ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ ТЫВА

Служба по гражданской обороне
и чрезвычайным ситуациям Республики Тыва

ПРИКАЗ

«25» июня 2018 года г. Кызыл № 94

Об утверждении нормативных правовых актов по обеспечению безопасности информационных ресурсов информационно-телекоммуникационной сети, в том числе по обеспечению технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну в Службе ГО и ЧС Республики Тыва и подведомственных ее учреждения.

С целью обеспечения безопасности информационных ресурсов информационно-телекоммуникационной сети, в том числе по обеспечению технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в соответствии с Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» приказываю:

1. Утвердить прилагаемые:

-Порядок доступа государственных гражданских служащих, работников Службы ГО и ЧС Республики Тыва в помещение, где ведется обработка персональных данных;

-Инструкцию администратора информационной системы персональных данных;

- Инструкцию администратора по информационной безопасности;

- Инструкцию пользователя информационной системы персональных данных;

-Инструкцию по организации антивирусной защиты в информационной системе персональных данных;

-Инструкцию по организации резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных Службе ГО и ЧС Республики Тыва;

- Инструкцию по работе с ключевыми носителями в информационных системах обработки персональных данных.

2.Управлению обработки вызовов «Системы-112»,оповещения и информирования населения разместить настоящий приказ на официальном сайте Службе ГО и ЧС Республики Тыва.

3.Руководителям структурных подразделений Службы ГО и ЧС Республики Тыва ознакомить с настоящим приказом сотрудников, осуществляющих обработку персональных данных, под роспись.

Руководитель А.А. Сарыглар

Утвержден
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

ПОРЯДОК

доступа государственных гражданских служащих, работников Службы ГО и ЧС Республики Тыва в помещения, где ведется обработка персональных данных

1. Настоящий Порядок регламентирует условия и порядок осуществления доступа государственных гражданских служащих, работников Службы ГО и ЧС Республики Тыва в помещения, где ведется обработка персональных данных (далее - Помещения).
2. Режим охраны Помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает руководитель Службы ГО и ЧС. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящего Порядка, специфику и условия работы конкретных работников.
3. Размещение и монтаж оборудования, функционирующего в Помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена ключей осуществляются в отсутствие лиц, не допущенных к работе с конфиденциальной информации.
4. На время отсутствия работников Службы ГО и ЧС Республики Тыва, осуществляющих обработку персональных данных, указанное оборудование при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае государственный гражданский служащий по согласованию с подразделением по защите информации обязан предусмотреть организационно - технические меры, исключающие возможность использования технических средств посторонними лицами в их отсутствие.
5. По окончании рабочего дня Помещения и установленные в них хранилища должны быть закрыты, хранилища опечатаны.
6. Печати, предназначенные для опечатывания хранилищ, должны находиться у работников Службы ГО и ЧС Республики Тыва, ответственных за эти хранилища.
7. При утрате ключа от хранилища или от входной двери в Помещение замок необходимо заменить.
8. Порядок хранения носителей конфиденциальной информации и других документов в хранилище, от которого утрачен ключ, до изменения замка устанавливает руководитель структурного подразделения, где обрабатывается персональные данные.
9. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в Помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству.
10. Прибывшие сотрудники должны оценить возможность компрометации хранящихся носителей конфиденциальной информации и других документов, составить

акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных ключей.

11. Контроль за порядком доступа лиц в помещения, где ведется обработка персональных данных в Службе ГО и ЧС Республики Тыва возлагается на руководителей соответствующих структурных подразделений.

12. Перечень лиц, допущенных в помещения, в которых ведется обработка персональных данных утверждается руководителем Службы ГО и ЧС.

Утверждена
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

Инструкция администратора информационной системы персональных данных

1. Общие положения

1.1. Администратор ИСПДн (далее - Администратор) назначается приказом Службы ГО и ЧС Республики, на основании Положения об обработке и защите персональных данных субъектов персональных данных в Службе ГО и ЧС Республики.

1.2. Администратор подчиняется руководителю Службы ГО и ЧС.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, Положением об обработке и защите персональных данных субъектов персональных данных в Службе ГО и ЧС, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами Службы ГО и ЧС Республики Тыва.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.5. Методическое руководство работой пользователя осуществляется сотрудником, ответственным за техническую защиту информации в Службе ГО и ЧС Республики Тыва (далее - ответственный за обеспечение защиты персональных данных).

