МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ПОЛИТИКИ
РЕСПУБЛИКИ ТЫВА
(Минтруд Республики Тыва)

П Р И К А З

К ы з ы л

18.01.2021г. № 20

Об организации работы по обеспечению безопасности информации, в том числе персональных данных, в Министерстве труда и социальной политики Республики Тыва

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ПРИКАЗЫВАЮ:

1. Назначить ответственным лицом за работу по обеспечению безопасности информации, в том числе персональных данных, в Министерстве труда и социальной политики Республики Тыва заместителя директора по информационным технологиям ГБУ «Центр административно-хозяйственного обеспечения Минтруда РТ», а в случае его отсутствия – начальника отдела автоматизации и информационно-технического обеспечения ГБУ «Центр административно-хозяйственного обеспечения Минтруда РТ».
2. Утвердить прилагаемый перечень должностных лиц Министерства труда и социальной политики Республики Тыва, ответственных за обработку и защиту персональных данных, обрабатываемых в министерстве.
3. Руководителям подведомственных учреждений:

- назначить ответственных лиц за работу по обеспечению безопасности информации, в том числе персональных данных;
- утвердить форму Инструкции ответственного лица за организацию обработки персональных данных и обеспечение безопасности персональных данных (Приложение 1);
- утвердить форму Инструкции ответственного лица за защиту информации (администратору безопасности) (Приложение 2);
- утвердить Инструкцию по организации парольной защиты в учреждении (Приложение 3);
- утвердить форму Регламента реагирования на инциденты информационной безопасности (Приложение 4);

- утвердить форму Инструкции по организации резервного копирования Баз Данных (Приложение 5);

- утвердить форму Инструкции по защите информации о событиях безопасности (Приложение 6);

- утвердить форму Порядка обращения со съемными машинными носителями персональных данных (мобильными техническими средствами) (Приложение 7);

- утвердить форму Порядка учета, хранения и уничтожения материальных носителей персональных данных (Приложение 8);

4. Руководителям подведомственных учреждений в срок до 19 февраля 2021 года представить заместителю директора по информационным технологиям ГБУ «Центр административно-хозяйственного обеспечения Минтруда РТ» Монгуш Б.Б. локальные акты о назначении ответственных лиц за работу по обеспечению безопасности информации и об утверждении вышеуказанных инструкций и регламентов на электронную почту mon-bulat@mail.ru.

5. Ответственному лицу за организацию обработки информации ограниченного доступа, в том числе персональных данных, организовать ознакомление под подпись сотрудников министерства.

6. Отделу организационного, документационного обеспечения и контроля направить настоящий приказ в подведомственные учреждения посредством электронного документооборота.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Министр  С.В. Монгуш

Приложение 1
к Приказу № 20 от «18» 01 2021 г.

Форма

ИНСТРУКЦИЯ
ответственного лица за организацию обработки персональных данных и обеспечение безопасности персональных данных

1. Основные положения

1.1. Настоящая Инструкция определяет должностные обязанности Ответственного за организацию обработки и обеспечение безопасности персональных данных на абонентском пункте _____*(перечень программ)*_____ .

1.2. Ответственный за организацию обработки и обеспечение безопасности персональных данных на _____*(перечень программ)*_____ назначается Приказом о назначении ответственных за обеспечение безопасности ПДн из числа сотрудников, относящихся к категории "руководящий состав" _____*Название организации*_____ в соответствии с распределением обязанностей.

1.3. Ответственный за организацию обработки и обеспечение безопасности персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных, настоящей Инструкцией и другими внутренними документами *Государственного бюджетного учреждения Республики Тыва «* _____*Название организации*_____*»*, регламентирующими вопросы организации обработки и обеспечения безопасности персональных данных.

