МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИТЫВА

П Р И К А З
Кызыл

от 12.08.2024
№ 475/24

Об организации защиты информации, обрабатываемой в информационных системах Министерства труда и социальной политики Республики Тыва

В целях организации защиты информации, обрабатываемой в Министерстве труда и социальной политики Республики Тыва, а также с целью выполнения требований Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», приказа ФСТЭК России от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну содержащихся в государственных информационных системах», постановления Правительства РФ 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», постановления Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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 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», приказа ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн 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 защищённости», приказа ФАПСИ от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», **ПРИКАЗЫВАЮ:**

1. Утвердить следующие документы:

Политика обработки персональных данных в Министерстве труда и социальной политики Республики Тыва (приложение № 1);

- Типовая форма согласия субъекта на обработку персональных данных;
- Типовая форма согласия на обработку персональных данных разрешенных субъектом персональных данных для распространения;
- Типовая форма заявления субъекта об отзыве согласия;
- Требования субъекта персональных данных о прекращении передачи (распространении, предоставлении, доступа) персональных данных, разрешенных субъектом персональных данных для распространения;
- Типовая форма запроса субъекта персональных данных на доступ к его персональным данным;
- Типовая форма повторного запроса субъекта персональных данных на доступ к его персональным данным;
- Типовая форма запроса субъекта персональных данных об уточнении персональных данных;
- Типовая форма запроса субъекта персональных данных о блокировании персональных данных;
- Типовая форма запроса субъекта персональных данных об уничтожении персональных данных;

Положение об обработке персональных данных в информационных системах персональных данных Министерства труда и социальной политики Республики Тыва (приложение № 2):

- Типовое обязательство работника Министерства труда и социальной политики Республики Тыва, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;
- Типовое обязательство работника Министерства труда и социальной политики Республики Тыва о неразглашении персональных данных;

- Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- Уведомление о получении персональных данных у третьей стороны;
- Уведомление субъекта персональных данных о прекращении обработки персональных данных;
- Типовая форма ответа на запрос о предоставлении персональных данных;
- Типовая форма мотивированного отказа на повторный запрос о предоставлении персональных данных;
- Уведомление субъекта персональных данных о внесении изменений в персональные данные;
- Уведомление субъекта персональных данных о блокировании персональных данных;
- Уведомление субъекта персональных данных об уничтожении персональных данных;
- Журнал учета передачи персональных данных;
- Журнал учета обращений и запросов субъектов по вопросам обработки персональных данных;

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Министерства труда и социальной политики Республики Тыва (приложение № 3):

- Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- План внутренних проверок режима защиты персональных данных в Министерстве труда и социальной политики Республики Тыва;
- Журнал проведения внутренних проверок режима защиты персональных данных в Министерстве труда и социальной политики Республики Тыва;
- Журнал ознакомления сотрудников с положениями законодательства РФ о персональных данных, локальными актами Министерства труда и социальной политики Республики Тыва по вопросам обработки персональных данных;

Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при

достижении целей обработки или при наступлении иных законных оснований (приложение № 4);

Правила рассмотрения запросов субъектов персональных данных или их представителей в Министерстве труда и социальной политики Республики Тыва (приложение № 5);

Правила работы с обезличенными данными в Министерстве труда и социальной политики Республики Тыва (приложение № 6):

- Уведомление об устранении допущенных нарушений;
- Уведомление об уничтожении;
- Уведомление об устранении допущенных нарушений;
- Уведомление об уничтожении.

Перечень информационных систем в Министерстве труда и социальной политики Республики Тыва (приложение № 7);

Правила доступа к персональным данным в Министерстве труда и социальной политики Республики Тыва (приложение № 8);

- Перечень лиц, допущенных к обработке персональных данных в Министерстве труда и социальной политики Республики Тыва;

Порядок доступа сотрудников в помещения Министерства труда и социальной политики Республики Тыва, в которых ведется обработка персональных данных (приложение № 9);

- Перечень лиц, допущенных в помещения Министерства труда и социальной политики Республики Тыва, где ведется обработка персональных данных;

Правила обработки персональных данных, осуществляемой без использования средств автоматизации в Министерстве труда и социальной политики Республики Тыва (приложение № 10);

Инструкция по обращению с машинными носителями персональных данных в Министерстве труда и социальной политики Республики Тыва (приложение № 11):

- Акт на списание и уничтожение машинных (бумажных) носителей информации;
- Журнал учета машинных носителей персональных данных;

Список лиц, допущенных к содержанию электронного журнала сообщений (приложение № 12);

Инструкция пользователя информационных систем Министерства труда и социальной политики Республики Тыва (приложение № 13);

Инструкция по организации парольной защиты в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 14);

Инструкция по организации антивирусной защиты в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 15);

Инструкция по выявлению инцидентов и реагированию на них в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 16):

- Карточка данных об инциденте безопасности обработки персональных данных в информационных системах Министерства труда и социальной политики Республики Тыва;
- Журнал реагирования на инциденты информационной безопасности в Министерстве труда и социальной политики Республики Тыва;
- План практических занятий и тренировок с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты;

Правила управления конфигурацией информационной системы и системы защиты информации информационной системы (приложение № 17);

Правила контроля и мониторинга за обеспечением уровня защищенности информации, содержащейся в информационной системе (Приложение № 18);

Инструкция по защите информации при выводе из эксплуатации информационной системы или об окончании обработки информации (приложение № 19);

Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 20):

- Журнал резервирования информационных ресурсов Министерстве труда и социальной политики Республики Тыва;

Порядок контроля выполнения мероприятий по обеспечению защиты информации в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 21):

- План мероприятий по защите информации;
- Журнал проведения мероприятий по защите информации в Министерстве труда и социальной политики Республики Тыва;

Регламент по использованию в Министерстве труда и социальной политики Республики Тыва мобильных технических средств (приложение № 22);

Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Министерстве труда и социальной политики Республики Тыва (приложение № 23):

- Правила по работе в локальной сети;

- Правила работы с электронной почтой;
- Правила по работе в сети Интернет;

Порядок охраны и порядок допуска лиц в помещения, в которых расположены элементы информационных систем персональных данных и ведется обработка персональных данных в рабочее и нерабочее время, а также в нештатных ситуациях (приложение № 24):

Журнал инструктажа сотрудников с документами в области обеспечения информационной безопасности с использованием средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ) в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 25);

Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации в информационных системах Министерства труда и социальной политики Республики Тыва (приложение № 26).

2. Определить хранилищем для размещения, эксплуатации и хранения СКЗИ: металлический шкаф (инв.№ 347), расположенный на цокольном этаже по адресу: ул. Московская, д.2.

2.1. Разрешить доступ к данному хранилищу следующим сотрудникам:

– заместитель директора Государственного бюджетного учреждения «Центр административно-хозяйственного обеспечения Министерства труда и социальной политики Республики Тыва», Мажаа К.К.

– главный специалист отдела автоматизации и информационно-технического обеспечения Государственного бюджетного учреждения «Центр административно-хозяйственного обеспечения Министерства труда и социальной политики Республики Тыва» Сенги-Доржу С-Б.С.

3. Разрешить доступ в помещения, в которых обрабатываются персональные данные, сотрудникам в соответствии с «Перечнем лиц, допущенных в помещения Министерства труда и социальной политики Республики Тыва, где ведется обработка персональных данных».

3.1. Должностные лица, допущенные к обработке защищаемых данных, должны обеспечивать:

– конфиденциальность защищаемых данных в соответствии с требованиями действующего законодательства РФ;

– выполнение требований документов «Инструкция пользователя информационных систем Министерства труда и социальной политики Республики Тыва» и «Порядок доступа сотрудников в помещения Министерства труда и социальной политики Республики Тыва, в которых ведется обработка персональных данных» в полном объеме.

3.2. Доступ лиц, не указанных в Перечне лиц, допущенных в помещения Министерства труда и социальной политики Республики Тыва, где ведется обработка персональных данных, осуществлять только в присутствии сотрудников Министерстве труда и социальной политики Республики Тыва, указанных в Перечне лиц, допущенных в помещения Министерства труда и социальной политики Республики Тыва, где ведется обработка персональных данных.

3.3. В случае оставления помещений, в которых обрабатываются защищаемые данные, сотрудникам Министерства труда и социальной политики Республики Тыва необходимо запирать помещения.

4. Контроль за своевременным ведением журналов и актуализации инструкций возлагается на администратора информационной безопасности.

5. Признать утратившим силу приказ от 19 апреля 2024 г. №257/24.

6. Контроль исполнения настоящего приказа возложить на заместителя министра труда и социальной политики Республики Тыва Ондара С.Д.

Министр

Документ подписан электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 09B2EA6F5D9B6AEB2E7E24111DA1FB80
Владелец: Сандан Эдуард Феликсович
Действителен с 30-10-2023 до 22-01-2025

Сандан. Э.Ф.

Приложение № 1
к приказу № 475/24 от 12.08.2024 г.

ПОЛИТИКА

по обработке персональных данных в информационных системах Министерства труда и социальной политики Республики Тыва

г. Кызыл, 2024

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящий документ (далее – Политика) определяет реализуемые меры защиты персональных данных, а также общие принципы получения, хранения, обработки, передачи и любого другого использования персональных данных, обрабатываемых в информационных системах в Министерства труда и социальной политики Республики Тыва (далее – Оператор). Политика является общедоступным документом Оператора и предусматривает возможность ознакомления с ней любых лиц.

1.2. Политика действует бессрочно после утверждения и до ее замены новой версией.

1.3. Обработка персональных данных Оператора осуществляется с соблюдением принципов и условий, предусмотренных настоящей Политикой и законодательством Российской Федерации в области персональных данных.

1.4. Цель разработки Политики - определение порядка обработки персональных данных (далее – ПДн) работников оператора и иных субъектов ПДн, персональные данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника оператора, при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

2. Термины и определения

2.1. Основные понятия, используемые в Политике:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

– сбор;
– запись;
– систематизацию;
– накопление;
– хранение;
– уточнение (обновление, изменение);
– извлечение;
– использование;
– передачу (распространение, предоставление, доступ);
– обезличивание;
– блокирование;
– удаление;
– уничтожение.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Цели сбора и обработки персональных данных

3.1. Обработка персональных данных Оператором осуществляется для целей, связанных с выполнением следующих функций:

3.1.1. Учет кадрового состава.

В состав ПДн, обрабатывающихся Оператором для выполнения функций учёта кадрового состава, входят документы, содержащие:

– фамилия, имя, отчество;

– день, месяц, год и место рождения;

– адрес регистрации по месту жительства;

– адрес фактического проживания;

– паспортные данные (серия, номер паспорта, кем и когда выдан), в том числе загранпаспорт;

– страховой номер индивидуального лицевого счета (СНИЛС);

– идентификационный номер налогоплательщика;

– контактные данные;

– сведения об образовании, квалификации;

– сведения о заработной плате, в том числе реквизиты банковских карт;

– сведения о семейном положении;

– сведения о трудовой деятельности (номер, серия и дата выдачи трудовой книжки и записях в ней);

– сведения о воинском учете;

– информация о приеме на работу, перемещении по должности, увольнении;

– информация об отпусках;

– информация о командировках.

ПДн, представленные работником, обрабатываются автоматизированным и без использования средств автоматизации способами. Оператор не принимает, не снимает и не хранит копии личных документов работников. Документы, которые работник предъявляет работодателю для хранения в оригинале, хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора.

После истечения срока нормативного хранения документов, которые содержат персональные данные работника, документы подлежат уничтожению. Для этого работодатель создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению. ПДн работников хранящиеся в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация.

3.1.2. Осуществление переподготовки и (или) повышения квалификации работников.

В состав ПДн, обрабатывающихся Оператором для выполнения функций осуществления переподготовки и (или) повышения квалификации работников, входят документы, содержащие:

– фамилия, имя, отчество;

– день, месяц, год и место рождения;

– адрес места жительства;

– паспортные данные (серия, номер паспорта, кем и когда выдан), в том числе загранпаспорт;

– страховой номер индивидуального лицевого счета (СНИЛС);

– сведения об образовании, квалификации;

– контактные данные.

ПДн, представленные работником, обрабатываются автоматизированным и без использования средств автоматизации способами. Министерства труда и социальной политики Республики Тыва не принимает, не снимает и не хранит копии личных документов работников. Документы, которые работник предъявляет работодателю для хранения в оригинале, хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора.

После истечения срока нормативного хранения документов, которые содержат персональные данные работника, документы подлежат уничтожению. Для этого работодатель создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению. ПДн работников хранящиеся в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация.

3.1.3. Бухгалтерский учет.

В состав ПДн, обрабатывающихся Оператором для выполнения функций бухгалтерского учета, входят документы, содержащие:

– фамилия, имя, отчество;

– день, месяц, год и место рождения;

– адрес места жительства;

– паспортные данные (серия, номер паспорта, кем и когда выдан), в том числе загранпаспорт;

– страховой номер индивидуального лицевого счета (СНИЛС);

– идентификационный номер налогоплательщика;

– сведения о заработной плате, в том числе реквизиты банковских карт;

– сведения о семейном положении;

– сведения о трудовой деятельности (номер, серия и дата выдачи трудовой книжки и записях в ней);

– информация о приеме на работу, перемещении по должности, увольнении;

– информация об отпусках;

– информация о командировках.

ПДн, представленные работником, обрабатываются автоматизированным и без использования средств автоматизации способами. Казенное предприятие Республики Тыва «Центр информационных технологий Республики Тыва» не принимает, не снимает и не хранит копии личных документов работников. Документы, которые работник предъявляет работодателю для хранения в оригинале, хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора.

После истечения срока нормативного хранения документов, которые содержат персональные данные работника, документы подлежат уничтожению. Для этого работодатель создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению. ПДн работников хранящиеся в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация.

4. Правовые основания обработки персональных данных

4.1. Обработка персональных данных осуществляется Оператором на законной и справедливой основе, на основании следующих документов:

– Постановление Правительства Республики Тыва от 18 апреля 2023 г. № 229 «Об утверждении Положения о Министерстве труда и социальной политики Республики Тыва»;

– договоры, заключенные между оператором и субъектом персональных данных;

– согласие на обработку персональных данных;

5. Порядок и условия обработки персональных данных

5.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

5.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

5.3. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

5.4. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

5.5. Обработка персональных данных осуществляется путем:

– получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;

– получения персональных данных из общедоступных источников;

– внесения персональных данных в журналы, реестры и информационные системы Оператора;

– использования иных способов обработки персональных данных.

5.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

– определяет угрозы безопасности персональных данных при их обработке;

– принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;

– назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;

– создает необходимые условия для работы с персональными данными;

– организует учет документов, содержащих персональные данные;

– организует работу с информационными системами, в которых обрабатываются персональные данные;

– хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

– организует обучение работников Оператора, осуществляющих обработку персональных данных.

5.9. Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого

требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

5.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

– номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

– подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным

данным нарушает права и законные интересы третьих лиц.

6.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

6.4. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

– иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

– Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

– иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

Приложение №1
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

Типовая форма согласия на обработку персональных данных

г. _____ «___» _____ 20___г.

Я, _____,
(Ф.И.О)

_____ серия _____ № _____ выдан _____
_____,
(вид документа, удостоверяющего личность)

_____
_____
_____,
(когда и кем)

проживающий(ая) по адресу: _____
_____
_____,
настоящим даю свое согласие на обработку _____
_____
_____
(наименование, ФИО и адрес оператора (органа исполнительной власти))

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

Согласие дается мною в целях _____
_____
_____
(цель обработки персональных данных)

и распространяется на следующую информацию:_____
_____
_____
_____
_____.
(перечень персональных данных)

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

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

Данное согласие действует с «___» _____ 20___ г. по «___» _____ 20___ г.

_____

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

Приложение №2
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

Типовая форма согласия на обработку персональных данных разрешенных субъектом персональных данных для распространения

г. _____ «___» _____ 20___г.

Я, _____,
(Ф.И.О)

_____ серия _____ № _____ выдан _____
_____,
(вид документа, удостоверяющего личность)

_____
_____
_____,
(когда и кем)

проживающий(ая) по адресу: _____
_____,
настоящим даю свое согласие на обработку _____
_____
_____
(наименование, ФИО и адрес оператора (органа исполнительной власти))

с целью _____
_____
_____
(цель обработки персональных данных)

в следующем порядке:

Категория персональных данных	**Перечень персональных данных**	**Разрешение к распространению (да/нет)**	**Условия и запреты**
Общие	Фамилия		
	Имя		
	Отчество		
	Год рождения		
	Месяц рождения		
	Дата рождения		
	…		

Специальные	Политические взгляды		
	религия		
	состояние здоровья		
	…		

Сведения об информационных ресурсах оператора, посредством которых будет осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	**Действия с персональными данными**

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

Данное согласие действует с «___» _____ 20___ г. по «___» _____ 20___ г.

_____

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

Приложение №3
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

Типовая форма заявления субъекта об отзыве согласия

Руководителю

_____
(Ф.И.О. руководителя)

_____
(адрес организации)

от_____
(Ф.И.О. субъекта)

_____
(адрес регистрации)

_____
(номер основного документа, удостоверяющего личность)

_____
(дата выдачи указанного документа)

_____
(наименование органа, выдавшего документ)

ЗАЯВЛЕНИЕ

Прошу Вас _____

_____

(прекратить обработку, блокировать/уточнить/изменить/уничтожить/устранить нарушения)

моих персональных данных в связи с _____

_____

_____

_____

_____

(указать причину)

«___» _____ 20___ г. _____ / _____ /
(подпись) (Ф.И.О.)

Приложение №4
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

Типовая форма заявления субъекта о прекращении передачи (распространения) персональных данных

Руководителю

_____
(Ф.И.О. руководителя)

_____
(адрес организации)

от_____
(Ф.И.О. субъекта)

_____
(телефон)

_____
(адрес электронной почты)

ЗАЯВЛЕНИЕ

Прошу Вас прекратить передачу (распространение) следующих моих персональных данных: _____
_____
_____
(указать перечень)

«___» _____ 20___ г. _____ / _____ /
(подпись) (Ф.И.О.)