2. Функции

2.1. Администратор обеспечивает устойчивую работоспособность элементов ИСПДн, средств ее защиты при обработке персональных данных, локальной вычислительной сети.

3. Должностные обязанности

3.1. Администратор обязан:

3.2. 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.

3.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

3.4. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

3.5. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

3.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.8. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

3.9. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователей ИСПДн.

3.10. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

3.11. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.12. 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 персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

3.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

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

4. Права и полномочия

4.1. Администратор имеет право:

4.2. Требовать от сотрудников Оператора соблюдения установленного комплекса мероприятий по обеспечению безопасности информации

4.3. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа;

4.4. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

5. Ответственность

5.1. Администратору необходимо отвечать за свои действия (бездействия) в рамках зафиксированных в п.п 3, 4 настоящей инструкции обязанностей, прав и полномочий

5.2. Администратор несет дисциплинарную, материальную, гражданско-правовую, административную и уголовную ответственность в порядке, предусмотренном законодательством.

Утверждены
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

Инструкция администратора по информационной безопасности

1. Общие положения

1.1. Настоящая инструкция определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при подготовке и обработки персональных данных на ПЭВМ, входящих в состав информационной системы персональных данных (далее по тексту - ИСПДн).

1.2. Администратор безопасности информации назначается из числа сотрудников Службы ГО и ЧС Республики Тыва и обеспечивает правильное использование и функционирование установленных средств защиты информации (далее по тексту - СЗИ) от несанкционированного доступа (далее по тексту - НСД).

1.3. Администратор безопасности информации имеет все права администратора СЗИ от НСД.

1.4. Настоящая Инструкция разработана на основании действующих нормативных документов по защите персональных данных.

2. Основные функции администратора безопасности

2.1. Контроль за выполнением требований действующих нормативных и руководящих документов по защите персональных данных, при проведении работ на ПЭВМ.

2.2. Своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);
- изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИСПДн.

2.3. Корректировка разрешительной системы доступа осуществляется на основании служебной записки пользователя, согласованной с ответственным за эксплуатацию объекта и утвержденной руководителем Службы ГО и ЧС Республики Тыва.

2.4. Контроль доступа пользователей к работе на ПЭВМ (в соответствии со списком допущенных сотрудников) и соблюдения пользователями требований нормативных и руководящих документов (в том числе путем просмотра системного журнала).

2.5. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на ПЭВМ, в том числе и в части периодического контроля за печатью файлов пользователей на принтере и соблюдением установленных правил и параметров регистрации и учета документов, бумажных и машинных носителей информации.

2.6. Сопровождение подсистемы обеспечения целостности информации на ПЭВМ:

- периодический контроль за отсутствием на жестком магнитном диске ПЭВМ

остаточной информации по окончании работы пользователей;

- поддержание установленного порядка и правил антивирусной защиты информации, обрабатываемой на ПЭВМ;
- контроль за соблюдением пользователями инструкции по антивирусному контролю. Программирование, выдача и учет выдачи пользователям электронных идентификаторов (ключей) от СЗИ НСД (при их наличии).

2.7. Контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ и устройств.

2.8. Контроль срока действия сертификатов соответствия ФСТЭК России на средства защиты от несанкционированного доступа и ФСБ России на средства криптографической защиты информации, установленных на ИСПДн.

3. Администратор безопасности имеет право:

3.1. Требовать от сотрудников соблюдения установленной технологии обработки конфиденциальной информации и исполнения настоящей Инструкции.

3.2. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа;

3.3. Участвовать в разработке заданий на проектирование элементов ИСПДн и иных информационных систем обработки конфиденциальной информации

3.4. Требовать от пользователей прекращения обработки информации в ИСПДн в случае:

- нарушения установленного порядка работ;
- нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСБ России или ФСТЭК России;
- получения информации о возможном проведении технической разведки в отношении ИСПДн.

