Методические рекомендации для организаторов Всероссийской акции, посвященной безопасности школьников в сети Интернет субъектов Российской Федерации по проведению акции в 2016 году

Содержание

Общие положения. Введение

Важность реализации мероприятий, направленных на обеспечение интернет-безопасности детей обозначена Национальной Стратегией действий в интересах детей на 2012-2017 гг. Так, в «мерах, направленных на обеспечение информационной безопасности детства» важный акцент ставится на «создании и внедрении программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости…».

В связи с глобальным процессом активного формирования и использования информационных ресурсов особое значение приобретает информационная безопасность детей. Доступ учащихся к информационным ресурсам сети Интернет дает возможность школьникам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельно обучаться, а также узнавать о проводимых конкурсах, олимпиадах и принимать участие в них. Использование Интернета в образовательной деятельности таит в себе много опасностей. Для преодоления негативного воздействия Интернета на детей необходимо их ознакомить с потенциальными опасностями в сети Интернет.

Для полноценного развития ребенка, способного успешно жить и саморазвиваться в современном мире, не нужно (и даже опасно) создавать идеальную информационную среду, важнее и продуктивнее заниматься развитием информационной безопасности личности школьника, обучать ребенка адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей.

Анализ современного состояния исследований по данному вопросу позволил выделить основные задачи в области информационной безопасности и защите информации. Значительное количество исследований посвящено защите информации при ее генерации, передачи, обработке и использовании,

а вот защите сознания и психики личности от негативного воздействия информации уделяется в этих исследованиях существенно меньше внимания. Данная проблема имеет междисциплинарный характер и для ее решения в дальнейшем будут необходимы исследования в различных отраслях научных знаний.

Бокова Людмила Николаевна**,** член Совета Федерации ФС РФ, Председатель Временной комиссии Совета Федерации по развитию информационного общества: «Интернет сегодня - не просто технологии, это безграничные возможности развития и личностного роста, это формирование новых навыков совершенствования и познания. Но как и любая высокотехнологичная система, Интернет требует хорошего уровня знаний и квалификации, иначе из друга и сподвижника он может превратиться во врага и источник повышенной опасности…».

П.А. Астахов, уполномоченный при Президенте Российской Федерации по правам ребенка: «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».

Всероссийская акция по безопасности школьников в сети Интернет пройдет по всей стране с 5 по 15 сентября 2016 года. Данные методические рекомендации адресованы организаторам акции в субъектах Российской Федерации.

Глоссарий

Интерне́т (англ. Internet) — всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. Построена на базе стека протоколов TCP/IP.

Информация - результат и отражение в человеческом сознании, многообразие внутреннего и окружающего миров (сведения об окружающих человека предметах, явлений, действия других людей).

Информационная безопасность может рассматриваться в следующих значениях:

1. Состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства, организации и т. п.);

2. Деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.

Информационная безопасность (англ. informationsecurity) — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) (англ. information security) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим

каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) (англ. IT security) — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Тематический урок — форма организации обучения с целью овладения учащимися изучаемым материалом по конкретной теме (знаниями, умениями, навыками, мировоззренческими и нравственно-эстетическими идеями).

Акция — действие, предпринимаемое для достижения какой-нибудь цели.

Выставка (по определению «Международного бюро выставок») — это показ, каково бы ни было его наименование, путём представления средств, имеющихся в распоряжении человечества для удовлетворения потребностей, а также в целях прогресса в одной или нескольких областях его деятельности.

Круглый стол — общество, конференция или собрание в рамках более крупного мероприятия (съезда, симпозиума, конференции). Используется в двух смыслах — как свободная конференция разнородных участников для непосредственного обсуждения определённых проблем (в частности, конфликтов) и — реже — как закрытое общество избранных, принимающее в кулуарах важные решения.

- цель обсуждения — обобщить идеи и мнения относительно обсуждаемой проблемы;
- все участники круглого стола выступают в роли пропонентов (должны выражать мнение по поводу обсуждаемого вопроса, а не по поводу мнений других участников); отсутствие набора нескольких ролей характерно не для всех круглых столов;

- все участники обсуждения равноправны; никто не имеет права диктовать свою волю и решения.

Презентация — (от лат. praesento — представление) — документ или комплект документов, предназначенный для представления чего-либо. Цель презентации — донести до аудитории полноценную информацию об объекте презентации в удобной форме.

Практическое занятие — одна из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения навыков и опыта творческой деятельности, овладения современными методами практической работы с применением технических средств.

Открытый урок — занятие или лекция, на которых присутствуют другие преподаватели или приглашенные лица. Проводятся квалифицированными преподавателями по трудным или слабо разработанным в методике разделам учебной программы, а также с целью показа и распространения наиболее эффективных приемов учебно-воспитательной работы. Такие уроки (лекции) способствуют внедрению достижений педагогической науки в практику, распространению педагогического опыта, повышению квалификации преподавателей.

Документы по проведению Всероссийской акции, посвященной безопасности школьников в сети Интернет

ПОЛОЖЕНИЕ

о проведении Всероссийской акции,

посвящённой безопасности школьников в сети Интернет

1. Общие положения

Важность реализации мероприятий, направленных на обеспечение интернет-безопасности детей обозначена Концепцией информационной безопасности детей, утверждённой распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р, и Национальной Стратегией действий в интересах детей на 2012-2017 гг. Так, в «мерах, направленных на обеспечение информационной безопасности детства» важный акцент ставится на «создании и внедрении программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики Интернет-зависимости…».

2. Учредители и организаторы Всероссийской акции

Учредителем Всероссийской акции, посвященной безопасности школьников в сети Интернет (далее по тексту - Всероссийская акция), является Министерство образования и науки Российской Федерации. Организатором акции 2016 года является компания «КреоГраф». Партнерами акции могут быть различные общественные организации, СМИ, другие заинтересованные структуры.

Всероссийская акция реализуется при поддержке Временной Комиссии Совета Федерации Федерального Собрания Российской Федерации по развитию информационного общества.

3. Цели и задачи Всероссийской акции

3.1 Цели:

развитие методов обучения обучающихся безопасному поведению в сети Интернет с использованием современных игровых и интерактивных технологий;

формирование устойчивых жизненных навыков обучающихся при работе в сети Интернет.

3.2. Задачи:

расширение знаний о киберугрозах среди обучающихся и формирование навыков распознания и оценки таких рисков;

выработка методических рекомендаций по организации работы в образовательных организациях по направлению «Интернет-безопасность для детей»;

знакомство с преимуществами знаний об Интернете и умений их применять;

изучение нормативных правовых документов по вопросам защиты обучающихся от информации, причиняющей вред их здоровью и развитию.

транслирование и популяризация лучших методик по развитию интернет-безопасности.

4. Условия и сроки проведения Всероссийской акции

4.1. Всероссийская акция проводится с 5 по 15 сентября 2016 года. Информация о проведении Всероссийской акции размещается на официальном сайте Организатора: www. деткивсетке.рф

4.2. Для участия в акции необходимо направить заявку по установленной форме (Приложение 1) и получить подтверждение от организаторов. Заявки принимаются с 20 июня по 15 августа 2016 года по адресам электронной почты: internetkonkurs@inbox.ru; konkurs@деткивсетке.рф; телефон для консультаций при подаче заявок:+7915-485-23-71

5. Участники и организаторы Всероссийской акции в субъектах Российской Федерации

5.1. Организаторами Всероссийской акции в субъектах Российской Федерации могут являться представители органов образования, а также других заинтересованных структур, работающих по тематике акции. Для получения статуса «Организатор Всероссийской акции в субъекте Российской Федерации» необходимо заполнить заявку организатора Всероссийской акции (Приложение 2) до 1 августа 2016 года и предоставить информацию об участниках акции (Приложение 3) до 5 сентября 2016 года в адрес организаторов.

5.2. Участниками Всероссийской акции могут быть общеобразовательные организации из всех субъектов Российской Федерации; обучающиеся общеобразовательных организаций.

