### Информационная безопасность детей и подростков в сети Интернет

В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов особое значение приобретает информационная безопасность детей. Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию.

**Тема: Информационная безопасность в сети Интернет.**

**Класс: 9-11.**

**Правовая база.**

Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права. Международные стандарты в области информационной безопасности детей нашли отражение и в российском законодательстве. Федеральный закон Российской Федерации № 436-ФЗ от 29 декабря 2010 года "О защите детей от информации, причиняющей вред их здоровью и развитию" устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищенности, 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 Российской Федерации от 21 июля 2011 г. № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию", направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Закон устанавливает порядок прекращения распространения продукции средства массовой информации, осуществляемого с нарушением законодательно установленных требований. Каждый выпуск периодического печатного издания, каждая копия аудио-, видео- или кинохроникальной программы должны содержать знак информационной продукции, а при демонстрации кинохроникальных программ и при каждом выходе в эфир радиопрограмм, телепрограмм они должны сопровождаться сообщением об ограничении их распространения. Закон запрещает размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенных для обучения детей, а также распространение рекламы, содержащей информацию, запрещенную для распространения среди детей, в детских образовательных организациях.

30.05.2011 на заседании Президиума Государственного совета и Комиссии по реализации приоритетных национальных проектов и демографической политике Уполномоченный при Президенте Российской Федерации по правам ребенка П.А. Астахов предложил провести в школах уроки медиа-безопасности. Данная инициатива поддержана Президентом России Д.А. Медведевым.

**Цель:** сформировать у школьников активную позицию в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им.

**Задачи:** ознакомить учащихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

**Оборудование:** плакаты по данной тематике (на доске), медиапроектор, экран, презентация Microsoft Power Point «Проблемы информационной безопасности в сети Интернет».

**Ведущие понятия:** угроза, безопасность, информация, угроза информационной безопасности.

**Ход занятия.**

1. Вступительная часть — сообщение цели занятия, основные правила, продолжительность и режим предстоящей работы.
2. Проведение экспресс-опроса участников об их ожиданиях от предстоящей работы.
3. Беседа учителя и учащихся строится на основе работы с материалами презентации «Проблемы информационной безопасности»

*Слайд 1*. Тема.

Учитель предлагает учащимся высказать мнение о том, как они понимают понятия «угроза», «безопасность», «информация», «угроза информационной безопасности».

*Слайд 2.* Знакомство с основными понятиями.

Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

Учитель просит учащихся назвать, какие они знают источники информации.

*Слайд 3.* Источники информации.

Средства массовой коммуникации, в т.ч. Интернет.

Литература.

Образование.

Личное общение.

Искусство.

Система социально-воспитательной работы и др.

Вывод. Любое из этих средств может быть использовано на благо или во вред личности!

*Слайд 4-7.* Справочная информация.

По последним данным, в России:

средний возраст начала самостоятельной работы в Сети - 10 лет (в 2009 году - 11 лет); и сегодня наблюдается тенденция к снижению возраста до 9 лет;

30% несовершеннолетних проводят в Сети более 3 часов в день (при норме 2 часа в неделю!).

Ежедневная детская аудитория Рунета:

46% (13-14 лет),

54% (15-16 лет);

самые "любимые" детьми ресурсы – социальные сети (78%); в них проводится до 60 минут в день.

Помимо социальных сетей, среди несовершеннолетних популярны следующие виды и формы онлайн-развлечений:

* сетевые игры;
* просмотр и скачивание фильмов, клипов, аудиофайлов, программ;
* обмен файлами;
* использование электронной почты, сервисов мгновенного обмена сообщениями, чатов;
* ведение блогов и пр.
* 4% детей сталкиваются в Интернете с порнографической продукцией
* 40% получают непосредственные предложения о встречах "в реале".

1. Давайте вместе подумаем. Вопросы для коллективного обсуждения:

– Почему тема информационной безопасности является важной и почему эти вопросы должны обсуждаться в школе?  
– Из возможных причин, какие можно выделите аспекты, связанные с сущностью Интернета и его значимостью как средства общения.

1. Работа в группах:

задание для групповой работы — подготовка коллективного ответа на вопрос: «Какие основные правила безопасного поведения в Интернете вы можете предложить?», «Какими правилами отбора (пользования) информации вы рекомендуете сверстникам пользоваться?», «Как оградить себя от кибер-преступлений?». (Возможные варианты работы: группы обсуждают все три вопроса. Каждая группа обсуждает только один из вопросов.).

1. Обсуждение результатов работы.
2. Продолжение работы с презентацией «Проблемы информационной безопасности».

*Слайды 8-11.* Три основных правила безопасного поведения в сети.

Защитите свой компьютер.