1.4. Ответственный за организацию обработки и обеспечение безопасности персональных данных обязан:

– организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых на _____*(перечень программ)*_____от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

– осуществлять внутренний контроль за соблюдением сотрудниками Государственного бюджетного учреждения Республики Тыва «_____*название организации*_____ » требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

– доводить до сведения сотрудников Государственного бюджетного учреждения Республики Тыва «____*(название организации)* _____» положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Государственном бюджетном учреждении Республики Тыва «*Название организации*»;

– в случае нарушения в Государственном бюджетном учреждении Республики Тыва «(*Название организации*)» требований к защите персональных данных, принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

1.5. Ответственный за организацию обработки и обеспечение безопасности персональных данных *Название программ* вправе иметь доступ к информации, касающейся обработки персональных данных в Государственном бюджетном учреждении Республики Тыва «*Название организации*» и включающей:

– цели обработки персональных данных;

– категории обрабатываемых персональных данных;

– категории субъектов, персональные данные которых обрабатываются;

– правовые основания обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых в Государственном бюджетном учреждении Республики Тыва «*Название организации*» способов обработки персональных данных;

– описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

– дату начала обработки персональных данных;

– срок или условия прекращения обработки персональных данных;

– сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

– сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

1.6. Ответственный за организацию обработки и обеспечение безопасности персональных данных в Государственном бюджетном учреждении Республики Тыва «*Название организации*» курирует ответственный специалист. В рамках данной деятельности, Ответственный за организацию обработки и обеспечение безопасности персональных данных *Название программ* выполняет следующие функции:

– организует планирование и проведение работ по защите персональных данных;

– организует работы по подготовке организационных и распорядительных документов по защите информации;

– организует работы по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;

– организует и проводит в установленном порядке расследование причин и условий появления нарушений защиты информации;

– организует доведение требований нормативно-правовых и законодательных актов Российской Федерации в области защиты информации до сведения пользователей;

– организует контроль за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации.

1.7. Ответственный за организацию обработки и обеспечение безопасности персональных данных _____(*Название программ*)_____несет ответственность за надлежащее выполнение возложенных на него функций по организации обработки персональных данных в Государственном бюджетном учреждении Республики Тыва «_____*Название организации*_____» в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Приложение 2
к Приказу № 20 от «18» 01 2021 г.

Форма

ИНСТРУКЦИЯ
ответственного лица за защиту информации (администратору безопасности)

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности ответственного за защиту информации (далее - администратора безопасности) Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

1.2. Администратор безопасности назначается Приказом руководителя Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

1.3. Администратор безопасности в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России, регламентирующими вопросы защиты персональных данных, внутренними организационно-распорядительными документами Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» по вопросам защиты информации и обеспечения безопасности персональных данных.

1.4. Администратор безопасности по вопросам обеспечения безопасности персональных данных подчиняется Ответственному за организацию обработки и обеспечение безопасности персональных данных в Государственном бюджетном учреждении Республики Тыва «_____Название организации_____».

1.5. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое).

1.6. Администратор безопасности осуществляет методическое руководство пользователями в вопросах обеспечения правильной работы с используемыми для обеспечения безопасности средствами защиты информации (далее - СЗИ). Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей, состояние и поддержание установленного уровня защищенности персональных данных_____Название программ_____и класса защищенности..

2. Задачи Администратора безопасности

2.1.Основными задачами Администратора безопасности являются:

– поддержание необходимого уровня защиты от несанкционированного доступа (далее - НСД) к персональным данным (далее - ПДн);

– обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации, в т. ч. ПДн;

– установка средств защиты информации и контроль выполнения правил их эксплуатации;

– сопровождение программных и технических СЗИ;

– периодическое обновление СЗИ (при необходимости);

– проведение комплекса мероприятий по предотвращению инцидентов информационной безопасности;

– оперативное реагирование на нарушения требований по информационной безопасности (далее – ИБ) _____Название программ_____и участие по их предотвращению.

