# Администрация
# муниципального образования город Салехард

# РАСПОРЯЖЕНИЕ

26 января 2016 года № 104-р

**Об утверждении инструкций по защите персональных данных в Администрации города Салехарда**

Во исполнение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также в целях выработки единой политики и подходов к обеспечению безопасности персональных данных и организации их обработки в информационных системах персональных данных Администрации города Салехарда:

1. Утвердить:

1.1. Инструкцию ответственного за организацию обработки персональных данных в Администрации города Салехарда (Приложение № 1);

1.2. Инструкцию ответственного за обработку персональных данных в структурном подразделении Администрации города Салехарда (Приложение № 2);

1.3. Инструкцию ответственного за обеспечение безопасности персональных данных в Администрации города Салехарда (Приложение № 3);

1.4. Инструкцию администратора информационной безопасности в Администрации города Салехарда (Приложение № 4);

1.5. Инструкцию пользователя информационной системы персональных данных в Администрации города Салехарда (Приложение № 5);

1.6. Инструкцию по организации антивирусной защиты информационных систем персональных данных в Администрации города Салехарда (Приложение № 6);

1.7. Инструкцию по организации парольной защиты информационных систем персональных данных в Администрации города Салехарда (Приложение № 7);

1.8. Инструкцию по организации резервирования и восстановления программного обеспечения, баз персональных данных в информационных системах персональных данных Администрации города Салехарда (Приложение № 8);

1.9. Инструкцию о порядке доступа в помещения Администрации города Салехарда в которых ведется обработка персональных данных (Приложение № 9);

1.10. Инструкцию по порядку учёта, хранения и уничтожения персональных данных в Администрации города Салехарда (Приложение № 10);

1.11. Инструкцию по порядку учёта, хранения съёмных носителей персональных данных в Администрации города Салехарда (Приложение № 11);

1.12. Инструкцию по модификации технических и программных средств в информационных системах персональных данных Администрации города Салехарда (Приложение № 12);

1.13. Журнал учёта допуска к работе пользователей информационных систем персональных данных Администрации города Салехард (Приложение № 13);

1.14. Журнал учёта защищаемых носителей информации Администрации города Салехарда (Приложение № 14);

1.15. Журнал учёта средств защиты информации, эксплуатационной и технической документации к ним, используемых в информационных системах персональных данных Администрации города Салехарда (Приложение № 15);

1.16. Журнал учёта проводимых внутренних проверок Администрации города Салехарда (Приложение № 16).

2. Поручить отделу специальных мероприятий Администрации города Салехарда (А.Н. Грачеву):

2.1. провести ознакомление с инструкциями, утвержденными в пункте 1 настоящего распоряжения, всех сотрудников Администрации города Салехарда в части, их касающейся;

2.2. организовывать ведение журналов, указанных в пункте 1 настоящего распоряжения, в Администрации города Салехарда без учёта юридических лиц.

3. Руководителям структурных подразделений Администрации города Салехарда, обладающих правами юридических лиц, принять аналогичные документы, указанных в пункте 1 настоящего распоряжения и обеспечить выполнение обязанностей оператора согласно действующего законодательства Российской Федерации.

4. Контроль за исполнением настоящего распоряжения возложить на начальника отдела специальных мероприятий Администрации города Салехарда А.Н. Грачева.

Глава Администрации города И.Л. Кононенко

Приложение № 1
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

ответственного за организацию обработки персональных данных
в Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**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.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Пользователь информационной системы персональных данных (ИСПДн)** – лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет основные обязанности, права ответственного лица за организацию обработки персональных данных Администрации города Салехарда (далее – Ответственный).

1.2. Ответственный назначается распоряжением Администрации города Салехарда из числа муниципальных служащих Администрации города Салехарда.

1.3. Ответственный в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Администрации города Салехарда.

## 2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

**Ответственный обязан:**

2.1. Знать и выполнять требования действующего законодательства РФ, нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий по организации обработки и безопасности персональных данных.

2.2. Принимать решения по проведению служебных расследований и выявлению виновных в нарушениях правил работы с документами, содержащими персональные данные, режима безопасности персональных данных или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.3. По результатам служебных расследований принимать меры по наказанию виновных в нарушении требований к защите и обработке персональных данных в соответствии с действующим законодательством Российской Федерации.

2.4. Утверждать перечень должностей работников, замещение которых предусматривает осуществление обработки персональных данных.

2.5. Утверждать списки пользователей ИСПДн, переданных для утверждения руководителями структурных подразделений.

## 3. ПРАВА ОТВЕТСТВЕННОГО

**Ответственный имеет право:**

3.1. Принимать решения о прекращении доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.2. Назначать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащие персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.3. Прекращать процесс обработки персональных данных или отстранять от работы пользователя ИСПДн при нарушениях установленной технологии обработки персональных данных или нарушениях режима конфиденциальности.

3.4. Рассматривать предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятию мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

## 4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственный несёт персональную ответственность за:

4.1.1. соблюдение требований настоящей Инструкции;

4.1.2 правильность и объективность принимаемых решений.

4.2. При нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, ответственный несет ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

ответственного за обработку персональных данных
в структурном подразделении Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**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.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн)** – лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет основные обязанности и права ответственного лица за обработку персональных данных в структурном подразделении Администрации города Салехарда (далее – структурное подразделение).

1.2 Ответственным за обработку персональных данных в структурном подразделении (далее - Ответственный) является руководитель этого подразделения или его заместитель и назначается распоряжением Администрации города Салехарда.

1.3. Назначенный Ответственный подчиняется ответственному за организацию обработки персональных данных Администрации города Салехарда.

1.4. Ответственный осуществляет методическое руководство внутри своего подразделения в сфере организации обработки персональных данных.

1.5. Требования Ответственного, связанные с выполнением им своих служебных обязанностей обязательны для исполнения всеми работниками его структурного подразделения, имеющими санкционированный доступ к персональным данным.

1.6. Ответственный отвечает за качество проводимых им работ по контролю действий при работе в информационной системе персональных данных (далее - ИСПДн), состояние и поддержание установленного уровня защиты ИСПДн.

