

**Муниципальное образование**

**Сельское поселение Сентябрьский**

**Нефтеюганский район**

**Ханты-Мансийский автономный округ – Югра**

**АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ СЕНТЯБРЬСКИЙ**

 **ПОСТАНОВЛЕНИЕ**

|  |  |  |
| --- | --- | --- |
| 23.08.2019 | № | 82-па |
|  |  |  |

п. Сентябрьский

О защите информации

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Возложить обязанности по защите информации:
	1. Назначить ответственным за организацию обработки персональных данных Главу сельского поселения Сентябрьский.
	2. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных (администратором информационной безопасности ИСПДн) заместителя главы поселения администрации сельского поселения Сентябрьский.
	3. Назначить ответственным за эксплуатацию ИС «СЭД Дело» администрации сельского поселения Сентябрьский специалиста по связям с общественностью 1 категории МКУ «Управление по делам администрации» .
	4. Утвердить перечень лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно [приложению 1](#Пр1) к настоящему постановлению.
	5. Утвердить перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн, в случае обезличивания ПДн и Перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно [приложению 2](#Пр2) к настоящему постановлению.
2. Создать комиссию по защите информации:
	1. Утвердить состав комиссии по защите информации согласно [приложению 3](#Пр4) к настоящему постановлению.
	2. Утвердить положение о комиссии по защите информации согласно [приложению 4](#Пр5) к настоящему постановлению.
3. Утвердить типовые формы документов по защите информации:
	1. Обязательство о неразглашении информации, содержащей персональные данные, типовую форму согласия субъекта на обработку их персональных данных и типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные, согласно [приложению 5](#пр8) к настоящему постановлению.
	2. Журналы по защите информации согласно [приложению 6](#Пр9) к настоящему постановлению.
	3. Акт определения уровня защищенности ПДн и класса защищенности ИС согласно [приложению 7](#Пр11) к настоящему постановлению.
	4. Акт об уничтожении персональных данных субъектов персональных данных согласно [приложению 8](#Пр10) к настоящему постановлению.
4. Утвердить перечень информационных систем персональных данных согласно [приложению 9](#Пр12) к настоящему постановлению.
5. Утвердить перечень обрабатываемых персональных данных согласно [приложению 10](#Пр13) к настоящему постановлению.
6. Утвердить положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения согласно [приложению 11](#Пр14) к настоящему постановлению.
7. Утвердить политику в отношении обработки персональных данных согласно [приложению 12](#Пр15).
8. Утвердить инструкции и правила по защите информации:
* Инструкцию ответственного за организацию обработки персональных данных согласно [приложению 13](#Пр16) к настоящему постановлению;
* Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно [приложению 14](#Пр19) к настоящему постановлению;
* Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно [приложению 15](#Пр31) к настоящему постановлению;
* Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно [приложению 16](#Пр18) к настоящему постановлению;
* Правила рассмотрения запросов субъектов персональных данных согласно [приложению 17](#Пр17) к настоящему постановлению;
* Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно [приложению 18](#Пр25) к настоящему постановлению;
* Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований согласно [приложению 19](#Пр24) к настоящему постановлению;
* Правила работы с обезличенными данными в случае обезличивания ПДн [приложению 20](#Пр24) к настоящему постановлению;
* Инструкцию по организации резервного копирования согласно [приложению 21](#Пр22_) к настоящему постановлению;
* Инструкцию по организации парольной защиты согласно
[приложению 22](#Пр21) к настоящему постановлению;
* Инструкцию по организации антивирусной защиты согласно
[приложению 23](#Пр22) к настоящему постановлению;
* Инструкцию о пропускном и внутриобъектовом режимах согласно [приложению 24](#Пр27) к настоящему постановлению;
* Инструкцию по работе с инцидентами информационной безопасности согласно [приложению 25](#Пр30) к настоящему постановлению;
1. Утвердить план мероприятий по защите информации согласно [приложению 26](#Пр32) к настоящему постановлению.

