

ИНСТРУКЦИЯ

по организации антивирусной защиты информационной системы персональных данных

1. Общие положения

Инструкция устанавливает требования антивирусной безопасности для информационной системы персональных данных (ИСПДн) некоммерческой организации «Фонд капитального ремонта многоквартирных домов Владимирской области» (далее по тексту - Фонд).

2. Общие требования

Антивирусные средства защиты должны быть лицензионными и иметь сертификат соответствия требованиям безопасности, выданный Федеральной службой по техническому и экспортному контролю (ФСТЭК) России.

Закупка средств антивирусной защиты должна быть централизованной. Все элементы ИСПДн рекомендуется оснащать одним антивирусным программным продуктом.

Параметры антивирусной политики задаются начальником отдела информационно-технического обеспечения.

Реализация параметров антивирусной политики осуществляется начальником отдела информационно-технического обеспечения.

Антивирусные средства защиты должны функционировать исправно и непрерывно. При сбоях в работе требуется немедленное вмешательство начальника отдела информационно-технического обеспечения для устранения неполадок.

При выборе антивирусных средств необходимо так же учитывать его быстродействие, для того, чтобы не перегружать системные процессы автоматизированного рабочего места и не создавать затруднений для работы пользователей ИСПДн.

3. Параметры антивирусной политики

Основными параметрами антивирусной политики являются периодичность обновления антивирусных баз, периодичность проверки наличия/отсутствия вирусных заражений и параметры проверки «на лету» при работе в сети Интернет.

Обновление антивирусных баз должно осуществляться по мере выхода новых баз. Для этого необходимо настроить каждое автоматизированное рабочее место ИСПДн на обновление из сети Интернет.

Периодичность проверки наличия/отсутствия вирусных заражений настраивается в консоли управления антивирусным средством и применяется на каждом автоматизированном рабочем месте ИСПДн. Данный параметр устанавливается на один раз в неделю (в любой день) на обеденный перерыв. Проверке должны подвергаться все разделы жесткого диска автоматизированного

рабочего места. На автоматизированных рабочих местах ИСПДн такие настройки делаются непосредственно на месте начальником отдела информационно-технического обеспечения.

Параметры проверки «на лету» при работе в сети Интернет должны включать в себя все возможные объекты реагирования. На автоматизированных рабочих местах ИСПДн такие настройки делаются непосредственно на месте начальником отдела информационно-технического обеспечения.

4. Порядок работы со средствами антивирусного контроля

На каждое автоматизированное рабочее место ИСПДн начальником отдела информационно-технического обеспечения устанавливается и настраивается антивирусное средство защиты.

Каждый пользователь автоматизированного рабочего места ИСПДн не должен препятствовать обновлению антивирусных баз или проверке наличия/отсутствия вирусных заражений, а так же реагировать на предупреждения антивирусного средства защиты при работе в сети Интернет, если при проверке «на лету» обнаружено вредоносное программное обеспечение или вирус.

Каждый пользователь ИСПДн в обеденный перерыв определенного дня недели, заранее оговоренного с начальником отдела информационно-технического обеспечения, должен оставлять свое автоматизированное рабочее место во включенном состоянии, для еженедельной проверки на наличие/отсутствие вирусных заражений.

Проверке на заражение подлежат файлы, полученные по электронной почте. В данном случае достаточно одним щелчком правой клавишей мыши на файле вызвать меню и выбрать в нем проверку на вирусы. В случае если файл заражен, обратиться к отправителю с просьбой повторно отправить не зараженный файл. Работа с зараженными файлами категорически запрещена.

При подозрении на вирусное заражение автоматизированного рабочего места, пользователь должен незамедлительно сообщить об этом ответственному за организацию обработки ПДн и начальнику отдела информационно-технического обеспечения. Работу на компьютере необходимо приостановить, базу данных с ПДн закрыть.

Признаками вирусного заражения являются:

- работоспособность компьютера значительно снижается;
- компьютер «подвисает»;
- появляются различного рода диалоговые окна Интернет-характера;
- самопроизвольно открываются/закрываются используемые в работе проводниковые окна, файлы, программы;
- появление на экране монитора баннера рекламного или эротического характера.

5. Последствия вирусных заражений

Антивирусная безопасность ИСПДн является неотъемлемой составной частью системы защиты ПДн.

Вирусное заражение одного автоматизированного рабочего места ИСПДн может вызвать заражение сегмента или всей локально-вычислительной системы.

Такое заражение выводит из строя все автоматизированные рабочие места. Серьезные вирусные заражения не «лечатся», и при возникновении такого заражения пользователь не имеет возможности сохранить последние данные, с которыми он работал, файлы, расположенные на жестком диске его компьютера, и восстановление работоспособности возможно только путем переустановки операционной системы. В этом случае пользователь теряет рабочее время и данные со своего компьютера.