## 2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

**Ответственный обязан:**

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий по организации обработки персональных данных.

2.2. Согласно утвержденному перечню должностей работников Администрации города Салехарда, замещение которых предусматривает осуществление обработки персональных данных, предоставлять и разрабатывать для утверждения ответственному за организацию обработки персональных данных в Администрации города Салехарда списки пользователей ИСПДн по установленной форме (изменения к списку лиц), доступ которых к обработке персональных данных необходим для выполнения должностных обязанностей.

2.3. Проводить консультации пользователей ИСПДн в своем структурном подразделении по соблюдению режима конфиденциальности.

2.4. Контролировать физическую сохранность средств и оборудования ИСПДн подразделения.

2.5. Контролировать соблюдение пользователями ИСПДн режима конфиденциальности, правил работы со съёмными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

2.6. Взаимодействовать с администратором информационной безопасности по вопросам обеспечения и выполнения требований обработки персональных данных.

2.7. Знать перечень и условия обработки персональных данных в Администрации города Салехарда, а также перечень обрабатываемых персональных данных в своем структурном подразделении.

2.8. Знать перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.9. Осуществлять контроль за порядком учёта, создания, хранения и использования машинных (выходных) документов, содержащих персональные данные.

2.10. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа

к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать о них администратору информационной безопасности.

2.11. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

## 3. ПРАВА ОТВЕТСТВЕННОГО

**Ответственный имеет право:**

3.1. Требовать от всех пользователей ИСПДн подразделения выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.4. Обращаться с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя ИСПДн в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.5. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

## 4. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. При несанкционированном доступе к защищаемой информации (ПДн), а именно:

4.1.1. выявление (обнаружение) сеансов работы с персональными данными незарегистрированных пользователей или пользователей, нарушивших установленный порядок доступа, или превышающих свои полномочия по доступу к данным;

4.1.2. выявление (обнаружение) действий постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора информационной безопасности или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учётной записи или любым другим методом.

4.2. Ответственный обязан:

4.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

4.2.2. известить администратора информационной безопасности о факте несанкционированного доступа, от имени учётной записи, которого была осуществлена попытка;

4.2.3 доложить ответственному за организацию обработки персональных данных Администрации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

## 5. ОТВЕТСТВЕННОСТЬ

5.1. Ответственный несет персональную ответственность за:

5.1.1. соблюдение требований настоящей Инструкции;
5.1.2. правильность и объективность принимаемых решений.

5.2. При нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, ответственный несет ответственность в соответствии с законодательством Российской Федерации.

Приложение № 3
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

ответственного за обеспечение безопасности персональных данных
в Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**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.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн)** – лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет основные обязанности, права ответственного лица за обеспечение безопасности персональных данных Администрации города Салехарда.

1.2. Ответственный за обеспечение безопасности персональных данных Администрации города Салехарда назначается распоряжением Администрации города Салехарда, руководитель подразделения по технической защите (безопасности) информации.

1.3. Ответственный за обеспечение безопасности персональных данных Администрации города Салехарда (далее - Ответственный) подчиняется ответственному за организацию обработки персональных данных Администрации города Салехарда.

1.4. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты.

## 2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

**Ответственный обязан:**

2.1. Знать и выполнять требования действующего законодательства РФ, нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий по организации обработки и безопасности персональных данных.

2.2. Контролировать администратора информационной безопасности по вопросам обеспечения и выполнения требований по безопасности персональных данных при их обработке в ИСПДн.

2.3. Осуществлять контроль над соблюдением режима обработки ПДн и режима защиты ПДн.

2.4. Осуществлять контроль за порядком учёта, создания, хранения и использования машинных (выходных) документов, содержащих персональные данные.

2.5. Организовывать аналитическую работу по соответствию существующих мер защиты ПДн, актуальным угрозам безопасности ПДн. При необходимости принимать меры к нейтрализации актуальных угроз безопасности ПДн, а также предупреждать появление новых, еще неизвестных угроз.

2.6. Контролировать актуальное состояние действующей документации по безопасности ПДн.

2.7. Осуществлять контроль над внесением изменений в штатное программное обеспечение.

2.8. Проводить и участвовать в служебных расследованиях с составлением заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

## 3. ПРАВА ОТВЕТСТВЕННОГО

**Ответственный имеет право:**

3.1. Требовать от всех пользователей ИСПДн подразделения выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.4. Обращаться с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя ИСПДн в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.5. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятию мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

## 4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственный несет персональную ответственность за:

4.1.1. соблюдение требований настоящей Инструкции;

4.1.2. правильность и объективность принимаемых решений.

4.1.3. При нарушении норм, регулирующих получение, обработку и защитуперсональных данных субъекта, ответственный несет ответственность в соответствии с законодательством Российской Федерации.

Приложение № 4
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

администратора информационной безопасности
в Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированное рабочее место (АРМ)** – это комплекс средств вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте работника и предназначенный для автоматизации его работы.

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

**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.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн)** – лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

**Безопасность информации** – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

**Доступ к информации** – возможность получения информации и ее использования.

**Несанкционированный доступ (НСД)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, представляемых АРМ.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и определяет порядок обеспечения безопасности информации при проведении работ администратором информационной безопасности (далее – АБ) в информационных системах персональных данных (далее – ИСПДн) Администрации города Салехарда.

1.2. АБ назначается распоряжением Администрации города Салехарда и получает неограниченные права на доступ к ресурсам ИСПДн.

1.3. АБ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПДн (далее - пользователей) и обслуживающего персонала.

1.4. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБ.

## 2. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**АБ обязан:**

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Осуществлять учёт съёмных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

2.3. Немедленно реагировать на сообщения пользователей о любых неисправностях в работе АРМ, СЗИ, системного и прикладного программного обеспечения (далее – ПО) ИСПДн.

2.4. Немедленно ставить в известность ответственного за обеспечение безопасности персональных данных обо всех неисправностях аппаратно-программных средств ИСПДн.

2.5. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними специалистами в Администрации города Салехарда.

2.6. Осуществлять заведение и удаление учётных записей пользователей, управлять их полномочиями и поддержанием правил разграничения доступа в ИСПДн.

