МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 30

П Р И К А З

№ 379 от 30.08.2024

О назначении ответственного лица
за организацию работы в сети Интернет и ограничении доступа

В соответствии с Федеральным законом от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", в целях обеспечения доступа участников образовательных отношений к сети Интернет в соответствии с утвержденными и введенными в действие Правилами использования сети Интернет в МОБУ СОШ № 30

приказываю:

1. Суховеева М.В., инженера-программиста, назначить ответственным лицом за организацию работы в сети Интернет и ограничение доступа в школе.
2. Суховееву М.В.:

- запланировать использование ресурсов сети Интернет на 2024/2025 учебный год в образовательном учреждении на основании заявок учителей и других работников образовательного учреждения;
- разработать, согласовать с педагогическим коллективом, представить на педагогическом совете образовательного учреждения регламент использования сети Интернет, включая регламент определения доступа к ресурсам сети Интернет.

3. Возложить ответственность за осуществление контроля использования обучающимися сети Интернет во время проведения уроков и других занятий в рамках учебного плана на учителя, ведущего занятие.
4. Возложить ответственность за осуществление контроля использования ресурсов сети Интернет во время свободного доступа обучающихся к сети Интернет вне учебных занятий:

- при работе обучающихся в компьютерном классе (кабинет № 17) на Ильину Е.В., учителя информатики и ИКТ;

5. Утвердить следующий график работы для использования компьютерной техники, включая доступ участников образовательных отношений к сети Интернет:

компьютерный класс:

- проведение уроков информатики и ИКТ, других предметных уроков с использованием персональных компьютеров – ежедневно с 8.00 до 13.50 в соответствии с расписанием;
- проведение различных внеклассных мероприятий и индивидуально-групповых занятий – ежедневно с 12.55 до 15.00 по договоренности с учителем информатики;

6. Всем членам администрации, учителям и обучающимся МОБУ СОШ № 30 строго руководствоваться «Правилами использования сети Интернет».
7. Ильина Е.В., учитель информатики:

- организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;

- организует контроль использования сети Интернет в образовательном учреждении, работы оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;
- устанавливает по согласованию с директором критерии доступа пользователей;
- обеспечивает контроль целостности эксплуатируемого на средствах вычислительной техники программного обеспечения с целью выявления несанкционированных изменений в нём;
- организует контроль за санкционированным изменением ПО, заменой и ремонтом средств вычислительной техники;
- немедленно докладывает директору о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимает необходимые меры по устранению нарушений.

8. Утвердить регламент работы педагогических работников и обучающихся МОБУ СОШ № 30 в сети Интернет (приложение 1).
9. Утвердить инструкцию пользователя по безопасной работе в сети Интернет (приложение 2).
10. Утвердить инструкцию для сотрудников о порядке действий при осуществлении контроля за использованием обучающимися сети интернет (приложение 3).
11. Утвердить План мероприятий по обучению подростков правилам безопасного поведения в сети Интернет и защите детей от информации, не совместимой с целями образования (приложение 4).
12. Утвердить Положение о защите обучающихся от информации, причиняющей вред их здоровью и (или) развитию в МОБУ СОШ № 30.
13. Контроль исполнения приказа оставляю за собой.

Директор МОБУ СОШ № 30 В.В.Бобнев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2F592C2BFECE9063CB2D81371474607D
Владелец: Бобнев Валентин Викторович
Действителен: с 28.02.2024 до 23.05.2025

С приказом ознакомлены:
Суховеев М.В.
Ильина Е.В.

Одежная Л.В.
33-34-11

Приложение 1

Регламент работы педагогических работников и обучающихся
МОБУ СОШ № 30 в сети Интернет

I. Общие положения

«Точка доступа» к сети Интернет предназначена для обслуживания образовательных, информационных потребностей работников и обучающихся. Педагогические работники, сотрудники и обучающиеся (в дальнейшем пользователь) допускаются к работе на бесплатной основе.

К работе в Интернет допускаются пользователи, прошедшие предварительную регистрацию в журнале «Регистрации пользователей сети Интернет» у должностного лица, ответственного за использование сети Интернет (в дальнейшем администратор), получении Регистрационной карточки с логином и паролем.

