|  |  |  |
| --- | --- | --- |
| Администрация муниципального образования «Сюмсинский район»  |  | «Сюмси ёрос»муниципал кылдытэтлэн Администрациез |

# ПОСТАНОВЛЕНИЕ

#

# от 16 октября 2020 года № 387

с. Сюмси

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования «Сюмсинский район»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июня 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 21 марта 2012 № 211 «Об утверждении [перечн](#P32)я 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», руководствуясь Уставом муниципального образования «Сюмсинский район», **Администрация муниципального образования «Сюмсинский район» постановляет:**

1. Утвердить прилагаемые Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования «Сюмсинский район».
2. Ознакомить работников, осуществляющих обработку персональных данных, имеющих доступ к персональным данным, с настоящим постановлением.

3. Контроль за исполнением настоящего постановления возложить на руководителя Аппарата Главы муниципального образования «Сюмсинский район», Районного Совета депутатов и Администрации.

Первый заместитель главы

Администрации района Л.Е.Даровских

|  |
| --- |
| УТВЕРЖДЕНЫ постановлением Администрации муниципального образования «Сюмсинский район»  от 16 октября 2020 года № 387 |

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования «Сюмсинский район»**

**1. Общие положения**

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования «Сюмсинский район» (далее - Правила) относятся к основным организационно-распорядительным документам системы документов информационной безопасности Администрации и разработаны в соответствии с требованиями постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (ПДн) в Администрации муниципального образования «Сюмсинский район» с целью своевременного выявления и предотвращения:

хищения технических средств и носителей информации;

утраты информации;

преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;

несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;

утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя: контроль организации защиты информации;

 контроль эффективности защиты информации.

**2 . Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных**

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются муниципальным служащим Администрации муниципального образования «Сюмсинский район», ответственным за организацию обработки ПДн в Администрации муниципального образования «Сюмсинский район» либо комиссией, образуемой Главой муниципального образования, не реже одного раза в год в соответствии с утвержденным графиком.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

соблюдения принципов обработки ПДн;

соответствия локальных актов в области ПДн в Администрации муниципального образования «Сюмсинский район» действующему законодательству Российской Федерации;

выполнения служащими Администрации требований и правил обработки ПДн в информационных системах персональных данных (ИСПДн) Администрации муниципального образования «Сюмсинский район»;

перечней ПДн, используемых для решения задач и функций структурными подразделениями в Администрации муниципального образования «Сюмсинский район» и необходимости обработки ПДн в ИСПДн Администрации муниципального образования «Сюмсинский район»;

актуальности содержащихся в Правилах обработки ПДн в Администрации муниципального образования «Сюмсинский район» каждой ИСПДн Администрации муниципального образования «Сюмсинский район» информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн Администрации муниципального образования «Сюмсинский район»;

актуальности перечня должностей муниципальных служащих Администрации, замещающих должности муниципальной службы в Администрации муниципального образования «Сюмсинский район», уполномоченных на обработку ПДн, имеющих доступ к ПДн;

актуальности перечня должностей муниципальных служащих Администрации, замещающих должности муниципальной службы в Администрации муниципального образования «Сюмсинский район»,

ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн в Администрации муниципального образования «Сюмсинский район»;

соблюдения обязанностей Администрации муниципального образования «Сюмсинский район» как оператора ПДн, предусмотренных действующим законодательством в области ПДн;

порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн Администрации, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;

 наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн Администрации муниципального образования «Сюмсинский район»;

актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;

актуальности перечня ИСПДн в Администрации муниципального образования «Сюмсинский район»;

знания и соблюдения служащими Администрации муниципального образования «Сюмсинский район» положений локальных актов Администрации муниципального образования «Сюмсинский район» в области обработки и обеспечения безопасности ПДн;

знания и соблюдения служащими Администрации муниципального образования «Сюмсинский район» инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдения служащими в Администрации муниципального образования «Сюмсинский район» конфиденциальности ПДн;

актуальности локальных актов Администрации муниципального образования «Сюмсинский район» в области обеспечения безопасности ПДн, в том числе в Технических паспортах ИСПДн;

соблюдения служащими в Администрации муниципального образования «Сюмсинский район» требований по обеспечению безопасности ПДн;

наличия локальных актов в Администрации муниципального образования «Сюмсинский район», технической и эксплуатационной документации технических и программных средств ИСПДн Администрации муниципального образования «Сюмсинский район»;

по иным вопросам.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает Главе муниципального образования.

При проведении внутреннего контроля на ИСПДн (отдельное автоматизированное рабочее место) Администрации муниципального образования «Сюмсинский район» составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте по форме, приведенной в приложении к настоящим Правилам.

**3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных**

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в Администрации муниципального образования «Сюмсинский район» производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в Администрации муниципального образования «Сюмсинский район».

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн в Администрации муниципального образования «Сюмсинский район» производится экспертное сравнение заявленной Администрацией в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых в Администрации мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн в Администрации муниципального образования «Сюмсинский район».