2.7. Управлять СЗИ в ИСПДн, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управлением учётными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей.

2.8. В случае отказа технических средств или программного обеспечения элементов ИСПДн, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.9. По указанию ответственного за обеспечение безопасности персональных данных, осуществлять разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.10. Осуществлять изменениями аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПДн.

2.11. Осуществлять установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению.

2.12. Осуществлять регистрацию и анализ событий в ИСПДн, связанных с защитой информации.

2.13. Осуществлять информирование пользователей ИСПДн об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПДн и отдельных СЗИ, а также их обучение.

2.14. Осуществлять сопровождение функционирования системы защиты информации ИСПДн в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

2.15. Осуществлять обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.

2.16. Осуществлять своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн.

2.17. Осуществлять анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий.

2.18. Осуществлять планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.

2.19. Осуществлять планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.20. Осуществлять анализ и оценку функционирования системы защиты информации ИСПДн, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПДн.

2.21. Осуществлять проверку состава технических средств, программного обеспечения и СЗИ.

2.22. Осуществлять контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.

2.23. Осуществлять еженедельное отслеживание появления новых видов уязвимостей ПО ИСПДн. По необходимости АБ производит устранение уязвимостей согласно рекомендациям разработчика.

2.24. Осуществлять периодический анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации.

2.25. Осуществлять контроль за событиями безопасности и действиями пользователей в ИСПДн. В частности, АБ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.26. Осуществлять контроль (анализ) защищенности информации, содержащейся в ИСПДн.

2.27. Осуществлять документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн.

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

## 3. ПРАВА АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**АБ имеет право:**

3.1. Инициировать прекращение обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.2. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.3. Проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

3.4. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

## 4. ДОСТУП К РЕСУРСАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обязательными условиями получения доступа к ресурсам ИСПДн АБ являются:

- право доступа в помещение;
- наличие допуска к персональным данным;
- право доступа к ИСПДн;
- знание технологии обработки информации в ИСПДн с учётом требований информационной безопасности.

4.2. Идентификация АБ в ИСПДн осуществляется по уникальному имени и персональному идентификатору (при его наличии).

4.3. Длина пароля АБ – не менее 6 буквенно-цифровых символов.

4.4. Уникальное имя, персональный идентификатор (при его наличии) и пароль АБ получает в установленном порядке. АБ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

4.5. При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

4.6. Регистрация пользователя осуществляется АБ в соответствии с «Инструкцией по организации парольной защиты информационных систем персональных данных в Администрации города Салехарда» и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

4.7. При заведении новой учётной записи, АБ должен проверить личность пользователя и его должностные обязанности.

4.8. Предоставление пользователям прав доступа к объектам доступа ИСПДн должно осуществляться на основании задач, решаемых пользователями.

4.9. АБ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

4.10. АБ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

## 5. ПОРЯДОК РАБОТЫ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ С РЕСУРСАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн.

АБ присваивает пользователям идентификационные данные к ресурсам ИСПДн.

При этом должны выполняться следующие требования:

- АБ определяет политику изменения учётных данных пользователей и периодически контролирует ее соблюдение;
- АБ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;
- изменение учётных данных пользователя производится АБ по требованию ответственного за обработку персональных данных в структурном подразделении, а также периодически по утвержденному плану и в случае увольнения работника;
- АБ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБ обязан потребовать у пользователя изменение пароля.

5.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ)

АБ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей ИСПДн, АБ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

5.3. Антивирусная защита ресурсов ИСПДн

АБ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;
- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей ИСПДн о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;
- имеет право на проведение внеплановой проверки на наличие вирусов;
- периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

5.4. Хранение дистрибутивов программного обеспечения СЗИ

АБ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПДн Администрации города Салехарда в месте, исключающем доступ посторонних лиц.

5.5. Проверка целостности системного и прикладного ПО

Контролю целостности подлежат файлы ПО ИСПДн с расширениями: *.exe, *.com, *.dll, *.sys, *.vxd,*.drv.

5.6. Конфигурирование ИСПДн

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями и непосредственной реализация конфигурации осуществляет АБ.

В ходе управления конфигурацией аттестованной ИСПДн и ее системы защиты информации АБ обязан осуществлять:

– поддержание конфигурации ИСПДн и ее системы защиты информации (структуры системы защиты информации ИСПДн, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПДн и ее системы защиты информации);

– управление изменениями базовой конфигурации ИСПДн и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПДн и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПДн и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

– определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПДн и ее системы защиты информации в документацию на систему защиты информации ИСПДн;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБ. При возникновении необходимости изменения конфигурации ИСПДн, аттестованной по требованиям безопасности информации, АБ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

5.7. Вывод ресурсов ИСПДн из эксплуатации

При невозможности ремонта различных ресурсов ИСПДн АБ обязан:

- физически уничтожать любые машинные носители, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПДн;

- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИСПДн.

5.8. Реагирование на сбои при регистрации событий безопасности

Реагирование на сбои при регистрации событий безопасности осуществляется АБ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности, АБ обязан:

- немедленно уведомить ответственного за организацию безопасности персональных данных Администрации города о данном факте;

- по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;

- восстановить работоспособность ИСПДн;

− по окончании работ по восстановлению работоспособности ИСПДн произвести запись в соответствующих журналах.

## 6. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1. К попыткам несанкционированного доступа относятся:

− сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

− действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи АБ или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учётной записи или любым другим методом.

6.2. При выявлении факта несанкционированного доступа АБ обязан:

− пресечь дальнейший несанкционированный доступ к ИСПДн;

− доложить ответственному за обеспечение безопасности персональных данных о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

− известить ответственного за обработку персональных данных в структурном подразделении, в котором работает пользователь ИСПДн, от имени учётной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

## 7. ОТВЕТСТВЕННОСТЬ

7.1. АБ несет персональную ответственность за:

− сохранность носителей информации и содержащейся на них информации в рабочее время;

− несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПДн;

− СЗИ, применяемые в ИСПДн Администрации города Салехарда;

− качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учётной записи АБ в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учётной записи.