Глава поселения А.В. Светлаков

 Приложение 1

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

Перечень лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

| **№** | **Должность** | **Ф.И.О.** | **Кабинет** |
| --- | --- | --- | --- |
|  | специалист по связям с общественностью 1 категории |  | Приемная |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

 Приложение 2

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

Перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн, в случае обезличивания ПДн

|  |  |
| --- | --- |
| **Должность** | **Ф.И.О.** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

 Приложение 3

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

Перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

|  |  |
| --- | --- |
| **№**  | **Должность** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

 Приложение 3

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

Состав комиссии по защите информации

|  |  |
| --- | --- |
| Председатель комиссии |  |
| Члены комиссии |  |
|  |
|  |

 Приложение 4

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПОЛОЖЕНИЕ
о комиссии по защите информации**

1. Общие положения
	1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.
2. Основные задачи комиссии
	1. Основными задачами комиссии являются:
		1. Сбор и анализ исходных данных по информационным системам.
		2. Определение значений параметров для установления уровня защищенности персональных данных и класса защищенности в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», руководящих документов Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».
		3. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных, класса защищенности государственной информационной системы, класса защищенности информационной системы, предназначенной для обработки конфиденциальной информации.
3. Порядок формирования комиссии
	1. Комиссия формируется из числа штатных сотрудников, участвующих в процессе обработки персональных данных.
	2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.
	3. Члены комиссии назначаются распоряжением Главы.
	4. В случае изменения состава Комиссии в приказ вносятся соответствующие изменения.
4. Полномочия комиссии
	1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:
		1. Получать необходимые сведения у всех работников, участвующих в обработке персональных данных.
		2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.
		3. Отслеживать технологический процесс обработки персональных данных.
		4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети.
		5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.
		6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.
		7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.
5. Отчетность комиссии
	1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.
	2. В результате своей деятельности Комиссия должна составить акт определения уровня защищенности ПДн при их обработке в ИСПДн и класса защищенности ИС и акт классификации информационной системы, предназначенной для обработки конфиденциальной информации.

 Приложение 5

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**Обязательство
о неразглашении информации, содержащей персональные данные**

Я,

(фамилия, имя, отчество полностью)

являясь работником Администрации сельского поселения Сентябрьский, в должности

 ,

(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| дата |  | подпись |  | расшифровка |

**Типовая форма согласия субъекта**

**на обработку их персональных данных**

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

(Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ серия \_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(вид документа, удостоверяющего личность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(когда и кем)

проживающий(ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

настоящим даю свое согласие уполномоченным должностным лицам

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

(наименование и адрес органа государственной власти)

на обработку моих персональных данных и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

(цель обработки персональных данных)

и распространяется на следующую информацию: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

(перечень персональных данных)

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая без ограничения сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, а также осуществление любых иных действий с моими персональными данными с учетом федерального законодательства.

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

Данное согласие действует с "\_\_" \_\_\_\_\_\_\_\_ 20\_\_ г. бессрочно и может быть отозвано в любое время по моему письменному заявлению.

"\_\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

**Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные**

Уважаемый(ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В соответствии с требованиями Федерального закона Российской Федерации N 152-ФЗ от 27 июля 2006 года "О персональных данных" уведомляем Вас, что обязанность предоставления Вами персональных данных установлена пунктом \_\_\_\_\_\_\_\_ Федерального закона от \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_, а также следующими нормативными актами:

(указать НПА)

В случае отказа Вами предоставить свои персональные данные Администрация не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:

(перечислить юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы).

В соответствии с действующим законодательством РФ в области персональных данных Вы имеете право: на получение сведений об администрации (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения Администрации, о наличии своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от Администрации разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов; обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Ответственный за обработку

персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

 подпись (расшифровка подписи)

 Приложение 6

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

ЖУРНАЛ
учета машинных носителей персональных данных (установленных в ПЭВМ)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер | Тип и ёмкость | Дата и место установки (использования) | Ответственное должностное лицо (Ф.И.О) |
|  |  |  |  |  |

ЖУРНАЛ
учета машинных носителей персональных данных (отчуждаемых)

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

ЖУРНАЛ
учета лиц, допущенных к персональным данным

|  |  |  |
| --- | --- | --- |
| № 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 |
|  |  |  |  |  |  |  |

ЖУРНАЛ
учета средств защиты информации

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

ЖУРНАЛ
учета средств криптографической защиты информации

| № п/п | Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | Отметка о выдаче | Отметка о подключении (установке) СКЗИ | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | Примечания |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| От кого получены | Дата и номер сопроводительного письма | Ф.И.О. пользователя криптосредств | Дата и расписка в получении | Ф.И.О. пользователя криптосредств, производившего подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | Номера аппаратных средств, в которые установлены или к которым подключены криптосредства | Дата изъятия (уничтожения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | Номер акта или расписка об уничтожении |
| 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

ЖУРНАЛ
учета хранилищ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Регистрационный (учетный) номер хранилища | Вид хранилища | Дата постановки на учет | Фамилия и подпись принявшего (ответственного), дата | Место расположения (номер помещения) | Дата и номер акта о выводе из эксплуатации | Примечание |
|  |  |  |  |  |  |  |  |

