МБОУ «Украинская СОШ

«Утверждаю»

Директор МБОУ «Украинская СОШ

_____ Прилипко Т.В.

Приказ № 92 от « 02» сентября 2022 г.

Рабочая программа по обеспечению безопасной информационной среды учащихся

ПАСПОРТ ПРОГРАММЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ В ШКОЛЕ

Нормативно-правовая база программы

- Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;
- Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 №152 «О персональных данных»;
- «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10 с изменениями и дополнениями от 29 июня 2011 г., 25 декабря 2013 г., 24 ноября 2015 г.
- Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471 -р»

Материально – техническое обеспечение учебного процесса

В школе созданы условия для всех участников образовательного процесса:

- 2 компьютерных класса (22 посадочных места);
- 1 учебный кабинет оборудованных мультимедийными комплектами;
  из них 1 кабинет оборудованы интерактивными досками в комплекте;
- имеется выход в Интернет;
- все компьютеры, используемые в учебном процессе, подключены к Интернету;
- 6 компьютеров, используемые в работе администрации, подключены к Интернету;
- создан и функционирует официальный сайт школы;
- функционирует электронный журнал/электронный дневник школы;

Цели и задачи программы

Цели программы

- Обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России.

• Формирование безопасной информационной образовательной среды в школе, обеспечение информационной безопасности учащихся, использующих Интернет в образовании и пропаганда безопасного поведения в сети Интернет.

Задачи программы:

• формирование у детей навыков самостоятельного и ответственного потребления информационной продукции;
• повышение уровня медиаграмотности детей;
• формирование у детей позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке;
• ценностное, моральное и нравственно-этическое развитие детей;
• формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;
• формирование 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;
• организация просветительской работы с родителями и общественностью;
• организация технического контроля безопасности.

Основные направления программы

• Разработка и внедрение эффективной модели организации процесса информатизации, включающей информационно-методическое, кадровое и материально-техническое обеспечение.
• Формирование и апробация инновационных подходов к информатизации школы.
• Оснащение школы современными электронными учебными материалами.
• Подготовка педагогических кадров к освоению и эффективному внедрению информационных и коммуникационных технологий в образовательный процесс.
• Обеспечение школы средствами информационных и коммуникационных технологий.

Планируемые результаты реализации программы

Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:
• обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу;

• поможет родителям грамотно организовать информационное пространство ребенка в семье;
• совместные усилия педагогов и родителей создадут рабочую среду ребенка и в школе, и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

Будет создана новая медиасреда, соответствующая следующим характеристикам:
• наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
• свободный доступ детей к историко-культурному наследию предшествующих поколений;
• качественный рост уровня медиаграмотности детей;
• увеличение числа детей, разделяющих ценности патриотизма;
• гармонизация меж- и внутрипоколенческих отношений;
• популяризация здорового образа жизни среди молодого поколения;
• формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;
• снижение уровня противоправного и преступного поведения среди детей;
• формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента. (Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471 -р»)

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». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование и стал неотъемлемой частью нашей повседневной жизни. Использование Интернета в образовательных учреждениях и дома расширяет информационное образовательное пространство обучающего и позволяет повысить эффективность обучения. Доступ учащихся к информационным ресурсам сети Интернет дает возможность школьникам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельного обучаться. Благодаря таким ресурсам у школьников появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие.

Использование Интернета в работе с детьми и в работе школы достаточно обширно:

- это использование электронной почты;
- поиск в сети нужной информации;
- создание собственных школьных веб-страниц;
- рассылка и/или съем материалов (нормативных документов, информации о семинарах и конкурсах и т.п.);
- обмен опытом;
- ответы на типичные вопросы;
- получение ("скачивание") небольших обучающих программ по разным предметам;
- участие в различных интернет - проектах, конкурсах, акциях.

Однако использование Интернета в образовательной деятельности таит в себе много опасностей, существует ряд аспектов, 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.

Важно, чтобы во всех школах был безопасный Интернет.

По статистическим данным на сегодняшний день в России насчитывается от 9 до11 млн. интернет-пользователей в возрасте до 14 лет. Две трети детей выходят в глобальную сеть самостоятельно, без присмотра родителей и педагогов.

Примерно 60% школьников посещают веб-страницы нежелательного и запрещенного содержания. У многих развивается интернет-зависимость и игромания.

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 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 вредоносного содержимого в рамках глобальных сетей).

ПРОГРАММА
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ
«БЕЗОПАСНЫЙ ИНТЕРНЕТ В ШКОЛЕ»

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.

Согласно Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471 -р, обеспечение информационной безопасности должно строиться на следующих принципах:

- признание детей равноправными участниками процесса формирования информационного общества в Российской Федерации;
- ответственность государства за соблюдение законных интересов детей в информационной сфере;
- необходимость формирования у детей умения ориентироваться в современной информационной среде;
- воспитание у детей навыков самостоятельного и критического мышления; развитие государственно-частного партнерства в целях обеспечения законных интересов детей в информационной среде;
- повышение эффективности сотрудничества представителей средств массовой информации и массовых коммуникаций и государственных органов в интересах защиты детей от информации, способной причинить вред их здоровью и развитию;
- обучение детей медиаграмотности;
- поддержка творческой деятельности детей в целях их самореализации в информационной среде;
- создание условий для формирования в информационной среде благоприятной атмосферы для детей вне зависимости от их социального положения, религиозной и этнической принадлежности;
- взаимодействие различных ведомств при реализации стратегий и программ в части, касающейся обеспечения информационной безопасности детей;
- обеспечение широкого доступа детей к историческому и культурному наследию России через использование современных средств массовых коммуникаций;

- открытость и взаимодействие с другой информационной культурой и традициями, формирование у детей объективного представления о российской культуре как неотъемлемой части мировой цивилизации.

Работа с учащимися должна вестись в зависимости от возрастных особенностей: начальное звено (1-4 классы), среднее (5-9 классы), старшее (10-11 классы). На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями.

Для организации безопасного доступа к сети Интернет в МБОУ «Украинская СОШ»;

созданы следующие условия:

1. В образовательном учреждении разработаны и утверждены:

— РЕГЛАМЕНТ работы в сети Интернет в МБОУ «Украинская СОШ»;

— ПОЛОЖЕНИЕ об использовании сети Интернет в МБОУ «Украинская СОШ»;

— ПОЛОЖЕНИЕ об информационной открытости МБОУ «Украинская СОШ»;

— ПОЛОЖЕНИЕ о сайте МБОУ «Украинская СОШ»;

— Порядок доступа педагогических работников к информационно телекоммуникационным сетям, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности;

— ПОЛОЖЕНИЕ об электронном журнале успеваемости/электронном дневнике учащегося в МБОУ «Украинская СОШ»;;

— ИНСТРУКЦИЯ для педагогических сотрудников о порядке действий при осуществлении контроля за использованием учащимися МБОУ «Украинская СОШ»;сети Интернет;

— КЛАССИФИКАТОР информации, не имеющей отношения к образовательному процессу;

— Регламент работы с электронной почтой в «Украинская СОШ»;;

— Инструкция по организации антивирусной защиты в МБОУ «Украинская СОШ»;;

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

3. На официальном сайте школы создана страница «Информационная безопасность», на которой размещены материалы, посвященные безопасному поведению в сети Интернет и его использованию. А также на сайте размещены полезные ссылки для обучающихся и родителей.

4. Ведется журнал учета работы в сети Интернет.

5. Ежегодно проводится Декада безопасности в сети Интернет.

Механизм реализации программы

Безопасность детей одна из главных задач цивилизованного общества, поэтому обеспечивать безопасность детей в Интернете должны все, кто причастен к этому обществу.