7.2. АБ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 5
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

пользователя информационной системы персональных данных
в Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированное рабочее место (АРМ)** – это комплекс средств вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте работника и предназначенный для автоматизации его работы.

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

**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.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн) –** лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

**Безопасность информации** – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

**Доступ к информации** – возможность получения информации и ее использования.

**Несанкционированный доступ (НСД)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, представляемых АРМ.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) Администрации города Салехарда.

1.2. Пользователи ИСПДн (далее - пользователи) получает свои права на доступ к ресурсам ИСПДн через администратора информационной безопасности (далее - АБ).

1.3. Пользователи допускаются к работе на основании утвержденного списка пользователей ИСПДн в Администрации города Салехарда.

## 2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

**Пользователь обязан:**

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, а также настоящей Инструкцией.

2.2. Выполнять на закрепленном за этим пользователем автоматизированном рабочем месте (далее – АРМ) входящим в ИСПДн, обработку персональных данных в объеме, необходимом для его служебной деятельности, соблюдая при этом технологический процесс обработки персональных данных.

2.3. Знать и соблюдать установленные требования к обработке персональных данных, учёту и хранению носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.4. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

2.5. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

2.6. Незамедлительно, в кратчайшие срок, сообщать непосредственному руководителю об утрате или недостаче носителей информации, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению персональных данных.

2.7. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флэш-накопители, дискеты, компакт –диски, документы, черновики, распечатки на принтерах и т.п.), передать непосредственному руководителю.

2.8. Соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты информационных систем персональных данных в Администрации города Салехарда».

2.9. Соблюдать требования антивирусной защиты в соответствии с «Инструкцией по организации антивирусной защиты информационных систем персональных данных в Администрации города Салехарда».

2.10. Получить уникальное имя пользователя и персональный идентификатор (при его наличии) от АБ. Знать и соблюдать в тайне свое имя пользователя и пароль, не допускать их запись на каких-либо носителях в целях напоминания.

2.11. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть закрыты.

2.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и

звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

2.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения выполнить следующие мероприятия:

2.8.1. приостановить обработку данных;

2.8.2 немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

2.8.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

2.8.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ).

2.9. Немедленно вызывать АБ и поставить в известность ответственного за обработку персональных данных в своем структурном подразделение при обнаружении:

2.9.1. нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

2.9.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

2.9.3. 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.), а также перебоев в системе электроснабжения;

2.9.4. некорректного функционирования установленных на АРМ технических средств защиты;

2.9.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

2.10. При утере или подозрении на утечку сведений о своем имени пользователя, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

2.11. Обо всех выявленных нарушениях, связанных с информационной безопасностью в Администрации города Салехарда, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

2.12. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

Пользователю **ЗАПРЕЩАЕТСЯ**:

– разглашать защищаемую информацию посторонним лицам;

– копировать защищаемую информацию на неучтенные внешние носители;

– самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

– подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПДн;

– сообщать (или передавать) посторонним лицам параметры своей учётной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;

– оставлять без присмотра и передавать другим лицам персональный идентификатор;

– привлекать посторонних лиц для ремонта или настройки АРМ без согласования с АБ;

– оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

– самостоятельно создавать совместно используемые сетевые ресурсы (папки общего доступа);

– вести обработки персональных данных на АРМ другого пользователя, если иное не оговорено оператором при его назначении;

– использовать в работе персональные данные субъектов, выходящие за рамки служебной деятельности пользователя;

– удалять или искажать программы и защищаемую информацию;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

## 3. ПОРЯДОК РАБОТЫ ПОЛЬЗОВАТЕЛЯ С РЕСУРСАМИ ИСПДн

3.1. Начало работы на АРМ

3.1.1. При включении АРМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ;

3.1.2. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБ.

3.2. Завершение работы на АРМ

3.2.1. По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения АРМ), либо завершить работу АРМ стандартным способом (при этом выключить АРМ).

3.3. Требования к распечатыванию информации

3.3.1. Все распечатываемые документы должны быть учтены;

3.3.2. Бракованные бумажные носители и черновики документов должны быть уничтожены;

3.3.3. При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

## 4. ПРАВА ПОЛЬЗОВАТЕЛЯ

Пользователь имеет право:

4.1. Обращаться к администратору информационной безопасности, ответственному за обработки персональных данных в своем структурном подразделении для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных.

4.2. Направлять предложения по установке нового (а также дополнительного) программного обеспечения.

4.3. Направлять предложения по модернизации АРМ, входящих в ИСПДн.

4.4. Получать консультации и разъяснения по нормативным документам, регламентирующими работу с персональными данными в Администрации города Салехарда.

4.5. Иметь доступ к информационным ресурсам персональных данных ИСПДн, вести обработку персональных данных и использовать их в работе в объеме, необходимом для осуществления своей служебной деятельности.

## 5. ОТВЕТСТВЕННОСТЬ

5.1. Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время);

– соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПДн и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. За разглашение ПДн и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 6
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**
по организации антивирусной защиты
информационных систем персональных данных в
Администрации города Салехарда

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированное рабочее место (АРМ)** – это комплекс средств вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте работника и предназначенный для автоматизации его работы.

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

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

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

## ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) Администрации города Салехарда от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора информационной безопасности (далее – АБ) и других должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПДн, за выполнение указанных требований.

1.2. К использованию в Администрации города Салехарда допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на автоматизированные рабочие места (далее – АРМ) и сервера ИСПДн Администрации города Салехарда осуществляется АБ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК России в области защиты персональных данных.

## ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

1.4. Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль дисков и файлов АРМ.

1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съёмных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

1.6. Процедура обновления баз данных средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПДн, работающих в сети, не реже одного раза в неделю для всех АРМ ИСПДн, работающих автономно.

1.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПДн.

1.8. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

## ОТВЕТСТВЕННОСТЬ

3.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПДн Администрации города Салехарда в соответствии с требованиями настоящей Инструкции возлагается на АБ и всех должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПДн Администрации города Салехарда.

3.2. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а так же проверка работоспособности средств антивирусной защиты) в ИСПДн Администрации города Салехарда, осуществляется АБ и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИСПДн Администрации города Салехарда.

Приложение № 7
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

по организации парольной защиты
информационных систем персональных данных в
Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн) –** лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Администрации города Салехарда, а также контроль над действиями пользователей ИСПДн и обслуживающего персонала системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности.

## 2. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДн самостоятельно с учётом следующих требований:

2.1.1. длина пароля должна быть не менее 6 символов;

2.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

2.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, АРМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

2.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях;

2.1.5. допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

2.2. В случае если формирование личных паролей пользователей ИСПДн осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

## 3. ВВОД ПАРОЛЯ

3.1. При вводе пароля пользователю ИСПДн необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2. При неверном вводе пароля более 5 раз, учётная запись пользователя ИСПДн должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

## 4. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем ИСПДн.

4.2. В случае прекращения полномочий пользователя ИСПДн (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя ИСПДн с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администратора информационной безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Временный пароль, заданный администратором информационной безопасности при регистрации нового пользователя ИСПДн, должен действовать в течение ограниченного срока времени. Пользователь ИСПДн должен изменить временный пароль при первом входе в систему.

## 5. ХРАНЕНИЕ ПАРОЛЯ

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

5.2. Запрещается сообщать свой пароль полностью или частично другим пользователям ИСПДн, запрещается спрашивать или подсматривать пароль других пользователей ИСПДн.

5.3. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учётной записью и паролем другого пользователя ИСПДн.

## 6. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

6.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя ИСПДн должна быть немедленно проведена внеплановая процедура смены пароля.

## 7. ОТВЕТСТВЕННОСТЬ

7.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учётной записи.

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты возлагается на администратора информационной безопасности.

7.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 8
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

по организации резервирования и восстановления
программного обеспечения, баз персональных данных в информационных системах
персональных данных Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн)** – лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

## 1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1.1. Настоящая Инструкция определяет действия связанные с функционированием информационных систем персональных данных (далее – ИСПДн) Администрации города Салехарда, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачей данной Инструкции является:

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

1.4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

1.5. Ответственным работником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор информационной безопасности.

1.6. Ответственным работником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается ответственный за обработку персональных данных в структурном подразделении.

## 1. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

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

2.2. Происшествие, вызывающее инцидент, может произойти:

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

2.3. В кратчайшие сроки, не превышающие одного рабочего дня, администратором информационной безопасности, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

## 3. МЕРЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ РАБОТЫ И ВОССТАНОВЛЕНИЯ РЕСУРСОВ

3.1. Технические меры

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

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

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;
- системы резервного питания.

3.1.2. Помещения, в которых размещаются элементы ИСПДн должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

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

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

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

3.1.6. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.1.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий диск, USB-накопитель и т.п.).

3.2. Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществляться:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение) с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учёта.

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

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

3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.

## 4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственность за поддержание установленного в настоящей инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных в информационной системе персональных данных Администрации города Салехарда возлагается на администратора информационной безопасности.

Приложение № 9
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**

о порядке доступа в помещения Администрации города Салехарда,
в которых ведётся обработка персональных данных

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированное рабочее место (АРМ)** – это комплекс средств вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте работника и предназначенный для автоматизации его работы.

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

**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.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 .Настоящая Инструкция разработана в соответствии с Федеральными законами от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлениями Правительства Российской Федерации от 21 марта 2012 года № 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 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными правовыми актами, которые регулируют отношения, связанные с защитой персональных данных, в целях обеспечения защиты персональных данных.

1.2 .Положения данной Инструкции обязательны для выполнения всеми работниками Администрации города Салехарда (далее – работники), которые выполняют работы, связанные с обработкой и хранением персональных данных с использованием и без использования средств автоматизации.

1.3 .Ответственным за организацию доступа в помещения Администрации города Салехарда, в которых ведется обработка персональных данных (далее – ПДн), является ответственный за обработку персональных данных в структурном подразделении.

1.4 .Работники, доступ которых к ПДн необходим для выполнения служебных обязанностей, допускаются к таким данным на основании утверждённого Перечня должностей работников Администрации города Салехарда, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ним.

## 2. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ПРЕДОТВРАЩЕНИЮ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ПОМЕЩЕНИЯ АДМИНИСТРАЦИИ ГОРОДА, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Размещение технических средств информационных систем персональных данных (устройств и носителей информации), наличие специального оборудования и охраны помещений, в которых ведется работа с ПДн (далее – помещения), режима обеспечения безопасности в этих помещениях, предусматривающего контроль доступа в них, должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.2. В отсутствии лиц, допущенных к работе с ПДн, входные двери помещений должны быть закрыты на ключ.

2.3. Пользователи, допущенные в установленном порядке к работе с ПДн в информационных системах персональных данных и прошедшие инструктаж по основам обеспечения режимных требований обязаны:

2.4.1. При уборке помещений посторонними лицами:

- прекратить работу на АРМ и выключить монитор;
- убрать материальные и съёмные носители ПДн, документы с рабочего стола в сейфы;
- сейфы закрыть на ключ;
- визуально проверить содержимое урн на наличие черновиков документов с ПДн. Уничтожение черновиков производить в бумагорезательных машинах установленным порядком.

2.4.2. При проведении мероприятий по обработке ПДн:

- обеспечить безопасность ПДн при их обработке;
- окна помещений закрыть шторами (жалюзи);

− исключить обзор мониторов АРМ посторонними лицами (посетителями), в том числе сотрудниками, не допущенными к работе с ПДн;

− исключить бесконтрольное пребывание в помещениях посторонних лиц (посетителей) с целью предотвращения неправомерного или случайного доступа к ПДн, их уничтожения, изменения, блокирования, копирования и распространения.

2.4.3. По окончании рабочего дня и перед закрытием помещений осмотреть и проверить:

− закрытие окон;

− выключение электроприборов и освещения;

− выключение основных технических средств обработки информации;

− закрытие и опечатывание всех сейфов;

− работоспособность пожарной и охранной сигнализации.

2.4. Нахождение в помещениях посторонних лиц, в том числе посетителей, в часы начала и окончания работы подразделений не допускается.

2.5. В нерабочее время, перед выходными и праздничными днями помещения опечатываются и сдаются под охрану. Ключи в опечатанном виде сдаются под роспись в книге приема и сдачи служебных помещений под охрану.

## 3. ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ АДМИНИСТРАЦИИ ГОРОДА, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Доступ в помещения работников, указанных пунктах 1.3 и 1.4, осуществляется после проверки помещений и снятия их с охранной сигнализации.

3.2. Доступ и нахождение в помещениях работников в нерабочее время, в выходные и праздничные дни допускается только с письменного разрешения руководителя подразделения.

3.3. Доступ в помещения граждан (посетителей) в рамках служебной деятельности подразделений осуществляется в рабочее время в установленные часы приёма посетителей. Доступ в помещения посетителей регулируется пользователем ИСПДн, осуществляющим приём граждан. Приём граждан производится по одному человеку и с его разрешения. Коллективные приёмы посетителей не допускаются.

3.4. Доступ в помещения и прием иностранных граждан не допускается. В исключительных случаях такой прием возможен только по распоряжению Главы Администрации города или его заместителя и согласованию с отделом специальных мероприятий Администрации города.

3.5. Доступ в помещения и нахождение в них должностных лиц Роскомнадзора (прокуратуры, следственных органов) разрешается по указанию Главы Администрации города или его заместителя с целью проведения ими проверочных мероприятий в рамках государственного контроля (надзора) деятельности Администрации города в сфере обработки ПДн.

3.6. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных в структурном подразделении.

## 4. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ УСТАНОВЛЕННОГО ПОРЯДКА ДОСТУПА

4.1. За нарушение требований к обеспечению безопасности ПДн при их обработке в АРМ, включая информационные системы персональных данных, за нарушение прав субъектов ПДн, установленных Федеральным законодательством и иными нормативными правовыми актами Российской Федерации, приведшее к несанкционированному, в том числе случайному, доступу к ПДн, повлёкшему уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия, предусмотрено наказание в соответствии с действующим законодательством Российской Федерации.

Приложение № 10
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**
по порядку учёта, хранения и уничтожения персональных данных
в Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**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.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Все информационные ресурсы, содержащие персональные данные, подлежат учёту.

1.2. Учёт осуществляется по журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники.

1.3. Ведется Перечень информационных ресурсов, содержащих персональные данные (далее - ПДн).

1.4. В журнале указываются следующие реквизиты информационных ресурсов, содержащих персональные данные: учётный номер и дата поступления, откуда поступил, срок обработки, а также другие возможные реквизиты, идентифицирующие информационный ресурс.

1.5. Носители информационных ресурсов, содержащих персональные данные, должны сдаваться на хранение.

## ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные субъекта ПДн хранятся в подразделении Администрации города Салехарда, которое их обработку отвечает за взаимодействие с субъектом.

2.2. ПДн на бумажном носителе хранятся в папках в сейфе или в металлическом шкафу.

2.3. Персональные данные субъекта ПДн в электронном виде хранятся в локализованных электронных базах данных компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные субъекта, обеспечиваются системой защиты персональных данных.

2.4. В нерабочее время помещение, где хранятся ПДн (хранилище ПДн), должно закрываться на ключ. В рабочее время, в случае ухода ответственного за обработку персональных данных в структурном подразделении, помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных ответственным за обработку персональных данных в структурном подразделении.

2.5. Работник Администрации города Салехарда, имеющий доступ к персональным данным субъектов ПДн, в связи с исполнением трудовых обязанностей, обеспечивает хранение информации, содержащей персональные данные субъекта, исключающее доступ к ним третьих лиц.

2.6. В отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов (соблюдение "политики чистых столов").

2.7. При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные субъектов ПДн лицу, на которое распоряжением будет возложено исполнение его трудовых обязанностей.

2.8. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные субъектов ПДн по указанию ответственного за обработку персональных данных в структурном подразделении, передаются другому работнику, имеющему доступ к персональным данным субъектов ПДн.

2.9. При увольнении работника, имеющего доступ к персональным данным субъектов ПДн, документы и иные носители, содержащие персональные данные субъектов ПДн, по указанию ответственного за обработку персональных данных передаются другому работнику, имеющему доступ к персональным данным субъектов ПДн.

2.10. Повседневный контроль за выполнением требований по защите хранилищ ПДн ответственный за обработку персональных данных в структурном подразделении.

2.11. Периодический контроль эффективности мер защиты хранилищ ПДн осуществляется комиссией, создаваемой распоряжением Администрации города Салехарда.

2.12. Уничтожение персональных данных субъектов ПДн на бумажном носителе, либо удаление электронных базах данных, содержащих персональные данные субъектов ПДн в электронном виде, осуществляется по истечении установленного срока обработки ПДн комиссией, создаваемой распоряжением Администрации города Салехарда.

## 3. ОТВЕТСТВЕННОСТЬ

3.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 11
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**
по порядку учёта, хранения съёмных носителей персональных данных
в Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Все находящиеся на хранении и в обращении съёмные носители ПДн подлежат учёту.

1.2. Носители информационных ресурсов, содержащих персональные данные, должны сдаваться на хранение.

## 2. ПОРЯДОК ИСПОЛЬЗОВАНИЯ СЪЁМНЫХ НОСИТЕЛЕЙ ПДн

2.1. Под использованием съёмных носителей ПДн при работе в ИСПДн понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между ИСПДн и носителями информации.

2.2. В ИСПДн допускается использование только учтенных съёмных носителей ПДн, которые являются собственностью Администрации города Салехарда и подвергаются регулярной ревизии и контролю.

2.3. К съёмным носителям ПДн предъявляются те же требования информационной безопасности, что и для стационарных автоматизированных рабочих мест (целесообразность дополнительных мер обеспечения информационной безопасности определяется администратором информационной безопасности).

2.4. Съёмные носители ПДн предоставляются работникам по инициативе ответственных за обработку персональных данных в структурном подразделении в случаях:

- необходимости выполнения вновь принятыми работникам своих должностных обязанностей;
- возникновения производственной необходимости по обработки ПДн.

## 3. ПОРЯДОК УЧЁТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЁМНЫМИ НОСИТЕЛЯМИ ПДн

3.1. Все находящиеся на хранении и в обращении съёмные носители ПДн подлежат учёту.