* Регулярно обновляйте операционную систему.
* Используйте антивирусную программу.
* Применяйте брандмауэр.
* Создавайте резервные копии важных файлов.
* Будьте осторожны при загрузке содержимого

Помните! После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

Защитите себя в Интернете.

* Думайте о том, с кем разговариваете.
* Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.
* Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

Помните! В Интернете не вся информация надежна и не все пользователи откровенны.

Думай о других пользователях.

* Закону необходимо подчиняться даже в Интернете.
* При работе в Интернете будь вежлив с другими пользователями Сети.
* Имена друзей, знакомых, их фотографии и другая личная информация не может публиковаться на веб-сайте без их согласия или согласия их родителей.
* Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено.
* Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.
* Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.

Помните! Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия

*Слайд 12.* Дополнительные правила безопасного поведения в сети Интернет.

Закрывайте сомнительные всплывающие окна! Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке. При отображении такого окна самым безопасным способом его закрытия является нажатие значка X (обычно располагается в правом верхнем углу). Невозможно знать наверняка, какое действие последует после нажатия кнопки «Нет».

Остерегайтесь мошенничества! В Интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение (например, в дискуссионных группах).

Помните! Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних.

*Слайд 13.* Подведение итогов работы. Учащиеся высказывают свое мнение, оправдались ли их ожидания от проделанной работы.

1. Размещение в дневниках правил безопасного поведения в сети.
2. Учитель благодарит учащихся за работу
3. Оценка учащимися занятия (на доску крепятся флажки. Красный – занятие понравилось; зеленый – занятие оставило равнодушным; синий – занятие не понравилось).

**Используемая литература и Интернет-ресурсы:**

1. В.В. Гафнер. Информационная безопасность: учебное пособие: ГОУ ВПО «Уральский государственный педагогический университет», Екатеринбург, 2009, ч. 1,2.

2. ["Основы безопасности детей и молодежи в Интернете" — интерактивный курс по Интернет-безопасности.](http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/html/etusivu.htm)

3.Портал Сети творческих учителей. <http://www.it-n.ru/communities.aspx?cat_no=71586&tmpl=com>

4. Вопросы обеспечения информационной безопасности от компании **Microsoft** [http://www.microsoft.com/rus/protect/default.mspx#](http://www.microsoft.com/rus/protect/default.mspx)

5. Вопросы безопасности - сайт от компании **Semantec** <http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids>

6. Ребенок в сети. Сайт от компании **Panda** <http://www.detionline.ru/>

7. Специальный портал созданный по вопросам безопасного использования сети Интернет. **Безопасный Интернет** <http://www.saferinternet.ru/>.

**Календарно-тематическое планирование**

|  |
| --- |
| Тема |
| Социальная сеть. История социальных сетей. |
| Мессенджеры. |
| Назначение социальных сетей и мессенджеров. |
| Пользовательский контент. |
| Персональные данные как основной капитал личного пространства в цифровом мире. |
| Правила добавления друзей в социальных сетях. |
| Профиль пользователя. |
| Анонимные социальные сети. |
| Сложные пароли |
| Онлайн генераторы паролей. |
| Правила хранения паролей. |
| Использование функции браузера по запоминанию паролей. |
| Виды аутентификации. |
| Настройки безопасности аккаунта. |
| Работа на чужом компьютере с точки зрения безопасности личного аккаунта. |
| Настройки приватности и конфиденциальности в разных социальных сетях. |
| Приватность и конфиденциальность в мессенджерах. |
| Персональные данные. |
| Публикация личной информации. |
| Определение кибербуллинга. |
| Возможные причины кибербуллинга и как его избежать? |
| Как не стать жертвой кибербуллинга. |
| Как помочь жертве кибербуллинга. |
| Настройки приватности публичных страниц. |
| Правила ведения публичных страниц. Овершеринг. |
| Фишинг как мошеннический прием. |
| Популярные варианты распространения фишинга. |
| Отличие настоящих и фишинговых сайтов. |
| Как защититься от фишеров в социальных сетях и мессенджерах. |
| Виды вредоносных кодов. |
| Возможности и деструктивные функции вредоносных кодов. |
| Вирусы |
| Как защитить компьютер от вредоносных программ |
| Итоговое занятие |

Нормативную правовую основу настоящей примерной образовательной программы по учебному курсу «Информационная безопасность» составляют следующие документы:

— Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

— ФГОС основного общего образования;

— ПООП основного общего образования;

— распоряжение Правительства РФ от 2 декабря 2015 г. № 2471-р «Об утверждении Концепции информационной безопасности детей»;

— Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

— Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»;

— Перечень поручений по реализации Послания Президента Федеральному Собранию от 27 февраля 2019 г. Пр-294.