По итогам сравнений принимается решение о достаточности применяемых в Администрации муниципального образования «Сюмсинский район» мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и возможности или необходимости принятия дополнительных мер или изменения установленного в Администрации муниципального образования «Сюмсинский район» порядка обработки и обеспечения безопасности ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и

обеспечению безопасности ПДн, в Администрации муниципального образования «Сюмсинский район» оформляется в виде отдельного документа, подписывается председателем комиссии и утверждается Главой муниципального образования.

По результатам принятых решений муниципальным служащим, в Администрации муниципального образования «Сюмсинский район» ответственным за организацию обработки ПДн в Администрации, организуется работа по их реализации.

ПРИЛОЖЕНИЕ

к Правилам осуществления внутреннего контроля соответствия

обработки персональных данных требованиям к защите

персональных данных в Администрации муниципального образования «Сюмсинский район»

**Форма**

Протокол №

контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте

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

(наименование структурного подразделения администрации сельсовета)

1. Объект контроля

Указать:

наименование автоматизированного рабочего места (АРМ);

заводской (инвентарный) номер системного блока ПЭВМ АРМ;

принадлежность к подразделению;

адрес размещения АРМ.

2. Назначение объекта

Указать:

тип информации, обрабатываемой (хранимой) на АРМ;

уровень защищенности персональных данных при их обработке в информационной системе.

3. Контролируемые вопросы

Состояние организации технической защиты информации при обработке (хранении) информации ограниченного доступа.

Контроль наличия руководящих документов, инструкций, документации, регламентирующей обработку (хранение) информации ограниченного доступа:

перечня защищаемых ресурсов и уровня их конфиденциальности;

перечня лиц, обслуживающих АРМ;

перечня лиц, имеющих право самостоятельного доступа в помещение с АРМ;

перечня лиц, имеющих право самостоятельного доступа к штатным средствам АРМ и уровень их полномочий;

распоряжения о назначения комиссии для определения уровня защищенности персональных данных;

распоряжения о назначении администратора информационной безопасности;

данных по уровню подготовки персонала;

инструкции по обеспечению защиты информации, обрабатываемой на АРМ; перечня программного обеспечения;

описания технологического процесса обработки информации;

схемы информационных потоков;

технического паспорта;

матрицы доступа субъектов к защищаемым информационным ресурсам; акта установки системы активного зашумления (при наличии);

 акта установки системы защиты информации от несанкционированного доступа (СЗИ НСД) (при наличии);

описания системы разграничения доступа и настроек СЗИ НСД;

инструкции администратору безопасности;

инструкции пользователю;

инструкции по антивирусному контролю;

распоряжения о допуске служащих;

распоряжения о вводе в эксплуатацию.

Контроль соответствия настройки подсистемы управления доступом, подсистемы регистрации и учета, подсистемы обеспечения целостности требованиям присвоенного класса защищенности от НСД.

В соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением Председателя Гостехкомиссии от 30 марта 1992 года, в настройках подсистемы управления доступом проверяется:

наличие требований к длине и сложности пароля;

ограничение максимального срока действия пароля;

настройки блокировки учетных записей при попытках несанкционированного доступа;

наличие административных прав у пользователей;

выполнение требований мандатного разграничения прав доступа к каталогам, программам, файлам.

В настройках подсистемы регистрации и учета контролируется:

отсутствие критических ошибок и несанкционированных запусков процессов, зарегистрированных в журнале приложений;

отсутствие зарегистрированных критических системных ошибок в системном журнале;

отсутствие зарегистрированных изменений действующих политик безопасности, прав доступа, настроек системы защиты информации в журнале системы защиты информации;

возможности несанкционированного доступа к информации, аудиты отказа, зарегистрированные в журнале безопасности.

В настройках подсистемы обеспечения целостности контролируется:

соответствие программного обеспечения, установленного на АРМ, аттестационным материалам;

отсутствие программных средств разработки и отладки приложений;

наличие средств антивирусного контроля, включая срок действия лицензии и периодичность обновления антивирусных баз.

Контроль наличия лицензионного программного обеспечения, установленного в процессе проведенной аттестации по требованиям безопасности информации.

Контроль срока действия лицензии, порядка и периодичности обновления баз антивирусной программы.

Контроль наличия сетевых плат (в том числе интегрированных) и физической возможности их использования.

Контроль возможности и фактов подключения незарегистрированных магнитных и иных носителей информации.

4. Метод проведения контроля:

Экспертно-документальный

5. Средства контроля:

Программные возможности операционной системы, установленной на контролируемом АРМ.

6. Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации

Контроль проводится в соответствии с требованиями:

- Указа Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- специальных требований и рекомендаций по технической защите конфиденциальной информации (приказ Гостехкомиссии России от 30 августа 2002 года № 282);

- руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (решение Председателя Гостехкомиссии от 30 марта 1992 года);

- руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (приказ Председателя Гостехкомиссии России от 4 июня 1999 года № 114);

- нормативных и руководящих документов ФСТЭК России по защите информации.

Контроль выполнили:

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

 должность подпись фамилия, инициалы

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

 должность подпись фамилия, инициалы

При проведении контроля присутствовали:

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

 должность подпись фамилия, инициалы

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

 должность подпись фамилия, инициалы

Дата проведения контроля: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .

(число, месяц, год)

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