УТВЕРЖДАЮ
Директор
_____ К.В.Багмет
Приложение №4 к приказу №26
от «29» апреля 2019 года

ПОЛИТИКА
антивирусной защиты
ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы»

1. Общие положения

Данный документ устанавливает требования и процедуры защиты информации, содержащейся и обрабатываемой в ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы» (далее – Центр ДПО), от несанкционированного копирования, модификации и разрушения, а также нарушении работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ (далее – антивирусная защита).

Средства антивирусной защиты информации (далее – САЗ) должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в Учреждении. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты информации могут не устанавливаться, по письменному согласованию с директором Центра ДПО.

Директор Центра ДПО организует проведение работ по антивирусной защите в Центре ДПО.

Установка, управление и мониторинг работы средств антивирусной защиты в Центре ДПО осуществляется администратором средств антивирусной защиты.

Обязанности по выполнению предписанных мер антивирусной защиты возлагаются на каждого работника Центра ДПО, имеющего доступ к автоматизированному рабочему месту.

2. Применение средств антивирусной защиты

Антивирусная защита строится на основе комплексного многоуровневого подхода. Комплексная антивирусная защита должна обеспечивается применением средств антивирусной защиты на разных уровнях:

1) Все АРМ;

2) Файловый сервер

Установка и настройка средств антивирусной защиты на автоматизированных рабочих местах и серверах выполняются Администратором САЗ (сотрудником организации, с которой Центром ДПО заключен договор на оказание услуг).

Администратор САЗ несет ответственность за мероприятия по антивирусной защите, выполняемые в автоматическом режиме:

1) установка обновлений САЗ и его баз данных не реже раза в 24 часа;

2) функционирование постоянной антивирусной защиты;

3) периодически, не реже раза в неделю, полный антивирусный контроль (сканирование) всех дисков и файлов АРМ и серверов ИС.

3. Обязанности администратора средств антивирусной защиты

Обязанности Администратора САЗ:

1) раз в неделю производить мониторинг сервера САЗ, на предмет контроля;

2) контролировать ежедневное автоматическое обновления баз данных средств антивирусной защиты на всех серверах и рабочих станциях пользователей;

3) контролировать раз в неделю автоматическую полную проверку рабочих станций пользователей и информационных ресурсов Центра ДПО;

4) уведомлять пользователей перед еженедельной антивирусной проверкой, посредством электронной почты;

5) своевременно устанавливать средства антивирусной защиты на всех серверах и рабочих станциях пользователей;

6) обеспечивать реагирование в случаях обнаружения программных вирусов и принять соответствующие меры по их ликвидации;

7) контролировать и своевременно уведомлять о необходимости обновления лицензии на САЗ;

8) участвовать совместно с комиссией по расследованию инцидентов ИБ в служебных проверках по фактам заражения вирусами в структурных подразделениях Центра ДПО;

9) уведомлять о выявлении факта нарушения работником требований настоящей политики по электронной почте руководителя структурного подразделения работника, и работника, ответственного за информационную безопасность.

4. Обязанности работников

Все работники Центра ДПО обязаны:

1) по окончании рабочего дня закрыть все работающие программы, сохранить все данные и перезагрузить компьютер для возможности выполнения антивирусной проверки;

2) проверять все съемные внешние носители на вирусную активность

перед их использованием на автоматизированных рабочих местах Центра ДПО;

3) при появлении на экране рабочего монитора информационного сообщения САЗ об обнаружении вирусов, приостановить работу на компьютере и сообщить об инциденте директору, для принятия необходимых мер по устранению.

Работнику Центра ДПО запрещается:

1) использовать компьютер до полного устранения вирусов, для предотвращения дальнейшего заражения ИР Центра ДПО;

2) использовать внешние съёмные носители, принадлежащих лицам, временно допущенным к работе на компьютере в Центре ДПО, без письменного разрешения директора.