

**Муниципальное образование сельское поселение Усть-Юган**

**Нефтеюганский район**

**Ханты-Мансийский автономный округ – Югра**

**АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**УСТЬ-ЮГАН**

**ПОСТАНОВЛЕНИЕ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.11.2018 |  |  | № | 239-па |

п. Усть-Юган

О защите информации

В соответствии с требованиями Федеральных законов Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», 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», п о с т а н о в л я ю:

1. Утвердить перечень должностей в МУ «Администрация сельского поселения Усть-Юган и в подведомственном ей учреждении, 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.
2. Утвердить перечень должностей в МУ «Администрация сельского поселения Усть-Юган и в подведомственном ей учреждении, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных, согласно [приложению № 2](#Пр3) к настоящему постановлению.
3. 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.
4. Утвердить типовые формы документов по защите информации:
	1. Согласие на обработку персональных данных согласно [приложению № 5](#Пр6) к настоящему постановлению.
	2. Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи с поступлением на работу (муниципальную службу) в МУ «Администрация сельского поселения Усть-Юган» и подведомственного ей учреждения согласно [приложению № 6](#Пр7) к настоящему постановлению.
	3. Обязательство о неразглашении информации, содержащей персональные данные, согласно [приложению № 7](#Пр8) к настоящему постановлению.
	4. Журналы по защите информации согласно [приложению № 8](#Пр9) к настоящему постановлению.
	5. Акт определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных и класса защищенности информационных систем согласно [приложению № 9](#Пр11) к настоящему постановлению.
	6. Акт об уничтожении персональных данных субъектов персональных данных согласно [приложению 3 10](#Пр12) к настоящему постановлению.
5. Утвердить перечень информационных систем персональных данных согласно [приложению № 11](#Пр13) к настоящему постановлению.
6. Утвердить перечень обрабатываемых персональных данных согласно [приложению № 12](#Пр14) к настоящему постановлению.
7. 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 № 13](#Пр15) к настоящему постановлению.
8. Утвердить политику в отношении обработки персональных данных согласно [приложению № 1](#Пр16)4 к настоящему постановлению.
9. Утвердить инструкции и правила по защите информации:
* Инструкцию ответственного за организацию обработки персональных данных согласно [приложению № 15](#Пр17) к настоящему постановлению;
* Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно [приложению № 16](#Пр18) к настоящему постановлению;
* Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно [приложению № 17](#Пр19) к настоящему постановлению;
* Инструкцию по организации антивирусной защиты в информационных системах персональных данных согласно [приложению №](#Пр22) 18 к настоящему постановлению;
* Инструкцию по обработке персональных данных без использования средств автоматизации согласно [приложению №](#Пр25) 19 к настоящему постановлению;
* Инструкцию по работе с инцидентами информационной безопасности согласно [приложению](#Пр26) № 20 к настоящему постановлению;
* Правила рассмотрения запросов субъектов персональных данных или их представителей согласно [приложению №](#Пр28) 21 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 [№](#Пр29) 22 к настоящему постановлению;
* Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно [приложению №](#Пр30) 23 к настоящему постановлению;
* Правила работы с обезличенными данными в случае обезличивания персональных данных согласно [приложению](#Пр31) № 24 к настоящему постановлению;
* Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований согласно [приложению №](#Пр32) 25 к настоящему постановлению.
* Инструкцию пользователя информационной системы персональных данных согласно [приложению №](#Пр32) 26 к настоящему постановлению.
1. Считать утратившим силу постановление администрации сельского поселения Усть-Юган от 18.04.2017 № 56-па «Об обработке персональных данных».
2. Настоящее постановление подлежит размещению на официальном сайте органа местного самоуправления сельского поселения Усть-Юган в сети интернет.
3. Контроль за исполнением постановления оставляю за собой.

|  |  |
| --- | --- |
| Глава поселения | В.А. Мякишев |

 [Приложение № 1](#Пр1)
 к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Перечень должностей в МУ «Администрация сельского поселения Усть-Юган» и в подведомственном ей учреждении, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Должность | ИСПДн | Способ обработки ПДн |
| МУ «Администрация сельского поселения Усть-Юган» |
| 1 | Глава поселения | - | неавтоматизированная |
| 2 | Заместитель Главы поселения | - | неавтоматизированная |
| 3 | Начальник организационно-правового отдела | «МАИС ЗАГС» | автоматизированная/ неавтоматизированная/ смешанная |
| 4 | Начальник отдела-главный бухгалтер | «1С: Бухгалтерия» | автоматизированная/ неавтоматизированная/ смешанная |
| 5 | Главный специалист финансово-экономического отдела | «1С: Бухгалтерия» | автоматизированная/ неавтоматизированная/ смешанная |
| 6 | Ведущий специалист организационно-правового отдела | «1С: Зарплата и кадры» | автоматизированная/ неавтоматизированная/ смешанная |
| 7 | Ведущий специалист по ведению реестра и учету муниципальной собственности | - | неавтоматизированная |
| 8 | Специалист 1 категории по благоустройству и землепользованию | - | неавтоматизированная |
| 9 | Бухгалтер | «1С: Бухгалтерия» | автоматизированная/ неавтоматизированная/ смешанная |
| 10 | Инспектор по первичному воинскому учету | «Военно-учетное подразделение ОМС 3.02» | автоматизированная/ неавтоматизированная/ смешанная |
| МКУ «Административно-хозяйственная службасельского поселения Усть-Юган» |
| 1 | Директор | - | неавтоматизированная |
| 2 | Начальник службы | - | неавтоматизированная |
| 3 | Специалист по работе с молодежью | - | неавтоматизированная |
| 4 | Делопроизводитель | - | неавтоматизированная |
| 5 | Специалист адресно-справочной работы | «Похозяйственный учет» | автоматизированная/ неавтоматизированная/ смешанная |
| 6 | Специалист по комплексной безопасности | - | неавтоматизированная |
| 7 | Экономист | «1С: Бухгалтерия» | автоматизированная/ неавтоматизированная/ смешанная |

[Приложение № 2](#Пр1)
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Перечень должностей в МУ «Администрация сельского поселения

Усть-Юган» и в подведомственном ей учреждении, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

|  |  |
| --- | --- |
| № п/п | Должность |
| МУ «Администрация сельского поселения Усть-Юган» |
| 1 | Начальник организационно-правового отдела |
| 2 | Начальник отдела – главный бухгалтер |
| 3 | Ведущий специалист по ведению реестра и учету муниципальной собственности |
| 4 | Ведущий специалист организационно-правового отдела |
| 5 | Бухгалтер |
| 6 | Главный специалист финансово-экономического отдела |
| 7 | Специалист 1 категории по благоустройству и землепользованию |
| 8 | Инспектор по первичному воинскому учету |
| МКУ «Административно-хозяйственная служба сельского поселения Усть-Юган |
| 1 | Начальник службы |
| 2 | Экономист |
| 3 | Специалист адресно-справочной работы |
| 4 | Специалист по комплексной безопасности |
| 5 | Специалист по работе с молодежью |
| 6 | Делопроизводитель |

[Приложение № 3](#Пр1)
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Состав

комиссии по защите информации

|  |  |
| --- | --- |
| Председатель комиссии | Щербакова Наталия Александровна – заместитель Главы поселения; |
| Заместитель председателя комиссии | Богомолова Ирина Николаевна – начальник организационно-правового отдела; |
| Члены комиссии: | Ряполова Галина Николаевна – директор МКУ «АХС сп Усть-Юган»; |
| Гаврилюк Анна Ивановна – начальник отдела –главный бухгалтер; |
| Бикбердина Венера Танилевна – ведущий специалист организационно-правового отдела. |

[Приложение № 4](#Пр1)
к постановлению администрации

сельского поселения Усть-Юган

от 23.11.2018 № 239-па

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения
	1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии по защите информации (далее - Комиссия).
2. Основные задачи комиссии по защите информации
	1. Основными задачами Комиссии являются:
		1. Сбор и анализ исходных данных по информационным системам Операторов.
		2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
		3. Определение значений параметров для установления уровня защищенности персональных данных 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».
		4. Определение класса защищенности информационных систем Операторов на основании собранных данных.
		5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.
3. Порядок формирования комиссии по защите информации
	1. Комиссия формируется из числа штатных сотрудников МУ «Администрация сельского поселения Усть-Юган» и подведомственного ей учреждения (далее – Операторов), 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 постановлением администрации сельского поселения Усть-Юган.
	4. В случае изменения состава Комиссии, в постановление администрации сельского поселения Усть-Юган вносятся соответствующие изменения.
4. Полномочия комиссии по защите информации
	1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:
* получать необходимые сведения у всех сотрудников Операторов, участвующих в обработке персональных данных;
* просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных;
* отслеживать технологический процесс обработки персональных данных;
* выявлять или получать готовые сведения о структуре локальной вычислительной сети Операторов;
* определять или получать готовые сведения о наличии и способах доступа к информационно-телекоммуникационной сети;
* определять или получать готовые сведения о технических и программных средствах обработки персональных данных;
* определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.
1. Отчетность комиссии по защите информации
	1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.
	2. В результате своей деятельности Комиссия должна составить акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем.

[Приложение № 5](#Пр1)
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Типовая форма

СОГЛАСИЕ
на обработку персональных данных

п. Усть-Юган «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

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

(фамилия, имя, отчество)

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

(вид документа, удостоверяющего личность)

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

(когда и кем)

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

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

настоящим даю свое согласие на обработку моих персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(наименование юридического лица)

(далее – оператор), расположенному по адресу: 628325, Тюменская Область, Ханты-Мансийский автономный округ-Югра, Нефтеюганский район, поселок Усть-Юган, дом 5 и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей:

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

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

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

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

 и распространяется на следующую информацию:

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

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

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

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

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

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

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

 (перечень третьих лиц, адрес расположения)

с целью исполнения обязательств представителя нанимателя в рамках служебного контракта/трудового договора, и в установленных Федеральными законами случаях их обязательного предоставления.

В соответствии со статьей 8 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» даю согласие на размещение моих персональных данных:

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

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

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

на официальном сайте органа местного самоуправления сельского поселения Усть-Юган, который является общедоступным источником персональных данных.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных с учетом федерального законодательства.

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

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

Я ознакомлен(а) с возможными последствиями моего отказа дать письменное согласие на получение персональных данных.

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

(Ф.И.О., подпись лица, давшего согласие)

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

Примечание:

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

[Приложение](#Пр1) № 6
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Типовая форма

Р А З Ъ Я С Н Е Н И Я
субъекту персональных данных юридических последствий отказа
предоставить свои персональные данные в связи с поступлением
на работу (муниципальную службу)

В соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006
№ 152-ФЗ «О персональных данных» оператором – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование юридического лица)

мне, разъяснено, что в случае моего отказа предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять их обработку, что приведет к следующим для меня юридическим последствия:

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

(возникновение, изменение или прекращение личных либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы)

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

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

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

 дата подпись расшифровка подписи

Юридические последствия отказа предоставить персональные данные разъяснил(а):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| должность |  | подпись |  | расшифровка |

[Приложение](#Пр1) № 7
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Типовая форма

Обязательство
о неразглашении информации, содержащей персональные данные

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

(фамилия, имя, отчество полностью)

являясь работником \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в должности \_\_\_\_\_\_\_\_\_\_,

 (наименование организации)

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

(указать должность)

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 |

14

[Приложение](#Пр1) № 8
к постановлению администрации сельского поселения Усть-Юган от 23.11.2018 № 239-па

Журналы по защите информации

Таблица 1

ЖУРНАЛ
учета машинных носителей персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер | Тип и ёмкость | Дата и место установки (использования) | Ответственное должностное лицо (Ф.И.О) |
|  1 |  2 |  3 |  4 |  5 |
|  |  |  |  |  |

Таблица 2

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

|  |  |  |
| --- | --- | --- |
| № п/п | Сведения о допуске к персональным данным | Сведения о прекращении допуска к персональным данным |
| Наименование информационных систем персональных данных /способ обработки ПДн | Ф.И.О, должность получившего допуск | Дата и номер распоряжения о допуске | Дата и подпись допускаемого лица | Дата и номер распоряжения о прекращении допуска |
|  |  |  |  |  |  |

Таблица 3

ЖУРНАЛ
учета средств защиты информации

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

Таблица 4

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 |
|  |  |  |  |  |  |  |

Таблица 5

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 |
|  |  |  |  |  |  |  |  |

Таблица 6

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](#Пр1) № 9
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

АКТ

определения уровня защищенности персональных данных при их

обработке в информационных системах персональных данных

и класса защищенности информационных систем

 «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

(наименование информационной системы)

|  |  |  |
| --- | --- | --- |
| Председатель комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО |
| Члены комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИОФИОФИО |

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

* категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

(биометрические, специальные, общедоступные, иные)

категории персональных данных;

* категории субъектов: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

(субъектов персональных данных, являющихся сотрудниками оператора или субъектов персональных данных, не являющихся сотрудниками оператора)

* объем обрабатываемых персональных данных: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (менее чем 100000, более чем 100000)

* тип актуальных угроз: для информационной системы актуальны угрозы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ типа;

(первого, второго, третьего)

* уровень значимости информации: информация имеет \_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ уровень значимости УЗ \_\_\_\_;

(высокий, средний, низкий)

 - масштаб информационной системы: информационная система имеет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ масштаб.