Приложение №5
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

запроса на доступ к персональным данным

В Министерство труда и социальной политики Республики Тыва
от _____
(ФИО заявителя)

_____
_____
адрес: _____
_____
паспорт серия _____№ _____
выдан _____
_____
телефон
_____
e-mail: _____

ЗАЯВЛЕНИЕ

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, а также:

– указать основания, цели и источник получения такой информации;

– указать способы и сроки ее обработки (в том числе сроки хранения);

– предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ) на основании договора с Министерством труда и социальной политики Республики Тыва или на основании федерального закона;

– предоставить информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– указать наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Министерства труда и социальной политики Республики Тыва, если обработка поручена или будет поручена такому лицу;

– предоставить сведения о том, какие юридические последствия для меня может повлечь её обработка.

В случае отсутствия такой информации прошу Вас уведомить меня об этом.

_____ _____

_____ _____

(подпись) *(ФИО)*

«___»_____ _____г.

Приложение №6
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

повторного запроса на доступ к персональным данным

В Министерство труда и социальной политики Республики Тыва
от _____
(ФИО заявителя)

_____
_____
адрес: _____
_____
паспорт серия _____№ _____
выдан _____
_____
телефон _____
e-mail: _____

ЗАЯВЛЕНИЕ

В связи с _____
_____
(указать обоснование направления запроса)

прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, а также:

– указать основания, цели и источник получения такой информации;

– указать способы и сроки ее обработки (в том числе сроки хранения);

– предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ) на основании договора с Министерством труда и социальной политики Республики Тыва или на основании федерального закона;

– предоставить информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– указать наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Министерства труда и социальной политики Республики Тыва, если обработка поручена или будет поручена такому лицу;

– предоставить сведения о том, какие юридические последствия для меня может повлечь её обработка.

_____ _____

(подпись) *(ФИО)*

«___»_____ _____ г.

Приложение №7
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

запроса об уточнении персональных данных

В Министерство труда и социальной политики Республики Тыва
от _____
(ФИО заявителя)

_____
адрес: _____
_____
паспорт серия _____№ _____
выдан _____
_____
телефон
_____
e-mail: _____

ЗАЯВЛЕНИЕ

Прошу уточнить обрабатываемые Вами мои персональные данные: _____,
(указать уточненные персональные данные заявителя)

в связи с _____
(указать причину уточнения персональных данных)

_____

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

«__» _____ 20__г. _____/_____
(подпись) *(расшифровка подписи)*

Приложение №8
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

запроса о блокировании персональных данных

В Министерство труда и социальной политики Республики Тыва
от _____
(ФИО заявителя)
_____
адрес: _____
_____
паспорт серия _____№ _____
выдан _____
_____
телефон
_____
e-mail: _____

ЗАЯВЛЕНИЕ

Прошу заблокировать обрабатываемые Вами мои персональные данные:

_____
(указать блокируемые персональные данные)

на срок: _____, в связи с _____.
(указать срок блокирования) *(указать причину)*

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

«__» _____ 20__г. _____/_____
(подпись) *(расшифровка подписи)*

Приложение №9
к Политике по обработке персональных данных
в информационных системах
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

запроса об унижении персональных данных

В Министерство труда и социальной политики Республики Тыва
от _____
(ФИО заявителя)

_____
адрес: _____
_____
паспорт серия _____№ _____
выдан _____
_____
телефон
_____
e-mail: _____

ЗАЯВЛЕНИЕ

Прошу Вас прекратить обработку и уничтожить мои персональные данные:

_____,
(указать уничтожаемые персональные данные)

в связи с _____.
(указать причину уничтожения персональных данных)

Ответ прошу направить в письменной форме по вышеуказанному адресу в срок, предусмотренный Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

«__» _____ 20__г. _____/_____
(подпись) *(расшифровка подписи)*

Приложение № 2
к приказу №_____ от __.__20__г.

ПОЛОЖЕНИЕ
об обработке персональных данных в информационных системах персональных данных Министерства труда и социальной политики Республики Тыва

2024

СОДЕРЖАНИЕ

1 Общие положения

1.1 Настоящее Положение об обработке персональных данных (далее – Положение) определяет порядок обработки персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн) Министерства труда и социальной политики Республики Тыва (далее – Оператор) в соответствии с законодательством Российской Федерации.

1.2 Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3 Для целей настоящего Положения используются следующие основные понятия:

– персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных);

– оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки 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;

– распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

– использование персональных данных – действия с персональными данными, совершаемые сотрудниками Министерства труда и социальной политики Республики Тыва в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

– автоматизированная обработка – обработка данных, выполняемая средствами вычислительной техники;

– блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

– уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных – система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

– защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном субъекте персональных данных.

2 Получение, обработка и защита персональных данных

2.1 Порядок получения персональных данных.

2.1.1 Персональные данные могут быть получены Министерством труда и социальной политики Республики Тыва только способами, предусмотренными действующим законодательством Российской Федерации. При этом получение письменного согласия, а также разъяснение субъекту персональных данных (далее – субъект ПДн) о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение, возлагается на Оператора. В случае отказа субъекта ПДн предоставить свои персональные данные ему должны быть разъяснены юридические последствия такого отказа.

2.1.2 Сотрудники Министерства труда и социальной политики Республики

Тыва имеют право получать только те персональные данные, которые необходимы им для выполнения своих служебных обязанностей.

2.1.3 Сотрудники Министерства труда и социальной политики Республики Тыва, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

2.2 Порядок обработки персональных данных.

2.2.1 Обработка персональных данных может осуществляться только в заявленных целях.

2.2.2 При определении объема и содержания обрабатываемых персональных данных, Министерства труда и социальной политики Республики Тыва должно руководствоваться Конституцией Российской Федерации, федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными нормативно-правовыми актами в области защиты персональных данных.

2.2.3 При принятии решений, затрагивающих интересы субъекта ПДн, Министерство труда и социальной политики Республики Тыва не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронно.

2.3 Порядок защиты персональных данных.

2.3.1 Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Министерством труда и социальной политики Республики Тыва за счет ее средств в порядке, установленном нормативно-правовыми актами Российской Федерации в области защиты персональных данных.

2.3.2 Министерство труда и социальной политики Республики Тыва обязано при обработке персональных данных субъектов ПДн принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.3.3 Соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн.

2.3.4 Применять технические средства охраны и сигнализации.

2.3.5 Взять со всех сотрудников, связанных с получением, обработкой и защитой персональных данных субъектов ПДн, типовое обязательство сотрудника Министерства труда и социальной политики Республики Тыва о неразглашении персональных данных и о прекращении обработки персональных данных в случае

расторжения с ним трудового договора.

2.3.6 Привлекать к дисциплинарной ответственности сотрудников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов ПДн.

2.3.7 Запретить допуск к персональным данным субъектов ПДн сотрудников Министерства труда и социальной политики Республики Тыва, не включенных в «Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем персональных данных, и доступ к обработке персональных данных, обрабатываемых в информационных системах персональных данных Министерства труда и социальной политики Республики Тыва».

2.3.8 Защита доступа к электронной базе данных, содержащей персональные данные субъектов ПДн, должна обеспечиваться путем использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн.

2.3.9 Копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях с письменного разрешения руководителя.

2.3.10 Субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных.

3 Хранение персональных данных

3.1 Сведения о субъектах ПДн в Министерстве труда и социальной политики Республики Тыва на материальных носителях должны храниться в специально оборудованных шкафах и сейфах, которые запираются и (или) опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственных сотрудников.

3.2 Материальные носители персональных данных, обработка которых осуществляется в различных целях, должны храниться отдельно. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.3 Обязанности по организации хранения сведений о субъектах ПДн, заполнения, хранения и выдачи документов, содержащих персональные данные, в ИС Министерства труда и социальной политики Республики Тыва возлагаются на

Ответственного за обработку и защиту персональных данных.

3.4 Съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн, должны быть промаркированы и учтены в Журнале регистрации, учета и выдачи машинных носителей персональных данных.

3.5 В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4 Передача персональных данных

4.1 При передаче персональных данных субъекта ПДн Министерство труда и социальной политики Республики Тыва должно соблюдать требования, установленные законами Российской Федерации, нормативно-правовыми актами ФСБ России и ФСТЭК России.

5 Уничтожение персональных данных

5.1 Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации в сфере обработки персональных данных.

5.2 Уничтожение документов, содержащих персональные данные, осуществляется в порядке, предусмотренном архивным законодательством Российской Федерации.

5.3 При необходимости уничтожения персональных данных Министерства труда и социальной политики Республики Тыва должно руководствоваться следующими требованиями:

5.3.1 Уничтожение персональных данных в ИСПДн Министерстве труда и социальной политики Республики Тыва осуществляется комиссией по проведению мероприятий по защите персональных данных.

5.3.2 Бумажные носители персональных данных должны уничтожаться при помощи специального оборудования (измельчителя бумаги).

5.3.3 Персональные данные, представленные в электронном виде, должны уничтожаться специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных.

5.3.4 После окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

6 Реагирование на запросы субъектов ПДн и их законных представителей

6.1 Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных.

6.2 При рассмотрении запросов, поступающих от субъектов ПДн и их законных представителей, Оператор руководствуется Правилами рассмотрения запросов.

6.3 Все обращения, поступающие от субъектов ПДн и их законных представителей, должны регистрироваться ответственным за обработку и защиту персональных данных в соответствующем журнале.

6.4 Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

7 Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

7.1 Лица, виновные в нарушении требований федеральных законов, несут предусмотренную законодательством Российской Федерации ответственность.

7.2 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение № 1
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

Типовое обязательство работника Министерства труда и социальной политики Республики Тыва, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Мне, _____,
(фамилия, имя, отчество полностью)

паспорт (иной документ, удостоверяющий личность) _____

_____
(серия, номер, кем и когда выдан)

_____

известно, что в период прохождения работы в Министерстве труда и социальной политики Республики Тыва персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат.

В случае расторжения со мной трудового договора, освобождения меня от замещаемой должности и увольнения из Министерства труда и социальной политики Республики Тыва, прекращения (расторжения) трудового договора обязуюсь:

1. Не разглашать персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей в Министерстве труда и социальной политики Республики Тыва, третьей стороне без письменного согласия субъектов персональных данных, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных законодательством.

2. Не использовать персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей в Министерстве труда и социальной

политики Республики Тыва, в коммерческих целях без письменного согласия субъектов персональных данных.

3. Прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей в Министерстве труда и социальной политики Республики Тыва.

4. Не копировать лично и не давать поручения копировать электронную базу данных, не допускать её копирования третьими лицами, сдать все имеющиеся электронные носители, принадлежащие Министерству труда и социальной политики Республики Тыва.

Мне разъяснены положения действующего законодательства об обеспечении сохранности персональных данных субъектов персональных данных.

Мне известно, что нарушение этих положений может повлечь дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

«____» _____ 20___г. _____

(подпись, расшифровка подписи)

Приложение № 2
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

Типовое обязательство
работника Министерства труда и социальной политики Республики Тыва о неразглашении персональных данных

Я, _____ ,
(фамилия, имя, отчество)

работник Министерства труда и социальной политики Республики Тыва, предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией (должностным регламентом) мне будет предоставлен допуск к персональным данным (далее – ПДн).

Я проинформирован(а) о факте обработки мной ПДн, обработка которых осуществляется Министерством труда и социальной политики Республики Тыва с использованием и без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Министерства труда и социальной политики Республики Тыва.

Настоящим добровольно принимаю на себя нижеследующие обязательства.

1. Не распространять третьим лицам ПДн, которая мне доверена (будет доверена) или станет известной в связи с выполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня ПДн сообщать непосредственному руководителю, а также лицу, ответственному за защиту ПДн в Министерстве труда и социальной политики Республики Тыва.

3. Выполнять относящиеся ко мне требования нормативных правовых актов, а также приказов, инструкций и положений в области обработки и защиты Информации, с которыми я ознакомлен(а).

4. Не использовать Информацию с целью получения выгоды.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

«___» _____ 20__ г. _____/_____
Ф.И.О. подпись

Один экземпляр обязательства получил

«___» _____ 20__ г. _____/_____
Ф.И.О. подпись

Приложение № 3
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

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

Мне,

_____,
(фамилия, имя, отчество полностью)

паспорт (иной документ, удостоверяющий личность) _____
_____
_____
(серия, номер, кем и когда выдан)

разъяснены юридические последствия отказа предоставить свои персональные данные Министерству труда и социальной политики Республики Тыва.

В соответствии с Постановлением Правительства РФ от 21.03.2012 г. №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» и «Правилами обработки персональных данных в Министерстве труда и социальной политики Республики Тыва, определён перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с решением вопросов в сфере деятельности, оказанием государственной услуги, реализацией права на труд, права на пенсионное обеспечение, права на медицинское страхование работников.

Я предупрежден, что в случае отказа предоставить свои персональные данные Министерству труда и социальной политики Республики Тыва при решении вопросов в сфере деятельности, пенсионного обеспечения и медицинского страхования не могут быть реализованы в полном объёме, а служебный (трудовой) контракт подлежит расторжению.

«____» _____ 20___г. _____
(подпись, расшифровка подписи)

Юридические последствия отказа предоставить персональные данные разъяснил (а):

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)

Приложение № 4
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

Уведомление о получении персональных данных у третьей стороны

Уважаемый(ая) _____,
(фамилия, имя, отчество полностью)

в связи с _____
(указать причину)

_____

_____

в Министерстве труда и социальной политики Республики Тыва возникла необходимость получения следующей информации, содержащей Ваши персональные данные: _____

_____

_____.
(перечислить информацию)

Просим Вас представить указанные сведения _____

_____
(кому, указать организацию)

в течение трех рабочих дней с момента получения настоящего уведомления.

В случае невозможности предоставить указанные сведения просим в указанный срок, дать письменное согласие на получение Министерству труда и социальной политики Республики Тыва из следующих источников: _____

_____

_____,
(указать источники)

следующими способами: _____

_____.
(автоматизированная обработка, иные способы)

По результатам обработки указанной информации Министерством труда и социальной политики Республики Тыва планируется принятие следующих решений, которые будут доведены до Вашего сведения: _____

_____

(указать решения и иные юридические последствия обработки информации)

Против принятого решения Вы имеете право заявить свои письменные возражения в срок до «__» _____20__г.

Информируем Вас о последствиях Вашего отказа дать письменное согласие на получение организацией указанной информации _____

_____

(перечислить последствия)

Информируем Вас о Вашем праве в любое время отозвать свое письменное согласие на обработку персональных данных.

Настоящее уведомление на руки получил:

«____» _____ 20___г. _____

(подпись, расшифровка подписи)

Приложение № 5
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

УВЕДОМЛЕНИЕ
о прекращении обработки персональных данных

Уважаемый(ая) _____!
(Имя, Отчество)

В связи с _____
сообщаем Вам, что обработка Ваших персональных данных прекращена.

_____	_____	_____
(должность)	*(подпись)*	*(расшифровка подписи)*

Приложение № 6
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

УВЕДОМЛЕНИЕ
о предоставлении персональных данных

Уважаемый(ая) _____!
(Имя, Отчество)

В Министерстве труда и социальной политики Республики Тыва производится обработка сведений, составляющих Ваши персональные данные, а именно:

_____
(указать сведения)

Цели обработки: _____.

Способы обработки: _____.

Другое (*в зависимости от запроса*).

По результатам обработки указанной информации нами планируется принятие следующих решений _____
_____,
которые будут доведены до Вашего сведения.

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

_____	_____	_____
(должность)	*(подпись)*	*(расшифровка подписи)*

Приложение № 7
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

мотивированного отказа на повторный запрос о предоставлении персональных данных

Уважаемый(ая) _____!
(Имя, Отчество)

На основании _____
(указать основание)

_____

в выполнении повторного запроса отказано.

_____ _____ _____
(должность) *(подпись)* *(расшифровка подписи)*

Приложение № 8
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

УВЕДОМЛЕНИЕ
о внесении изменений в персональные данные

Уважаемый(ая) _____!
(Имя, Отчество)

В связи с _____
сообщаем Вам, что Ваши персональные данные уточнены в соответствии со сведениями:
_____.

_____ _____ _____
(должность) *(подпись)* *(расшифровка подписи)*

Приложение № 9
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

УВЕДОМЛЕНИЕ
о блокировании персональных данных

Уважаемый(ая) _____!
(Имя, Отчество)

В связи с _____ сообщаем Вам, что Ваши персональные данные _____
(указать персональные данные)

_____

_____

_____

заблокированы на срок _____.

_____ _____ _____
(должность) *(подпись)* *(расшифровка подписи)*

Приложение № 10
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ТИПОВАЯ ФОРМА

УВЕДОМЛЕНИЕ
об уничтожении персональных данных

Уважаемый(ая) _____!
(Имя, Отчество)

Настоящим уведомлением сообщаем Вам, что в соответствии с требованиями статьи 21 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», Ваши персональные данные в информационной системе персональных данных Министерства труда и социальной политики Республики Тыва уничтожены.

_____	_____	_____
(должность)	*(подпись)*	*(расшифровка подписи)*

Приложение № 11
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ЖУРНАЛ УЧЕТА ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ
Министерства труда и социальной политики Республики Тыва

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых ПДн	Цель получения ПДн	Отметка о передаче или отказе в передаче ПДн	Дата передачи/отказа в предоставлении ПДн	Подпись запрашивающего лица	Подпись ответственного сотрудника

Приложение № 12
к Положению об обработке персональных данных
в информационных системах персональных данных
Министерства труда и социальной политики Республики Тыва

ЖУРНАЛ №____

учета обращений субъектов персональных данных по вопросам обработки их персональных данных в информационных системах персональных данных Министерства труда и социальной политики Республики Тыва

Начат «___» _____ 20___ г. На ____ листах

Окончен «___» _____ 20___ г.

_____ _____

(ФИО ответственного лица за ведение журнала) (подпись)

№ п/п	Дата обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении или отказе в предоставлении персональных данных (предоставлено/отказано)	Дата передачи/отказа в предоставлении персональных данных	Подпись ответственного сотрудника
1	2	3	4	5	6	8

Приложение № 3
к приказу №_____ от __.__20__г.

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О ПЕРСОНАЛЬНЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Министерства труда и социальной политики Республики Тыва (далее – Правила) устанавливают порядок осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в Министерстве труда и социальной политики Республики Тыва.

2. Осуществление внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в Министерстве труда и социальной политики Республики Тыва осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Постановлением Правительства РФ 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки ПДн.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн (далее – внутренний контроль) является обеспечение защиты ПДн от несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля.

5. Внутренний контроль делится на текущий, плановый и внеплановый.

6. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки ПДн в Министерстве труда и социальной

политики Республики Тыва (далее – ответственный за организацию обработки) в ходе мероприятий по обработке ПДн.

Ответственный за организацию обработки имеет право:

– запрашивать у сотрудников Министерства труда и социальной политики Республики Тыва информацию, необходимую для реализации полномочий;

– требовать от уполномоченных на обработку ПДн должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;

– принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить руководству Министерства труда и социальной политики Республики Тыва предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

– вносить руководству Министерства труда и социальной политики Республики Тыва предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о ПДн.

7. Плановый внутренний контроль осуществляется комиссией, образуемой приказом руководителя Министерства труда и социальной политики Республики Тыва, в состав которой входят работники Министерства труда и социальной политики Республики Тыва, допущенные к обработке ПДн.

Плановый внутренний контроль соответствия обработки ПДн установленным требованиям в Министерстве труда и социальной политики Республики Тыва проводится на основании утвержденного руководителем Министерства труда и социальной политики Республики Тыва плана осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям, разрабатываемого председателем комиссии. Периодичность плановой проверки – не реже одного раза в год.

8. Внеплановый внутренний контроль может осуществляться на основании поступившего в Министерстве труда и социальной политики Республики Тыва письменного заявления о нарушениях правил обработки ПДн (внеплановые проверки). Проведение внеплановой проверки организуется председателем комиссии в течение 3 рабочих дней с момента поступления соответствующего заявления.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

9. При проведении внутреннего контроля ответственным за организацию обработки или комиссией должны быть полностью, объективно и всесторонне изучены:

– наличие, учет, порядок хранения и обезличивания ПДн;

– порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке;

– порядок и условия применения средств защиты информации;

– эффективность принимаемых мер по обеспечению безопасности ПДн;

– состояние учёта ПЭВМ и съемных носителей информации, содержащей ПДн;

– соблюдение правил доступа к ПДн;

– наличие (отсутствие) фактов несанкционированного доступа к ПДн;

– порядок проведения мероприятий и результаты по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– порядок проведения мероприятий по обеспечению целостности ПДн.

9. В отношении ПДн, ставших известными членам комиссии или ответственному за организацию обработки в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность ПДн.

10. Срок проведения плановой и внеплановой проверки не может составлять более 30 дней со дня принятия решения о её проведении.

11. Результаты внутреннего контроля оформляются в виде протокола проведения внутренней проверки (далее – протокол).

12. При выявлении в ходе внутреннего контроля нарушений ответственным за организацию обработки либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

13. Протоколы хранятся у ответственного за организацию обработки в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки самостоятельно в январе года, следующего за проверочным годом

14. О результатах внутреннего контроля и мерах, необходимых для устранения нарушений, руководству Министерства труда и социальной политики Республики Тыва докладывает ответственный за организацию обработки либо председатель комиссии.

Приложение №1
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

ПРАВИЛА
оценки вреда в информационных системах Министерства труда и социальной политики Республики Тыва который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных

1. Назначение

Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных (далее – Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения требований, указанных в Федеральном законе от27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Общие положения

Настоящие Правила являются дополнением к действующим нормативным документам по вопросам обеспечения безопасности информации и не исключает обязательного выполнения их требований.

Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

3. Методика оценки возможного вреда субъектам персональных данных

Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, с целью их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении персональных данных.

Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

• неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

• неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

• неправомерное изменение персональных данных является нарушением целостности персональных данных;

• нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности персональных данных;

• нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;

• обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных является нарушением конфиденциальности персональных данных;

• неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

• несанкционированная обработка неправильных, либо неполных персональных данных является нарушением целостности персональных данных.

Субъекту персональных данных может быть причинён вред в форме:

• убытков – расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

• морального вреда – нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;

• имущественный вред – ущерб, нанесённый имущественному положению юридического или физического лица вследствие причинения ему вреда или неисполнения условий договора.

В оценке возможного вреда необходимо исходить из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:

• низкий уровень возможного вреда – если нарушение свойств безопасности может привести к незначительным негативным последствиям для субъектов персональных данных.

• средний уровень возможного вреда – если нарушение свойств безопасности может привести к негативным последствиям для субъектов персональных данных.

• высокий уровень возможного вреда – если нарушение свойств безопасности может привести к значительным негативным последствиям для субъектов персональных данных.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер

Оценка возможного вреда субъектам персональных данных осуществляется ответственным за организацию обработки персональных данных, в соответствии с методикой, описанной в разделе 3 настоящих Правил.

По результатам оценки составляется Акт оценки вреда в ИС Министерства труда и социальной политики Республики Тыва, который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных (Приложение №1 к настоящим Правилам).

Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», определяется лицом, ответственным за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение №1
к Правилам оценки вреда, который может быть причинен
субъектам персональных данных в случае
нарушения требований федерального законодательства
по защите персональных данных

ТИПОВАЯ ФОРМА

УТВЕРЖДАЮ
Министр Министерства труда и
социальной политики Республики
Тыва
Сандан Э.Ф.
«____» _____ ____

АКТ
оценки вреда в информационных системах Министерства труда и социальной политики Республики Тыва, который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных

Руководствуясь Правилами оценки вреда в ИС Министерства труда и социальной политики Республики Тыва, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ИС Министерства труда и социальной политики Республики Тыва Ответственный за организацию обработки персональных данных определил:

В результате нарушения безопасности персональных данных субъекту персональных данных может быть причинен ущерб в виде имущественного вреда/ морального вреда /убытков. В результате субъектам персональных данных может быть причинён вред, который оценивается как низкий/средний/высокий.

_____
ФИО

_____
Должность ответственного

Приложение №2
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

План внутренних проверок режима защиты персональных данных Министерства труда и социальной политики Республики Тыва

№ п/п	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Контроль соблюдения правил обработки ПДн	Ежемесячно	
2.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
3.	Контроль соблюдения режима парольной защиты	Ежемесячно	
4.	Контроль выполнения антивирусной защиты	Еженедельно	
5.	Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС	Еженедельно	
7.	Контроль над обеспечением резервного копирования	Ежемесячно	
8.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также анализ появления новых, еще неизвестных, угроз	Ежегодно	
9.	Поддержание в актуальном состоянии нормативно-организационных документов	Ежеквартально	
10.	Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное программное обеспечение, специально дорабатываемое собственными разработчиками или сторонними организациями (при наличии)	Ежемесячно	
11.	Тестирование всех функций СЗИ от НСД с помощью специальных программных средств	Ежегодно	

Приложение №3
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

ЖУРНАЛ ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

№ п/п	Дата проведения	Мероприятие	Исполнитель	Результат	Подпись
1					

Приложение №4
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

ЖУРНАЛ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ С ДОКУМЕНТАМИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

Фамилия И. О. ознакамливающегося	Наименование документа									
	Политика по обработке персональных данных	Положение по организации и проведению работ по обеспечению безопасности персональных данных	Правила обработки персональных данных	Перечень персональных данных в информационной системе и подлежащих защите	Инструкция пользователя информационных систем	Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации	Инструкция по организации парольной защиты в информационных системах	Инструкция по организации антивирусной защиты в информационных системах	Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена	Инструкция по обращению с сертифицированными средствами криптографической защиты

Приложение № 4
к приказу №_____ от __.__20__г.

ПРАВИЛА
обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

1. Наименования информационных систем

1.1. Наименования информационных систем (далее – ИС) Министерства труда и социальной политики Республики Тыва (далее – Министерство) указано в таблице 1.

Таблица 1 – Наименования информационных систем

Наименование информационной системы	
Полное	**Сокращенное**
Информационная система «Катарсис»	Катарсис
АС АСП «Тула»	Тула

2. Основание и цели обработки персональных данных

2.1. Основания обработки персональных данных в Министерстве, а также источники их получения указаны в таблице 2.

Таблица 2 – Основание обработки персональных данных в информационных системах

Наименование ИС	**Основание обработки**	**Цель обработки**	**Источники получения ПДн**
Информационная система «Катарсис»	Обработка ПДн в Министерстве осуществляется в процессе ведения уставной деятельности организации, в частности, в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Министерство выступает в качестве исполнителя государственных услуг	Для оказания государственных услуг	ФИО, прописка, паспортные данные, кем и когда выдан паспорт, ИНН, СНИЛС, оплата труда, дата, место, год рождения.
АС АСП «Тула»	Обработка ПДн в Министерстве	Для оказания	ФИО,

Наименование ИС	Основание обработки	Цель обработки	Источники получения ПДн
	осуществляется в процессе ведения уставной деятельности организации, в частности, в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Министерство выступает в качестве исполнителя государственных услуг	государственных услуг	прописка, паспортные данные, кем и когда выдан паспорт, ИНН, СНИЛС, оплата труда, дата, место, год рождения.

3. Перечень персональных данных о субъекте персональных данных, обрабатываемых в информационных системах и категории субъектов, персональные данные которых обрабатываются

Перечень персональных данных о субъекте персональных данных, обрабатываемых в информационных системах, и категории субъектов, персональные данные которых обрабатываются, указаны в таблице 3.

Таблица 3 – Перечень персональных данных, обрабатываемых в информационных системах

Наименование ИС	Тип субъектов персональных данных	Состав сведений	Допустимые операции
Информационная система «Катарсис»	Не являются сотрудниками оператора	ФИО, прописка, паспортные данные, кем и когда выдан паспорт, ИНН, СНИЛС, оплата труда, дата, место, год рождения	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача (предоставление), блокирование, удаление, уничтожение
АС АСП «Тула»	Не являются сотрудниками оператора	ФИО, прописка, паспортные данные, кем и когда выдан паспорт, ИНН, СНИЛС, оплата труда, дата, место, год рождения	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача (предоставление), блокирование, удаление, уничтожение

4. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных

4.1. К принимаемым в Министерстве мерам по выявлению и предотвращению нарушений законодательства в сфере персональных данных относятся:

– организация режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей персональных данных;

– утверждение министром документа, определяющего перечень лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем, и доступ к обработке информации в информационных системах;

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

– назначение сотрудника, ответственного за обработку и защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

– ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями действующего законодательства о персональных данных и иными документами по вопросам обработки персональных данных;

– определение угроз безопасности персональных данных при их обработке в информационных системах;

– осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;

– установление правил доступа к персональным данным, обрабатываемым в информационных системах;

– осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности персональных данных.

5. Определение сроков обработки персональных данных в информационных системах

5.1 Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не

установлен законодательством Российской Федерации и/или договором, стороной которого является субъект персональных данных.

5.2 Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации в сфере обработки персональных данных.

5.3 Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований определен в разделе 5 «Положения об обработке персональных данных в информационных системах Министерства труда и социальной политики Республики Тыва».

Приложение № 5
к приказу №_____ от __.__20__г.

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1 Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов ПДн или их представителей в Министерстве труда и социальной политики Республики Тыва (далее – Правила) устанавливают единый порядок рассмотрения запросов субъектов ПДн или их представителей в Министерстве труда и социальной политики Республики Тыва (далее – Оператор).

1.2. Рассмотрение запросов субъектов ПДн или их представителей в Министерстве труда и социальной политики Республики Тыва осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки ПДн.

1.3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

1.4. Целью настоящих Правил является реализация прав субъекта ПДн на получение информации, касающейся обработки его ПДн в Министерстве труда и социальной политики Республики Тыва.

1.5. К субъектам, ПДн которых обрабатываются, относятся:

– граждане, обратившиеся в Министерстве труда и социальной политики Республики Тыва с жалобами, заявлениями и по другим вопросам, касающимся установленной сферы деятельности;

– граждане, претендующие на замещение должности государственной гражданской службы и должности технического (рабочего) персонала в Министерстве труда и социальной политики Республики Тыва;

– граждане, замещающие (замещавшие) должности государственной гражданской службы и должности технического (рабочего) персонала в Министерстве труда и социальной политики Республики Тыва.

2 Права субъекта персональных данных

2.1 Право субъекта ПДн на доступ к его ПДн:

2.1.1. Субъект ПДн имеет право на получение сведений, указанных в пункте 2.1.7, за исключением случаев, предусмотренных пунктом 2.1.8. 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.

2.1.2. Сведения, указанные в пункте 2.1.7, должны быть предоставлены субъекту ПДн оператором 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.

2.1.3. Сведения, указанные в пункте 2.1.7, предоставляются субъекту ПДн или его представителю оператором при обращении либо при получении запроса субъекта ПДн или его представителя. В запросе указываются сведения о субъекте ПДн или его представителе в соответствии с пунктом 3.2.

2.1.4. В случае если сведения, указанные в пункте 2.1.7, 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 пункте 2.1.7, 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 выгодно приобретателем или поручителем по которому является субъект ПДн.

2.1.5. Субъект ПДн вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 2.1.7, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в пункте 2.1.4, 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 со сведениями, указанными в пункте 3.2, должен содержать обоснование направления повторного запроса.

2.1.6. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 2.1.4 и 2.1.5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

2.1.7. 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 работников 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 представления таких данных не предусмотрен федеральным законом;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– 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 № 152-ФЗ или другими федеральными законами.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

2.2. Право на обжалование действий или бездействия оператора:

2.2.1. Если субъект ПДн считает, что оператор осуществляет обработку его ПДн с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

2.2.2. 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.

3 Порядок предоставления оператором сведений по запросу субъекта персональных данных

3.1. При обращении либо при получении запроса субъекта ПДн или его представителя, сведения должны быть предоставлены в доступной форме. Запрос регистрируется в день поступления по правилам делопроизводства.

3.2. Запрос субъекта ПДн должен содержать сведения, позволяющие провести его идентификацию:

– фамилию, имя, отчество субъекта ПДн и его представителя;

– номер основного документа, удостоверяющего личность субъекта ПДн или его представителя;

– сведения о дате выдачи указанного 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.

3.3. Оператор, при получении запроса субъекта ПДн или его представителя, обязан сообщить в порядке статьи 14 Федерального закона № 152-ФЗ субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн в течение 30 (тридцати) дней с даты получения запроса.

В случае отказа в предоставлении информации о наличии ПДн, оператор обязан дать в письменной форме мотивированный ответ со ссылкой на действующее законодательство, являющееся основанием для такого отказа. Отказ в предоставлении информации направляется в срок, не превышающий 30 (тридцать) дней со дня получения запроса субъекта ПДн.

3.4. В случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, оператор в срок, не превышающий 7 (семь) рабочих дней, вносит в них необходимые изменения. О внесённых изменениях уведомляется субъект ПДн или его представитель.

3.5. В случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн в срок, не превышающий 7 (семь) рабочих дней. Об уничтоженных ПДн уведомляется субъект ПДн или его представитель.

3.6. Возможность ознакомления с ПДн предоставляется на безвозмездной основе лицом, ответственным за обработку ПДн.

Приложение № 6
к приказу №_____ от __.__20__г.

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Настоящие Правила работы с обезличенными данными в Министерстве труда и социальной политики Республики Тыва (далее – Правила) устанавливают порядок проведения мероприятий в Министерстве труда и социальной политики Республики Тыва (далее – Министерство) по обезличиванию ПДн, порядок и условия работы с обезличенными данными.

2. Обезличивание ПДн и работа с обезличенными данными в Министерстве осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Постановлением Правительства РФ 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки ПДн.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

4. Целью обезличивания ПДн в Министерстве является обеспечение защиты ПДн граждан от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

5. Обезличивание ПДн может быть проведено для решения следующих задач:

- получения статистических данных;
- снижения ущерба от разглашения защищаемых ПДн;
- снижения класса используемых ИС.

Кроме того, обезличивание ПДн может быть проведено по достижению сроков обработки или в случае утраты необходимости в достижении целей обработки, если иное не предусмотрено законодательством Российской Федерации.

6. В случае достижения целей обработки ПДн или в случае утраты необходимости в их достижении, сотрудник Министерства, обрабатывающий ПДн, обязан:

- незамедлительно прекратить обработку ПДн;

– обезличить соответствующие ПДн в срок, не превышающий 30 дней с даты достижения целей обработки ПДн или утраты необходимости достижения этих целей.

7. ПДн не обезличиваются в случаях, если:

– договором (соглашением), стороной которого или поручителем, по которому является субъект ПДн, предусмотрен иной порядок обработки ПДн;

– законодательством установлены сроки обязательного архивного хранения материальных носителей ПДн;

– в иных случаях, прямо предусмотренных законодательством.

8. В случае выявления недостоверности ПДн, неправомерности действий с ПДн сотрудник Министерства, обрабатывающий ПДн, обязан осуществить незамедлительное блокирование указанных ПДн и в срок, не превышающий 3 рабочих дней с даты такого выявления, устранить допущенные нарушения.

В случае подтверждения факта недостоверности ПДн сотрудник Министерства, обрабатывающий ПДн, уточняет ПДн и снимает с них блокирование на основании документов, представленных:

– субъектом ПДн (его законным представителем);

– уполномоченным органом по защите прав субъектов ПДн;

– иными лицами.

9. В случае невозможности устранения допущенных нарушений сотрудник Министерства, обрабатывающий ПДн, в срок, не превышающий 10 рабочих дней с даты выявления неправомерности действий с ПДн, обезличивает ПДн.

Об устранении допущенных нарушений или об обезличивании ПДн сотрудник Министерства, обрабатывающий ПДн, уведомляет субъекта ПДн (его законного представителя) по форме уведомления об устранении допущенных нарушений или уведомления об уничтожении (Приложение №1, 2) и (или) уполномоченный орган по защите прав субъектов ПДн по форме уведомления об устранении допущенных нарушений или уведомления об уничтожении (Приложение №3, 4).

10. В случае отзыва субъектом ПДн согласия на обработку своих ПДн сотрудник Министерства, обрабатывающий ПДн, обязан прекратить обработку ПДн х и обезличить их в срок, не превышающий 30 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством, договором или соглашением между Министерства и субъектом ПДн. Об обезличивании ПДн сотрудник Министерства, обрабатывающий ПДн, уведомляет субъекта ПДн (его законного представителя).

11. Способы обезличивания:

11.1. К способам обезличивания ПДн при условии дальнейшей обработки ПДн относятся:

– уменьшение перечня обрабатываемых сведений, замена части сведений словными обозначениями, обобщение (понижение) точности некоторых сведений;

– деление сведений на части и обработка их в разных ИС, другие способы.

11.2. К способам обезличивания ПДн в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей относятся:

– сокращение перечня ПДн;

– уничтожение ПДн.

