

Спиридонова Надежда Михайловна

учитель информатики и ИКТ

Муниципальное автономное общеобразовательное учреждение лицей №23

город Калининград

## **СЦЕНАРИЙ УРОКА ИНФОРМАТИКИ «БЕЗОПАСНЫЙ ИНТЕРНЕТ»**

Интернет уже давно перестал быть неким изолированным виртуальным пространством только для посвященных. В Сеть в России ежедневно выходят десятки миллионов людей, при этом несовершеннолетние пользователи составляют значительную часть онлайн-сообщества. [1]

Информационная безопасность детей сегодня приобретает особое значение. Просвещение подрастающего поколения, знание ребёнком элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав детей.

**Тип занятия:** урок-проблема.

### **Цели урока**

*Образовательные –*

1. Повышение осведомленности школьников об их правах и обязанностях во время пребывания в глобальной сети,
2. Предоставление полного и всестороннего описание вероятных случаев нарушения законов об информационной безопасности,
3. Обучение навыкам безопасного использования интернета и эффективным способам решения данных проблем и предотвращения подобных ситуаций.

*Деятельностные –*

1. Формировать и развивать умение выделять главные и второстепенные причины возникновения проблем, связанных с Интернет, уметь анализировать их и находить средства и способы разрешения возникающих проблем.

## **Формирование УУД**

*Личностные* – умение четко формулировать и ясно излагать свои мысли или способности анализировать сложные ситуации.

*Регулятивные* – уметь формулировать собственную позицию в понимании проблемы и искать творческие пути ее решения, развивать умение аргументировать свою точку зрения.

*Коммуникативные* – формировать навык продуктивного общения в условиях учебного процесса, в той или иной мере приближенных к реальным условиям.

*Познавательные* – формировать и развивать умение строить доказательства, систематизировать материал, находить нужную информацию из разных источников.

## **Учебные задачи урока:**

- выявить основные проблемы, связанные с пребыванием в Интернете,
- обсудить возможные варианты, обменяться опытом решения проблем,
- получить представление о приемлемых моделях поведения в Интернете через обучающие и развивающие видеоматериалы от Youtube.com и Google,
- проверить полученные знания с помощью Интернет-теста и онлайн-тренажеров.

## **Активные методы обучения, используемые на уроке:**

Метод эвристических вопросов. Метод синектики

**Время проведения урока:** в начале учебного года при изучении темы «Правила поведения и техника безопасности при работе на компьютере» во всех классах согласно нагрузки.

**Возрастная аудитория:** учащиеся 8-11 классов.

### Ресурсы урока:

Компьютер с медиа-проектором и выходом в Интернет.  
Программа iSpring QuizMaker ознакомительная версия для создания тестов.  
Файл ТЕСТ «Безопасный Интернет».swf.

### СЦЕНАРИЙ урока:

#### **Есть проблема!**

Сейчас без Интернета довольно трудно представить нашу жизнь. Интернет – это работа, обучение, огромная масса полезной информации. Интернет – это общение и, конечно же, развлечения (игры, кино, музыка и прочие замечательные ресурсы).

Но, как и в реальной жизни, Интернет таит в себе массу опасностей: обман, грубость, насилие, мошенничество, вирусы...

**Как проводить время в Интернет интересно, не подвергая себя опасности?**

**Как избежать обмана и мошенничества в Интернете? Как грамотно работать с ресурсами Интернета и при этом самому не нарушать Закон?..**

Вопросов много... Обсуждение этих проблем будем начинать не с самой задачи (проблемы), а с анализа некоторых общих признаков, которые как бы вводят в ситуацию постановки проблемы, неоднократно уточняя ее смысл. А если проблема не решается, то целесообразным будет вернуться к анализу ситуации, ее порождающей.

*Работа учащихся регламентируется следующими правилами.*

1. При анализе проблем необходимо максимально использовать свой личный опыт, а также имеющиеся знания.
2. Не следует спешить подводить итог, если даже, кажется, что найдено удачное решение, надо постараться его развить, оценить.

Итак, начинаем!

