Приложение № 3
к Постановлению администрации муниципального района «Тоджинский кожуун Республики Тыва»
от «25» августа 2021 г. № 248

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» в администрации муниципального района «Тоджинский кожуун Республики Тыва»

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального района «Тоджинский кожуун Республики Тыва» (далее – Правила) разработаны в соответствии с требованиями постановления 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».

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных 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 ПД 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 ПД

В целях осуществления внутреннего контроля соответствия обработки ПД установленным требованиям организуется проведение периодических проверок условий обработки ПД. Проверки осуществляются не реже одного раза в год в соответствии с утвержденным графиком.

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

- соблюдения принципов обработки ПД;
- соответствия правовых актов администрации муниципального района «Тоджинский кожуун Республики Тыва» в области ПД действующему законодательству Российской Федерации;
- выполнения муниципальными служащими (работниками) администрации муниципального района «Тоджинский кожуун Республики Тыва» требований и правил обработки ПД в информационных системах персональных данных (далее – ИСПД);
- актуальности информации о законности целей обработки ПД и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПД;
- правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПД в каждой ИСПД;
- актуальности перечня должностей должностных лиц, уполномоченных на обработку ПД, имеющих доступ к ПД;
- соблюдения прав субъектов персональных данных, чьи ПД обрабатываются в ИСПД;
- соблюдения обязанностей оператора ПД, предусмотренных действующим законодательством в области ПД;
- порядка взаимодействия с субъектами персональных данных, ПД которых обрабатываются в ИСПД, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПД, 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 ПД и отзыве согласий субъектами персональных данных;
- наличия необходимых согласий субъектов персональных данных, чьи ПД обрабатываются в ИСПД;
- актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;
- актуальности перечня ИСПД;
- знания и соблюдения муниципальными служащими (работниками) администрации муниципального района «Тоджинский кожуун Республики Тыва» положений действующего законодательства Российской Федерации в области ПД, правовых актов муниципального района «Тоджинский кожуун Республики Тыва»;
- соблюдения муниципальными служащими (работниками) администрации муниципального района «Тоджинский кожуун Республики Тыва» конфиденциальности ПД;
- соблюдения муниципальными служащими (работниками) требований по обеспечению безопасности ПД;

– наличия и актуальности локальных актов, технической и эксплуатационной документации технических и программных средств ИСПД.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает председателю администрации муниципального района «Тоджинский кожуун Республики Тыва» (заместителю председателя администрации муниципального района «Тоджинский кожуун Республики Тыва»).

При проведении внутреннего контроля на ИСПД 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 ПД

Во время осуществления внутреннего контроля соответствия обработки ПД установленным требованиям производится соответствие оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПД и принимаемых мер по обработке и обеспечению безопасности ПД в администрации муниципального района «Тоджинский кожуун Республики Тыва».

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПД, для каждой ИСПД производится экспертное сравнение заявленной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПД и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПД и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПД.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПД и принимаемых мер по обработке и обеспечению безопасности ПД, оформляется в виде отдельного документа, подписывается начальником Управления делами администрации муниципального района «Тоджинский кожуун Республики Тыва» и утверждается председателем администрации муниципального района «Тоджинский кожуун Республики Тыва».

Приложение
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных в администрации муниципального
района «Тоджинский кожуун Республики Тыва»

Протокол № ___
контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке в ИС администрации муниципального района «Тоджинский кожуун Республики Тыва»

1. Объект контроля:

наименование автоматизированного рабочего места (далее – АРМ);

заводской (инвентарный) номер системного блока персональной электронно-вычислительной машины АРМ;

адрес размещения АРМ.

2. Назначение объекта:

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;

– перечень защищаемых ресурсов и уровня их конфиденциальности;

– перечень лиц, обслуживающих АРМ;

– перечень лиц, имеющих право самостоятельного доступа в помещение с АРМ;

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

– распоряжение о назначении администратора информационной безопасности;

– данные по уровню подготовки персонала;

– инструкции по обеспечению защиты информации, обрабатываемой на АРМ;

– перечень программного обеспечения;

– описание технологического процесса обработки информации;

– схемы информационных потоков;

– технический паспорт;

– матрицы доступа субъектов к защищаемым информационным ресурсам;

– акт установки системы активного зашумления (при наличии);

– акт установки системы защиты информации от несанкционированного доступа (далее – СЗИ НСД) (при наличии);

– описание системы разграничения доступа и настроек СЗИ НСД;

– инструкции администратора безопасности;

– инструкции пользователя;

– инструкции по антивирусному контролю;

– распоряжения о допуске муниципальных служащих (сотрудников) администрации муниципального района «Тоджинский кожуун Республики Тыва»;

– распоряжение о вводе в эксплуатацию.

Контроль соответствия настройки СЗИ НСД требованиям присвоенного уровня защищенности ПД.

При контроле следует руководствоваться требованиями следующих документов:

–постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

–приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

–приказ ФСТЭК России 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».

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 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

–постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

–приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

–приказа ФСТЭК России 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».

Контроль выполнил:

должность	подпись	фамилия, инициалы

При проведении контроля присутствовали:

должность	подпись	фамилия, инициалы
должность	подпись	фамилия, инициалы

Дата проведения контроля: _____

(число, месяц, год)