в части обработки и защиты персональных данных осуществляют руководители отделов Управления.

8.2. Контроль выполнения требований по защите персональных данных, обрабатываемых в информационных системах Управления, осуществляет ответственный за организацию обработки персональных данных в информационных системах персональных данных.

Приложение 1
к Положению о порядке обработки
персональных данных в управлении

СОГЛАСИЕ
на обработку персональных данных

«____» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____

_____

настоящим даю свое согласие на обработку моих персональных данных _____

_____
(наименование и адрес оператора)

и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей _____

_____

_____
(цель обработки персональных данных)

и распространяется на следующую информацию: _____

_____

_____

_____

_____

_____, полученных лично от меня для обработки и передачи в документальной и электронной форме в различные государственные органы власти, если этого требует законодательство Российской Федерации или Ханты-Мансийского автономного округа – Югры, а также третьим лицам _____

_____

_____
(наименование и адреса третьих лиц)

с целью исполнения обязательств представителя нанимателя в рамках трудового договора, и в установленных Федеральными законами случаях их обязательного предоставления. Также не возражаю против обработки сведений обо мне, содержащих данные об имени, фамилии, отчестве, должности, телефонном номере и адресе электронной почты, полученных мною для их использования в служебных целях, в т. ч. размещения в государственных информационных системах, используемых в рамках обеспечения доступа к информации о деятельности управления.
Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных с учетом федерального законодательства.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

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

(Ф.И.О., подпись лица, давшего согласие, реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

Примечание:

1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность субъекта персональных данных.
2. Письменное согласие заполняется и подписывается субъектом персональных данных собственноручно в присутствии должностного лица оператора.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

Приложение 2
к Положению о порядке обработки
персональных данных в управлении

Форма разъяснения
субъекту персональных данных

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в Управление.

В соответствии со статьями 65,86 Трудового кодекса Российской Федерации определен перечень персональных данных, которые субъект персональных данных обязан предоставить в Управление 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 управлении

Обязательство о неразглашении персональных данных

Я,_____

_____

(фамилия, имя, отчество, должность)

в период трудовых отношений с Управлением 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 Управления третьей стороне без письменного согласия работников, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью работников, 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.

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.

До моего сведения доведены и разъяснены 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 4
к Положению о порядке обработки
персональных данных в управлении

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

Я _____
_____,
(ФИО, должность)

номер телефона (рабочий)_____,
адрес электронной почты (рабочий) _____,

именуемый в дальнейшем «Субъект персональных данных», согласно статье 10.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», даю согласие МКУ «Управление градостроительства, землепользования и природопользования города Урай», далее «Оператор», на распространение моих персональных данных.

Цель распространения: Размещение персональных данных на официальном сайте органов местного самоуправления города Урай **http://uray.ru** в информационно-телекоммуникационной сети «Интернет».

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Общедоступные	Фамилия			
	Имя			
	Отчество			
	Должность			
	Номер телефона (рабочий)			
	Эл.почта (рабочая)			

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 до «31» декабря 2027г.

Данные об Операторе:

Муниципальное казенное учреждение «Управление градостроительства, землепользования и природопользования города Урай»

ИНН 8606015271\ ОГРН 1128606001248

628285, Ханты-Мансийский автономный округ - Югра, г. Урай, мкр. 2, дом 59 (3 эт).

Субъект персональных данных:

«30» декабря 2022 г. _____ _____
(подпись) (фамилия, имя, отчество)

Приложение 5 к приказу
от 30.12.22 №167

Инструкция пользователя информационной системы персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 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. Данная инструкция определяет общие обязанности, права и ответственность пользователя информационной системы персональных данных (далее – ИСПДн) Управления по обеспечению информационной безопасности при работе со сведениями.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник Управления, 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 знать и соблюдать:

- порядок обработки персональных данных в Управлении, утвержденный настоящим приказом;
- утвержденные настоящим приказом инструкции и другие организационно-распорядительные документы Управления в части обеспечения безопасности информации.
- 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;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);
- хранить в тайне свои идентификационные данные (имена, пароли и т.д.);
- осуществлять вход в ИСПДн только под своими идентификационными данными;
- 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);

- немедленно 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;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ;
- экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;
- соблюдать установленный режим разграничения доступа к информационным ресурсам;
- немедленно выполнять предписания ответственного за выполнение работ по обеспечению безопасности персональных данных, предоставлять свое АРМ для контроля;
- ставить в известность ответственного за выполнение работ по обеспечению безопасности персональных данных 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.);
- при работе в ИСПДн использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с ответственным за организацию работ по обеспечению безопасности персональных данных;
- осуществлять установленным порядком (сочетанием клавиш Shift+Del), уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;
- уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;
- сообщать непосредственному руководителю обо всех проблемах, связанных с эксплуатацией ИСПДн.