Выход в сеть Интернет осуществляется по графику за закрепленным рабочим местом пользователя на основании предварительной записи в журнале «Учета времени работы в сети Интернет» у администратора или при наличии свободных мест в зависимости от категории пользователя:

- обучающимся предоставляется доступ в Интернет согласно расписанию занятий и после уроков;
- педагогическим работникам предоставляется доступ согласно служебным запискам на имя директора с указанием планируемого времени работы. Время работы в Интернет лимитируется администрацией образовательного учреждения.
- остальным пользователям предоставляется доступ при наличии резерва пропускной способности канала передачи.

Для работы в Интернет необходимо иметь при себе регистрационную карточку.

По всем вопросам, связанным с доступом в Интернет, следует обращаться к администратору Интернет-класса.

II. Правила работы

Время работы в сети регистрируется в журнале «Учета времени работы в сети Интернет».

Для доступа в Интернет используются программы «Internet Explorer», «Google Chrome», «Yandex Browser». Отправка электронной почты с присоединенной к письму информацией, запись информации на дискеты и оптические диски осуществляется у администратора.

При работе в Интернет пользователь обязан:

1. Выполнять все требования администратора.
2. В начале работы пользователь должен зарегистрироваться в системе, т.е. внести свой логин и пароль.
3. Запрещается работать под чужим регистрационным именем, сообщать кому-либо роль, одновременно входить в сеть более чем с одной рабочей станции.
4. Каждому пользователю, при наличии технической возможности, предоставляется персональный каталог для хранения личных данных общим объемом не более 5 Мб, возможность работы с почтовым ящиком для отправки и получения электронной почты.
5. Пользователю разрешается копировать информацию на диски, предварительно проверенные на вирус.
6. Пользователю запрещается любое копирование на жесткие диски.

7. Пользователю запрещено вносить изменения в программное обеспечение установленное на рабочей станции.
8. Запрещена передача информации, представляющей коммерческую или государственную тайну. Распространение информации, порочащей честь и достоинство граждан.
9. Запрещается работать с объемными ресурсами (video, audio, chat, игры и др.) без согласования с администратором.
10. Запрещается доступ к сайтам, содержащим информацию, противоречащую общепринятой этике.
11. Пользователь обязан сохранять оборудование в целостности и сохранности. При нанесении ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность в соответствии действующим законом.
12. Пользователь должен помнить свой пароль. В случае утраты пароля пользователь обязан сообщить об этом администратору.
13. При возникновении технических проблем пользователь обязан поставить в известность администратора.
14. За нарушения правил работы в сети Интернет пользователь получает первое предупреждение и лишается права выхода в Интернет сроком на 1 месяц. При повторном нарушении – пользователь лишается доступа в Интернет.

III. Правила регистрации

Для доступа в Интернет пользователь должен пройти процесс регистрации:
1.Пользователь обязан ознакомиться с «Регламентом работы обучающихся и педагогических работников в сети Интернет», расписаться в журнале учета работы в сети Интернет обучающихся и педагогических работников МОБУ СОШ № 30, получить регистрационную карточку.
2. Регистрационные логин и пароль обучающиеся получают у администратора.
3. Регистрационные логин и пароль сотрудники получают у администратора при предъявлении письменного заявления.
4. Перед работой необходимо ознакомиться с «Памяткой использования ресурсов сети Интернет».

Приложение 2

Инструкция пользователя по безопасной работе в сети Интернет

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью школы и предоставляются учащимся и учителям.

ПК, серверы, ПО, оборудование ЛВС и коммуникационное, пользователи образуют систему локальной сети МОБУ СОШ № 30.

1. Общие положения.

1.1. Настоящая инструкция является дополнением к Правилами использования сети Интернет.

1.2. Целью настоящей инструкции является регулирование работы системных администраторов и пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования.

1.3. К работе в системе допускаются лица, прошедшие инструктаж и регистрацию у ответственного за работу в сети Интернет.

1.4. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение системного администратора.

1.5. По уровню ответственности и правам доступа к СЕТИ пользователи СЕТИ разделяются на следующие категории: системные администраторы и пользователи.

