

УТВЕРЖДЕНА

Приказом директора областного  
государственного бюджетного  
учреждения «Комплексный центр  
социального обслуживания  
Еврейской автономной области»

от 09.01 2019 г. № 19

**ИНСТРУКЦИЯ**  
**по проведению антивирусного контроля**  
**в ОГБУ «КЦСО ЕАО»**

1. Общие требования

1.1. Настоящая инструкция определяет требования к организации защиты АРМ, хранящих защищаемую информацию, от разрушающего воздействия компьютерных вирусов и устанавливает ответственность оператора и сотрудников, эксплуатирующих АРМ, за их выполнение.

1.2. Инструкция распространяется на все АРМ существующие и вновь приобретаемые в ОГБУ «КЦСО ЕАО». Для отдельных АРМ могут быть разработаны свои инструкции, учитывающие особенности работы.

1.3. К использованию на АРМ, допускаются только лицензионные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

1.4. Установка и настройка средств антивирусного контроля на АРМ осуществляется администратором безопасности или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

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

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке системы (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, CD-ROM). 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 безопасности информации 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.) работник самостоятельно или вместе с администратором безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции.

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

- приостановить работу с АРМ;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора 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;

2.5. Ярлык для запуска антивирусной программы должен быть вынесен в окно «Рабочий стол» операционной системы Windows.

### 3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на оператора эксплуатирующего АРМ.

3.2. Ответственность за проведение мероприятий антивирусного контроля в отделе и соблюдение требований настоящей Инструкции возлагается на администратора безопасности и всех работников, являющихся пользователями АРМ.

3.3. Периодический контроль за состоянием антивирусной защиты на АРМ, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется ответственным за обеспечение безопасности персональных данных.

Подготовил:  
Специалист по технической поддержке

Согласовано:  
Администратор  
безопасности информации