 (федеральный, региональный, объектовый)

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

Результат оценки вреда:

Для информационной системы актуальны угрозы \_\_\_\_\_ 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, \_\_\_\_\_\_\_\_ степень ущерба) (целостность, \_\_\_\_\_\_\_\_ степень ущерба) (доступность, \_\_\_\_\_\_\_\_ степень ущерба)] – таким образом, комиссия установила \_\_\_\_\_\_\_\_\_ уровень значимости (УЗ \_\_\_\_) (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_).

|  |  |  |
| --- | --- | --- |
| Председатель комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО |
| Члены комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИОФИОФИО |

«\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ г.

[Приложение](#Пр1) № 10
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-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 27.07.2006 № 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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_подпись |  | расшифровка\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_расшифровка |

[Приложение](#Пр1) № 11
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

Перечень информационных систем персональных данных

|  |  |
| --- | --- |
| Наименование ИСПДн | Адрес расположения |
| «Похозяйственный учет» | п. Усть-Юган, д. 5, кабинет 5 |
| «1С: Бухгалтерия» | п. Усть-Юган, д. 5, кабинеты 3,4 |
| «1С: Зарплата и кадры» | п. Усть-Юган, д. 5, кабинет 9 |
| «Военно-учетное подразделение ОМС 3.02» | п. Усть-Юган, д. 5, кабинет 5 |
| «МАИС ЗАГС» | п. Усть-Юган, д. 5, кабинет 9 |

[Приложение](#Пр1) № 12
к постановлению администрации сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ПЕРЕЧЕНЬ
обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

| Группа персональных данных | Состав персональных данных | Цели обработки персональных данных |
| --- | --- | --- |
| 1. Обработка персональных данных в ИСПДн

«Военно-учетное подразделение ОМС 3.02» |
| Общедоступные | Фамилия, имя, отчество  | осуществление первичного воинского учета |
| Место рождения |
| Место работы  |
| Профессия |
| Специальность |
| Военно-учетная специальность |
| Сведения о приеме и снятии с воинского учета |
| Пол |
| Дата рождения |
| Разряд, категория |
| Табельный номер |
| Номер учетной карточки к военному билету |
| Документ, удостоверяющий личность (тип документа, серия, номер, дата выдачи, кем выдан) |
| Гражданство |
| Реквизиты загранпаспорта (серия, номер, кем и когда выдан) |
| Адрес места жительства |
| Адрес регистрации по месту жительства, дата регистрации, в том числе при смене места регистрации |
| Телефон (служебный, рабочий, мобильный) |
| Семейное положение |
| Информация о членах семьи (степень родства, ФИО, дата рождения, адрес проживания) |
| Информация об образовании (уровень образования, наименование учебного заведения, год окончания учебы) |
| Сведения о получении военных образований (уровень, наименование военного учебного заведения, факультет, количество курсов, реквизиты диплома, дата получения, профессия) |
| Знание иностранных языков, степень владения |
| Сведения о воинском учете (категория годности, реквизиты военного билета (серия, номер, дата выдачи, кем выдан), место принятия присяги, дата принятия присяги, разряд состава запаса, номер военно-учетной специальности, кодовое обозначение военно-учетной специальности, воинская должность, состав воинского учета, получение мобилизационного предписания, воинское звание, категория запаса, группа учета, профиль воинского учета, сведения о судимости, индивидуальные дозы облучения, спортивные разряды (звания), данные об увольнении из Вооруженных сил Российской Федерации (дата увольнения, номер и дата приказа) |
| Сведения о поощрении, государственных и ведомственных наградах (наименование награды, наименование документа, серия и номер, дата выдачи) |
| Сведения о прохождении военной, альтернативной гражданской службы (воинская часть, воинская должность, период службы, полное кодовое обозначение ВУС, тип (марка) ВВТ, дата и основания увольнения |
| Сведения о медицинском освидетельствовании (дата прохождения комиссии, комиссия, заключение комиссии, дата повторного освидетельствования, ранения, контузии, характер ранения, контузии, дата ранения) |
| Сведения о военных сборах (год прохождения, период прохождения, воинская часть, тип (марка) ВВТ, должность) |
| Сведения о боевых действиях (место прохождения, период прохождения, воинская часть, занимаемая должность) |
| Данные о бронировании (дата бронирования, спец. Учет, удостоверение отсрочки, период отсрочки) |
| Основные антропометрические данные (рост, размер головного убора, размер противогаза, размер обмундирования, ростовка, размер обуви) |
| Информация о пребывании в мобилизационном людском резерве |
| Занимаемая должность |
| Биометрические | Данные дактилоскопической регистрации |
| Специальные | Национальность |
| 2. Обработка персональных данных в ИСПДн «Похозяйственный учет» |
| Общедоступные | Фамилия, имя, отчество | регистрационный  учетграждан, ведение похозяйственных книг |
| Занимаемая должность |
| Место работы  |
| СНИЛС |
| ИНН |
| Адрес регистрации по месту жительства/ по месту пребывания, дата регистрации, в том числе при смене места регистрации/ места пребывания |
| Дата рождения |
| Знание иностранных языков, степень владения |
| Семейное положение, дата регистрации/дата расторжения брака |
| Реквизиты актовой записи о регистрации/расторжении брака (где, кем, номер) |
| Информация о членах семьи (степень родства, ФИО, дата рождения, адрес регистрации) |
| Социальное положение (наименование, код льгот, серия, №, дата выдачи удостоверения, лицевой счет, дата отмены льгот) |
| Документ, удостоверяющий личность (тип документа, серия, номер, дата выдачи, кем выдан, код подразделения) |
| Место рождения |
| Пол |
| Гражданство |
| Вид занятости |
| Статус занятости, трудоспособность |
| Реквизиты актовой записи о смерти (где, кем, номер) |
| Информация об образовании (наличие начального образования, класс, курс обучения) |
| Группа инвалидности (№, серия, дата удостоверения, дата отмены) |
| Реквизиты договоров найма на жилое помещение, сроки найма |
| Статус собственника, доля в собственности жилого помещения |
| Место и дата прибытия граждан |
| Специальные | Национальность |
| 3. Обработка персональных данных в ИСПДн «Зарплата и кадры» |
| Общедоступные | Фамилия, имя, отчество (в том числе при смене) | обеспечение кадровой работы, реализация трудовых отношений |
| Дата рождения |
| Место рождения |
| Адрес регистрации по месту жительства, дата регистрации, в том числе при смене места регистрации |
| Адрес места жительства |
| Телефон (мобильный, домашний, рабочий) |
| Место работы, подразделение  |
| Занимаемая должность |
| Документ, удостоверяющий личность (тип документа, серия, номер, дата выдачи, кем выдан, код подразделения) |
| Гражданство |
| СНИЛС |
| ИНН |
| Адрес электронной почты |
| Информация о членах семьи (степень родства, ФИО, дата рождения) |
| Пол |
| Табельный номер |
| Социальное положение (льготы) |
| Информация об образовании (уровень образования, наименование учебного заведения, год окончания учебы, специальность) |
| Данные о трудовой деятельности |
| Данные об отпусках, в том числе без сохранения заработной платы, по уходу за ребенком, командировках, работах в выходные и праздничные дни |
| Сведения о периодах временной нетрудоспособности |
| Вид занятости |
| Знание иностранных языков |
| Данные об ученой степени, ученых званий, научных трудов, изобретений |
| Информация о начислениях и удержаниях |
| Сведения об инвалидности (дата выдачи, срок действия) |
| Статус застрахованного лица |
| Семейное положение |
| Сведения о воинском учете (отношение к воинской обязанности, к воинскому учету, наличие мобилизационного предписания, реквизиты военного билета, воинское звание, состав (профиль), категория запаса, годность к военной службе, номер команды/партии) |
| 4. Обработка персональных данных в ИСПДн «1С: Бухгалтерия» |
| Общедоступные | Фамилия, имя, отчество (в том числе при смене) | - ведение бухгалтерского учета;- реализация трудовых отношений;- награждение граждан, удостоенных наградами Главы поселения;- пенсионное обеспечение муниципальных служащих;- обеспечение установленных законодательством Российской Федерации условий труда, гарантий и компенсаций;- исполнение судебных актов, актов других органов и должностных лиц; |
| Дата рождения |
| Место рождения |
| Адрес регистрации по месту жительства, дата регистрации, в том числе при смене места регистрации |
| Адрес места жительства |
| Телефон (мобильный, домашний, рабочий) |
| Место работы, подразделение  |
| Занимаемая должность |
| Документ, удостоверяющий личность (тип документа, серия, номер, дата выдачи, кем выдан, код подразделения) |
| Гражданство |
| СНИЛС |
| ИНН |
| Адрес электронной почты |
| Информация о членах семьи (степень родства, ФИО, дата рождения) |
| Пол |
| Табельный номер |
| Социальное положение (льготы) |
| Информация об образовании (уровень образования, наименование учебного заведения, год окончания учебы, специальность) |
| Данные о трудовой деятельности |
| Данные об отпусках, в том числе без сохранения заработной платы, по уходу за ребенком, командировках, работах в выходные и праздничные дни |
| Сведения о периодах временной нетрудоспособности |
| Вид занятости |
| Дата приема на работу/увольнения, перевода на другую работу |
| Знание иностранных языков |
| Данные об ученой степени, ученых званий, научных трудов, изобретений |
| Информация о начислениях и удержаниях |
| Сведения об инвалидности (дата выдачи, срок действия) |
| Статус застрахованного лица |
| Семейное положение |
| Сведения о воинском учете (отношение к воинской обязанности, к воинскому учету, наличие мобилизационного предписания, реквизиты военного билета, воинское звание, состав (профиль), категория запаса, годность к военной службе, номер команды/партии) |
|  | Банковские реквизиты |  |
| 5. Обработка персональных данных без использования средств автоматизации |
| Общедоступные | Фамилия, имя, отчество (в том числе при смене) | - решение вопросов местного значения;- обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, окружных законов и иных нормативно-правовых актов субъектов Российской Федерации, нормативно-правовых актов органов местного самоуправления;- оказание муниципальных услуг; - выполнение отдельных государственных полномочий;- противодействие коррупции;- создание общедоступных источников персональных данных; - размещение на официальном сайте органов местного самоуправления сельского поселения Усть-Юган; - осуществление аналитических, статистических или иных исследовательских целей;- награждение граждан, удостоенных наградами Главы поселения;- учет граждан, удостоенных государственных и ведомственных наград, наград Главы поселения, Главы Нефтеюганского района;- регистрационный учет граждан; - ведение похозяйственных книг;- ведение бухгалтерского учета;- осуществление первичного воинского учета;- рассмотрение обращений граждан и последующее уведомление их о результатах рассмотрения;- оформление трудовых отношений;- пенсионное обеспечение муниципальных служащих;- обеспечение кадровой работы, в том числе содействие работникам в прохождении муниципальной службы (выполнении работы), обучении и должностном росте;- формирование резерва управленческих кадров;- учет результатов исполнения работниками должностных обязанностей;- обеспечение личной безопасности и сохранности имущества работника;- обеспечение установленных законодательством Российской Федерации условий труда, гарантий и компенсаций;- защита законных интересов физических и юридических лиц, общества и государства от административных правонарушений;- исполнение судебных актов, актов других органов и должностных лиц;- принятие решения о трудоустройстве;- установление личности. |
| Место рождения |
| Место работы, подразделение |
| Телефон (мобильный, домашний, рабочий) |
| Профессия |
| Данные о трудовой деятельности |
| Занимаемая должность |
| Данные об отпусках, в том числе без сохранения заработной платы, по уходу за ребенком, командировках, работах в выходные и праздничные дни) |
| Сведения о периодах временной нетрудоспособности |
| Банковские реквизиты |
| Военно-учетная специальность |
| Сведения о приеме и снятии с воинского учета |
| Пол |
| Дата рождения |
| Табельный номер |
| Номер учетной карточки к военному билету |
| Документ, удостоверяющий личность (тип документа, серия, номер, дата выдачи, кем выдан, код подразделения) |
| Гражданство |
| Реквизиты загранпаспорта (серия, номер, кем и когда выдан) |
| Адрес места жительства |
| Адрес регистрации по месту жительства/ по месту пребывания, дата регистрации, в том числе при смене места регистрации/ места пребывания |
| СНИЛС |
| ИНН |
| Семейное положение |
| Социальное положение (информация о льготах, реквизиты удостоверения) |
| Информация о членах семьи (степень родства, ФИО, дата рождения, адрес регистрации, адрес проживания) |
| Информация об образовании (уровень образования, наименование учебного заведения, место его нахождения, год окончания учебы, специальность, квалификация, класс, курс обучения, факультет или отделение (если не окончил, то с какого курса ушел)) |
| Сведения о получении военных образований (уровень, наименование военного учебного заведения, факультет, количество курсов, реквизиты диплома, дата получения, профессия) |
| Знание иностранных языков и языков народов СНГ, степень владения |
| Данные об ученой степени, ученых званий, научных трудов, изобретений, печатной продукции |
| Сведения о воинском учете (отношение к воинской обязанности, категория годности, реквизиты военного билета (серия, номер, дата выдачи, кем выдан), место принятия присяги, дата принятия присяги, разряд состава запаса, номер военно-учетной специальности, кодовое обозначение военно-учетной специальности, воинская должность, состав воинского учета, получение мобилизационного предписания, воинское звание, категория запаса, группа учета, профиль воинского учета), данные об увольнении из Вооруженных сил Российской Федерации (дата увольнения, номер и дата приказа) |
| Информация о спортивных разрядах, званиях |
| Сведения о наличии/отсутствии судимости, фактов привлечения к судебной ответственности |
| Сведения о поощрении, государственных и ведомственных наградах, наградах Главы поселения, Главы Нефтеюганского района (наименование награды, наименование документа, серия и номер, дата выдачи) |
| Сведения о прохождении военной, альтернативной гражданской службы (воинская часть, воинская должность, период службы, полное кодовое обозначение ВУС, тип (марка) ВВТ, дата и основания увольнения |
| Сведения о медицинском освидетельствовании (дата прохождения комиссии, комиссия, заключение комиссии, дата повторного освидетельствования, ранения, контузии, характер ранения, контузии, дата ранения) |
| Сведения о военных сборах (год прохождения, период прохождения, воинская часть, тип (марка) ВВТ, должность) |
| Сведения о боевых действиях (место прохождения, период прохождения, воинская часть, занимаемая должность) |
| Данные о бронировании (дата бронирования, спец. Учет, удостоверение отсрочки, период отсрочки) |
| Основные антропометрические данные (рост, размер головного убора, размер противогаза, размер обмундирования, ростовка, размер обуви) |
| Место и дата прибытия граждан |
| Информация о пребывании в мобилизационном людском резерве |
| Адрес электронной почты |
| Реквизиты документов, подтверждающих право собственности, владения, пользования жилым помещением, земельным участком |
| Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера |
| Реквизиты актовой записи о регистрации/ расторжении брака, о рождении/ смерти, установлении отцовства |
| Сведения о назначенной пенсии за выслугу лет, по старости |
| Информация о жилищном фонде сельского поселения Усть-Юган (вид пользования/владения, сроки найма, год постройки, количество комнат, этажность, площадь, материал стен, перегородок, материал кровли, кадастровый номер, кадастровая и рыночная стоимость) |
| Информация о хозяйственных постройках, расположенных в сельском поселении Усть-Юган |
| Информация о земельных участках, находящихся в пользовании граждан (вид пользования/владения, сроки аренды, площадь, кадастровый номер, кадастровая и рыночная стоимость) |
| Информация о транспортных, средствах, принадлежащих жителям поселения |
| Сведения о повышении квалификации, профессиональной переподготовке, аттестации, прохождении квалификационного экзамена, прохождения инструктажей, обучении и проверке знаний, включении в резерв управленческих кадров, исключении из резерва управленческих кадров, присвоении классного чина, дипломатического ранга |
| Контактные данные кадровой службы предыдущих работодателей |
| Информация о пребывании за границей |
| Информация об участии в центральных, республиканских, краевых, областных, окружных, городских, районных, местных выборных органах |
| Данные водительского удостоверения |
| Сведения о состоянии здоровья |
| Информация о наличии родственников в организации, навыков машинописи, стенографии, работы с диктофоном, компьютером |
| Данные полиса обязательного медицинского страхования |
| Данные о применении/снятии дисциплинарного взыскания |
| Данные о доплатах, надбавках, начислениях и удержаниях |
| Реквизиты трудового договора, дополнительного соглашения к трудовому договору |
| Вид, характер работы |
| Реквизиты трудовой книжки и вкладыша в нее |
| Сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых государственным гражданским служащим или муниципальным служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации или муниципальной службы, размещались общедоступная информация, а также данные, позволяющие его идентифицировать  |
| Специальные | Национальность | Ведение первичного воинского учета, ведение похозяйственных книг, ведение кадрового учета |
| Биометрические | Фотография | Установление личности, размещение на официальном сайте органа местного самоуправления сельское поселение Усть-Юган |
| 6. Обработка персональных данных в ИСПДн «МАИС ЗАГС» |
| Общедоступные | Фамилия, имя, отчество (в том числе при смене) | Выполнение отдельных государственных полномочий |
| Место рождения |
| Данные о трудовой деятельности |
| Пол |
| Дата рождения |
| Документ, удостоверяющий личность (тип документа, серия, номер, дата выдачи, кем выдан, код подразделения) |
| Гражданство |
| Адрес места жительства |
| Адрес регистрации по месту жительства/ по месту пребывания, дата регистрации, в том числе при смене места регистрации/ места пребывания |
| Семейное положение |
| Информация о членах семьи (степень родства, ФИО, дата рождения, адрес регистрации, адрес проживания) |
| Информация об образовании (уровень образования, наименование учебного заведения, место его нахождения, год окончания учебы, специальность, квалификация, класс, курс обучения, факультет или отделение (если не окончил, то с какого курса ушел)) |
| Реквизиты актовой записи о регистрации/ расторжении брака, о рождении/ смерти, установлении отцовства |
| Специальные | Национальность | Выполнение отдельных государственных полномочий |