1.6. Пользователь подключенного к СЕТИ компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.7. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым системным администратором.

1.8 Каждый сотрудник создает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 8 символов и состоять из букв и цифр.

1.9. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет, передача их кому-либо запрещена.

1.10. Для работы на компьютере кроме пользователя необходимо разрешение системного администратора. Никто не может давать разрешение на даже временную работу на компьютере, без разрешения системного администратора.

1.11. В случае нарушения правил пользования сетью, связанных с администрируемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, администратор имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.12. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо

другом, пользователь должен немедленно сообщить об этом системному администратору СЕТИ.
1.13. Системный администратор и лицо, обслуживающее сервер и следящее за правильным функционированием СЕТИ. Системный администратор дает разрешение на подключение компьютера к СЕТИ, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ.
1.14. Системный администратор информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности СЕТИ на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам СЕТИ.
1.15. Системный администратор имеет право отключить компьютер пользователя от СЕТИ в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.
1.16. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе.
2. Пользователи СЕТИ обязаны:
2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.
2.2. При доступе к внешним ресурсам СЕТИ, соблюдать правила, установленные системными администраторами для используемых ресурсов.
2.3. Немедленно сообщать системному администратору СЕТИ об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администраторы, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры.
2.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в СЕТИ.
2.5. Немедленно отключать от СЕТИ компьютер, который подозревается в заражении вирусом. Компьютер не должен подключаться к СЕТИ до тех пор, пока системные администраторы не удостоверятся в удалении вируса.
2.6. Обеспечивать беспрепятственный доступ специалистам к сетевому оборудованию и компьютерам пользователей.
2.7. Выполнять предписания специалистов, направленные на обеспечение безопасности СЕТИ.
2.8. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору.
3. Пользователи СЕТИ имеют право:
3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Системные администраторы вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.
3.2. Обращаться к администратору СЕТИ по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы

(например, установка на компьютере коллективного доступа), должны санкционироваться системным администратором СЕТИ.
3.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов СЕТИ.
3.4. Вносить предложения по улучшению работы с ресурсом.
4. Пользователям СЕТИ запрещено:
4.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами).
4.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования со специалистами.
4.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к СЕТИ, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.
4.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.
4.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без ведома системного администратора, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет.
4.6. Самовольно подключать компьютер к СЕТИ, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.
4.7. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с системным администратором СЕТИ. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен.
4.8. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
4.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.
4.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором: пытаться обходить установленный межсетевой экран при соединении с сетью Интернет.
4.11. Осуществлять попытки несанкционированного доступа к ресурсам СЕТИ, проводить или участвовать в сетевых атаках и сетевом взломе.
4.12. Использовать СЕТЬ для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.
4.13. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (системный администратор) не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

4.14. Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера Сети, равно как и любых других компьютеров в Интернет.
4.15. Закрывать доступ к информации паролями без согласования с системным администратором.
5. Работа с электронной почтой:
5.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.
5.2. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными.
5.3. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.
5.4. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными.
5.5. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.
5.6. Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.
5.7. Журналы почтовых серверов должны проверяться на предмет выявления использования неутвержденных почтовых клиентов сотрудниками организации, и о таких случаях должно докладываться.
5.8. Почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось с помощью цифровой подписи отправителя.
5.9. Необходимо организовать обучение пользователей правильной работе с электронной почтой.
5.10. Справочники электронных адресов сотрудников не могут быть доступны всем и являются конфиденциальной информацией.
5.11. Если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью организации, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в организации программ и алгоритмов.
5.12. Никто из посетителей, контрактников или временных служащих не имеет права использовать электронную почту организации.
5.13. Вся информация, классифицированная как критическая или коммерческая тайна, при передаче ее через открытые сети, такие как Интернет, должна быть предварительно зашифрована.
5.14. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности школы.
5.15. Пользователи не должны позволять кому-либо посылать письма от чужого имени.
5.16. Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.
5.17. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