ЖУРНАЛ

учета выдачи паролей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Дата получения пароля | Ф.И.О. получателя | Подпись получателя |
|   |   |  |   |

ЖУРНАЛ

учета обращений субъектов персональных данных по вопросам обработки персональных данных

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

ЖУРНАЛ

антивирусных проверок

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата и время проверки | Наименование ИСПДн (составной части ИСПДн) | Какими средствами проводилась проверка | Результаты проверки | Наименование инфицированных файлов, источника поступления (носитель, организация) | Примечание (принятые меры) | Фамилия и подпись лица, проводившего проверку |
| кол-во проверенных файлов | кол-во инфицированных файлов |
| 1 |   |   |   |   |   |   |   |   |

ЖУРНАЛ

учета выявленных инцидентов информационной безопасности

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата и время | Описание инцидента | Ответственный за реагирование на инцидент | Отметка об устранении инцидента | Дата устранения инцидента | Подпись ответственного лица | Примечание |
|  |  |  |  |  |  |  |  |

ЖУРНАЛ

учета передачи персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Сведения о запрашивающем лице | Состав запрашиваемых персональных данных | Цель получения персональных данных | Отметка о передаче или отказе в передаче персональных данных | Дата передачи/отказа в передаче персональных данных | Подпись запрашивающего лица |
|  |  |  |  |  |  |  |

ЖУРНАЛ

периодического тестирования средств защиты информации

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование средства защиты информации от НСД или криптосредства | Регистрационные номера СЗИ от НСД или криптосредства | Дата тестирования | Фамилия и подпись ответственного пользователя, проводившего тестирование | Наименование теста, используемые средства для проведения теста | Результат тестирования (успешный/неуспешный), комментарий | Дата очередного тестирования |
|  |  |  |  |  |  |  |  |

ЖУРНАЛ

уничтожения носителей персональных данных

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование ИСПДн, в которой уничтожаются персональные данные  | Ф.И.О. субъекта, персональные данные которого подлежат уничтожению | Обоснование уничтожения | Наименование файла, и его месторасположение | Дата уничтожения | Ф.И.О. и подпись Исполнителя  | Ф.И.О. и подпись ответственного за обработку персональных данных |
|  |  |  |  |  |  |  |  |

 Приложение 7

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**АКТ**

определения уровня защищенности ПДн и класса защищенности ИС «СЭД Дело» администрации сельского поселения Сентябрьский

|  |  |
| --- | --- |
| Председатель комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Рассмотрев исходные данные об информационной системе «СЭД Дело» администрации сельского поселения Сентябрьский (далее - ИС), комиссия определила:

* Категории персональных данных обрабатываемых в ИС: в информационной системе обрабатываются иные категории персональных данных;
* Категории субъектов: персональные данные субъектов персональных данных, являющихся сотрудниками оператора;
* Объем обрабатываемых персональных данных: менее 100 000;
* Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;
* Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;
* Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить четвертый уровень защищенности (УЗ4) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

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

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

Комиссия утвердила следующее:

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

|  |  |  |
| --- | --- | --- |
| Председатель комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| Члены комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  |
|  |

«\_\_»\_\_\_\_\_\_\_\_\_\_2019 г.

 Приложение 8

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**АКТ**

**об уничтожении персональных данных субъектов персональных данных**

Комиссия в составе:

|  |  |  |
| --- | --- | --- |
| **Роль** | **ФИО** | **Должность** |
| **Председатель** |  |  |
| **Члены комиссии** |  |  |
|  |  |
|  |  |

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

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

Указанные персональные данные уничтожены путем

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

|  |  |  |  |
| --- | --- | --- | --- |
| Председатель комиссии: |  |  |   |
|  | подпись |  | расшифровка |
| Члены комиссии: |  |  |   |
|  | подпись |  | расшифровка |
|  |  |  |  |
|  | подпись |  | расшифровка |

 Приложение 9

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**Перечень информационных систем персональных данных**

|  |  |
| --- | --- |
| **Наименование** | **Адрес расположения** |
| Информационная система «СЭД Дело» администрации сельского поселения Сентябрьский | 628330, Ханты-Мансийский автономный округ - Югра автономный округ, Нефтеюганский район, поселок Сентябрьский, территория КС-5, дом 10 |

 Приложение 10

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПЕРЕЧЕНЬ**обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

| **Группа персональных данных** | **Состав персональных данных** | **Цели обработки персональных данных** |
| --- | --- | --- |
| Сведения о гражданах | 1. фамилия, имя и отчество;
2. число, месяц, год и место рождения;
3. адрес и дата регистрации по месту жительства (месту пребывания);
4. вид, серия, номер документа, удостоверяющего личность;
5. номер контактного телефона или сведения о других способах связи.
 | Осуществление контроля за сроками исполнения поручений в системе автоматизации делопроизводства и электронного документооборота «Дело». |