5.3. Для оперативного получения информации, консультаций, размещения материалов всем участникам акции рекомендуется зарегистрироваться в специализированной группе в социальных сетях.

6. Механизмы, способы и методы проведения Всероссийской акции

6.1. В рамках Всероссийской акции в сроки ее проведения могут быть проведены следующие мероприятия: урок, лекция, викторина, семинар, деловая игр и т.п. по безопасности школьников в сети Интернет. Примеры рекомендуемых форм мероприятий приведены в Приложении 4 настоящего Положения.

6.2. Мероприятия могут проходить как в очной, так и в заочной форме (online-трансляции, видеоуроки и т.д.). При заочной форме проведения необходимо прислать ссылку на мероприятие в сети Интернет организаторам акции.

6.3. Длительность мероприятия должна составлять не менее 40 минут.

6.4. Организаторы акции в субъектах Российской Федерации могут создавать специализированные информационные ресурсы или использовать имеющиеся для освещения мероприятий Всероссийской акции.

6.5. Для оценки материалов участников акции создается Экспертный совет из числа представителей Министерства образования и науки Российской Федерации, представителей организаторов, СМИ и общественных объединений.

6.6. Для осуществления эффективной работы организаторам и участникам акции предоставляются методические материалы по ее проведению не позднее, чем за 10 дней до начала проведения.

6.7. Для освещения мероприятий Всероссийской акции проводится информационная кампания в федеральных, региональных СМИ и сети Интернет. С планируемым перечнем федеральных СМИ и этапами информационной кампании можно ознакомиться в Приложении 5.

7. Подведение итогов Всероссийской акции

7.1. Все Организаторы акции в субъектах Российской Федерации, приславшие официальные заявки и получившие статус Организатора, получают именные дипломы Министерства образования и науки Российской Федерации.

7.2.Общеобразовательные организации по итогам проведения открытых уроков по безопасности школьников в сети Интернет получают дипломы участников.

7.3. Дипломы победителей и памятные подарки получают 15 победителей Всероссийской акции, выбранные Экспертным Советом.

7.4. По итогам проведения Всероссийской акции за активное участие (наибольшее количество участников) субъекта Российской Федерации органу исполнительной власти, осуществляющему государственное управление в сфере образования, Организатору акции в субъекте Российской Федерации, а также всем участникам Всероссийской акции субъекта Российской

Федерации, вручаются дипломы Министерства образования и науки Российской Федерации и Совета Федерации Федерального Собрания Российской Федерации.

8. Ожидаемые результаты

8.1.В рамках Всероссийской акции будет проведено не менее 550 мероприятий не менее, чем в 40 субъектах Российской Федерации.

8.2. Выявлены лучшие методики и технологии проведения мероприятий по развитию интернет-безопасности школьников в сети Интернет.

8.3. Определены перспективы реализации подобных акций в 2017 году.

9. Контактная информация Организаторов Всероссийской акции

Министерство образования и науки Российской Федерации, г. Москва, Люсиновская ул., дом 51, конт. тел.(495)237-91-83

Общество с ограниченной ответственностью «КреоГраф», г. Калуга, ул. Плеханова, 30-26, координатор Всероссийской акции Бородина Марина*:+7 915 485-23-71*

Приложение 1

к Положению

Анкета участника

Всероссийской акции, посвящённой безопасности школьников

в сети Интернет

Субъект РФ	
Контактное лицо (ФИО, должность)	
Контактный телефон	
e-mail	
Наименование образовательной организации	
Полный адрес местонахождения	
Форма мероприятия[1]	
Количество участников (школьников) мероприятия Всероссийской акции - класс обучения	
Информационный ресурс, на котором размещается информация о мероприятии	

Дата заполнения

Подпись заявителя[2]

[1]С приложением сценария по каждому приводимому мероприятию, но не более 3 сценариев

[2] Подразумевает автоматическое согласие на обработку персональных данных в соответствии с ФЗ 152

Приложение 2

к Положению

Заявка Организатора в субъекте Российской Федерации
Всероссийской акции, посвящённой безопасности школьников
в сети Интернет

Субъект РФ	
Фамилия, имя, отчество	
Место работы, должность	
Контактный телефон	
e-mail	

Дата заполнения

Подпись заявителя[3]

Приложение 3

к Положению

Информация об участниках акции

Субъект Российской Федерации: _____			
Перечень форм мероприятий[4]	Общеобразовательная организация	Количество участников - класс обучения	Указание информационного ресурса

[3] Подразумевает автоматическое согласие на обработку персональных данных в соответствии с ФЗ 152

[4] Приложить 3 лучших сценария мероприятий, проведенных в субъекте Российской Федерации

Организационно-подготовительный этап

(выбор предлагаемых тем, поиск соответствующего образовательного материала)

Организаторами Всероссийской акции в субъектах Российской Федерации являются представители органов образования или другие заинтересованные структуры, работающие по тематике акции, подавшие заявку до 01.08.2016 года и получившие подтверждение от организаторов.

Участниками Всероссийской акции являются общеобразовательные организации из всех субъектов Российской Федерации; обучающиеся общеобразовательных организаций, подавшие заявку до 15.08.2016 года и получившие подтверждение от организаторов.

Для оперативного получения информации, консультаций, размещения материалов всем участникам акции рекомендуется зарегистрироваться в специализированной группе «Детки в сетке» в социальных сетях: https://vk.com/public126003528 или https://www.facebook.com/groups/1834636730089363/.

Информация об участвующих во Всероссийской акции 2016 года организаторах в субъектах РФ и участниках размещена на сайте: деткивсетке.рф.

Примерные темы для проведения мероприятий в рамках акции:

1. Для чего нужен Интернет? Возможности сети.
2. Интернет – друг или враг?
3. Какие существуют риски при пользовании интернетом, и как их можно снизить?
4. Какие виды мошенничества существуют в сети Интернет? Как защититься от мошенничества в сети Интернет?
5. Что такое безопасный чат? Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

6. Социальные сети: преимущества и опасности.

7. Формирование навыков поведения в информационном обществе с целью обеспечения личной и информационной безопасности.

8. Профессии, связанные с обеспечением Интернет-безопасности.

Источники поиска образовательного материала:

1. Методические материалы акции: методические рекомендации организаторам акции, информационное письмо участникам акции, документы акции.
2. Формирование поисковых запросов в сети Интернет.
3. Специальная литература по теме.
4. Методические рекомендации федеральных, региональных учреждений образования по тематике акции.
5. Авторские разработки по теме.

Проведение образовательных мероприятий в общеобразовательных организациях. Возможные формы предполагаемых мероприятий

Среди многообразия возможных форм проводимых мероприятий и уроков необходимо выбрать оптимальную, которая бы отвечала следующим принципам:

1. Соответствие выбранной формы теме проведения мероприятия.
2. Ресурсные возможности учителя и класса.
3. Интеллектуальные и психологические потребности классного коллектива.
4. Эффективная достижимость результатов при выборе данной формы.

Некоторые примеры форм мероприятий:

1. Мероприятия в форме соревнований и игр: конкурс, турнир, эстафета, дуэль, КВН, деловая игра, ролевая игра, кроссворд, викторина и т.д.

2. Уроки, основанные на формах, жанрах и методах работы, известных в общественной практике: исследование, изобретательство, анализ первоисточников, комментарий, мозговая атака, интервью, репортаж, рецензия и т.д.

3. Уроки, основанные на нетрадиционной организации учебного материала: урок мудрости, откровение, урок-блок, урок-"дублер начинает действовать" и т.д.

4. Уроки, напоминающие публичные формы общения: пресс-конференция, брифинг, аукцион, бенефис, регламентированная дискуссия, панорама, телемост, репортаж, диалог, "живая газета", устный журнал и т.д.

5. Уроки, основанные на имитации деятельности учреждений и организаций: следствие, патентное бюро, ученый совет и т.д.