**Проблема 1.** *Как проводить время в Интернет интересно, не подвергая себя опасности? Какие простые правила следует соблюдать?*

Обсуждение, обмен мнениями, опытом.

Итог: Варианты решения проблемы.

Рекомендации специалистов. Демонстрация видеоролика от Youtube: «Развлечения и безопасность в Интернете» [2]

**Проблема 2.** *В Интернете так много всяких конкурсов, лотерей и заманчивых предложений! Какие опасности таятся здесь?*

Обсуждение, обмен мнениями, опытом.

Итог: Варианты решения проблемы.

Рекомендации специалистов. Демонстрация видеоролика от Youtube: «Остерегайся мошенничества в Интернете» [2]

**Проблема 3.** *Но нам часто приходится пользоваться ресурсами разных сайтов и в учебных целях: надо написать реферат, доклад, сообщение, найти какие-то сведения, фотографии... Как грамотно работать с ресурсами Интернета и при этом самому не нарушать Закон?*

Обсуждение, обмен мнениями, опытом.

Итог: Варианты решения проблемы.

Рекомендации специалистов. Демонстрация видеоролика от Youtube: «Как обнаружить ложь и остаться правдивым в Интернете» [2]

**Проблема 4.** *Наши электронные почтовые ящики: странные письма, спам, взломы... Пример фишингового письма, отправленного от имени почтового сервиса[5]. Как вы думаете, для чего нужны злоумышленникам логины и пароли от почтовых ящиков или аккаунтов социальных сетей обычных людей? Имеется ли у вас подобный печальный опыт?*

Обсуждение, обмен мнениями, опытом.

Итог: Варианты решения проблемы.

Рекомендации специалистов. Демонстрация видеоролика «10 советов от Google начинающему интернет-пользователю с Николаем Фоменко. Выбираем пароль». [6]

### Подведем итоги

Мы выявили основные проблемы, связанные с пребыванием в Интернете, обсудили возможные варианты и обменялись опытом решения проблем, получили представление о приемлемых моделях поведения в Интернете (Youtube и Google помогли нам в этом).

Осталось проверить полученные знания с помощью теста и онлайн-тренажеров.

**ТЕСТ«Безопасный Интернет»** – вам предлагается ответить на 9 вопросов, связанных с правилами безопасного поведения в Интернете. Тест настроен на отправку результатов тестирования в электронный почтовый ящик учителя – автора урока.

Критерии оценивания:

оценка 2	≤ 40% правильных ответов,
оценка 3	41 – 60 % правильных ответов
оценка 4	61 – 80 % правильных ответов,
оценка 5	81 – 100 % правильных ответов.

Выставление оценок в журнал.

### Домашнее задание

1. Проверить пароли от своих почтовых ящиков или аккаунтов социальных сетей с помощью онлайн-тренажера «Конфиденциальность и безопасность в Интернете» Информационно-образовательного портала сети образовательных учреждений Ярославской области – задание «100 – Сделайте качественный пароль» [3]

2. Изучив разделы *Ресурсы о безопасности* и *Полезный контент* сайта Безопасный Интернет для детей <http://i-deti.org> , выяснить (с записью в

тетради), по каким телефонам можно получить телефонную или онлайн-консультацию в случае, если вы пострадали от злоумышленников в Интернете или обнаружили нежелательный контент. Какие источники развлекательного и образовательного характера привлекли ваше внимание и чем?

## ПРИЛОЖЕНИЕ

**Тест «Безопасный Интернет»** Вопросы к тесту взяты с Интернет-теста информационного раздела сети образовательных учреждений Ярославской области, посвященный безопасной работе в сети Интернет [4]

### 1. Какую персональную информацию не следует публиковать в сети Интернет в открытом доступе?

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> номер домашнего телефона  | <input checked="" type="checkbox"/> свои фотографии      |
| <input checked="" type="checkbox"/> номер мобильного телефона | <input type="checkbox"/> никнейм                         |
| <input checked="" type="checkbox"/> свой e-mail               | <input type="checkbox"/> кличку своего домашнего питомца |
| <input type="checkbox"/> названия любимых книг, песен         |  |
| <input checked="" type="checkbox"/> номер своей школы, класса |  |

