Кировский муниципальный район Ленинградской области
Муниципальное бюджетное учреждение дополнительного образования
«Кировский центр информационных технологий»
187341, г. Кировск, ул. Кирова, д.8

УТВЕРЖДЕНО
Директор МБУДО « Кировский ЦИТ»
_____ Н.Н.Вахренева
Приказ № 39
от «04»февраля 2016 года

Инструкция

по организации антивирусной защиты

в МБУДО «Кировский ЦИТ»

Общие положения

Настоящая Инструкция определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) МБУДО «Кировский ЦИТ» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

ИСПДн (Информационная система персональных данных) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

К использованию в МБУДО «Кировский ЦИТ» допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению отделами автоматизации и безопасности информации.

Установка средств антивирусного контроля на компьютерах на серверах и рабочих станциях ИСПДн осуществляется уполномоченными сотрудниками инженерной службы МБУДО «Кировский ЦИТ».

Настройка параметров средств антивирусного контроля осуществляется сотрудниками МБУДО «Кировский ЦИТ» в соответствии руководствами по применению конкретных антивирусных средств.

Применение средств антивирусного контроля

Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться не реже чем раз в три дня в автоматическом режиме.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистого" (не зараженного вирусами) и защищенного носителя информации. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в 3 месяца.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после

установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка:

• на защищаемых серверах и рабочих станциях ИСПДн - ответственным за обеспечение информационной безопасности подразделения;

• на других серверах и рабочих станциях, не требующих защиты ИСПДн - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

Действия при обнаружении вирусов

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.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь сотрудников инженерной службы МБУДО «Кировский ЦИТ» для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

• приостановить работу;

• немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя 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 лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов инженерной службы МБУДО «Кировский ЦИТ»);

• по факту обнаружения зараженных вирусом файлов составить служебную записку в инженерную службу МБУДО «Кировский ЦИТ», 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.

Ответственность

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем подсистему АС, в соответствии с требованиями настоящей Инструкции возлагается на главного инженера МБУДО «Кировский ЦИТ».

Ответственность за проведение мероприятий антивирусного контроля в учреждении и соблюдение требований настоящей Инструкции возлагается на главного инженера МБУДО «Кировский ЦИТ».

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений организации осуществляется инженерной службой МБУДО «Кировский ЦИТ».