2.2. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- 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;
- осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.), в том числе для временного хранения;
- оставлять включенное без присмотра свое АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);
- 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;
- 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);
- 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;
- подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;
- осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;

- фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;
- разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;
- вносить изменения в файлы, принадлежащие другим пользователям;
- осуществлять передачу защищаемой информации по незащищенным каналам сетей связи общего пользования;
- отключать (блокировать) средства защиты информации;
- осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;
- производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) АРМ и серверов;
- закрывать доступ к информации паролями без согласования с ответственным за выполнение работ по обеспечению безопасности персональных данных;
- использовать для доступа к ИСПДн технологии беспроводного доступа;
- выполнять какие-либо действия на АРМ до прохождения им процедуры идентификации - аутентификации.

3. Права пользователя

3.1. Пользователь имеет право:

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;
- 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;
- своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей;
- требовать от непосредственного руководителя 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:

- ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуальных устройств идентификации и целостность установленного программного обеспечения;
- 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 6 к приказу
от 30.12.22 №167

ПОЛИТИКА
в отношении обработки персональных данных

1. Общие положения

1.1. Политика в отношении обработки персональных данных в управлении (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 Управлении (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 управление.

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 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 п. 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 п. 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 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 п. 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 п. 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 п. 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 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 п. 6.3 настоящей Политики, должен содержать основание направления повторного запроса.

6.6. Оператор в праве отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 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 п. 7.7 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 п. 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 настоящим Федеральным законом права субъекта персональных данных;

8.3.5. Источник получения персональных данных.

8.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 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 частью 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. Назначен ответственный за организацию обработки персональных данных.

9.2. Изданы документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.3. Проведено ознакомление 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. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

10.2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.

10.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

10.4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.

10.5. Ведется учет машинных носителей персональных данных.

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

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

10.8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

10.9. Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

Приложение 7 к приказу
от 30.12.22 №167

Правила рассмотрения запросов
субъектов персональных данных или их представителей

1. В соответствии с частями 1 и 7 статьи 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее - ФЗ №152-ФЗ), статьей 89 Трудового кодекса Российской Федерации субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (далее - сведения).

2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных в управлении (далее – Оператор), предусмотренной частью 7 статьи 14 ФЗ №152-ФЗ и статьей 89 ТК Российской Федерации.

3. 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.

4. 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.

5. 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 по форме согласно приложению 8 к настоящему приказу.

6. 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.

7. 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.

8. 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.

9. 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:

– Оператор обязан сообщить в порядке, предусмотренном статьей 14 ФЗ №152-ФЗ, 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.

– 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 ФЗ №152-ФЗ 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.

– 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.

– 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 8 к приказу
от 30.12.22 №167

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям по безопасности информации

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» (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 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.

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

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

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

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

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

– 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;

– порядок и условия применения средств защиты информации;

– соблюдение правил доступа к персональным данным;

– 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 в ходе проверки имеют право:

– запрашивать у работников информацию, необходимую для реализации своих полномочий;

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

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

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

– 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.

Приложение 9 к приказу
от 30.12.22 № 167

ИНСТРУКЦИЯ ПО РАБОТЕ С МАШИННЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Общие положения

Настоящая Инструкция по работе с машинными носителями информации в информационных системах (далее – Инструкция) регламентирует порядок использования и работы со съемными носителями информации во всех подлежащих в соответствии с требованиями законодательства по защите информационных системах управления.

Инструкция является документом обязательным для исполнения всеми пользователями информационных систем (далее – ИС) управления.

Порядок использования съемных носителей информации

Под использованием съемных носителей информации в ИС понимается их подключение к автоматизированным рабочим местам (далее – АРМ) с целью обработки, приема/передачи информации между АРМ и носителями информации.

В ИС допускается использование только учтенных съемных носителей информации, которые являются собственностью управления и подвергаются регулярной ревизии и контролю.

Съемные носители информации предоставляются пользователям ИС по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника управления производственной необходимости.

Порядок учета, хранения и обращения со съемными носителями, твердыми копиями и их утилизации

Все находящиеся на хранении и в обращении съемные носители подлежат учёту.