2.2.В рамках выполнения основных задач Администратор безопасности осуществляет:

– текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

– текущий контроль технологического процесса автоматизированной обработки информации (ПДн);

– текущий контроль неизменности состояния СЗИ, их параметров и режимов защиты;

– текущий контроль физической сохранности средств и оборудования;

– контроль исполнения пользователями установленных _____Название программ_____правил организации парольной защиты (аутентификация и идентификация пользователей);

– анализ журналов учета событий безопасности СЗИ с целью выявления возможных нарушений;

– учет машинных носителей информации;

– контроль действий пользователей при работе с машинными носителями информации;

– регистрация полномочий пользователей в разрешительной системе доступа (матрица доступа) и их своевременная корректировка;

– контроль за соблюдением пользователями установленных _____Название программ_____правил по организации антивирусной защиты;

– участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности;

– контроль соблюдения нормативных требований по защите, обеспечение комплексного использования технических средств, методов и организационных мероприятий по безопасности пользователями;

– методическую помощь пользователям по вопросам обеспечения безопасности информации и работы с используемыми СЗИ.

3. Обязанности Администратора безопасности

3.1.Администратор безопасности обязан:

– знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации;

– участвовать в установке, настройке и сопровождении СЗИ;

– вести учет средств защиты информации, используемых для защиты персональных данных;

– участвовать в приеме новых программных средств обработки информации;

– обеспечить доступ к защищаемой информации пользователям согласно их правам доступа, при получении оформленного соответствующим образом разрешения (заявки);

– уточнять в установленном порядке обязанности пользователей при обработке ПДн;

– анализировать состояние защиты;

– контролировать правильность функционирования средств защиты информации и неизменность их настроек;

– контролировать физическую сохранность технических средств обработки информации;

– контролировать исполнение пользователями введенного режима безопасности, а также правильность работы со средствами защиты информации;

– контролировать исполнение пользователями правил парольной политики;

– вести контроль над процессом осуществления резервного копирования объектов защиты;

– еженедельно анализировать электронные журналы учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений;

– не допускать установку, использование, хранение и распространение _____Название программ_____программных средств, не связанных с выполнением функциональных задач;

– вести контроль за соблюдением установленного _____Название программ_____порядка организации работы с машинными носителями информации;

– не допускать к работе посторонних лиц;

– осуществлять периодические контрольные проверки автоматизированных рабочих мест (далее - АРМ) пользователей;

– оказывать помощь пользователям в части применения средств защиты и консультировать по вопросам введенного режима защиты;

– в случае необходимости информировать руководство о состоянии защиты, о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации;

– в случае отказа работоспособности СЗИ принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу;

– в случае выявления нарушений режима безопасности ПДн, а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий;

– в случае изменения используемых информационных технологий, состава и размещения средств и систем информации, условий их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в «Аттестате соответствия»), произвести извещение органа по аттестации, выдавшего «Аттестат соответствия»;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки информации, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта не рекомендуется передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. При передаче ремонтным организациям узлов и блоков с элементами накопления, и хранения информации проводится гарантированное уничтожение защищаемой информации с использованием сертифицированных средств защиты;

– осуществлять периодическое проведение поиска и анализа уязвимостей путем использования средств анализа (контроля) защищенности (сканеров безопасности). В качестве источников информации об уязвимостях также должны использоваться опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств.

4. Права Администратора безопасности

4.1.Администратор безопасности имеет право:

– отключать от ресурсов пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам или нарушивших другие требования по ИБ;

– давать пользователям обязательные для исполнения указания и рекомендации по вопросам ИБ;

– инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств;

– осуществлять контроль информационных потоков, генерируемых пользователями при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа;

– осуществлять взаимодействие с руководством Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» и персоналом по вопросам обеспечения ИБ;

– запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение;

– запрашивать и получать от пользователей информацию и материалы, необходимые для организации своей работы;

– вносить на рассмотрение руководства Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» предложения по улучшению состояния безопасности;

– принимать участие в проведении мероприятий по контролю за обеспечением безопасности;

– вносить изменения в конфигурацию, предварительно произведя анализ потенциального воздействия планируемых изменений на эффективность СЗИ, согласовав внесение планируемых изменений с ответственным за организацию обработки ПДн, и получив разрешение органа по аттестации, выдавшего «Аттестат соответствия»;

– действовать в обход установленных процедур идентификации и аутентификации только для восстановления функционирования в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5. Действия Администратора безопасности при обнаружении попыток несанкционированного доступа

5.1.К попыткам НСД относятся:

– сеансы работы с телекоммуникационными ресурсами незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам с использованием учетной записи администратора или другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

5.2.При выявлении факта/попытки НСД Администратор безопасности обязан:

– прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;

– доложить в случае необходимости Ответственному за организацию обработки и обеспечение безопасности ПДн о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

– известить начальника структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– проанализировать характер НСД;

– по решению руководства осуществить действия по выяснению причин, приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.