6. Уроки, основанные на имитации деятельности при проведении общественно - культурных мероприятий: заочная экскурсия, экскурсия в прошлое, путешествие, прогулки и т.д.

7. Уроки, опирающиеся на фантазию: урок-сказка, урок-сюрприз т.д.

8. Использование на уроке традиционных форм внеклассной работы: "следствие ведут знатоки", спектакль.

9. Интегрированные уроки.

10. Трансформация традиционных способов организации урока: лекция-парадокс, парный опрос, экспресс-опрос, урок-защита оценки, урок-консультация, урок-практикум, урок-семинар и т.д.

11. Формы однотипных уроков:

- Уроки творчества: урок изобретательства, урок-выставка, урок-сочинение, урок - творческий отчет и т.д.
- Уроки, созвучные с общественными тенденциями: урок - общественный смотр знаний, урок-диспут, урок-диалог и т.д.
- Межпредметный и внутрикурсовой уроки: одновременно по двум предметам, одновременно для учащихся разных возрастов и т.д.
- Уроки с элементами историзма: урок об ученых, урок-бенефис, урок-исторический обзор, урок-портрет и т.д.
- Театрализованные уроки: урок-спектакль, урок воспоминаний, урок-суд, урок-аукцион и т.д.
- Игровые уроки: урок - деловая игра, урок - ролевая игра, урок с дидактической игрой, урок-соревнование, урок-путешествие и т. д.
- Вспомогательные уроки: урок-тест, урок для родителей, урок консультация и т.д.

12. Специализированные мероприятия:

-акции

-выставки

-квесты

-ярмарки

- парады

-игры по станциям и игры – «ассорти» (с заданиями без подготовки)

-брейн-ринги

-конкурсы видеороликов

- диспуты идр.

Использование информационных ресурсов сети Интернет и мультимедийных изданий в подготовке и проведении мероприятий.

Возможности Интернета безграничны. Уже никто не сомневается, что здесь можно найти практически все на любую тему. Принципы поисковых запросов: корректность формулировок, конкретность, отсутствие лишних символов и другие всегда помогут получить кладезь полезной информации на заданную тему, успех зависит от настойчивости и целеустремленности пользователя.

Много интересной информации можно найти и по теме интернет-безопасности. Это не только текстовая аналитика, научные работы и методические разработки, но и мультимедийные возможности: видеоуроки, видеоролики, видеообращения, материалы СМИ, online-трансляции, видеоконференции и другое. Все эти приемы хороши для использования при проведении тематических уроков и внеклассных мероприятий, они не только существенно украсят, но и сделают более доступным и ярким материал по любой теме.

Рекомендуемые формы проведения мероприятий

I. Анкетирование обучающихся

Для изучения проблемы безопасности в сети Интернет и отношения к ней школьников разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде. Анкетирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде.

II. Проведение урока «Интернет-безопасность для детей»

Цель: обеспечение информационной безопасности школьников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

ознакомить учащихся:

- с правилами ответственного и безопасного поведения в современной информационной среде;
- с вредоносными программами;
- со способами защиты от противоправных посягательств в сети Интернет;
- как сделать более безопасным свое общение в сети Интернет;
- как общаться в социальных сетях (сетевой этикет), избегать выкладывать в сеть компрометирующую информацию и т.д.

Темы бесед с 1 по 11 классы могут быть следующие:

- Интернет среди нас;
- Я и мои виртуальные друзья;
- Интернет в моей семье;
- Мой Интернет;
- Интернет и природа;
- Мой социум в Интернете;
- Интернет и моя будущая профессия;
- Интернет в современной школе;
- Интернет и мое здоровье и т.д.

Задачи:

1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование обучающихся о способах незаконного распространения такой информации в информационно-

телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет-безопасности обучающиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;

критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

анализировать степень достоверности информации и подлинность ее источников;

применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

III. Общешкольное родительское собрание «Интернет-безопасность для детей»

Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети. Привлечение родителей позволяет достичь высоких результатов в воспитании. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения. Формы работы с родителями могут быть разнообразны: выступления на родительских собраниях, информация на сайте школ.

План собрания:

1. Анкетирование родителей, которое позволит выявить отношение родительской общественности к внедрению в образовательный процесс ИКТ.
2. Беседа по проблеме доступа ребенка к сети Интернет.

Примерный список вопросов, которые планируется обсудить на родительском собрании:

– В каком возрасте следует разрешить детям посещение интернета?

- Следует ли разрешать детям иметь собственные учетные записи электронной почты?
- Какими внутрисемейными правилами следует руководствоваться при использовании интернета?
- Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?
- Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, MailAgent)?
- Могут ли дети стать интернет-зависимыми?
- Что должны знать дети о компьютерных вирусах?
- Как проследить какие сайты посещают дети в интернете?
- Что следует предпринять, если моего ребенка преследуют в интернете?
- Помогает ли фильтрующее программное обеспечение?
- На какие положения политики конфиденциальности детского сайта нужно обращать внимание?
- Какие угрозы встречаются наиболее часто?
- Как научить детей отличать правду ото лжи в Интернет?

IV. Конкурс рисунков для младших школьников (2-4 классы) «Интернет среди нас».

Целью данного конкурса является формирование у младших школьников четкого представления о правилах работы с компьютером и поведения в сети Интернет.

В рамках классного часа или урока окружающего мира обучающимся 2-4 классов целесообразно предложить компьютерную игру о правилах поведения в сети Интернет «Прогулка через ИнтерНетЛес» (http://www.wildwebwoods.org/popup.php?lang=ru), где в игровой форме показано какие опасности могут встречаться при работе в сети Интернет, рассказано о сетевом взаимодействии и об этикете, а также о защите прав детей.

V. Проведение единого классного часа «Безопасный Интернет»

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

- информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;
- информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
- обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);
- профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);
- предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Вопросы для обсуждения:

1. Для чего нужен Интернет?

2. Какие существуют риски при пользовании Интернетом, и как их можно снизить?
3. Какие виды мошенничества существуют в сети Интернет?
4. Как защититься от мошенничества в сети Интернет?
5. Что такое безопасный чат?
6. Виртуальный собеседник предлагает встретиться, как следует поступить?
7. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

В ходе проведения классного часа дети должны научиться:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Рекомендации по проведению уроков и открытых уроков

СЦЕНАРНЫЙ ПЛАН

к видеоуроку

«Безопасность в сети Интернет».

Цель урока: *развить информационную компетентность учащихся, обучить правилам безопасной работы в Интернете.*

Задачи урока:

- обучающие

- ✓ *познакомить с «полезными» и «вредными» сторонами Интернета;*
- ✓ *сформировать у учащихся понятия о существующих угрозах Интернета и способах их преодоления;*
- ✓ *обобщить и закрепить с учащимися материал по теме «Безопасность в Интернете».*

-развивающие

- ✓ *развивать познавательные интересы;*
- ✓ *развивать самоконтроль;*
- ✓ *развивать умение конспектировать.*

-воспитательные

- ✓ *воспитание информационной культуры учащихся, внимательности, аккуратности, дисциплинированности, усидчивости.*

Тип урока: *урок усвоения новых знаний.*

Необходимое техническое оборудование *компьютерный класс, интерактивная доска, проектор, видеокамера, осветительное, звукозаписывающее оборудование, кран и штативы для видеокамер*

№	*Этап урока*	*Деятельность учителя*	*Видеокадр*	*Время (в мин.)*
3	***Постановка темы и целей урока***	**Формулирует тему** и **цели** урока (слайд №1). Рассказывает о **плане работы** на урок.	**Средний план преподавателя**	3
4	***Изучение нового материала. Вопросы для самопроверки***	**Акцентирует внимание** на том, что Интернет это прекрасное место для общения, обучения и отдыха (слайд №2). **Рассказывает** о существующих угрозах и подробно разбирает каждую	**Кадры** информации о компьютерах и Интернете, всемирная паутина существующие угрозы в интернете. Локализация (хроника)	25

		из них и как можно их избежать (слайды №3 - №9).		
5	***Физкультминутка***	**Показывает** упражнения (слайд №10).	**Кадры доступа к интернету**	7
6	***Закрепление-диагностика знаний, умений и навыков Тезисы и выводы***	**Напоминает** правила охраны труда при работе за компьютером (слайд № 11).	**Кадры сайтов Работа за компьютером**	10

Тема урока: «Безопасность в сети Интернет»

Разработка учителя информатики и ИКТ
высшей квалификационной категории
МАОУ «Видновская гимназия» г. Видное
Кузнецова Ольга Владимировна

Учащиеся: ученики 8-11 классов

Цели урока:

- Обеспечение информационной безопасности учащихся путем привития им навыков ответственного и безопасного поведения в современной информационно-коммуникационной среде. Обучение детей личной и информационной безопасности в Интернете; развитие самоконтроля учащихся и воспитание внимательного отношения к информационным ресурсам.
- Формирование навыков поведения в информационном обществе с целью обеспечения личной и информационной безопасности.

