Утверждена
распоряжением Администрации Главы
Республики Тыва и Аппарата
Правительства Республики Тыва
от « 21 » августа 2013 г. № 154-РА

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 Администрации Главы Республики Тыва и Аппарата Правительства Республики Тыва (далее – Администрация Главы 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 подразделения.

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 структурного подразделения

Администрации Главы Республики Тыва 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 НСД;

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.