

УТВЕРЖДАЮ



О.А. Филиппова  
2018 г.

## **ИНСТРУКЦИЯ по организации антивирусной защиты в МАОУ СОШ № 45 города Тюмени**

### **1. Общие требования**

1.1. Настоящая инструкция определяет требования к организации защиты автоматизированной системы объекта информатизации (АС) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителя и сотрудников отдела, эксплуатирующих и сопровождающих АС, за их выполнение. Инструкция распространяется на все АС существующие и вновь разрабатываемые в структурных подразделениях. Для отдельных АС могут быть разработаны свои инструкции, учитывающие особенности работы АС.

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

1.3. Установка и настройка средств антивирусного контроля на компьютерах (серверах) АС осуществляется администратором защиты АС или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. Данные требования не распространяются на рабочие станции с установленными операционными системами, для которых отсутствуют какие-либо средства антивирусного контроля.

### **2. Применение средств антивирусного контроля**

2.1. В начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов рабочих станций. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), 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. 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).

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

2.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), администратором защиты АС должна быть выполнена антивирусная проверка на защищаемых серверах и рабочих станциях.

2.4. 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 администратором защиты АС должен провести внеочередной антивирусный контроль своей рабочей станции.

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

- приостановить работу в АС;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора защиты, 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.

2.5. Не реже одного раза в неделю проводить обновление антивирусных баз в установленном порядке.

### **3. Ответственность**

3.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения эксплуатирующего объект информатизации.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей инструкции возлагается на администратора защиты и пользователей АС.

3.3. Периодический контроль за состоянием антивирусной защиты в АС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции осуществляется ответственным по защите информации на данном объекте.