Принято педагогическим советом
протокол от "29" августа 2019 г. № 1

Утверждено и введено в действие приказом
от "1" сентября 2019 г. №267
Директор _____ Имамов И.Ф.

ПОЛОЖЕНИЕ
по организации антивирусной защиты компьютеров и информационных систем

I. Общие положения

1.1. Настоящее Положение определяет порядок организации антивирусной защиты компьютеров и информационных систем в МБОУ «Лицей №177» Ново-Савиновского района г. Казани (далее - лицей) с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и персональные данные, обрабатываемые и хранимые лицеем, возникновения фактов заражения программного обеспечения компьютерными вирусами.
1.2. Положение разработано в соответствии с действующими редакциями нормативных документов:

- ФЗ "Об образовании в Российской Федерации" от 29.12.2012 №273-ФЗ;
- ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 №436-ФЗ;
- ФЗ "О персональных данных" от 27.07.2006 №152-ФЗ;
- "Уголовного кодекса Российской Федерации" от 13.06.1996 №63-ФЗ (глава 28. "Преступления в сфере компьютерной информации");
- Постановления Главного государственного санитарного врача РФ от 29.12.2010 №189 "Об утверждении СанПиН 2.4.2.2821-10 "Санитарно- эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях";
- Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 05.12.2016 №646;
- Устава МБОУ «Лицей №177» Ново-Савиновского района г. Казани.

II. Ответственность при организации антивирусной защиты

2.1. Ответственность за организацию антивирусной защиты в лицее возлагается на администратора информационной безопасности, который назначается директором лицея из числа штатных сотрудников.
2.2. Администратор информационной безопасности обеспечивает функционирование, поддерживает работоспособность систем защиты информации и резервного копирования на уровне серверов и автоматизированных рабочих мест пользователей.
2.2. Периодический контроль состояния антивирусной защиты в лицее осуществляется заместителем директора по информатизации.

III. Порядок организации антивирусной защиты

3.1. В лицее средства антивирусного контроля устанавливаются и настраиваются администратором информационной безопасности на все серверы и автоматизированные рабочие места пользователей для обеспечения защиты от внедрения вредоносного программного обеспечения (далее - ВПО) в них со съемных носителей, через локальную и глобальную сети.

3.2. Все устанавливаемые программы антивирусного контроля должны быть лицензионными или свободно-распространяемыми (СПО).

3.3. При осуществлении антивирусной защиты выполняются следующие обязательные мероприятия:

- Контроль съемных носителей информации на предмет наличия на них ВПО до начала работы с ними.
- Проверка всех электронных отправлений на предмет наличия ВПО.
- Периодическая проверка на предмет наличия ВПО жестких дисков (не реже одного раза в неделю).
- Внеплановая проверка жестких дисков и съемных носителей информации в случае подозрения на наличие ВПО.
- Восстановление работоспособности программных средств и информационных систем, поврежденных программными вирусами.
- Обновление баз данных средств антивирусной защиты должно осуществляется в автоматическом режиме (не реже одного раза в сутки).

IV. Порядок действий при обнаружении ВПО

4.1. При обнаружении ВПО на съемных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользователь персонального компьютера обязан:

а) Приостановить работу с источником угрозы (съемным носителем, электронным отправлением, Интернет-ресурсом), иные работы на автоматизированном рабочем месте не запрещаются.

б) Сообщить администратору информационной безопасности об обнаружении ВПО.

в) Принять меры по локализации и удалению ВПО, рекомендованные администратором информационной безопасности.

г) В случае невозможности удаления ВПО вновь обратиться к администратору информационной безопасности.

4.2. В случае невозможности удаления пользователем ВПО, администратор информационной безопасности обязан:

а) Лично принять меры по локализации и удалению ВПО на рабочем месте пользователя.

б) При неустранении проблемы совместно с системным администратором попытаться выявить источник и способ проникновения ВПО на серверное и телекоммуникационное оборудование лицея.

в) При необходимости обратиться в организацию, осуществляющую техническую поддержку средств антивирусной защиты. При передаче образцов зараженных файлов, а также при предоставлении информации о вирусной атаке в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации, администратором информационной безопасности должны быть соблюдены требования конфиденциальности обрабатываемой в лицее информации.