Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 19 города Новоалтайска Алтайского края»

ПРИНЯТО
на заседании педагогического совета
от «12» декабря 2019 г.
Протокол № 2/12

УТВЕРЖДАЮ:
Директор МБОУ «СОШ № 19 города Новоалтайска Алтайского края»
_____ О.А.Долматов
Приказ № 132
от «12» декабря 2019 г.

Инструкция по организации антивирусной защиты

1. ***Общие положения.***

Настоящая инструкция Муниципального бюджетного общеобразовательного учреждения ««Средняя общеобразовательная школа № 19 города Новоалтайска Алтайского края» – (далее Школа) предназначена для определения порядка проведения антивирусного контроля и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами компьютерного оборудования Школы.

1.1. Ответственным за организацию антивирусной защиты в Школе является программист школы, имеющий доступ к головному компьютеру сервера и локальной сети Школы.

1.2. На компьютерном оборудовании Школы может использоваться только лицензионное антивирусное программное обеспечение, либо свободнораспространяемое программное обеспечение.

1.3. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты Школы.

1.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flashнакопителях и т.п.).

1.5. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.6. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

1.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

1.8. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2. ***Требования к выполнению мероприятий ответственным за организацию антивирусной защиты в Школе, направленных на решение задач по антивирусной защите.***

2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.

2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю во вторник с 17.00).

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы (далее ИКС) Школы.

2.4. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.7. Обеспечение бесперебойной работы компьютерного оборудования Школы для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. ***Требования к проведению мероприятий по антивирусной защите ответственными за точки доступа к сети Интернет и ответственным за организацию антивирусной защиты в Школе.***

3.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и сервера и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на сервере и персональных компьютерах Школы;
- 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.);
- при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. ***Действия ответственных сотрудников за точки доступа к сети Интернет и ответственного за организацию антивирусной защиты в Школе при обнаружении компьютерного вируса***

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты

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

- провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. ***Ответственность.***

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором Школы;

5.2. Ответственность за проведение мероприятий антивирусного контроля в Школе возлагается на ответственного за организацию антивирусной защиты.

5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных автоматизированных рабочих местах возлагается на ответственных приказом директора Школы за них.

5.4. Периодический контроль за состоянием антивирусной защиты в Школе осуществляется заместителем директора Школы по информатизации и фиксируется актом проверки (не реже 1 раз в квартал).

№№	**Тематическая категория**	**Содержание**
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
2	Злоупотребление свободой СМИ — экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы

3	Злоупотребление свободой СМИ — наркотические средства	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ — информация с ограниченным доступом	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Злоупотребление свободой СМИ — скрытое воздействие	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	А) Экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы; Б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: ✓ насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; ✓ подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; ✓ осуществление террористической деятельности либо публичное оправдание терроризма; ✓ возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; ✓ унижение национального достоинства; ✓ осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо

		вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; ✓ пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; ✓ воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения; ✓ публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; ✓ применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; ✓ посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; ✓ нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением
7	Вредоносные программы	Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
8	Преступления	Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); оскорбление (унижение чести и достоинства другого

		лица, выраженное в неприличной форме); публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; склонение к потреблению наркотических средств и психотропных веществ; незаконное распространение или рекламирование порнографических материалов; публичные призывы к осуществлению экстремистской деятельности; информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; публичные призывы к развязыванию агрессивной войны
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну