

МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ

СЕЛЬСКОЕ ПОСЕЛЕНИЕ ШАПША

Ханты-Мансийский автономный округ – Югра

**АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ ШАПША**

**РАСПОРЯЖЕНИЕ**

от 09.12.2015 № 234-р

*д. Шапша*

Об организации работ по обеспечению безопасности

персональных данных при их обработке, в том числе

в информационных системах персональных данных

в администрации сельского поселения Шапша

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Утвердить:

1.1. Инструкцию администратора информационной безопасности в информационных системах персональных данных администрации сельского поселения Шапша согласно приложению 1;

1.2. Инструкцию по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных администрации сельского поселения Шапша согласно приложению 2;

1.3. Инструкцию ответственного за эксплуатацию информационной системы персональных данных администрации сельского поселения Шапша согласно приложению 3;

1.4. Инструкцию по организации парольной защиты в информационных системах персональных данных администрации сельского поселения Шапша согласно приложению 4;

1.5. Инструкцию по организации антивирусной защиты в информационных системах персональных данных администрации сельского поселения Шапша согласно приложению 5;

1.6. Инструкцию по организации резервирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных администрации сельского поселения Шапша согласно приложению 6;

1.7. Инструкцию о порядке работы пользователей информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации сельского поселения Шапша согласно приложению 7;

1.8. Инструкцию о порядке проверки электронного журнала обращений к информационным системам персональных данных администрации сельского поселения Шапша согласно приложению 8;

1.9. Инструкцию работнику, ведущему обработку персональных данных без использования средств автоматизации администрации сельского поселения Шапша согласно приложению 9;

1.10. Перечень должностей администрации сельского поселения Шапша, доступ которых к персональным данным, обрабатываемых в информационных системах персональных данных, необходим для выполнения должностных обязанностей, согласно приложению 10;

1.11. Перечень должностей администрации сельского поселения Шапша, обрабатывающих персональные данные без использования средств автоматизации, согласно приложению 11;

1.12. Форму обязательства о неразглашении информации, содержащей персональные данные, согласно приложению 12.

2. Работникам администрации сельского поселения Шапша, осуществляющим обработку персональных данных без использования средств автоматизации, руководствоваться инструкцией по обработке персональных данных без использования средств автоматизации согласно приложению 9.

3. Контроль за выполнением распоряжения оставляю за собой.

Глава сельского поселения Шапша Л.А.Овчерюкова

Приложение 1

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
администратора информационной безопасности в информационных системах персональных данных администрации

сельского поселения Шапша

I. Общие положения

 1. Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) администрации сельского поселения Шапша.

2. Используемые основные понятия:

Оператор – администрация сельского поселения Шапша, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью [персональных данных](http://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5);

администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности ПДн (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

3. Администратор информационной безопасности (далее – Администратор) назначается из числа работников Оператора в соответствии с распоряжением (приказом) Оператора.

4. Администратор в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности ПДн при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

II. Обязанности администратора информационной безопасности

 1.Администратор обязан:

1.1. Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн при их обработке в ИСПДн.

1.2. Знать перечень обрабатываемых ПДн, состав, структуру,

назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

1.3. Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование.

1.4. Еженедельно осуществлять резервное копирование информации, содержащей ПДн.

1.5. Обязан осуществлять периодический контроль за выполнением работниками Оператора, эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

1.6. Участвовать в работе комиссий внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

1.7. Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к ИСПДн согласно приложению 10 к распоряжению.

 1.8. Обязан немедленно сообщать ответственному за организацию обработки ПДн информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

установить причины, по которым стал возможным НСД;

установить последствия, к которым привел НСД;

зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

провести проверку настроек средств защиты информации (СЗИ) и операционных систем (ОС) на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, принятой Оператором, при необходимости провести настройку;

провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты ПДн.

1.9. Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ.

 1.10. Обязан вести журнал учета средств защиты информации, эксплуатационной и технической документации к ним согласно приложению 1 к настоящей инструкции.

1.11. Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ.

1.12. Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты.

1.13. Обязан проводить мероприятия по организации антивирусной защиты согласно приложению 7 к распоряжению.

1.14. Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно приложению 4 к распоряжению.

1.15. Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации, согласно приложению 2 к настоящей инструкции.

1.16. Обязан вести журнал учета лиц, допущенных к работе с персональными данными в ИСПДн, согласно приложению 2 к распоряжению.

III. Права администратора информационной безопасности

 3.1. Администратор в ИСПДн имеет право:

3.1.1. Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн Оператора.

3.1.2. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.1.3. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к ответственному за организацию обработки ПДн в ИСПДн и/или ответственному за эксплуатацию ИСПДн.

IV. Ответственность Администратора информационной безопасности

1. На Администратора в ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн Оператора.

2. Администратор в ИСПДн несет ответственность в соответствии с действующим законодательством РФ.