4. Администратор безопасности обязан:

4.1. Обеспечивать правильное функционирование и поддерживать работоспособность средств и СЗИ от НСД в пределах возложенных на него функций;

4.2. В случае отказа СЗИ от НСД принимать меры по их восстановлению;

4.3. Проводить инструктаж пользователей по правилам работы на ПЭВМ, с установленной СЗИ от НСД;

4.4. Немедленно докладывать (по подчиненности) ответственному за эксплуатацию ИСПДн, Руководителю Службы ГО и ЧС Республики Тыва Республики или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к персональным данным, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности ИСПДн.

4.5. Вносить изменения в документацию ИСПДн в соответствии с требованиями нормативных документов в части, касающейся СЗИ от ПСД;

4.6. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению;

4.7. Осуществлять не реже одного раза в неделю обновление антивирусных баз

на ПЭВМ в ИСПДн;

4.8. Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать по подчинённости;

4.9. Вводить полномочия работников в разрешительную систему доступа, обеспечивать их своевременную корректировку;

4.10. Требовать от пользователей прекращения обработки информации ИСПДн при появлении информации о возможном проведении технической разведки в отношении ИСПДн или при нарушении правил обработки конфиденциальной информации.

4.11. Заблокировать учетные записи пользователей на ПЭВМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае не продления сертификата соответствия ФСТЭК России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия совместного решения.

4.12. Контролировать действия пользователей по правильности хранения и затирания информации на внешних и внутренних накопителях информации.

Утверждена
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

Инструкция пользователя информационной системы персональных данных

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее по тексту - ИСПДн) осуществляет обработку персональных данных в ИСПДн.

1.2. Пользователем является каждый работник Службы ГО и ЧС Республики Тыва, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Положением об обработке и защите персональных данных субъектов персональных данных в Службе ГО и ЧС Республики Тыва, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами Службы ГО и ЧС Республики Тыва.

1.5. Методическое руководство работой пользователя осуществляется сотрудником ответственным за техническую защиту информации в Службы ГО и ЧС Республики Тыва (далее - ответственный за обеспечение защиты персональных данных).

2. Должностные обязанности

Пользователь обязан:

2.1. 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.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены должностными обязанностями или регламентом.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 4).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. При работе с конфиденциальной информацией обрабатывать информацию в папках соответствующего уровня конфиденциальности.

2.8. Обо всех выявленных нарушениях, связанных с информационной

безопасностью,а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты персональных данных.

2.9. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн;

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

3.Пользователям запрещается:

2.11. Разглашать защищаемую информацию третьим лицам.

2.12. Копировать защищаемую информацию на любые носители и папки непредназначенные для обработки конфиденциальной информации.

2.13. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.14. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

2.15. Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

2.16. Отключать (блокировать) средства защиты информации и изменять их настройки.

2.17. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

2.18. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

2.19. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.20. использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.

2.21. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- Пароль должен состоять не менее чем из 6 символов.
- В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

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

- Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
- Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
- Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.
- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.7. За нарушение положений данной инструкции к работнику может быть применена ответственность, предусмотренная действующим законодательством РФ

Утверждена
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

Инструкция
по организации антивирусной защиты в информационной системе персональных данных

1.Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационной системы персональных данных от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и работников подразделений, эксплуатирующих и сопровождающих информационную систему за их выполнение.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, прошедшие установленным образом процедуру оценки соответствия и централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка средств антивирусного контроля на компьютерах серверах ЛВС ИСПДн осуществляется администратором ИСПДн. Настройка параметров средств антивирусного контроля осуществляется администратором ИСПДн и контролируется администратором безопасности ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех критичных областей ЭВМ (файлы автозагрузки, оперативная память, загрузочные сектора жестких дисков, каталоги операционных систем).

2.2. Обязательному антивирусному контролю подлежат любые файлы, которые могут содержать вредоносный код (анализ файлов производится по содержанию файлов, а не по файловому расширению), информация, получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM , DVD-ROM, Flash cards и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2.4. Установка (изменение) системного и прикладного программного обеспечения осуществляется только Администратором ИСПДн.

2.5. Факт выполнения установки (изменения) программного обеспечения должен регистрироваться средствами СЗИ от НСД в специальном электронном журнале и контролируется подразделением по защите информации.

2.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов,

искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник обязан привлечь Администратора ИСПДн для определения им факта наличия или отсутствия компьютерного вируса.