6. Ответственность Администратора безопасности

6.1.Администратор безопасности несет ответственность за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей Инструкцией и другими локальными нормативными документами Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» по защите информации.

6.2.Нарушение данной Инструкции Администратором безопасности, повлекшее уничтожение, блокирование, модификацию, несанкционированное копирование охраняемой Государственным бюджетным учреждением Республики Тыва «_____Название организации_____» информации, нарушение работы АРМ пользователей, других элементов оборудования, может повлечь дисциплинарную (вплоть до увольнения), административную или уголовную ответственность в соответствии с действующим Российским законодательством и Трудовым кодексом Российской Федерации.

Приложение 3
к Приказу № 20 от «18» 01 2021 г.

Форма

Инструкция
по организации парольной защиты

1Общие положения

1.1 Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» (

1.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора безопасности.

1.3 Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2 Порядок организации парольной защиты

2.1 Личные пароли должны генерироваться и распределяться централизованно администратором безопасности с учетом следующих требований:

- длина пароля должна быть не менее шести символов, алфавит пароля - не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - от 3 до 15 минут;
- в числе символов пароля обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому.

2.2 Ответственность за правильность формирования и распределения паролей возлагается на администратора безопасности.

2.3 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 180 дней.

2.4 Блокировка программно-технических средств или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации должна составлять от 3 до 15 минут.

2.5 Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.6 В случае прекращения полномочий администратора безопасности производится полная внеплановая смена всех паролей.

2.7 В случае компрометации личного пароля пользователя системы должны быть немедленно предприняты меры в соответствии с п. 2.4 или п. 2.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.8 Использование 2-х последних значений паролей при создании новых паролей не допустимо.

2.9 Хранение пользователем значений своих паролей на бумажном носителе допускается только в опечатанном печатью конверте в сейфе у администратора безопасности.

2.10 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.). Вводимые символы пароля должны отображаться условными знаками «*», «•» или иными знаками.

2.11 Повседневный контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2.12 Временные пароли, заданные при внедрении системы защиты информации сотрудниками сторонних организаций, рекомендуется изменить при первом входе в систему.

2.13 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3 Ответственность

3.1 Ответственность за соблюдение требований хранения и использования паролей возлагается на их владельца.

3.2 Ответственность за соблюдение требований, а также за своевременное информирование о необходимости смены паролей в подразделении возлагается на администратора безопасности.

Приложение 4
к Приказу № 20 от «18» 01 2021 г.

Форма

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности

1 Общие положения

1.1 Настоящий регламент определяет действия лиц Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» в случае возникновения инцидентов в процессах обработки информации, в т. ч. персональных данных (далее – ПДн).

1.2 Положения настоящего регламента обязательны для исполнения всеми должностными лицами, допущенными к работе _____Название программ_____в части выполнения возложенных на них обязанностей.

1.3. Общими требованиями ко всем лицам, в случае возникновения инцидента являются:

– лицо, обнаружившее инцидент, немедленно ставит в известность администратора безопасности;

– администратор безопасности обязан провести анализ ситуации и, в случае невозможности исправить положение, поставить в известность руководство Государственного бюджетного учреждения Республики Тыва «_____Название организации_____». Кроме этого, администратор безопасности для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей;

– по факту возникновения инцидента и выяснению причин его проявления по решению руководства может быть назначена комиссия по реагированию на инциденты ИБ и проведено служебное расследование.

2 Действия пользователей при возникновении инцидентов

2.1 Сбой программного обеспечения.