### 2. Последствиями сетевой атаки для Вашего компьютера могут быть:

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> неработоспособность программ     | <input checked="" type="checkbox"/> заражение компьютера вредоносными программами |
| <input type="checkbox"/> поломка компьютера                          |   |
| <input checked="" type="checkbox"/> кража или уничтожение информации |   |

### 3. Поддельный сайт – это...

- сайт, распространяющий поддельные, пиратские ключи для платного программного обеспечения
- сайт, замаскированный под внешний вид какого-либо другого сайта
- сайт, созданный для распространения спама
- здесь нет правильного ответа

**4. Вы получили от друзей неожиданные файлы неизвестного вам содержания. Ваши действия:**

- откроете файл и ознакомитесь с содержимым
- сохраните файл на компьютер, затем проверите антивирусной программой и в случае отсутствия вирусов откроете файл
- удалите письмо с подозрительным файлом, не открывая его

**5. В ваш почтовый ящик пришло письмо, в котором говорится, что его надо переслать пяти друзьям. Какое действие предпринять?**

- переслать его пяти друзьям
- переслать его не пяти, а десяти друзьям
- не пересылать такие письма
- ответить отправителю, что вы больше не хотите получать такие письма

**6. Что такое кибербуллинг?**

- мошенничества, совершаемые в сети Интернет
- размещение в сети Интернет провокационных сообщений с целью вызвать конфликты между участниками беседы
- любые сообщения или публикации в сети, размещаемые с целью запугать, оскорбить или иначе притеснить другого

**7. Как надо хранить свои пароли (например, от электронной почты или профиля в социальной сети)?**

- записывать в блокнот
- сохранять в скрытом файле на компьютере
- использовать менеджер паролей
- запоминать
- наклеить цветные стикеры с паролями на монитор

**8. Мошенничество, при котором злоумышленники обманным путем выманивают у доверчивых пользователей сети личную информацию, называется:**

- |                               |   |
|-------------------------------|---|
| <input type="radio"/> крекинг | <input checked="" type="radio"/> фишинг |
| <input type="radio"/> серфинг | <input type="radio"/> биллинг           |

**9. Укажите, каким способом вирус может попасть на Ваш компьютер (выберите один или несколько вариантов):**

- по электронной почте
- при скачивании зараженных файлов из интернет
- через флеш-накопители
- при загрузке зараженного веб-сайта

## ИСТОЧНИКИ И РЕСУРСЫ:

1. Сергей Плуготаренко. Мнения экспертов. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт <http://i-deti.org/experts/48/>. 2011-2012
2. Видеоролики от Youtube.com: «Развлечения и безопасность в Интернете», «Остерегайся мошенничества в Интернете», «Как обнаружить ложь и остаться правдивым в Интернете» <http://i-deti.org/video/>. 2011-2012
3. Онлайн-тренажер «Конфиденциальность и безопасность в Интернете» Информационно-образовательного портала сети образовательных учреждений Ярославской области – задание «100 – Сделайте качественный пароль» [http://www.edu.yar.ru/safety/dni\\_media\\_bezopasnosti/game.html](http://www.edu.yar.ru/safety/dni_media_bezopasnosti/game.html), 2011
4. Интернет-тест информационного раздела сети образовательных учреждений Ярославской области, посвященный безопасной работе в сети Интернет // [http://www.edu.yar.ru/safety/dni\\_media\\_bezopasnosti/testirovanie.html](http://www.edu.yar.ru/safety/dni_media_bezopasnosti/testirovanie.html), 2011
5. Пример фишингового письма, отправленного от имени почтового сервиса. Википедия – свободная энциклопедия. Фишинг. <http://ru.wikipedia.org/wiki/%D4%E8%F8%E8%ED%E3>
6. Видеоролик «10 советов от Google начинающему интернет-пользователю с Николаем Фоменко. Выбираем пароль»: <http://www.youtube.com/watch?v=QvOlgob5njQ>