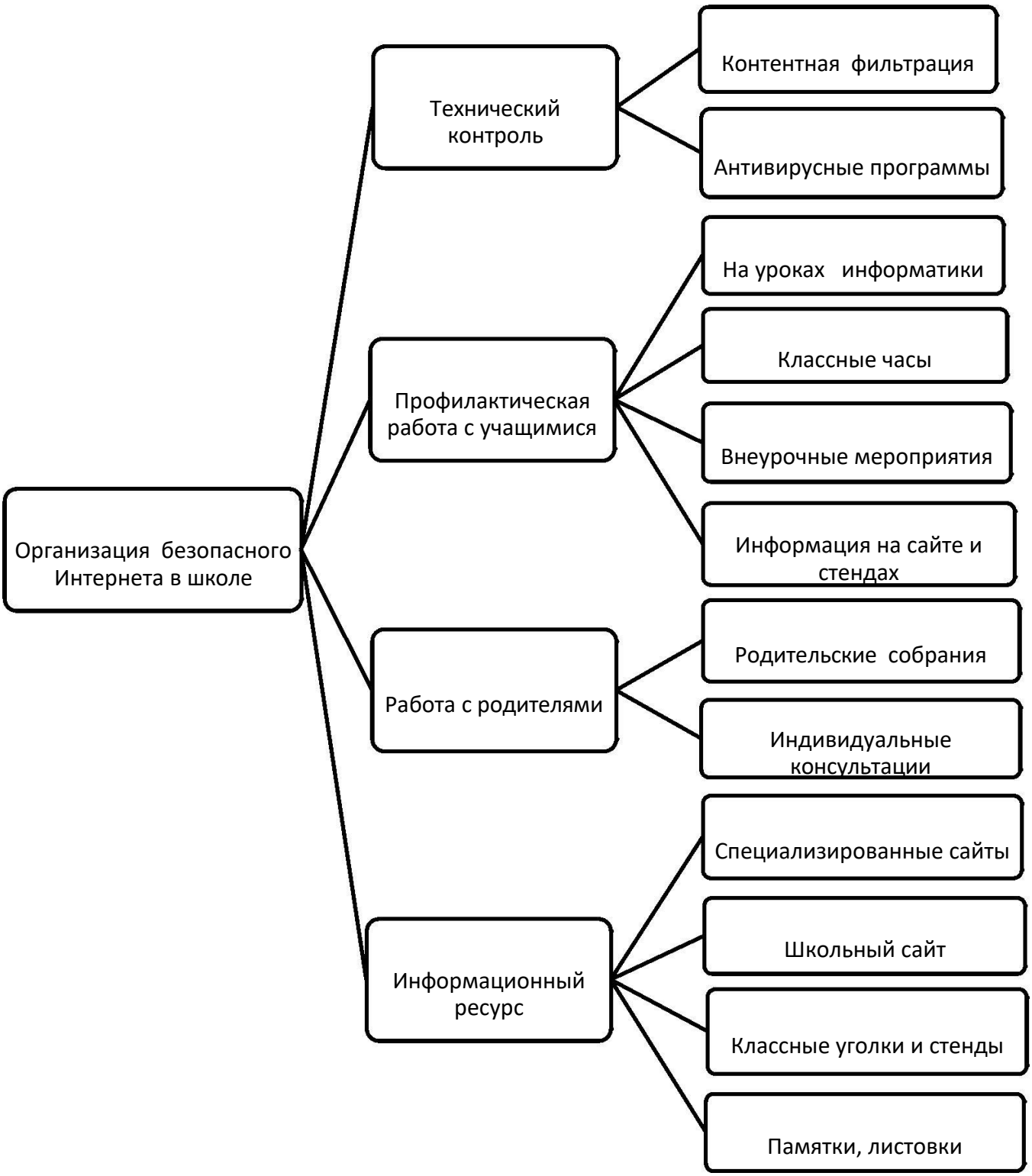
Контроль за учащимися в сети Интернет осуществляют:

1) во время проведения занятий - учитель, проводящий занятие;

2) во время использования сети Интернет для свободной работы учащихся - лицо, назначенное приказом директора школы по вопросам регламентации доступа к информации в Интернете.

Данные лица обладают необходимой квалификацией и знаниями в области информационных технологий.

Для решения вопросов безопасности Интернета в школе организован технический контроль, ведется профилактическая работа с обучающимися и их родителями, доступны информационные ресурсы для всех участников образовательного процесса.



Технический контроль

Чтобы ограничить доступ учащихся к информации, которая может оказать на них негативное воздействие, в школе установлена специальная система фильтрации NetPolice Pro, исключающая доступ к такой информации. Программой блокируется доступ к сайтам, содержащим материалы, которые определены как опасные. Антивирусный пакет компании «Касперский», установленный на все компьютеры, также позволяет ограничить доступ юных пользователей Интернета к нежелательному контенту и обеспечить безопасность школьной компьютерной сети.
Обе программы позволяют организовать доступ в Интернет по «черным» и «белым» спискам.

Профилактическая работа с обучающимися

Для преодоления негативного воздействия сети Интернет школа должна проводить целенаправленную воспитательную работу с педагогическим коллективом, учащимися, родителями.
Необходимо научить детей извлекать из ресурсов только лучшее и безопасное, делать осознанный и грамотный выбор.
Необходимо обсуждать с детьми все вопросы, которые возникают у них при использовании Интернет. Чем больше взрослые будут знать о том, как дети используют Интернет, тем проще определить и объяснить, что является приемлемым и безопасным.
Работа с учащимися проводится с учетом их возрастных особенностей. В начальной школе - в виде сказок, игр. В среднем звене - в виде бесед, ролевых игр, диспутов, тренингов. В старшем звене – в виде проектов, участия в акциях.
Ежегодно в нашей школе проходит традиционная Декада безопасности в сети Интернет. Программа, посвященная этой Декаде, включает в себя ряд мероприятий, направленных на обучение учителей, родителей и детей правилам безопасного пользования Интернетом. Это классные часы по теме «Безопасность в сети Интернет»; выпускаются листовки с памятками для учащихся «Безопасность в Интернете», проводится онлайн - тестирование по интернет - безопасности.
Ежегодно учащиеся нашей школы принимают участие во всероссийской акции «Час кода», а также являются активными участниками «Единого урока по безопасности в сети и квеста «Сетевичок».

Профилактическая работа с родителями

Формы работы с родителями различны - родительские собрания, индивидуальные беседы, лекции. Родители должны понимать, что никто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Только они могут полностью контролировать своих детей.
Для разъяснения родителям опасностей Интернета проводятся родительские собрания «Безопасный Интернет - детям».

Информационный ресурс

Для достижения положительных результатов необходимо проводить комплексную работу семьи и школы. Именно учителя и родители смогут предостеречь детей от возможных опасностей и ошибок. Существует ряд сайтов, посвященных безопасности детей в Интернете: http://персональныеданные.дети, http://rkn.gov.ru/personal-data/, http://сетевичок.рф/, www.detionline.org, www.interneshka.ru , ресурсы которых оказывают огромную помощь, как взрослым, так и детям. Также информация для родителей и детей по безопасной работе в Интернет размещена на официальном сайте школы и в классных уголках.
Таким образом, в школе необходимо регулярно вести работу по формированию безопасной информационной образовательной среды школы, обеспечению информационной безопасности учащихся, использующих Интернет в образовании, и пропаганде безопасного поведения в сети Интернет.

Прогноз возможных негативных последствий и способы коррекции, компенсации негативных последствий

Запрет доступа к негативной информации формирует у ребенка желание получить эту информацию, во что бы то ни стало. И эту информацию он может получить вне школы и дома у друзей или знакомых. Поэтому очень важно формировать информационную культуру и создать индивидуальную рабочую среду ребенку и в школе и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

Планируемые результаты

Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:

- обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу;
- поможет родителям грамотно организовать информационное пространство ребенка в семье;
- совместные усилия педагогов и родителей создадут рабочую среду ребенка и в школе, и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

Будет создана новая медиасреда, соответствующая следующим характеристикам:

- наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
- свободный доступ детей к историко-культурному наследию предшествующих поколений;
- качественный рост уровня медиаграмотности детей;
- увеличение числа детей, разделяющих ценности патриотизма;
- гармонизация меж- и внутрипоколенческих отношений;
- популяризация здорового образа жизни среди молодого поколения;
- формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;
- снижение уровня противоправного и преступного поведения среди детей;
- формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента». (Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р).

Перспективы дальнейшей работы школы по созданию Интернет - пространства для участников образовательного процесса

Формирование информационной культуры и безопасности - процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Задача взрослых (педагогов, родителей) - формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности. А для этого необходимо повышать квалификацию

педагогов по вопросам информационной безопасности, чтобы уметь оперативно ориентироваться и ориентировать детей по безопасному поведению в Интернете. Регулярно проводить родительский всеобуч по вопросам кибербезопасности и работать не вдогонку, а на опережение.

