Приложение к приказу № 46-УД
От 11 ноября 2022года

Регламент
организации антивирусной защиты МАОДО «ДШИ им. А.В.Ливна»

1. Общие положения

1.1 Настоящий Регламент разработан с целью определения системы мер направленных на защиту автоматизированных рабочих мест и сервера МАОДО «ДШИ им.А.В.Ливна» (далее – учреждение) от вредоносною программного обеспечения.
1.2 Настоящий Регламент устанавливает требования к конфигурации системы антивирусной зашиты учреждения и к мероприятиям, обеспечивающим поддержание этой системы в работоспособном состоянии.
1.3 Настоящем Регламенте используются следующие основные термины и понятия:

- антивирусное программное обеспечение (Антивирус) – специализированный комплекс программных средств, обеспечивающий функции предотвращения, защиты и восстановления компьютера от действий вредоносного программного обеспечения (далее – ПО).
- вредоносное ПО (Вирус) категория специально разработанного ПО, запуск и воспроизведение которого влечет за собой сбои в работе автоматизированного рабочего места (далее - АРМ) и серверов, несанкционированную модификацию, повреждение, удаление или кражу информации, ПО возможность несанкционированного и скрытного использования компьютерного оборудования,в том числе в противоправных целях.
- заражение вредоносным ПО – компьютерный процесс, в результате которого вредоносное ПО начинает свое функционирование в составе другого ПО или самостоятельно. Заражение может осуществляться без участия пользователя за счет автоматического использования вредоносным ПО уязвимостей системного ПО, так и с участием пользователя, самостоятельно запускающего вредоносное ПО.
- лечение вредоносного ПО – компьютерный процесс, в результате которою вредоносное ПО или его компоненты блокируются для запуска и удаляются с носителей информации, а модифицированные вирусом файлы восстанавливаются до первоначального состояния путем удаления из него компонентов вредоносногоПО.

1.4.На серверах и всех АРМ временно или постоянно подключаемых к информационным активам учреждения, должно быть установлено лицензионное и сертифицированное для применения на территории РФ и антивирусное ПО состав и конфигурация которого соответствует требованиям настоящего Регламента.
1.5.Запрещается несанкционированная деинсталляция или деактивация антивирусного ПО, а также изменение его настроек.
1.6.Администрирование средств антивирусной зашиты осуществляется ответственным лицом с помощью специализированных средств входящих н составантивирусного ПО.
1.7.Техническое сопровождение средств антивирусной защиты осуществляется ответственным лицом.

2. Требования к структуре и составу средств антивирусной защиты

2.1. Защита информационных активов учреждения от компьютерных вирусов достигается за счет внедрения и подержания в работоспособном состоянии комплексной системы антивирусной защиты предназначенной дли решения следующих задач:

- перекрытия всех возможных каналов распространения вирусов, к числу которых относятся: электронная почта, протоколы передачи информации телекоммуникационной сети учреждения, съемные носители, носители информации н составе АРМ и сервера, папки общего пользования на файловом сервере;

- непрерывный антивирусный мониторинг и периодическое антивирусное сканирование всех серверов и рабочих станций, подключаемых к локальной сети: автоматическое реагирование па заражение компьютерными вирусами и на вирусные эпидемии, включающее в себя: оповещения, лечение (удаление) вирусов н комплексную проверку информационной системы, подвергнувшейся заражению.

2.2.Система комплексной антивирусной защиты строится из следующих компонентов и средств:
- антивирусной защиты серверов: антивирусной зашиты АРМ:
- антивирусной защиты сервера электронной почты:
- антивирусной зашиты сетевою трафика, возникающего при работе с ресурсами публичных сетей передачи данных.

2.3.Для повышения уровня зашиты информационных активов от вирусов на АРМ и серверах следует использовать, антивирусное ПО различных производителей.

2.4.Для проверки и блокирования действий вредоносных сетевых потоков данных допускается использовать специализированные программно-аппаратные комплексы антивирусной зашиты, сертифицированные для применения н» территории РФ.

3. Требования к конфигурации средств антивирусной защиты

3.1.Требования к сканированию по расписанию:
- антивирусное сканирование серверов и АРМ по расписанию производится не реже чем раз в неделю;
- в ходе сканирования по расписанию осуществляется проверка всех файлов (вне зависимости от их типа), а также оперативной памяти и загрузочных секторов подключенных носителей информации;
- в случае обнаружения вируса должна осуществляться попытка лечения с предварительным безопасным сохранением резервной копии файла.
- в случае неудачного лечения, зараженный файл отравляется в карантинную зону: сканирование АРМ так же должно осуществляться при включении АРМ.