Задачи урока:

- Научить учащихся критически относиться к информационной продукции, распространяемой в сети Интернет;

- отличать достоверные сведения от недостоверных, вредную информацию от безопасной;
- избегать информации, способной причинить вред здоровью, нравственному и психическому развитию, чести, достоинству и репутации учащихся;
- распознавать признаки злоупотребления неопытностью и доверчивостью учащихся, попытки вовлечения их в противоправную деятельность;
- познакомить учащихся с нормами и правилами поведения в сети Интернет.

Тип урока: урок усвоения новых знаний.

Оборудование: компьютерный класс, компьютер, акустические колонки, проектор, видеокамера, штатив, свет, микрофон

План урока:

1. Организационный момент (1-2 минуты)
2. Постановка целей и задач урока, мотивация учебной деятельности учащихся (3-4 минуты)
3. Объяснение нового материала (15-20 минут)
4. Первичная проверка понимания: обсуждение по вопросам (5 минут)
5. ФИЗКУЛЬТМИНУТКА (5 минут)
6. Тест проверочный (5-7 минут)
7. Постановка домашнего задания (2-3 минуты)
8. Рефлексия (подведение итогов урока)

Ход урока:

№	Этап урока	Деятельность учителя	Деятельность ученика	Время

1.	Постановка целей и задач урока, мотивация учебной деятельности учащихся	Демонстрирует видеоролик	Смотрят видеоролик	3
2.	Объяснение нового материала	Раздает бланки «Памятка безопасного использования Интернета», демонстрирует видеоролик	Смотрят видеоролик и заполняют «Памятку» правилами безопасной работы в сети Интернет	20
3.	Первичная проверка понимания: обсуждение по вопросам	Обсуждает с учащимися ключевые вопросы изучаемой темы	Задают вопросы учителю и отвечают на его вопросы, дополняют «Памятку» информацией	5
4.	Физкультминутка	Показывает упражнения	Выполняют упражнения	5
5.	Проверочный тест	Демонстрирует видео с вопросами теста и его результатами	Отвечают на вопросы теста, подсчитывают баллы и определяют свой уровень знаний по безопасному использованию Интернета	5
6.	Рефлексия (подведение итогов урока)	Раздает учащимся карточки. Обобщает и систематизирует знания, полученные на уроке, вместе с учениками делает выводы	На карточке отмечают уровень полезности урока. Делают выводы.	5
7.	Тезисы и выводы	Напоминает правила охраны труда при работе за компьютером	Закрепляют урок по информатике и безопасности.	2

Вопросы для самопроверки:

- Чем опасны сайты подделки?
- Как распознать подделку?
- Что такое Спам? Как бороться со Спамом?
- Какие существуют методы блокировки Спам рекламы?
- Что относится к персональным данным, а что к личной (конфиденциальной) информации?

- Какую информацию можно публиковать в сети?
- Почему не стоит публиковать свои полные данные?
- Анонимность в сети: правда или вымысел?
- Какие правила поведения в сети нужно соблюдать?
- Какие опасности подстерегают нас в открытых сетях?
- Как не стать жертвой преступника при использовании открытых сетей?
- Какие правила пользования чужой техникой нужно помнить?
- Лицензионное соглашение/правила пользования: читать или нет?
- Почему важно знать правила использования программного продукта/интернет-ресурса?
- Виды Интернет-мошенничества (объекты мошенничества)?
- Какие виды преступлений распространены в Интернете?
- Как не стать жертвой киберпреступника?

Открытый урок

Открытое учебное занятие является формой распространения и пропаганды передового опыта, элементом методической работы преподавателя. Целью открытого учебного занятия является показ передовых форм и методов учебно-воспитательной работы, анализ дидактической эффективности использования технических средств обучения и применения ИКТ, обобщение приемов научной организации и контроля качества учебного процесса. Применение новых педагогических технологий, приемов и методов преподавания, при помощи которых реализуются цели занятия, формирование знаний, умений и навыков на основе самостоятельной познавательной деятельности учащихся, являются основными требованиями к открытому уроку.

Открытое занятие должно служить иллюстрацией выводов, к которым пришел преподаватель в результате педагогического эксперимента, работы над педагогической темой, результата работы по педагогической технологии

или на основании многолетнего опыта работы.

Методическая цель открытого занятия может быть сформулирована следующим образом:

- методика использования персонального компьютера в решении практических задач;

- методика организации самостоятельной работы учащихся;

- активизация познавательной деятельности учащихся на занятиях (практических, лабораторной работе...) в процессе работы с наглядными пособиями и дидактическим материалом.

- методика использования ИКТ в процессе изложения нового материала, проверки знаний, межпредметных связей и т.п.

Формы и методы

В принципе, тип и форма проведения урока, методы организации работы детей могут быть любые. Но при этом необходимо помнить, что открытый урок – не время для апробации новых способов организации учебной деятельности учащихся. Открытый урок должен пройти в привычной, известной и учителю, и учащимся форме, только тогда и учитель, и его подопечные смогут чувствовать себя уверенно и комфортно. Нельзя поделиться с коллегами опытом, которого не имеешь. Не убедительно для присутствующих звучат слова учителя о том, что он «хотел попробовать, как это получится» после неудавшегося урока.

Преобладание объяснительно-иллюстративных методов не обеспечивает деятельностный подход к обучению, формированию ключевых компетентностей учащихся – а именно это является важнейшей составляющей современного образовательного процесса. Преподаватель должен продемонстрировать не свои знания в предметной области и ИКТ – компетентность, а умение организовать работу учащихся по достижению поставленных учебных целей. С осторожностью нужно подходить и тщательно планировать использование таких форм проведения открытого урока как:

Лекция. Гости идут на открытый урок не для того, чтобы прослушать монолог учителя, а для того, чтобы посмотреть, как учитель организует работу учащихся.

Однако, если на уроке ожидается присутствие преподавателей только одной учебной дисциплины, способных по достоинству оценить необычность, оригинальность, новизну в структуре и содержании лекции, визуальном сопровождении и др., и при этом планируется на определенном этапе вовлечение учащихся в обсуждение (лекция с элементами беседы) то эта форма проведения урока может быть оправдана.

Урок – конференция. Вереница докладов, чаще всего скачанных с интернета, следующих один за другим и монотонно читаемых с листа, способна утомить кого угодно, и естественно, не поразит никого из присутствующих. В условиях тотального дефицита времени гостям гораздо важнее увидеть, как учитель добивается усвоения обязательного программного материала, чем послушать серию докладов учеников по материалу, в котором они часто сами плохо разбираются (с демонстрацией презентации, изобилующей текстовой информацией, и читаемой со слайдов самим докладчиком). Понятно, что и учащиеся, занятые подготовкой такого доклада, и учитель «убили» массу времени при подготовке к уроку, но также жаль и то, что все присутствующие на уроке не много для себя с него вынесут.

