УТВЕРЖДЕНА
приказом МБДОУ д/с №49
от «20» июля 2017 г. № 109

Инструкция по организации антивирусной защиты

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АВЗ	– антивирусная защита
АРМ	– автоматизированное рабочее место
ИСПДн	– информационная система персональных данных
ОС	– операционная система
ПДн	– персональные данные
ПМВ	– программно-математическое воздействие
ПО	– программное обеспечение

1. Общие положения

1.1. Настоящая инструкция по организации антивирусной защиты (далее – Инструкция) определяет требования к организации защиты информации от разрушающего воздействия компьютерных вирусов в МБДОУ д/с №49 (далее –

Учреждение), а также устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИСПДн.

1.2. Целями защиты является противодействие угрозам несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты информации.

1.3. В целях перекрытия всех возможных каналов проникновения вредоносных программ в ИСПДн антивирусное программное обеспечение должно применяться на автоматизированных рабочих местах, серверах, средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах, мобильных технических средствах и иных точках доступа в информационную систему, подверженных заражению вредоносными программами через съемные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы).

1.4. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, купленные у разработчиков (поставщиков) указанных средств и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

1.5. Установка, конфигурирование и управление средствами антивирусной защиты осуществляется ответственным за обеспечение безопасности персональных данных.

1.6. После установки и настройки средств АВЗ в обязательном порядке должно быть произведено тестирование системы АВЗ.

1.7. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.

1.8. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИСПДн и своевременное информирование ответственного за обеспечение безопасности персональных данных в случае обнаружения действий вредоносных программ возлагается на пользователей ИСПДн.

2. Реализация антивирусной защиты

2.1. Ежедневно, при загрузке компьютеров, в автоматическом режиме должен проводиться антивирусный контроль всех электронных носителей информации ПДн.

Обязательной проверке в масштабе времени, близком к реальному, подлежат любые объекты (файлы) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов.

2.2. Настройка средств антивирусной защиты должна реализовывать следующие функции:

- непрерывный автоматический мониторинг информационного обмена в ИСПДн с целью выявления программно-математического воздействия;
- автоматическую проверку на наличие вредоносных программ или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

- реализацию механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;
- автоматическую проверку критических областей АРМ и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги ОС «system» и «system32» при каждом запуске ОС;
- полную автоматическую проверку носителей информации всех АРМ и серверов не реже одного раза в неделю;
- оповещение в масштабе времени, близком к реальному, об обнаружении вирусов.

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

2.4. Устанавливаемое ПО должно быть предварительно проверено на наличие вирусов. Непосредственно после установки ПО, должна быть выполнена антивирусная проверка.

2.5. При возникновении подозрения на наличие вируса должна быть провести внеочередную антивирусную проверку АРМ.

3. Обновление базы данных признаков вредоносных программ

3.1. Обеспечение актуальности базы данных признаков вредоносных программ производится периодическим их обновлением. Получение базы данных должно происходить из доверенных источников.

3.2. Обновление должно происходить в автоматическом режиме с получением уведомлений о необходимости обновления и непосредственном обновлении базы данных.

3.3. Должен осуществляться контроль целостности обновлений базы данных признаков вредоносных программ.

4. Права и обязанности сотрудников

4.1. Ответственный за обеспечение безопасности персональных данных несет персональную ответственность за организацию и осуществление АВЗ.

4.2. Руководители отделов управления образования администрации г.Белгорода обязаны осуществлять постоянный контроль выполнения пользователями ИСПДн правил Инструкции.

4.3. Руководители отделов управления образования администрации г.Белгорода имеют право обращаться к ответственному за обеспечение безопасности персональных данных за оказанием методической и практической помощи в обеспечении АВЗ.

4.4. Пользователь ИСПДн обязан удостовериться, что на АРМ установлено и активно антивирусное ПО. В случае его отсутствия необходимо известить об этом ответственного за обеспечение безопасности персональных данных.

4.5. При подозрении на заражение вирусом или его обнаружении пользователь ИСПДн должен приостановить работу на АРМ с последующим его выключением. После чего немедленно сообщить об этом ответственному за обеспечение безопасности персональных данных или руководителю отдела. Возобновление работы возможно лишь после полной нейтрализации угрозы.

4.6. Пользователь ИСПДн при работе со съемными носителями информации (flash-накопители, оптические диски, жесткие диски USB и т.д.) обязан перед началом работы осуществить их полную проверку на предмет наличия вредоносных программ.

4.7. Запрещается сохранять (скачивать) и открывать вложения из писем электронной почты от неизвестных отправителей. Если отправитель известен, то необходимо уточнить у него факт отправки письма лично, после чего сохранить вложение и перед открытием проверить антивирусом.

4.8. При появлении любых предупреждающих сообщений (сообщения об обнаружении вируса, истечения срока лицензии, о неактуальности базы данных признаков вредоносных программ) необходимо сообщить об этом ответственному за обеспечение безопасности персональных данных.

4.9. Пользователь ИСПДн, в случае служебной необходимости, имеет право обратиться к ответственному за обеспечение безопасности персональных данных с просьбой о временной приостановке активных компонентов и задач АВЗ.

5. Ответственность за нарушение требований инструкции

5.1. Каждый пользователь ИСПДн несет персональную ответственность за нарушение требований Инструкции.

5.2. Нарушение требований Инструкции является чрезвычайным происшествием и влечет за собой ответственность, предусмотренную действующим законодательством РФ.