Таблица 2. Правовое основание обработки персональных данных и сроки их хранения

| **Категория персональных данных** | **Основание для обработки персональных данных** |
| --- | --- |
| Иные категории ПДн | Конституция Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных» |

 Приложение 11

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**Положение**

об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Общие положения
	1. Положение об организации режима обеспечения безопасности помещений, в которых размещены ИС Администрации сельского поселения Сентябрьский, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
	2. Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа.
2. Границы контролируемой зоны
	1. Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.
	2. План-схемы контролируемой зоны помещений приведены в приложении 1 к настоящему положению.
3. Порядок доступа в помещения
	1. Перечень лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей), приведен в приложении 1 к настоящему постановлению.
	2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения, разрешено в период рабочего времени в соответствии с утвержденным графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.
	3. Лица, не указанные в п. 3.1 настоящего Положения допускаются в помещения в присутствии лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей).

План-схема границ контролируемой зоны Администрации сельского поселения Сентябрьский (территория КС-5, дом 10)



- граница контролируемой зоны

 Приложение 12

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПОЛИТИКА**

**в отношении обработки персональных данных**

1. Общие положения
	1. Политика в отношении обработки персональных данных в Администрации сельского поселения Сентябрьский (далее – Политика) разработана в соответствии с Конституцией Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации.
	2. Политика определяет порядок и условия обработки персональных данных в Администрации сельского поселения Сентябрьский (далее – Оператор) с использованием средств автоматизации и без использования таких средств.
	3. Обработка персональных данных осуществляется в целях предоставления государственных и муниципальных услуг в соответствии с административными регламентами предоставления указанных услуг на основании соглашений, заключенных федеральными органами исполнительной власти и органами государственных внебюджетных фондов с Оператором, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
2. Основные понятия, используемые в настоящей Политике
	1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
	2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
	3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
	4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
	5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
	6. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
	7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
	8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
	9. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
	10. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
3. Принципы обработки персональных данных
	1. Обработка персональных данных осуществляется на законной основе.
	2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
	3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
	4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.
	5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.
	6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.
	7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
4. Условия обработки персональных данных
	1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:
		1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
		2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;
		3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
		4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
		5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
		6. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
		7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
		8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
	2. В случае если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.
5. Конфиденциальность персональных данных
	1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
6. Право субъекта персональных данных на доступ
к его персональным данным
	1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
	2. Сведения, указанные в п. 6.7 настоящей Политики, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
	3. Сведения, указанные в п. 6.7 настоящей Политики, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
	4. В случае если сведения, указанные в п. 6.7 настоящей Политики, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
	5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в п. 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемы персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.3 настоящей Политики, должен содержать основание направления повторного запроса.
	6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.
	7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
		1. Подтверждение факта обработки персональных данных Оператором;
		2. Правовые основания и цели обработки персональных данных;
		3. Цели и применяемые Оператором способы обработки персональных данных;
		4. Наименование и местонахождение Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
		5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
		6. Сроки обработки персональных данных, в том числе сроки их хранения;
		7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
		8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;
		9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.
		10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.
7. Право на обжалование действий или бездействий Оператора
	1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
	2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
8. Обязанности Оператора при сборе персональных данных
	1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 6.7 настоящей Политики.
	2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
	3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных п. 8.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
		1. Наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;
		2. Цель обработки персональных данных и ее правовое основание;
		3. Предполагаемые пользователи персональных данных;
		4. Установленные настоящим Федеральным законом права субъекта персональных данных;
		5. Источник получения персональных данных.
	4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 8.3 настоящего Положения, в случаях, если:
		1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;
		2. Персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
		3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
		4. Предоставление субъекту персональных данных сведений, предусмотренных частью 8.3 настоящей Политики, нарушает права и законные интересы третьих лиц.
9. Меры направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом
«О персональных данных»
	1. Назначен ответственный за организацию обработки персональных данных.
	2. Изданы документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
	3. Утверждены правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.
	4. Проведена оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых оператором мер.
	5. Проведено ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.
10. Меры по обеспечению безопасности персональных данных
при их обработке
	1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.
	2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.
	3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.
	4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.
	5. Ведется учет машинных носителей персональных данных.
	6. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.
	7. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
	8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

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

1. Порядок управления учетными записями
	1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.
	2. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещено.
	3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн.