[Приложение](#Пр1) № 13
к постановлению администрации

сельского поселения Усть-Юган

 от 23.11.2018 № 239-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 Операторов, в которых размещены информационные системы, 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», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказом ФСТЭК России от 11.02.2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
	2. Обеспечение безопасности помещений Операторов, где расположены информационные системы персональных данных (далее – ИСПДн), ведется обработка персональных данных (далее – ПДн), а также где расположено коммутационное оборудование и сервера, направлено на исключение возможности несанкционированного доступа к техническим средствам, входящим в состав ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.
	3. Защита от проникновения посторонних лиц в помещения операторов обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией.
2. Предъявляемые требования к помещениям и порядок доступа к ним
	1. Помещения Операторов, в которых размещены ИСПДн и ведется обработка ПДн (далее - помещения), должны соответствовать следующим требованиям:
* обеспечивать сохранность технических средств;
* исключать возможность бесконтрольного проникновения в помещения;
* исключать возможность визуального просмотра обрабатываемой информации посторонними лицами;
* 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.
	1. Перечень должностей Операторов, доступ которых в помещения необходим для выполнения ими должностных (трудовых) обязанностей приведен в приложении 1 к настоящему постановлению.
	2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 2.2 настоящего Положения, разрешено в период рабочего времени в соответствии с утвержденным графиком работы Операторов, 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. 2.2 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.
	4. В случае отсутствия сотрудников в помещении в рабочее время, помещение должно быть закрыто на ключ.
	5. Вскрытие и закрытие помещений осуществляется сотрудниками данной ИСПДн.
	6. Перед закрытием помещения по окончании рабочего времени лица, непосредственно обрабатывающие персональные данные, обязаны:
* убрать бумажные и электронные носители, содержащие персональные данные, в металлические шкафы (сейфы), опечатать их;
* отключить технические средства обработки информации и электроприборы от сети.
	1. Сотрудник, последний покидающий помещение, обязан:
* закрыть окна;
* выключить освещение;
* закрыть дверь помещения.
	1. Перед открытием помещения первый прибывший сотрудник обязан:
* провести внешний осмотр двери и дверного замка с целью установления их целостности;
* открыть дверь и осмотреть помещение;
* проверить наличие и целостность замков на металлических шкафах (сейфах) с целью установления их целостности.
	1. При обнаружении факта взлома двери (дверного замка) помещения сотрудник обязан:
* не вскрывая помещение, незамедлительно сообщить непосредственному руководителю;
* в присутствии не менее двух лиц и непосредственного руководителя вскрыть помещение и осмотреть его;
* составить акт о факте взлома двери (дверного замка) и направить его руководителю.
1. 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-схема контролируемой зоны помещений по адресу: 628325, Тюменская область, ХМАО-Югра, Нефтеюганский район, п. Усть-Юган, дом 5, приведена в приложении 1 к настоящему положению.
2. Перечень помещений, в которых осуществляется обработка

персональных данных

* 1. Перечень помещений, в которых осуществляется обработка персональных данных, приведен в приложении 2 к настоящему положению.
1. Организация и порядок производства ремонтно-строительных

работ

* 1. Рабочие и специалисты ремонтно-строительных организаций допускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего лица из числа сотрудников.
	2. Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.
1. Организация охраны
	1. Для охраны помещений Операторов, используется охранная сигнализация.
	2. Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо закрывать его на ключ.
2. Уборка помещений
	1. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.
	2. 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.

46

Приложение 1

к Положению 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

Рисунок 1 - План-схема границ контролируемой зоны Оператора

 - граница контролируемой зоны

47

Приложение 2

к Положению 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

Перечень помещений Операторов, в которых осуществляется

обработка персональных данных с использованием информационных систем обработки персональных данных

|  |  |  |
| --- | --- | --- |
| № п/п | Помещение | Наименование должностей, доступ которых в Помещения необходим для выполнения ими должностных (трудовых) обязанностей |
|  | Кабинет № 3 | Бухгалтер, Главный специалист, Экономист |
|  | Кабинет № 4 | Главный бухгалтер, директор МКУ «АХС сп Усть-Юган» |
|  | Кабинет № 5 | Специалист адресно-справочной работы, инспектор по первичному воинскому учету |
|  | Кабинет № 9 | Начальник организационно-правового отдела, ведущий специалист, делопроизводитель, специалист по работе с молодежью |

[Приложение](#Пр1) № 14
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ПОЛИТИКА

в отношении обработки персональных данных

1. Общие положения
	1. Политика в отношении обработки персональных данных в МУ «Администрация сельского поселения Усть-Юган» и подведомственном ей учреждении (далее – Оператор) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологий и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и другими нормативными правовыми актами, регулирующими отношения, связанные с обработкой персональных данных.
	2. Политика определяет порядок и условия обработки персональных данных Оператора с использованием средств автоматизации и без использования таких средств.
	3. Политика вступает в силу с момента подписания постановления администрации сельского поселения Усть-Юган Главой поселения.
	4. Политика подлежит пересмотру в ходе периодического анализа со стороны руководства МУ «Администрация сельского поселения Усть-Юган», а также в случаях изменения законодательства Российской Федерации в области обеспечения безопасности персональных данных (далее - ПДн).
	5. Политика подлежит опубликованию на официальном сайте органа местного самоуправления сельского поселения Усть-Юган в течение 10 дней после её утверждения.
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. Цели обработки персональных данных

Обработка ПДн осуществляется Оператором в следующих целях:

- решение вопросов местного значения;

- обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, окружных законов и иных нормативно-правовых актов субъектов Российской Федерации, нормативно-правовых актов органов местного самоуправления;

- оказание муниципальных услуг;

- выполнение отдельных государственных полномочий;

- противодействие коррупции;

- создание общедоступных источников персональных данных;

- размещение на официальном сайте органов местного самоуправления сельского поселения Усть-Юган;

- осуществление аналитических, статистических или иных исследовательских целей;

- награждение граждан, удостоенных наградами Главы поселения;

- учет граждан, удостоенных государственных и ведомственных наград, наград Главы поселения, Главы Нефтеюганского района;

- регистрационный учет граждан;

- ведение похозяйственных книг;

- ведение бухгалтерского учета;

- осуществление первичного воинского учета;

- рассмотрение обращений граждан и последующее уведомление их о результатах рассмотрения;

- реализация трудовых отношений;

- принятие решения о трудоустройстве;

- пенсионное обеспечение муниципальных служащих;

- обеспечение кадровой работы, в том числе содействие работникам в прохождении муниципальной службы (выполнении работы), обучении и должностном росте;

- формирование резерва управленческих кадров;

- учет результатов исполнения работниками должностных обязанностей;

- обеспечение личной безопасности и сохранности имущества работника;

- обеспечение установленных законодательством Российской Федерации условий труда, гарантий и компенсаций;

- защита законных интересов физических и юридических лиц, общества и государства от административных правонарушений;

- исполнение судебных актов, актов других органов и должностных лиц;

- установление личности.

