Приложение к приказу №126-О от 23.10.2023

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ РАБОЧЕЙ СТАНЦИИ

по организации антивирусной защиты

в МБДОУ ДС ОВ №42 муниципального образования Северский район

Защита информации от несанкционированного воздействия программных вирусов на рабочей станции достигается со стороны пользователей строгим соблюдением правил приема, ввода в эксплуатацию и эксплуатации на рабочем месте программных средств общего и специального назначения, а также средств защиты информации;

Ответственность за организацию и выполнение мероприятий по защите информации от несанкционированного воздействия программных вирусов возлагается на специалиста, назначенного приказом начальника управления образования осуществлять деятельность по защите информации. Начальник управления образования, обеспечивает практическое выполнение мероприятий по защите.

Непосредственную ответственность за организацию антивирусной защиты на рабочих местах несут ответственные пользователи.

Должностные лица, обрабатывающие информацию на средствах вычислительной техники (пользователи) обязаны строго соблюдать установленные правила применения средств антивирусной защиты при работе.

Хранение и установку средств антивирусной защиты, контроль за их применением осуществляет заместитель начальника управления образования либо сотрудник, на которого согласно приказу начальника управления образования возложена обязанность осуществлять деятельность по защите информации.

Передача полученных средств антивирусной защиты на объекты, не входящие в состав управления образования, а также установка других средств защиты информации от несанкционированного воздействия программных вирусов запрещаются. За несанкционированное распространение средств антивирусной защиты виновные несут ответственность в соответствии с действующим законодательством.

Порядок применения средств антивирусной защиты устанавливается в соответствии с требованиями документации на средства антивирусной защиты и должен включать следующие виды работ:

а) обязательный входной контроль на отсутствие программных вирусов всех поступающих машинных носителей информации, а также поступающих

по каналам связи вычислительных сетей информационных ресурсов в виде файлов;

б) периодическую проверку пользователями несъемных магнитных носителей информации (жёсткие диски… желательно не реже одного раза в сутки) и обязательную проверку используемых в работе съемных магнитных носителей информации (дискеты, флэшки) перед началом работы с ними;

в) внеплановую проверку магнитных носителей в случае подозрения на наличие вируса, либо по требованию ответственного за обеспечение безопасности информации;

г) восстановление работоспособности программных средств и данных в случае их повреждения программными вирусами.

В случае обнаружения программных вирусов или факта несанкционированной модификации (уничтожения) информации пользователь обязан немедленно прекратить все работы, доложить о случившемся специалисту по защите информации, и принять меры локализации или (в крайнем случае) удаления программных вирусов с помощью имеющихся средств антивирусной защиты.

Ликвидация последствий воздействия программных вирусов осуществляется пользователями и ответственным за обеспечение безопасности информации.

О факте обнаружения программных вирусов сообщается в организацию-отправитель, от которой поступили машинные носители информации, для принятия мер по их локализации и устранению.

Носителями могут быть гибкие магнитные диски (дискеты), а так же компакт-диски, флэшки, моби-рэки, съемные жесткие диски и т.д.

До полного уничтожения программных вирусов использование зараженных машинных носителей информации и вычислительной техники, на которых эти магнитные носители информации были установлены, запрещено.

Отключать установленные на средствах вычислительной техники средства антивирусной защиты запрещается.