11.3. Уничтожение части ПДн, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных ПДн, зафиксированных на материальном носителе (закрашиванием, вырезанием и т.д.).

12. Правила работы с обезличенными данными:

12.1. Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

12.2. Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

12.3. При обработке обезличенных ПДн с использованием средств автоматизации необходимо:

– использование паролей;

– использование антивирусных программ;

– соблюдение правил доступа в помещения, в которых ведётся обработка ПДн.

12.4. При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

– хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

– соблюдение правил доступа в помещения, в которых ведётся обработка ПДн.

Приложение №1
к Правилам работы с обезличенными данными в
Министерстве

Уведомление об устранении допущенных нарушений

Уважаемый(ая) _____,
(фамилия, имя, отчество)

в связи с _____

_____

_____

сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

«____» _____ 20___ г. _____ _____
(подпись) (расшифровка подписи)

Приложение №2
к Правилам работы с обезличенными данными в
Министерстве

Уведомление об уничтожении

Уважаемый(ая) _____,
(фамилия, имя, отчество)

в связи с _____

_____

_____

сообщаем Вам, что Ваши персональные данные уничтожены.

«____» _____ 20___ г. _____ _____
(подпись) (расшифровка подписи)

Приложение №3
к Правилам работы с обезличенными данными в
Министерстве

Уведомление об устранении допущенных нарушений

В отношении порядка обработки персональных данных, принадлежащих:

_____

(фамилия, имя, отчество)

_____,

(если имеются, дополнительные сведения для идентификации: дата рождения / адрес)

были допущены нарушения, в связи с _____

_____

_____

сообщаем, что все допущенные нарушения при обработке персональных данных устранены.

«____» _____ 20___ г. _____ _____

(подпись) (расшифровка подписи)

Приложение №4
к Правилам работы с обезличенными данными в
Министерстве

Уведомление об уничтожении

В связи с _____
_____
_____
сообщаем, что обработка персональных данных, принадлежащих
_____
(фамилия, имя, отчество)
_____,
(если имеются, дополнительные сведения для идентификации: дата рождения / адрес)

была прекращена, а сами данные уничтожены.

«____» _____ 20___ г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 7
к приказу №_____ от __.__20__г.

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Наименование информационной системы (ИС)	Тип ИС[1]	Уровень защищенности ПДн	Класс защищенности ГИС	Акт классификации
Катарсис	ГИС	УЗ-3	К3	Акт от 21.11.2024 г.
АС АСП Тула	ГИС	УЗ-3	К3	Акт от 13.07.2021г.

[1] Типы ИС: ИСПДн – ИС персональных данных, ГИС – государственная ИС

Приложение № 8
к приказу №_____ от __.__20__г.

ПРАВИЛА
доступа к персональным данным в Министерстве труда и социальной политики Республики Тыва

1. Общие положения

1.1. Настоящие правила определяют порядок доступа к персональным данным, обрабатываемым в информационных системах Министерства труда и социальной политики Республики Тыва (далее – информационные системы).

2. Организация доступа к персональным данным

2.1. В Министерстве труда и социальной политики Республики Тыва утверждается перечень должностей, которым предоставляется доступ к персональным данным, обрабатываемым в информационных системах, для выполнения ими трудовых и служебных обязанностей (далее – лица, допущенные к персональным данным).

3. Обязанности лиц, допущенных к персональным данным

3.1. Лица, допущенные к персональным данным обязаны:

– соблюдать конфиденциальность персональных данных;

– обеспечивать безопасность персональных данных при обработке в соответствии с Федеральным законом № 152-ФЗ;

– не делать неучтенных копий на бумажных и электронных носителях;

– не оставлять включенными АРМ (автоматизированное рабочее место),

– после окончания работы (в перерывах) не оставлять материалы с конфиденциальной информацией на рабочих столах. Покидая рабочее место, пользователь обязан убрать документы и электронные носители с конфиденциальной информацией в закрываемые на замок шкафы (сейфы);

– при работе с документами, содержащими персональные данные, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;

– не выносить документы и иные материалы с персональными данными из служебных помещений, предназначенных для работы с ними;

– не вносить изменения в настройку средств защиты информации;

– немедленно сообщать лицу, ответственному за организацию обработки персональных данных, об утрате, утечке или искажении

персональных данных, об обнаружении неучтенных материалов с указанной информацией;

– не допускать действий, способных повлечь утечку персональных данных.

3.2. Лица, допущенные к персональным данным, должны ознакомиться с настоящими правилами под роспись.

3.3. Лица, виновные в нарушении требований настоящих правил и иных документов, регламентирующих вопросы защиты персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
Правилам доступа к персональным данным в
Министерстве труда и социальной политики Республики Тыва

ПЕРЕЧЕНЬ
лиц, допущенных к обработке персональных данных в Министерстве труда и социальной политики Республики Тыва

№ п/п	ФИО	Должность
1.	Куулар Орланмай Дадар-ооловна	Заместитель министра труда и социальной политики Республики Тыва
2.	Монгуш Аяна Кан-ооловна	Начальник отдела экономического планирования и социальных выплат Министерства труда и социальной политики Республики Тыва
3.	Доржу Юлия Дугаржаповна	Начальник отдела правового, кадрового, организационного, документационного обеспечения и контроля
4.	Ооржак Эллада Макаровна	Консультант по кадровым вопросам отдела правового, кадрового, организационного, документационного обеспечения и контроля Министерства труда и социальной политики Республики Тыва
5.	Агбаан Ай-чечек Шолбановна	Юрист отдела правового, кадрового, организационного, документационного обеспечения и контроля Министерства труда и социальной политики Республики Тыва
6.	Иргит Алена Максимовна	Начальник отдела социального обслуживания населения
7.	Кужугет Чечек Юрьевна	Консультант отдела социального обслуживания населения
8.	Киштеек Станислав Олегович	Консультант отдела социального обслуживания населения
9.	Хомушку Анай-Хаак Васильевна	Начальник отдела по вопросам семьи, детей и демографической политики
10.	Дамбар Саяна Николаевна	Консультант отдела по вопросам

		семьи, детей и демографической политики
11.	Ооржак Дайгана Адыгжыевна	Консультант отдела по вопросам семьи, детей и демографической политики
12.	Саая Азияна Уран-ооловна	Начальник отдела содействия занятости населения
13.	Чамзырай Чойгана Валерьевна	Консультант отдела содействия занятости населения
14.	Хомушку Долаана Окал-ооловна	Начальник отдела оплаты труда и трудовых отношений
15.	Хуурак Анжела Хирлиг-ооловна	Консультант отдела оплаты труда и трудовых отношений
16.	Ооржак Шуру Александровна	Консультант отдела оплаты труда и трудовых отношений
17.	Сайн-Белек Айлана Ивановна	Главный специалист отдела оплаты труда и трудовых отношений

Приложение № 9
к приказу №_____ от __.__20__г.

ПОРЯДОК ДОСТУПА СОТРУДНИКОВ В ПОМЕЩЕНИЯ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Настоящий Порядок доступа сотрудников в помещения Министерства труда и социальной политики Республики Тыва (далее – Министерство), в которых ведется обработка персональных данных (далее – ПДн), разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства РФ 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» и другими нормативными правовыми актами.

2. ПДн относятся к конфиденциальной информации. Сотрудники Министерства, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено Федеральным законом.

3. Обеспечение безопасности ПДн от уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн достигается, в том числе установлением правил доступа в помещения, где обрабатываются ПДн в ИС и без использования средств автоматизации.

4. Размещение ИС, в которых обрабатываются ПДн, осуществляется в охраняемых помещениях.

5. Для помещений, в которых обрабатываются ПДн, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ПДн и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

6. При хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

7. В помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации,

допускаются только сотрудники Министерства, уполномоченные на обработку ПДн установленным образом.

8. Ответственными за организацию доступа в помещения Министерства, в которых ведется обработка ПДн, являются руководители структурных подразделений Министерства.

9. Нахождение лиц, не являющихся уполномоченными на обработку ПДн, в помещениях Министерства возможно только в присутствии уполномоченного сотрудника Министерства на время, ограниченное необходимостью решения вопросов, связанных с исполнением функций и (или) осуществлением полномочий структурного подразделения Министерства.

10. Внутренний контроль над соблюдением порядка доступа в помещения, в которых ведется обработка ПДн, проводится лицом, ответственным за обеспечение безопасности ПДн.

Приложение № 1
к Порядку доступа сотрудников в помещения
Министерства труда и социальной политики Республики Тыва,
в которых ведется обработка персональных данных

ПЕРЕЧЕНЬ ЛИЦ, ДОПУЩЕННЫХ В ПОМЕЩЕНИЯ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА, ГДЕ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	ФИО	Должность	Кабинет
1.	Оолак Виктория Викторовна	Начальник отдела по работе с обращениями граждан и документационного обеспечения ГБУ «ЦАХО Минтруда РТ»	101
2.	Сарыглар Долгармаа Аратовна	Главный специалист отдела обращений граждан ГБУ «ЦАХО Минтруда РТ»	101
3.	Монгуш Аяна Кан-ооловна	Начальник отдела экономического планирования, бюджетной отчетности и контроля	103
4.	Агбаан Ай-Чечек Шолбановна	Консультант отдела правового, кадрового, организационного, документационного обеспечения и контроля	104
5.	Середар Ольга Николаевна	Начальник отдела кадрового, организационного, правового обеспечения и контроля ГБУ «ЦАХО Минтруда РТ»	104
6.	Сундуй Оюуна Игорьевна	Главный специалист отдела кадрового, организационного и правового обеспечения и контроля ГБУ «ЦАХО Минтруда РТ»	104
7.	Санаа Милана Орлановна	Ведущий эксперт отдела экономического планирования, бюджетной отчетности и контроля	105
8.	Саныга Вилора Сарыг-ооловна	Главный специалист отдела экономического планирования, бюджетной отчетности и контроля	105
9.	Бадыргы Алдынай чанзановна	Консультант отдела экономического планирования, бюджетной отчетности и контроля	105
10.	Седен Урана Белековна	Главный специалист отдела экономического планирования, бюджетной отчетности и контроля	106

11.	Кара-оол Юлия Родионовна	Консультант отдела экономического планирования, бюджетной отчетности и контроля	106
12.	Доржу Юлия Дугаржаповна	Начальник отдела правового, кадрового, организационного, документационного обеспечения и контроля	107
13.	Ооржак Эллада Макаровна	Консультант по кадровым вопросам отдела правового, кадрового, организационного, документационного обеспечения и контроля	107
14.	Хомушку Анай-Хаак Васильевна	Начальник отдела семейной политики	108
15.	Дамбар Саяна Николаевна	Консультант отдела семейной политики	108
16.	Ооржак Дайгана Адыгжыевна	Консультант отдела семейной политики	108
17.	Тюлюш Сирена Робертовна	Консультант отдела семейной политики	108
18.	Хомушку Долаана Окал-ооловна	Начальник отдела оплаты труда и трудовых отношений	109
19.	Хуурак Анжела Хирлиг-ооловна	Консультант отдела оплаты труда и трудовых отношений	109
20.	Ооржак Шуру Александровна	Консультант отдела оплаты труда и трудовых отношений	109
21.	Донгак Азияна Саян-ооловна	Консультант отдела оплаты труда и трудовых отношений	109
22.	Шаптан Чинчи Хеймер-ооловна	Консультант отдела социального обслуживания населения	110
23.	Артаа Азияна Вячеславовна	Начальник отдела по работе с инвалидами и НКО	110
24.	Аранчын Диана Эдер-ооловна	Консультант отдела социального обслуживания населения	110
25.	Иргит Алена Максимовна	Начальник отдела социального обслуживания населения	111
26.	Кужугет Чечек Юрьевна	Консультант отдела социального обслуживания населения	111
27.	Данзылаар Алеся Геннадьевна	Главный специалист отдела содействия занятости населения	112
28.	Сайн-Белек Айлан Ивановна	Главный специалист отдела анализа и рынка труда	112
29.	Эрелчин Роланда Кангын-ооловна	Начальник отдела содействия занятости населения	114
30.	Саая Азияна Уран-ооловна	Консультант отдела содействия занятости населения	115

31.	Чамзырай Чойгана Валерьевна	Консультант отдела содействия занятости населения	115
32.	Тюлюш Оксана Ак-ооловна	Начальник отдела по организации и сопровождению социальных контрактов	117
33.	Баз-оол Аяна Викторовна	Главный специалист отдела по организации и сопровождению социальных контрактов	117
34.	Монгуш Айлана Григорьевна	Главный специалист отдела по организации и сопровождению социальных контрактов	117
35.	Урангай Людмила Васильевна	Начальник отдела анализа и рынка труда	119
36.	Дотпаа Аржаана Александровна	Главный специалист отдела анализа и рынка труда	119

Приложение № 10
к приказу №_____ от __.__20__ г.

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Общие положения

Настоящие Правила разработаны в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15.09.2008 № 687, и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

Обработка персональных данных, полученных от работника, содержащихся в информационной системе 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.

Документ, содержащий персональные данные – материальный носитель с зафиксированной на нем в любой форме информацией, содержащей персональные данные работников (или граждан в договорах с физическими лицами) в виде текста, фотографии и (или) их сочетания.

Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации:

- 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, в специальных разделах или на полях форм.
- 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.

• Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-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 субъектов Российской Федерации, а также локальными правовыми актами организации.

• При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

• 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, вымарывание).

• 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.

С учетом большого объема (массовости) документов, содержащих персональные данные, и строго регламентированного порядка их хранения пометка конфиденциальности на них не ставится.

С настоящей инструкцией должны быть ознакомлены под роспись работники, допускаемые к обработке персональных данных без использования средств автоматизации. Листы ознакомления хранятся у ответственного за систему защиты информации в информационной системе персональных данных.

2. Порядок обработки персональных данных

Персональные данные должны обособляться от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

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, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Работники, осуществляющие обработку персональных данных, информируются непосредственным начальником (руководителем) о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Типовые формы документов должны быть составлены 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.

Хранение документов, содержащих персональные данные, осуществляется в металлических шкафах или сейфах.

Уничтожение документов, содержащих персональные данные, осуществляется способом, не позволяющим в дальнейшем ознакомиться с персональными данными.

3. Обязанности сотрудника, допущенного к обработке персональных данных

При работе с документами, содержащими персональные данные, сотрудник обязан исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками своего структурного подразделения).

При выносе документов, содержащих персональные данные, за пределы территории лицея по служебной необходимости, сотрудник должен принять все возможные меры, исключающие утрату (утерю, хищение) таких документов.

При утрате (утере, хищении) документов, содержащих персональные данные, работник обязан немедленно доложить о таком факте директору лицея. По каждому такому факту назначается служебное расследование.

4. Сотрудникам, допущенным к обработке персональных данных запрещается

Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.

Делать неучтенные копии документов, содержащих персональные данные.

Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.

Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.

Выносить документы, содержащие персональные данные, из помещений лицея без служебной необходимости.

5. Ответственность

Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений. Контроль за выполнением положений настоящей Инструкции возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ.

В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).

Приложение № 11
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ ПО ОБРАЩЕНИЮ С МАШИННЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1 Общие положения

1.1. Настоящая Инструкция по работе с отчуждаемыми носителями персональных данных в Министерстве труда и социальной политики Республики Тыва (далее – Инструкция) содержит обязательные для всех сотрудников Министерства труда и социальной политики Республики Тыва (далее – Министерство) правила обращения с отчуждаемыми (съемными) носителями, использующимися для записи персональных данных и ключевыми носителями информации.

1.2. Под съемными носителями информации понимаются различные по физической структуре и конструктивному исполнению носители информации, используемые для записи и накопления информации с целью непосредственного ввода её в ЭВМ, обработки и передачи при помощи технических средств.

1.3. Под ключевым носителем информации понимается съемный носитель информации, на который записана уникальная секретная ключевая информация (идентификатор пользователя, закрытый ключ электронной подписи), используемая для подтверждения целостности, подлинности и авторства электронных документов, передаваемых в электронном виде.

1.4. Секретная ключевая информация, находящаяся на ключевом носителе, относится к категории сведений ограниченного распространения.

1.5. Настоящей Инструкцией определяется порядок учета, хранения и обращения со съемными и ключевыми носителями информации (далее – носитель информации) и их утилизации. К съемным носителям информации относятся носители для однократной или многократной записи такие, как CD-R, CD-RW, DVD-R, DVD-RW, USB флеш-накопители, дискеты и т.д.

1.6. Инструкция регламентирует порядок обслуживания и обеспечение безопасности несъемных электронных носителей информации, к которым относятся базы данных на жестких магнитных дисках, содержащие информацию, подлежащую защите.

1.7. Под безопасностью персональных данных на электронных носителях информации понимается сохранение конфиденциальности, исключение несанкционированного проникновения либо иных действий, в том числе не имеющих злого умысла, которые могут привести к потере, искажению, изменению, копированию и другим нежелательным действиям с персональными данными.

1.8. Организационное и техническое обеспечение безопасности конфиденциальной информации, хранящейся на электронных носителях информации во всех информационных системах (далее – ИС) Министерства, с использованием допустимых программно-аппаратных методов защиты, контроль за действиями сотрудников Министерства при работе с указанными носителями информации возлагается на администратора информационной безопасности (далее – администратор ИБ).

1.9. Все находящиеся на хранении и в обращении носители информации конфиденциальной информации подлежат учёту. Каждый носитель информации с записанными на нем защищаемыми данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

1.10. Учет носителей информации осуществляет администратор ИБ.

1.11. При обработке конфиденциальной информации пользователи ИС Министерства должны использовать только специально предназначенные для этого разделы (каталоги) электронных носителей информации или съемные маркированные носители информации.

1.12. При хранении носителей информации должны соблюдаться условия, обеспечивающие сохранность конфиденциальной информации и исключающие несанкционированный доступ к ней.