2.1.1 Администратор безопасности выясняет причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор сообщает руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» для принятия решения, по существу.

2.2 Отключение электропитания технических средств.

2.2.1 Администратор проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О

произошедшем инциденте администратор сообщает руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» для принятия решения, по существу.

2.3 Выход из строя технических средств (рабочих станций, источников бесперебойного питания, программно-аппаратных средств межсетевого экранирования и т.д.).

2.3.1 Администратор совместно с администратором безопасности выполняют мероприятия по ремонту неисправного технического средства.

2.3.2 В случае необходимости уведомить о выходе из строя технических средств администратора.

2.3.3 При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий с составлением акта. О произошедшем инциденте необходимо сообщить администратору безопасности для принятия решения, по существу.

2.4 Обнаружение вредоносной программы в программной среде средств автоматизации.

2.4.1 При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженную рабочая станцию рекомендуется физически отсоединить от локальной вычислительной сети, и администратор безопасности проводит анализ состояния рабочей станции.

2.4.2 После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

2.4.3 По факту появления ВП в локальной вычислительной сети может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается Ответственным за организацию обработки и обеспечение безопасности ПДн.

2.5 Утечка информации.

2.5.1 При обнаружении утечки информации ставится в известность администратор безопасности. По факту может быть произведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.6 Взлом операционной системы средств автоматизации (несанкционированное получение доступа к ресурсам операционной системы).

2.6.1. При обнаружении взлома рабочей станции ставятся в известность администратор и администратор безопасности.

2.6.2. По возможности производится временное отключение рабочей станции от локальной вычислительной сети для проверки на наличие ВП.

2.6.3. Администратором безопасности проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов - скриптов и журналов сервера, производится

смена всех паролей, которые имели отношение к данному серверу.

2.6.4 В случае необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

2.6.5 По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах.

2.7 Попытка несанкционированного доступа (НСД).

2.7.1. При попытке НСД администратором безопасности проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.7.2 Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, администратором устанавливаются такие обновления.

2.7.3 По факту попытки НСД может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается Ответственным за организацию обработки и обеспечение безопасности ПДн.

2.7.4 В случае установления в ходе служебного расследования факта осуществления попытки НСД, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.8 Компрометация ключевой информации (паролей доступа).

2.8.1 При компрометации ключевой информации (пароля доступа) администратором безопасности принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

2.8.2 О произошедшем инциденте сообщается руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» для принятия решения, по существу.

2.9 Физическое повреждение или хищение оборудования технических средств.

2.9.1 Сотрудником, обнаружившим физическое повреждение элементов, ставятся в известность: администратор, администратор безопасности.

2.9.2 Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов и возможные угрозы информационной безопасности.

2.9.3 О факте повреждения элементов в случае необходимости администратор безопасности докладывает руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

2.9.4 В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

2.9.5 Администратором безопасности проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.9.6 При необходимости администратором проводятся мероприятия по восстановлению программного обеспечения из эталонных копий с составлением акта.

2.10 Невыполнение установленных правил ИБ, использование с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.10.1 Сотрудником, обнаружившим невыполнение установленных правил ИБ, использование с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность администратор безопасности.

2.10.2 Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.10.3 Об обнаруженном факте администратор безопасности в случае необходимости докладывает руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

2.10.4 При необходимости по решению руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» по фактам выявленных нарушений проводится служебное расследование.

2.11 Ошибки сотрудников.

2.11.1 В случае возникновения сбоя, связанного с ошибками сотрудников, администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения.

2.11.2 При необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий с составлением акта.

2.11.3 В случае нанесения значительного ущерба вследствие ошибок работников по решению руководства Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» может быть проведено служебное расследование.

2.12 Отказ в обслуживании.

2.12.1 Сотрудником, обнаружившим отказ в обслуживании, ставятся в известность администратор безопасности.

2.12.2. Администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.12.3 Администратором безопасности проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.12.4 При необходимости, проводятся мероприятия по восстановлению программного обеспечения с составлением акта.