5.18. Конфиденциальная информация не может быть послана с помощью электронной почты.
5.19. Если будет установлено, что сотрудник неправильно использует электронную почту с умыслом, он будет наказан.
5.20. Нельзя сообщать сторонним лицам электронные адреса сотрудников.
5.21. Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.
5.22. Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).
5.23. Использовать несуществующие обратные адреса при отправке электронных писем.
6. При работе с веб-ресурсами:
6.1. Пользователи используют программы для поиска информации в WWW только в случае, если это необходимо для выполнения своих должностных обязанностей.
6.2. Использование ресурсов сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать школе.
6.3. По использованию Интернет ведется статистика и поступает в архив школы.
6.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.
6.5. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности школы.
6.6. Все программы, используемые для доступа к сети Internet, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности.
6.7. Все файлы, загружаемые с помощью сети Internet, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.
6.8. Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Internet. Доступ к сети Internet предоставляется по служебной записке.
6.9. В организации должен вестись список запрещенных сайтов. Программы для работы с Internet должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.
6.10. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.
6.11. Запрещено получать и передавать через СЕТЬ информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
6.12. Запрещено получать доступ к информационным ресурсам СЕТИ или сети Интернет, не являющихся публичными, без разрешения их собственника.
7. Ответственность:
7.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.
7.2. Системный администратор отвечает за бесперебойное функционирование вверенной ему СЕТИ, качество предоставляемых пользователям сервисов.

7.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в СЕТИ и за ее пределами.
7.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы с СЕТЬЮ.
7.5. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или СЕТИ компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.

Приложение 3

Инструкция для педагогических работников
и сотрудников МОБУ СОШ № 30
о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательного учреждения при обнаружении:
1) обращения обучающихся к контенту, не имеющему отношения к образовательной деятельности;
2) отказа при обращении к контенту, имеющему отношение к образовательной деятельности, вызванного техническими причинами.
2. Контроль использования обучающимися сети Интернет осуществляют:
1) во время занятия — проводящий его преподаватель;
2) во время использования сети Интернет для свободной работы обучающихся — сотрудник ОУ, назначенный руководителем ОУ в установленном порядке.
3. Преподаватель:
— определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательной деятельности соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;
— наблюдает за использованием обучающимися компьютеров и сети Интернет;
— способствует осуществлению контроля объемов трафика ОУ в сети Интернет;
— запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;
— доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;
— принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательной деятельности.
4. При обнаружении ресурса, который, по мнению преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.
5. В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

Приложение 4

План мероприятий
по обучению подростков правилам безопасного поведения в сети Интернет и защите детей от информации, не совместимой с целями образования

Пояснительная записка

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование.

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

«Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать» (П.А.Астахов, уполномоченный при Президенте Российской Федерации по правам ребенка).

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 г. о защите несовершеннолетних и человеческого достоинства в Интернете, Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочного плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносным содержимым в рамках глобальных сетей).

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и

развитию"). Преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих школьников.

Для организации безопасного доступа к сети Интернет созданы следующие условия:

1. Разработаны и утверждены:

- РЕГЛАМЕНТ по работе учителей и школьников в сети Интернет
- ПРАВИЛА использования сети Интернет
- ИНСТРУКЦИЯ пользователя по безопасной работе в сети Интернет.
- ИНСТРУКЦИЯ для сотрудников о порядке действий при осуществлении контроля за использованием учащимися общеобразовательного учреждения сети Интернет.
- КЛАССИФИКАТОР информации, доступ к которой учащихся запрещен и разрешен (входит в ПРАВИЛА использования сети Интернет)

2. Контроль использования учащимися сети Интернет осуществляется с помощью программно-технических средств и визуального контроля.

Цели, задачи, основные мероприятия реализации плана

Цель: обеспечение информационной безопасности детей и подростков при обучении, организации внеучебной деятельности и свободном использовании современных информационно-коммуникационных технологий (в частности сети Интернет).

Задачи:

- формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;
- формирования информационной культуры как фактора обеспечения информационной безопасности;
- изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
- формирование знаний в области безопасности детей использующих Интернет;
- организации просветительской работы с родителями и общественностью.