Приложение 1

к инструкции администратора

информационной безопасности

в информационных системах

персональных данных администрации

сельского поселения Шапша

**ЖУРНАЛ**

**учета средств защиты информации,**

**эксплуатационной и технической документации к ним**

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

Приложение 2

к инструкции администратора

информационной безопасности

в информационных системах

персональных данных администрации

сельского поселения Шапша

**ЖУРНАЛ УЧЕТА**

**машинных носителей информации**

**администрации сельского поселения Шапша**

Начат: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.

Окончен: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.

На \_\_\_ листах

Срок хранения \_\_\_\_\_\_\_\_\_\_ лет

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата, учетный номер | Тип машинного носителя | Количество экземпляров | Расписка в получении | Расписка в обратном приеме | Место хранения машинного носителя | Отметка об уничтожении машинных носителей информации (номер и дата акта) |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Приложение 2

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ

по учету лиц, допущенных к работе с персональными данными
в информационных системах персональных данных
администрации сельского поселения Шапша

1. Настоящая инструкция разработана в соответствии с требованиями подпункта «в» пункта 13 Положения об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, и определяет порядок учета лиц, допущенных к работе с ПДн в информационных системах.

2. Используемые термины:

Оператор – администрация сельского поселения Шапша, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

3. Основанием для допуска работника к работе с ПДн является включение его в список допущенных лиц к обработке ПДн. Включение в список лиц, допущенных к работе с персональными данными, осуществляется распоряжением (приказом) Оператора, основанным на письменном ходатайстве руководителя структурного подразделения, согласованном с ответственным за организацию обработки ПДн Оператора.

4. Основанием для прекращения допуска работника к работе с ПДн является распоряжение (приказ) Оператора.

5. Учет лиц, допущенных к работе с ПДн в ИСПДн, ведется в журнале учета лиц, допущенных к работе с персональными данными в ИСПДн. Журнал учета лиц, допущенных к работе с ПДн в ИСПДн, учитывается в соответствии с правилами ведения делопроизводства и ведется администратором.

6. Форма журнала учета лиц, допущенных к работе с ПДн в ИСПДн, установлена приложением 1 к настоящей инструкции.

Приложение 1

к инструкции по учету лиц,

допущенных к работе

с персональными данными

в информационных системах

персональных данных администрации

сельского поселения Шапша

**Журнал**

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

**администрации сельского поселения Шапша**

|  |  |  |
| --- | --- | --- |
| № 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, номер распоряжения о допуске | дата и подпись допускаемого лица | дата, номер распоряжения о прекращении допуска | номер распоряжения об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 3

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
ответственного за эксплуатацию
информационной системы персональных данных
администрации сельского поселения Шапша

I. Общие положения

1. Настоящая инструкция определяет права и обязанности лица, ответственного за эксплуатацию информационной системы персональных данных (далее – ИСПДн) администрации сельского поселения Шапша по вопросам защиты информации в ИСПДн, используемой в работе структурного подразделения.

 2. Используемые термины:

Оператор – администрация сельского поселения Шапша, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

3. Ответственный за эксплуатацию ИСПДн назначается из числа работников Оператора, эксплуатирующих ИСПДн, и осуществляет контроль за соблюдением порядка работы пользователей ИСПДн дополнительно к своим непосредственным обязанностям.

4. Ответственный за эксплуатацию ИСПДн назначается распоряжением (приказом) Оператора.

II. Обязанности ответственного за эксплуатацию ИСПДн

 Ответственный за эксплуатацию ИСПДн обязан:

1. Знать перечень автоматизированных рабочих мест (далее – АРМ), входящих в состав ИСПДн, и перечень задач, решаемых с их использованием.
2. Обеспечивать периодический контроль за выполнением пользователями ИСПДн требований инструкций по обеспечению безопасности обработки ПДн;
3. Немедленно сообщать ответственному за обеспечение безопасности ПДн Оператора об обнаруженных фактах (попытках) несанкционированного доступа к информации и АРМ и принимать необходимые меры по пресечению нарушений.
4. Осуществлять контроль за правильностью использования и хранения машинных носителей информации и документов, содержащих ПДн.
5. Осуществлять контроль за правильностью использования и хранения персональных идентификаторов и личных паролей пользователями.
6. Разъяснять работникам структурного подразделения вопросы обеспечения информационной безопасности и правила работы с используемыми средствами зашиты информации.
7. Контролировать исполнение работниками структурного подразделения правил организации парольной защиты.
8. Контролировать использование работниками структурного подразделения средств защиты информации, установленных на АРМ, входящих в ИСПДн.
9. Обязан контролировать прохождение антивирусного контроля при применении машинных носителей информации.
10. Немедленно прекращать работы на АРМ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

III. Права ответственного за эксплуатацию ИСПДн

 Ответственный за эксплуатацию ИСПДн имеет право:

1. Требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации в ИСПДн.
2. Инициировать проведение служебных расследований по фактам нарушения требований защиты информации, утвержденных соответствующими инструкциями, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.
3. Подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы.

