

Министерство образования и молодежной политики Свердловской области
государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский горнозаводской колледж имени Демидовых»

Рассмотрено
на заседании Совета
автономного учреждения
№ протокола 5
« 03 » 07 2020 г.

Введено в действие приказом
№ 448 от « 03 » 07 2020 г.

**ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ГАПОУ СО «УрГЗК»**

1. Общие положения

1.1. Настоящая Инструкция по организации антивирусной защиты информационной системы персональных данных в государственном автономном профессиональном образовательном учреждении Свердловской области «Уральский горнозаводской колледж имени Демидовых» (далее – инструкция) определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность администратора безопасности ИСПДн, ответственного за обеспечение безопасности персональных данных (далее – ПДн), и сотрудников государственного автономного профессионального образовательного учреждения Свердловской области «Уральский горнозаводской колледж имени Демидовых» (далее – колледж), эксплуатирующих и сопровождающих ИСПДн, за выполнение требований по организации антивирусной защиты.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка средств антивирусного контроля на серверах и рабочих станциях пользователей ИСПДн осуществляется сотрудником колледжа, уполномоченным на техническое сопровождение ИСПДн (далее – специалист), в соответствии с инструкцией по эксплуатации средств защиты информации.

1.4. Настройка параметров средств антивирусного контроля осуществляется специалистами в соответствии с руководствами по применению конкретных антивирусных средств.

1. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

2.2. 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 (магнитных дисках, лентах, CD - ROM и т.п.).

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 «чистой» (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере.

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).

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. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения (далее – ПО) компьютера должна быть выполнена антивирусная проверка на защищаемых серверах и автоматизированных рабочих местах (далее – АРМ) администратором безопасности ИСПДн.

2.5. Факт выполнения антивирусной проверки после установки (изменения) ПО должен регистрироваться в журнале учета мероприятий по обеспечению защиты персональных данных за подписью лица, установившего (изменившего) ПО, и лица, его контролировавшего.

2. Действия при обнаружении вирусов

3.1. 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 колледжа самостоятельно или вместе с

администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

3.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники колледжа обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИСПДн, 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 специалиста).

3. Ответственность

4.1. Ответственность за организацию антивирусного контроля в колледже, в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИСПДн.

4.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности ПДн и всех сотрудников, являющихся пользователями автоматизированной системы.

4.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками колледжа, осуществляется ответственным за обеспечение безопасности ПДн.

5. Срок действия Инструкции

5.1. Настоящая Инструкция вступает в силу с момента ее утверждения и отменяет ранее действующую Инструкцию по организации антивирусной защиты информационной системы персональных данных.

5.2. Инструкция принимается на Совете автономного учреждения и утверждается директором.

5.3. Порядок внесения изменений в Инструкцию аналогичен порядку ее принятия.

5.4. Настоящая Инструкция действует до принятия новой Инструкции, регулирующей однородные отношения.