2.7. В случае обнаружения при проведении автоматической антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

_-приостановить работу;

-немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя отдела и ответственного за обеспечение информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

-провести совместно с Администратором ИСПДн или уничтожение зараженных файлов;

-в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

-по факту обнаружения зараженных вирусом файлов составить служебную записку в подразделение по защите информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3.Ответственность

3.1. Ответственность за организацию и проведение мероприятий антивирусного контроля, контроль за состоянием антивирусной защиты и выполнением требований настоящей Инструкции в ИСПДн возлагается на подразделение по защите информации.

4. Обозначения и сокращения

ИСПДн - информационная система персональных данных
ЛВС - локальная вычислительная сеть
НСД - несанкционированный доступ
ПДн - персональные данные
ЭВМ -электронно-вычислительная машина
СЗИ - средства защиты информации
СЗПДн - система (подсистема) защиты персональных данных

Утверждена
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

Инструкция
по организации резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных Службы ГО и ЧС Республики Тыва

1. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных Службы ГО и ЧС Республики Тыва (далее - ИСПДн).
2. Резервированию подлежат все общесистемные и специальные программные средства, программное обеспечение средств защиты информации и базы персональных данных. Периодичность резервного копирования основной информации осуществляется не реже одного раза в неделю. Резервное копирование общесистемных, специальных программ и программного обеспечения средств защиты информации производится не реже одного раза в месяц.
3. Допускается автоматическое резервирование (с помощью специальных программных средств) и ручное резервирование. Порядок автоматизированного резервирования определяется в соответствии с технической и эксплуатационной документацией средств резервного копирования. Ручное резервирование копирование основных файлов информационной системы персональных данных (ИСПДн) определяется настоящей инструкцией. При ручном копировании используется стандартные средства операционной системы или специальные программы записи данных на оптические носители информации оптические накопители типа CD или DVD. За хранение резервных копий при автоматическом копировании, ответственность за накапливаемый массив информации несет системный администратор или администратор безопасности. При ручном копировании ответственность возлагается на пользователей информационных ресурсов.
4. Восстановление информации при автоматическом резервировании происходит с помощью специальных программных средств. Восстановление не должно превышать 8 часов с момента потери или искажении информации. При ручном копировании информации пользователь может самостоятельно восстановить нужную информацию из ранее сохраненных копий массивов информации.

Утверждена
приказом Службы ГО и ЧС
Республики Тыва от «25» 06 2018г.
№ 94

Инструкция
по работе с ключевыми носителями в информационных системах обработки персональных данных

1. Общие положения

1.1. В информационных системах обработки персональных данных Службы ГО и ЧС Республики Тыва для обеспечения контроля за целостностью передаваемых по технологическим цепочкам ЭД, для подтверждения их подлинности и авторства используются средства электронной цифровой подписи, позволяющие работникам проставлять на ЭД персональные коды аутентификации (далее - КА). Применение КА позволяет следующим в технологической цепочке работникам убедиться, что документ не искажен и подготовлен именно тем работником, кому это предписано технологическим процессом.

1.2. Каждому работнику, которому в соответствии с его функциональными обязанностями предоставлено право постановки на ЭД кодов аутентификации, выдается персональный ключевой носитель.

1.3. Для организации двухфакторной аутентификации каждому пользователю ИСПДн выдается персональный ключевой носитель.

1.4. Персональный ключевой носитель - это аппаратный носитель информации, на который записана уникальная секретная ключевая информация («секретный ключ ЭЦП», идентификатор пользователя), и предназначенная для постановки уникального кода аутентификации (КА) конкретного работника на обработанные им ЭД или для авторизации в ИСПДн.

1.5. Информация («секретный» ключ ЭЦП работника, идентификатор пользователя), находящаяся на персональном ключевом носителе, относится к категории сведений ограниченного распространения и имеет гриф «Для служебного пользования» (ДСП).

1.6. Персональный ключевой носитель изготавливается в КЦ, или при помощи СЗИ от НСД.

1.7. В Службе ГО и ЧС Республики Тыва учет и хранение персональных ключевых носителей работников осуществляет администратор информационной безопасности который ведет «Журнал учета ключевых носителей».При изменении полномочий работника, его увольнения либо компрометации ключевого носителя уничтожается все ключевая информация, и подписывается акт об уничтожения ключевой информации с ключевых носителей.