Перечень приложений:

Приложение 1. План мероприятий по обеспечению информационной безопасности обучающихся;

Приложение 2. Методические рекомендации «Безопасный Интернет»;

Приложение 3. Памятка родителям по управлению безопасностью детей в интернете;

Приложение 4. Памятка для детей по безопасному поведению в интернете;

Приложение 5. Классификатор информации, не имеющей отношения к образовательному процессу;

Приложение 6. Инструкция по организации антивирусной защиты в МБОУ «Украинская СОШ»;

Приложение 7. Инструкция для педагогических работников о порядке действий при осуществлении контроля за использованием учащимися МБОУ «Украинская СОШ»; сети Интернет;

Приложение 1.

План мероприятий по обеспечению информационной безопасности обучающихся МБОУ «Украинская СОШ»;

№ п/п	Наименование мероприятия	Срок исполнения	Исполнители, ответственные за реализацию мероприятия	Ожидаемые результаты (количественные и качественные показатели)
I. Создание организационно-правовых механизмов защиты детей от распространения информации, причиняющей вред их здоровью и развитию				
1.1	Проведение внеурочных занятий с учащимися по теме «Приемы безопасной работы в Интернете»	Ежегодно сентябрь	Классные руководители	100% охват учащихся школы
1.2	Ознакомление родителей с Положением о защите детей от информации, причиняющей вред их здоровью и развитию	Январь - февраль 2018	Классные руководители	100% ознакомление родителей с информацией по медиабезопасности
1.3	Ознакомление родителей с программой информационной безопасности	Март 2018	Классные руководители	100% ознакомление родителей
1.4.	Функционирование контент - фильтра в образовательном учреждении	В течение образовательного процесса	Зам. директора ответственный администратор	Обеспечение контент - фильтрации трафика
1.5.	Функционирование антивирусных программ в образовательном учреждении	В течение образовательного процесса	Зам. директора ответственный администратор	Обеспечение антивирусной защиты всех ПК
II. Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно-программных и техникотехнологических устройств				
2.1.	Мониторинг функционирования и использования в школе программного продукта, обеспечивающего контент - фильтрацию Интернет - трафика.	Ежеквартально	Рабочая комиссия	Обеспечение контент фильтрации трафика.

2.2.	Мониторинг функционирования и использования в школе программного продукта, обеспечивающего антивирусную защиту всех ПК	Ежеквартально	Рабочая комиссия	Обеспечение антивирусной защиты всех ПК.
2.3.	Мониторинг качества предоставления провайдером услуги доступа к сети Интернет образовательным учреждениям с обеспечением Контент - фильтрации Интернет - трафика	Ежеквартально	Рабочая комиссия	100% обеспечение услуги доступа в сеть Интернет школе с обеспечением Контент - фильтрации Интернет - трафика
III. Профилактика у обучающихся интернет - зависимости, игровой зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации.				
3.1.	Проведение медиауроков по теме «Информационная безопасность»	По рабочим программам	Классные руководители, учитель информатики	Обеспечение 100% охвата учащихся школы Повышение грамотности обучающихся по проблемам информационной безопасности.
3.2.	Проведение недели (месячника) «Интернет безопасность» для учащихся 1 -4 классов, 5-9 классов и их родителей.	По планам ведомственных организаций	Классные руководители, учитель информатики, библиотекарь.	Повышение грамотности обучающихся, родителей (законных представителей) по проблемам информационной безопасности
3.3.	Ведение раздела «Информационная безопасность» на школьном сайте	В течение образовательного процесса	Администратор сайта	Актуальность раздела.
3.4.	Организация и проведение обучающих семинаров для учителей по созданию надежной системы защиты детей от противоправного контента в образовательной	Два раза в год	Зам. директора	Повышение грамотности по проблемам информационной безопасности всех участников

	среде школы и дома.			образовательного процесса
3.5.	Организация свободного доступа обучающихся и учителей к высококачественным и сетевым образовательным ресурсам, в том числе к системе современных учебных материалов по всем предметам.	В течение образовательного процесса	Ответственный администратор	100% обеспечение доступа обучающихся и учителей к электронным образовательным ресурсам через сеть Интернет
3.6.	Внедрение и использование программно-технических средств, обеспечивающих исключение доступа обучающихся школы к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания	В течение образовательного процесса	Ответственный администратор	Отслеживание созданных, обновленных программно-технических средств, обеспечивающих исключение доступа обучающихся школы к ресурсам сети Интернет и установка их на компьютеры

Приложение 2.

Методические рекомендации «Безопасный Интернет»

В наши дни компьютер становится привычным элементом не только в научных лабораториях, но и дома, в школьных классах. Так, например, в Российской Федерации в настоящее время уже эксплуатируется не менее 5 млн. персональных компьютеров. В Западной Европе компьютер используют свыше 60% взрослого населения. Людей, ежедневно проводящих за компьютером по нескольку часов, становится все больше. При этом уже мало кто сомневается, что работа на персональном компьютере влияет на физическое и психологическое здоровье человека не самым лучшим образом. Длительное пребывание у экрана, неподвижность позы пользователя ПК, электромагнитные поля и излучения, мелькание изображения на экране - все это небезвредно для здоровья.

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет - это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины.

Одним из средств решения этой проблемы может стать просвещение общественности и специальная подготовка профессионалов, в первую очередь, педагогов в сфере безопасного поведения человека, специалиста, школьника в мире компьютерных технологий и Интернет.

В данном разделе представлены материалы для разработки классных часов для школьников трех возрастных групп, направленные на обеспечение необходимыми знаниями в области психолого-педагогического и здоровьесберегающего сопровождения образовательного процесса, персонала и школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности. Кроме того, пособие может быть интересно родителям школьников, так как содержит советы и рекомендации, как сделать компьютер и Интернет безопасным для своего ребенка.

Данные рекомендации - практическая информация для родителей и классных руководителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Родительское собрание

Тема: «Интернет: плюсы и минусы»

Цель: рассказать родителям, какие угрозы существуют и как их избежать.

«Ваши дети дома?»

Незатейливый вопрос, адресованный родителям, каждый вечер звучит в телеэфире. Дети дома, но в безопасности ли они?

С тех пор, как Интернет перестал быть роскошью и пришел буквально в каждый дом, он стал неотъемлемой частью жизни не только взрослых, но и детей.

Даже родители, некогда расценивавшие доступ во Всемирную сеть как баловство, вынуждены признать: Интернет содержит массу полезной для ребенка информации, помогает в выполнении школьных заданий, расширяет кругозор и является своеобразным «окном в большой мир».

С другой стороны, только очень наивный взрослый не знает, сколько в Сети ресурсов, которые отнюдь не назовешь безопасными - особенно для детей, любопытных и жадных до новых знаний. Судите сами: программы, запрещающие доступ к «плохим» ресурсам, не оправдывают надежд, поскольку просто не в силах фильтровать все вредоносное содержимое.

Как должны родители помочь детям снизить эти риски? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка. Вот вы, родители, на данный момент знаете, какими сайтами пользуются ваши дети? Нет? Очень печально. Именно с этого надо начинать работу с безопасным интернетом.

Для детей и молодежи Интернет главным образом является социальной средой, в которой можно не только встречаться с друзьями, но и с незнакомцами. В Интернете пользователя могут обидеть, запугать или даже оскорбить. Лучшей защитой является руководство собственным здравым смыслом. Наиболее важной задачей является предупреждение детей об опасностях Интернета, чтобы они вели себя осторожно. Кроме того, необходимо обсуждать с детьми все вопросы, которые могут у них возникнуть при использовании Интернета. Не отвергайте детей, а наоборот, постарайтесь как можно ближе расположить их доверие. Тогда вы будете в курсе той информации, которой владеют ваши дети.

Даже если ребенок не сталкивался с оскорблениями в Интернете, рекомендуется обсудить с ним следующие вопросы:

- Не распространяйте контактную или личную информацию, например, фотографии, без тщательного обдумывания возможных последствий. Интерактивная дружба может закончиться. Когда это произойдет, личная информация может быть отправлена злоумышленникам.
- В Интернете каждый человек имеет право на уважительное отношение.
- Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте.

Безопасное использование в соответствии с возрастом

Дети до 7 лет

Во время первого знакомства с Интернетом закладывается фундамент для его последующего использования и формирования хороших манер у детей. Детям дошкольного возраста нравится установленный порядок, и это является идеальным способом развития у детей навыков безопасного использования Интернета.