1. Категории субъектов, персональные данные которых обрабатываются
	1. В соответствии с целями обработки ПДн, указанными в п. 3. настоящей Политики, Оператором осуществляется обработка следующих категорий субъектов персональных данных:
* физические лица, обратившиеся за государственной или муниципальной услугой (заявители) и их представители;
* собственники и наниматели жилых помещений и члены их семей;
* собственники и арендаторы земельных участков и нежилых помещений;
* участники аукционов по приватизации муниципального имущества;
* сотрудники, в том числе уволенные;
* родственники сотрудников, в том числе уволенных;
* физические лица, обратившиеся в учреждение с жалобой (обращением);
* физические лица, подлежащие награждению наградами Главы поселения, награжденные государственными и ведомственными наградами, наградами Главы поселения, Главы Нефтеюганского района;
* граждане, претендующие на замещение должностей муниципальной службы и члены их семей;
* граждане, состоящие в резерве управленческих кадров и члены их семей;
* граждане, претендующие на включение в резерв управленческих кадров и члены их семей;
* призывники;
* военнослужащие и члены их семей;
* лица, состоящие на воинском учете в с.п. Усть-Юган и члены их семей;
* физические лица, участвующие в конкурсах, грантах, мероприятиях, проводимых Администрацией поселения;
* физические лица, которым осуществляется перечисление средств, удерживаемых у сотрудников в соответствии с судебными решениями или их заявлениями, в том числе алиментов;
* физические лица, оказывающие услуги по договорам гражданско-правового характера или по договорам оказания услуг и выполнения работ;
* физические лица, совершившие административное правонарушение, а также иные участники производства по делам об административных правонарушениях, в том числе и несовершеннолетние лица, совершившие административное правонарушение и общественно опасные деяния, не подлежащие уголовной ответственности, родители или иные законные представители несовершеннолетних, а также иные участники производства по делам об административных правонарушениях и материалов о фактах совершения несовершеннолетними, не подлежащими уголовной ответственности, общественно опасных деяний, обработка персональных данных которых необходима для реализации полномочий Администрации поселения;
* физические и их законные представители, обратившиеся в администрацию поселения с заявлениями;
* индивидуальные предприниматели, осуществляющие деятельность на территории сельского поселения Усть-Юган;
* депутаты Совета депутатов сельского поселения Усть-Юган;
* руководители организаций, осуществляющие деятельность на территории сельского поселения Усть-Юган;
* Члены Общественного совета сельского поселения Усть-Юган;
* Члены Общества инвалидов сельского поселения Усть-Юган;
* Члены Совета ветеранов сельского поселения Усть-Юган;
* Члены Совета молодежи при Совете депутатов сельского поселения Усть-Юган;
* получатели муниципальной пенсии за выслугу лет;
* физические лица, выполняющие работы по договорам гражданско-правового характера.
1. Принципы обработки персональных данных
	1. Обработка ПДн осуществляется на законной основе.
	2. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.
	3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.
	4. Обработке подлежат только те ПДн, которые отвечают целям их обработки.
	5. Содержание и объем ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточным по отношению к заявленным целям их обработки.
	6. При обработке ПДн обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.
	7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
2. Условия обработки персональных данных
	1. Условия обработки специальных категорий ПДн:
* Обработка специальных категорий ПДн осуществляется Оператором с условием, что субъект ПДн дал согласие в письменной форме на обработку своих ПДн.
	1. Условия обработки иных категорий ПДн:
		1. Обработки иных категорий ПДн осуществляется Оператором с соблюдением следующих условий:
* обработка ПДн 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;
* обработка ПДн 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](http://www.consultant.ru/document/cons_doc_LAW_103023/) от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта ПДн на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
* обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
* обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн.
	1. Условия обработки общедоступных категорий ПДн:
		1. Осуществляется обработка ПДн, сделанных общедоступными с согласия субъекта ПДн.
	2. Поручение обработки ПДн:
		1. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.
		2. Лицо, осуществляющее обработку ПДн по договору с Оператором, соблюдает принципы и правила обработки ПДн, предусмотренные настоящей Политикой. В договоре с Оператором определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также указаны требования к защите обрабатываемых ПДн.
		3. 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.
1. Конфиденциальность персональных данных
	1. Сотрудники Оператора, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.
2. Общедоступные источники персональных данных
	1. В целях информационного обеспечения Оператор размещает ПДн на общедоступных источниках. Сведения о субъекте ПДн исключаются из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.
	2. В общедоступные источники ПДн включены следующие сведения:

- фамилия, имя, отчество;

- должность;

- номер телефона;

- место работы;

- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера отдельных категорий лиц и членов их семей;

- фотография;

- адрес электронной почты;

- иные сведения, указанные в согласии на обработку персональных данных.

1. Согласие субъекта персональных данных на обработку его персональных данных
	1. При необходимости обеспечения условий обработки ПДн субъекта может предоставляться согласие субъекта ПДн на обработку его ПДн.
	2. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, ели иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Оператором.
	3. Согласие на обработку ПДн может быть отозвано субъектом ПДн.
	4. Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн возлагается на Оператора.
	5. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_112701/) электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:
* фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
* фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
* наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
* срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
* подпись субъекта персональных данных.
	1. Порядок получения в форме электронного документа согласия субъекта ПДн на обработку его ПДн в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.
	2. В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн.
	3. В случае смерти субъекта ПДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.
1. Право субъекта персональных данных на доступ
к его персональным данным
	1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:
* подтверждение факта обработки ПДн Оператором;
* правовые основания и цели обработки ПДн;
* цели и применяемые Оператором способы обработки ПДн;
* наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
* обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
* сроки обработки ПДн, в том числе сроки их хранения;
* порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
* информацию об осуществленной или о предполагаемой трансграничной ПДн;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.
	1. Субъект ПДн имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:
* обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
* обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно- процессуальным [законодательством](http://www.consultant.ru/document/cons_doc_LAW_34481/) Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;
* обработка ПДн осуществляется в соответствии с [законодательством](http://www.consultant.ru/document/cons_doc_LAW_32834/) о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
* доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;
* обработка ПДн осуществляется в случаях, предусмотренных [законодательством](http://www.consultant.ru/document/cons_doc_LAW_66069/) Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.
	1. Субъект ПДн имеет право на получение сведений, указанных в п. 10.1. настоящей Политики, за исключением случаев, при которых доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц. Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн 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. 10.1. настоящей Политики, должны быть предоставлены субъекту ПДн Оператору в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.
	3. Сведения, указанные в п. 10.1. настоящей Политики, предоставляются субъекту ПДн или его представителю <Оператором при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн <Оператором, подпись субъекта ПДн 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. 10.1. настоящей Политики, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 10.1. настоящей Политики, и ознакомления с такими ПДн 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 ПДн.
	5. Субъект ПДн вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в п. 10.1. настоящей Политики, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 10.5. настоящей Политики, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать основание направления повторного запроса.
	6. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, несоответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.
1. Право на обжалование действий или бездействий Оператора
	1. Если субъект ПДн считает, что Оператор осуществляет обработку его ПДн с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке.
	2. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
2. Меры, направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006

№ 152-ФЗ «О персональных данных»

* 1. Назначение ответственного за организацию обработки ПДн.
	2. Издание документа, определяющего политику Оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
	3. Применение правовых, организационных и технических мер по обеспечению безопасности ПДн.
	4. Утверждение правил проведения внутреннего контроля соответствия обработки ПДн требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальных актов Оператора.
	5. Проведение ознакомления сотрудников Оператора непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о персональных данных, в том числе, документами, определяющими политику Оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн.
1. Меры по обеспечению безопасности персональных данных
при их обработке
	1. Определение угроз безопасности ПДн при их обработке в ИСПДн.
	2. Применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн.
	3. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.
	4. Ведение учета машинных носителей ПДн.
	5. Выполнение мер по обнаружению фактов несанкционированного доступа к ПДн и принятию соответствующих мер.
	6. Определение комплекса мер по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
	7. Установление правил доступа к ПДн, обрабатываемым в ИСПДн.
	8. Для исключения несанкционированного просмотра ПДн на устройствах вывода (отображения, печати) информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны, их не размещают напротив оконных проемов, входных дверей, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.
	9. Выявление, анализ и устранение уязвимостей ИСПДн на этапах создания и эксплуатации ИСПДн. Такие проверки проводятся с периодичностью один раз в год, с учетом того, что должны быть проведены обязательные проверки для критических уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИСПДн. При выявлении уязвимости составляется отчет и разрабатывается план по их устранению.
	10. Непрерывный контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности персональных данных.

[Приложение](#Пр1) № 15
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в информационных системах персональных данных

1. Общие положения
	1. Ответственный за организацию обработки персональных данных в МУ «Администрация сельского поселения Усть-Юган» и подведомственном ей учреждении назначается распоряжением администрации сельского поселения Усть-Юган и отвечает за организацию обеспечения своевременного и квалифицированного выполнения сотрудниками Оператора требований по организации обработки и обеспечения безопасности персональных данных (далее - ПДн).
	2. Ответственный за организацию обработки персональных данных (далее - Ответственный) 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»;
* 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»;
* Иными нормативными правовыми актами, регламентирующими вопросы обработки и защиты персональных данных;
* Политикой в отношении обработки персональных данных;
* Настоящей Инструкцией.
1. Основные функции и обязанности ответственного

за организацию обработки персональных данных

* 1. Функции Ответственного:

Доведение до сведения допущенных к обработке ПДн сотрудников положений законодательства о персональных данных, локальных актов по вопросам обработки и защиты персональных данных.

Общий контроль за соблюдением сотрудниками законодательства о персональных данных и мер по защите персональных данных.

Осуществление контроля за выполнением разовых и периодических мероприятий по обеспечению безопасности персональных данных.

Взаимодействие с субъектами персональных данных по вопросам обработки и защиты персональных данных.

Взаимодействие c органами, контролирующими обработку и защиту персональных данных, при проведении проверок.

Поддержание локальных организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных в актуальном состоянии.

2.2. Ответственный обязан:

Знать:

* перечень ПДн, обрабатываемых Оператором;
* перечень ИСПДн Оператора;
* перечень должностей Оператора, доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей;
* условия и технологический процесс обработки ПДн Оператором;
* законодательство Российской Федерации о ПДн.

Представлять по требованию руководителя Оператора отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных сотрудниками нарушениях установленных требований по защите информации.

Следить за изменениями законодательства Российской Федерации о ПДн, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации в ИСПДн и правилам обработки ПДн.

Осуществлять внутренний контроль за соблюдением Оператором и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите ПДн, а также локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и ПДн, машинными носителями ПДн.

Доводить до сведения сотрудников Оператора положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обеспечения и защиты обработки ПДн, требований к защите ПДн путем проведения занятий и инструктажа сотрудников с периодичностью один раз в год.

Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

По запросу субъекта персональных данных сообщать ему сведения об обработке его персональных данных, в том числе ознакомить с Политикой обработки персональных данных Оператора.

По запросу субъекта персональных данных организовать уточнение, блокирование или уничтожение персональных данных указанного субъекта.

Вести журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных (таблица 4 приложения 8).

Осуществлять контроль за сбором с сотрудников, допущенных к обработке ПДн, письменного обязательства о соблюдении режима конфиденциальности персональных данных и соблюдении правил их обработки (обязательство о неразглашении информации, содержащей ПДн).

Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения должностных (трудовых) обязанностей.

Осуществлять контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн с периодичностью один раз в три месяца в соответствии с Инструкцией по идентификации и аутентификации пользователей. А также контролировать наличие документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей с периодичностью раз в пол года.

Осуществлять сопровождение и решение вопросов проверочной комиссии надзорных органов в сфере обработки ПДн при проведении проверочных мероприятий.

Принимать меры по реагированию в случае возникновения нештатных и аварийных ситуаций с целью ликвидации их последствий.

Вносить свои предложения по совершенствованию мер защиты ПДн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

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

3. Права ответственного за организацию обработки

персональных данных

3.1. Ответственный имеет право:

Иметь доступ к информации, касающейся обработки персональных данных Оператором и включающей:

* цели обработки ПДн;
* категории обрабатываемых ПДн;
* категории субъектов, ПДн которых обрабатываются;
* правовые основания обработки ПДн;
* перечень действий с ПДн, общее описание используемых Операторм способов обработки ПДн;
* дату начала обработки ПДн;
* срок или условия прекращения обработки ПДн;
* сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
* сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

Требовать от сотрудников выполнения федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативно-правовых актов в части работы с ПДн.

Требовать от сотрудников Оператора письменных объяснений при нарушении требований по обработке и обеспечении безопасности ПДн.

Не допускать сотрудников до обработки персональных данных до подписания ими письменного обязательства о неразглашении информации, содержащей персональные данные.

Указывать сотрудникам, допущенным к обработке ПДн, на необходимость выполнения установленных мер по обеспечению безопасности персональных данных.

Указывать сотрудникам, участвующим в обработке персональных данных, на необходимость осуществления уточнения, блокирования или уничтожения персональных данных по запросу субъекта.

Право доступа ко всем локальным нормативным актам в области обработки и защиты персональных данных.

Блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн.

Запрашивать и получать от всех сотрудников сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного.

Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости ПДн.

Привлекать к реализации мер, направленных на выполнение требований законодательства о ПДн, иных сотрудников Оператора с возложением на них соответствующих обязанностей и закреплением ответственности.

Проходить обучение по защите ПДн в учебных центрах и центрах повышения квалификации.

 Выносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обеспечением безопасности персональных данных.

4. Ответственность

4.1. Ответственный за организацию обработки персональных данных несет ответственность за:

4.1.1. Соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обработке и обеспечению безопасности ПДн.

4.1.2. Осведомленность сотрудников, участвующих в обработке персональных данных, в вопросах обеспечения безопасности ПДн.

4.1.3. Комплектность и содержание локальных нормативных актов в области защиты ПДн.

4.1.4. Выполнение обязанностей перед субъектами ПДн и уполномоченным органом по защите прав субъектов персональных данных.

 4.2. 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.

[Приложение](#Пр1) № 16
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

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

1. Общие положения
	1. Настоящая Инструкция определяет основные функции, обязанности, права и ответственность ответственного за обеспечение
	безопасности персональных данных в информационных системах персональных данных (далее - администратора безопасности) информации при эксплуатации ИСПДн и является дополнением к действующим нормативным документам по вопросам обеспечения режима обращения конфиденциальной информациии не исключает обязательного выполнения их требований. С настоящей Инструкцией должен быть под роспись ознакомлен администратор безопасности информации.
	2. Администратор безопасности информации назначается распоряжением администрации сельского поселения Усть-Юган.
	3. Администратор безопасности информации подчиняется лицу, ответственному за организацию обработки ПДн.
	4. Администратор безопасности информации в своей работе руководствуется настоящей инструкцией, Инструкцией по обеспечению безопасности СО ПДн, и другими локально-нормативными актами администрации Нефтеюганского района.
	5. Администратор безопасности информации отвечает за поддержание необходимого уровня безопасности объектов защиты.
	6. Администратор безопасности информации является ответственным должностным лицом администрации сельского поселения Усть-Юган, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.
	7. Администратор безопасности информации осуществляет методическое руководство пользователей ИСПДн и системных администраторов, в вопросах обеспечения безопасности ПДн.
	8. Требования администратора безопасности информации, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.
	9. Администратор безопасности информации несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.
2. Основные функции администратора безопасности информации
	1. Организация предоставления пользователям ИСПДн операторов технической возможности уничтожать либо обезличивать ПДн в необходимых случаях.
	2. По указанию лица, ответственного за организацию обработки ПДн, администратор безопасности информации организует предоставление пользователям ИСПДн операторов возможность осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных.
	3. Подготовка и корректировка, при необходимости, инструкции пользователей защищаемых ИСПДн.
	4. Организация выполнения всех действий по настройке и сопровождению СЗПДн в процессе ее эксплуатации.
	5. Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.
	6. Настройка и сопровождение подсистемы управления доступом
	к информации в процессе эксплуатации ИСПДн включает:
		1. Подготовку идентификаторов и паролей доступа, доведение их
		до пользователей.
		2. Формирование матрицы доступа для ИСПДн.
		3. Настройку полномочий для каждого пользователя ко всем элементам защищаемых информационных ресурсов в соответствии с требованиями документов «Матрица доступа к ресурсам ИСПДн Оператора.
		4. Ввод описаний пользователей ИСПДн в информационные базы СЗИ, установленных в ИСПДн.
		5. Разблокирование ПЭВМ, анализ информации о несанкционированных действиях (НСД).
		6. Своевременное удаление описания пользователя из базы данных СЗИ при смене пользователя.
		7. Контроль состава технических средств и программного обеспечения ИСПДн.
		8. Контроль за отсутствием физического доступа к основным техническим средствам и системе (далее так же – ОТСС) (опечатывание).
	7. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн включает:
		1. Определение информации, подлежащей регистрации в системном журнале СЗИ;
		2. Регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
		3. Сохранение зарегистрированной информации, необходимой для возможного расследования фактов НСД или восстановления информационных ресурсов.
	8. Сопровождение подсистемы обеспечения целостности информации ИСПДн включает:
		1. Тестирование установленной в ИСПДн СЗИ от НСД при изменении программной среды или полномочий пользователей.
		2. Восстановление программной среды, программных средств и настроек СЗИ при сбоях.
		3. Создание двух копий дистрибутивов программных средств СЗИ от НСД, контроль их работоспособности и целостности.
		4. Контроль поддержания установленного порядка и правил антивирусной защиты информации в ИСПДн со стороны пользователей.
		5. Участие в периодическом обновлении антивирусных средств, установленных в ИСПДн.
	9. Немедленное реагирование на инциденты безопасности.
3. Обязанности

Администратор безопасности информации обязан:

* 1. Знать сведения, необходимые для установки, настройки и управления СЗИ установленных операторами, изложенные в технической документации, поставляемой совместно с дистрибутивами СЗИ.
	2. Проверять готовность средств и систем защиты информации к работе поддерживать их работоспособность.
	3. Периодически анализировать состояние защиты ИСПДн и ее отдельных подсистем.
	4. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
	5. Проводить обучение лиц, использующих средства защиты информации, применяемые в ИСПДн Оператора, правилам работы с ними.
	6. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также соблюдение правил работы с элементами ИСПДн и средствами защиты информации.
	7. Контролировать размещение информационных систем, специального оборудования и охрану помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключение возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
	8. Контролировать соответствие фактического состава пользователей и объектов доступа ИСПДн с данными документа «Матрица доступа к ресурсам ИСПДн Оператора с внесением изменений в него при необходимости.
	9. Не допускать к работе на элементах ИСПДн посторонних лиц.
	10. Периодически контролировать соответствие фактического состава технических средств и программного обеспечения ИСПДн с данными технического паспорта, целостность печатей (пломб) системных блоков ОТСС.
	11. Осуществлять контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
	12. Принимать меры по восстановлению в случае неработоспособности операционной системы, прикладных программ и системы защиты информации. Если восстановление функционирования программной среды штатными средствами операционной системы невозможно или не было заранее подготовлено,
	то необходима полная переустановка ПО.
	13. Допускать к обслуживанию и ремонту технических средств работников, имеющих соответствующее разрешение на работу.
	14. Регистрировать и проводить учет машинных носителей ПДн.
	15. Уничтожать машинные носители ПДн.
	16. Снимать все узлы и блоки с элементами накопления и хранения ПДн (ЖМД, USB-накопители и т.д.) и оставлять их в хранилищах при сдаче в ремонт технических средств ИСПДн.
	17. Участвовать в приемке новых программных средств.
	18. Принимать меры по немедленному реагированию на инциденты безопасности ПДн.
	19. Докладывать лицу, ответственному за организацию обработки ПДн, о нештатных ситуациях на объектах ИСПДн, инцидентах нарушения информационной безопасности и допущенных пользователями нарушениях установленных требований по защите информации.
1. Права
	1. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и в расследовании фактов несанкционированного доступа.
	2. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
2. Ответственность

Администратор безопасности информации несет ответственность за:

* 1. Разглашение сведений, составляющих конфиденциальную информацию, ставшую известной ему по роду работы.
	2. Несанкционированное предоставление доступа к защищаемой информации, передачу посторонним лицам информацию об идентификаторах
	и паролях пользователей.
	3. Несанкционированное отключение СЗИ в ИСПДн.
	4. Некачественное проведение работ по обеспечению защиты информации и сопровождению используемой СЗИ.

[Приложение](#Пр1) № 17
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ИНСТРУКЦИЯ

ответственного за эксплуатацию информационной системы

персональных данных

1. Общие положения
	1. Настоящая инструкция определяет основные функции, обязанности, права и ответственность ответственного за эксплуатацию информационной системы персональных данных (далее - ИСПДн) Оператора по вопросам защиты персональных данных (далее - ПДн) в ИСПДн.
	2. Ответственный за эксплуатацию ИСПДн Оператора назначается распоряжением администрации селського поселения Усть-Юган из числа руководителей отделов, эксплуатирующих ИСПДн.
	3. Ответственный за эксплуатацию ИСПДн осуществляет контроль за соблюдением порядка работы пользователей ИСПДн, на которых проводится обработка ПДн, дополнительно к своим непосредственным обязанностям.
	4. Ответственный за эксплуатацию ИСПДн непосредственно подчиняется ответственному за организацию обработки ПДн Оператора в части, касающейся защиты ПДн в ИСПДн Оператора, и осуществляет контроль за выполнением требований организационно-распорядительных документов по обеспечению безопасности ПДн при ее обработке в ИСПДн Оператора.
2. Основные функции ответственного за эксплуатацию

информационной системы персональных данных

* 1. Функции ответственного за эксплуатацию ИСПДн:

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

2.1.2. Ежедневный контроль над отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

* 1. Обязанности ответственного за эксплуатацию ИСПДн:

2.2.1. Знать:

* перечень ПДн, обрабатываемых в ИСПДн Оператора;
* перечень и состав ИСПДн Оператора;
* перечень должностей сотрудников Оператора, доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей;
* условия и технологический процесс обработки ПДн в ИСПДн Оператора.

2.2.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также локальных нормативных актов, регламентирующих порядок действий по защите ПДн.

2.2.3. Осуществлять внутренний контроль за соблюдением сотрудниками ИСПДн Оператора требований законодательства Российской Федерации в области ПДн.

2.2.4. Обеспечивать контроль соблюдения сотрудниками Оператора локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и ПДн, машинными носителями ПДн.

2.2.5. Осуществлять контроль за выполнением сотрудниками ИСПДн мероприятий по защите ПДн в ИСПДн.

2.2.6. Осуществлять контроль за хранением документов, содержащих ПДн, и отсутствием несанкционированного доступа к данным документам, их уничтожение по достижению целей обработки либо контроль процедуры их уничтожения.

2.2.7. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых для выполнения должностных (трудовых) обязанностей.

2.2.8. При появлении новой должности или исключении существующей должности из списка должностей в ИСПДн, которым необходим доступ к ПДн, своевременно предоставить данные ответственному за организацию обработки ПДн в ИСПДн для внесения изменений в перечень должностей Оператора, доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей.

2.2.9. Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

2.2.10. Своевременно реагировать на попытки несанкционированного доступа к ПДн.

2.2.11. Немедленно сообщить ответственному за организацию обработки ПДн в части, касающейся защиты ПДн, об обнаруженных фактах (попытках) несанкционированного доступа к ПДн и автоматизированным рабочим местам (далее - АРМ), и принимать необходимее меры по пресечению нарушений.

2.2.12. Немедленно прекращать работы на АРМ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности ПДн.

2.2.13. Блокировать доступ к ПДн при обнаружении нарушений порядка их обработки.

2.2.14. Осуществлять взаимодействие по обеспечению безопасности ПДн с администратором информационной безопасности ИСПДн и ответственным за организацию обработки ПДн в ИСПДн.

2.2.15. Вносить свои предложения по совершенствованию мер защиты ПДн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

1. Права ответственного за эксплуатацию информационной системы персональных данных

3.1. Ответственный за эксплуатацию ИСПДн имеет право требовать от сотрудников ИСПДн выполнения федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативно-правовых актов в части работы с ПДн.

3.2. Ответственный за эксплуатацию ИСПДн имеет право требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации в соответствии с документом «Описание технологического процесса обработки персональных данных в информационной системе персональных данных» и выполнения инструкций по обеспечению безопасности ПДн в ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право инициировать проведение служебных расследований по фактам нарушения требований защиты ПДн, утвержденных соответствующими инструкциями, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических компонентов ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право давать свои предложения по совершенствованию организационных и технических мер защиты ПДн.

3.4. Блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн.

3.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости ПДн.

3.6. Иметь доступ к информации, касающейся обработки ПДн в соответствующей ИСПДн и включающей:

* цели обработки ПДн;
* категории обрабатываемых ПДн;
* категории субъектов, ПДн которых обрабатываются;
* правовые основания обработки ПДн;
* перечень действий с ПДн, общее описание используемых Оператором способов обработки ПДн;
* дату начала обработки ПДн;
* срок или условия прекращения обработки ПДн;
* сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
* сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.
1. Ответственность ответственного за эксплуатацию

информационных систем персональных данных

* 1. Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия и действия сотрудников вверенной ИСПДн в соответствии с действующим законодательством Российской Федерации.
	2. На ответственного за эксплуатацию ИСПДн возлагается персональная ответственность за качество проводимых им работ в ИСПДн Оператора.