2 Обязанности работника

2.1. Сотрудник Министерства обязан:

– при получении носителей информации убедиться, что они правильно маркированы, и расписаться в соответствующем журнале;

– сдавать свой персональный ключевой носитель на временное хранение ответственному за обеспечение безопасности персональных данных (далее – ПДн) на время длительного отсутствия на рабочем месте, в период отпуска и болезни и т.п.;

– сдавать свой съемный носитель на временное хранение администратору ИБ на время длительного отсутствия на рабочем месте, в период отпуска и болезни и т.п.;

– в случае утери ключевого носителя немедленно сообщить об этом ответственному за обеспечение безопасности ПДн и принять участие в служебном расследовании факта утери ключевого носителя;

– в случае утери съемного носителя немедленно сообщить об этом администратору ИБ и принять участие в служебном расследовании факта утери съемного носителя;

– в случае перевода на другую работу, увольнения и т.п. сдать по окончании последнего сеанса работы свой носитель информации администратору ИБ и/или

ответственному за обеспечение безопасности ПДн под роспись в соответствующих журналах;

– хранить носитель конфиденциальной информации только в личном сейфе, либо в сейфе уполномоченного сотрудника.

2.2. Сотрудникам Министерства запрещается:

– хранить носители конфиденциальной информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра в незапертом помещении или передавать на хранение другим лицам;

– выносить учтенные носители информации из служебных помещений для работы с ними на дому и т.д.;

– передавать свой носитель информации другим лицам (кроме как для хранения уполномоченному лицу);

– оставлять носитель информации без личного присмотра;

– делать неучтенные копии с носителей информации.

2.3. При отправке или передаче конфиденциальных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

2.4. Вынос съемных носителей, не содержащих ПДн, для непосредственной передачи адресату осуществляется только с письменного разрешения администратора ИБ на основании запроса сторонней организации.

2.5. Вынос съемных носителей ПДн для непосредственной передачи адресату осуществляется только с письменного разрешения ответственного за обеспечение безопасности ПДн в ИС Министерства на основании запроса сторонней организации с обязательной регистрацией в Журнале регистрации запросов на предоставление ПДн.

2.6. Для защиты носителей информации от несанкционированного доступа, использования или повреждения во время транспортировки из одной организации в другую необходимо использовать надежных курьеров и транспорт, а также упаковку, защищающую носители от постороннего вмешательства и позволяющую выявить попытки ее вскрытия.

2.7. О фактах утраты носителей конфиденциальной информации либо разглашения содержащихся на них сведений немедленно ставится в известность руководителя Министерства администратора ИБ и ответственного за обеспечение безопасности ПДн. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета носителей информации.

2.8. Съемные носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей конфиденциальной информации осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по форме (Приложение №1 к настоящей Инструкции).

2.9. При изменении полномочий работника, его увольнения либо компрометации ключевого носителя, уничтожается все ключевая информация и подписывается акт об уничтожения ключевой информации с ключевых носителей (Приложение №2 к настоящей Инструкции).

2.10. Носители, на которые осуществляется резервное копирование защищаемой информации, должны регулярно (не реже одного раза в 6 месяцев) проверяться на отсутствие сбоев уполномоченными сотрудниками.

2.11. При повторном использовании носителей информации предыдущее содержимое должно надежно удаляться администратором информационной безопасности.

2.12. Повседневный и периодический контроль над действиями сотрудников Министерства при работе с носителями информации возлагается на администратора ИБ.

3 Требования по работе с ключевым носителем

3.1. Для получения доступа к защищённым данным, хранящимся в памяти ключевого носителя, требуется ввести PIN-код (Personal Identification Number), являющегося аналогом пароля.

3.2. Пользователь должен выполнять следующие требования:

– изменить PIN-код сразу после получения ключевого носителя (USB-ключ/смарт-карту eToken). PIN-код необходимо хранить в тайне;

– соблюдать требования к ПИН-коду ключевого носителя, к его периодической смене.

3.3. При последовательном вводе более пяти неправильных PIN-кодов ключевой носитель блокируется. Для разблокировки ключевого носителя необходимо обратиться к администратору информационной безопасности.

3.4. В случае утраты ключевого носителя закрытый ключ восстановить невозможно. **Зашифрованная с помощью утерянного закрытого ключа информация восстановлению не подлежит.**

4 Ответственность

4.1. Сотрудник Министерства несет персональную ответственность за сохранность и правильное использование вверенный ему носитель информации.

4.2. За нарушение положений данной Инструкции к сотруднику может быть применена дисциплинарная ответственность, а также ответственность, предусмотренная действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции обращению с машинными носителями персональных данных
Министерства труда и социальной политики Республики Тыва

Акт уничтожения съемных носителей персональных данных

Комиссия в составе:
1. _____,
2. _____,
3. _____
провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
1			
2			
…			

Всего съемных носителей _____
_____.
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации _____
_____
_____
(механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем _____
_____
_____
(разрезания, демонтажа и т.п.).

Председатель комиссии: _____/_____
Члены комиссии: _____/_____
_____/_____

Приложение № 2
к Инструкции обращению с машинными носителями персональных данных
Министерства труда и социальной политики Республики Тыва

Акт уничтожения ключевой информации с ключевых носителей

Проведено уничтожение ключевой информации с ключевых носителей:

Порядковый номер	Регистрационный номер	Вид ключевой информации (Э/Р)

С перечисленных ключевых носителей уничтожена ключевая информация посредством: _____
_____
_____
(программы _____, разрезания, сжигания).

В журнале регистрации ключевых носителей сделаны соответствующие записи.

Пользователь _____ /_____
«___» _____ 20___г.

Администратор
информационной безопасности _____/_____
«___» _____ 20___г.

Приложение №3
к Инструкции обращению с машинными носителями
персональных данных Министерства труда и социальной политики Республики Тыва

ЖУРНАЛ
УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ
В МИНИСТЕРСТВЕ

Журнал начат «____» _____ 20__ г.
Должность
_____/ _____ /
подпись *ФИО*

Журнал завершен «____» _____ 20__ г.
Должность
_____/ _____ /
подпись *ФИО*

Журнал составлен на _____ листах

№ п/п	Рег. №	Дата выдачи/сдачи	Тип носителя	Вид защищаемой информации	ФИО пользователя, получившего носитель	подпись пользователя, получившего носитель	подпись администратора информационной безопасности
1	2	3	4	5	7	8	9

Приложение № 12
к приказу №_____ от __.__20__г.

СПИСОК ЛИЦ, ДОПУЩЕННЫХ К СОДЕРЖАНИЮ ЭЛЕКТРОННОГО ЖУРНАЛА СООБЩЕНИЙ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

К содержанию электронного журнала сообщений допускаются следующие лица:

№ п/п	ФИО	Должность
1.	Мажаа Кудер Керимович	Заместитель директора по информационным технологиям и коммуникациям ГБУ «ЦАХО Минтруда РТ»
2.	Сенги-Доржу Сайын-Белек Саянович	Гл. специалист отдела автоматизации и информационно-технического обеспечения ГБУ «ЦАХО Минтруда РТ»

Приложение № 13
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Общие положения

1.1. Пользователями ИС Министерства, являются сотрудники, допущенные к работе в ИС Министерства, в соответствии с приказом об утверждении списка лиц, которым необходим доступ к защищаемой информации, обрабатываемой в ИС Министерства, для выполнения служебных (трудовых) обязанностей.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в ИС Министерства.

1.3. Пользователем является каждый сотрудник, согласно матрицы доступа, участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

2. Права и обязанности пользователя

2.1. Работники, получившие доступ к защищаемой информации, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки защищаемой информации немедленно информировать администратора информационной безопасности.

2.2. Защищаемая информация не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2.3. В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Министерства, полученные в течение срока работы.

2.4. Пользователь обязан:

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

– знать и соблюдать установленные требования по режиму обработки

защищаемой информации, учету, хранению и пересылке носителей информации, обеспечению безопасности данных, а также руководящих и организационно-распорядительных документов;

– соблюдать требования парольной политики (Инструкция по организации парольной защиты в информационных системах Министерства);

– соблюдать установленную технологию обработки информации;

– руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники (СВТ) и средств защиты информации (СЗИ);

– экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами;

– при отсутствии визуального контроля за рабочим местом: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

– при выходе в течение рабочего дня из помещения, в котором размещается ИС, пользователь обязан:

– блокировать ввод-вывод информации на своем рабочем месте ИС в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИС;

– блокировать вывод информации на монитор рабочих станций.

– немедленно ставить в известность администратора информационной безопасности:

– нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах рабочих станций или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИС;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС.

– обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИС;

– для получения консультаций по вопросам работы и настройке элементов ИС необходимо обращаться к администратору информационной безопасности.

2.5. Пользователю ЗАПРЕЩАЕТСЯ:

– разглашать защищаемую информацию третьим лицам;

– выполнять работы с документами ограниченного распространения на

дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;

– передавать или принимать без расписки документы ограниченного распространения;

– оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;

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

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИС;

– подключать к АРМу нештатные устройства;

– записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);

– отключать (блокировать) средства защиты информации;

– использовать компоненты программного и аппаратного обеспечения ИС подразделения в неслужебных целях;

– обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИС;

– самостоятельно вносить изменения в состав, конфигурацию и размещение ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (ПО), установленного в ИС;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора информационной безопасности;

– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с администратором информационной безопасности;

– принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.6. Пользователь имеет право:

– присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию АРМа, закрепленного за ним;

– обращаться к администратору информационной безопасности с просьбой

об оказании технической и методической помощи по обеспечению безопасности обрабатываемой в ИС Министерства информации, а также по вопросам эксплуатации установленных СЗИ;

– обращаться к системному администратору (СА) с просьбой об оказании технической и методической помощи по использованию установленных программных и технических средств ИС;

– обращаться к ответственному за организацию обработки защищаемой информации по вопросам эксплуатации ИС Министерства (выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты информации).

3. Ответственность

3.1. Пользователь несет персональную ответственность:

– за соблюдение режима безопасности защищаемых данных при их обработке и хранении в ИС Министерства;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС Министерства;

– за соблюдение требований инструкции, нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с защищаемой информацией.

3.2. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

Приложение № 14
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИС Министерства, требования к содержанию паролей, а также контроль за действиями пользователей автоматизированной системы при работе с идентификаторами и персональными паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИС Министерства и контроль за данными действиями возлагается на администратора информационной безопасности Министерства - администратора средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

1.3. Контроль за действиями пользователей ИС Министерства при работе с паролями, соблюдением порядка их смены, хранения и за соответствие паролей требованиям настоящей инструкции возлагается на администратора информационной безопасности.

2. Правила формирования паролей

2.1. Персональные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационных систем самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 6 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abcd и т. д.), общепринятые сокращения (ADMIN, SECRET, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

– использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

– личный пароль пользователь не имеет права сообщать никому;

– новый пароль не должен совпадать с одним из трех предыдущих паролей

– пользователь обязан сохранять в тайне свой личный пароль.

2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

2.3. При технологической необходимости использования учетных данных некоторых сотрудников в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) администратором информационной безопасности по запросу от начальников отдела, в состав которого входит АРМ ИС Министерства, предоставляется одноразовый пароль на данную учетную запись. По возвращению сотрудник обязан сменить персональный пароль на все локальное программное обеспечение.

3. Ввод пароля

3.1. В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля в ИС Министерства определены правила ввода пароля:

- символы вводимого пароля не отображаются на экране в явном виде;
- учёт всех попыток (успешных и неудачных) входа в систему.

3.2. При первоначальном вводе или смене пароля пользователя действуют следующие правила:

- символы вводимого пароля не должны явно отображаться на экране;
- для подтверждения правильности ввода пароля (с учетом первого правила) - ввод пароля необходимо проводить 2 раза.

3.3. Ввод пароля должен осуществляться непосредственно пользователем ИС Министерства (владельцем пароля). Пользователю запрещается передавать пароль для ввода другим лицам. Передача пароля для ввода другим лицам является разглашением конфиденциальной информации и влечёт за собой ответственность согласно положениям данной Инструкции и в соответствии с действующим законодательством Российской Федерации.

3.4. Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь ИС Министерства должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPS LOCK (если это необходимо), а также проконтролировать

расположение клавиатуры (клавиатура должна располагаться таким образом, чтобы исключить возможность увидеть набираемый текст посторонними).

3.5. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

4. Порядок смены личных паролей

4.1. Полная плановая смена паролей проводится регулярно, не реже одного раза в квартал.

4.2. При смене пароля администратором безопасности производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя – предъявления стороннего идентификатора.

4.3. Внеплановая смена персонального пароля или удаление учетной записи пользователя ИС Министерства в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.4. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и т.д.) администратора информационной безопасности и других сотрудников, которым для выполнения их должностных обязанностей были предоставлены полномочия по управлению парольной защитой ИС Министерства.

4.5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

4.6. Сотрудники, имеющие доступ к ИС Министерства, в течение 3-х часов после смены своих паролей должны передать их новые значения вместе с именами соответствующих учетных записей в запечатанном конверте администратору информационной безопасности на хранение. При получении конверта с новыми паролями конверт со старыми паролями уничтожается.

4.7. Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться администратором информационной безопасности с момента получения письменного уведомления из отдела государственной службы и кадров Министерства.

4.8. Удаление учетных записей пользователей, уволенных, переведенных в другое структурное подразделение, филиал, региональный центр должно производиться администратором информационной безопасности немедленно с

момента получения письменного уведомления из отдела государственной службы и кадров Министерства.

4.9. Отдел государственной службы и кадров Министерства должен известить администратора информационной безопасности о состоявшемся приказе в течение 24 часов после увольнения, перевода сотрудника в другое структурное подразделение, филиал, региональный центр.

5. Хранение пароля

5.1. Хранение сотрудником зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе администратора информационной безопасности.

5.2. При возникновении производственной необходимости в срочном доступе в автоматизированную систему временно отсутствующего пользователя разрешается произвести смену пароля пользователя его непосредственным руководителем. При этом должен быть составлен акт о вскрытии конверта с паролем и о его повторном опечатывании с новым паролем.

5.3. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.4. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

6.1. В случае возникновения необходимости в смене пароля в виду компрометации пользователь должен:

- немедленно сменить свой пароль;
- известить администратора информационной безопасности.

6.2. В случае компрометации (утеря, передача парольной информации) персонального пароля пользователя ИС Министерства должны быть немедленно предприняты меры в соответствии с п. 4.3 или п.4.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.2. Ответственность за организацию парольной защиты в Министерстве возлагается на администратора информационной безопасности.

Приложение № 15
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ИС МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты ИС Министерства труда и социальной политики Республики Тыва от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Министерства труда и социальной политики Республики Тыва, эксплуатирующих и сопровождающих ИС, за выполнение требований настоящей Инструкции.

1.2. Для обеспечения информационной безопасности к использованию в ИС Министерства труда и социальной политики Республики Тыва допускаются только лицензионные и сертифицированные ФСТЭК России и (или) ФСБ России антивирусные средства, закупленные у официальных разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля, контроль за состоянием антивирусной защиты в ИС Министерства труда и социальной политики Республики Тыва осуществляется администратором информационной безопасности, в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. После установки и настройки средств антивирусного контроля администратором информационной безопасности в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

1.5. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

1.6. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИС Министерства труда и социальной политики Республики Тыва и своевременное информирование администратора информационной безопасности в случае обнаружения действий вредоносных программ возлагается на сотрудников Министерства труда и социальной политики Республики Тыва.

2. Применение средств антивирусного контроля

2.1. ИС Министерства труда и социальной политики Республики Тыва подлежат обязательному антивирусному контролю, а также любая на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

2.2. Антивирусный контроль ИС Министерства труда и социальной политики Республики Тыва должен проводиться ежедневно в автоматическом режиме при начальной загрузке автоматизированного рабочего места (АРМ).

2.3. Настройка средств антивирусной защиты должна реализовывать следующие функции:

– непрерывный автоматический мониторинг информационного обмена в ИС с целью выявления программно-математического воздействия (далее – ПМВ);

– автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИС всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

– реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

– автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы;

– полная автоматическая проверка носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;

– регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты. Для чего администратором информационной безопасности необходимо один раз в неделю осуществлять установку пакетов обновлений вирусных баз, контроль их подключения к антивирусному пакету и осуществлять проверку АРМ на наличие вирусов;

– автоматическое документирование состояния системы антивирусной защиты ИС.

2.4. Пользователи ИС Министерства труда и социальной политики Республики Тыва при работе со съемными носителями информации (flash-накопители, дискеты 3,5”, CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ выполнив следующие действия:

- Подключить съемный носитель информации.
- Открыть значок Рабочего стола «Мой компьютер».
- Установить курсор мыши на имя выбранного носителя.
- По правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

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

2.6. Установка (изменение) системного и прикладного программного обеспечения должна осуществляться только в присутствии администратора информационной безопасности. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) системного программного обеспечения должна проводиться антивирусная проверка. В ИС Министерства труда и социальной политики Республики Тыва запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

2.7. При возникновении подозрения на наличие в системе компьютерного вируса, (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) сотрудником Министерства труда и социальной политики Республики Тыва должен быть проведён внеочередной антивирусный контроль рабочей станции (самостоятельно или вместе с администратором информационной безопасности). Для проведения контроля должны использоваться актуальные версии антивирусных сканеров (cureit, avz и др.), запускаемых без установки в системе

2.8. В случае обнаружения при проведении антивирусной проверки наличия в системе компьютерного вируса сотрудники Министерства труда и социальной политики Республики Тыва обязаны:

– немедленно поставить в известность администратора информационной безопасности и прекратить какие-либо действия на персональном компьютере приостановить работу;

– поставить в известность владельца зараженных файлов.

2.9. В случае обнаружения наличия в системе компьютерного вируса необходимо:

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

– провести локализацию вируса в системе;

– обеспечить удаление вируса из системы;

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, необходимо направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

– по факту обнаружения вируса должна быть составлена служебная записка администратору информационной безопасности, в которой требуется указать

предположительный источник (отправителя, владельца и т.д.) вируса, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Пользователю ИС Министерства труда и социальной политики Республики Тыва запрещается:

– использовать на СВТ съемные носители информации без предварительной проверки установленными средствами антивирусной защиты.

Пользователь обязан:

– ежедневно при начальной загрузке АРМ убедиться в наличии резидентного антивирусного монитора и в случае его отсутствия уведомить об этом администратора информационной безопасности;

– самостоятельно запускать внеплановую антивирусную проверку АРМ при получении уведомления о наличии в системе вируса, а также при возникновении подозрения на наличие вируса.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в ИС Министерства труда и социальной политики Республики Тыва, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех сотрудников, являющихся пользователями ИС Министерства труда и социальной политики Республики Тыва.

3.3. Периодический контроль за состоянием антивирусной защиты в ИС Министерства труда и социальной политики Республики Тыва, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками Министерства труда и социальной политики Республики Тыва осуществляется администратором информационной безопасности.