Дети до 7 лет могут не полностью понимать информацию, доступную в Интернете, и, например, не отличать рекламу от действительного содержимого. В этом возрасте родителям необходимо помогать детям в поиске подходящего материала. Дети часто не видят разницы между использованием Интернета и играми или рисованием на компьютере.

На этом этапе вы можете установить первые внутренние правила использования компьютера.

Время, проводимое за компьютером, необходимо ограничить по причинам, связанным со здоровьем.

Поместите компьютер, например, в гостиной. При использовании Интернета дошкольниками рекомендуется присутствие взрослого.

Доступ к Интернету для дошкольников необходимо ограничить до списка знакомых веб-сайтов, выбранных заранее. Более подготовленные дети могут найти знакомые сайты в меню «Избранное» обозревателя Интернета.

Самым безопасным решением является создание для ребенка персональной рабочей среды, в которой выбор сайтов ограничивается только указанными сайтами.

Дети 7-9 лет

Юные школьники будут иметь дело с Интернетом не только у себя дома, но и в школе, и у друзей. Вы вместе с детьми должны обсудить, как использовать Интернет надлежащим образом и согласовать правила, которым необходимо следовать. Дети 7-9 лет уже могут иметь относительно хорошее представление о том, что они видят. Тем не менее, они не готовы к обращению со всем материалом, доступным в Интернете, особенно с пугающим или неуместным материалом (изображения, текст или звук). Разговор об этих материалах и объяснение различных вещей, с которыми дети могут столкнуться в Интернете, поможет детям стать ответственными и способными самостоятельно и безопасно работать в Интернете. Вы можете поделиться собственными мнениями и взглядами на использование Интернета, чтобы помочь своим детям.

В этом возрасте ограничения, защита и использование Интернета под присмотром по-прежнему являются первостепенными. Родителям и детям рекомендуется согласовать правила использования Интернета и пересматривать их по мере взросления детей.

Использование Интернета дома по-прежнему разрешено только в присутствии родителей. Это обеспечивает получение помощи в любой проблемной ситуации.

Если компьютер установлен в комнате, которой пользуется вся семья, использование Интернета становится естественным для повседневной жизни.

Ребенок еще не может определить надежность веб-сайта самостоятельно, поэтому ему всегда следует спрашивать разрешения у родителей перед публикацией личной информации.

Для предотвращения доступа к неуместным сайтам можно также применять программы фильтрации, но важно, чтобы родители по-прежнему активно участвовали в использовании

Интернета ребенком.

Дети 10-12 лет

Школьники уже могут знать, как использовать Интернет в различных целях. Родители могут поддержать ребенка, выяснив, какие сайты могут помочь с домашним заданием, содержат информацию о хобби или других увлечениях ребенка. Интернет может также использоваться для планирования вопросов, касающихся всей семьи. Это дает возможность родителям и детям обсудить надежность разных сайтов, а также источники поиска полезной и качественной информации.

Ребенку необходим родительский присмотр и контроль, а также знание правил правильной работы в Сети. Тем не менее, ребенок может узнать, как избавиться от присмотра и обойти правила, если он будет считать их слишком ограничивающими или несоответствующими его потребностям.

Родителям и детям необходимо прийти к соглашению относительно разрешенных и запрещенных действий в Интернете, а также его использования. В соглашении должны быть учтены все потребности и мнения. Договоритесь, какую личную информацию можно разглашать и в каких случаях, а также поговорите о рисках, связанных с разглашением информации.

Если ребенок уже заинтересовался общением в чатах или IRC, вам следует обсудить с детьми их безопасность и контролировать их опыт в интерактивных обсуждениях.

Многие дети любопытны и любознательны, поэтому родителям необходимо акцентировать внимание на необходимости безопасного и осторожного использования.

Систему безопасности информации также необходимо обновлять.

Дети 13-15 лет

В этом возрасте Интернет становится частью социальной жизни детей: в Интернете они знакомятся и проводят время, ищут информацию, связанную с учебой или увлечениями. При более высоком уровне грамотности использование Интернета открывает множество возможностей. Родителям, может быть, очень сложно узнать о том, чем их ребенок занимается в Интернете. В этом возрасте дети также склонны к риску и выходу за пределы дозволенного. Технические ограничения и запреты могут оказаться неэффективным способом повышения уровня безопасности в Интернете.

Дети 13-15 лет могут захотеть сохранить свои действия в тайне, особенно если родители раньше не интересовались и не узнавали о способах использования Интернета ребенком. Важным моментом для семьи становится участие в открытых дискуссиях, а для родителей — заинтересованность в том, что ребенок делает и с кем использует интернет ресурсы.

Что за угрозы подстерегают наших детей в виртуальном мире? Этот вопрос задают многие родители, которые ещё не сталкивались с проблемами использования интернета. Поэтому целью собрания является рассказать, какие угрозы существуют и как их избежать.

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым!

Если вы не знаете с чего начать, ознакомьтесь с приведенными ниже советами, которые помогут вам научить детей принципам безопасной работы в Интернете.

1.	Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Путешествуйте в Интернете вместе с детьми.
2.	Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.
3.	Если ваши дети общаются в чатах, пользуются программами мгновенной передачи сообщений, играют в сетевые игры или занимаются в Интернете чем-то другим, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.
4.	Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.
5.	Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы.
6.	Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения нисколько не изменяются.
7.	Добейтесь от детей уважения к собственности других пользователей Интернета. Расскажите детям, что незаконное копирование продуктов труда других людей, в том числе музыки, видеоигр и других программ, почти не отличается от воровства в магазине.
8.	Убедите детей в том, что они не должны встречаться с интернет - друзьями лично. Скажите, что интернет - друзья могут на самом деле быть не теми, за кого они себя выдают.
9.	Объясните детям, что верить всему, что они видят или читают в Интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации им следует обратиться за советом к вам.
10.	Контролируйте действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб - узлы посещают ваши дети, и узнавать, что они там делают.

Представьте себе Интернет, в котором нет порнографических сайтов, сомнительных социальных сетей, откровенных блогов, онлайн-казино, страниц, пропагандирующих фашизм, насилие и религиозную нетерпимость - словом, представьте себе действительно безопасный Интернет, в который вы спокойно «отпустите» своего ребенка одного. Недавно об этом можно было только мечтать, сейчас же каждый может убедиться в том, что мечта стала явью - достаточно скачать с сайта www.icensor.ru и установить на домашнем компьютере программу «ИнтернетЦензор».

Безусловный плюс «Интернет Цензора» в том, что программу эту каждый родитель может «подстроить» под себя и своего ребенка, адаптировать к его интересам и увлечениям. Вам понадобится лишь пара минут на то, чтобы разрешить доступ к той или иной страничке. С другой стороны, если тот или иной «открытый» сайт покажется вам вредным для ребенка, запретить доступ к нему тоже не составит труда.

«Интернет Цензор» — удобная и простая программа, не требующая мощного компьютера и специальных знаний. Распространяется она бесплатно, так же бесплатны и все обновления - это принципиальная позиция создателей программы, изменять которой они не собираются.

Говоря о безопасности детей в Интернете, акцент следует сделать на то, что самое главное - это доверие между родителями и ребенком, готовность взрослых к диалогу, обсуждению непростых вопросов, да и просто разговорам о том, «что такое хорошо и что такое плохо».

Материалы для разработки классного часа.
Интернет для обучающихся начальных классов.
Безопасность детей в Интернете

Пока мы спорим "пущать" или "не пущать" учеников начальной школы в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете. Как?

Проблема относительно «свежая», но, решается «старыми» методами.

1) Родители должны знать, чем заняты их дети. Самое простое - разговаривать с детьми: чем живет, чем интересуется, какие сайты любит посещать и почему, с кем дружит, в том числе, и в Интернете. Кроме того (не вместо - кроме!) семейный фильтр на поисковой машине, контроль по логам и проч.

Дети должны владеть основами безопасного пользования Интернет-сетями. Мы учим их не разговаривать с незнакомцами? Мы объясняем, что нельзя называть незнакомцам свой домашний адрес? Ну, и в сети все то же самое.

