МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «Средняя общеобразовательная школа № 33» имени Алексея Владимировича Бобкова

ПРИКАЗ №183/1

от 15 июня 2018 г.

О безопасной работе
в сети Интернет

В целях обеспечения безопасной работы в сети Интернет и безопасного функционирования локальной информационной сети МБОУ «СОШ № 33», в соответствии с письмом от 14 мая 2018 г. № 08-1184 Министерства образования и науки Российской федерации Департамента государственной политики в сфере образования общего образования, а также учитывая изменения в законодательстве Российской Федерации в области защиты информации, направленные на ужесточение требований при работе в сети Интернет государственных и муниципальных служащих с электронными сервисами

ПРИКАЗЫВАЮ:

1. Утвердить Свод правил по безопасной работе сотрудников МБОУ «СОШ № 33» при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем (Приложение № 1).
2. Ознакомить под расписку всех сотрудников, являющихся пользователями сети.
3. Контроль исполнения приказа оставляю за собой.

Директор МБОУ «СОШ № 33» Н.М. Лушникова

Приложение № 1

СВОД ПРАВИЛ
по безопасной работе сотрудников МБОУ «СОШ № 33»
при использовании сети Интернет

1. Общие положения

1.1. Настоящий Свод правил по безопасной работе сотрудников МБОУ «СОШ № 33» разработан в соответствии с рекомендациями Письма № 08-1184 от 14 мая 2018 г. Министерства образования и науки Российской федерации Департамента государственной политики в сфере образования общего образования.

1.2. Свод правил основан на требованиях Федерального закона от 27.07.2006 № 149- ФЗ «Об информации, информационных технологиях и о защите информации», нормативных правовых актах Российской Федерации, регулирующих отношения в области защиты информации.

1.3. Целями Свода правил являются:

- регулирование работы пользователей при использовании сети Интернет и осуществлении информационного взаимодействия с сервисами государственных информационных систем;
- обеспечение целостности, конфиденциальности и доступности хранящейся и передаваемой информации, находящейся на автоматизированных рабочих местах (далее –АРМ) или локальной вычислительной сети (далее – ЛВС);
- соблюдение требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области защиты информации.

1.4. При работе в сети Интернет и информационных системах пользователи руководствуются законодательством Российской Федерации, нормативными правовыми актами, иными документами в области информационных технологий и безопасности информации, а также Сводом правил.

2. Общие правила пользования на АРМ

2.1. Пользователь отвечает за правильность включения (выключения) АРМ и все действия при работе на нем.

2.2. АРМ разрешается использовать исключительно в служебных целях.

2.3. Пользователь обязан исключить возможность неосторожного причинения вреда техническим и информационным ресурсам.

2.4. Соблюдать требования парольной политики (Раздел 6 Свода правил).

2.5. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к специалисту по информационной безопасности.

Пользователям запрещается:

2.6. Открывать на АРМ файлы и запускать программы, полученные из непроверенных источников.

2.7. Отключать (блокировать) средства защиты информации.

2.8. Привлекать посторонних лиц для производства ремонта или настройки АРМ.

3. Правила пользования в сети Интернет

3.1. Ресурсы сети Интернет предоставляются пользователям для получения информации необходимой для выполнения профессиональных обязанностей.

3.2. Пользователь обязан не предпринимать попыток несанкционированного доступа к информационным ресурсам, доступ к которым ему ограничен.

3.3. Пользователь может посещать только те ресурсы, содержание которых не противоречит законодательству Российской Федерации, а цель посещения должна быть связана с его служебной деятельностью.

3.4. Внимательно набирать имена сайтов, особенно на которых проводятся финансовые операции. Поддельные сайты могут иметь отличие даже одного знака или тот же вид, что и оригинальные. Такие сайты могут содержать невидимые области, нажатие на которые может

привести к заражению АРМ вредоносными программами или перенаправление на зараженные сайты.

3.5. Пользователям запрещается:

- использовать доступ к сети Интернет в личных целях;

- посещать досугово-развлекательные сайты;

- использовать доступ к сети Интернет для распространения и тиражирования информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

4. Правила работы с электронной почтой

4.1. Для служебной деятельности необходимо использовать электронную почту домена, почтовые сервера Правительства Российской федерации. **Использование иных общедоступных почтовых сервисов должно быть исключено**. Используя общедоступные почтовые сервисы Вы **сознательно** предоставляете передаваемую информацию этим сервисам и она может быть доступна третьим лицам.

4.2. При получении электронного письма с вложением необходимо внимательно посмотреть адрес отправителя. В случае, если этот адрес неизвестен, или отличается от реального хотя бы одним знаком, открытие вложений таких писем не безопасно, поскольку могут содержать вредоносные программы.

4.3. При получении письма от неизвестного адресата, необходимо связаться с исполнителем и уточнить происхождение файлов. В случае невозможности установить происхождение письма, необходимо его удалить, не сохраняя и не запуская приложенные файлы.

4.4. Запрещается передавать информацию ограниченного доступа через сеть Интернет (в том числе посредством электронной почты) без использования средств защиты информации.

4.5. Необходимо своевременно очищать свой почтовый ящик.

5. Правила антивирусной защиты

5.1. Для обеспечения антивирусной защиты должно использоваться сертифицированное лицензионное антивирусное программное обеспечение.

5.2. Ярлык антивирусной программы, как правило, находится в области уведомления или на вкладке «отображать скрытые значки» (нижний правый угол экрана).

5.3. Пользователи при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

5.4. Обновление антивирусной программы, как правило, производится автоматически, в противном случае необходимо обратиться к администратору ЛВС.

5.5. Периодическое тестирование всего установленного программного обеспечения на предмет компьютерных вирусов производится автоматически. Полную проверку АРМ необходимо проводить при установке антивирусной программы, в случаях подозрения заражением, периодически 1 – 2 раза в год.

5.6. В случае обнаружения подозрительных программ срабатывает антивирус и необходимо прекратить какие-либо действия на АРМ и обратиться к техническому специалисту.

5.7. В случае обнаружения вируса, не поддающегося лечению, технический специалист, ответственный за обеспечение безопасности информации, принимает меры по восстановлению работы.

5.8. В тех случаях, когда заражение вирусом АРМ все-таки произошло, необходимо:

- немедленно отключить компьютер для остановки действий вредоносной программы, т.к. во время включений и перезагрузок происходят изменения файловой системы компьютера;

- не пытаться самостоятельно изменять расширения зараженных файлов, а также удалять любые файлы с рабочего компьютера и электронные сообщения;

- обратиться к техническому специалисту по информационным технологиям;

По информации производителей антивирусных программ возможность восстановления информации – минимальна, т.к. каждое вредоносное сообщение содержит индивидуальный файл-шифровальщик.

6. Парольная политика

6.1. Идентификация и проверка подлинности пользователя при входе в АРМ, информационную систему может осуществляться по паролю условно-постоянного действия.

6.2. Полная плановая смена паролей пользователей должна проводиться, по необходимости, только техническим специалистом.

6.4. Правила формирования пароля:

6.4.1. Пароль должен состоять не менее чем из трех символов.

6.4.2. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- цифры (от 0 до 9).

7. Ответственность Пользователя

Пользователи несут персональную ответственность за свои действия в период осуществления информационного взаимодействия с использованием АРМ;

За нарушение настоящего Свода правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, АРМ пользователя может быть отключен от ЛВС до выяснения обстоятельств нарушения.

Нарушение требований законодательства Российской Федерации об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную ответственность в соответствии с законодательством Российской Федерации.