Утверждено
приказом МБУК «ЦБС» города Смоленска
от 16.06.2017 г. № 49/1

ИНСТРУКЦИЯ
по организации антивирусной защиты информационной системы персональных данных

1. Инструкция устанавливает требования антивирусной безопасности для информационной системы персональных данных (ИСПДн) МБУК «ЦБС» города Смоленска в целом и их элементов в частности.
2. Общие требования

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

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

Параметры антивирусной политики задаются ответственным за организацию обработки ПДн.

Реализация параметров антивирусной политики осуществляется инженером-программистом.

Антивирусные средства защиты должны функционировать исправно и непрерывно. При сбоях в работе требуется немедленное вмешательство инженера-программиста 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 Интернете.

Обновление антивирусных баз должно осуществлять по мере выхода новых баз. Для это 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 подвергается все разделы жесткого диска автоматизированного рабочего места. На автоматизированных рабочих местах ИСПДн такие настройки делаются непосредственно на месте

инженером-программистом.

Параметры проверки «на лету» при работе в Интернете должны включать в себя все возможные объекты реагирования. На автоматизированных рабочих местах ИСПДн такие настройки делаются непосредственно на месте инженером-программистом.

4. Порядок работы со средствами антивирусного контроля

На каждое автоматизированное рабочее место ИСПДн инженером-программистом 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 заместителем директора по автоматизации и информационным технологиям, должен оставлять свое автоматизированное рабочее место во включенном состоянии, для еженедельной проверки на наличие/отсутствие вирусных заражений.

Каждый пользователь при работе со съемными носителями ПДн (дискеты, диски, USB-носители, съемные жесткие диски, карты памяти, в том числе в составе мобильного телефона) должен перед использованием носителя проверить его на наличие вирусов или вредоносного программного обеспечения. Для этого необходимо:

– подключить/вставить в системный блок своего компьютера или ноутбука носитель;

– двойным щелчком левой клавиши мыши открыть ярлык «Мой компьютер»;

– в открывшемся окне проводника найти носитель;

– одни щелчком правой клавиши мыши вызвать «выплывающее» меню и выбрать в нем проверку на вирусы. Обычно данный пункт меню имеет эмблему и название антивирусного средства, установленного на автоматизированном рабочем месте;

– дождаться окончания проверки и при отрицательном результате начать работу с носителем;

– при положительном результате проверки, при условии невозможности «вылечить» зараженный файл, пользователь должен обратится к инженеру-программисту или ответственному за организацию обработки ПДн, но не начинать работу с носителем.

Инженер-программист или ответственный за организацию обработки ПДн, при обращении к ним пользователей ИСПДн с зараженными носителями ПДн должны еще раз проверить носитель, выяснить причину невозможности «вылечить» зараженный файл (например, устаревшая

антивирусная база) и по возможно удалить этот файл.

Проверке на заражение так же 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, обратится 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 заместителю директора по автоматизации и информационным технологиям. 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.