2) Учитель должен понимать, зачем он отправляет детей в Интернет. Учить «с Интернетом» нынче модно. Всегда ли это оправдано? Предположим, учитель сформулировал конкретные задачи урока, реализуемые с помощью Интернет-ресурсов. Какие здесь могут быть варианты обеспечения безопасности:

- закрытые среды обучения, например, учебные блоги, где могут оставлять свои комментарии только те, кто получил соответствующий доступ от учителя, ведущего блог;
- постановка конкретной учебной задачи: что хочу найти? где? как использую?
- формирование навыков критического мышления;
- список проверенных учителем ресурсов, с которых предлагается использовать информацию;
- все те же фильтры и контроль системного администратора, если таковой в школе

имеется.

Самое главное - приучать детей не «проводить время» в Интернете, а активно пользоваться полезными возможностями сети.

1. Вступительное слово учителя.

Как вы думаете, ребята, для чего школьникам нужен Интернет?

Варианты ответов:

1. как площадка для общения (школьные сайты, блоги, форумы; сайты\блоги\форумы по интересам; электронная почта\ аська);
2. источник информации (использовать Интернет кроме\вместо учебника, графика, справочная информация, литература);
3. дистанционное обучение (дистанционные курсы, мастер-классы, консультирование болеющих детей и детей на домашнем обучении);
4. участие в сетевых конкурсах, олимпиадах, проектах.

Послушаем стихотворение о том, как правильно и безопасно пользоваться Интернетом:

Несколько правил Интернет-безопасности

1- й чтец:

Интернет бывает разным:

Другом верным иль опасным.

И зависит это все От тебя лишь одного.

Если будешь соблюдать Правила ты разные- Значит для тебя общение В нем будет безопасное!

Будь послушен и внимательно Прочти, запомни основательно Правил свод, что здесь изложен,

Для детишек он не сложен!

2- й чтец:

Если ты не в первый раз Компьютер сам включаешь И легко без лишних фраз Сайты, чаты посещаешь,

Себя в нем мастером считаешь.

Вдруг однажды сам решил

В тайне от родителей

Потихоньку завести

Для общения в сети электронный адрес.

3- й чтец:

Указал без разрешения

Адрес, улицу и дом, и квартиру в нем.

Разместил на сайте ты фотографии семьи.

Не забыл секреты старших - все в анкете указал,

Все, что вспомнил, все, что знал!

Переписываться стал, подписался на рассылку,

Фильмы разные качал.

В общем, пока взрослых нет, заходил ты в Интернет.

4- й чтец:

И теперь сидишь довольный: стал мгновенно знаменит!

О тебе все знают в школе! Что там в школе и в районе,

Во всем мире знаменит! От друзей секретов нету - Это всем давно известно.

Все тебе охотно пишут

И секреты узнают. Целый мир про вас всё знает И при встрече сообщает:

«Знаем, знаем, мы читали, фотографии видали.

Прочитали, что твой папа на работу опоздал,

А у мамы из кастрюли суп на плитку убежал.

И про школьные проблемы всё читали и всё знаем!»

5- й чтец:

А по почте счёт пришёл вам за работу Интернета.

Там стоят такие цифры! Что у мамы почему-то Враз глаза большими стали и обратно не встают.

Потихоньку плачет мама, и сердитый ходит папа.

Ведь они не знают правду, почему их узнают?

Почему по счету нужно им вложить такие деньги?!

6- й чтец:

Все при встрече, сразу быстро им твердят одно и то же:

- Знаем, знаем, прочитали, фотографии видали!...

И воришка, к сожаленью, всё найдёт без промедленья,

Где и что у вас лежит.

А теперь запомни, Друг мой!

Правила не сложные: В Интернете, как и в жизни,

Должен ты всё понимать:

Информацию и фото с мамой вместе размещать.

На рассылку подписаться или мультики скачать,

Должен с нею всё решать!

Хочешь с мамой или с папой - это сам ты выбирай.

В Интернете, как и в жизни, Безопасность соблюдай!

- О каких несложных, но очень важных и нужных правилах пользования Интернетом говорится в этом стихотворении?

- Какие еще советы и предложения вы могли бы сами дать своим сверстникам, чтобы их нахождение в сети Интернет было полезным и безопасным?

Ну, и в заключение беседы можно использовать так называемое Джентельменское соглашение родителей (учителей) и детей Перед первым выходом в Интернет как можно четче оговорите правила пользования сетью. Обсудите с ребенком, куда ему можно заходить (возможно на первых порах стоит составить список сайтов), что можно и что нельзя делать, сколько времени можно находиться в Интернете.

Сообщите ему о том контроле, который Вы намерены осуществлять: проверка посещенных ребенком страниц, контроль времени, проведенного в Сети, проверка адресов электронной почты. Объясните ребенку, что Вы доверяете ему и заботитесь о его безопасности.

Договоритесь с ребенком о соблюдении им следующих правил:

1. Сообщить родителям свое регистрационное имя и пароль, если ребенку разрешено участвовать в чатах или блогах, e-mail адрес и пароль почтового ящика.
2. Никому, кроме родителей, эти сведения сообщать категорически нельзя.
3. Не сообщать без разрешения родителей для каждого отдельного случая личную информацию (домашний адрес, номер телефона, номер школы, место работы родителей).
4. Не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет.
5. Сразу обратиться к родителям, если ребенок увидит нечто неприятное, тревожащее, угрожающее на сайте или в электронной почте.
6. Не соглашаться лично встретиться с человеком, с которым ребенок познакомился в Сети.
7. Если кто-то предлагает ребенку какой-то "секрет" - тут же сообщить об этом родителям.
8. Не скачивать, не устанавливать, не копировать ничего с дисков или из Интернета без разрешения родителей на каждый отдельный случай.
9. Не делать без разрешения родителей в Интернете ничего, что требует оплаты.
10. Проявлять уважение к собеседникам в Интернете, вести себя так, чтобы не обидеть и не рассердить человека.

В течение некоторого времени сопровождайте ребенка в его путешествиях по сети для того, чтобы убедиться, что ребенок соблюдает ваш уговор.

Методическая разработка классного часа на тему:
«БезОпасный Интернет» (5 - 7 класс)

Цель: Познакомить учащихся с опасностями, которые подстерегают их в Интернете и помочь избежать этих опасностей.

Подготовительная работа: классный руководитель проводит опрос учащихся по вопросам:

1) У вас на домашнем компьютере установлен Интернет?
2) Что вам больше всего нравится в Интернете?
3) Как ваши родители воспринимают ваши занятия в Интернете? Почему?

Оборудование: компьютер, проектор, презентация, памятка учащимся.

Ход занятия

Учитель: Раньше подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. И начать наш классный час я хочу с обработанных данных проводимого опроса. Давайте обратим внимание, что наибольший процент ответов на последний вопрос связан с безопасностью в Интернете. И ваши родители во многом правы! Очень большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности. И ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и «Как их избежать?» нам поможет этот классный час.

Вопрос 1. «Какие опасности подстерегают нас в Интернете?»

1) Преступники в Интернете.

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

2) Вредоносные программы.

К вредоносным программам относятся вирусы, черви и «троянские кони» - это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

3) Интернет-мошенничество и хищение данных с кредитной карты.

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing»,состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

4) Азартные игры.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

5) Онлайновое пиратство.

Онлайновое пиратство - это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом - например, музыки, фильмов, игр или программ - без разрешения правообладателя.

6) Интернет-дневники.

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

7) Интернет-хулиганство.

Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим.

8) Недостоверная информация.

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

9) Материалы нежелательного содержания.

К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

Учитель: А сейчас мы немного отдохнём. Музыкальная пауза.

(Во время музыкальной паузы учащиеся выполняют движения)

Частушки:

(Руки на пояс, поднимаем плечи по очереди, голову слегка влево, вправо).

Пропоем сейчас частушки,

Чтоб чуть-чуть нам отдохнуть.

Про здоровый образ жизни Не забудем намекнуть.

(На первые две строчки частушки закрывать глаза руками и открывать, на другие две - потягиваться).

На компьютере играли,

Наши глазоньки устали,

А теперь мы отдохнем И опять играть начнем.

(Руки на поясе, наклоны влево, вправо).

Нужно спортом заниматься И в жару нам, и в мороз,

Если где-то ты не сможешь,

То не хмурь уж ты свой нос.

(Хлопать в ладоши).

