Муниципальное бюджетное общеобразовательное учреждение ПГО
«Основная общеобразовательная школа пос. Станционный - Полевской»

УТВЕРЖДАЮ
Директор школы
_____ О.А. Попова
Приказ № 1/8 – Д от 09.01.2019г.

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации от несанкционированного копирования, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

1.2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты в МБОУ ПГО «ООШ п. Станционный – Полевской» (далее – Учреждение), задачи, обязанности и права ответственных лиц за организацию антивирусной защиты, порядок установки и применения обновлений, подключения средств антивирусной защиты, основные правила антивирусной защиты информационной системы персональных данных, а также порядок ликвидации последствий воздействия программных вирусов.

1.3. Приказом директора из числа работников ОУ назначается ответственный за организацию антивирусной защиты, на которого возлагаются ответственность за решение задач по установке и сопровождению средств антивирусной защиты ИСПДн. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя.

1.4. Обязанности ответственного за организацию антивирусной защиты могут совмещать должностные лица, назначенные директором ОУ.

1.5. Действие настоящей инструкции распространяется в полном объеме на ОУ и обязательна для выполнения всеми сотрудниками, имеющими допуск к ИСПДн.

1.6. Факт выполнения антивирусной проверки программного обеспечения регистрируется в журнале за подписью лица, ответственного за антивирусную защиту.

2. МЕРОПРИЯТИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

2.1. Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных лицензионных антивирусных средств, обладающих сертификатами регулирующих органов РФ.

2.2. Инсталляция (установка) и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

2.3. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах Учреждения.

2.4. При загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2.5. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а так же информация на съемных носителях (магнитные диски, флеш - диски, CD-ROM и т.д.);
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц);
- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;

2.6. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

2.7. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2.8. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

2.9. Антивирусная проверка и контроль файлов на съёмных носителях должны проводиться в каждом случае подключения этих носителей к школьным компьютерам.

2.10. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- Непосредственно после установки (изменения) программного обеспечения компьютера;
- 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.).
- При получении файлов и папок по электронной почте;

2.11. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется ответственным за информатизацию образовательного процесса.

3. ПРАВА И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА АНТИВИРУСНУЮ ЗАЩИТУ

3.1. К основным обязанностям ответственного за антивирусную защиту в ОУ относятся:

- управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;
- обеспечение соблюдения в учреждении политики антивирусной защиты информации;
- ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;
- выявление фактов заражения программными вирусами;
- организация процесса установки и обновления средств антивирусной защиты информации на персональных компьютерах (ПК) пользователей;
- обеспечение технического сопровождения в случаях обнаружения программных вирусов;
- осуществление контроля за состоянием системы антивирусной защиты информации.

3.2. Ответственный за антивирусную защиту имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;
- осуществлять контроль состояния средств антивирусной защиты информации;
- проводить служебные проверки по фактам заражения программными вирусами средств вычислительной техники в образовательном учреждении;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации.

4. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПРОГРАМНЫХ ВИРУСОВ

4.1. Основными путями проникновения вирусов в информационно - вычислительную сеть организации являются:

- гибкие магнитные диски,
- компакт-диски,
- съемные накопители информации,
- электронная почта,
- файлы, получаемые из сети Интернет.

4.2. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения ответственного лица.

4.3. В случае обнаружения программных вирусов при входном контроле пользователь должен:

- приостановить процесс приема-передачи информации;
- сообщить ответственному лицу о факте обнаружения программного вируса;
- принять меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
- сообщить о факте обнаружения программного вируса в структурное подразделение, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

4.4. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с Администратором безопасности ИСПДн провести внеочередной антивирусный контроль своего АРМ.

4.5. При самостоятельном проведении антивирусного контроля - уведомить о результатах Администратора безопасности ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4.6. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

- Приостановить обработку данных;
- Немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения Администратора безопасности ИСПДн и владельца заражённых файлов.
- Совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;
- По возможности произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь Администратора безопасности ИС ПДн).

2. При невозможности ликвидации последствий заражения программными вирусами необходимо:

- заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- осуществить полную переустановку программного обеспечения на зараженном компьютере.

4.3. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;
- использовать средства антивирусной защиты информации, отличные от поддерживаемых компьютерами ОУ;
- без разрешения ответственного за антивирусную защиту копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4.4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется.

4.5. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования, проводимого по приказу директора школы.

5. ОТВЕТСТВЕННОСТЬ

5.1. Ответственность за организацию антивирусной защиты возлагается на руководителя ОУ.

5.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на Администратора безопасности ИСПДн.

5.3. Ответственный за антивирусную защиту несет ответственность:

- за своевременную установку средств антивирусной защиты информации;
- за эксплуатацию системы антивирусной защиты информации;
- за своевременное обновление средств антивирусной защиты информации.

5.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации, несут пользователи, за которыми закреплены АРМ.

5.5. За нарушение настоящей Инструкции Администратора безопасности ИСПДн, ответственный за антивирусную защиту и пользователи несут ответственность, установленную нормативными правовыми актами и действующим законодательством Российской Федерации.