[Приложение](#Пр1) № 18
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных

1. Общие положения
	1. Настоящая Инструкция разработана в соответствии с ГОСТ Р 51188-98 и предназначена для организации порядка проведения антивирусного контроля операторами с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы операторов и возникновения фактов заражения программного обеспечения компьютерными вирусами.
	2. Требования настоящей Инструкции обязательны для выполнения всеми пользователями, обрабатывающими персональные данные посредством электронно-вычислительной техники операторов.
	3. Инструкция устанавливает обязанности пользователей, ответственность за соблюдением мероприятий по защите от вирусов, определяет порядок антивирусного контроля на автономных средствах вычислительной техники, обновления баз вирусных сигнатур и антивирусного программного обеспечения, действий при обнаружении компьютерных вирусов.
2. Антивирусное программное обеспечение
	1. В ИСПДн операторов в качестве антивирусного средства используется сертифицированное по требованиям безопасности информации антивирусное программное обеспечение «Kaspersky Endpoint Security 10 для Windows».
	2. Использование указанного антивирусного ПО должно осуществляться в соответствии с инструкцией пользователя антивирусной программы.
3. Обязанности пользователей
	1. Изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.
	2. В ходе работы в ИСПДн следить за работоспособностью установленного антивирусного ПО и своевременностью установки обновлений компонентов антивирусной программы и вирусных баз.
	3. Сообщать администратору безопасности информации о необходимости проведения обновления антивирусной программы.
	4. Прекращать работу в ИСПДн и сообщить администратору безопасности информации о сигнализации антивирусной программы о вирусной активности.
	5. При проведении работ в ИСПДн с использованием внешних МНИ пользователь обязан перед первым обращением к используемому МНИ проверить его на наличие вредоносных программ и закладок.
	6. Использовать антивирусное программное обеспечение при работе с сетями общего пользования (Интернет).
4. Пользователю запрещается
	1. Отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.
	2. Использовать средства антивирусной защиты информации, отличные от поддерживаемых операторами.
5. Порядок антивирусного контроля
	1. Обязательному антивирусному контролю подлежит любая информация, вводимая с отчуждаемых машинных носителей и полученная из сетей общего пользования.
	2. После установки или изменения программного обеспечения антивирусный контроль должен осуществляться для жестких магнитных дисков.
	3. Профилактический антивирусный контроль должен проводиться не реже одного раза в неделю с лечением (уничтожением) обнаруженных зараженных объектов.
	4. Перед проведением контроля необходимо обновить имеющееся антивирусное ПО до последней версии компонентов ПО и вирусных баз.
	5. При возникновении подозрения на наличие компьютерных вирусов (нестабильная работа ПЭВМ, появление графических или звуковых эффектов, искажения данных и т.п.) следует незамедлительно сообщить об этом администратору безопасности информации, и провести антивирусный контроль ПЭВМ.
	6. При обнаружении вирусов принять меры по недопущению их распространения: определить отчуждаемые машинные носители информации (МНИ), использованные в работе за период после последнего антивирусного контроля, и проверить их на наличие вирусов. Провести лечение или уничтожение зараженных файлов на ЖМД и отчуждаемых МНИ.
	7. При обнаружении нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку. Данный файл не должен содержать информацию ограниченного распространения.
6. Порядок обновления баз вирусных сигнатур
 и антивирусного программного обеспечения
	1. Установка и обновление средств антивирусного контроля на технических средствах ИСПДн осуществляется администратором безопасности информации.
	2. Обновления компонентов антивирусного ПО и баз данных вирусных сигнатур администратор безопасности информации получает по сети Интернет с сайта производителя антивирусного ПО.
7. Ответственность за соблюдением мероприятий по защите от вирусов
	1. Администратор безопасности информации несет ответственность за:
		1. своевременное получение и распространение обновленных баз данных вирусных сигнатур;
		2. своевременное обновление новых лицензионных ключей на антивирусное ПО при истечении их срока действия;
		3. обучение пользователей правилам антивирусного контроля;
		4. соблюдение графика антивирусного контроля пользователями;
		5. последствия заражения ПЭВМ компьютерными вирусами в соответствии с действующим Российским законодательством.
	2. Администратор безопасности информации имеет право:
		1. вносить предложения по совершенствованию системы антивирусной защиты информации операторов;
		2. проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники;
	3. Пользователь несет ответственность за:
		1. допущенное по своей халатности заражение ПЭВМ компьютерными вирусами;
		2. последствия заражения ПЭВМ компьютерными вирусами в соответствии с действующим Российским законодательством.

[Приложение](#Пр1) 19
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ИНСТРУКЦИЯ

по обработке персональных данных без использования средств автоматизации

1. Общие положения
	1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в МУ «Администрация сельского поселения Усть-Юган» и подведомственное ей учреждение, или сотруднику (далее – субъекту персональных данных) МУ «Администрация сельского поселения Усть-Юган» и подведомственного ей учреждения.
	2. Обработка персональных данных, содержащихся в информационных системах персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
	3. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационных системах персональных данных либо были извлечены из нее**.**
	4. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти.
2. Особенности организации обработки персональных данных,

осуществляемой без использования средств автоматизации

* 1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).
	2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
	3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Оператора или лица, осуществляющие такую обработку по договору с Оператором, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти, а также локальными правовыми актами Оператора.
	4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:
* типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;
* типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;
* типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.
	1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).
	2. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.
1. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации
	1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
	2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
	3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

[Приложение](#Пр1) 20
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ИНСТРУКЦИЯ

по работе с инцидентами информационной безопасности

1. Общие положения
	1. Настоящая инструкция устанавливает порядок действий по управлению инцидентами информационной безопасности (далее - ИБ) в МУ «Администрация сельского поселения Усть-Юган» и подведомственном ей учреждении.
	2. Ответственность за выявление инцидентов ИБ и реагирование на них в МУ «Администрация сельского поселения Усть-Юган» и подведомственном ей учреждении возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - ИСПДн) (далее - администратор информационной безопасности ИСПДн).

1.3. В случае обнаружения инцидента ИБ администратор информационной безопасности ИСПДн руководствуется настоящей Инструкцией.

1. Порядок выявления инцидентов информационной безопасности

2.1. Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки персональных данных (далее - ПДн) принимают решение об определении события информационной безопасности к относящимся или не относящимся к инцидентам информационной безопасности (далее - ИБ).

2.2. Инциденты информационной безопасности могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение ПДн, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам Оператора или их хищение.

2.3. Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или иным способом). Среди инцидентов такого типа можно выделить следующие наиболее распространенные:

* утечка ПДн;
* неправомерный доступ к ПДн;
* удаление ПДн;
* компрометация ПДн;
* саботаж;
* мошенничество;
* использование ПДн в личных целях или в мошеннических операциях.

2.4. Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом. Среди инцидентов такого типа можно выделить следующие наиболее распространенные:

* атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
* перехват и подмена трафика;
* фишинг;
* размещение конфиденциальной/провокационной информации в сети Интернет;
* взлом, попытка взлома, сканирование портала;
* сканирование сети, попытка взлома сетевых узлов;
* вирусные атаки;
* неправомерный доступ к ПДн.

2.5. Данный перечень не является исчерпывающим. В общем случае инцидентом является единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое угрожает информационной безопасности ИСПДн.

1. Анализ исходной информации и принятие решения о проведении разбирательства инцидента информационной безопасности
	1. Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн проводят анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий. Источниками и причинами возникновения инцидентов в ИСПДн могут являться:
* действия организаций и отдельных лиц враждебные интересам Оператора;
* отсутствие персональной ответственности сотрудников оператора и их руководителей за обеспечение ИБ, в том числе ПДн;
* недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе ПДн;
* отсутствие моральной и материальной стимуляции за соблюдение правил и требований ИБ;
* недостаточная техническая оснащённость подразделений, ответственных за обеспечение ИБ;
* совмещение функций по разработке и сопровождению или сопровождению и контролю за ИСПДн;
* наличие привилегированных бесконтрольных пользователей в ИСПДн;
* пренебрежение правилами и требованиями ИБ сотрудниками Оператора;
* другие причины.
	1. По усмотрению руководителя Оператора инцидент ИБ, не приведший к негативным последствиям и совершенный впервые, фиксируется администратором информационной безопасности ИСПДн в «Журнале учета выявленных инцидентов информационной безопасности» (таблица 5 приложения 8) с присвоением статуса «Разбирательство не требуется».
	2. В случае нарушения прав субъекта персональных данных разбирательство инцидента и реагирование на него происходит в порядке и сроки, предусмотренном в документе Оператора «Правила рассмотрения запросов субъектов персональных данных».
	3. В случае наличия признаков инцидента ИБ в полученной информации, администратор информационной безопасности ИСПДн определяет предварительную степень важности инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует руководителя Оператора об инциденте ИБ, производит запись в «Журнале учета выявленных инцидентов информационной безопасности» (таблица 5 приложения 8) с присвоением ему статуса «В процессе разбирательства».
	4. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте ИБ, администратор информационной безопасности ИСПДн, по согласованию с ответственным за организацию обработки ПДн, определяет и инициирует первоочередные меры, направленные на локализацию инцидента ИБ и на минимизацию его последствий.
1. Разбирательство инцидента информационной безопасности
	1. Цели и этапы разбирательства инцидента ИБ:
		1. Целями разбирательства инцидента ИБ являются:
* выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
* защита репутации Оператора и его ресурсов;
* обеспечение безопасности ПДн;
* обеспечение прав субъектов ПДн на обеспечение безопасности и конфиденциальности их ПДн, обрабатываемых Оператором;
* предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации.
	+ 1. Разбирательство инцидента ИБ, состоит из следующих этапов:
* подтверждение/опровержение факта возникновения инцидента ИБ;
* подтверждение/корректировка уровня значимости инцидента ИБ;
* уточнение дополнительных обстоятельств (деталей) инцидента ИБ;
* получение (сбор) доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;
* минимизация последствий инцидента ИБ;
* информирование и консультирование сотрудников Оператора по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
* разработка мероприятий по обнаружению и/или предупреждению инцидентов ИБ.

4.2. Порядок проведения разбирательства инцидента ИБ:

4.2.1. В процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

* дата и время совершения инцидента ИБ;
* Ф.И.О, должность и подразделение Нарушителя ИБ (для внутреннего инцидента);
* уровень критичности инцидента ИБ;
* обстоятельства и мотивы совершения инцидента ИБ;
* информационные ресурсы, затронутые инцидентом ИБ;
* характер и размер реального и потенциального ущерба;
* обстоятельства, способствовавшие совершению инцидента ИБ.

4.2.2. Администратор информационной безопасности в процессе проведения расследования инцидента ИБ, при необходимости, запрашивает информацию у специалистов Оператора.

4.2.3. После получения необходимой информации по инциденту ИБ администратор информационной безопасности ИСПДн проводит анализ полученных данных.

4.2.4. В течение 5 (пяти) рабочих дней администратор информационной безопасности ИСПДн запрашивает у начальника отдела объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение 2 (двух) рабочих дней и представлена его непосредственным руководителем администратору информационной безопасности ИСПДн в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную записку администратору информационной безопасности ИСПДн, составляется акт в соответствии с установленным у Оператора порядке.

4.2.5. Администратор информационной безопасности ИСПДн проводит оценку негативных последствий от реализации инцидента ИБ. В ходе данной оценки учитываются:

* прямой финансовый ущерб;
* репутационный ущерб;
* потенциальный ущерб;
* косвенные потери, связанные с недоступностью сервисов, потерей информации;
* другие виды ущерба или аспекты негативных последствий для Оператора или субъектов ПДн.

4.2.6. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа Нарушителя ИБ к информационным ресурсам (далее - ИР) на время проведения расследования, предварительно сделав заявку. Подобное отключение инициируется администратором информационной безопасности ИСПДн с обязательным предварительным устным согласованием с руководителем Нарушителя ИБ.

4.2.7. В случае, если у Нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам администратор информационной безопасности ИСПДн по согласованию с руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имевшихся у Нарушителя ИБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным порядком Оператора. Если нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с ИР высокого уровня безопасности, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа ответственным за организацию обработки персональных данных, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами Оператора.

4.2.8. Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только по заявке руководителя Нарушителя ИБ.

5. Оформление результатов проведенного разбирательства

* 1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором информационной безопасности ИСПДн в «Журнале учета выявленных инцидентов информационной безопасности» и учитывается при подготовке итогового заключения по инциденту ИБ (таблица 5 приложения 8).