В заявке указывается:

* содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной 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 (учетной записи) данного сотрудника;
* полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).
	1. Заявку рассматривает руководитель, визируя ее, 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 защиты на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.
	2. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор производит необходимые операции по созданию (удалению) учетной записи пользователя, 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 должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 90 дней.
	3. 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 в заявке делается отметка о выполнении задания за подписью исполнителя - администратора информационной безопасности.
	4. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему 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.
	5. Исполненные заявка и задание (за подписью администратора информационной безопасности) 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 сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.
	1. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.
	2. Ответственный за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятия мер в случае утраты и (или) компрометации средств аутентификации является администратор безопасности.
1. Перечень программного обеспечения, разрешенного к установке на рабочее место пользователя

|  |  |  |
| --- | --- | --- |
| № п/п | Тип ПО | Наименование ПО |
|  | Операционная система | Microsoft Windows 7 Professional |
|  | Пакет офисных приложений | Microsoft Office 2007 и выше |
|  | Браузер | Internet Explorer 9 и выше |
|  | Система электронного документооборота\* | Клиентская часть «СЭД ДЕЛО» |
|  | Архиватор | 7-Zip |
|  | Средство работы с PDF файлами | Acrobat Reader версии 9 и выше |

Примечание \*: использование ПО определяется необходимостью работы в информационной системе с использование толстого клиента.

 Приложение 13

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных**

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

* Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
* Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
* Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
1. Обязанности

Ответственный за организацию обработки персональных данных обязан:

* Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;
* Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;
* Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.
1. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

1. Права

Ответственный за организацию обработки персональных данных имеет право:

* Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;
* Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

 Приложение 14

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в
информационных системах персональных данных**

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

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

1. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

* Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;
* Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных;
* Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;
* Осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);
* Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;
* Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;
* Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;
* Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;
* Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;
* 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;
* Обязан проводить мероприятия по организации антивирусной защиты;
* Организовать защиту информации при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны;
* 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 инструкции по организации парольной защиты в информационных системах персональных данных;
* Выполнять своевременное обновление программного обеспечения элементов ИСПДн и средств защиты персональных данных в ручном режиме по мере появления таких обновлений;
* Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;
* Осуществлять хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты или компрометации средств аутентификации;
* Выполнять проверку электронных журналов средств защиты информации и штатных журналов операционной системы на наличие ошибок, состава и времени изменений, которые привели к изменению состояния защищенности или к несанкционированному доступу;
* Обязан немедленно сообщать ответственному за организацию обработки персональных данных 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 и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;
* Осуществлять контроль состава технических средств, программного обеспечения и средств защиты информации;
* Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.
1. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

* + Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
	+ Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
	+ Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;
1. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

 Приложение 15

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ**

**ответственного за эксплуатацию информационных систем персональных данных**

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за эксплуатацию информационной системы персональных данных.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

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

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

 Приложение 16

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**Правила работы лиц, доступ которых к персональным данным,
в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей**

Допуск для работы на автоматизированных рабочих местах
(далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

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

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

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

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.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных 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 в 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;
* Выполнять требования инструкции по организации антивирусной защиты в полном объеме;
* Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
* Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
* 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;
* Некорректного функционирования установленных на АРМ технических средств защиты;
* Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

* Использовать компоненты программного и аппаратного обеспечения АРМ в личных 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;
* Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-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 машинные носители и распечатки, содержащие персональные данные;
* Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;
* Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

 Приложение 17

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей**

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
* Подтверждение факта обработки персональных данных;
* Правовые основания и цели обработки персональных данных;
* Цели и применяемые оператором способы обработки персональных данных;
* Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);
* Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
* Сроки обработки персональных данных, в том числе сроки их хранения;
* Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.
1. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
2. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
3. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
4. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.
5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в [пункте 5](#Par159) настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в [пункте 4](#Par158) настоящих правил, должен содержать обоснование направления повторного запроса.
6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным [пунктами 5](#Par159) и [6](#Par160) настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.
7. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:
* Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.
* В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.
* Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
* Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

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

 Приложение 18

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПРАВИЛА**

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

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в Администрации сельского поселения Сентябрьский требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.
2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.
3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.
4. Плановые проверки проводятся не чаще чем один раз в три месяца.
5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.
6. Основанием для проведения проверки служит распоряжение Главы поселения Сентябрьский «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»
7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:
* соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;
* соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
* достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;
* отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
* порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
* порядок и условия применения средств защиты информации;
* соблюдение правил доступа к персональным данным;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.
1. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:
* запрашивать у работников информацию, необходимую для реализации своих полномочий;
* требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
* принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
* вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
* вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.
1. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес Главы результаты проведения проверки в форме служебной записки.