Каждый съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

Для получения электронного внешнего носителя, пользователь обращается к непосредственному руководителю, руководитель структурного подразделения пишет служебную записку на имя ответственного за организацию работ по обеспечению безопасности персональных данных и другой защищаемой информации в управлении о выдаче пользователю внешнего электронного носителя, далее ответственный за организацию работ по обеспечению безопасности персональных данных.

Учет и выдачу съемных носителей осуществляет ответственный за организацию работ по обеспечению безопасности персональных данных, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации согласно приложению к инструкции.

При использовании пользователей съемных носителей информации **необходимо:**

- соблюдать требования настоящей Инструкции;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;
- бережно относится к носителям информации;
- извещать ответственного за организацию работ по обеспечению безопасности персональных данных о фактах утраты (кражи) носителей информации;

При использовании носителей конфиденциальной информации **запрещено:**

- использовать носители конфиденциальной информации в личных целях;
- передавать носители конфиденциальной информации другим лицам (за исключением ответственного за организацию работ по обеспечению безопасности персональных данных);
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации) инициированное пользователем ИС между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с ответственным за организацию работ по обеспечению безопасности персональных данных). Ответственный за организацию работ по обеспечению безопасности персональных данных оставляет за собой право блокировать или ограничивать использование носителей информации.

Факт несанкционированного и/или нецелевого использовании носителей информации считается инцидентом информационной безопасности. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно принятому порядка управления инцидентами по информационной безопасности, утвержденного настоящим приказом.

Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется ответственным за организацию работ по обеспечению безопасности персональных данных после сдачи пользователями, с отметкой в журнале.

В случае увольнения или перевода работника в другое структурное подразделение предоставленные носители конфиденциальной информации сдаются ответственному за организацию работ по обеспечению безопасности персональных данных.

Роли и ответственность

Ответственность за соблюдение указанных требований возлагается на всех работников управления.

Все исключения из основных требований должны быть согласованы с ответственным за организацию обработки персональных данных, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на руководителей структурных подразделений.

Приложение к Инструкции по работе с машинными носителями информации в информационных системах

ЖУРНАЛ учета машинных носителей (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

Приложение 10 к приказу
от 30.12.22 № 167

Инструкция администратора безопасности информационных систем персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 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 безопасности информационных систем персональных данных управления.

1.3. Администратор безопасности ИСПДн (далее – Администратор) назначается приказом управления и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИСПДн 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 ИСПДн.

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 управления в части его касающейся.

2.2. Знать перечня обрабатываемых в управлении 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:

- порядки информационной безопасности, утвержденные приказом управления №254 от 30.12.2016 «Об утверждении документов по информационной безопасности»;
- утвержденные настоящим приказом инструкции и другие организационно-распорядительные документы управления в части обеспечения безопасности информации.

2.4. Контролировать соответствие ОТСС ИС техническим паспортам на ИС.

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

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

- 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;

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

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

- 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 неизменность настроек средств защиты информации:

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

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

- средства защиты информации должны обеспечивать запрет удаленного доступа к ИС;

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

- средства доверенной загрузки должны обеспечивать:

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

• контроль доступа пользователей к процессу загрузки операционной системы;

• 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 утвержденном журнале.

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:

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

• 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.

- подключения машинных носителей информации и вывода информации на носители информации:

• 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.

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

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

- попыток доступа программных средств к защищаемым объектам доступа:

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

- попыток удаленного доступа:

• 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 управлении 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:

- контроль за событиями безопасности и действиями пользователей в ИС;

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

- 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;

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

- 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:

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

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

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

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

– 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;

– вносить свои предложения по совершенствованию мер защиты в ИС.

3.2. Администратору запрещается:

- 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;

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

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

- выключать СЗИ без письменной санкции руководства;

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

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

- нарушать правила эксплуатации оборудования ИС и СЗИ.

- 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 управления в соответствии с положениями законодательства Российской Федерации в области защиты информации

С инструкцией ознакомлен:

_____ _____ «_____» _____ 20____г.

(подпись) Ф.И.О.

_____ _____ «_____» _____ 20____г.

(подпись) Ф.И.О.

Приложение 11 к приказу
от 30.12.22 № 167

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

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

Форма журнала
учета выдачи персональных идентификаторов и электронных ключей

№ 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 журнала

учета ремонтных работ на АРМ ИСПДн управления

№ п/п	Дата записи	Наименование, местоположение АРМ	Краткое описание выполненной работы	Дата, время начала работ	Дата, время окончания работ	ФИО исполнителей работ, название организации	Подпись лица ответственного за защиту информации	Примечание

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 акта

об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 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