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

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