3.2. Каждый съёмный носитель ПДн с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учётный номер.

3.3. Учёт и выдачу съёмных носителей ПДн осуществляет администратор информационной безопасности. Факт выдачи съемного носителя ПДн фиксируется в журнале учёта съёмных носителей ПДн.

3.4. Работники получают учтенный съёмный носитель ПДн от уполномоченного работника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учёта. По окончании работ пользователь сдает съёмный носитель ПДн для хранения уполномоченному работнику, о чем делается соответствующая запись в журнале учёта.

3.5. При использовании работниками съёмных носителей ПДн необходимо:

3.5.1. Соблюдать требования настоящей Инструкции;

3.5.2. Использовать съёмные носители ПДн исключительно для выполнения своих служебных обязанностей;

3.5.3. Ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;

3.5.4. Бережно относится к съёмным носителям ПДн;

3.5.5. Обеспечивать физическую безопасность съёмным носителям ПДн всеми разумными способами;

3.5.6. Извещать администратора информационной безопасности о фактах утраты (кражи) съемного носителя ПДн.

3.6. При использовании съёмных носителей ПДн **запрещено**:

3.6.1. Использовать съёмные носители ПДн в личных целях;

3.6.2. Передавать съёмные носители ПДн другим лицам (за исключением администратора безопасности);

3.6.3. Хранить съёмные носители ПДн вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

3.6.4. Выносить съёмные носители ПДн из служебных помещений для работы с ними на дому и т. д.

3.7. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником между ИСПДн и неучтенными (личными) съёмными носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администратором информационной безопасности заранее). Администратор информационной безопасности оставляет за собой право блокировать или ограничивать использование съёмных носителей информации.

3.8. Информация об использовании работником х носителей ПДн в ИСПДн протоколируется и, при необходимости, может быть предоставлена администратором информационной безопасности.

3.9. В случае выявления фактов несанкционированного и/или нецелевого использовании съёмных носителей ПДн инициализируется служебная проверка, проводимая комиссией, создаваемой распоряжением Администрации города Салехарда (далее – комиссия).

3.10. По факту выясненных обстоятельств, комиссия составляется акт расследования инцидента и передается Главе Администрации города для принятия мер согласно действующему законодательству Российской Федерации.

3.11. Информация, хранящаяся на съёмных носителях ПДн, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

3.12. При отправке или передаче персональных данных адресатам на съёмные носители ПДн записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съёмных носителях ПДн осуществляется в порядке, установленном для документов для служебного пользования.

3.13. Вынос съёмных носителей ПДн для непосредственной передачи адресату осуществляется только с письменного разрешения администратора информационной безопасности.

3.14. В случае утраты или уничтожения съёмных носителей ПДн либо разглашении содержащихся в них сведений немедленно ставится в известность администратор информационной безопасности. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учёта бумажных и съёмных носителей ПДн.

3.15. Съёмные носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съёмных носителей ПДн осуществляется комиссии. По результатам уничтожения съёмных носителей ПДн составляется акт уничтожения ПДн.

3.16. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные съёмные носители ПДн изымаются.

## 4. ОТВЕТСТВЕННОСТЬ

4.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 12
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**И Н С Т Р У К Ц И Я**
по модификации технических и программных
средств в информационных системах персональных данных
Администрации города Салехарда

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированное рабочее место (АРМ)** – это комплекс средств вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте работника и предназначенный для автоматизации его работы.

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

**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.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Администратор информационной безопасности** – лицо, ответственное за защиту автоматизированных рабочих мест от несанкционированного доступа к информации.

**Пользователь информационной системы персональных данных (ИСПДн) –** лицо, назначаемое оператором для непосредственной обработки персональных данных в объеме служебной деятельности с использованием информационной системы персональных данных, а также результатов ее функционирования.

**Безопасность информации** – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

**Доступ к информации** – возможность получения информации и ее использования.

**Несанкционированный доступ (НСД)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, представляемых АРМ.

# 1. ПОРЯДОК ИЗМЕНЕНИЯ КОНФИГУРАЦИИ ТЕХНИЧЕСКИХ И ПРОГРАММНЫХ СРЕДСТВ

1.1. Настоящая Инструкция регламентирует обеспечение безопасности информации при проведении обновления (модификации) общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе информационных системах персональных данных (далее – ИСПДн) Администрации города Салехарда.

1.2. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется по согласованию с органом аттестации, проводившим аттестацию данной ИСПДн, а именно:

- в отношении системных и прикладных программных средств – администратору информационной безопасности;
- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору информационной безопасности.

1.3. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора информационной безопасности ***ЗАПРЕЩЕНО***.

1.4. Внесение всех изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется заявкой ответственного за обработку персональных данных в структурном подразделении (далее - ответственный в структурном подразделении). Форма заявки приведена в приложении № 1.

1.5. В заявке могут указываться следующие виды необходимых изменений в состав аппаратных и программных средств ИСПДн:

- установка (развертывания) на автоматизированном рабочем месте (далее – АРМ) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ);
- обновление (замена) на АРМ программных средств, необходимых для решения определенной задачи (обновление версий программ используемых для решения определенных задач);

удаление с АРМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной АРМ).

1.6. Заявку пользователя ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает ответственный в структурном подразделении, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору информационной безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию ИСПДн, указанного в заявке АРМ.

1.7. Подготовка обновления (модификации) общесистемного и прикладного программного обеспечения ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производятся администратором информационной безопасности по согласованию с органом по аттестации, проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного в структурном подразделении.

1.8. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

1.9. Установка или обновление программного обеспечения (далее – ПО) на ИСПДн производится с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком.

1.10. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, и, насколько это возможно, на отсутствие опасных функций.

1.11. После установки (обновления) ПО администратор информационной безопасности должен произвести требуемые настройки средств управления доступом к компонентам ИСПДн и проверить работоспособность ПО, правильность их настройки. Администратор информационной безопасности делает отметку о выполнении на обратной стороне заявки (Приложение № 2) и в техническом паспорте на ИСПДн.