Приложение 4

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
по организации парольной защиты
в информационных системах персональных данных
администрации сельского поселения Шапша

 1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

 2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 6 символов;

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

символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущих;

пользователь не имеет права сообщать личный пароль другим лицам;

все используемые пароли должны ежемесячно сменяться на новые.

 3. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

 4. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. либо при наличии технологической необходимости использования имен и паролей работников (пользователей ИСПДн) в их отсутствие, работники обязаны при первой же возможности сменить разглашенный пароль на новый в соответствии с требованиями настоящей инструкции. Также сразу же после смены своих паролей, их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение администратору информационной безопасности в ИСПДн или руководителю структурного подразделения. Опечатанные конверты с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов должны применяться

личные печати владельцев паролей (при их наличии у пользователей).

 5. Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

 6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

 7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора информационной безопасности в ИСПДн.

 8. В случае компрометации (утеря, передача другому лицу) личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п. 5 или п. 6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

 9. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора информационной безопасности в ИСПДн.

Приложение 5

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
по организации антивирусной защиты
в информационных системах персональных данных
администрации сельского поселения Шапша

I. Общие требования

 1. Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все ИСПДн, существующие и вновь разрабатываемые в администрации поселения. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы ИСПДн.

 2. Используемые термины:

Оператор – администрация сельского поселения Шапша, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности персональных данных (далее – ПДн) (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

 3. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

 4. Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

II. Применение средств антивирусного контроля

1. При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых

приложений, находящихся в автозагрузке, реестра операционной системы.

 2. Полному антивирусному контролю автоматизированные рабочие места (АРМ) Оператора должны подвергаться не реже одного раза в неделю.

 3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

 4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

 5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ ИСПДн.

 6. При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

 7. В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов работник структурного подразделения обязан:

приостановить работу в ИСПДн;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов.

III. Ответственность

 1. Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение 6

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
по организации резервирования и восстановления

программного обеспечения и баз персональных данных
в информационных системах персональных данных
администрации сельского поселения Шапша

I. Общие положения

 1. Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

 2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности ИСПДн администрации поселения.

3. Используемые термины:

администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности персональных данных (далее – ПДн) (конфиденциальности, целостности и доступности) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн).

II. Резервируемое программное обеспечение

и базы персональных данных

 1. В ИСПДн резервированию подлежит:

общее программное обеспечение (операционная система и программные драйверы устройств (принтеры, мониторы, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

III. Порядок резервирования и хранения резервных копий

 1. Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

 2. Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

 3. Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

 4. Резервирование баз ПДн, а также текстовых и табличных файлов, содержащих ПДн, допускается только на учтенные установленным порядком машинные носители информации.

 5. Резервирование осуществляется ежемесячно, под контролем ответственных за эксплуатацию ИСПДн.

 6. Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации ПДн.

 7. К резервному носителю ПДн должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

 8. Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

 9. Копирование информации с резервных носителей ПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

IV. Порядок восстановления работоспособности ИСПДн

 1. Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

 2. Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

 3. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Приложение 7

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
о порядке работы пользователей
информационных систем персональных данных
в части обеспечения безопасности персональных данных
при их обработке в информационных системах персональных данных
администрации сельского поселения Шапша

 1. Настоящая инструкция определяет порядок действий пользователей информационных систем персональных данных (далее – ИСПДн) в части обеспечения безопасности персональных данных (далее – ПДн) при их обработке в ИСПДн.

2. Используемые термины:

Оператор – администрация сельского поселения Шапша, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

 3. Допуск пользователей для работы за автоматизированным рабочим местом (далее – АРМ) осуществляется на основании утверждаемого перечня должностей Оператора, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных обязанностей согласно приложению 10 к распоряжению.

 4. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения, транспортировки информации.

 5. Пользователь несет ответственность за правильность включения и выключения АРМ, входа в систему и все действия при работе в ИСПДн.

 6. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

 7. Запись информации, содержащей ПДн, может, осуществляется пользователем ИСПДн на съемные машинные носители информации, соответствующим образом учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения, транспортировки информации.

 8. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты согласно приложению 5 к распоряжению.

 9. Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки ПДн в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации ИСПДн;

знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме согласно приложению 4 к распоряжению;

хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

выполнять требования инструкции по организации антивирусной защиты в полном объеме согласно приложению 5 к распоряжению; немедленно известить администратора информационной безопасности в ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

1. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ ИСПДн;
2. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
3. некорректного функционирования установленных на АРМ технических средств защиты;
4. непредусмотренных отводов кабелей и подключенных устройств.