Мы пропели вам частушки Хорошо ли, плохо ли,

А теперь мы вас попросим,

Чтобы вы похлопали.

Учитель: Мы с вами уже рассмотрели те опасности, которые нам могут встретиться в Интернете. А теперь давайте посмотрим, как этих опасностей можно избежать.

Вопрос 2. «Как этих опасностей избежать?»

1) Преступники в Интернете.

Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

2) Вредоносные программы.

А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.

Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.

В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

3) Интернет-мошенничество и хищение данных с кредитной карты.

А)Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес вебсайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые

предоставляют многие банки в России.

4) Азартные игры.

Помните, что нельзя играть на деньги. Ведь, в основном, подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, те, которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

5) Онлайновое пиратство.

Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях - распространителях пиратских продуктов, которые преследуют только одну цель - обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

6) Интернет-дневники.

Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

7) Интернет-хулиганство.

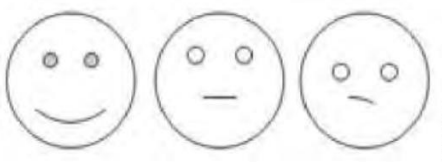
Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

8) Недостоверная информация.

Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ - газетам, журналам и книгам.

9) Материалы нежелательного содержания.

Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®). Научитесь критически относиться к содержанию онлайновых материалов и не доверять им.



Учитель: А теперь подведём итоги нашего классного часа. У вас на столе лежат три картинки. Выберите и положите перед собой ту, которая соответствует вашему настроению.

- Классный час понравился. Узнал что-то новое.
- Классный час понравился. Ничего нового не узнал.
- Классный час не понравился. Зря время потерял.

Учитель: А на память об этом классном часе я хочу подарить каждому из вас памятку по безопасному поведению в Инернете.

В Сети ты можешь встретить все, что угодно - от уроков истории и новостей до нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной.

Чтобы разобраться, какой информации в Сети можно, а какой нельзя доверять, следуй простым советам:

1. Относись к информации осторожно. То, что веб-сайт здорово сделан, еще ни о чем не говорит. Спроси себя: за что этот сайт выступает? В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел “О нас” или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.
2. Следуй правилу трех источников. Проведи свое расследование и сравни три источника информации прежде чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить, если ты будешь использовать их в своей домашней работе.
3. Как предоставлять достоверную информацию?

Будь ответственным - и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.

4. Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его - спроси разрешения.
5. Сообщая о неприемлемом контенте, ты не становишься доносчиком. Наоборот, ты помогаешь делу безопасности Сети.
6. Когда ты грубишь в Интернете, ты провоцируешь других на такое же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.
7. Все, что ты размещаешь в Интернете, навсегда останется с тобой - как татуировка. Только ты не сможешь эту информацию удалить или контролировать ее использование. Ты ведь не хочешь оправдываться за свои фотографии перед будущим работодателем?
8. Защищай себя - сейчас и в будущем. Подумай, прежде чем что-либо разместить в Интернете.

И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но — как и реальный мир - Сеть тоже может быть опасна!

Методические материалы для разработки классного часа
«Что нужно знать старшекласснику об Интернете?»

Юридические аспекты и общие свойства:

- У Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность.
- Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления.
- Интернет стал достоянием всего человечества.
- У Интернета имеется много полезных и вредных свойств, эксплуатируемых заинтересованными лицами.
- Интернет, прежде всего, средство открытого хранения и распространения информации. По маршруту транспортировки незашифрованная информация может быть перехвачена и прочитана.
- Интернет может связать каждый компьютер с любым другим, подключённым к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему.
- Сайты в Интернете распространяют информацию по такому же принципу, то есть индивидуально, по инициативе читателя.
- Спам-серверы и «зомби-сети» распространяют информацию по инициативе отправителя и забивают почтовые ящики пользователей электронной почты спамом точно так же, как забивают реальные почтовые ящики распространители рекламных листовок и брошюр.
- Распространение информации в Интернете имеет такую же природу, как и слухи в социальной среде. Если к информации есть большой интерес, она распространяется широко и быстро, нет интереса — нет распространения.
- Чтение информации, полученной из Интернета или любой другой сети ЭВМ, относится, как правило, к непубличному воспроизведению произведения. За распространение информации в Интернете (разглашение), если это государственная или иная тайна, клевета,

другие запрещённые законом к распространению сведения, вполне возможна юридическая ответственность по законам того места, откуда информация введена.

Сервисы

В настоящее время в Интернет существует достаточно большое количество сервисов, обеспечивающих работу со всем спектром ресурсов. Наиболее известными среди них являются:

электронная почта (E-mail), обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами;

телеконференции, или группы новостей (Usenet), обеспечивающие возможность коллективного обмена сообщениями;

сервис FTP — система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов;

сервис Telnet, предназначенный для управления удаленными компьютерами в терминальном режиме;

World Wide Web (WWW, W3) — гипертекстовая (гипермедиа) система,

предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство;

сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов;

сервис IRC, предназначенный для поддержки текстового общения в реальном времени

(chat);

Перечисленные выше сервисы относятся к стандартным. Это означает, что принципы построения клиентского и серверного программного обеспечения, а также протоколы взаимодействия сформулированы в виде международных стандартов. Следовательно, разработчики программного обеспечения при практической реализации обязаны выдерживать общие технические требования.

Наряду со стандартными сервисами существуют и нестандартные, представляющие собой оригинальную разработку той или иной компании. В качестве примера можно привести различные системы типа Instant Messenger (своеобразные Интернет-пейджеры — ICQ, AOl, Demos on-line и т. п.), системы Интернет-телефонии, трансляции радио и видео и т. д. Важной особенностью таких систем является отсутствие международных стандартов, что может привести к возникновению технических конфликтов с другими подобными сервисами.

Для стандартных сервисов также стандартизируется и интерфейс взаимодействия с протоколами транспортного уровня. В частности, за каждым программным сервером резервируются стандартные номера TCP- и UDP-портов, которые остаются неизменными независимо от особенностей той или иной фирменной реализации как компонентов сервиса, так и транспортных протоколов. Номера портов клиентского программного обеспечения так жестко не регламентируются. Это объясняется следующими факторами:

во-первых, на пользовательском узле может функционировать несколько копий клиентской программы, и каждая из них должна однозначно идентифицироваться транспортным протоколом, то есть за каждой копией должен быть закреплен свой уникальный номер порта;

во-вторых, клиенту важна регламентация портов сервера, чтобы знать, куда направлять запрос, а сервер сможет ответить клиенту, узнав адрес из поступившего запроса.

Услуги

Сейчас наиболее популярные услуги Интернета — это:

Всемирная паутина

Веб-форумы

Блоги

Вики-проекты

Интернет-магазин ы Интернет-аукцион ы Социальные сети

Электронная почта и списки рассылки Группы новостей (в основном, Usenet)

Файлообменные сети

Электронные платёжные системы

Интернет-радио

Интернет-телевидение

IP-телефония

Мессенджеры

FTP-серверы

IRC (реализовано также как веб-чаты)

Поисковые системы Интернет-реклама Удалённые терминалы Удалённое управление Многопользовательские игры Web 2.0

Интернет-зависимость

С возрастанием популярности Интернета проявились и негативные аспекты его применения. В частности, некоторые люди настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Психологическую в своей основе интернет-зависимость сравнивают с наркоманией — физиологической зависимостью от наркотических веществ, где также присутствует психический компонент. Интернет-зависимость определяется как навязчивое желание подключиться к

Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в стране таковых 4—6 %.

Интернет-зависимость — психическое расстройство, навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. Интернет-зависимость является широко обсуждаемым вопросом, но её статус пока находится на неофициальном уровне: расстройство не включено в официальную классификацию заболеваний DSM-IV.

Происхождение проблемы

Информация для человека имеет огромное значение. Компьютер и Интернет являются мощным инструментом обработки и обмена информацией, кроме того, благодаря компьютеру стали доступными различные виды информации. Это и считается первопричиной компьютерной или интернет зависимости, так как в определённом смысле, они страдают нарушением процессов обмена информацией.

Проблема интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми.