5.2. Администратор информационной безопасности ИСПДн формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.

5.3. Итоговое заключение по инциденту ИБ администратор информационной безопасности ИСПДн направляет директору, начальникам отделов, затронутых инцидентом ИБ, и ответственному за организацию обработки ПДн.

5.4. Администратор информационной безопасности ИСПДн фиксирует завершение разбирательства в «Журнале учета выявленных инцидентов информационной безопасности» (таблица 5 приложения 8) и присваивает инциденту статус «Разбирательство завершено».

1. Завершение разбирательства инцидента

информационной безопасности

* 1. По завершению разбирательства инцидента ИБ, администратор информационной безопасности ИСПДн передает имеющиеся материалы в объеме, достаточном для принятия решения, ответственному за организацию обработки ПДн для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.
	2. На основании полученных результатов разбирательства ответственный за организацию обработки персональных данных в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в будущем:
* повторное ознакомление Нарушителя ИБ с правилами по обеспечению безопасности ПДн;
* просмотр и анализ имеющихся прав доступа к ИР у Нарушителя ИБ;
* доведение до всех сотрудников Оператора внутренних нормативных документов;
* обсуждение инцидента ИБ на совещании руководителей;
* отмена неактуальных прав доступа к ИР;
* проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
* и другие обоснованные мероприятия.
	1. О результатах проведенного разбирательства инцидента ИБ ответственный за организацию обработки ПДн по необходимости инициирует подготовку сообщения об инциденте ИБ в адрес руководителя Оператора.
1. Обязанности и права участников разбирательства инцидента информационной безопасности
	1. Администратор информационной безопасности ИСПДн обязан:
* объективно и основательно проводить разбирательство каждого инцидента ИБ;
* определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;
* фиксировать в «Журнале учета выявленных инцидентов информационной безопасности» (таблица 5 приложения 8) всю исходную информацию об инциденте ИБ и результаты его расследования;
* предоставлять отчеты и рекомендации по проведенным разбирательствам ответственному за организацию обработки ПДн и руководителю Оператора;
* проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе, совместно с ответственным за организацию обработки ПДн, разрабатывать рекомендации и предложения по снижению ущерба от подобных инцидентов ИБ и минимизации возможности их повторения в будущем.
	1. Администратор информационной безопасности ИСПДн имеет право:
* по согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам инцидента ИБ у Нарушителя ИБ;
* запрашивать и получать от руководителей и сотрудников Оператора, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента ИБ;
* инициировать отключение от ИР сотрудников Оператора, нарушивших правила или требования ИБ, на период проведений расследования инцидента ИБ, в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты ИБ;
* по результатам расследования инцидента ИБ инициировать изменения ИР Оператора с целью повышения их защищенности и снижения рисков инцидентов ИБ;
* инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной или материальной ответственности, согласно внутренним нормативным документам Оператора.

7.3. Начальники отделов и сотрудники Оператора обязаны:

* предоставлять по запросам администратора информационной безопасности ИСПДн устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента ИБ;
* информировать администратора информационной безопасности ИСПДн о выявленных инцидентах ИБ.

[Приложение](#Пр1) № 21
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

П Р А В И Л А

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

* + 1. Настоящие Правила рассмотрения запросов определяют основания, порядок рассмотрения запросов субъектов персональных данных или их представителей операторам.
		2. Лица, замещающие должности муниципальной службы, и иные работники операторов, граждане, претендующие на замещение вакантных должностей операторов, а также граждане, персональные данные которых обрабатываются операторами, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:
1. Подтверждение факта обработки персональных данных операторами.
2. Правовые основания и цели обработки персональных данных.
3. Применяемые операторами способы обработки персональных данных.
4. Наименование и место нахождения операторов, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с операторами или на основании федерального закона.
5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.
6. Сроки обработки персональных данных, в том числе сроки их хранения операторами.
7. Порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных.
8. Информацию об осуществленной или предполагаемой трансграничной передаче данных.
9. Наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению операторов, если обработка поручена или будет поручена такой организации или лицу.
10. Иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.
	* 1. Лица, указанные в [пункте](#Par306) 2 настоящих Правил рассмотрения запросов (далее – субъекты персональных данных), вправе требовать от операторов уточнения их 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 [подпунктах 2.1](#Par307)-[2.10 пункта](#Par316) 2 настоящих Правил рассмотрения запросов, должны быть предоставлены субъекту персональных данных операторами 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 [подпунктах 2.1](#Par307)-[2.10 пункта 2](#Par316) настоящих Правил рассмотрения запросов, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом операторов, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:
	1. Номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе.
	2. Сведения, подтверждающие участие субъекта персональных данных в правоотношениях с операторами (документ, подтверждающий прием документов на участие в конкурсе на замещение вакантных должностей операторов, осуществление операторами муниципальной функции), либо сведения, иным образом подтверждающие факт обработки персональных данных операторами.
	3. 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.

* + 1. В случае, если сведения, указанные в [подпунктах 2.1](#Par307)-[2.10 пункта](#Par316) 2 настоящих Правил рассмотрения запросов, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к операторам или направить повторный запрос в целях получения указанных сведений 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.
		2. Субъект персональных данных вправе обратиться повторно к операторам или направить повторный запрос в целях получения сведений, указанных в [подпунктах 2.1](#Par307)-[2.10 пункта](#Par316) 2 настоящих Правил рассмотрения запросов, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в [пункте](#Par322) 6 настоящих Правил рассмотрения запросов, 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](#Par319) 5 настоящих Правил рассмотрения запросов, должен содержать обоснование направления повторного запроса.
		3. Операторы (уполномоченное должностное лицо операторов) вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным [пунктами](#Par322) 6 и [7](#Par323) настоящих Правил рассмотрения запросов. Такой отказ должен быть мотивированным.
		4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

[Приложение](#Пр1) № 22
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

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

1. Общие положения

1.1. Лицами, участвующими в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных (далее - ИСПДн) являются сотрудники МУ «Администрация сельского поселения Усть-Юган» и подведомственного ей учреждения в соответствии с утвержденным Перечнем должностей в МУ «Администрация сельского поселения Усть-Юган» и подведомственного ей учреждения, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей (далее - Пользователи).

1.2. Пользователи должны принимать все необходимые меры по защите персональных данных (далее - ПДн) и контролю за соблюдением прав доступа к ней.

1.3. Пользователи ИСПДн в своих должностных (трудовых) обязанностях обязаны руководствоваться настоящей Инструкцией и должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушение.

1.4. Основными задачами при обработке ПДн в ИСПДн являются:

− обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту ПДн в Российской Федерации в процессе создания, хранения, передачи и удаления документов, содержащих ПДн в ИСПДн Оператора;

− обеспечение в ИСПДн необходимого уровня безопасности обработки, хранения и передачи ПДн;

− обеспечение необходимого уровня безопасности носителей ПДн;

− обеспечение безопасности ПДн при ее копировании, размножении.

2. Обязанности лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

2.1. При первичном допуске к работе в ИСПДн пользователь изучает требования настоящего документа, разрешительную систему доступа к ИСПДн, технологический процесс обработки информации в ИСПДн, руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности ПДн.

2.2. Каждый пользователь ИСПДн, имеющий доступ к автоматизированному рабочему месту (далее - АРМ), программному обеспечению (далее - ПО) и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

− строго соблюдать установленные правила обеспечения безопасности ПДн при работе с программными и техническими средствами ИСПДн, в том числе положения настоящего документа;

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

− при работе в ИСПДн выполнять только те обязанности, которые прописаны в должностной инструкции;

− не разглашать известные им ПДн лицам, не имеющим допуска к этим ПДн;

− располагать во время работы экран монитора в помещении так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами, и основные технические средства и системы (далее – ОТСС) в соответствии с Техническим паспортом на ИСПДн;

− помнить свой идентификатор и пароль;

− держать свой пароль в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников Оператора, в т.ч. руководителей) личный пароль;

− осуществлять ввод пароля только в условиях, исключающих его просмотр;

− не хранить записки-памятки с личным паролем на видном и/или в легко доступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.;

− своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн (далее - администратор информационной безопасности ИСПДн) о фактах компрометации пароля (когда пароль стал или может быть известен ещё кому - либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИСПДн до специального разрешения администратора информационной безопасности ИСПДн;

− немедленно известить администратора информационной безопасности ИСПДн в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

o несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

o 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;

o некорректного функционирования установленных на АРМ технических средств защиты;

o непредусмотренных отводов кабелей и подключенных устройств.

− при работе в ИСПДн использовать только учтенные съемные машинные носители ПДн, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности ИСПДн. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

− при работе со съемными машинными носителями ПДн 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 в ИСПДн;

− выполнять требования Инструкции по организации антивирусной защиты в ИСПДн в полном объеме;

− осуществлять установленным порядком уничтожение ПДн с машинных носителей ПДн;

− немедленно выполнять предписания администратора информационной безопасности ИСПДн в части обеспечения безопасности ПДн;

− соблюдать установленный режим разграничения доступа к информационным ресурсам;

− все изменения конфигурации технических и программных средств ИСПДн, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИСПДн, производить только по согласованию с администратором информационной безопасности ИСПДн;

− обеспечить сохранность оборудования и физической целостности системных блоков компьютеров;

− при отсутствии необходимости работы компьютера выключить (блокировать нажатием клавиш Windows+L) его.

3. Права лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

3.1. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для обработки, хранения и транспортировки ПДн разрешается использовать в ИСПДн только те машинные носители ПДн, которые учтены в «Журнале учета машинных носителей персональных данных» (таблица 1 приложения № 8).

3.2. Пользователь ИСПДн имеет право участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи ПДн и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными.

3.3. Своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей.

3.4. Требовать от администратора информационной безопасности ИСПДн смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Лицам, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей, запрещается

4.1. Пользователю ИСПДн категорически запрещается:

− самостоятельно устанавливать, тиражировать или модифицировать ПО, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные администратором информационной безопасности ИСПДн сетевые программы на компьютерах, вскрывать компьютер, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование;

− запускать любые системные или прикладные программы, не входящие в состав ПО;

− 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 ПО АРМ;

− записывать и хранить ПДн на неучтенных машинных носителях ПДн (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 свой электронный идентификатор, машинные носители ПДн и распечатки, содержащие ПДн;

− умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты ПДн;

− размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей ПДн;

− осуществлять попытки НСД к ресурсам ИСПДн, проводить или участвовать в сетевых атаках и сетевом взломе;

− производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

− привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности ИСПДн;

− отключать (блокировать) средства защиты информации;

− сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИСПДн;

− хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

− выполнять работы с документами, содержащими ПДн, на дому, выносить их за пределы контролируемой зоны;

− вводить в ОТСС ПДн под диктовку или с микрофона;

− закрывать доступ к информации паролями без согласования с администратором информационной безопасности ИСПДн;

− передавать свои учетные носители кому-либо;

− запускать файлы-вложения, которые содержатся в спам-письмах.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам НСД относятся:

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

− действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора информационной безопасности ИСПДн или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа (далее - НСД) лицо, выявившее факт НСД (пользователь, ответственный за организацию обработки ПДн, ответственный за эксплуатацию ИСПДн, администратор информационной безопасности ИСПДн) обязан:

− законными способами прекратить НСД к ПДн;

− известить администратора информационной безопасности ИСПДн о факте НСД;

− известить руководителя пользователя, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

− известить руководителя Оператора.

6. Порядок учета, хранения и выдачи машинных носителей

персональных данных

6.1. Порядок хранения и учета машинных носителей ПДн:

− машинные носители, содержащие ПДн, подлежат обязательному учёту администратором информационной безопасности ИСПДн. Учёт осуществляется с помощью «Журнала учёта машинных носителей ПДн» (таблица 1 приложения 8);

− учёт машинных носителей ПДн включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей, номер инвентарного учета и иные номера;

− носители должны храниться в сейфе, расположенном в помещении Оператора, и изыматься только для выполнения должностных обязанностей;

− при поступлении нового машинного носителя, который будет использоваться для хранения или передачи ПДн, администратор информационной безопасности ИСПДн регистрирует его в «Журнале учёта машинных носителей ПДн».

6.2. Порядок регистрации выдачи машинных носителей ПДн:

− учет выдачи машинных носителей ПДн ведётся в «Журнале учёта машинных носителей ПДн», в котором указывается регистрационный (учетный) номер машинного носителя ПДн, дата, время, фамилия, имя и отчество должностного лица, получившего машинный носитель ПДн, его роспись;

− в случае возврата должностным лицом машинного носителя ПДн в «Журнале учёта машинных носителей ПДн» администратором информационной безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

7. Ответственность лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

7.1. Персональную ответственность за соблюдение установленных требований настоящего положения несут пользователи ИСПДн и администратор информационной безопасности ИСПДн.

