муниципальное бюджетное общеобразовательное учреждение
городского округа Тольятти
«Школа имени академика Сергея Павловича Королёва»

ПРИНЯТО

Педагогическим советом
МБУ «Школа имени С.П. Королёва»
Протокол № 4 от "29" ноября 2016 г.

Председатель _____ Т.Н.Подоляко

УТВЕРЖДАЮ

Директор МБУ «Школа имени С.П. Королёва»

_____ Т.Н. Подоляко

приказ № 977 от "30" ноября 2016 г.

ПРАВИЛА
антивирусной защиты информации в образовательной организации

1. Общие сведения

1.1. Настоящие Правила обязательны для исполнения всеми сотрудниками МБУ «Школа имени С.П. Королёва» (далее Школа) и определяют условия работы на АРМ с установленным средством антивирусной защиты информации.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области защиты информации и направлены на нейтрализацию угроз безопасности информации связанных с вирусной активностью.

1.3. Настоящие правила носят общий характер и не отменяют действия организационно-распорядительной и эксплуатационной документации на объекты информатизации Школы, аттестованные по требованиям безопасности информации.

1.4. Ознакомление сотрудников Школы с настоящими Правилами осуществляется Ответственным за антивирусную защиту в Школы под роспись. Перечень АРМ с установленным Антивирусом

2. Термины и сокращения

Автоматизированное рабочее место (АРМ) – персональный компьютер с периферийным оборудованием и предустановленным программным обеспечением;

Антивирусный контроль – проверка на вирусы с помощью средства антивирусной защиты информации;

Аттестация объектов информатизации – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие

системы защиты информации объекта информатизации требованиям безопасности информации;

Вредоносное программное обеспечение (компьютерный вирус) — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера;

Единая служба технической поддержки (ЕСТП) – единая точка контакта между Поставщиками ИТ услуг и пользователями ИТ услуг. ЕСТП управляет ИТ инцидентами, Запросами на ИТ обслуживание, а также взаимодействует с пользователями ИТ услуг;

ИТ обращение – обращение пользователя услуг в ЕСТП по телефону, по электронной почте или путем самостоятельной регистрации обращения в портале самообслуживания. ИТ обращение может быть зарегистрировано как ИТ инцидент или как Запрос на ИТ обслуживание;

Информационная безопасность - процесс обеспечения конфиденциальности, целостности и доступности информации.

Инцидент информационной безопасности – факт и/или событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности;

Компрометация в криптографии - факт и/или событие, свидетельствующего получении доступа постороннего лица к защищаемой информации, а также подозрение на него. Чаще всего рассматривают компрометацию закрытого ключа, закрытого алгоритма, цифрового сертификата, учётных записей (паролей), абонентов или других защищаемых элементов, позволяющих удостоверить личность участника обмена информацией.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

Съемные носители информации - любой материальный объект или среда передачи, способный достаточно длительное время сохранять (нести) в своей структуре занесённую в/на него информацию. Это может быть, например, лента с намагниченным слоем (в бобинах и кассетах), фотоматериал, пластик со специальными свойствами (например, оптические диски —CD, DVD и

т.д.), ЭМИ (электромагнитное излучение), твердотельные носители информации (Flash и т.д).

3. Общие правила

3.1. Для организации антивирусной защиты допускаются к использованию только лицензионные средства антивирусной защиты информации, сертифицированные ФСТЭК России.

3.2. Ответственный за антивирусную защиту информации в Школе назначается приказом руководителя образовательной организации.

3.3. Ответственный за обеспечение средствами антивирусной защиты информации (в том числе сертифицированный ФСТЭК России дистрибутив, ключевая информация) – НАИЦГ РС(Я), в рамках предоставления централизованного информационно-технологического сервиса «Обеспечение системой централизованной антивирусной защиты пользователей системы единой службы каталогов (Active Directory) и подключение пользователей, не вошедших в единую службу каталогов путем выдачи дистрибутивов, активация лицензий» в составе предоставления государственной услуги «Предоставление централизованных информационно - технологических сервисов», в соответствии с ежегодно утверждаемым Министерством связи и информационных технологий Республики Саха (Якутия) государственным заданием.

3.4. Активация и обновление Антивируса осуществляется автоматизировано.

3.5. Порядок и периодичность проведения антивирусного контроля, а также настройки и параметры антивирусной защиты определяется автоматически настроенными политиками системы централизованной антивирусной защиты.

3.6. Обязательному дополнительному антивирусному контролю подлежит любая информация на съёмных машинных носителях информации, поступающая для обработки на АРМ сотрудника Организации. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

3.7. 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.) необходимо провести внеочередной антивирусный контроль для определения факта наличия или отсутствия компьютерного вируса.

3.8.1 В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов необходимо:

- приостановить работу;
- сообщить о факте обнаружения заражённых компьютерным вирусом файлов Ответственному за антивирусную защиту информации в Организации;

- совместно с Ответственным за антивирусную защиту информации в Организации сообщить о факте обнаружения заражённых компьютерным вирусом файлов ИТ обращением в ЕСТП;
- сообщить о факте обнаружения заражённых компьютерным вирусом файлов иным сотрудникам Организации, использующим в работе указанные файлы;
- провести анализ необходимости дальнейшего использования заражённых файлов;
- провести лечение или уничтожение заражённых файлов;
- принимать участие в проведении служебной проверки по факту выявленной вирусной активности в случае принятия решения о ее проведении.

3.8.2. В случае сообщения антивирусной проверки о необнаруженных угрозах необходимо:

- приостановить работу;
- сообщить об обнаружении подозрительной вирусной активности Ответственному за антивирусную защиту информации в Организации;
- совместно с Ответственным за антивирусную защиту информации в Организации сообщить об обнаружении подозрительной вирусной активности ИТ обращением в ЕСТП;
- сообщить об обнаружении подозрительной вирусной активности иным сотрудникам Организации, использующим в работе указанные файлы;
- провести анализ необходимости дальнейшего использования подозрительных файлов;
- принимать участие в проведении служебной проверки по факту обнаружения подозрительной вирусной активности в случае принятия решения о ее проведении.

4. Ответственность

4.1. Ответственность за создание, использование и распространение вредоносных компьютерных программ предусмотрена ст. 273 Уголовного Кодекса Российской Федерации.