№ п/п	Наименование мероприятия	Срок реализации	Ответственный исполнитель	Ожидаемые результаты
1.	Изучение нормативных документов, регламентирующих вопросы использования в образовательном процессе информационно-коммуникационной сети Интернет			
1.1.	Организация и проведение совещаний, семинаров	Сентябрь Апрель	Администрация ОУ	Организация деятельности ОУ в правовом поле
1.2.	Приведение в соответствие с существующим законодательством локальных нормативных документов школы	В течение всего периода	Администрация ОУ	Обновление локальных нормативных актов, должностных инструкции
1.3.	Обсуждение вопросов обеспечения информационной безопасности обучающихся на заседаниях коллегиальных органов	Общее собрание работников – март	Администрация ОУ	Координация деятельности сотрудников

	школы			
1.4.	Создание и реализация программ обучения навыкам безопасного поведения в Интернет-пространстве, профилактике Интернет-зависимости, рисков вовлечения в противоправную деятельность	По запросу участников образовательных отношений	Администрация ОУ	Система работы школы по обеспечению информационной безопасности
2.Организационно-распорядительная деятельность				
2.1.	Назначение ответственных лиц, обеспечивающих безопасность работы в сети Интернет	Сентябрь	Администрация ОУ	Обеспечение системы работы
2.2.	Установка, регистрация и обновление технических и программно-аппаратных средств защиты на школьные компьютеры	В течение всего периода	Администрация ОУ	Ограничение доступа к запрещенной информации, обеспечение адаптации к изменяющимся угрозам, условиям эксплуатации, требованиям законодательства РФ и предписаниям надзорных органов.
2.3.	Ведение журнала регистрации учета работы учащихся и сотрудников в сети Интернет	В течение всего периода	Ответственный за кабинет № 17	Упорядочение доступа в Интернет
2.4.	Дополнение Правил пользования сетью Интернет	В течение всего периода	Администрация ОУ	Ознакомление участников образовательных отношений
2.5.	Осуществление внутреннего контроля безопасного доступа в Интернет	По плану школы	Администрация ОУ	Контроль исполнения локальных нормативных актов школы
2.6.	Мониторинг технических и программно-аппаратных	Ежегодно, апрель	Администрация ОУ	Регулирование деятельности по

	средств защиты, а также официальной регистрации установленных на компьютерное оборудование средств контентной фильтрации			использованию СКФ
3.Организация образовательной деятельности				
3.1.	Использование учебников в соответствии со списком, утвержденных и (или) рекомендованных Минобрнауки РФ	В течение всего периода	Администрация ОУ	
3.2.	Организация изучения обучающимися правил личной безопасности при работе в сети Интернет и этике поведения в Интернете в рамках реализации общеобразовательных программ по информатике и информационно-коммуникационным технологиям на всех уровнях общего образования (1-11 классы), а также дополнительных общеобразовательных программ	В течение всего периода	Администрация ОУ, учителя-предметники, классные руководители	Обеспечение полноты реализации лицензионных программ
3.3.	Создание и распространение информационных буклетов и памяток для участников образовательных отношений	В течение всего периода	Администрация ОУ, учителя-предметники, классные руководители	Создание рекламных продуктов
3.4.	Организация внеклассных мероприятий, тематических классных часов, работы школьных радио и печатных средств информации по вопросам формирования онлайн-репутации молодых пользователей	В течение всего периода	Администрация ОУ, учителя-предметники, классные руководители	Формирование законопослушного поведения учащихся

	информационных ресурсов, соблюдения авторских прав на материалы, размещенные в сети, обеспечения конфедециальности информации и безопасности общения в социальных сетях, защиты от вредоносных сайтов и вирусов в сети Интернет и др.			
3.5.	Организация участия детей в творческих конкурсах соответствующей тематики	В течение всего периода	Администрация ОУ, учителя-предметники, классные руководители	Повышение социальной активности учащихся
4.Организация работы с родителями				
4.1.	Проведение тематических родительских собраний об обеспечении дома защиты детей от информации, причиняющей вред их здоровью и развитию.	В течение всего периода	Администрация ОУ, классные руководители	Вовлечение родителей в деятельность школы по обеспечению информационной безопасности детей.
4.2.	Просвещение родителей (законных представителей) в вопросах информационной безопасности через страницу школьного сайта.	В течение всего периода	Администрация ОУ, классные руководители	