7.2. За разглашение ПДн и нарушение порядка обращения с машинными носителями ПДн администратор информационной безопасности ИСПДн, а также пользователи ИСПДн, работающие с этими машинными носителями ПДн, могут быть привлечены к дисциплинарной и иной, предусмотренной законодательством Российской Федерации, ответственности.

7.3. Пользователи несут персональную ответственность за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

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

7.5. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование ПДн, нарушение работы компьютеров пользователей ИСПДн или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

[Приложение](#Пр1) № 23
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки

персональных данных требованиям к защите персональных данных

1. Общие положения
	1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в МУ «Администрация сельского поселения Усть-Юган» и подведомственном ей учреждении требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Правила), разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации.
2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных к требованиям защиты персональных данных
	1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в МУ «Администрация сельского поселения Усть-Юган» и подведомственном ей учреждении организовывается проведение ежегодных проверок.
	2. Проверки проводятся ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных и ответственным за эксплуатацию информационной системы персональных данных.
	3. Плановые проверки условий обработки персональных данных проводятся на основании утвержденного руководителем Оператора ежегодного плана внутренних проверок режима защиты персональных данных (плановые проверки).
	4. Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки персональных данных, по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных. Проведение внеплановой проверки организуется в течение 10 (десяти) рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.
	5. В проведении проверки условий обработки персональных данных не могут участвовать сотрудники Оператора, прямо или косвенно заинтересованных в ее результате.
	6. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников Оператора, участвующих в процессе обработки 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;
* 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 соблюдения парольной защиты;
* порядок и условия соблюдения антивирусной защиты;
* порядок и условия обеспечения резервного копирования;
* эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в ИСПДн;
* условия соблюдения режима защиты при подключении к информационно-телекоммуникационным сетям;
* порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн;
* порядок и условия применения средств защиты информации;
* соблюдение учета носителей персональных данных;
* соблюдение правил доступа к персональным данным;
* соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
* мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
	1. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в ИСПДн, а также ответственный за эксплуатацию ИСПДн в ходе проверки имеют право:
* запрашивать у сотрудников информацию, необходимую для реализации своих полномочий;
* требовать от уполномоченных на обработку персональных данных сотрудников 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. Проверка условий обработки персональных данных должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.
	2. По результатам проведенной проверки условий обработки персональных данных ответственный за организацию обработки персональных данных предоставляет руководителю <Оператора письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.

[Приложение](#Пр1) № 24
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ПРАВИЛА

работы с обезличенными данными в случае обезличивания персональных данных

1. Общие положения
	1. Настоящие правила работы с обезличенными данными в случае обезличивания персональных данных (далее - Правила) Оператором разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными Оператором.
2. Термины и определения
	1. 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
	1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем Оператора и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
	2. 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 персональных данных;
* другие способы.
	1. 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 данными в случае обезличивания персональных данных
	1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.
	2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.
	3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

 парольной политики;

антивирусной политики;

правил работы со съемными машинными носителями;

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем персональных данных.

* 1. 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](#Пр1) № 25
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

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

1. Общие положения
	1. Настоящий документ устанавливает порядок уничтожения персональных данных 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».
2. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований
	1. 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.
	2. Вопрос об уничтожении документов, содержащих персональные данные, рассматривается на заседании Комиссии по защите информации.
	3. Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных данных. Результаты уничтожения документов оформляются актом (акт составляется в свободной форме).
	4. Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста, или сжигаются.
	5. После уничтожения материальных носителей ответственный за организацию обработки персональных данных подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №\_\_(дата)».
	6. Уничтожение информации на носителях необходимо осуществлять путем стирания информации с помощью системы защиты информации от несанкционированного доступа с гарантированной очисткой информации, установленной на АРМ.
	7. 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](#Пр1) № 26
к постановлению администрации

 сельского поселения Усть-Юган

 от 23.11.2018 № 239-па

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных

1. Общие положения
	1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
	2. Пользователем является каждый работник операторов, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
	3. Настоящая инструкция содержит общие сведения о работе пользователя на защищенной от несанкционированного доступа автоматизированной системе (АС) при обработке персональных данных и является дополнением к его должностным обязанностям.
	4. Пользователь несет персональную ответственность за свои действия.
	5. Пользователь в своей работе руководствуется настоящей инструкцией, и другими регламентирующими документами администрации сельского поселения Усть-Юган.
	6. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных».
	7. В случае получения согласия на обработку персональных данных
	от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются работниками операторов.
	8. Пользователям запрещается осуществлять обработку персональных данных, не указанных в перечне обрабатываемых персональных данных (приложение № 12).
	9. При наличии технической возможности, пользователь должен удалять или обезличивать обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное
	не предусмотрено федеральным законом.
	10. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Пользователи должны принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
	11. В случае выявления неправомерной обработки персональных данных пользователь обязан осуществить блокирование неправомерно обрабатываемых персональных данных или обеспечить их блокирование.
	12. Методическое руководство работой пользователя в вопросах защиты ПДн осуществляется администратором безопасности информации.
2. Обязанности Пользователя
	1. Перед работой на защищаемом АРМ Пользователь должен пройти соответствующую подготовку (инструктаж), и ознакомиться под роспись с перечнем обрабатываемых персональных данных и внутренними документами, устанавливающими порядок обработки ПДн, а также своими правами и обязанностями в этой области.
	2. Пользователь обязан 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.
	3. При сборе персональных данных пользователь обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных, в том числе содержащей:
		1. Подтверждение факта обработки персональных данных операторами.
		2. Правовые основания и цели обработки персональных данных.
		3. Цели и применяемые операторами способы обработки персональных данных.
		4. Место нахождения операторов, сведения о лицах (за исключением работников операторов), которые имеют доступ к персональным данным
		или которым могут быть раскрыты на основании договора с операторами или
		на основании федерального закона.
		5. Обрабатываемые персональные данные, относящиеся
		к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления 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 фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению операторов, если обработка поручена или будет поручена такому лицу.
		10. Иные сведения, предусмотренные федеральными законами.
	4. В случае отказа субъекта ПДн от предоставления персональных данных, являющихся обязательными в соответствии с федеральным законом, пользователь обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
	5. При получении персональных данных не от субъекта персональных данных, пользователь, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
		1. Наименование, либо фамилию, имя, отчество и адрес операторов или его представителя.
		2. Цель обработки персональных данных и ее правовое основание.
		3. Предполагаемые пользователи персональных данных.
		4. Установленные Федеральным законом «О персональных данных» права субъекта персональных данных.
		5. Источник получения персональных данных.
	6. Пользователь освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п.2.5 настоящей Инструкции, случаях, если:
		1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим операторами.
		2. Персональные данные получены операторами 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. Операторы осуществляют обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных.
		5. Предоставление субъекту персональных данных сведений, предусмотренных п.2.5 настоящей Инструкции, нарушает права и законные интересы третьих лиц.
	7. Пользователь обязан соблюдать условия использования средств защиты информации, предусмотренных эксплуатационной и технической документации.
	8. Пользователь обязан соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
	9. Пользователь должен осуществлять свою деятельность в соответствии с правилами разграничения доступа операторов.
	10. Соблюдать требования парольной политики (раздел 4 настоящей Инструкции).
	11. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 7 настоящей Инструкции).
	12. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, в зависимости от этажности или наличия близлежащих зданий равной этажности и (или) выхода оконных проемов на неконтролируемую территорию, шторы должны быть завешаны (жалюзи закрыты).
	13. Перед началом работы, пользователь должен убедиться в актуальности антивирусных баз.
	14. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к администратору безопасности информации
	15. Для хранения информации, содержащей конфиденциальную информацию, должны использоваться только машинные носители информации (МНИ), поставленные на учет операторами. Ответственный за регистрацию МНИ – администратор безопасности информации.
	16. При отсутствии визуального контроля за рабочей станцией доступ
	к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Win><L>.
	17. В случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций пользователь должен принимать соответствующие меры по реагированию.
3. Пользователю запрещается
	1. Распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.
	2. Копировать защищаемую информацию на внешние носители
	без разрешения своего руководителя, если это непосредственно не предусмотрено должностными обязанностями.
	3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
	4. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
	5. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
	6. Отключать (блокировать) средства защиты информации.
	7. Обрабатывать на АРМ информацию и выполнять другие работы,
	не предусмотренные должностными обязанностями.
	8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
	9. Привлекать посторонних лиц для производства ремонта или настройки АРМ.
	10. В процессе работы на ПЭВМ озвучивать голосом обрабатываемую информацию.
4. Организация парольной защиты
	* 1. Личные пароли доступа к элементам ИСПДн выдаются пользователям администратором безопасности информации или создаются самостоятельно.
		2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
		3. Лица, использующих паролирование, обязаны:
5. четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
6. своевременно сообщать администратору безопасности информации
об утере, компрометации, несанкционированном изменении паролей
и несанкционированном изменении сроков действия паролей.
	* 1. Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть.
		2. Пароль должен состоять не менее чем из 6 символов.
		3. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

* + 1. Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123456», «111111», «qwerty» и им подобные, а также имена и даты рождения себя и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
		2. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
		3. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
		4. Запрещается выбирать пароли, которые уже использовались ранее.
		5. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
		6. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
		7. При вводе неверного имени или пароля предоставляется повторная попытка их введения. Количество попыток - 3 раза. В случае неверного ввода имени пользователя и (или) пароля за указанное число попыток ПЭВМ блокируется и выдается сообщение о необходимости вызова администратора безопасности информации.
		8. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
		9. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
1. Порядок работы с персональными идентификаторами (USB-ключами)
	1. Персональный идентификатор выдается администратором безопасности информации.
	2. Персональный идентификатор используется для входа
	в автоматизированную систему — при появлении экрана приветствия (приглашение на вход в систему) необходимо предъявить свой персональный идентификатор и ввести пароль. При вводе правильного пароля осуществится вход в систему.
	3. Пользователю запрещается:
		1. Передавать персональный идентификатор другим пользователям.
		2. Оставлять персональный идентификатор в компьютере в случае покидания рабочего места.
	4. Пользователь обязан сообщать администратору безопасности информации об утере и повреждении персонального идентификатора.
2. Порядок работы на АС
	1. Перед началом работы убедиться в целостности печати (пломбы)
	на системном блоке, отсутствии подключения посторонних устройств.
	2. Для входа в автоматизированную систему используется два способа:
		1. При помощи имени пользователя и пароля.
		2. При помощи персонального идентификатора и пароля.
	3. Копирование защищаемой информации должно осуществляться пользователем на МНИ, учтенных операторами.
	4. Перед работой с информацией на отчуждаемых МНИ пользователь обязан убедиться в отсутствии на них вирусов с использованием штатных антивирусных программ, установленных на АС, в соответствии с документом «Инструкция
	по антивирусной защите при работе в информационных системах персональных данных операторов.
	5. В случае обнаружения вирусов на МНИ пользователь обязан прекратить работу на АС и сообщить об этом администратору безопасности информации. Возобновление работы производить после получения разрешения от администратора безопасности информации.
3. Правила работы в сетях общего доступа и (или) международного обмена
	1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
	2. При работе в Сети запрещается:
		1. Осуществлять работу при отключенных средствах защиты (антивирус и других).
		2. Передавать по Сети защищаемую информацию без использования средств шифрования.
		3. Запрещается скачивать из Сети программное обеспечение и другие файлы.
		4. Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).
		5. Запрещается нецелевое использование подключения к Сети.
4. Реагирование на инциденты нарушения информационной

безопасности и сбои

* 1. Пользователь должен обращать внимание и сообщать о любых замечаниях или предполагаемых недостатках или угрозах в области безопасности. При наличии такой информации пользователь должен сообщать ее администратору безопасности информации. Пользователь ни при каких обстоятельствах не должен самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности, так как это может быть интерпретировано как неправомочное использование системы.
	2. Инцидентами нарушения информационной безопасности являются компрометация парольной информации (разглашение пароля, ввод пароля в присутствии посторонних лиц), получение предупредительных сообщений от средств защиты информации, странное поведение системы, подозрения в НСД, отсутствие (повреждение, недоступность информационных ресурсов), нарушение физической целостности технических средств или их печатей (пломб), утеря персонального идентификатора и т.п.
	3. При возникновении (подозрении) инцидентов нарушения информационной безопасности пользователь информационной системы должен:

зафиксировать симптомы инцидента (появляющиеся сообщения);

физически отключить АРМ, прекратить обработку ПДн;

не допускать использования МНИ на других АРМ;

незамедлительно информировать любыми доступными средствами своего непосредственного руководителя и администратора безопасности информации.

1. Ответственность

Пользователь ИСПДн несет ответственность за нарушение требований обработки конфиденциальной информации.