УТВЕРЖДАЮ
Заведующий МБДОУ
«ЦРР-детский сад № 188»
_____Г.И.Лифанова
приказ от 29.01.2018 № 13-О

Инструкция
по организации антивирусной защиты
в муниципальном бюджетном дошкольном образовательном учреждении
«Центр развития ребенка — детский сад № 188»

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с действующим законодательством Российской Федерации в целях предотвращения несанкционированных вредоносных воздействий на информационные ресурсы муниципального бюджетного дошкольного образовательного учреждения «Центр развития ребенка — детский сад № 188» (далее — Учреждение), определения требований к организации антивирусной защиты информационных систем и персональных компьютеров.

1.2. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.

1.3. Основными задачами системы обеспечения антивирусной защиты являются:
- исключение или существенное затруднение противоправных действий в отношении информационных систем Учреждения как носителей защищаемой информации;
- обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.

1.4. Обеспечение антивирусной защиты включает:
- регулярные профилактические работы;
- анализ ситуации проявления вредоносных программ и причины их появления;
- уничтожение вредоносных программ на автоматизированных рабочих местах (АРМ) (серверах);
- принятие мер по предотвращению причин появления вредоносных программ.

2. Требования к антивирусному программному обеспечению

2.1. В Учреждении допустимо использование только лицензионного антивирусного программного обеспечения.

2.2. Обнаружение возможно большего числа известных вредоносных программ, а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

2.3. Исчерпывающий список защищаемых точек (АРМ и т.д.) возможного проникновения вредоносных программ.

2.4. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного программного обеспечения.
2.5. Соответствие системных требований антивирусного программного обеспечения платформам, характеристикам и комплектации применяемой вычислительной техники.
2.6. Надежность и работоспособность антивирусного программного обеспечения в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде.
2.7. Наличие документации, необходимой для практического применения и освоения антивирусного программного обеспечения, на русском языке.

3. Установка антивирусного программного обеспечения

3.1. Установка антивирусного программного обеспечения на компьютерах Учреждения осуществляется уполномоченным сотрудником Учреждения.
3.2. Установка антивирусного программного обеспечения производится на каждый защищаемый компьютер Учреждения. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
3.3. Антивирусное программное обеспечение запускается автоматически при запуске операционной системы.

4. Порядок обновление баз данных антивирусной защиты информации

4.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.
4.2. Обновление антивирусных баз на защищаемых компьютерах осуществляется в порядке определенном техническими требованиями к конкретному ПО.
4.3. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к сети Интернет должно осуществляться с использованием съемных носителей информации, в обязательном порядке проверяемых антивирусными ПО перед их использованием.
4.4. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к сети Интернет, осуществляется автоматически и контролируется пользователем самостоятельно.

5. Порядок применения средств антивирусной защиты

5.1. Порядок применения средств антивирусной защиты информации устанавливается в соответствии с требованиями разработчика программного обеспечения и с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;
- 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 неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;

- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

5.2. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

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

5.4. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов Учреждения от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна проводиться в нерабочее время, за исключением внештатных ситуаций.

6. Действия при обнаружении вредоносных программ или подозрении на их наличие

6.1. 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.) сотрудник Учреждения самостоятельно или с ответственным за антивирусную защиту должен провести внеочередной антивирусный контроль компьютера.

6.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:
- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов заведующего и ответственного за антивирусную защиту Учреждения, а также сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

7. Ответственность

7.1. Ответственность за организацию антивирусного контроля в Учреждении, в соответствии с требованиями настоящей Инструкции возлагается на заведующего Учреждением.

7.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту Учреждения и всех сотрудников, являющихся пользователями персональных компьютеров Учреждения.

7.3. Периодический контроль за состоянием антивирусной защиты в Учреждении, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками Учреждения осуществляется ответственным за антивирусную защиту Учреждения.