Приложение № 2
к приказу ГАПОУ МИК
от «___»_____20___ года №_____

УТВЕРЖДАЮ
Директор ГАПОУ МИК
И.В.Горшкова
«___»_____2021г.

ПОЛОЖЕНИЕ
об организации антивирусной защиты в
ГАПОУ МИК

I. Общие положения

1. Настоящее Положение разработано во исполнение федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», с учетом ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» и устанавливает порядок антивирусной защиты и антивирусного контроля в ГАПОУ МИК (далее – образовательное учреждение).

2. Настоящее Положение разработано в целях осуществления антивирусной защиты информационных ресурсов образовательного учреждения.

3. Целью мероприятий по антивирусной защите является:

защита информационных ресурсов образовательного учреждения от несанкционированного копирования, искажения и разрушения;

минимизация риска отказов и нестабильной работы технологических и информационных процессов, при воздействии вирусов и других вредоносных программ;

минимизация финансовых, репутационных потерь и трудовых затрат при устранении последствий воздействия вредоносного кода.

4. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в образовательном учреждении.

5. Требования настоящего Положения распространяются на сотрудников образовательного учреждения и применяются для всех объектов информатизации, эксплуатируемых в образовательном учреждении.

6. Антивирусная защита в образовательном учреждении построена на ролевой модели.

II. Термины, определения, сокращения

Пользователь САВЗ – пользователь ОИ, на котором установлен САВЗ.

САВЗ – средство антивирусной защиты.

ОИ – объект информатизации. В данное понятие входят серверы, компьютеры, планшеты, смартфоны (устройства, операционная система которых позволяет установить САВЗ).

Компьютерный вирус – это программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей без ведома пользователя.

III. Распределение ролей и ответственности в системе антивирусной защиты

7. Администратор антивирусной защиты:

производит установку, настройку САВЗ на серверах, компьютерах пользователей и контролирует их работу;

осуществляет мониторинг работы САВЗ серверов и компьютеров пользователей;

предпринимает необходимые действия по отражению и устранению последствий вирусных атак;

участвует в анализе вирусных инцидентов и предлагает меры по повышению защищенности сети образовательной от угрозы вирусных атак.

8. Ответственный за антивирусный контроль:

разрабатывает и согласовывает требования к системе антивирусной защиты;

осуществляет мониторинг работы САВЗ серверов и компьютеров пользователей;

регистрирует вирусные инциденты и информирует об их возникновении руководство образовательного учреждения;

совместно с системными администраторами участвует в анализе вирусных инцидентов и предлагает меры по повышению защищенности сети образовательного учреждения от угрозы вирусных атак;

оформляет инцидент информационной безопасности при поступлении информации об обнаружении вредоносного кода от пользователя САВЗ или системного администратора.

9. Каждый работник образовательного учреждения выполняет роль «пользователя САВЗ».

10. Пользователь САВЗ при обнаружении вредоносного кода (получение оповещения САВЗ) обязан:

прекратить (приостановить) свою работу на ОИ;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, ответственного за антивирусный контроль, а также смежные подразделения, использующие эти файлы в работе;

оценить необходимость дальнейшего использования файлов, зараженных вирусом;

провести «лечение» или уничтожение зараженных файлов. При необходимости для выполнения требований данного пункта следует привлечь администратора антивирусной защиты.

11. Пользователю САВЗ запрещается отключать средства антивирусной защиты информации.

12. Роли «администратор антивирусной защиты» и «ответственный за антивирусный контроль» согласно ролевой модели текущего раздела назначаются приказом руководителя образовательного учреждения.

13. Роли «администратор антивирусной защиты» и «ответственный за антивирусный контроль» входят в функции ответственного за информационную безопасность.

14. Каждый работник образовательного учреждения несет ответственность за невыполнение или недобросовестное выполнение перечисленных выше обязанностей согласно назначенной роли. Руководители структурных подразделений несут ответственность за ознакомление работников подразделений с настоящим Положением.

IV. Порядок применения средств антивирусной защиты информации

15. САВЗ устанавливаются на всех объектах информатизации, эксплуатируемых в образовательном учреждении. При технологической необходимости на отдельные средства вычислительной техники САВЗ могут не устанавливаться, список исключений утверждается ответственным за антивирусный контроль. САВЗ устанавливается централизованно. Допускаются исключения в централизованной установке, список ОИ, не содержащих САВЗ, утверждается ответственным за антивирусный контроль.

16. Все САВЗ работает в режиме мониторинга в реальном времени. САВЗ проверяют все файлы на локальных и сетевых жестких дисках, съемных носителях, в приложениях к письмам электронной почты, загружаемых из сети Интернет и др., к которым обращается операционная система. Отключение САВЗ допускается только с разрешения ответственного за антивирусный контроль в исключительных случаях.

17. Проверка критических областей операционной системы и загрузочных секторов накопителей информации ОИ проводится автоматически САВЗ при каждой загрузке операционной системы.

18. Полная проверка всех накопителей информации ОИ проводиться САВЗ автоматически ежемесячно по расписанию.

19. В случае наличия признаков вредоносных программ пользователь САВЗ обязан незамедлительно произвести внеплановую полную проверку накопителей информации ОИ и отчуждаемых носителей и создать условия для ее завершения (не извлекать носитель, не останавливать проверку, т.п.).

20. Обновление антивирусных баз проводиться автоматически по централизованно установленному расписанию не реже одного раза в сутки. Не допускается отключение автоматического обновления САВЗ. В случае невозможности автоматического обновления, обновление баз производится вручную системным администратором с той же периодичностью.

21. При подключении к ОИ отчуждаемого накопителя информации автоматически проводится полная его проверка на наличие вредоносного кода.

22. САВЗ настроено на автоматическое удаление или блокировку исполнения обнаруженного вредоносного кода.

23. К использованию в образовательном учреждении допускаются только централизованно закупленные лицензионные САВЗ, распространяемые ответственным за антивирусный контроль.

24. В случае необходимости использования сторонних САВЗ, их применение необходимо согласовать с ответственным за антивирусный контроль.

25. При обнаружении вирусов на ОИ, работающем в локальной сети (широковещательном сегменте локальной сети), проверке подлежат все ОИ, включенные в эту сеть и работающие с общими данными и программным обеспечением.

V. Признаки вредоносных программ

26. Для проведения полной внеплановой проверки накопителей информации ОИ и отчуждаемых носителей определены следующие признаки вредоносных программ:

прекращение работы или неправильная работа ранее успешно функционировавших программ;

медленная работа компьютера;

невозможность загрузки операционной системы;

исчезновение файлов и каталогов или искажение их содержимого;

изменение даты и времени модификации файлов;

изменение размеров файлов;

неожиданное значительное увеличение количества файлов на диске;

существенное уменьшение размера свободной оперативной памяти;

вывод на экран непредусмотренных сообщений или изображений;

подача звуковых сигналов системным блоком, не свойственных при обычной работе;

потеря работоспособности или частые зависания в работе компьютера.

государственное автономное профессиональное образовательное учреждение «медногорский индустриальный колледж» г.медногорска оренбургской области (ГАПОУ МИК)

Разработчик:
Администратор
информационной безопасности Горелов С.Н.

Согласовано:
Зам. директора по БОП В.А.Малин