1.8. Контроль за обеспечением безопасности технологии обработки электронных документов в АС, в том числе за действиями работников, выполняющих свою

работу с применением персональных ключевых носителей, осуществляется работниками отдела, ответственными за информационную безопасность.

2. Обязанности работника

2.1. Работник, которому в соответствии с его должностными функциями предоставлено право постановки на ЭД персональных КА, ОБЯЗАН:

-Лично присутствовать при изготовлении своего персонального ключевого носителя (от момента включения до момента выключения «АРМ генерации ключей»), чтобы быть уверенным в том, что содержание его ключевых носителей не компрометировано;

-Под роспись в «Журнале учета ключевых носителей»(Приложение №1) получить ключевые носители, убедиться, что они правильно маркированы.

-Сдавать свой персональный ключевой носитель на временное хранение ответственному за информационную безопасность на время длительного отсутствия работника на рабочем месте, в период отпуска и болезни и т.п.;

-В случае порчи ключевого носителя работник обязан передать его уполномоченному работнику, который в присутствии работника делает новую рабочую копию ключевого носителя. Все эти действия должны быть зафиксированы в «Журнале выдачи ключевых носителей» (Приложение №1).

2.2. Работнику запрещается:

-передавать свой персональный ключевой носитель другим лицам (кроме как для хранения лицу, ответственному за информационную безопасность в запечатанном конверте);

-оставлять персональный ключевой носитель без личного присмотра;

-делать неучтенные копии ключевого носителя

-подписывать своим персональным уникальным КА любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;

-сообщать кому-либо, что он является владельцем уникального КА для данного технологического процесса.

2.3. Если у работника появилось подозрение, что его персональный ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом работнику , ответственному за информационную безопасность, сдать ему скомпрометированный ключевой носитель, соблюдая обычную процедуру с пометкой в журнале о причине компрометации, написать объяснительную записку о факте компрометации персонального ключевого носителя на имя руководителя Службы ГО и ЧС Республики Тыва.

2.4. В случае утери персонального ключевого носителя работник обязан немедленно сообщить об этом работнику, ответственному за информационную безопасность,написать объяснительную записку об утере носителя на имя руководителя Службы ГО и ЧС Республики Тыва и принять участие в служебном расследовании факта утери персонального ключевого носителя.

2.5. В случае перевода работника на другую работу, увольнения и т.п. он обязан сдать (сразу по окончании последнего сеанса работы) свой персональный ключевой носитель лицу, ответственному за информационную безопасность под роспись в журнале учёта ключевых носителей.

3. Ответственность

3.1. Работник несет персональную ответственность за сохранность и правильное использование вверенной ему персональной ключевой информации и содержание документов, на которых стоит его персональный код аутентификации.

3.2. За нарушение положений данной Инструкции к работнику может быть применена дисциплинарная ответственность, а так же ответственность предусмотренная действующим законодательством РФ

4. Обозначения и сокращения

АС - автоматизированной системе;

ЗАРМ - защищаемое автоматизированное рабочее место;

ВП - вредоносная программа;

ИБ - информационная безопасность;

ИСПДн - информационная система персональных данных;

КА - коды аутентификации;

КЗ - контролируемая зона;

КЦ - ключевой центр;

МЭ - межсетевой экран;

НСД - несанкционированный доступ;

ПДн - персональные данные;

ПМВ - программно-математическое воздействие;

СЗИ - средства защиты информации;

СЗПДн - система (подсистема) защиты персональных данных; ЭД - электронные документы.

Приложение №1

Журнал
регистрации и выдачи ключевых носителей

Рег. №	Дата формирования ключевой информации	Вид ключевой информации	Наименование пользователя	Ф.И.О. администратора КЦ	Подпись	Отправлено (дд/мм/гг, подпись)	Получено (дд/мм/гг подпись)	Уничтожено (№ акта, дд/мм/гг)
1	2	3	4	5	6	7	8	9

Утверждаю
Руководитель Службы ГО и ЧС
Республики Тыва
« » 2017г.

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 _____
(Ф И О.)
(Подпись) **(Дата)**
Администратор ИБ _____
(Ф И О.)
(Подпись) **(Дата)**