Приложение 2, утвержденное приказом №74 от 12.07.2010

Инструкция об организации антивирусной защиты в Управлении Роспотребнадзора по ЕАО.

г. Биробиджан

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с руководящим документом ФСТЭК России «Средства защиты информации. Антивирусные средства» и предназначена для сотрудников Управления Роспотребнадзора по ЕАО (далее - Управления).

1.2. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

1.3. Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля.

2. Требования к порядку организации антивирусной защиты

2.1. В Управлении к применению допускаются, лицензионные сертифицированные Федеральной службой технического и экспортного контроля Российской Федерации (далее – ФСТЭК России) антивирусные программные средства, закупленные Управлением у официального дистрибутора указанных средств.

2.2. Установка, настройка и регулярное обновление антивирусных средств осуществляется сотрудниками Управления.

2.3. Разработка инструкций и проведение антивирусного контроля осуществляется администратором информационной безопасности в Управлении.

3. Требования по обеспечению антивирусной защиты

3.1. Сотрудники Управления не должны допускать присутствия и использования на персональных компьютерах (далее – ПК) любого программного обеспечения (далее – ПО) не связанного с выполнением своих должностных обязанностей (функций своего подразделения в технологическом процессе).

3.2. Установка (изменение) системного и прикладного программного обеспечения на персональных компьютерах, а также в системах и средствах обработки передачи и хранения информации, должна осуществляться только администратором информационной безопасности в Управлении. Устанавливаемое (изменяемое) программное обеспечение необходимо предварительно проверить на отсутствие вредоносных программ – компьютерных вирусов. После установки (изменения) программного обеспечения на ПК, должна быть выполнена полная проверка на отсутствие программ-вирусов.

3.3. Обязательному дополнительному антивирусному контролю подлежит любая информация (файлы любых форматов, файлы баз данных, исполняемые файлы и т.д.), получаемая и передаваемая по телекоммуникационным каналам, сети Интернет, а также информация со съемных носителей (магнитные диски, ленты, CD-ROM, DVD-ROM, USB-устройства и т.п.).

Антивирусный контроль входящей информации со съемных носителей из внешних сетей передачи данных необходимо проводить на съемных носителях, до переноса информации на жёсткий диск ПК или сетевой диск ЛВС.

Информация, получаемая по телекоммуникационным каналам, должна проверятся во время, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

3.4. При возникновении подозрения на наличие компьютерного вируса сотрудник Управления должен произвести внеочередной антивирусный контроль, или при необходимости – привлечь администратора информационной безопасности для определения факта наличия или отсутствия компьютерных вирусов и принятия соответствующих мер.

3.5. Периодичность проведения антивирусного контроля приведена в Приложении № 1 к Инструкции.

При обнаружении компьютерного вируса сотрудник Управления **обязан**:

- приостановить свою работу на ПК;
- поставить в известность о факте обнаружения зараженных вирусом файлов начальника отдела, владельца этих файлов, смежные отделы, использующие эти файлы;
- сообщить о факте обнаружения администратору информационной безопасности.

4. Ответственность при организации антивирусного контроля

4.1. Ответственность за организацию и сопровождение антивирусной защиты в Управлении в соответствии с требованиями настоящей Инструкции, возлагается на администратора информационной безопасности.

4.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на пользователей автоматизированных рабочих мест Управления.

4.3. Периодический контроль за выполнением всех требований настоящей Инструкции и состоянием антивирусной защиты отдельных компьютеров, систем и сетей осуществляется администратором информационной безопасности.

Приложение № 1 к Инструкции

Периодичность антивирусного контроля

Вид проверяемой информации	Расположение проверяемой информации	Средство проверки	Периодичность проверки	Проверяющий
Вновь устанавливаемое общесистемное ПО	Сервер ЛВС	Антивирус Касперского	Перед установкой	Администратор
Вновь устанавливаемое прикладное ПО	Рабочая станция	Антивирус Касперского	Перед установкой	Администратор
Входящие файлы, полученные по телекоммуникационным каналам, из сторонних сетей	Рабочая станция (почтовый клиент, пользователь Интернет)	Антивирус Касперского	Во время получения файлов, сразу после получения	Пользователь рабочей станции
Исходящие файлы, передаваемые по телекоммуникационным каналам	Рабочая станция (почтовый клиент)	Антивирус Касперского	После формирования файла, перед его отправкой	Пользователь рабочей станции
Файлы, полученные на съемных носителях информации	Съемный носитель информации	Антивирус Касперского	Перед обработкой полученной информации	Пользователь рабочей станции
Файлы, записываемые на сервера ЛВС	Локальные диски рабочей станции	Антивирус Касперского	Антивирусный монитор (постоянно)	Пользователь рабочей станции
Файлы, находящиеся на локальных дисках ПК	Локальные диски рабочей станции	Антивирус Касперского	Один раз в неделю	Пользователь рабочей станции
Файлы, находящиеся на дисках сервера ЛВС	Дисковые накопители серверов	Антивирус Касперского	Один раз в неделю	Администратор