Работа в группах. Очень сложная методически форма организации работы. Немногие учителя ею владеют настолько, чтобы делиться своим опытом. В большинстве случаев объявленная преподавателем работа в группах на самом деле групповой не является. Групповая работа предусматривает совместную деятельность по созданию определенного продукта, при этом предполагается разделение труда по выполнению задачи между всеми участниками и подготовку коллективного отчета. Кроме того, большой фрагмент урока для присутствующих оказывается «закрытым» - трудно проследить за ходом рассуждений учащихся, за их совместной работой сидя за последней партой. Планируя работу в группах, следует позаботиться о включение гостей в

активную деятельность: создать из присутствующих педагогов отдельную группу и предложить им выполнить задание, привлечь педагогов к работе ученических групп в качестве наблюдателей или участников, предложить учителям ознакомиться с накопленным дидактическим или методическим материалом и др.

Викторины (которые чаще всего проводятся по вопросам, которые по умолчанию должны быть усвоены на предыдущих уроках всеми обучающимися), конкурсы и мини-спектакли лучше перенести на вторую половину дня. Для урока в 8-11 классах больше подходят дидактические и деловые игры. Как показывает опыт, наиболее удачными получаются комбинированные уроки, предполагающие смену видов деятельности учащихся.

Перед уроком:

Дайте краткую характеристику класса, в котором будет проходить занятие (охарактеризуйте учебные возможности детей, их успеваемость по данному предмету и по другим).

Сообщите гостям, какой УМК вы используете, каково место данного урока в системе уроков он занимает, что и как изучалось на предыдущем уроке, какое задание получили учащиеся на дом. Ознакомьте присутствующих с проектом урока, озвучьте, какие методы обучения и формы организации работы вы намерены использовать, на что нужно обратить особое внимание.

Подготовьте раздаточный материал: на столах гостей должны быть те же дидактические материалы, что и у учащихся. Не забудьте положить учебники, задачники и другую литературу, которая будет использоваться учениками на уроке. Распечатайте план урока в нужном количестве экземпляров. Кроме того, хорошо, если гостям будет предоставлена возможность ознакомиться и с другими документами и материалами: календарно-тематическим планом, разработанными учителем методическими и дидактическими материалами, отражающими опыт работы и др.

Обговорите с гостями возможность фото- и видеосъемки во время урока.

Психологическая подготовка учащихся к открытому уроку

На открытом уроке, еще в большей степени, чем на обычном, дети испытывают потребность в признании и чувство неловкости от допущенных ошибок. Боязнь показаться глупым, подвести преподавателя и свой класс, часто нагнетаемая самим преподавателем, делает детей скованными и малоактивными. Это сказывается и на ходе урока, и на его результатах, и на общем впечатлении о нем. Учитель-мастер, знающий характер каждого учащегося, уровень его подготовки и подготовленности, умеющий адекватно оценить потенциал ребенка, найдет возможность его включения в работу таким образом, чтобы он мог показать себя с лучшей стороны и продемонстрировать результат своей деятельности приемлемым для себя способом.

О предстоящем открытом занятии лучше всего объявить учащимся на уроке, ему предшествующем. Не следует заранее позиционировать открытый урок как особое мероприятие, требующее от участников свершения каких-либо подвигов. Но при этом следует попросить учащихся не опаздывать на урок, быть вежливыми с гостями и друг с другом и обратить внимание на внешний вид. Перед открытым уроком учащиеся должны получить привычное для себя домашнее задание.

Рекомендации по организации и проведению «круглых столов», практических занятий, презентаций

Тема безопасности в сети Интернет имеет важнейшее значение при решении задач обучения и воспитания подрастающего поколения. В рамках Всероссийской акции по безопасности школьников в сети Интернет пройдут множество мероприятий в различных формах их проведения. В данном разделе рекомендаций более подробно мы остановимся на следующих: «круглый стол», практическое занятие, презентация и приведем примеры их проведения.

Круглый стол — общество, конференция или собрание в рамках более крупного мероприятия (съезда, симпозиума, конференции). Используется в двух смыслах — как свободная конференция разнородных участников для непосредственного обсуждения определённых проблем (в частности, конфликтов) и — реже — как закрытое общество избранных, принимающее в кулуарах важные решения.

- цель обсуждения — обобщить идеи и мнения относительно обсуждаемой проблемы;
- все участники круглого стола выступают в роли пропонентов (должны выражать мнение по поводу обсуждаемого вопроса, а не по поводу мнений других участников); отсутствие набора нескольких ролей характерно не для всех круглых столов;
- все участники обсуждения равноправны; никто не имеет права диктовать свою волю и решения.

Практическое занятие — одна из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения навыков и опыта творческой деятельности, овладения современными методами практической работы с применением технических средств.

Презентация — (от лат. praesento — представление) — документ или комплект документов, предназначенный для представления чего-либо (организации, продукта и т.п.). Цель презентации — донести до аудитории полноценную информацию об объекте презентации в удобной форме.

Проведение круглого стола «Основы безопасности в сети Интернет»

Использованные материалы: Методические рекомендации: Методика организации недели «Безопасность Интернет»./Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. В. - Тамбов, ИПКРО 2012.

Цель: формирование устойчивых жизненных навыков при работе в сети Интернет.

Работе круглого стола предшествует предварительная подготовка обучающихся по предложенной тематике. Перечень вопросов для обсуждения выявляется в результате анкетирования обучающихся. Примерные вопросы для обсуждения на круглом столе:

7. Для чего нужен Интернет?
8. Какие существуют риски при пользовании интернетом, и как их можно снизить?
9. Какие виды мошенничества существуют в сети Интернет?
10. Как защититься от мошенничества в сети Интернет?
11. Что такое безопасный чат?

6.Виртуальный собеседник предлагает встретиться, как следует поступить?

7. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

При подведении итогов круглого стола обучающимся можно предложить правила поведения в сети Интернет.

Примерный сценарный план:

время (минуты)	**этап**	**примечание**
1-3	Приветствие	
3-5	Цели круглого стола	
5-10	Введение. Проблематика темы безопасности в сети интернет.	Модератор
11-14	Какие существуют риски при пользовании интернетом, и как их можно снизить?	Спикер 1
15-20	Вопросы, Обсуждение. Дискуссия.	
21-24	Как защититься от мошенничества в сети Интернет?	Спикер 2
25-30	Вопросы, Обсуждение. Дискуссия.	
31-34	Безопасные социальные сети: простые правила.	Спикер 3
35-40	Вопросы, Обсуждение. Дискуссия.	
41-44	Итоговые тезисы.	Модератор, участники
44-45	Окончание круглого стола	

План практического занятия по теме «Безопасность при работе в Интернет»

Разработка педагога дополнительного образования
высшей квалификационной категории
МОУ ДОД ДДТ «Кировский» г. Новосибирска
Мельникова Алексея Владимировича

Задачи:

1. Ознакомить уч-ся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
2. Научить избегать этих угроз.
3. Рассказать о действиях, которые необходимо предпринять при столкновении с этими угрозами.
4. Освоить практические навыки работы в сети Интернет.

Литература и интернет-ресурсы:

1. Сайт **http://content-filtering.ru/children/**
2. Блинков И.А.: Безопасность детей и молодежи в сети Интернет
3. Брошюра «Безопасность детей в Интернете» изд. Microsoft
4. Чат **http://prikol.interchat.ru/**
5. Сайт МБОУ лицея № 176 **http://licei176.ru/**

Программное обеспечение:

1. Microsoft Windows XP,
2. Microsoft Internet Explorer

Сценарный ход занятия:

I. Организационный момент

II. Программы, позволяющие путешествовать по сети Интернет – браузеры (Internet Explorer, Opera, Firefox, и др.) Как пользоваться браузером (на примере Internet Explorer)

Значение Интернет

В Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями.

Но сеть Интернет скрывает и угрозы.