 10. Пользователю АРМ категорически запрещается:

использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию

аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.);

оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации с них.

Приложение 8

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
о порядке проверки электронного журнала обращений
к информационным системам персональных данных
администрации сельского поселения Шапша

I. Задачи аудита

 1. Под аудитом понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени. Общими задачами аудита являются:

контролирование состояния защищенности системы;

выявление причин произошедших изменений;

определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;

установление времени изменений.

 2. Аудит средств защиты осуществляет администратор информационной безопасности в ИСПДн.

3. Используемые термины:

администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности персональных данных (далее – ПДн) (конфиденциальности, целостности и доступности) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн).

II. Журналы записей о событиях

 1. События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

 2. Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

 3. В состав используемых в ИСПДн средств защиты информации должно входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее – программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

штатные журналы операционной системы Windows;

журналы событий средств защиты информации.

III. Штатные журналы операционной системы

 1. В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

 2. Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;

системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;

журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

 3. Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

 4. Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows – в оснастке «Просмотр событий» («Event viewer»).

IV. Журнал событий средств защиты информации

 1. Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

 V. Аудит

 1. Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.), подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

VI. Просмотр событий электронных журналов

 1. Администратор информационной безопасности в ИСПДн производит проверку электронных журналов ежемесячно с записью результатов проверок в журнал учета проверок электронных журналов обращений к ИСПДн.

 2. Форма журнала учета проверок электронных журналов обращений к ИСПДн представлена в приложении к настоящей инструкции.

 3. В случае обнаружения нарушений администратор

информационной безопасности в ИСПДн докладывает о данном факте ответственному за организацию обработки ПДн в ИСПДн администрации поселения.

Приложение

к инструкции о порядке проверки

электронного журнала обращений
к информационным системам

персональных данных администрации

сельского поселения Шапша

**ЖУРНАЛ**

**учета проверок электронных журналов обращений**

**к информационным системам персональных данных**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата проверки | Наименование ИСПДн, компьютера, технического средства | Наименование проверяемого журнала | Выявленные нарушения требований безопасности, нештатные ситуации | Подпись администратора безопасности | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 9

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ИНСТРУКЦИЯ
работнику, ведущему обработку персональных данных
без использования средств автоматизации
 администрации сельского поселения Шапша

I. Общие положения

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

 2. Обработка ПДн, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн осуществляются при непосредственном участии человека.

 3. Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в информационной системе ПДн либо были извлечены из нее.

 4. При обработке ПДн, осуществляемой без использования средств автоматизации, должны выполняться требования настоящей инструкции.

5. Используемые термины:

Оператор – администрация сельского поселения Шапша, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

II. Особенности организации обработки персональных данных

без средств автоматизации

 1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

 2. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

 3. Лица, осуществляющие обработку ПДн без использования средств автоматизации, в том числе работники Оператора или лица, осуществляющие такую обработку по договору с Оператором, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

 4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

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

типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку ПДн;

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

типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

 5. При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится Оператор, или в иных аналогичных целях должны соблюдаться следующие условия:

необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию Оператора, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Оператора.

 6. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

 7. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

 8. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

III. Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

 1. Обработка ПДн без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

 2. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

 3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

Приложение 10

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ПЕРЕЧЕНЬ

должностей администрации сельского поселения Шапша,
доступ которых к персональным данным, обрабатываемым

в информационных системах персональных данных,

необходим для выполнения служебных обязанностей

 1.Должности муниципальной службы:

 глава сельского поселения Шапша

главный специалист.

2. Должности, не отнесенные к должностям муниципальной службы, и осуществляющие техническое обеспечение деятельности администрации сельского поселения Шапша:

начальник организационно-технического сектора;

инспектор по делопроизводству;

главный бухгалтер финансово-экономического сектора;

бухгалтер;

экономист.

Приложение 11

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ПЕРЕЧЕНЬ

должностей администрации сельского поселения Шапша,
обрабатывающих персональные данные

без использования средств автоматизации

1.Должности муниципальной службы:

 глава сельского поселения Шапша

главный специалист.

2. Должности, не отнесенные к должностям муниципальной службы, и осуществляющие техническое обеспечение деятельности администрации сельского поселения Шапша:

начальник организационно-технического сектора;

инспектор по делопроизводству;

главный бухгалтер финансово-экономического сектора;

бухгалтер;

экономист.

Приложение 12

к распоряжению администрации

сельского поселения Шапша

от 09.12.2015 № 234-р

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (Ф.И.О.)паспорт серии\_\_\_, номер\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

« \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ года, исполняющий (-ая)  обязанности по должности в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
администрации сельского поселения Шапша, предупрежден (-а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.
3. Не использовать информацию, содержащую персональные данные, с целью получения личной выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (-а) о том, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

Дата Подпись