Приложение № 20
к приказу Директора МБОУ СОШ д.Султанбеково
МР Аскинский район РБ
от «21» 11 2018 г. № 88 од

Положение
по организации антивирусной защиты

1. Общие положения

1.1. Настоящее Положение определяет требования к организации защиты Информационных систем персональных данных (далее – ИСПДн) МБОУ СОШ д.Султанбеково МР Аскинский район РБ (далее - Оператор) от воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее - вредоносного ПО), устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих ИСПДн за их выполнение.

1.2. Целью мероприятий по антивирусной защите является предотвращение потери информации в ИСПДн.

1.3. Задачами антивирусной защиты являются:

– проведение профилактических работ с применением антивирусных диагностических средств;

– непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации ИСПДн.

1.4. Компоненты ИСПДн, подлежащие защите от вирусов:

– интернет шлюзы, установленные в точках подключения к сетям общего пользования, а также ведомственным сетям;

– сервера;

– автоматизированные рабочие места (далее- АРМ).

1.5. Основные источники вирусов:

– съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;

– локальная сеть, в том числе система электронной почты и Интернет;

– жесткий диск, на который попал вирус в результате работы с зараженными программами.

2. Организация мероприятий по антивирусной защите

2.1. Планированием и организацией проведения мероприятий по антивирусной защите занимается Ответственный за обеспечение безопасности персональных данных.

2.2. К использованию допускаются только лицензионные и сертифицированные ФСТЭК России средства антивирусной защиты.

2.3. Обновление антивирусных баз должно производиться в автоматическом режиме. В случае сбоя автоматического обновления обновление баз должно производиться вручную.

2.4. Мероприятия по антивирусной защите включают в себя:

– профилактика вирусов;

– анализ ситуаций;

- применение средств антивирусной защиты;
- проведение расследований инцидентов связанных с вирусами.

3. Профилактика вирусов

3.1. Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая быстрая антивирусная проверка;
- ежеквартальная выборочная проверка ИСПДн серверов БД на наличие вирусов бесплатными антивирусными утилитами, даже при отсутствии внешних проявлений вирусов;
- изучение информации по сообщениям в журналах и Интернете о новых вирусах и их способах распространения и заражения и информирование сотрудников Оператора о новых способах распространения вредоносного ПО и других актуальных угрозах;
- ограничение доступа к компонентам ИСПДн третьих лиц.

3.2. При обнаружении вирусов на АРМ и серверах, работающих в локальной сети, внеплановой проверке подлежат все АРМ и сервера, входящие в один сегмент сети с зараженным АРМ или сервером, или работающие с общими данными и программным обеспечением.

4. Анализ ситуаций

4.1. При возникновении подозрения на наличие вредоносного ПО (ошибки в работе программ, появление графических и звуковых эффектов, искажения данных, пропадание файлов, частое появление сообщений о системных ошибках, замедление работы компьютера и т.п.) сотрудник самостоятельно может провести внеочередной антивирусный контроль, либо обратиться к Ответственному за обеспечение безопасности ИСПДн.

4.2. При возникновении подозрения на наличие вредоносного ПО на серверах и интернет шлюзах Ответственный за обеспечение безопасности ИСПДн организует осуществление внеочередного антивирусного контроля.

4.3. При обнаружении вредоносного ПО Ответственный за обеспечение безопасности ИСПДн выполняет анализ ситуации. В результате анализа делается вывод о способе уничтожении вирусов.

5. Применение средств антивирусной защиты

5.1. Лечение или уничтожение вредоносного ПО осуществляется в автоматическом режиме средствами антивирусной защиты, а в ситуациях, когда это невозможно – вручную.

5.2. В случае уничтожения вредоносным ПО файлов баз данных и содержащихся на файловом сервере Ответственному за обеспечение безопасности ИСПДн организовать их восстановление, используя последнюю резервную копию.

5.3. После уничтожения вредоносного ПО и восстановления зараженных файлов необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить компьютер.

5.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), поступающая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

5.5. Файлы, помещаемые на архивное хранение, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в квартал в ручном или автоматическом режиме.

5.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на предмет отсутствия вредоносных файлов.

6. Ответственность

6.1. За невыполнение требований настоящего Положения применяется дисциплинарная ответственность в порядке, определенным законодательством Российской Федерации и локальными актами Оператора.

.