Наиболее часто встречающиеся угрозы при работе в Интернет:

1. Угроза заражения вредоносным программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы. Эти методы довольно часто используется хакерами для распространения троянских вирусов;

2. Доступ к нежелательному содержимому. Это насилие, наркотики, страницы подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию;
3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи;
4. Поиск развлечений (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег.
5. Неконтролируемые покупки.

Посещение сайта **http://content-filtering.ru/children/**

Чтение вступительной статьи на сайте

Переход по ссылке «Средние классы»

Чтение раздела «Вы должны это знать», и обсуждение правил безопасности.

Деление учащихся на группы.

Задание для каждой группы:

Зайти на страницы сайта, посвященные различным видам деятельности в сети Интернет. Прочитать правила работы, и объяснить, чем может обернуться невыполнение этих правил.

Обобщение полученной информации:

Рекомендации, с помощью которых посещение Интернет может стать менее опасным:

1. Посещайте Интернет вместе с родителями, или делитесь с ними успехами и неудачами в деле освоения Интернет;
2. Если в Интернет вас что-либо беспокоит, то вам следует не скрывать этого, а поделиться своим беспокойством со взрослыми;
3. При общении в чатах, использовании программ типа ICQ, использовании on-line игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Выберите регистрационное имя (псевдоним), не содержащее никакой личной информации;
4. Нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.;
5. Уважайте собеседников в Интернет. Правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
6. Никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
7. Далеко не все, что можно прочесть или увидеть в Интернет – правда. Спрашивайте у взрослых о том, в чем вы не уверены;

Составление сводной таблицы правил поведения в сети Интернет

Никогда	Всегда
Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы без разрешения родителей	Всегда будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть
Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями	Всегда спрашивай у родителей разрешения посидеть в чате
Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения	Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство

взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах	беспокойства или волнение. Не забудь обсудить это с родителями
Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера	Всегда держи информацию о пароле при себе, никому его не говори
Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые	Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман
	Всегда держись подальше от сайтов "только для тех, кому уже есть 18". Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой счет за Интернет

Если ты услышишь или увидишь, что твои друзья заходят в «небезопасные зоны», напомни им о возможных опасностях и посоветуй, как им правильно поступить.

Будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в «небезопасную зону» или загрузить на свой компьютер вирус или программу-шпион.

Если вы получили оскорбляющие сообщения, расскажите об этом родителям.

Всегда принимайте помощь от взрослых или друзей, разбирающихся в вопросах безопасного Интернета. Мама и папа могут не знать ответов на все интересующие вас вопросы.

Задание:

Обсудите предложенные идеи по сохранению безопасности в сети Интернет со своими друзьями. Возможно, вы придумаете новые и дополните список правил.

Практическая работа.

1. Зайдите в Гостевую книгу сайта МБОУ лицея № 176 **http://licei176.ru/** и оставьте в ней запись, используя правила безопасности и сетевого этикета, с которыми мы сегодня ознакомились.
2. Зайдите в детский чат **http://prikol.interchat.ru/**, зарегистрируйтесь там, и пообщайтесь, используя правила безопасности и сетевого этикета, с которыми мы сегодня ознакомились.

III. Подведение итогов занятия

IV. Домашнее задание.

Составьте список правил сетевого этикета и оформите его в электронном виде (Word, презентация). Можно с иллюстрациями.

Презентации

Невозможно заниматься темой безопасности в сети интернет, не используя широкие возможности сети. Одной из ярких возможностей донесения любой информации сегодня являются презентации. Презентация - это серия слайдов, которые могут содержать различные типы контента, такие как изображения, файлы мультимедиа, текст, эффекты и т.д.

Презентации бывают разных видов и, как правило, отличаются своей функциональностью и стоимостью. Чем объемнее и технологичнее презентация, тем сложнее ее выполнение. Зависит всё, конечно же, от уровня аудитории.

Презентации можно разделить на следующие виды:

1. Бумажные презентации:

В основном они используются для раздаточного материала отдельно каждому лицу, для личного ознакомления. В отличие от электронной презентации, в бумажной презентации можно использовать более подробное описание темы. Однако недостаток такого вида презентации в том, что рассеивается внимание во время выступления и добиться нужного понимания всех участников бывает не всегда возможно.

2. Электронные презентации:

Такой вид презентации воспроизводится на большом экране, или с помощью проектора. Он самый выигрышный, потому что в данном случае можно использовать все возможные технические и функциональные возможности (такие как видео, аудио и интерактивные элементы), необходимые для визуального представления и нужного Вам эффекта.

Виды электронных презентаций:

- *Управляется по щелчку.* Процессом презентации управляет ведущий, сопровождая своими комментариями.
- *Самовоспроиводимая презентация.* Презентации такого вида используются без участия пользователя. В основном демонстрируются на мониторах в презентационных, торговых залах, выставочных стендах и т.д.

Формат презентации:

- *Power Point Презентации.* Power Point позволяет создавать презентации в виде слайд-шоу, с применением анимации, звука и сценария. Презентации такого типа могут производить впечатление, если созданы профессиональным дизайнером и все ее составляющее – графика, текст, анимация – выполнены в едином стиле.
- *PDF Презентации.* Набор статичных страниц, в основном применяются для рассылок или распечатки на принтере. Отличаются простотой, красивым фирменным стилем, правильно представленной информацией. Недостаток – статичность.

Способ представления информации:

- Статичные презентации;
- Анимированные презентации;
- Мультимедийные презентации;
- Видео презентации (информация представлена в виде видеофильма);
- 3D-презентации (информация представлена в трехмерной графики и трехмерной анимации).

Назначение презентации:

Какой бы вид презентации Вы не выбрали, главным остается ее содержание и качество исполнения.

Примеры презентаций размещены в разделе Приложения.

Подготовка отчетных и презентационных материалов по итогам проведения образовательных мероприятий

(форма отчетных документов, формат и способ отправки для оценки)

Организаторы в субъекте РФ Всероссийской акции, посвящённой безопасности школьников в сети Интернет до 16 сентября 2016 года должны отправить отчет о проведенных мероприятиях на электронные адреса Организатора акции: konkurs@деткивсетке.рф, internetkonkurs@inbox.ru.

Требования к отчету Всероссийской акции. Отчет предоставляется формате: Microsoft Word. Содержание отчета должно включать статистический отчет о проведенных мероприятиях и аналитический отчет:

1. Статистическая форма отчета

Субъект Российской Федерации: _____				
Общее количество мероприятий, проведенных в субъекте РФ в рамках Всероссийской акции	Общее количество образовательных организаций, принявших участие в акции в субъекте РФ	Общее количество участников акции в субъекте РФ, в т.ч. по категориям (родители, учащиеся по классам)	Три лучших мероприятия акции в субъекте РФ по выбору организатора (название, учитель, образовательная организация)[5]	Указание информационного ресурса, на котором размещены информационные материалы о ходе проведения Всероссийской акции

2. Аналитический отчет

[5] Обязательное приложение трех лучших сценариев к статистическому отчету

По итогам проведения Всероссийской акции информация о ходе и результатах проведенных образовательных мероприятий в субъекте РФ должна быть предоставлена в виде аналитического отчета, который не должен превышать 3 печатных страниц, шрифт Times New Roman, высота шрифта не менее кегль 14, межстрочный интервал 1,5.

Рекомендуемые критерии оценки работ участников при проведения Всероссийского конкурса безопасности школьников в сети Интернет.

1. Соответствие основным тезисам Положения о Конкурсе:
- соответствие целям и задачам;
- соответствие тематике;
- соответствие представленных форм и технологий;
- соответствие категории участников;
- соответствие временным и техническим параметрам.
2. Наличие авторского подхода в представленных материалах.
3. Инновационность подходов.
4. Доступность заявленных методов, возможность практического применения и транслирования.
5. Логика и системность материала.
6. Наличие результатов в представленных технологиях, соответствие достигнутых результатов результатам Конкурса.
7. Наличие технологий, способствующих популяризации тематике Конкурса.