3.4. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора информационной безопасности.

3.5. Сотрудники Министерства труда и социальной политики Республики Тыва, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение № 16
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ
по выявлению инцидентов и реагированию на них в информационных системах Министерства труда и социальной политики Республики Тыва

1 Общие положения

1.1. Настоящая Инструкция по выявлению инцидентов и реагированию на них в информационных системах Министерства труда и социальной политики Республики Тыва (далее – Инструкция) разработана в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

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

– Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

1.2. Настоящая Инструкция регламентирует организационные и технические вопросы по выявлению инцидентов и реагированию на них в информационных системах (далее – ИС) Министерства труда и социальной политики Республики Тыва (далее – Министерство).

1.3. Настоящая Инструкция применяется для ИС и средств, которые обеспечивают безопасность информации (при ее автоматизированной обработке).

1.4. Цель настоящей Инструкции – выявление инцидентов и реагирование на них, распределение обязанностей и ответственности участвующих в процессе выявления инцидентов и реагированию на них.

1.5. Инцидентом называется событие (или группа событий), которое может привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации (далее – инцидент). Инцидентом, в общем случае, называется любое нарушение инструкций и приказов.

1.6. Требования настоящей инструкции обязательны для выполнения всеми пользователями ИС и администратором информационной безопасности (далее – администратор ИБ).

2 Выявление инцидентов информационной безопасности

2.1. Инциденты затрагивают следующие свойства информации:

– нарушение конфиденциальности;

– нарушение целостности;

– нарушение доступности.

Инциденты могут преследовать нарушение дополнительных (производных) свойств информации:

– нарушение надежности;

– нарушение достоверности;

– нарушение принципа неотказуемости.

2.2. Основными источниками информации об инцидентах являются:

– факты, выявленные администратором ИБ, а также другими сотрудниками организации;

– результаты работы средств мониторинга информационной безопасности, результаты проверок и аудита (внутреннего или внешнего);

– обращения субъектов информации с указанием инцидента;

– другие источники информации.

2.3. Пользователь ИС может выявить признаки наличия инцидента путем анализа текущей ситуации на предмет ее соответствия. Выявленные несоответствия дают основания предполагать факт возникновения инцидента. Любые сведения о происшествие или об инциденте должны быть незамедлительно переданы выявившим их сотрудником администратору ИБ любым доступным способом.

3 Регламент выявления инцидентов

3.1. Администратор ИБ проводит сканирование сети 1 раз в месяц с помощью ПИ «Сетевой сканер безопасности XSpider» или иным средством анализа защищенности, сертифицированным ФСТЭК России.

3.2. После проведения сканирования все отчеты сохраняются в pdf формате и проводятся мероприятия по исключению выявленных уязвимостей.

3.3. В процессе анализа администратор ИБ проводит проверку наличия в выявленном факте нарушений. Если были выявлены нарушения и уязвимости, то делается соответствующая запись в журнале реагирования на инциденты информационной безопасности, заполняется Карточка данных об инциденте, в противном случае записи не производятся.

3.4. В случае наличия признаков инцидента в полученной информации, администратор ИБ определяет предварительную степень важности инцидента и принимает решение о необходимости проведения разбирательства.

3.5. В срок не более трех рабочих дней с момента поступления информации об инциденте администратор ИБ определяет и инициирует первоочередные меры,

направленные на локализацию инцидента и на минимизацию его последствий, после чего заполняется Разрешение инцидента.

3.6. В случае возникновения инцидента, повлекшего неправомерную передачу (предоставление, распространение, доступ) персональных данных Оператор в течение 24 часов с момента обнаружения направляет информацию об этом инциденте в национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) путем заполнения уведомления на сайте Роскомнадзора.

4 Разбирательство инцидента информационной безопасности

4.1. Целями разбирательства инцидентов являются:

– выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

– обеспечение безопасности информации в ИС;

– предотвращение несанкционированного доступа к информации и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.2. Разбирательство инцидента состоит из следующих этапов:

– подтверждение/опровержение факта возникновения инцидента;

– подтверждение/корректировка уровня значимости инцидента;

– уточнение дополнительных обстоятельств (деталей) инцидента;

– получение (сбор) доказательств возникновения инцидента, обеспечение их сохранности и целостности;

– минимизация последствий инцидента;

– информирование и консультирование сотрудников по действиям обнаружения, устранения последствий и предотвращения инцидентов;

– разработка мероприятий по обнаружению и/или предупреждению инцидентов.

4.3. В процессе проведения разбирательства инцидента обязательными для установления являются:

– дата и время совершения инцидента;

– ФИО, должность нарушителя;

– уровень критичности инцидента;

– обстоятельства и мотивы совершения инцидента;

– информационные ресурсы, затронутые инцидентом;

– характер и размер реального и потенциального ущерба;

– обстоятельства, способствовавшие совершению инцидента.

4.4. После получения необходимой информации по инциденту администратор ИБ проводит анализ полученных данных.

5 Завершение разбирательства, превентивные мероприятия

5.1. По окончании разбирательства инцидента осуществляющий разбирательство сотрудник Министерства передает имеющиеся материалы (в объеме, достаточном для принятия решения) вышестоящему руководителю для решения вопроса о целесообразности привлечения нарушителя к дисциплинарной ответственности.

5.2. В случае инцидента, повлекшего неправомерную передачу (предоставление, распространение, доступ) персональных данных Оператор в течение 72 часов с момента обнаружения направляет информацию о результатах внутреннего расследования путем заполнения уведомления на сайте Роскомнадзора.

5.3. На основании полученных результатов разбирательства руководитель в срок не более трех рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем, включающих:

– повторное ознакомление нарушителя с инструкциями;

– анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя;

– доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов;

– обсуждение инцидента;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к информации и (или) передачи их лицам, не имеющим права доступа к такой информации;

– другие обоснованные мероприятия.

5.4. О результатах проведенного разбирательства инцидента администратор ИБ по необходимости инициирует подготовку сообщения об инциденте на имя руководителя.

6 Права, обязанности и ответственности участников разбирательства

6.1. Администратор ИБ имеет право:

– по согласованию с непосредственным руководителем нарушителя требовать предоставлений письменных объяснений по обстоятельствам инцидента у нарушителя;

– запрашивать и получать устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента;

– инициировать процедуры привлечения нарушителя к дисциплинарной/материальной ответственности.

6.2. Администратор ИБ обязан:

– объективно и основательно проводить разбирательство каждого инцидента;

– определять первоочередные меры, направленные на локализацию инцидента и минимизацию негативных последствий;

– проводить анализ обстоятельств, способствовавших совершению каждого инцидента, и на его основе, разрабатывать рекомендации по снижению ущерба от подобных инцидентов и минимизации возможности их повторения в будущем.

6.3. Руководители и сотрудники обязаны:

– предоставлять по запросам проводящего разбирательство сотрудника устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента;

– информировать администратора ИБ о выявленных инцидентах.

Приложение № 1
к Инструкции по выявлению инцидентов
и реагированию на них в информационных системах
Министерства

Карточка данных об инциденте безопасности обработки персональных данных в информационных системах Министерства труда и социальной политики Республики Тыва

Дата события			
Номер события[1)]:		(Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:	
Информация о сообщающем лице			
Фамилия		Адрес	
Управление			
Телефон		Электронная почта	
Описание события			
Описание события:			
• Что произошло			
• Как произошло			
• Почему произошло			
• Пораженные компоненты			
• Негативное воздействие на Организацию			
• Любые идентифицированные уязвимости			
Детали события			
Дата и время возникновения события			
Дата и время обнаружения события			
Дата и время сообщения о событии			
Закончилось ли событие? *(отметить квадрат)*	Да □	Нет □	
Если «да», то уточнить, как долго длилось событие в днях/часах/минутах			

[1)] (Номера событий назначаются ответственным за выявление и реагирование на инциденты безопасности обработки информации в ИС)

Дата инцидента			
Номер инцидента[2)]:		(Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:	
Информация об администраторе ИБ			
Фамилия		Адрес	
Телефон		Электронная почта	
Информация об ответственном за выявление и реагирование на инциденты безопасности обработки персональных данных в ИС			
Фамилия		Адрес	
Телефон		Электронная почта	
Описание инцидента безопасности обработки персональных данных в ИС			
Дальнейшее описание инцидента:			
• Что произошло			
• Как произошло			
• Почему произошло			
• Пораженные компоненты			
• Негативное воздействие на Организацию			
• Любые идентифицированные уязвимости			
Детали инцидента безопасности обработки персональных данных в ИС			
Дата и время возникновения инцидента			
Дата и время обнаружения инцидента			
Дата и время сообщения об инциденте			
Закончился ли инцидент? *(отметить квадрат)*	Да ☐	Нет ☐	
Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится			

[2)] (Номера инцидентов назначаются ответственным за выявление и реагирование на инциденты безопасности обработки информации в ИС)

Разрешение инцидента					
Дата начала расследования инцидента					
Фамилия лица (лиц), проводившего (их) расследование инцидента					
Дата окончания инцидента					
Дата окончания воздействия					
Дата завершения расследования инцидента					
Ссылка и место хранения отчета о расследовании					
Причастные лица					
(Один из)	Лицо (PE)	☐	Легально учрежденная организация/учреждение (OI)	☐	
Организованная группа (GR)		☐	Случайность (AC)	☐	
			Нет виновного (NP) *Например, природные факторы, отказ оборудования, ошибка человека*	☐	
Описание нарушителя					
Действительная или предполагаемая мотивация					
(Один из)	Криминальная/финансовая выгода(CG)	☐	Развлечение/хакерство (PH)	☐	
Политика/Терроризм (PT)		☐	Месть (RE)	☐	
			Другие мотивы (OM)	☐	
			Определить:		
Действия, предпринятые для разрешения инцидента					
(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением…»)					
Действия, запланированные для разрешения инцидента					
(например, см. выше)					
Прочие действия					
(например, по-прежнему требуется проведение расследования для другого персонала)					

Приложение № 2
к Инструкции по выявлению инцидентов
и реагированию на них в информационных системах
Министерства

ЖУРНАЛ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

№ п/п	Краткое описание инцидента	ФИО сотрудника, обнаружившего инцидент,	Дата и время пресечения	Дата, время доведения информации об инциденте	Подпись администратора ИБ

		должность, дата и время обнаружения	несанкционированного воздействия	администратору ИБ, ФИО и должность администратора ИБ	
1.					

Приложение № 3
к Инструкции по выявлению инцидентов
и реагированию на них в информационных системах
Министерства

ПЛАН
практических занятий и тренировок с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты

Мероприятие	Срок выполнения	Примечание
Проведение практических занятий и тренировок с персоналом информационных систем по блокированию угроз безопасности информации и реагированию на инциденты	Постоянно	Мероприятие проводится не реже одного раза в два года

Приложение № 17
к приказу №_____ от __.__20__г.

ПРАВИЛА

управления конфигурацией информационной системы и системы защиты информации информационной системы

1 Общие положения

Правила управления конфигурацией информационной системы и системы защиты информации информационной системы (далее – ИС) Министерства труда и социальной политики Республики Тыва (далее – Министерство) определяют общие функции, ответственность, права и обязанности ответственных за управление конфигурацией лиц.

2 Объекты управления конфигурацией

Объектами управления конфигурацией являются:

– технические средства ИС, осуществляющие обработку информации (СВТ, компоненты ЛВС, средства и системы передачи, приема и обработки информации);

– программные средства (ОС, общесистемное и прикладное ПО);

– СЗИ;

– ВТСС, их коммуникации, средства и системы передачи данных, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, не предназначенные для обработки информации, но размещенные в помещениях, в которых расположены технические средства ИС;

– информационные технологии.

3 Управление изменениями

Действия по внесению изменений в конфигурацию ИС Министерства и систему защиты ИС Министерства разрешены следующим лицам:

– Администратор ИС;

– Администратор безопасности;

Все изменения в конфигурации ИС Министерства и системы защиты ИС необходимо согласовывать с администратором безопасности.

Перед внесением изменений в конфигурацию ИС, способных привести к нарушению конфиденциальности, целостности или доступности значимых объектов, должна производиться оценка возможных последствий от таких изменений. Внесение изменений возможно только в случае, если такие изменения не приведут к отказу ИС и/или нарушению информационной безопасности.

4 Установка (инсталляция) только разрешенного к использованию программного обеспечения и его компонентов

Установка (инсталляция) в ИС Министерства программного обеспечения и (или) его компонентов осуществляется от имени администратора с учетом Перечня программного обеспечения, разрешенного к использованию в ИС Министерства.

5 Контроль действий по внесению изменений

Администратор безопасности осуществляет мониторинг изменений конфигурации ИС с целью подтверждения защищённости после внесения изменений в конфигурацию и анализа их эффективности. Пользователям ИС не допускается вносить изменения в конфигурацию ИС самостоятельно (устанавливать новое, удалять или изменять настройки имеющегося ПО, устанавливать новые ТС, отключать средства обеспечения ИБ и т.п.).

6 Ответственность

Каждый работник, имеющий доступ в ИС, несёт персональную ответственность за обеспечение ИБ в соответствии с требованиями настоящих Правил. Лица, нарушившие требования безопасности могут быть привлечены к дисциплинарной или административной ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение № 18
к приказу №_____ от __.__20__г.

ПРАВИЛА

контроля и мониторинга за обеспечением уровня защищенности информации, содержащейся в информационных системах Министерства труда и социальной политики Республики Тыва

1. Контроль состояния информационной безопасности является неотъемлемой составной частью работ по поддержанию требуемого режима защиты ИС.

2. Контроль состояния информационной безопасности в ходе эксплуатации объектов информатизации проводится с определённой периодичностью (не реже чем раз в три года), с целью подтверждения сохранения защитных функций и проверки выполнения пользователями объектов информатизации и ответственными лицами структурного подразделения министерства, ответственное за обеспечение безопасности ПДн при их обработке в ИС.

3. Контроль проводится также в случаях нарушения информационной безопасности с целью определения причин произошедших нарушений и выработке мер по противодействию повторным нарушениям информационной безопасности.

4. Основными задачами контроля (аудита) являются:

– проверка соответствия системы обеспечения информационной безопасности требованиям действующего законодательства, стандартов, положениям локальных нормативных актов;

– проверка соответствия организации работ по обеспечению информационной безопасности требованиям установленного режима защиты ИС;

– оценка обоснованности принимаемых мер защиты информации и соответствия их установленным требованиям информационной безопасности;

– проверка своевременности и полноты выполнения сотрудниками требований законодательства и локальных нормативных актов по обеспечению информационной безопасности.

5. Для реагирования на события безопасности в ИС должны осуществляться централизованный сбор, запись, хранение, мониторинг и корреляция информации о событиях безопасности.

6. События безопасности, подлежащие регистрации в ИС, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС.

7. Подлежат регистрации события безопасности, связанные с применением

выбранных мер по защите информации в ИС.

8. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется администратором информационной системы, исходя из возможностей реализации угроз безопасности информации, и фиксируется в журнале учета мероприятий по контролю режима защиты конфиденциальной информации (ПДн) и выполнения обязательных процедур.

9. Сбор, запись и хранение информации о событиях безопасности должен предусматривать:

– возможность выбора администратором безопасности информации событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности;

– генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);

– хранение информации о событиях безопасности.

10. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учётом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

11. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

– предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (ёмкости) памяти) при регистрации событий безопасности;

– реагирование на сбои при регистрации событий безопасности путём изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

12. Администратор безопасности информации осуществляет мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирует на них. Мониторинг (просмотр и анализ) записей регистрации (аудита) проводиться для всех событий, подлежащих регистрации, и с периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности в ИС. В случае выявления признаков событий безопасности в ИС осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

13. Информация о событиях безопасности подлежит защите и

обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

14. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору безопасности.

Приложение 1
к Правилам контроля и мониторинга
за обеспечением уровня защищенности информации,
содержащейся в информационных системах
Министерства труда и социальной политики
Республики Тыва

Лист ознакомления

с Правилами контроля и мониторинга за обеспечением уровня защищенности информации, содержащейся в информационных системах Министерства труда и социальной политики Республики Тыва

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Приложение № 19
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ

по защите информации при выводе из эксплуатации информационной системы или об окончании обработки информации

1. Общие положения

1.1. Настоящая инструкция определяет перечень мероприятий по защите информации при выводе из эксплуатации информационных систем Министерства труда и социальной политики Республики Тыва (далее – ИС Министерства).

2. Выявление, анализ и устранение уязвимостей информационной системы

2.1. Обеспечение защиты информации при выводе из эксплуатации ИС Министерства осуществляется в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

– архивирование информации, содержащейся в информационной системе;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.2. Процедуры вывода из эксплуатации должны быть документированы.

Приложение № 20
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ

по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах Министерства труда и социальной политики Республики Тыва

1. Общие положения

1.1. Настоящая инструкция по резервированию и восстановлению работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ) разработан с целью обеспечения возможности незамедлительного восстановления защищаемых данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Данный документ:

– определяет правила и объемы резервирования, а также порядок восстановления работоспособности Министерства труда и социальной политики Республики Тыва;

– предназначен для исполнения сотрудником, в обязанности которого входит техническое обслуживание ИС Министерства труда и социальной политики Республики Тыва (далее – администратор), а так же сотрудников Министерства труда и социальной политики Республики Тыва, участвующих в обработке защищаемых данных (ЗД) в ИС (далее – пользователи);

– описывает действия администратора и пользователей по обеспечению резервного копирования и восстановления ЗД, обрабатываемых в ИС Министерства труда и социальной политики Республики Тыва.

1.3. Носители информации, используемые для резервирования защищаемой информации ИС Министерства труда и социальной политики Республики Тыва, подлежат защите в той же степени, что и резервируемая информация.

1.4. Контроль за исполнением настоящего порядка осуществляет администратор информационной безопасности в Министерства труда и социальной политики Республики Тыва.

2. Назначение и область действия

2.1. Резервируемой информацией следует считать любые защищаемые данные в электронном виде. Резервируемая информация разделяется по способу обработки (по способу хранения) на две категории:

– обработка (хранение) в базе данных;

– любом другом виде.

2.2. Резервному копированию подлежат все информационные ресурсы ИС Министерства труда и социальной политики Республики Тыва, содержащие защищаемую информацию, а именно:

– файлы баз данных;

– электронные документы;

– файлы сообщений электронной почты;

– отсканированные и хранящиеся в ИС Министерства труда и социальной политики Республики Тыва изображения документов и фотографии субъектов.