 Приложение 18

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПОРЯДОК
уничтожения персональных данных при достижении
целей обработки и (или) при наступлении иных законных оснований**

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №\_\_(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

 Приложение 20

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПРАВИЛА**

**работы с обезличенными данными в случае обезличивания ПДн**

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными в Администрации сельского поселения Сентябрьский.

1. Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

* персональные данные – любая информация, относящаяся прямо или косвенно к 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;
* обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
1. Условия обезличивания

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

Способы обезличивания при условии дальнейшей обработки персональных данных:

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

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

1. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

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

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

* парольной политики;
* антивирусной политики;
* правил работы со съемными носителями (если они используется);
* правил резервного копирования;
* правил доступа в помещения, где расположены элементы информационных систем.

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

* правил хранения бумажных носителей;
* правил доступа к ним и в помещения, где они хранятся.

 Приложение 21

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ
по организации резервирования**

1. Общие положения

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

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

1. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

* Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, 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.
1. Порядок резервирования и хранения резервных копий

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.

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.

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

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

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

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

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

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

1. Порядок восстановления работоспособности ИСПДн

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

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, предъявляемым к определенному уровню защищенности персональных данных и классу защищенности информационной системы.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций.

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.

|  |
| --- |
| Учетная карточка резервного носителя персональных данных№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|   |   |   |   |
| **Дата резервного копирования** | **Объект копирования** | **Кто производил копирование** | **Подпись** |
|  |  |  |  |
|  |  |  |  |
|   |   |   |   |

 Приложение 22

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ
по организации парольной защиты**

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.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

* Длина пароля должна быть не менее 8 символов;
* В числе символов пароля обязательно должны присутствовать буквы, 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;
* При смене пароля должны быть изменены не менее 3 символов;
* Пользователь не имеет права сообщать личный пароль другим лицам;

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

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение 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.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

В случае 3-х кратного ввода не верного пароля пользователя ИСПДн должна осуществляться перезагрузка АРМ.

В случае 15-ти кратного ввода не верного ПИН аппаратного идентификатора пользователя, идентификатор должен быть заблокирован.

 Приложение 23

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ
по организации антивирусной защиты**

1. Общие требования

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 существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

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

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусные средства.

1. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

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

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).

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

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.

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.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

* 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.
1. Обновление баз САВЗ

Обновление баз САВЗ на АРМ ИСПДн, не имеющих подключения к локальной вычислительной сети (ЛВС) Администрации и сетям связи общего пользования, осуществляется администратором ИСПДн вручную с использованием учтенных носителях информации, в обязательном порядке проверяемых САВЗ перед их использованием или подключением к АРМ ИСПДн, еженедельно.

Обновление баз САВЗ на АРМ ИСПДн, не имеющих подключения к ЛВС Администрации, но подключенных к сетям связи общего пользования, осуществляется ежедневно в установленное время с официального сервера обновлений производителя САВЗ.

При централизованном управлении антивирусной защитой консоль (сервер) администрирования ежедневно в установленное время обновляет базы САВЗ с официального сервера обновлений производителя САВЗ и размещает их в общедоступное для АРМ ИСПДн хранилище.

Обновление баз САВЗ на АРМ ИСПДн, подключенных к ЛВС Администрации, осуществляется ежедневно в установленное время из общедоступного хранилища консоли (сервера) администрирования.

При локальном управлении антивирусной защитой роль консоли (сервера) администрирования по обновлению баз САВЗ и их размещению в общедоступное хранилище выполняет САВЗ, установленное на одном из АРМ ИСПДн.

1. Ответственность

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 24

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ**

**о пропускном и внутриобъектовом режимах**

1. Общие положения

Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами ИС в Администрации сельского поселения Сентябрьский в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн). При обеспечении доступа лиц соблюдаются требования по защите ПДн.

Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников Администрации сельского поселения Сентябрьский, сотрудников иных организаций и учреждений, граждан в помещения.

Контроль за порядком обеспечения доступа лиц в помещения отделов возлагается на руководителей подразделений.

Помещения и оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в данные помещения и к данному оборудованию посторонних лиц.

1. Организация пропускного и внутриобъектового режима

Пропускной режим в Администрации сельского поселения Сентябрьский устанавливается в целях:

* исключения фактов хищений собственности;
* исключения фактов вандализма со стороны недобросовестных посетителей;
* исключения возможности несанкционированного доступа персонала и посетителей в помещения.