Интернет-зависимость и официальная медицина

Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

Зависимость (наркотическая) в медицинском смысле определяется как навязчивая потребность в использовании привычного вещества, сопровождающаяся ростом толерантности и выраженными физиологическими и психологическими симптомами. Рост толерантности означает привыкание ко всё большим и большим дозам [1]. Также зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определённой деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр, обжорства или гиперрелигиозности. Очевидно, его можно употреблять и при рассмотрении интернет-зависимости. Здесь характер зависимости иной, чем при употреблении наркотиков или алкоголя, то есть физиологический компонент полностью отсутствует. А вот психологический проявляется очень ярко. Таким образом, можно определить интернетзависимость как нехимическую зависимость — навязчивую потребность в использовании Интернета, сопровождающуюся социальной дезадаптацией и выраженными психологическими симптомами.

Интернет-зависим ые

По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4—6%. Несмотря на отсутствие официального признания проблемы, интернетзависимость уже принимается в расчёт во многих странах мира. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

Классификация интернет-зависимости, её причин и симптомов

Основные 5 типов интернет-зависимости таковы:

1. Навязчивый веб-серфинг — бесконечные путешествия по Всемирной паутине, поиск информации.
2. Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы

переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.

3. Игровая зависимость — навязчивое увлечение компьютерными играми по сети.

4. Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернетаукционах.

5. Киберсексуальная зависимость — навязчивое влечение к посещению порносайтов и занятию киберсексом.

Интернет-зависимость и проблемы в семье

Проблемы в семье, как правило, возникают в результате недостатка внимания к тому или иному члену семьи. Ссоры и непонимание проблем зависимого человека только усугубляют положение отношений в семье. Так как интернет-зависимый человек поглощает много информации и, возможно, знаний, подобные изменения вызывают внутреннюю напряжённость и обеспокоенность. Семейные скандалы могут лишь еще больше повредить психику человека. Лучший способ решить проблемы семьи — это и любовь, и взаимопонимание, и мудрость домочадцев. Плавно выводить человека на семейное позитивное общение и, главное, увеличивать совместное общение с живой природой, к примеру: с помощью прогулок.

Пути решения проблемы

Самый простой и доступный способ решения зависимости — это приобретение другой зависимости. Любовь к здоровому образу жизни, общение с живой природой, творческие прикладные увлечения, такие, как рисование, как правило, выводят человека из зависимости.

Ведущим специалистом в изучении интернет-зависимости сейчас считается Кимберли Янг — профессор психологии Питсбургского университета в Брэтфорде (США), автор известной книги «Пойманные в Сеть» (англ. «Caught in the Net»), переведённой на многие языки. Она также является основателем Центра помощи людям, страдающим интернет-зависимостью (англ. Center for On-Line Addiction). Центр, созданный в 1995 году, консультирует психиатрические клиники, образовательные заведения и корпорации, которые сталкиваются со злоупотреблением интернетом. Центр свободно распространяет информацию и методики по освобождению от интернет-зависимости.

В 2009 году писатель Станислав Миронов опубликовал в свободном доступе на одном из литературных ресурсов роман Virtuality, рассказывающий о проблеме интернетзависимости, где автор классифицирует интернет-зависимость не только как психическое расстройство, но и как острую социальную проблему, предлагая пути её решения. О печатном издании романа упоминаний не имеется.

Методическая разработка классного часа на тему:
«Этика сетевого общения» (8 - 9 класс).

Цель мероприятия:

- познакомить ребят с основными нормами поведения в сети Интернет, особенностями общения в чатах, по электронной почте.

Лучше построить классный час в форме беседы, в которой учащиеся должны привести примеры непорядочного поведения в сети Интернет: нетерпимости, навязывания своих убеждений, экстремизма.

В качестве вступительного слова ребятам можно предложить ситуации, часто встречающиеся в последнее время при пользовании сетью Интернет, и выяснить мнение ребят по той или иной проблеме (ситуации).

Например:

1. В последнее время чешские школьники, как и учащиеся в других странах, частенько шантажируют одноклассников и учителей, выкладывая нелицеприятные видеоролики о них в Интернете. Для рассылки фотографий, звуковых и видеофайлов дети также пользуются электронной почтой и мобильными телефонами.

Чтобы решить эту проблему, чиновники предлагают учителям просто конфисковывать у детей сотовые аппараты или же запрещать их использование во время уроков. Кроме того, преподавателям рекомендуется приглашать родителей в школу и обсуждать с ними поведение малолетних шантажистов; есть и более радикальная мера — перевод провинившегося в другой класс. Ну, а, если школьник упорствует, продолжая выкладывать фотографии и видео, чиновники советуют педагогам обращаться в полицию.

- Как вы оцениваете такое поведение своих сверстников в других странах?
- Какие методы воздействия на Интернет-шантажистов можете предложить?

2. Онлайновое запугивание — к сожалению, довольно распространенное сегодня явление. Согласно недавнему исследованию, в США трое из четырех подростков подвергались запугиванию в Сети в течение последнего года. И только один ребенок из десяти рассказал об онлайновых угрозах родителям или другим взрослым. Многие подростки не говорят о происшедшем родителям, поскольку намерены сами решать подобные проблемы. 31% опрошенных не обсуждают инциденты, так как боятся, что родители ограничат им доступ в Интернет. Треть респондентов заявили, что не говорили со взрослыми об онлайновых угрозах, поскольку опасались, что в результате у них могут возникнуть проблемы с родителями.

- Подвергались ли вы подобному воздействию?
- Как нужно правильно вести себя в подобной ситуации, по вашему мнению?

3. Хотя Интернет - специфическая среда для общения, в ней существуют определенные правила вежливости, которые получили название «сетевой этикет». Правила сетевого этикета широко обсуждаются в Интернете, но, к сожалению, культура общения остается на низком уровне. В сети нередко можно наблюдать грубость, речевую агрессию, нетерпимость к чужим

мнениям. В связи с этим, необходимо рассмотреть пример крайне негативного сетевого поведения, предложить дать ему нравственную оценку и указать на недопустимость такого поведения. Например, сообщение в новостях: «Группа хакеров повредила на этой неделе несколько церковных страниц, поместив на них высказывания почитателей культа Сатаны, его изображения и другие символы Сатанизма». Предложить учащимся дать им оценку.

Работая в Интернете, учащиеся обязательно должны столкнуться с проблемой виртуального общения (чат, форум, электронная почта, телеконференции). Если мы общаемся с незнакомыми людьми, то возникает ситуация разговора с виртуальными личностями. Человек может изменять свой статус, скрывать возраст, пол, преувеличивать силу, красоту, а также почти безнаказанно проявлять агрессивные черты характера, которые он вынужден подавлять в повседневной жизни. Для того чтобы избежать отрицательных последствий общения в Интернете, следует придерживаться определенных правил:

- не нужно слепо верить в то, что собеседник говорит о себе;
- следите за своими словами (не употребляйте грубых выражений);
- не сообщайте незнакомому лично человеку ваш домашний адрес, телефонный номер;
- если вы чувствуете дискомфорт в общении, уходите.

Можно предложить учащимся составить свои принципы общения в Интернете.

Рассмотрим подробнее неформальный кодекс поведения в сети Интернет, регулирующий общение пользователей друг с другом и так называемый сетевой этикет (netiquette — от слияния англ. слов net — сеть и etiquette — этикет). Сетевой этикет — это некоторое количество базовых правил поведения в сети, однако эти правила время от времени подвергаются изменениям, что-то устаревает и теряет свою актуальность в связи с развитием технологий Интернет, а что-то добавляется новое.

Сетевой этикет регулирует:

- правила обмена сообщениями по электронной почте
- стилистику сетевой коммуникации при коллективных обсуждениях
- общие правила написания публикуемых текстов в сети и пр.

При переписке по электронной почте каждый пользователь должен помнить о некоторых правилах.

- Приветствуйте собеседника в начале письма и прощайтесь в конце.
- По электронной почте можно обращаться к незнакомым людям, но при условии, что адрес был опубликован его владельцем.
- Пишите кратко, грамотно и аккуратно.
- Отвечая на сообщение, необходимо цитировать его наиболее существенные места.
- Удобно, когда письма пользователя заканчиваются краткой «подписью», автоматически добавляемой к каждому сообщению, отправляемому пользователем, однако эта подпись не

должна быть длиннее четырех-пяти строк. Очень важно указать в подписи своё имя-отчество полностью, чтобы получателю было удобно обратиться к Вам. Если указаны только инициалы, то отвечающему придётся искать имена в других источниках, на это потребуется время. Подразумевать же, что все точно помнят наше имя-отчество, - это неверно. У всех свои особенности памяти и объёмы информации, а также круг общения.

