Приложение №9 к приказу от 04.03.2022 №31-О

ИНСТРУКЦИЯ
по организации антивирусной защиты в муниципальном бюджетном учреждении «Централизованная библиотечная система»

1. Общие положения

1.1. Настоящая инструкция определяет требования к организации защиты информационных систем персональных данных (далее - ИСПДн) в муниципальном бюджетном учреждении «Централизованная библиотечная система» (далее- Учреждение) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.3. К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации антивирусные средства.

1.4. Установка и настройка средств антивирусного контроля на компьютерах осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. При загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль дисков и файлов на них.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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 три месяца.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения также должна быть выполнена антивирусная проверка на компьютере.

2.5. 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 тому подобное) пользователь самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

2.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов в уполномоченную организацию по обеспечению безопасности персональных данных;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

2.7. Обновление баз системы антивирусного контроля должно проводиться не реже одного раза в неделю.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей инструкции возлагается на ответственного за организацию обработки персональных данных.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей инструкции возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.

3.3. Периодический контроль за состоянием антивирусной защиты в ИСПДн, за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции осуществляется уполномоченной организацией по обеспечению безопасности персональных данных.

3.4. Ответственность за организацию своевременного обновления антивирусных баз возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.