Внутриобъектовый режим устанавливается в целях:

* соблюдения персоналом и посетителями правил внутреннего распорядка и пожарной безопасности;
* установления порядка допуска персонала в помещения ограниченного доступа предприятия;
* исключения возможности бесконтрольного передвижения посетителей по территории предприятия.

Надёжность пропускного и внутриобъектового режимов достигается:

* осуществлением контроля за перемещением персонала;
* осуществлением охраны помещений предприятия силами сторожей-вахтеров, ЧОП;
* контролем за состоянием технических средств охраны.

Ответственным за организацию пропускного и внутриобъектового режимов является Глава.

Организация пропускного и внутриобъектового режимов предприятия осуществляется руководителями соответствующих подразделений.

1. Порядок доступа в помещения сотрудников и граждан
	1. Перечень лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых) обязанностей приведен в приложении 1 к настоящему постановлению.
	2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящей Инструкции, разрешено в период рабочего времени в соответствии с утвержденным графиком работы, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.
	3. Лица, не указанные в п. 3.1 настоящей Инструкции, допускаются в помещения в присутствии лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых) обязанностей.
2. Внутриобъектовый режим на территории Администрации сельского поселения Сентябрьский.

Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объектах является Глава.

Сотрудники по окончании рабочего дня должны закрывать кабинеты на ключ, ключи от помещений, в которых размещена информационная система персональных данных, хранятся у сотрудников.

В случае отсутствия сотрудников в кабинетах в рабочее время помещения должны быть закрыты на ключ.

На территории помещений, в которых расположена информационная система персональных данных, запрещается:

* + проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;
	+ курить;
	+ пользоваться неисправными или самодельными электронагревательными и другими электробытовыми приборами;
	+ загромождать территорию, основные и запасные входы (выходы), лестничные площадки материалами и предметами, которые создают помехи для системы видеонаблюдения, затрудняют эвакуацию людей, материальных ценностей, препятствуют ликвидации очагов возгорания;
	+ совершать действия, нарушающие установленные режимы функционирования пожарной сигнализации.
1. Организация и порядок производства ремонтно-строительных работ в здании

Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего лица из числа сотрудников.

Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.

1. Организация охраны

Должна быть организована охрана помещений Администрации сельского поселения Сентябрьский. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо запирать его на ключ.

1. Уборка помещений

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть заблокированы все АРМ, на которых хранятся ПДн, носители, содержащие ПДн, должны быть убраны в сейф.

8. Требования по техническому укреплению

Ответственный за обеспечение безопасности ПДн обеспечивает обязательное выполнение мероприятий по техническому укреплению помещений, в которых обрабатываются ПДн, и должен руководствоваться следующими основными требованиями:

* двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;
* конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. Рамы указанных оконных проемов оборудуются запорными устройствами. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи.

 Приложение 25

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ИНСТРУКЦИЯ**

**по работе с инцидентами информационной безопасности**

Ответственность за выявление инцидентов ИБ и реагирование на них в Администрации сельского поселения Сентябрьский возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед Главой) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Предположение о том, что произошел инцидент безопасности в ИС, базируется на трех основных факторах:

* события информационной безопасности поступают одновременно из нескольких источников (пользователи, средства защиты, журнальные файлы);
* средства защиты сигнализируют о множественном повторяющемся событии или попытках нарушения установленных правил;
* анализ электронных журналов средств защиты информации и штатных журналов операционной системы на наличие ошибок дает основание для вывода системным администраторам о возможности наступления события инцидента.

В информационной системе подлежат регистрации следующие события:

* вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
* подключение машинных носителей информации и вывод информации на носители информации;
* запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
* попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
* попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, а также сроки хранения определяются администратором информационной безопасности согласно требованиям предъявляемым к информационным системам определенного класса защищенности.

События безопасности подлежат защите согласно организационным мерам, а также матрице доступа и соответствующим настройкам системы защиты информации на ограничение доступа пользователей к настройкам и изменениям параметров средств защиты информации.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

* замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
* установка дополнительного ПО;
* изменение сетевых настроек рабочего места;
* замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов Администрации сельского поселения Сентябрьский, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Выявление (поиск), анализ и устранение уязвимостей в информационной системе включает в себя:

* выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
* разработку по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
* анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
* устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
* информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Необходимо использовать для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

Необходимо уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях.

Доступ к функциям выявления (поиска) уязвимостей предоставляется только администраторам (предоставление такой возможности только администраторам безопасности).

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретной ИСПДн.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется:

* в отношении системных и прикладных программных средств - администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;
* в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных работников и подразделений, запрещено.

Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой ответственного за эксплуатацию ИСПДн.