Используемые и рекомендуемые источники

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. 10 плюсов социальных сетей/ С. Лешик; коммент. Кирилл Хломов//Здоровье школьника. - 2013. - № 4. - С. 56- 59: фот. (Психология: трудный возраст).
3. Арутюнов В. В. А есть ли защита там, в облаках? // Современная библиотека, 2014. №№ 3. С. 62-69
4. Ащеулова И. Правила компьютерной безопасности//Мурзилка. 2014. № 9.- С. 18-20.
5. Безопасность в глобальном информационном пространстве: V Международный форум безопасного Интернета/ И. Щеголев [и др.]//Школьная библиотека. - 2014. - № 5. - С. 3-6 : 5 фот., 2 схемы (Конференции. Совещания. Семинары) Доклады участников V Международного форума безопасного Интернета, состоявшегося 21 апреля 2014 года в Москве.
6. Гуляева Зинаида. Неделя безопасного Рунета//Библиотека. 2014. № 1. С. 73.
7. Джордан Ш. Мобильность на страже детской безопасности//Компьютер-mouse. 2014.№ 1.С. 24-25 : 2 фот.
8. Кибербезопасность: московский форум//Современная библиотека. - 2014. - № 2. - С. 31-35: ил. (ИКТ). Обзор Международного форума по кибербезопасности.
9. Клепа и железный друг [Электронный ресурс - http://klepa.ru]: 2014. № 8. С. 1-33:
10. Короповская В. П. Проекты Google для работы школьников с книгой//Школьная библиотека: сегодня и завтра. 2014. № 4. С. 59-63
11. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации.-М.: Изд. дом «Академия»2006. С.256

12. Лауфер П. «Березовый лес» или «лес березовый»?//Юный эрудит, 2014. № 3. С. 24-26.

13. Лебедева О. Компьютерная грамотность и безопасность подростков в сетевом режиме//Библиотека. 2014. № 4. С. 29-30.

14. Мухачева О. А. Воспитываем «электронного гражданина»: методическая помощь и детям, и взрослым//Библиотечное дело. 2014. № 11. С. 22-23.

15. Партыка Т.Л., Попов И.И. Информационная безопасность.- 2-е изд., М.: ФОРУМ:ИНФРА-М, 2007. С.368

16. Поташник М.М., Левит М.В. Как подготовить и провести открытый урок (современная технология) – М.: Педагогическое общество России, 2008.

17. Поташник М.М. Требования к современному уроку – М.: Центр педагогического образования, 2008.

18. Примочкин Б. Интернет-зависимый ребенок: что делать//Игра и дети. [Электронный ресурс - http://www.i-deti.ru/arhiv/2013/3/internet-zavisimyy-rebyonok-chto-delat-strategiya-i-taktika-vzroslyh-no32013]: 2013.№3.С.34-35..

19. Редькина Н. С. Качество онлайн - услуг//Научные и технические библиотеки. 2014. № 8. С. 18-27.

20. Риски и угрозы в Интернете для детей и подростков//Основы безопасности жизнедеятельности. - 2014. - № 1. - С. 41-46: 2 фот. (Информационная безопасность). О проблеме нарастания новых рисков, связанных с распространением информации в Интернете.

21. Савельев И. Дети "паутины"//Семья и школа. 2014. № 7/8. С. 52-55.

22. Смирнова С. Маленькие дети в Интернете//Здоровье школьника.2014.№ 3.С. 75-76:2 фот. . - ISSN 1818-099X.

23. Смирнова С. Мы в ответе за тех, кого подключили//Здоровье школьника. 2014.№ 4.С.73-74

24. Укрощение цифровой обезьяны: как избавиться от интернет - зависимости/Алекс Сучжон-Ким Пан; [пер. с англ.: Ю. Жизненко, О. Кутуев]. - Москва: АСТ, 2014.С 319.

25. Холостов К. Помощь из сети//Юный техник. 2013. № 6. С. 70-75.

26. Храмов В.В.(под ред.). Защита информации в вычислительных системах // М.: ПНЦ РАН, 2002.С. 318

Электронные ресурсы:

https://www.youtube.com

https://ru.wikipedia.org

http://www.kaspersky.ru

http://ito.edu.ru

http://www.единыйурок.рф

http://минобрнауки.рф

http://nsportal.ru

http://деткивсетке.рф

http://www.pandia.org/

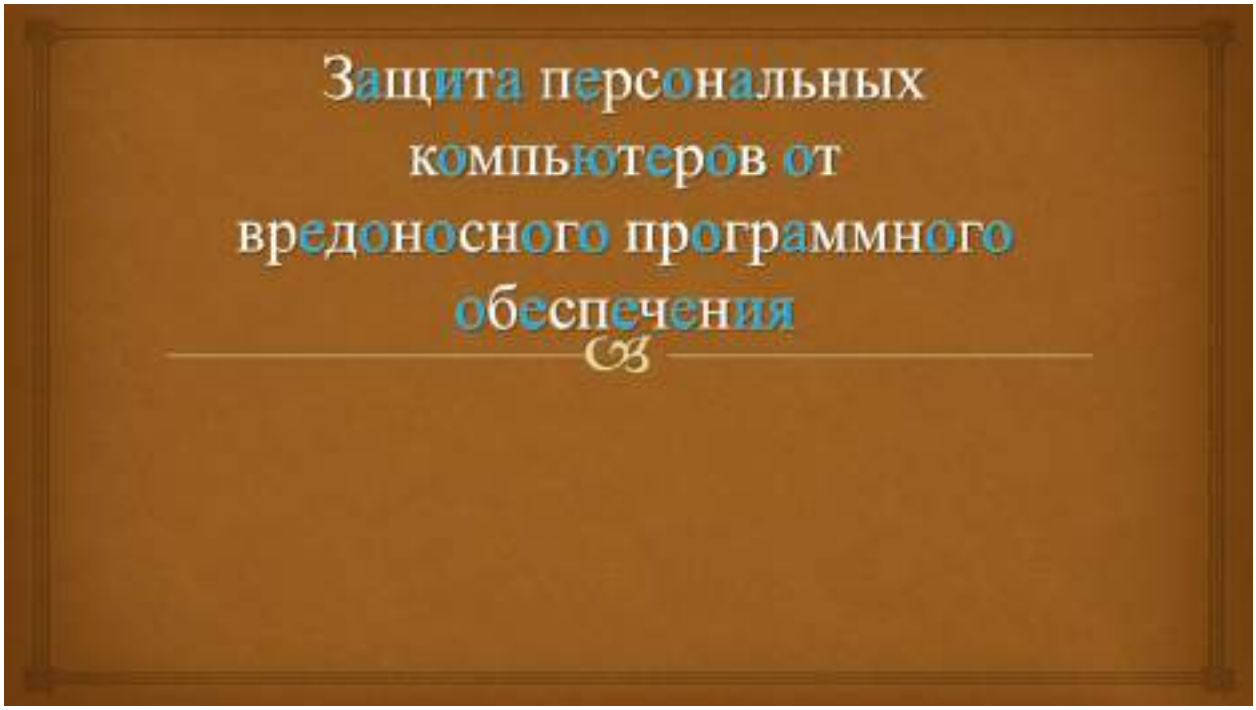
http://methodological_terms.academic.ru/

http://www.wildwebwoods.org/popup.php?lang=ru

http://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/urok-po-bezopasnosti-v-seti

Приложение

Материалы предоставлены КубГТУ и ИКСиИБ



Классификация компьютерных вирусов

Имеются несколько признаков классификации существующих вирусов:

- *По среде обитания;*
- *По методу существования в компьютерной среде;*
- *По принципу функционирования*;

По среде обитания вирусы можно разделить на такие виды:

1. *Загрузочные вирусы.*
2. *Файловые вирусы.*
3. *Файлово-загрузочные вирусы.*
4. *Сетевые вирусы.*
5. *Документные вирусы.*

Загрузочные вирусы проникают в загрузочные сектора устройств хранения данных (жесткие диски, дискеты, переносные запоминающие устройства). При загрузке операционной системы с зараженного диска происходит активация вируса. Его действия могут состоять в нарушении работы загрузчика операционной системы, что приводит к невозможности ее работы, либо изменении файловой таблицы, что делает недоступным определенные файлы.