2.12.5 О причинах инцидента и принятых мерах администратор безопасности в случае необходимости информирует руководство Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

2.13 Несанкционированные изменения состава программных и аппаратных средств (конфигурации).

2.13.1 В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.13.2 Администратором совместно с администратором безопасности проводятся мероприятия по восстановлению программного обеспечения, а также (при необходимости) проверка на наличие компьютерных ВП.

2.13.3 Об инциденте необходимо доложить руководству Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

2.14 Техногенные и природные проявления нештатных ситуаций.

2.14.1 При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику, обнаружившему факт возникновения нештатной ситуации:

- немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему администратору и администратору безопасности.

2.14.2 После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.14.3 Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

Приложение 5
к Приказу № 20 от «18» 01 2021 г.

Форма

ИИНСТРУКЦИЯ
по организации резервного копирования

1 Общие положения

Настоящая инструкция определяет действия Государственного бюджетного учреждения Республики Тыва «_____Название организации_____», меры и средства поддержания непрерывности работы и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

Целью настоящего документа является превентивная защита элементов от предотвращения потери защищаемой информации.

Задачей данной инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за проведение резервного копирования назначается администратор. Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности.

2 Порядок организации резервного копирования

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемой информации – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты),

с которых осуществляется их установка на элементы – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Резервному копированию подлежит информация следующих основных категорий:

– персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;

– информация, обрабатываемая пользователями, а также информация, необходимая для восстановления работоспособности, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;

– рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения;

– регистрационная информация системы информационной безопасности;

– другая информация, по мнению пользователей и администраторов, являющаяся критичной для работоспособности.

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Машинные носители информации, на которые произведено резервное копирование, должны быть учтены в журнале учета машинных носителей для архивного копирования, который находится у администратора безопасности. В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

Физический доступ к архивным копиям предоставляется только администратору и администратору безопасности.

Передача машинных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

В случае необходимости восстановление данных из резервных копий производится администратором или администратором безопасности.

Восстановление данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему,

воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

3 Ответственность

Ответственность за своевременное осуществление резервного копирования возлагается на администратора. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

Приложение 6
к Приказу № 20 от «18» 01 2021 г.

Форма

Инструкция
по защите информации о событиях безопасности

1 Общие положения

Настоящая инструкция по организации защиты информации о событиях безопасности Государственного бюджетного учреждения Республики Тыва «_____Название организации_____», определяет основные мероприятия по защите информации о событиях безопасности.

2 Основные мероприятия по защите информации о событиях безопасности

События безопасности, подлежащие регистрации, определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации, отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также нарушения штатного функционирования средств защиты информации.

Определены следующие события безопасности, подлежащие регистрации:

1) События, связанные с регистрацией входа (выхода) субъектов доступа в систему и загрузки операционной системы. Состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2) События, связанные с регистрацией подключения машинных носителей информации и вывода информации на носители информации. Состав и содержание регистрационных записей включает: дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

3) События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4) События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная),

идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

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

6) События, связанные с изменением привилегий учетных записей.

7) События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления.

8) События, связанные с регистрацией запланированного обновления операционных систем (далее – ОС), которые ведутся в штатных журналах ОС. Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации, и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов.

Так же подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется администратором безопасности, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

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

Для обеспечения защиты информации о событиях безопасности, перед установкой средств защиты информации (далее – СЗИ) осуществляется синхронизация системного времени и даты. Администратор безопасности осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы и установленных СЗИ.

В целях предотвращения сбоев при регистрации событий безопасности СЗИ и ОС:

1. Администратору безопасности необходимо еженедельно проверять журналы регистрации событий СЗИ и ОС на наполненность и, в случае необходимости, производить их архивацию.

2. Увеличить при необходимости объем выделяемой под журналы событий безопасности СЗИ и ОС памяти.

3. Включить автоматическую перезапись новых событий безопасности поверх устаревших для предотвращения возникновения ошибок переполнения журналов.

4. Настройки прав учетных записей пользователей должны исключать возможность внесения пользователями изменений в журналы событий безопасности, настройки СЗИ и ОС.

