УТВЕРЖДАЮ
Директор ГБОУ СО «Школа-Интернат АОП №1 г. Саратова»

_____Л.А. Сидоренко
«10» марта 2019 г.

ИНСТРУКЦИЯ

по организации антивирусной защиты
ГБОУ СО «Школа-Интернат АОП №1 г. Саратова»

г. Саратов

2019 г.

1. Общие требования

1.1. Настоящая Инструкция определяет требования к организации защиты информационных ресурсов и программного обеспечения компонентов информационной системы (далее ИС) от разрушающего воздействия компьютерных вирусов, а также порядок применения средств антивирусного контроля в информационной системе персональных данных (далее ИСПДН), предназначенных для обработки, и передачи информации, содержащей персональные данные. Устанавливает ответственность руководителей и сотрудников подразделений в ГБОУ СО «Школа-интернат АОП № 1 г. Саратова» (далее Учреждение), эксплуатирующих и сопровождающих ИСПДН.

1.2. Целями организации противодействия вредоносным программам является:

предотвращение негативных воздействий вредоносных программ;

сохранение работоспособности ИСПДН в штатном режиме, целостности обрабатываемой информации и восстановление функционирования АРМ в случае воздействия вредоносных программ;

исключение несанкционированных действий с данными, обрабатываемыми, хранимыми и передаваемыми в ИСПДН.

1.3. Настоящая Инструкция предназначена для в ИСПДН всех должностных лиц и сотрудников подразделений Учреждения, использующих в работе ИСПДН.

1.4. Доведение Инструкции до сотрудников Учреждения в части их касающейся осуществляется Администратором информационной безопасности ИСПДН под роспись в журнале или на самом документе.

1.5. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором информационной безопасности ИСПДН семинары и персональные инструктажи (при необходимости) пользователей ИСПДН.

1.6. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например:

в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;

злоумышленных действий,

1.7. Исполнение настоящей Инструкции определяется Администратором информационной безопасности ИСПДН по согласованию с ответственным за обеспечение безопасности персональных данных (ПД) Учреждения.

1.8. Ответственность за:

соблюдение требований настоящей Инструкции возлагается на сотрудников подразделений Учреждения, использующих в работе ИСПДН;

организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на Администратора информационной безопасности ИСПДН,

2. Применение средств антивирусной защиты

2.1. Для выполнения антивирусного контроля и защиты ИСПДН допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и рекомендованные к применению ФСТЭК (Федеральная Служба Технического и Экспортного Контроля РФ).

2.2. В целях обеспечения антивирусной защиты ИСПДН производится антивирусный контроль.

2.3. Установка средств антивирусного контроля на компьютерах на серверах и рабочих станциях ИСПДН осуществляется Администратором информационной безопасности ИСПДН.

2.4. Определение параметров и режимов работы средств антивирусного контроля осуществляется Администратором информационной безопасности ИСПДН в соответствии с руководствами по применению конкретных антивирусных средств и технологическим процессом обработки ПД.

2.5. Пользователи ИСПДН при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.

2.6. Антивирусный контроль дисков и файлов после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.7. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДН (сканирование).

2.8. Пользователи проводят обновления антивирусных баз на АРМ (в случае отсутствия механизмов централизованного распространения антивирусных баз).

2.9. При необходимости Администратор информационной безопасности ИСПДН должен производить обновление антивирусных программных средств.

2.10. Обязательному антивирусному контролю подлежат все файлы на машинных носителях, получаемые для обработки в ИСПДН.

2.11. Вновь получаемые файлы должны пройти антивирусный контроль до начала обработки в ИСПДН.

2.12. Используемые для записи и хранения машинные носители информации (МНИ), перед использованием должны проходить антивирусный контроль, с выполнением соответствующей записи о проверке

в Журнале антивирусных проверок информационных ресурсов ИСПДН (Приложение 1).

2.13.МНИ с программным обеспечением (ПО), при постановке на учет (реестр, список, журнал), должны быть предварительно проверены Администратором безопасности ИСПДН на отсутствие вирусов, исполнитель должен выполнить соответствующую отметку в Журнале антивирусных проверок ИСПДН.

2.14. Передаваемые в сторонние организации документы и файлы на машинных носителях должны проходить антивирусный контроль непосредственно перед записью на носитель, а запись должна быть выполнена за время текущего сеанса работы пользователя.

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

2.16. На объекте вычислительной техники (ОВТ) (АРМ, сервер) запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.

2.17. Администратор информационной безопасности ИСПДН хранит эталонные копии антивирусных программных средств.

2.18. Периодический контроль, с записью в Журнале антивирусных проверок информационных ресурсов ИСПДН, за состоянием антивирусной защиты. Также контроль за соблюдением пользователями установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется Администратор информационной безопасности ИСПДН и ответственным за обеспечение защиты ПД.

2.19. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на АРМ (серверах).

2.20. Факт выполнения периодической и внеочередной антивирусной проверки МНИ в ИСПДн должен регистрироваться в Журнале антивирусных проверок информационных ресурсов СМЭВ.

2.21. 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.) пользователь обязан немедленно сообщить о своих подозрениях Администратору информационной безопасности ИСПДН.

2.22. Администратору информационной безопасности ИСПДН совместно с пользователем должен выполнить внеочередной антивирусный контроль.

2.23. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

2.24. Обновление вирусных баз осуществляется ежедневно путем настройки в антивирусном средстве доступа к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, системный администратор один раз в неделю осуществляет установку пакетов обновлений вирусных баз, осуществляет контроль их подключения к антивирусному пакету и проверку жесткого диска и съемных носителей на наличие вирусов.

2.25. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

немедленно поставить в известность Администратора информационной безопасности ИСПДН и прекратить какие-либо действия на АРМ;

совместно с Администратором информационной безопасности ИСПДН провести анализ необходимости дальнейшего их использования;

2.26. Администратор информационной безопасности ИСПДН проводит расследование факта заражения АРМ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль;

в случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, Администратор информационной безопасности ИСПДН отключает АРМ для устранения возможности дальнейшего распространения вируса.

2.27. Администратор информационной безопасности ИСПДН передает его в организацию, с которой заключен договор на антивирусную поддержку;

по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору информационной безопасности ИСПДН, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

2.28. При необходимости Администратор информационной безопасности ИСПДН разрабатывает инструкции по работе пользователей с программными средствами антивирусной защиты.

3. Порядок пересмотра Инструкции

3.1. Инструкция подлежит полному пересмотру в случае приобретения Учреждением новых средств защиты, существенно изменяющих порядок работы с ними.

3.2. Полный пересмотр данной Инструкции проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДН.

3.3. В остальных случаях Инструкция подлежит частичному пересмотру.

3.4. Изменения в Инструкции (сведения о них) фиксируется в листе регистрации изменений (Приложение 2).

3.5. Вносимые изменения не должны противоречить другим положениям Инструкции.

С инструкцией ознакомлен/а/ (составлена на 6 листах):

Приложение 1.

Журнал антивирусных проверок информационных ресурсов ИСПДН

№ п/п	Дата выполнения работы	Вид проводимой проверки (периодическая, внеочередная, текущая)	Тип и регистрационный номер МНИ, наименование проверяемых информационных ресурсов: логический диск, каталог (полный путь), файл (полный путь)	Результаты проверки	Расписка исполнителя работ	Принятые меры и дата проведенной работы	Расписка администратора безопасности
1	2	3	4	5	6	7	8

Приложение 2

ЛИСТ № ___ регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)