Например:

С уважением,

Иван Иванович Тел. 8(XXX) XX-XX-XXX E-mail: aaa@mail.ru

- В переписке личного характера можно придерживаться разговорного стиля.
- Не следует переправлять чье-то личное сообщение другим людям или в телеконференцию без предварительного согласия его автора.
- Если вы заняты и не можете быстро ответить на поступившее сообщение, отправьте пару строк с подтверждением получения и обещанием ответить при первой возможности.
- Если сообщение поступило от незнакомого лица, следует понять, обосновано оно или нет. В первом случае - ответить в течение трех дней. Во втором - не отвечать.
- Текст письма нужно структурировать по смыслу, абзацы отделять пустой строкой.
- Если вы отправляете заархивированный файл, поинтересуйтесь заранее, сможет ли получатель письма его распаковать (то есть, имеет ли он на своем компьютере нужную программу-архиватор).
- Строка текста должна ограничиваться 60-70 символами, справа без выравнивания.
- Нежелательно посылать письма большого объема - около одного мегабайта, поскольку пользователь, работающий с бесплатным почтовым ящиком, может такое послание не прочитать из-за ограничений на объем входящей корреспонденции.
- К незнакомым людям можно обращаться с просьбами о консультации, с вежливыми предложениями и пожеланиями, не претендуя на получение ответа.
- Неполучение ответа следует рассматривать как нежелательность или невозможность установления контакта и повторять не следует.
- При обращении к незнакомым людям следует воздерживаться от просьб, вызывающих необходимость использования других средств связи, отличных от электронной почты.
- Если в письмо вложен файл, то в тексте письма обязательно должно был указано, что приложено и зачем.

И наконец, существуют общие Правила общения в Сети :

1. Помните, что Вы говорите с человеком.
2. Придерживайтесь тех же стандартов поведения, что и в реальной жизни.
3. Помните, где Вы находитесь в киберпространстве.
4. Уважайте время и возможности других.
5. Сохраняйте лицо.
6. Помогайте другим там, где Вы это можете делать.
7. Не ввязывайтесь в конфликты и не допускайте их.
8. Уважайте право на частную переписку.
9. Не злоупотребляйте своими возможностями.
10. Учитесь прощать другим их ошибки.

Приложение 3.

ПАМЯТКА РОДИТЕЛЯМ
ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ В ИНТЕРНЕТЕ

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, им следует уяснить некоторые моменты.

Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций. В заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете.

Если вы не уверены, с чего начать, вот несколько мыслей о том, как сделать посещение Интернета для детей полностью безопасным.

- Установите правила работы в Интернете для детей и будьте непреклонны.
- Научите детей предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:
- Представляясь, следует использовать только имя или псевдоним.
- Никогда нельзя сообщать номер телефона или адрес проживания или учебы.
- Никогда не посылать свои фотографии.
- Никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.
- Объясните детям, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.
- Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом вам.

Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

Настаивайте, чтобы дети уважали собственность других в Интернете.

Объясните, что незаконное копирование чужой работы - музыки, компьютерных игр и других программ - является кражей.

Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

Скажите детям, что не все, что они читают или видят в Интернете, - правда. Приучите их спрашивать вас, если они не уверены.

Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

Поощряйте детей делиться с вами их опытом в Интернете.

Посещайте Сеть вместе с детьми. Регулярно посещайте Интернет-дневник своего ребенка, если он его ведет, для проверки.

Будьте внимательны к вашим детям!

Приложение 4.

ПАМЯТКА ДЛЯ ДЕТЕЙ
ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, ребенок должен предпринимать следующие меры предосторожности при работе в Интернете:

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
- Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.

Приложение 5.

Классификатор информации, не имеющей отношения к образовательному процессу

1. Классификацию информации, запрещенной законодательством Российской Федерации к распространению и не имеющей отношения к образовательному процессу, осуществляют специальные экспертно-консультативные органы (советы) при органах управления образованием.

2. Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации. Классификатор информации, не имеющей отношения к образовательному процессу, может содержать как части (разделы), рекомендуемые к применению в единообразном виде на всей территории Российской Федерации, так и части (разделы), рекомендуемые к использованию экспертно-консультативными органами (советами) регионального и (или) муниципального уровня.

3. В соответствии с законодательством Российской Федерации образовательное учреждение свободно в выборе и применении классификаторов информации, не имеющей отношения к образовательному процессу, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.

4. Рекомендации по формированию Классификатора информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, разработаны в соответствии с проведенным анализом законодательства Российской Федерации и международных договоров Российской Федерации.

№	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

Приводимый далее перечень категорий Классификатора информации, не имеющей отношения к образовательному процессу, носит рекомендательный характер и может быть дополнен, расширен или иным образом изменен в установленном порядке, в том числе с учетом специфики образовательного учреждения, социокультурных особенностей автономного округа и иных обстоятельств.

№	Тематическая категория	Содержание
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям

4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация: • фотоальбомы и фотоконкурсы; • рейтинги открыток, гороскопов, сонников; • гадания, магия и астрология; • ТВ-программы; • прогнозы погоды; • тесты, конкурсы онлайн; • туризм, путешествия; • тосты, поздравления; • кроссворды, сканворды, ответы к ним; • фантастика; • кулинария, рецепты, диеты; • мода, одежда, обувь, модные аксессуары, показы мод; • тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; • о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними; • о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; • о службах знакомств, размещении объявлений онлайн; • анекдоты, «приколы», слухи; • о сайтах и журналах для женщин и для мужчин; • желтая пресса, онлайн-ТВ, онлайн-радио; • о знаменитостях; • о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайновые и оффлайновые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
7	Корпоративные сайты, интернет - представительства	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты

	негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	коммерческих фирм, компаний, предприятий, организаций
8	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги
9	Отправка SMS с использованием интернет - ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты
11	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и пр.
12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
15	Онлайн - казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц
17	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет - представительства кадровых агентств, банки вакансий и резюме
18	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет - каталоги, системы поиска и навигации в Интернете
19	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
20	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
21	СМИ (ресурсы данной категории, не	СМИ, содержащие новостные ресурсы и сайты

	имеющие отношения к образовательному процессу)	СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
23	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет - магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
24	Убийства, насилие	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
25	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу сайты для анонимного общения в режиме онлайн.

Приложение 6.

Инструкция по организации антивирусной защиты в МБОУ Сеченовская средняя школа

1. Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в МБОУ Сеченовской средней школе (далее - ОУ) и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей ОУ к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Директором школы назначается лицо, ответственное за организацию антивирусной защиты в ОУ.

1.3. В ОУ может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты в ОУ.

1.5. 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, flash-накопителях и т.п.).

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

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

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

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

2. Мероприятия, направленные 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).

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) ОУ.

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 ОУ 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

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов 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:

3.3.1. непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах ОУ;

3.3.2. 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.);

3.3.3. при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса

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

4.1.1. приостановить работу;

4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ОУ;

4.1.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4.1.4. 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 ОУ.

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

5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется директором ОУ и фиксируется Актом проверки.

Приложение 7.

Инструкция для педагогических работников о порядке действий при осуществлении контроля за использованием учащимися МБОУ Сеченовская средняя школа сети Интернет

Настоящая инструкция устанавливает порядок действий сотрудников образовательного учреждения при обнаружении:

1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;

2) отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

Контроль использования обучающимися сети Интернет осуществляют:

1) во время занятия — проводящий его преподаватель;

2) во время использования сети Интернет для свободной работы обучающихся — дежурный преподаватель.

Преподаватель:

— определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе 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 образовательному процессу.

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.

В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

Перечень локальных актов и документов

1. Регламент работы в сети Интернет в МБОУ «Украинская СОШ»;;
2. Положение об использовании сети Интернет в МБОУ «Украинская СОШ»;;
3. Положение об информационной открытости МБОУ «Украинская СОШ»;;
4. Положение о сайте МБОУ «Украинская СОШ»;;
5. Положение об электронном журнале успеваемости/электронном дневнике учащегося в МБОУ «Украинская СОШ»;
6. Регламент работы с электронной почтой в МБОУ «Украинская СОШ»;.