5. При появлении ошибок ОС или СЗИ пользователю необходимо уведомить администратора безопасности и приостановить работу до устранения ошибки.

Приложение 7
к Приказу от «20» 01 2021 г. № 20

Форма

Порядок обращения со съемными машинными носителями персональных данных (мобильными техническими средствами)

Настоящий Порядок определяет правила обращения со съемными машинными носителями персональных данных (мобильных технических средств) Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

В качестве мобильных технических средств рассматриваются 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).

При использовании мобильных технических средств запрещается:

1) Обрабатывать защищаемую информацию на ноутбуках, используемых в качестве основных технических средств и систем (ОТСС) за пределами контролируемой зоны;

2) Выносить за пределы контролируемой зоны ноутбуки, используемые в качестве ОТСС, кроме случаев передачи в ремонт;

3) Использовать мобильные технические средства в целях, не связанных с обработкой защищаемой информации, в том числе персональных данных (ПДн);

4) Использовать съемные машинные носители информации, не зарегистрированные в журнале учета съемных носителей информации;

5) Подключать к элементам внешние устройства, не входящие в состав (мобильные телефоны, цифровые фотоаппараты, адаптеры беспроводной связи и иные).

6) Использовать незащищенные беспроводные сети (WiFi, Bluetooth и др.);

7) Хранить на мобильных технических средствах личной информации, а также информации, не имеющей отношения к служебной деятельности (музыкальные файлы, фоновые изображения и прочее).

Устройства ввода аудио (микрофоны) и видео (веб-камеры) информации мобильных технических средств, должны быть отключены.

Администратором безопасности обеспечивается:

1) Запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

2) Запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);

3) Очистка 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;

4) Предоставление доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

5) Запрет использования устройств ввода аудио (микрофоны) и видео (веб-камеры) информации технических средств;

Подключение мобильных технических средств к ресурсам должно осуществляться только по проводным каналам связи. Использование для подключения к ресурсам незащищенных беспроводных точек доступа (Wi-Fi и др.) запрещено.

Администратором безопасности обеспечивается запрет подключения к беспроводным сетям доступа технических средств, имеющих в своем составе модули беспроводного доступа (моноблоки, стационарные АРМ, принтера и другие технические средства).

Ответственность за правильную эксплуатацию мобильных и технических средств, имеющих в своем составе модули беспроводного доступа, несут пользователи и Администратор безопасности.

Контроль за соблюдением пользователями правил эксплуатации мобильных технических средств и технических средств, имеющих в своем составе модули беспроводного доступа возлагается на Администратора безопасности.

Контроль за соблюдением пользователями правил эксплуатации мобильных технических средств возлагается на администратора безопасности.

Приложение 8
к Приказу № 20 от «18» 01 2021 г.

Форма

Порядок учета, хранения и уничтожения материальных носителей персональных данных

1. Общие положения

1.1. Настоящий Порядок устанавливает организацию учета, хранения и уничтожения материальных носителей персональных данных (электронные, магнитные, оптические, бумажные) Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

1.2. Настоящий Порядок разработан на основании следующих документов:

- Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 21 марта 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Требования по обеспечению безопасности при использовании материальных носителей персональных данных

2.1. При обращении с материальными носителями персональных данных выполняются следующие основные правила:

– находящиеся на хранении и в обращении материальные носители персональных данных подлежат учёту;

– раздельному учету в журналах учета подлежат машинные носители, съемные машинные носители персональных данных (флэш-накопители, CD-диски и т.п.), бумажные носители персональных данных (в соответствии с номенклатурой делопроизводства);

– пользователи для работы могут использовать только учтенные материальные носители персональных данных;

– машинные носители персональных данных, срок эксплуатации которых истек, а также бумажные носители, потерявшие актуальность или необходимость их

использования (достижение цели обработки, истечение срока хранения) уничтожаются в установленном порядке;

– все съемные машинные и бумажные носители информации хранятся в запираемых шкафах (сейфах), а также раздельно, в соответствии с целями обработки ПДн.

