«Согласовано»
Председатель ПК
МБОУ СОШ № 6
_____И.П.Алексеева
Протокол №___
от _____2018 г.

Утверждено
Приказом МБОУ СОШ № 6
№240/ОД от 31.08.2018г.

РЕГЛАМЕНТ

по организации антивирусной защиты компьютерной техники и работы сотрудников и обучающихся образовательной организации МБОУ «СОШ №6» в сети Интернет

1. Общие положения

1.1. Настоящий Регламент разработан в целях систематизации мероприятий по обслуживанию и использованию локальной сети и сети Интернет (далее - сети) в образовательном учреждении МБОУ СОШ № 6 (далее – ОУ) и определяет порядок работы с этими сетями обучающихся, сотрудников ОУ и других лиц.
1.2. Ознакомление с Регламентом и его соблюдение обязательны для всех обучающихся, сотрудников ОУ, а также иных лиц, допускаемых к работе с сетями в данном ОУ.
1.3. Настоящий Регламент имеет статус локального нормативного акта ОУ. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Регламентом, применяются нормы действующего законодательства.

2. Ответственный сотрудник

2.1. Ответственный сотрудник за организацию подключения к сети Интернет, организацию антивирусной защиты и контентной фильтрации назначается приказом по ОУ.
2.2. Ответственный сотрудник за настройку локальной вычислительной сети установку и настройку антивирусного программного обеспечения, программного обеспечения контентной фильтрации назначается приказом по ОУ.

3. Техническое обслуживание сетей в ОУ

3.1. Подключение оборудования и настройку сетей в ОУ производит ответственный сотрудник за настройку соответствующих сетей. Другим лицам запрещается осуществлять попытки подключения оборудования и настройки сети самостоятельно.
3.2. При отсутствии специалиста в ОУ настройка сетей осуществляется специалистами «Выборг-интернет» при подаче телефонной заявки.

4. Обязанности ответственного сотрудника за организацию подключения к сети Интернет и организацию антивирусной защиты и контентной фильтрации

4.1. Организует установку антивирусного программного обеспечения и постоянного обновления антивирусных баз на всех персональных компьютерах ОУ.
4.2. Организует установку программного обеспечения контентной фильтрации на персональные компьютеры, имеющие доступ к сети Интернет и к которым имеют доступ обучающиеся ОУ.
4.3. Принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.
4.4. Использует меры дисциплинарного характера для предотвращения доступа к ресурсам, не имеющим отношения к образовательному процессу. По каждому выявленному факту доступа к таким ресурсам, ответственный сотрудник за контроль над использованием сети Интернет или выявивший данный факт сотрудник составляет докладную записку на имя руководителя ОУ. Ответственность за последствия доступа к нежелательным ресурсам несет лицо, осуществившее доступ к этим ресурсам.
4.5. Осуществляет контроль за наличием подключения персональных компьютеров в компьютерных классах и библиотеке ОУ к сети Интернет.
4.6. Подает телефонную заявку провайдеру «Выборг-интернет» при отсутствии подключения персональных компьютеров ОУ к сети Интернет, если невозможно устранить возникшую проблему собственными силами ОУ с последующим контролем исполнения.
4.7. Обеспечивает возможность использования обучающимися и сотрудниками ОУ ресурсов сети Интернет в компьютерном классе (кабинете информатики) и библиотеке во внеурочное время по расписанию работы компьютерных классов и библиотеки.
4.8. Организует ведение журналов учета работы в сети Интернет в компьютерном классе, а также осуществляет контроль за его ведением.

5. Памятка ответственного сотрудника за организацию подключения к сети Интернет, организацию антивирусной защиты

1. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.
2. Регулярно проверять состояние антивирусного программного обеспечения, а именно
   а. Режим автоматической защиты должен быть включен постоянно

b. Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
c. Просматривать на компьютере журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.

3. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
4. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.
5. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.
6. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

6. Памятка пользователя сети Интернет

1. Пользователь обязан выполнять все требования ответственного сотрудника за организацию подключения к сети Интернет (или администратора локальной сети).
2. За одним рабочим местом должно находиться не более одного пользователя.
3. Запрещается работать под чужим регистрационным именем, одновременно входить в систему более чем с одной рабочей станции.
4. Каждый пользователь при наличии технической возможности может иметь персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб. Аналогично может быть предоставлена возможность работы с почтовым ящиком. При возникновении проблем необходимо обратиться к дежурному администратору.
5. Пользователю разрешается переписывать полученную информацию на личные носители, которые предварительно проверяются на наличие вирусов.
6. Разрешается использовать оборудование классов только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения проектов. Любое использование оборудования в коммерческих и других не образовательных целях запрещено.

7. Запрещена передача внешним пользователям информации, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайне, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.
8. Запрещается работать с объемными ресурсами (video, audio, chat) без согласования с администратором.
9. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
10. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах, а также производить запись на жесткий диск рабочей станции. Запрещается перегружать компьютер без согласования с ответственным сотрудником за организацию подключения к сети Интернет (или администратором локальной сети).
11. Пользователь обязан сохранять оборудование в целости и сохранности.

При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. В случае нарушения правил работы пользователь лишается доступа в сеть. За административное нарушение, не влекущее за собой порчу имущества, вывод оборудования из рабочего состояния и не противоречащие принятым правилам работы пользователь получает первое предупреждение. При повторном административном нарушении - пользователь лишается доступа в Интернет без права восстановления.

При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

7. Особые положения

7.1. В случае отсутствия ответственного сотрудника за организацию подключения к сети Интернет, организацию антивирусной защиты и контентной фильтрации, его обязанности возлагаются руководителем ОУ на другого сотрудника образовательного учреждения.

Исп.
Ответственный по информационной
безопасности МБОУ СОШ № 6

Тур С.Н.