2.3. Резервному копированию могут так же подвергаться:

– системное и прикладное программное обеспечение ИС Министерства труда и социальной политики Республики Тыва;

– средства защиты информации.

3. Порядок резервирования

3.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых защищаемых данных - не реже одного раза в месяц;

– для технологической информации - не реже раза в два месяца;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС Министерства труда и социальной политики Республики Тыва - не реже раза в квартал, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2. Резервирование защищаемых информационных ресурсов ИС Министерства труда и социальной политики Республики Тыва, не содержащих персональные данные, выполняется администратором информационной безопасности.

3.3. Определяется 2 вида резервирования данных:

– полное резервирование данных – резервное копирование всех защищаемых данных, хранящихся в ИС Министерства труда и социальной политики Республики Тыва;

– неполное резервирование данных – резервное копирование части защищаемых данных, хранящихся в ИС Министерства труда и социальной политики Республики Тыва.

3.4. Целью неполного резервирования является сохранение изменений в ИС Министерства труда и социальной политики Республики Тыва с момента полного резервирования защищаемых данных.

3.5. Резервирование ЗД осуществляется в автоматическом режиме на локальном дисковом массиве сервера.

3.6. Резервное копирование баз данных выполняется ежедневно в конце рабочего дня ответственным специалистом на учтенный съемный носитель информации.

3.7. Восстановление файлов ИС Министерства труда и социальной политики Республики Тыва производится путем разархивирования файлов базы данных в исходный каталог.

3.8. Необходимо регулярно периодичностью один раз в квартал создавать резервные копии путем копирования информации на зарегистрированный отчуждаемый носитель информации.

3.9. Периодичность проведения работ по резервированию защищаемой информации определяется администратором информационной безопасности с учётом специфики работы ИС Министерства труда и социальной политики Республики Тыва, но не менее 1 раза в квартал для полного резервирования и 1 раза в месяц для неполного резервирования.

3.10. В случаях, когда защищаемые ресурсы хранятся на компьютерах пользователей локально, допустимо перекладывать ответственность за проведение неполного резервирования данных на пользователей ИС Министерства труда и социальной политики Республики Тыва.

3.11. События резервирования защищаемых данных фиксируются в Журнале резервирования информационных ресурсов ИС Министерства труда и социальной политики Республики Тыва. В журнале указывается: дата, вид резервирования, наименование резервируемого информационного ресурса, количество и общий размер файлов, серийный номер носителя информации, ответственное лицо.

3.12. Администратор ИС Министерства труда и социальной политики Республики Тыва использует средства резервного копирования ИС для резервирования данных на отчуждаемый носитель. В случаях, когда резервирование данных средствами ИС не представляется возможным, администратором информационной безопасности может использовать средство резервного копирования, не входящее в состав ИС Министерства труда и социальной политики Республики Тыва.

3.13. Администратор не имеет право ознакомиться с резервируемыми защищаемыми данными. Факт ознакомления администратора с резервируемыми защищаемыми данными может быть расценён как превышение служебных

полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных Правонарушениях Российской Федерации.

3.14. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.15. Носители должны храниться не менее года, для возможности восстановления данных.

3.16. В случае удаления ЗД субъекта из ИС Министерства труда и социальной политики Республики Тыва должна быть так же удалена резервная копия этих данных.

4. Порядок хранения резервных копий

4.1. Хранение резервных копий ЗД должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

4.2. Хранение носителей резервных копий защищаемой информации должно быть организовано в сейфе или несгораемом, металлических шкафу с устройством опечатывания у администратора информационной безопасности.

4.3. Доступ к местам хранения резервных копий должен быть предоставлен только администратору информационной безопасности.

4.4. На носителе информации, содержащем резервные копии ЗД, не должна храниться посторонняя информация.

5. Порядок восстановления информации после сбоя

5.1. При искажении, модификации, блокировании, удалении ЗД необходимо руководствоваться следующим порядком восстановления.

– в случае возникновения инцидента информационной безопасности, связанного с ЗД, следует незамедлительно сообщить об этом администратору;

– ответственным за восстановление ЗД из резервных копий является администратор, начальник подразделения, в котором произошел инцидент и/или администратор информационной безопасности;

– администратор обязан срочно уведомить администратора информационной безопасности в ИС Министерства труда и социальной политики Республики Тыва о факте сбоя в работе ИС, повлёкшего нарушение целостности ЗД;

– администратор должен оценить причину возникновения неисправности и принять меры по устранению технических неисправностей при неполадках программного или аппаратного обеспечения компьютера, или воспользоваться резервной копией при проблемах, связанных непосредственно с ЗД;

– факты восстановления ЗД должны фиксироваться в Журнале резервирования информационных ресурсов ИС Министерства труда и социальной политики Республики Тыва (в графе «вид резервирования» указывается «полное восстановление» либо «частичное восстановление»).

Приложение №1
к Инструкции по резервированию и восстановлению работоспособности
технических средств и программного обеспечения, баз данных
и средств защиты информации в информационных системах
Министерства труда и социальной политики Республики Тыва

ЖУРНАЛ РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/_____/
подпись ФИО
Журнал завершен «____» _____ 20___ г.
Должность _____
_____/_____/
подпись ФИО
Журнал составлен на _____ листах

№ п/п	Дата	Вид резервирования (полное, частичное)	Наименование резервируемого информационного ресурса	Количество (общий размер файлов)	Тип носителя	Серийный номер носителя информации	Ответственное лицо	Примечание
1.								

Приложение № 21
к приказу №_____ от __.__20__г.

ПОРЯДОК

контроля выполнения мероприятий по защите информации в информационных системах Министерства труда и социальной политики Республики Тыва

1. Общие положения

Настоящий порядок регламентирует порядок и сроки проведения мероприятий по обеспечению защите информации в информационных системах (далее - ИС) Министерства труда и социальной политики Республики Тыва.

2. **Контроль выполнения мероприятий по защите информации**

Выполнение мероприятий по защите информации проводится в соответствии с Планом мероприятий по защите информации. Сведения о выполнении мероприятий заносятся в «Журнал проведения мероприятий по защите информации в Министерстве труда и социальной политики Республики Тыва.

В ходе контроля выполнения мероприятий по защите информации осуществляется проверка соответствия проводимых мероприятий утвержденному плану.

Приложение № 1
к Порядку контроля выполнения мероприятий
по защите информации в информационных системах Министерства труда и социальной политики Республики Тыва

ПЛАН

мероприятий по защите персональных данных

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Выявление УБПДН и определение нарушителей безопасности информации	Перед созданием системы защиты и при необходимости	Разрабатывается (либо актуализируется) Модель угроз безопасности и модель нарушителя безопасности информации
2.	Определение требуемого уровня защищенности ПДн	Перед созданием системы защиты и при необходимости	Определение требуемого уровня защищенности ПДн проводится при создании ИС ПДн, при выявлении новых обрабатываемых ПДн, при изменении состава, структуры самой ИС ПДн или технических особенностей ее построения (при изменении программного обеспечения, топологии и прочего)
3.	Проектирование системы защиты ИС ПДн	До ввода в эксплуатацию и при необходимости	Разработка Проекта на систему защиты. Выбор мер по защите ПДн проводится исходя из уровня защищенности ПДн ИС ПДн и УБПДН, включенных в Модель угроз безопасности, а также с учетом структурно-функциональных характеристик ИС ПДн (проводится совместно с лицензиатом ФСТЭК России)
4.	Документальное регламентирование работы с информацией	До ввода в эксплуатацию и при необходимости	Назначение приказами ответственного за обработку и защиту ПДн, разработка положения по обработке ПДн, инструкций для ответственных лиц по обработке и защите ПДн, либо внесение изменений в существующую организационно-распорядительную документацию

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
5.	Получение Министерством письменного согласия субъектов ПДн (физических лиц) на обработку ПДн	Постоянно	Письменное согласие получается при передаче ПДн субъектами ПДн Министерства для обработки в ИС. Форма согласия утверждается Положением об обработке ПДн
6.	Ограничение доступа сотрудников Министерства к ПДн	До ввода в эксплуатацию и при необходимости	В случае изменения структуры ИС необходимо разграничивать доступ сотрудников Министерства к персональным данным субъектов ПДн (сотрудники наделяются минимальными полномочиями доступа, необходимыми для выполнения ими своих обязанностей, например, могут иметь права только на просмотр ПДн)
7.	Реализация мер по обеспечению безопасности информации, определенных на этапе проектирования системы защиты	До ввода в эксплуатацию и при необходимости	Разработка и утверждение эксплуатационной документации на систему защиты. Закупка и внедрение сертифицированных СЗИ
8.	Направление в уполномоченный орган (Роскомнадзор) уведомления о своем намерении осуществлять обработку ПДн с использованием средств автоматизации	При необходимости	Уведомление направляется при вводе в эксплуатацию новых ИС Министерства, либо при внесении изменений в существующие ИС
9.	Аттестация ИС по требованиям безопасности информации	Один раз в три года или при необходимости	Проводится совместно с лицензиатами ФСТЭК России
10.	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	Один раз в три года или при необходимости	Проводится оператором самостоятельно или с привлечением лицензиатов ФСТЭК России
11.	Оформление правового основания обработки Информации	При вводе ИС в эксплуатацию	При вводе ИС в эксплуатацию оформляется приказ о вводе ее в эксплуатацию

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
12.	Повышение квалификации сотрудников в области защиты информации	Постоянно	Ответственный за обработку и защиту информации должен повышать квалификацию не менее одного раза в два года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обработку и защиту информации)
13.	Внутренний контроль соответствия обработки ПДн законодательству Российской Федерации, требованиям к защите ПДн, политике Министерства в отношении обработки ПДн, локальным актам Министерства	Постоянно	Проводится с целью выявления и устранения неправомерных действий с информацией
14.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью контроля обработки информации в ИС
15.	Пересмотр перечня лиц, имеющих доступ в помещения, в которых ведется обработка Информации и расположены средства криптографической защиты информации, и к Информации	Раз в три месяца	Проводится с целью поддержания указанного перечня в актуальном состоянии

Приложение № 2
к Порядку контроля выполнения мероприятий
по защите информации в информационных системах
Министерства труда и социальной политики Республики Тыва

ФОРМА

ЖУРНАЛ №____

проведения мероприятий по защите информации в Министерстве труда и социальной политики Республики Тыва

Начат «___» _____ 20___ г. На ____ листах
Окончен «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) (подпись)

№ п/п	Дата проведения	Мероприятие	Исполнитель	Результат	Подпись
1	2	3	5	6	7

Приложение № 22
к приказу №_____ от __.__20__г.

РЕГЛАМЕНТ
по использованию мобильных технических средств

1. Общие положения

Настоящий Регламент устанавливает порядок использования мобильных технических средств в Министерстве труда и социальной политики Республики Тыва

2. Основные термины и определения

Мобильные технические средства - съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

3. Порядок использования мобильных технических средств

− для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы, разрешены следующие виды доступа: (проводной (коммутируемый), широкополосный и иные виды доступа;

− использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30 «Меры защиты информации в государственных системах»;

− использование мобильных технических средств ограничивается задачами (функциями) информационной системы, для решения которых использование таких средств необходимо;

− осуществление мониторинга и контроля применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;

− запрещен запуск без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством;

− обеспечение запрета использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

− обеспечение запрета использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);

− обеспечение очистки машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами контролируемой зоны;

− обеспечение предоставления доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

− обеспечение запрета использования мобильных технических средств, на которые в информационной системе может быть осуществлена запись информации (перезаписываемых съемных машинных носителей информации).

Приложение № 23
к приказу №_____ от __.__20__г.

ИНСТРУКЦИЯ
о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Министерстве труда и социальной политики Республики Тыва

1 Общие положения

1.1. Настоящая Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Министерстве труда и социальной политики Республики Тыва (далее – Инструкция) предназначена для сотрудников Министерстве труда и социальной политики Республики Тыва (далее – Министерства), выполнение должностных обязанностей которых связано с использованием персональных компьютеров (пользователей), и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов информационно-вычислительных сетей общего пользования (далее – ИВС ОП), в том числе сети Интернет, а также основные требования по обеспечению безопасности информации.

1.2. Руководители структурных подразделений Министерства, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

1.3. Администратор информационной безопасности (далее – администратор ИБ) организует ознакомление пользователей с настоящей Инструкцией.

1.4. Доступ к ИВС ОП осуществляется с рабочей станции (далее – РС) пользователя. Ответственность за действия на компьютере другого человека несет пользователь РС, с которого совершено это действие.

1.5. Основными угрозами безопасности информации при использовании ИВС ОП в Министерстве являются:

– заражение информационно-вычислительных ресурсов Министерства программными вирусами;

– несанкционированный доступ внешних пользователей к информационно-вычислительным ресурсам Министерства (в т.ч. сетевые атаки);

– внедрение в информационные системы (далее – ИС) Министерства программных закладок;

– загрузка трафика нежелательной корреспонденцией (спамом);

– несанкционированная передача служебной информации ограниченного доступа сотрудниками Министерства в сеть Интернет (внутренний нарушитель);

– блокировка межсетевого взаимодействия с ИВС ОП путем нарушения целостности данных о настройках коммуникационного оборудования, обеспечивающего взаимодействие с ИВС ОП;

– нарушение целостности и достоверности открытых и общедоступных информационных ресурсов Министерства, размещаемых в ИВС ОП.

1.6. Основными методами обеспечения безопасности информации при использовании ИВС ОП для предотвращения указанных угроз являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов;

– использование сертифицированных средств защиты информации, в том числе антивирусных и криптографических;

– мониторинг вторжений (атак) из ИВС ОП, нарушающих или создающих предпосылки к нарушению установленных требований по защите информации, и анализ защищенности, предполагающий применение специализированных программных средств (сканеров безопасности);

– контроль информации, загружаемой или передаваемой в ИВС ОП;

– запрет обращения к нежелательным ресурсам ИВС ОП;

– шифрование информации при обмене с другими организациями при ее передаче по ИВС ОП, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации.

2 Доступ к Интернет-ресурсам

2.1. Министерства обеспечивает доступ пользователей сети к ресурсам ИВС ОП.

2.2. Открытие и контроль доступа регулируется администратором ИБ. Подключение сотрудников Министерства к ИВС ОП осуществляется только на основании списка лиц, допущенных к ресурсам ИВС ОП.

2.3. Доступ к ресурсам ИВС ОП предоставляется сотрудникам Министерства только для выполнения ими прямых должностных обязанностей.

2.4. Самостоятельная организация дополнительных точек доступа к ИВС ОП (удаленный доступ, канал по локальной сети, GPRS и пр.) запрещена.

3 Основные ограничения при работе в сети Интернет

3.1. Пользователям запрещается:

– загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;

– нецелевое использование подключения к ИВС ОП;

– осуществлять работу при отключенных средствах защиты информации, установленных на РС;

– допускать к работе посторонних лиц;

– передавать по сети ИВС ОП защищаемую информацию без использования средств шифрования;

– совершать любые попытки деструктивных действий по отношению к нормальной работе внутренней сети Министерства и ИВС ОП (рассылка вирусов, сетевые атаки и т.п.);

– применять имена пользователей и пароли, используемые в Министерстве в ИС за пределами Министерства;

– использовать электронную служебную почту Министерства в личных целях;

– использовать для служебной переписки иную электронную почту отличную от служебной электронной почты Министерства;

– посещать игровые, социальные, развлекательные и прочие сайты, не имеющие отношения к деятельности сотрудника Министерства;

– посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

– посещать ресурсы трансляции потокового видео и аудио (веб-камеры, трансляция ТВ и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;

– играть на компьютере автономно и в сети;

– производить какие-либо действия с информацией, зараженной вирусом;

– подключаться к ресурсам ИВС ОП, используя РС Министерства через не служебный канал доступа, сотовый телефон, модем, и др. устройства;

– создавать личные веб-страницы и хостинг (размещение web- или ftp-сервера) на компьютере пользователя;

– нарушать закон об авторском праве: копировать и использовать материалов и программ, защищенных законом об авторском праве;

– совершать действия, противоречащие законодательству, а также настоящей Инструкции.

3.2. Пользователь обязан:

– знать и уметь пользоваться антивирусным ПО. При обнаружении вируса он должен сообщить об этом администратору ИБ;

– информировать администратора ИБ о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети;

– знать и соблюдать установленные правила работы в локальной сети (Приложение №1 к настоящей Инструкции);

– знать и соблюдать установленные правила работы с электронной почтой (Приложение №2 к настоящей Инструкции);

– знать и соблюдать установленные правила работы в сети Интернет (Приложение №3 к настоящей Инструкции).

3.3. Пользователи несут персональную ответственность за содержание передаваемой, принимаемой и печатаемой информации.

3.4. Администратор ИБ обязан:

– производить подключение к сети ИВС ОП только через специализированное устройство (Firewall) для обеспечения защиты информационной сети;

– знать и правильно использовать аппаратно-программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;

– оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;

– ежемесячно вести учет и анализ использования ресурсов сети ИВС ОП по каждому пользователю;

– принимать меры для предотвращения и устранения нарушений требований настоящей инструкции пользователями и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

3.5. Администратор ИБ имеет право:

– при обнаружении доступа к развлекательным сайтам, запретить доступ к сайту;

– при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети ИВС ОП;

– в целях обеспечения безопасности электронной системы Министерства производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

4 Контроль использования ресурсов сети интернет

4.1. В целях обеспечения информационной безопасности и безопасности внутренней сети Министерства администратор ИБ осуществляет:

– контроль посещения ресурсов сети Интернет сотрудниками Министерства, а также получаемых и передаваемых сотрудниками данных, в том числе и по электронной почте;

– контроль над соблюдением настоящей Инструкции;

– организацию и контроль над безопасным использованием ресурсов сети ИВС ОП.

5 Действия в нештатных ситуациях

5.1. При утрате (в том числе частично) подключения к сети ИВС ОП лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику за организацию подключения к сети Интернет.

5.2. При заражении компьютера вирусами его использование немедленно прекращается сотрудником, обнаружившим заражение. О сложившейся ситуации сообщается администратору ИБ. Компьютер отключается от сети до момента очистки от всех вирусов.

Приложение № 1
к Инструкции о порядке работы при подключении
к сетям общего пользования и (или) международного обмена
в Министерстве

Правила по работе в локальной сети

1. Пользователи сети обязаны:

– при доступе к внешним ресурсам сети, соблюдать правила, установленные администратором информационной безопасности (далее – администратор ИБ) для используемых ресурсов;

– немедленно сообщать администратору ИБ об обнаруженных проблемах в использовании предоставленных ресурсов. Администратор ИБ, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры;

– не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;

– обеспечивать беспрепятственный доступ администратора ИБ к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;

– выполнять предписания администраторов ИБ, направленные на обеспечение безопасности сети;

– в случае обнаружения неисправности (например, сильный посторонний шум или запах, необычное поведение затрудняющее работу) компьютерного оборудования или программного обеспечения, пользователь должен немедленно обратиться к администратору ИБ;

– удалять с сетевых ресурсов устаревшие или не используемые файлы, владельцем или создателем которых он является.

2. Пользователи сети имеют право:

– использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Администратор ИБ вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;

– обращаться к администратору ИБ по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на

загруженность или безопасность системы, должны санкционироваться администратором ИБ;

– обращаться за помощью к администратору ИБ при решении задач использования ресурсов сети;

– вносить предложения по улучшению работы с ресурсом.

3. Пользователям сети запрещено:

– разрешать посторонним лицам пользоваться вверенным им компьютером;

– использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей, без согласования с администратором ИБ;

– самостоятельно устанавливать или удалять установленные администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

– повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

– вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с администратором ИБ, изменять настройки BIOS, а также производить загрузку PC с дискет;

– самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный администратором ИБ. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;

– работать с каналоемкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с администратором ИБ. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя, вызвавшего перегрузку, может быть прекращен;

– получать и передавать в сеть информацию, противоречащую действующему законодательству Российской Федерации и нормам морали общества, представляющую коммерческую или государственную тайну;

– обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;

– использовать иные формы доступа к сети, за исключением разрешенных администратором ИБ;

– осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;

– использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

Приложение № 2
к Инструкции о порядке работы при подключении
к сетям общего пользования и (или) международного обмена
в Министерстве

Правила работы с электронной почтой

1. Электронная почта предоставляется сотрудникам Министерства только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или изменение параметров почтового ящика проводится администратором информационной безопасности (далее – администратор ИБ) на основании служебной записки.

2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные Министерства. Прямой доступ к другим почтовым системам может быть блокирован. Для получения писем с других систем допускается использовать переадресацию, которая может быть настроена с помощью администратора ИБ.

3. Все электронные письма, создаваемые и хранимые на компьютерах Министерства, являются собственностью Министерства и не считаются персональными.

4. Министерства оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины.

5. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

6. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

7. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

8. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается, как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

9. Размер вложений у отправляемых писем не должен превышать 20 Мб.

10. При работе с электронной почтой сотрудникам Министерства запрещается:

– использовать адрес электронной почты для оформления подписок;

– публиковать свой электронный адрес либо адреса других сотрудников Министерстве на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;

– рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

– распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

– распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

– распространять информацию ограниченного доступа, предназначенную для служебного использования;

– предоставлять кому-либо пароль доступа к своему почтовому ящику.

Приложение № 3
к Инструкции о порядке работы при подключении
к сетям общего пользования и (или) международного обмена
в Министерстве

Правила по работе в сети Интернет

1. Сотрудники Министерства используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.

2. По использованию ресурсов Интернет сотрудниками Министерства необходимо ведение статистики.

3. Действия любого сотрудника Министерства, подозреваемого в нарушении правил пользования Интернетом, протоколируются и могут использоваться для принятия решения о применении к нему санкций.

4. Сотрудникам Министерства, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.

5. Все программы, предназначенные для доступа к сети Интернет, должны быть утверждены администратором информационной безопасности (далее – администратор ИБ), и на них должны быть настроены необходимые уровни безопасности.

6. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

7. Запрещено обращаться к ресурсам сети Интернет несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием.

8. Запрещается скачивать и запускать с любых ресурсов любые неизвестные исполняемые файлы без согласования с администратором информационной безопасности.

9. Запрещается использовать иные формы доступа к сети Интернет, за исключением разрешенных администратором ИБ.

10. Ответственность за все действия в сети Интернет, произведенные с рабочей станции, под именем и с паролем сотрудника Министерства, им самим или

другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе.

Приложение № 24
к приказу №_____ от __.__20__г.

ПОРЯДОК ОХРАНЫ И ПОРЯДОК ДОПУСКА ЛИЦ В ПОМЕЩЕНИЯ, В КОТОРЫХ РАСПОЛОЖЕНЫ ЭЛЕМЕНТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В РАБОЧЕЕ И НЕРАБОЧЕЕ ВРЕМЯ, А ТАКЖЕ В НЕШТАТНЫХ СИТУАЦИЯХ

1. Настоящий Порядок охраны и Порядок доступа лиц в помещения, в которых расположены элементы информационных систем персональных данных и ведется обработка персональных данных в рабочее и нерабочее время, а так же нештатных ситуациях (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Министерстве труда и социальной политики Республики Тыва (далее - Министерство) и обеспечения соблюдения требований законодательства о персональных данных.
2. Настоящий Порядок обязателен для применения и исполнения всеми работниками Министерства.
3. Объектами охраны Министерства:

- помещения, в которых происходит обработка информации ограниченного доступа с использованием средств автоматизации или без использования данных средств;
- помещения, в которых установлены компьютеры, серверы и коммутационное оборудование, как защищенные, так и не защищенные средствами криптографической защиты (далее - СКЗИ), участвующие в обработке персональных данных в информационных системах.
- помещения, в которых хранятся ключевые документы СКЗИ.

4. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.
5. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-накопители) хранятся в металлических шкафах, оборудованных опечатывающими устройствами.
6. Доступ в помещения

ДОСТУП В ПОМЕЩЕНИЯ В РАБОЧЕЕ ВРЕМЯ

В рабочее время доступ в помещения, в которых расположены элементы ИСПДн, разрешен только работникам, указанным в соответствующем

утвержденном перечне лиц.

В рабочее время помещения, где расположены элементы ИСПДн, должны закрываться назамок и открываться только для санкционированного прохода,

Доступ обслуживающего персонала для уборки помещения допускается только вприсутствии пользователей ИСПДн.

ДОСТУП В ПОМЕЩЕНИЯ В НЕРАБОЧЕЕ ВРЕМЯ

В нерабочее время доступ в помещения, в которых расположены элементы ИСПДн,разрешен только работникам, указанным в соответствующем перечне лиц при наличии служебной записки, подписанной руководителем подразделения и заверенной ответственнымза обеспечение безопасности ПДн.

ДОСТУП В ПОМЕЩЕНИЯ В НЕШТАТНЫХ СИТУАЦИЯХ

Если перед вскрытием помещений обнаружено нарушение целостности замков, то Помещения не вскрываются, составляется акт о случившемся и немедленно докладывается руководителю организации, администратору ИБ и службе безопасности, и принимаются мерыпо охране помещений до прибытия службы безопасности.

В дневное время суток сотрудник, обнаруживший нештатную ситуацию, должен поставить в известность непосредственного руководителя структурного подразделения —устно, администратора ИБ — устно, при необходимости — письменно.

В ночное время суток при возникновении нештатной ситуации, должна быть оповещенаслужба безопасности (охрана), Событие в обязательном порядке регистрируется в журнале дежурств, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных лиц, описанием действий, направленных на устранение нештатной ситуации. Если создается угроза уничтожения ПДн, то дежурный по организации вместе с подразделением охраны имеет право вскрыть помещения и принять меры к спасению технических средств и документов,

При этом также составляется служебная записка о случившемся и немедленнодокладывается лицу, ответственному за обеспечение безопасности ПДн.

7. Вскрытие и закрытие (опечатывание) помещений, в которых ведется обработка персональных данных, производится работниками, имеющими право доступа в данные помещения.

8. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

- убрать бумажные носители персональныхданных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть и опечатать шкафы;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети;
- выключить освещение;
- закрыть окна;
- подключить охранную сигнализацию либо опечатать помещение.

9. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери и замка;
- открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

10. При обнаружении неисправности двери и запирающих устройств работники обязаны:

- не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю и специалисту по защите информации;
- в присутствии не менее двух иных работников, включая непосредственного руководителя структурного подразделения, вскрыть помещение и осмотреть его;
- составить акт о выявленных нарушениях и передать его руководителю структурного подразделения Министерства для организации служебного расследования.

11. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

12. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты. Присутствие иных лиц, не имеющих права доступа к персональным данным, должны быть исключено.

При невозможности обеспечения отсутствия иных лиц в помещении при обработке персональных данных, необходимо развернуть монитор (при обработке ПДн на АРМ) таким образом, чтобы исключить подсматривание.

13. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении или лица, ответственного за данное помещение.

14. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей отделов, обрабатывающих персональные данные.

Приложение № 25
к приказу №_____ от __.__20__г.

Журнал инструктажа сотрудников с документами в области обеспечения информационной безопасности с использованием средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ) в информационных системах
Министерства труда и социальной политики Республики Тыва

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

Фамилия ознакамливающегося		Наименование документа						
	Инструкция по обращению с сертифицированными средствами криптографической защиты информации	Руководящие документы ФСБ России в области защиты ПДн с использованием СКЗИ	Инструкция по выявлению инцидентов и реагированию на них в информационных системах	Эксплуатационная документация на СКЗИ ViPNet Client	Эксплуатационная документация на СЗИ Secret Net Studio	Эксплуатационная документация на антивирус Kaspersky Endpoint Security для Windows	Эксплуатационная документация на антивирус Doctor Web для Windows	Эксплуатационная документация на сетевой сканер безопасности XSpider

Приложение № 26
к приказу №_____ от __.__20__г.

Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации в информационных системах Министерства труда и социальной политики Республики Тыва

1 Общие положения

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем (далее – ИС) Министерства труда и социальной политики Республики Тыва, меры и средства поддержания непрерывности работы и восстановления работоспособности ИС Министерства труда и социальной политики Республики Тыва после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИС Министерства труда и социальной политики Республики Тыва от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

– определение мер защиты от прерывания;

– определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех сотрудников Министерства труда и социальной политики Республики Тыва, имеющих доступ к ресурсам ИС Министерства труда и социальной политики Республики Тыва, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

– система жизнеобеспечения;

– система обеспечения отказоустойчивости;

– система резервного копирования и хранения данных;

– система контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2 Порядок реагирования на аварийную ситуацию

2.1. В настоящем документе под аварийной ситуацией (инцидентом) понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС Министерства труда и социальной политики Республики Тыва, предоставляемых пользователям ИС. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении №1 к настоящей инструкции – «Источники угроз».

2.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в журнале учета мероприятий по контролю обработки и защиты в ИС Министерства труда и социальной политики Республики Тыва.

2.3. Инцидент может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Министерства труда и социальной политики Республики Тыва администратор информационной безопасности, ответственный за обеспечение безопасности ПДн, ответственный за организацию обработки ПДн предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.5. Уровни реагирования на инцидент. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

– **уровень 1** – незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИС Министерства труда и социальной политики Республики Тыва и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

– **уровень 2** – авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИС Министерства труда и социальной политики Республики Тыва и средств защиты. Эти инциденты выходят за рамки Министерства труда и социальной политики Республики Тыва ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

а) отказ элементов ИС Министерства труда и социальной политики Республики Тыва и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования;

б) отсутствие администратора информационной безопасности более чем на сутки из-за:

- химического выброса в атмосферу;
- сбоев общественного транспорта;

- эпидемии;
- массового отравления персонала;
- сильного снегопада;
- торнадо;
- сильных морозов;

– **уровень 3** – катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС Министерства труда и социальной политики Республики Тыва и средств защиты, а также к угрозе жизни пользователей ИС Министерства труда и социальной политики Республики Тыва, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИС Министерства труда и социальной политики Республики Тыва и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

– пожар в здании;

– взрыв;

– просадка грунта с частичным обрушением здания;

– массовые беспорядки в непосредственной близости от объекта.

3 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

– системы жизнеобеспечения, что включает:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа;

– пожарные сигнализации и системы пожаротушения;

– системы вентиляции и кондиционирования.

3.2. Все критичные помещения Министерства труда и социальной политики Республики Тыва (помещения, в которых размещаются элементы ИС Министерства труда и социальной политики Республики Тыва и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИС описан в Порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.4. Ответственные за реагирование сотрудники ознакомляют всех сотрудников Министерства труда и социальной политики Республики Тыва, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

3.5. Должно быть проведено обучение должностных лиц Министерства труда и социальной политики Республики Тыва, имеющих доступ к ресурсам ИС Министерства труда и социальной политики Республики Тыва, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

– оказание первой медицинской помощи;

– пожаротушение;

– эвакуация людей;

– защита материальных и информационных ресурсов;

– методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

– выключение оборудования, электричества, водоснабжения, газоснабжения.

3.6. Администратор информационной безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИС Министерства труда и социальной политики Республики Тыва.

3.7. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

3.8. Ответственность за организацию обучения должностных лиц несет руководитель отдела. Сроки и порядок их обучения согласуется с администратором информационной безопасности.

Приложение №1
к Инструкции по действиям персонала
во внештатных ситуациях при обработке
защищаемой информации в информационных системах
Министерства труда и социальной политики Республики Тыва

Источники угроз

1. Технологические угрозы	
1.1	Пожар в здании
1.2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
1.3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
1.4	Химический выброс в атмосферу
2. Внешние угрозы	
2.1	Массовые беспорядки
2.2	Сбои общественного транспорта
2.3	Эпидемия
2.4	Массовое отравление персонала
3. Стихийные бедствия	
3.1	Удар молнии
3.2	Сильный снегопад
3.3	Сильные морозы
3.4	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
3.5	Затопление водой в период паводка
3.6	Наводнение, вызванное проливным дождем
3.7	Торнадо
3.8	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
4. Телеком и ИТ угрозы	
4.1	Сбой системы кондиционирования
4.2	Сбой ИТ-систем
5. Угроза, связанная с человеческим фактором	
5.1	Ошибка персонала, имеющего доступ к помещению, где расположено серверное оборудование
5.2	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
6. Угрозы, связанные с внешними поставщиками	
6.1	Отключение электроэнергии
6.2	Сбой в работе интернет-провайдера
6.3	Физически разрыв внешних каналов связи

Лист ознакомления

с приказом от «____» ___________2024 г. №______

«Об организации защиты информации, обрабатываемой в информационных системах Министерства труда и социальной политики Республики Тыва

№ п/п	ФИО	Должность	Дата ознакомления	Подпись

ЖУРНАЛ ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___

Должность _____

_____/_____ /

подпись ФИО

Журнал завершен «____» _____ 20___ г.

Должность _____

_____/_____ /

подпись ФИО

Журнал составлен на _____ листах

ЖУРНАЛ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ С ДОКУМЕНТАМИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

ЖУРНАЛ
УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

ЖУРНАЛ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МИНИСТЕРСТВЕ ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

ЖУРНАЛ РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ РЕСПУБЛИКИ ТЫВА

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

ЖУРНАЛ №____

проведения мероприятий по защите информации в Министерстве труда и социальной политики Республики Тыва

Начат «___» _____ 20___ г. На ____ листах
Окончен «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) (подпись)

ЖУРНАЛ №____

поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Начат «___» _____ 20___ г. На ____ листах
Окончен «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) (подпись)

Журнал инструктажа сотрудников с документами в области обеспечения информационной безопасности с использованием средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ) в информационных системах Министерства труда и социальной политики Республики Тыва

Журнал начат «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал завершен «____» _____ 20___ г.
Должность _____
_____/ _____ /
подпись ФИО

Журнал составлен на _____ листах

ЖУРНАЛ №____
регистрации входа в помещение, содержащее серверное и телекоммуникационное оборудование Министерства труда и социальной политики Республики Тыва

Начат «___» _____ 20___ г. На ____ листах
Окончен «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) (подпись)

ЖУРНАЛ №____
выдачи магнитных карточек доступа в помещение содержащее серверное и телекоммуникационное оборудование Министерства труда и социальной политики Республики Тыва

Начат «___» _____ 20___ г. На ____ листах
Окончен «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) (подпись)

№ п/п	Дата проведения	Мероприятие	Исполнитель	Результат	Подпись

Фамилия И. О. ознакамливающегося	Наименование документа										
	Политика по обработке персональных данных	Положение по организации и проведению работ по обеспечению безопасности персональных данных	Правила обработки персональных данных	Перечень персональных данных в информационной системе и подлежащих	Инструкция пользователя информационных систем	Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации	Инструкция по организации парольной защиты в информационных системах	Инструкция по организации антивирусной защиты в информационных системах	Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена	Инструкция по обращению с сертифицированными средствами криптографической защиты информации

№ п/п	Рег. №	Дата выдачи/сдачи	Тип носителя	Вид защищаемой информации	ФИО пользователя, получившего носитель	подпись пользователя, получившего носитель	подпись администратора информационной безопасности
№ п/п	Рег. №	Дата выдачи/сдачи	Тип носителя	Вид защищаемой информации	ФИО пользователя, получившего носитель	подпись пользователя, получившего носитель	подпись администратора информационной безопасности

№ п/п	Краткое описание инцидента	ФИО сотрудника, обнаружившего инцидент, должность, дата и время обнаружения	Дата и время пресечения несанкционированного воздействия	Дата, время доведения информации об инциденте администратору ИБ, ФИО и должность администратора ИБ	Подпись администратора ИБ
№ п/п	Краткое описание инцидента	ФИО сотрудника, обнаружившего инцидент, должность, дата и время обнаружения	Дата и время пресечения несанкционированного воздействия	Дата, время доведения информации об инциденте администратору ИБ, ФИО и должность администратора ИБ	Подпись администратора ИБ

№ п/п	Дата	Вид резервирования (полное, частичное)	Наименование резервируемого информационного ресурса	Количество (общий размер файлов)	Тип носителя	Серийный номер носителя информации	Ответственное лицо	Примечание
№ п/п	Дата	Вид резервирования (полное, частичное)	Наименование резервируемого информационного ресурса	Количество (общий размер файлов)	Тип носителя	Серийный номер носителя информации	Ответственное лицо	Примечание

№ п/п	Дата проведения	Мероприятие	Исполнитель	Результат	Подпись
№ п/п	Дата проведения	Мероприятие	Исполнитель	Результат	Подпись