Файловые вирусы чаще всего внедряются в исполнительные модули программ (файлы с помощью которых производится запуск той или иной программы), что позволяет им активироваться в момент запуска программы, влияя на ее функциональность. Реже файловые вирусы могут внедрятся в библиотеки операционной системы или прикладного ПО, исполнительные пакетные файлы, файлы реестра Windows, файлы сценариев, файлы драйверов. Внедрение может проводиться либо изменением кода атакуемого файла, либо созданием его модифицированной копии. Таким образом, вирус, находясь в файле, активируется при доступе к этому файлу, инициируемому пользователем или самой ОС. Файловые вирусы – наиболее распространенный вид компьютерных вирусов.

Файлово-загрузочные вирусы обедняют в себе возможности двух предыдущих групп, что позволяет им представлять серьезную угрозу работе компьютера.

Сетевые вирусы распространяются посредством сетевых служб и протоколов. Таких как рассылка почты, доступ к файлам по FTP, доступ файлам через службы локальных сетей. Что делает их очень опасными, так как заражение не остается в пределах одного компьютера или даже одной ловальной сети, а начинает распространятся по разнообразным каналам связи.

Документные вирусы (их часто называют макровирусами) заражают файлы современных офисных систем (Microsoft Office, Open Office…) через возможность использования в этих системах макросов. Макрос – это определенный, заранее определенный набор действий, микропрограмма, встроенная в документ и вызываемая непосредственно из него для модификации этого документа или других функций. Именно макрос и является целью макровирусов.

По методу существования в компьютерной среде вирусы делятся на такие виды:

1. Резидентные
2. Нерезидентные

Резидентный вирус, будучи вызван запуском зараженной программы, остается в памяти даже после ее завершения. Он может создавать дополнительные процессы в памяти компьютера, расходуя ресурсы. Может заражать другие запущенные программы, искажая их функциональность. Может "наблюдать" за действиями пользователя, сохраняя информацию о его действиях, введенных паролях, посещенных сайтах и т.д.

Резидентный вирус является неотъемлемой частью зараженной программы и может функционировать только во время ее работы. Однако не все компьютерные вирусы представляют серьезную угрозу. Некоторые вирусы тяжелых последствий после завершения своей работы не вызывают; они могут завершить работу некоторых программ, отображать определенные визуальные эффекты, проигрывать звуки, открывать сайты, или просто снижать производительность компьютера, резервируя под себя системные ресурсы. Таких вирусов подавляющее большинство. Однако есть и действительно опасные вирусы, которые могут уничтожать данные пользователя, документы, системные области, приводить в негодность операционную систему или даже аппаратные компоненты компьютера.

По принципу своего функционирования вирусы можно разделить на несколько типов:

1. **Вирусы-паразиты (Parasitic)** – вирусы, работающие с файлами программ, частично выводящие их из строя. Могут быть легко выявлены и уничтожены. Однако, зачастую, файл-носитель остается не пригодным.
2. **Вирусы-репликаторы (Worm)** – вирусы, основная задача которых как можно быстрее размножится по всем возможным местам хранения данных и коммуникациям. Зачастую сами не предпринимают никаких деструктивных действий, а являются транспортом для других видов вредоносного кода.
3. **Троянцы (Trojan)** – получили свое названия в честь "Троянского коня", так как имеют схожий принцип действия. Этот вид вирусов массирует свои модули под модули используемых программ, создавая файлы со схожими именами и параметрами, а так же подменяют записи в системном реестре, меняя ссылки рабочих модулей программ на свои, вызывающие модули вируса. Деструктивные действия сводятся к уничтожению данных пользователя, рассылке СПАМа и слежения за действиями пользователя. Сами размножатся зачастую не могут. Выявляются достаточно сложно, так как простого сканирования файловой системы не достаточно.

4. **Вирусы-невидимки (Stealth)** – названы по имени самолета-невидимки "stealth", наиболее сложны для обнаружения, так как имеют свои алгоритмы маскировки от сканирования. Маскируются путем подмены вредоносного кода полезным во время сканирования, временным выведением функциональных модулей из работы в случае обнаружения процесса сканирования, сокрытием своих процессов в памяти и т.д.

5. **Самошифрующиеся вирусы** – вирусы вредоносный код которых хранится и распространяется в зашифрованном виде, что позволяет им быть недоступными для большинства сканеров.

6. **Мутирующиеся вирусы** – вирусы не имеющие постоянных сигнатур. Такой вирус постоянно меняет цепочки своего кода в процессе функционирования и размножения. Таким образом, становясь неуязвимым для простого антивирусного сканирования. Для их обнаружения необходимо применять эвристический анализ.

7. **"Отдыхающие" вирусы** – являются очень опасными, так как могут очень продолжительное время находится в состоянии покоя, распространяясь по компьютерным сетям. Активация вируса происходит при определенном условии, зачастую по определенной дате, что может вызвать огромные масштабы одновременного заражения. Примером такого вируса является вирус CHIH или Чернобыль, который активировался в день годовщины аварии на ЧАЭС, вызвав выход из строя тысяч компьютеров.

Основные источники вирусов:

- Носитель, на котором находятся зараженные вирусом файлы;
- Компьютерная сеть, в том числе система электронной почты и Internet;
- Жесткий диск, на который попал вирус в результате работы с зараженными программами;
- Вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Основные методики обнаружения и защиты от вирусов:

- сканирование;
- эвристический анализ;
- использование антивирусных мониторов;
- обнаружение изменений;
- использование антивирусов, встроенных в BIOS компьютера.

Сканирование

Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов.

ЭВРИСТИЧЕСКИЙ АНАЛИЗ

Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы. Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов.

Антивирусы

В настоящее время существует различное множество всяких антивирусов, Одни из самых надежных и, в то же время, самых известных:

- Антивирус Лаборатории Касперского
- Avast!(он же бесплатный антивирус)
- Dr.Web
- ESET NOD32

Антивирусные мониторы

Целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

ОБНАРУЖЕНИЕ ИЗМЕНЕНИЙ

Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам. Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название программы-ревизоры). Ревизор может найти изменения, сделанные известным или неизвестным вирусом

Защита, встроенная в BIOS компьютера

В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.

Профилактика

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасный функционал системы (например, автозапуск-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.


#Кибербезопасность личности:
школьники
ИКСиИБ: 350000, г. Краснодар, ул. Красная 91, каб. 204
CSI: Капитан команды Сологубова Лариса
Тел: 8(905)402-39-85
Электронная почта: enactus_ktiib@mail.ru


#Цель: Повышение уровня грамотности населения при работе в открытых информационно-телекоммуникационных сетях.
#Задачи:
1. Разработка анкет, тестовой базы по определению уровня осведомленности в области информационной безопасности различных категорий населения (дети, взрослые, пенсионеры).
2. Разработка методических рекомендаций для проведения занятий по повышению уровня информационной грамотности.
3. Разработка интерактивного ресурса помощи гражданам в вопросе осведомленности правовых основ информационной безопасности.


#Целевая аудитория


#Самые незащищенные


#Почему именно дети?
DANGER
Заманчивые предложения
ОПАСНО


#Угрозы в сети Интернет
18+


#Нормативно-правовые документы по защите прав детей
• Конвенция о правах ребенка
• Семейный кодекс Российской Федерации
• Федеральный закон "Об основных гарантиях прав ребёнка в Российской Федерации“
• Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»
• Закон РФ "Об образовании в Российской Федерации"


#Нормативное регулирование детей от «вредной» информации
О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ
Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»
О СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ
Федеральный закон Российской Федерации № 2124-1 «О средствах массовой информации»
О РЕКЛАМЕ
Федеральный закон Российской Федерации № 38-ФЗ «О рекламе»