3.2.Параметры сканирования в реальном времени:
- на всех АРМ и файловых серверах должна быть включена опция сканирования в реальном времени. Автоматической проверке должны подвергаться все файлы, к которым осуществляется доступ, или которые создаются вновь;
- на рабочих станциях осуществляется проверка подключенных съёмных носителей информации, загрузочных областей, сжатых файлов иOLE-контейнеров;
- должны быть настроены фильтры интернет-контента.
- Антивирусные средства должны обеспечивать перехват и блокировку выполнения скриптов, размещенных на веб-странице, если их запуск может нанести вред системе; антивирусная защита должна включать в себя средства отслеживания обращений к сетевым ресурсам, поддерживать блокировку переходов на ресурсы с вредоносным ПО блокировку передачи вредоносных данных при осуществлении сетевых подключений;
- антивирус должен осуществлять проверку и защиту создаваемых, отправляемых и получаемых работниками учреждения сообщений электронной почты от угроз со стороны вредоносною ПО;
- в ходе сканирования в реальном времени производится проверка типов файлов, потенциально подверженных заражению компьютерными вирусами. Перечень типов файлов предоставляется и поддерживается в актуальном состоянии разработчиком антивирусного ПО;
- в случае обнаружения вируса реализуется набор автоматических действий по реагированию, предусмотренный разработчиком антивирусного ПО для данного типа вируса: антивирусное ПО так же должно поддерживать функции анализа активности установленного ПО, мониторинга реестра операционных систем семейства Microsoft Windows (или иной операционной системы установленной на ПК), межсетевого

экрана, обнаружения сетевых атак и вторжений.

3.3. Возможности деактивации и деинсталляция антивирусного ПО а также изменения настроек (за исключением настроек ручного сканирования рабочих станций) должны быть недоступны для пользователей.
3.4. Антивирусное ПО должно оповещать пользователя о критичных событиях на АРМ, связанных с выявлением деятельности вредоносного ПО.
3.5. Обновление ПО и баз данных антивирусной защиты должно осуществляться ежедневно, с учетом выпуска соответствующих обновлений разработчиком антивирусного ПО. Резервные копии БД конфигурации антивирусных средств создаются еженедельно. Данные копии хранятся в течение одного месяца.

4. Требовании к контролю функционировании средств антивирусной зашиты

4.1. Все события, связанные с обнаружением и лечением вирусов, изменением состояния антивирусных средств, установкой и распространением обновлений должны протоколироваться.
4.2. Локальная сеть учреждения должна провериться специалистом по защите информации на регулярной основе, не реже чем один раз в неделю и в рабочее время, с целью выявления АРМ и серверов, на которых не установлено антивирусное ПО. В случае выявления нарушений, данные АРМ и сервера должны быть максимально ограничены в сетевых подключениях к локальной сети до момента установки на них антивирусного ПО с актуальными базами защиты от угроз.
4.3. Специалистом но защите информации должны рассылаться посредством электронной почты предупреждающие сообщения пользователям в следующих случаях:
- при обнаружении вирусной эпидемии;
- в случае изменения конфигурации компонентов антивирусной защиты, существенно влияющей на функционирование АРМ и информационных систем.

4.4. В случае выявления серверов или АРМ, являющихся источниками заражения вирусами, которые не удается вылечить стандартными средствами, демонстрирующих в работе признаки заражения неизвестными вирусами и потенциальную опасность источника вирусных эпидемий, данные компьютеры должны быть отключены от локальной сети до момента устранения выявленных угроз.
4.5. Для точного определения потенциальной угрозы со стороны неизвестных файлов или сайтов сети Интернет, но которые предположительно содержат в себе полезную информацию или ПО, следует использовать публичные сервисы проверки подозрительных файлов и ссылок. Оценка степени угрозы для файлов и сайтов осуществляется исключительно специалистом по защите информации.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты возлагается на программиста учреждения.
5.2. Ответственность за проведение мероприятий антивирусного контроля в учреждении возлагается на программиста учреждения.
5.3. Ответственность за соблюдение требований настоящего Регламента при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу класса, оборудованного АРМ и другой компьютерной техники.