Ответственным за хранение, учет и выдачу съемных машинных носителей информации является администратор безопасности.

2.2 Порядок учета материальных носителей персональных данных.

Все находящиеся на хранении и в обращении материальные носители персональных данных учитываются в журнале учета машинных носителей персональных данных, журнале учета съемных машинных носителей персональных данных и журнале учета бумажных носителей персональных данных.

Каждый материальный носитель персональных данных должен иметь уникальный регистрационный (учетный) номер. В качестве регистрационных номеров допускается использовать идентификационные (серийные) номера машинных носителей, присвоенные производителем этих машинных носителей, номера инвентарного учета, в т.ч. инвентарные номера технических средств, имеющих встроенные носители информации, учетные номера по номенклатуре дел для бумажных носителей и иные учетные номера.

Учет встроенных в стационарные технические средства машинных носителей персональных данных может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей персональных данных, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Учет и выдачу съемных машинных носителей персональных данных осуществляет администратор безопасности. Факт выдачи и получения съемного машинного носителя конкретным сотрудником фиксируется в журнале учета съемных машинных носителей персональных данных.

Учет и выдачу бумажных носителей персональных данных осуществляет руководитель подразделения, сотрудник которого использует эти бумажные носители.

После окончания работ пользователь сдает материальный носитель, о чем делается соответствующая запись в соответствующем журнале учета материальных носителей персональных данных. При наличии личного сейфа у пользователя допускается хранение учтенных материальных носителей в личных сейфах, в противном случае, материальные носители персональных данных должны храниться в сейфе у ответственного за учет материальных носителей персональных данных.

В случае передачи материальных носителей между пользователями с разными правами доступа к персональным данным, при необходимости, должно обеспечиваться уничтожение (стирание) информации (на машинных и съемных машинных носителях), а также при передаче материальных носителей (машинных и съемных машинных) в сторонние организации для ремонта или утилизации, администратор безопасности должен осуществлять контроль уничтожения

(стирания) информации на этих носителях. При этом, уничтожение (стирание) информации на материальных носителях должно исключать возможность восстановления защищаемой информации.

Сотрудникам запрещается подключать неучтенные носители информации и информационно-телекоммуникационные средства.

2.3 Порядок уничтожения информации на материальных носителях персональных данных и уничтожения материальных носителей персональных данных.

Меры по уничтожению (стиранию) информации на материальных носителях персональных данных, исключающие возможность восстановления защищаемой информации:

– удаление файлов на машинном носителе (съемном машинном носителе) информации штатными средствами операционной системы и последующее форматирование машинного носителя (съемного машинного носителя) информации штатными средствами операционной системы;

– удаление файлов на машинном носителе (съемном машинном носителе) информации средствами гарантированного удаления информации (СЗИ Secret Net Studio, средство гарантированного удаления Terrier и т.п.);

– «вымарывание» информации на бумажных носителях.

Материальные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

Уничтожение материальных носителей персональных данных осуществляется комиссией по уничтожению, назначаемой руководителем Государственного бюджетного учреждения Республики Тыва «_____Название организации_____».

Уничтожение материальных носителей персональных данных осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.). Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов.

По результатам уничтожения комиссией составляется акт уничтожения материальных носителей персональных данных, уничтоженные материальные носители персональных данных снимаются с материального учета. (делается запись в журналах их учета и регистрации). В номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

В порядке, установленном законодательством Российской Федерации, для уничтожения материальных носителей и информации на материальных носителях может привлекаться подрядная организация, имеющая необходимую производственную базу для обеспечения установленного порядка уничтожения документов и носителей. В этом случае, уполномоченное должностное лицо Государственного бюджетного учреждения Республики Тыва «_____Название организации_____», сопровождает материальные носители, содержащие персональные данные, до

производственной базы подрядчика и присутствует при процедуре уничтожения материальных носителей (например, сжигание или химическое уничтожение). После уничтожения материальных носителей, уполномоченным должностным лицом Государственного бюджетного учреждения Республики Тыва «_____Название организации_____» и подрядчиком подписывается соответствующий акт в трех экземплярах.