В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

* установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;
* обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
* изменение настроек средств защиты информации;
* удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору защиты для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке ИСПДн.

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 производится администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

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

Установка и обновление ПО (системного, тестового и т.д.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.)‚ полученных установленным порядком, прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

Все добавляемые программные и аппаратные компоненты должны быть предварительно установленными порядком проверены на работоспособность, а также отсутствие опасных функций.

После установки (обновления) ПО, администратор защиты должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается распоряжением руководителя.

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с работниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. В данном случае администратор защиты обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за защиту информации.

Копии заявок могут храниться у администратора защиты:

* для восстановления конфигурации ИСПДн после аварий;
* для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
* для проверки правильности установки и настройки средств защиты ИСПДн факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора защиты и работника ответственного за эксплуатацию данной ИСПДн.

Данный раздел определяет порядок контроля соблюдения условий использования средств защиты информации (далее — СЗИ).

Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как работниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

Право проверки соблюдения условий использования средств защиты информации имеют:

* руководитель;
* ответственный за защиту информации;
* администратор безопасности.

Пользователю ИСПДн категорически запрещается:

* обрабатывать конфиденциальную информацию с отключенными СЗИ;
* менять настройки СЗИ.

Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

В информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

* контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
* контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
* контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
* исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

В информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

* контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;
* контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;
* контроль реализации правил разграничения доступом в соответствии с УПД.2;
* контроль реализации полномочий пользователей в соответствии с УПД.4 и ПД.5;
* контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;
* устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

В информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

 Приложение 26

 к постановлению администрации

 сельского поселения Сентябрьский

 от 23.08.2019 № 82 -па

**ПЛАН**

мероприятий по защите информации в Администрации сельского поселения Сентябрьский

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План мероприятий) содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в информационных системах Администрации сельского поселения Сентябрьский.

Выбор конкретных мероприятий осуществляется на основании перечня актуальных угроз безопасности, указанных в Модели угроз безопасности для соответствующей ИС.

В План мероприятий включены следующие категории мероприятий:

* организационные (административные);
* физические;
* технические (аппаратные и программные);
* контролирующие.

В План мероприятий включена следующая информация:

* название мероприятия;
* периодичность мероприятия (разовое/периодическое);
* исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы Администрации сельского поселения Сентябрьский.

План мероприятий по защите информации

| **Мероприятие** | **Периодичность** | **Исполнитель/ Ответственный** |
| --- | --- | --- |
| **Организационные мероприятия** |
| Обследование информационных систем | Разовоесрок до  |  |
| Определение перечня ИСПДн | Разовоесрок до  |  |
| Определение обрабатываемых ПДн и объектов защиты | Разовоесрок до  |  |
| Определение круга лиц, участвующих в обработке ПДн | Разовоесрок до. |  |
| Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей | Разовоесрок до  |  |
| Назначение ответственного за обеспечение безопасности ПДн | Разовоесрок до  |  |
| Классификация всех выявленных ИСПДн | Разовоесрок до  |  |
| Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн. | Разовоесрок до  |  |
| Организация порядка резервного копирования защищаемой информации на твердые носители | Разовоесрок до. |  |
| Организация информирования сотрудников о порядке обработки ПДн и их обучения | Разовоесрок до  |  |
| Организация информирования сотрудников о введенном режиме защиты ПДн | Разовоесрок до  |  |
| Подготовка и утверждение комплекта нормативной документации, регламентирующей обработку ПДн в ИСПДн | Разовоесрок до  |  |
| **Физические мероприятия** |
| Установление границ контролируемой зоны ИСПДн | Разовоесрок до  |  |
| Организация постов охраны для пропуска в контролируемую зону | Разовоесрок до  |  |
| Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПД снаружи здания | Разовоесрок до  |  |
| **Технические мероприятия** |
| Внедрение специальной подсистемы управления доступом, регистрации и учета  | Разовоесрок до  |  |
| Внедрение межсетевого экранирования  | Разовоесрок до  |  |
| Внедрение криптографической защиты  | Разовоесрок до  |  |
| **Контролирующие мероприятия** |
| Контроль над соблюдением режима обработки ПДн | Еженедельно |  |
| Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | Ежемесячно |  |
| Контроль состава технических средств, программного обеспечения и средств защиты информации | Ежемесячно |  |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Ежегодно |  |
| Проведение анализа электронных журналов средств защиты информации и штатных журналов операционной системы на наличие ошибок | Ежемесячно |  |
| Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Еженедельно |  |
| Контроль за обеспечением резервного копирования | Ежемесячно |  |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз | Ежегодно |  |
| Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно |  |