1.12. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств АРМ, с отметками о внесении изменений в состав программных средств должны храниться вместе с техническим паспортом на ИСПДн у администратора информационной безопасности. Эти документы могут впоследствии использоваться:

- для восстановления конфигурации АРМ после аварий;
- для контроля правомерности установки на АРМ средств, для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты АРМ.

1.13. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора информационной безопасности и ответственным в структурном подразделение.

1.14. С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе на АРМ конкретной ИСПДн, должно соответствовать персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать на данном АРМ.

1.15. Использование несколькими работниками одного и того же имени пользователя («группового имени») при работе в ИСПДн ***ЗАПРЕЩЕНО.***

1.16. Процедура регистрации (создания учётной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного в структурном подразделении.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учётной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учётной записи) данного работника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

1.17. Заявку рассматривает ответственный в структурном подразделение, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору информационной безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

1.18. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор информационной безопасности производит необходимые операции по созданию (удалению) учётной записи пользователя ИСПДн, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей ИСПДн должен быть установлен режим принудительного запроса смены пароля для доступа к ресурсам ИСПДн, не реже одного раза в 3 месяца.

1.19. После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения

изменений в списки пользователей ИСПДн в заявке делается отметка о выполнении задания за подписью исполнителя – администратор информационной безопасности.

1.20. Работнику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается соответствующее ему имя пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (- ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

1.21. Исполненные заявка и задание (за подписью администратора безопасности ИСПДн) передаются руководителю на хранение.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;

- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

- для проверки работниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

**Приложение № 1**
**ОБРАЗЕЦ**

**ЗАЯВКА**
**на внесение изменений в состав аппаратно-программных средств ИСПДн АРМ**

Прошу произвести следующие изменения конфигурации программных (аппаратно-программных) средств ИСПДн АРМ_____:
наименование АРМ
установить (обновить, удалить) новое программное обеспечение (аппаратно-программные средства, компоненты):

_____

_____

_____,

необходимые для решения следующих задач:

_____

_____

_____

_____

_____

_____

Ответственный за обработку персональных данных в структурном подразделение _____
(подпись, фамилия, инициалы)

«___» _____ 20_____года

**Приложение № 2**
**ОБРАЗЕЦ**
*Обратная сторона заявки*

**Отметка о выполнении**
**(о внесении изменений в состав аппаратно-программных средств АРМ)**

В соответствии с «Инструкцией по модификации технических и программных средств в информационных системах персональных данных Администрации города Салехарда» рабочей группой в составе:

Администратор информационной безопасности_____
Ответственный за обработку персональных данных в структурном подразделении _____
_____
Пользователь ИСПДн_____

указанные в заявке изменения внесены (не внесены по следующей причине):_____
_____
краткое описание причины
_____
_____
_____
Изменения в технический паспорт на АРМ (ссылка на данную заявку) внесены.
Администратор информационной безопасности _____
(подпись, фамилия, инициалы)

Ответственный за обработку персональных
данных в структурном подразделение _____
(подпись, фамилия, инициалы)

Пользователь ИСПДн _____
(подпись, фамилия, инициалы)

«___» _____ 20_____года

Приложение № 13
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**ЖУРНАЛ УЧЁТА**
**ДОПУСКА К РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ**
**ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**
**АДМИНСТРАЦИИ ГОРОДА САЛЕХАРДА**

Начат «___» _____20__ г.

Окончен «___» _____20__ г.

На _____листах

| _____ | _____ | _____ |
|---|---|---|
| (должность руководителя) | (подпись) | (Фамилия И.О.) |
| | М.П. | |

| № п/п | Сведения о допуске к персональным данным | | | | Сведения о прекращении допуска к персональным данным | |
|---|---|---|---|---|---|---|
| | Наименование информационной системы персональных данных | ФИО, должность получившего допуск | Дата и номер приказа о допуске | Дата и подпись допускаемого лица | Дата и номер приказа о прекращении допуска | Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |
| 7. | | | | | | |
| 8. | | | | | | |
| 9. | | | | | | |
| 10. | | | | | | |
| 11. | | | | | | |
| 12. | | | | | | |
| 13. | | | | | | |
| 14. | | | | | | |

Приложение № 14
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**ЖУРНАЛ УЧЁТА**
**ЗАЩИЩАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ**
**АДМИНИСТРАЦИИ ГОРОДА САЛЕХАРДА**

Начат «___» _____20___г.

Окончен «___» _____20___ г.

На _____листах

| _____ | _____ | _____ |
|---|---|---|
| (должность руководителя) | (подпись) | (Фамилия И.О.) |
| | М.П. | |

| Регистрационный номер, дата регистрации | Тип защищаемого носителя информации (заводской номер) | Назначение (содержимое) носителя | Расписка в получении (Ф.И.О., подпись, дата) | Расписка об обратном приёме (Ф.И.О., подпись, дата) | Местонахождение (хранение) носителя, Ф.И.О. ответственного | Уничтожение носителя (№ и дата акта), отметка об отправке (№ и дата сопр. письма) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Приложение № 15
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**ЖУРНАЛ УЧЁТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, ИСПОЛЬЗУЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ГОРОДА САЛЕХАРДА**

Начат «___» _____20___г.

Окончен «___» _____20___ г.

На _____листах

| _____ | _____ | _____ |
|---|---|---|
| (должность руководителя) | (подпись) | (Фамилия И.О.) |
| | М.П. | |

Приложение № 16
к распоряжению Администрации
города Салехарда
от 26 января 2016 г. № 104-р

**ЖУРНАЛ УЧЁТА ПРОВОДИМЫХ ВНУТРЕННИХ ПРОВЕРОК**

**АДМИНСТРАЦИИ ГОРОДА САЛЕХАРДА**

Начат «___»_____20__ г.

Окончен «___»_____20__ г.

На _____листах

| _____ | _____ | _____ |
|---|---|---|
| (должность руководителя) | (подпись) | (Фамилия И.О.) |
| | М.П. | |

| № п/п | Наименование внутренней проверки | Краткое описание | Дата проведения проверки | Подпись ответственного за контроль эффективности мер по защите информации | Примечание |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |