БЕЗОПАСНЫЙ ИНТЕРНЕТ

УРОКИ КИБЕРБЕЗОПАСНОСТИ В ШКОЛЕ

СБОРНИК МЕТОДИЧЕСКИХ РАЗРАБОТОК

ДУБНА, 2015

Методические разработки педагогов образовательных учреждений г.Дубны Московской области в рамках проведения всероссийского урока кибербезопасности

Октябрь 2015 г.

г. Дубна

Ответственный редактор:

Е.В.Рожкова, директор Муниципального бюджетного учреждения «Центр развития образования города Дубны Московской области»

Редакционная группа:
Е.В. Рожкова
Е.Г. Белоскова
М.А. Калмыкова

Технический редактор:
М.А. Калмыкова

Методические разработки педагогов образовательных учреждений г.Дубны Московской области в рамках проведения всероссийского урока кибербезопасности.

Сборник адресован администрации общеобразовательных учреждений, специалистам, педагогам, классным руководителям.

Материалы сборника опубликованы на сайте Муниципального учреждения «Центр развития образования г.Дубны Московской области» http://mucro.goruno-dubna.ru

Муниципальное бюджетное учреждение «Центр развития образования города Дубны Московской области»,
141980, г. Дубна, Московская область, ул. Мира, д.1.
Тел.: 8 (496) 214-02-50

СОДЕРЖАНИЕ

План - конспект урока на тему
«Безопасный интернет» (5-9 класс)

Антонова Ольга Алексеевна
учитель информатики
МБОУ «Гимназия №3 г.Дубны Московской области»

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

Задачи:

- изучение информированность пользователей о безопасной работе в сети интернет;
- знакомство с правилами безопасной работы в сети интернет;
- ориентирование в информационном пространстве;
- способствовать ответственному использованию online-технологий;
- формирование информационной культуры обучающихся, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами;
- воспитание дисциплинированности при работе в сети.

Обучающиеся должны знать:

- перечень информационных услуг сети интернет;
- правилами безопасной работы в сети интернет;
- опасности глобальной компьютерной сети.

Обучающиеся должны уметь:

- Ответственно относиться к использованию on-line-технологий;
- работать с web-браузером;
- пользоваться информационными ресурсами;
- искать информацию в сети интернет.

Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный, (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Ссылки на web-ресурсы:

1) http://www.kaspersky.ru – антивирус «лаборатория касперского»;
2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;
3)http://www.interneshka.net – международный онлайн-конкурс по Безопасному использованию интернета;
4)http://www.saferinternet.ru – портал российского оргкомитета по Безопасному использованию интернета;
5) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;
6) http://www.rgdb.ru – российская государственная детская библиотека.

Этапы урока:

1.Организация начала урока. Постановка цели урока. Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html Постановка темы и главного вопроса урока.
2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).
3. Практическая работа. Поиск информации в сети интернет. Дискуссия по найденному материалу.
4. Закрепление изученного материала. Рекомендации по правилам безопасной работы в интернет. Тестирование.

5. Подведение итогов урока. Оценка работы группы. Домашнее задание.

Ход урока

1. Организация начала урока. Постановка цели урока.

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всем мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И ни когда-то, а прямо сейчас (просмотр видеоролика «дети и интернет» – 1 мин. (по выбору))

(http://www.youtube.com/watch?v=hbvgg6-3ewo&feature=autoplay&list=pld70b32df5c50a1d7&playnext=1 Как оставаться в безопасности на youtube

Http://www.youtube.com/watch?v=3ap1rkr0rce&feature=relmfu Развлечения и безопасность в интернете

Http://www.youtube.com/watch?v=amcsvzxcd9w&feature=bfa&list=pld70b32df5c50a1d7&lf=autoplay остерегайся мошенничества в интернете

Http://www.youtube.com/watch?v=xrsnlkvempy&feature=relmfu мир глазами Gmail - защита от спама)

Как не стать жертвой сети интернет? Тема нашего урока - «безопасный Интернет».

Главный вопрос урока: как сделать работу в сети безопасной?

2. Изучение нового материала.

Игра «за или против».

Учитель предлагает игру «за или против». На слайде – несколько Высказываний. Попробуйте привести аргументы, отражающие Противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного Образования. И это хорошо!
2. Интернет – это глобальный рекламный ресурс. И это хорошо!
3. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.
4. Интернет является мощным антидепрессантом.
5. В интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Учитель предлагает ученикам ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». (Целесообразно заранее нескольким обучающимся подготовить короткие сообщения по темам: «интернет-зависимость», «вредоносные и нежелательные программы», «психологическое воздействие на человека через интернет», «материалы нежелательного содержания», «интернет-мошенники»).

Физ. Минутка «Собери рукопожатия».

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей.

Обсуждение.

- кому сколько человек удалось поприветствовать?
- у кого-то возник психологический дискомфорт? Если – да, то чем он был вызван?

Анализ ситуации.

Общаясь в интернете, мы очень часто добавляем незнакомых людей. В свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту. Учитель предлагает ответить на главный вопрос урока – «как сделать работу в сети безопасной?»

3. Практическая работа.

Что можно? Что нельзя? К чему надо относиться осторожно? Обучающимся предлагается посмотреть ресурсы
Http://content-filtering.ru/aboutus,
Http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.html,
Http://www.youtube.com/watch?v=y37ax5tpc3s&feature=related.
Учитель спрашивает, что об этом можно прочитать на web-страницах и просит обучающихся сформулировать правила безопасной работы.

4. Закрепление изученного материала.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Современный интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем Собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео,

Включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше интернет-общение будет приносить пользу.

Рефлексия.

Учитель предлагает учащимся проанализировать свою работу на уроке.

И помните, интернет может быть прекрасным и полезным
Средством для обучения, отдыха или общения с друзьями. Но – как и
Реальный мир – сеть тоже может быть опасна!

Подводя итог урока, учитель оценивает активность работы учащихся. За самостоятельную индивидуальную работу можно поставить оценки.

Информация о домашнем задании, инструкция о его выполнении:
1. Дать определение понятию «информационная безопасность».
2. Составить информационный лист «моя безопасная сеть».

Внеклассное мероприятие «Я и мой компьютер»

Бовкунова Наталья Валерьевна,
учитель начальных классов
«МБОУ г.Дубны Московской области,
лицей №6 имени академика Г.Н.Флёрова»

Цели:

- повторить и закрепить состав основных устройств компьютера;
- развивать логическое мышление обучающихся;
- развивать мотивацию к здоровому образу жизни;
- оказать просветительскую и консультационную помощь в определении их отношения к компьютерной зависимости.

Задачи:

образовательные:

- повторение и закрепление знаний учащихся об устройстве персонального компьютера;
- информирование детей о пользе и вреде общения с компьютером;

развивающие:

- развитие логического мышления обучающихся;
-развитие познавательного интереса за счет игровых технологий;
- развитие творческих способностей школьников.

воспитательные:

- воспитание уважения к сопернику, умения достойно вести спор, находчивость;
- привлечение внимания к последствиям компьютерной зависимости.

Предварительная работа:

-анкетирование родителей: тест на детскую компьютерную зависимость
-анкетирование учащихся
- подготовка выставки творческих работ обучающихся, на тему « Компьютер–за и против»

Временные затраты: 45 минут

Оборудование: ноутбук, экран, мультимедийная установка, презентация

Ход мероприятия

I. Актуализация темы.

Мероприятие начинается с песни «До чего дошел прогресс» (муз.Е. Крылатова, сл. Ю. Энтина).
Учитель. Здравствуй дорогие друзья! Отгадайте загадку и ребусы и подумайте о чем пойдет разговор на нашем занятии.

Что за чудо агрегат
Может делать всё подряд –
Петь, играть, читать, считать,
Самым лучшим другом стать?
(Компьютер)

Недавно на родительском собрании проводили опрос и выяснилось, что некоторые из вас проводят за компьютером и компьютерными играми больше двух часов в день.

Проводя с компьютером, так много времени, вы наверно должны знать устройство компьютера, правила работы с ним, как не навредить своему здоровью, работая за компьютером. И сегодня мы это выясним.

1-й ведущий Человек всегда старался в большей или меньшей степени облегчить свою жизнь, в том числе и в плане умственной деятельности, и это не так уж плохо. Ведь в процессе поиска появляются на свет замечательные изобретения. Одно из них – персональный компьютер. Без него невозможно представить себе современный мир, иногда кажется, что компьютеры проникли всюду. Поэтому, кроме умения читать и писать сегодняшний школьник должен осваивать еще одну разновидность грамотности – компьютерную.

Задание Расшифруйте пословицу.

Координаты: (2,2), (4,3), (5,2), (1,3), (3,1).

	1	**2**	**3**	**4**	**5**
1	сканер	до	думает	и	печать
2	не	компьютер	кормит	бумага	а
3	человек	но	шифр	решает	принтер

«Компьютер решает, а человек думает»

II. Комплектация компьютера

СЦЕНКА 1

Сережа играет за компьютером. Входит бабушка с дневником.
Бабушка Внучек за что же ты двойку получил по математике?
Володя Да за примеры!
Бабушка Как же так? Все домашние задания на 5 делаешь, а тут вдруг два?
Володя Да я дома все на калькуляторе считаю. Вот смотри и умножу, и разделю, и прибавлю и вычту. А на уроке на сотовом телефоне батарейка села, поэтому и двойка.
Бабушка Ох, наверно внучек от компьютера вирус подхватил, слыхала я есть такие компьютерные вирусы. Пойду доктору позвоню.
Бабушка охая уходит, заходит мама.
Мама Сынок мне учительница русского языка сказала, что ты правила не учишь?!
Володя Мамуль, ну зачем мне учить правила. Ведь компьютер все за меня сам исправляет, да еще и запятые ставит. Ни подтирать, ни замазывать, ни переписывать не надо. Красота!
Мама огорченно уходит. Заходит папа.
Папа Сережа, ты в библиотеке был, книг для доклада по окружающему миру набрал?
Володя Ой пап, уморил! В библиотеке, ха-ха! Я и не знаю, где она находится. В Интернете все найти можно. Быстро и удобно. И вообще, родители, отстали вы от жизни. В ногу со временем идти надо!
Учитель Да, часто компьютер порождает иллюзии у детей: зачем учить таблицу умножения, стихи, готовить доклады, читать книги, да и вообще думать, если есть ЭВМ и Интернет. Лучше уж усовершенствовать или обновить свой ПК, чем напрягать извилины. Это самое настоящее заблуждение! Ведь у нас в голове спрятано нечто посложнее процессора, поэтому мозг человека нуждается в постоянной тренировке на протяжении всей жизни. Управлять компьютером должны люди, хорошо разбирающиеся в математике, физике, технике. Сейчас мы проверим ваши знания об устройстве компьютера.
Конкурс «Компьютерное хозяйство»

Задание командам: слушать внимательно задания и «вставлять» необходимые слова

1.	Оглянись, дружок, вокруг! Вот… - верный друг. Он всегда тебе поможет: Сложит, вычтет и умножит. *(компьютер)*	2.	Наверху машины всей Размещается… - Словно смелый капитан! А на нем горит … *(дисплей, экран)*	3.	Ну а рядом главный блок: Там бежит электроток К самым важным микросхемам. Этот блок зовут … *(системным)*
4.	Это вот - … Вот где пальцам физкультура И гимнастика нужны! Пальцы прыгать там должны! *(клавиатура)*	5.	А вот это…, братцы, Тут нам надо разобраться, Для чего же этот ящик? Он в себя бумагу втащит, И сейчас же буквы, точки, Запятые – строчка к строчке – Напечатает в момент! Очень нужный инструмент. *(принтер)*	6.	В зоопарке есть зайчишка, У компьютера есть… Эта… не простая, Эта… вот какая: Скромный серый коробок, Длинный тонкий проводок, Ну а на коробке – Две или три кнопки. *(мышка)*
7.	Сетевая паутина Оплела весь белый свет, Не пройти детишкам мимо. Что же это? *(интернет)*				

Дети называют, показывают предметы, определяют их предназначение.

III. Компьютер-друг.

Уточнение знаний о компьютере.

Учитель. Ещё несколько десятков лет назад компьютер был диковинкой, а сегодня он стал доступен обычной семье.

-Ребята у кого дома есть компьютер? Кто им пользуется?

-А как вы используете компьютер? (Слушаем музыку, играем, выполняем задания, готовим сообщения).

Каждое современное предприятие внедряет компьютерные технологии в производственный процесс.

-Ребята, где вы видели компьютер? (В авиа и железнодорожных кассах, в банках, магазинах, поликлинике, на работе у родителей).

Сегодня мы поговорим об компьютере: назовем положительные и негативные его стороны, определим основные виды опасностей, подстерегающих детей в и составим правила безопасного пользования.

Анализ тестирования обучающихся(приложение 2)

Итак. Компьютер помогает нам общаться, узнавать новое и т. д.

Учитель Все вы знаете, что компьютер сейчас работает и с числами, и с текстом, и с фотографиями, и с рисунками, звуком и видео информацией. Но первый компьютер был изобретен для вычислений, его так и называли электронно- вычислительная машина. Но неужели до этого у людей не было приспособлений для счета?

Конечно, были. Давайте с вами вспомним (пальцы, счеты, калькулятор, арифмометр)

Это была небольшая разминка, а теперь задания усложняются

Конкурс «Не зевай, поспевай» (детям предлагается при правильном ответе хлопнуть в ладоши)

1. Какой из перечисленных элементов входит в состав компьютера: канат, антенна, системный блок, пропеллер?
2. Как называют новичков в компьютерном деле: кофейник, чайник, самовар, утюг?
3. Как иначе называют Internet: телешоу, вирусная программа, телескоп, всемирная паутина?
4. Как называют людей, которые при помощи компьютера вскрывают секретные файлы спецслужб: хакеры, тараканы, вирусы, блохи?
5. Печатающее устройство, которое выводит информацию на бумагу: модем, сервер, печатная машина, принтер.
6. Устройство, при помощи которого можно управлять игрой на экране: мышь, указка, собака, палец.
7. Рычаг, служащий для управления игрой на экране монитора: джойстик, карандаш, гайка, шуруп.
8. Устройство служит для длительного хранения информации и для переноса информации с одного компьютера на другой: блокнот, дискета, кассета, сумка.
9. Область на диске или другом носителе информации, там хранятся тексты программ, документы и любые другие данные: файл, склад, библиотека, полка.
10. Специально написанная программа, обладающая свойством размножаться и разрушать компьютерные программы: бактерия, папирус, вирус, хакер.

Учитель Да, удивили вы нас.

1 ученик. Наш компьютер помогает инженеру и врачу,
Астроному, агроному, продавцу и скрипачу.
Все длиннющие расчеты выполняет тот же час
Без ошибок, если школьник
Выдаст правильный приказ.

IV. Физкультминутка

Учитель. Машина исполняет ваши команды четко, а давайте проверим, сможете ли вы также правильно выполнять команды.

Встали из-за парт и слушаем внимательно. (Упражнения из комплекса зрительной гимнастики.)

Раз – налево, два – направо,
Три – наверх, четыре – вниз.
А теперь по кругу смотрим,
Чтобы лучше видеть мир.
Взгляд направим ближе, дальше,
Тренируя мышцу глаз.
Видеть скоро будем лучше,
Убедитесь вы сейчас.
А теперь нажмем немного
Точки возле своих глаз.
Сил дадим им много - много,
Чтоб усилить 1000 раз!

О компьютерных играх.

2 ученик	**3 ученик**
Много игр на белом свете, Вот они играйте, дети! Щелк! – и сам в мультфильме ты! Можешь прыгать с высоты, Пропасти перелетать И принцесс освобождать. И в бою со злым драконом	За компьютером сижу, На экран его гляжу. Увлекла меня с утра Интересная игра. До чего люблю я, братцы, С грозной нечестью сражаться: Поражения не зная,

Не остаться побежденным! Это все компьютер смог! И теперь, не чуя ног, Мы к компьютеру летим: Подружиться с ним хотим!	Злобных монстров побеждаю! Но, чтоб я не расслаблялся, Хитрый монстр теперь попался, И на уровне на пятом Он убил меня, ребята. Я убит… Вот это да! Это вам не ерунда! Хорошо, что монстр злой- Виртуальный не живой!

СЦЕНКА 2

В центре комнаты стоит компьютер, за которым увлеченно играет мальчик Сережа. Слышны звуки компьютерных игр. В комнату входит Мама.

Мама. Сережа, обед готов, идем кушать!

Сережа (раздраженно). Мама, мне некогда, я скоро перейду на второй уровень.

Мама (уходя). Что случилось с ребенком? Раньше был прекрасный аппетит!

В комнату входит бабушка.

Бабушка. Внучок, сходи, милый, в магазин за хлебом.

Сережа. Бабушка, не отвлекай меня, я должен закончить миссию в игре.

Бабушка. Какой был безотказный, во всем помогал…

Придется идти самой… Ох, беда, беда компьютерная!

К окну подходят несколько одноклассников Сережи.

Одноклассники. Сережа, пошли гулять во двор, в снежки играть.

Сережа. Не пойду! Мне это не надо. Мне и у компьютера хорошо!

Одноклассники. Сережа, в спортзал пора! Сегодня тренировка. Спартакиада скоро.

Сережа. Вот пристали! Надоел мне спорт.

Одноклассники. А ведь был лучшим спортсменом среди нас …

В комнату к Сереже заходит друг Саша.

Саша (пытаясь сесть рядом с Сережей). Давай поиграем вместе!

Сережа (отталкивая друга) . Еще чего! Мне и одному неплохо!

Саша (обиженно). Но мы же с тобой друзья…

Сережа. Сейчас мой друг – Супермен.

Саша (удивленно, залу) Променял друга на компьютерную игру?!

Саша уходит.

Учитель.

Итак. Не все игры построены на агрессии. Есть логические игры, игры для изучения школьных предметов. Есть тренажеры, с помощью которых можно получить важные и полезные навыки. Есть игровые тесты, которые помогут проверить свои знания.

Компьютерные технологии способствуют повышению качества характера ребенка: они создают условия для успешной социализации детей в обществе, формированию самостоятельности, целеустремленности, умения ставить перед собой задачу и добиваться ее решения, нормализации эмоционально – волевой и личностной сферы дошкольников.

Способствуют развитию психических процессов: памяти, внимания, воображения, мышления.

Дети с обучающими играми приобретают самостоятельность, собранность, сосредоточенность, усидчивость; приобщаются к сопереживанию, сотрудничеству, соперничеству.

Компьютер-враг

Учитель Некоторые дети, к сожалению, очень много времени проводят за компьютером, забывая о своем здоровье. Если после дня, проведенного у компьютера, кружится голова, болит шея, краснеют и чешутся глаза, большинство пользователей сразу вспоминают страшные байки о радиации, исходящей от компьютера. Они не верят, что все это происходит по их вине, из-за элементарного несоблюдения правил работы с ПК.

Каждая из команд получит по два вредных совета, за одну минуту вы должны подумать, чем опасны эти советы, и дать полезную подсказку.

1 совет Никогда не мойте руки, Монитор, клавиатуру. Это глупое занятие Не приводит ни к чему. Вновь испачкаются руки, Монитор, клавиатура. Так зачем же тратить силы, Время попусту терять.	**Учитель** **Грязная клавиатура** является источником распространения вредных микробов, поэтому надо регулярно протирать ее спиртом, не допускать сильного загрязнения, обязательно мыть руки перед работой на компьютере. Грязь и пыль на мониторе ухудшает качество изображения, поэтому необходимо регулярно стирать с него пыль.
2 совет Хочешь зрение улучшить, Сядь поближе к монитору, Лучше сразу носом ткнуться И сидеть так часов десять. И тогда уж через месяц Будет глаз как у орла.	**Учитель** Чтобы глаза не уставали и зрение не ухудшалось, надо сесть подальше от монитора, оптимально – 70 см. Зашторьте окна, чтобы не было бликов на экране. Монитор отклоните немного назад. Обязательно делайте зарядку для глаз.
3 совет Нет приятнее занятья, Чем, сутулясь сильно-сильно Посидеть у монитора. Тренируйтесь ежедневно, И наступит день счастливый – Вас в какое-нибудь царство Примут главным горбуном.	**Учитель** У тех, кто неправильно сидят за компьютером, со временем будут возникать серьезные проблемы с мышцами и суставами. Нельзя сутулиться, сидеть желательно на кресле с подлокотниками и регулировкой высоты сиденья. Занятия на компьютере детям нужно обязательно чередовать с физической нагрузкой через каждые 15 мин. занятий.
4 совет Посмотрите, что твориться В каждом доме по ночам: Повернувшись к монитору Молча школьники сидят. Ни за что не позволяют Их укладывать в кровать. Не хотят они, трудяги, Годы детские свои Провести под одеялом На подушке без штанов.	**Учитель** Ни в коем случае нельзя детям работать на компьютере в ночное время, так как у ребенка биологические часы сбиваются очень быстро, он будет с трудом засыпать, а днем чувствовать себя вялым и раздражительным. Даже в дневное время детям можно заниматься за компьютером не более 40 мин. с перерывами.

Итог

-Что мы можем сделать, чтобы не попасть в компьютерную зависимость? (Нужно стать грамотным пользователем, осваивать полезные программы, нужно поменьше играться, а заняться спортом, общаться с друзьями, читать книги и т. п.)

Чем именно вреден компьютер и как долго можно находиться перед ним? Происходит обсуждение.

Разработка классного часа «Безопасное использование интернет»

Горбунова Юлия Александровна,
учитель начальных классов
МБОУ «Средняя общеобразовательная школа
№4 г.Дубны Московской области»
Сайт: http://gorbunova.goruno-dubna.ru/
e-mail yulya_gorbunova_1980@mail.ru

Известно, что Интернет - сказочная страна. Конечно, здесь не поджидают за каждым кустом зубастые волки, но всё же не имея нужных знаний и опыта тут легко попасться в ловушку нечистоплотных пользователей или наткнуться на неподходящий контакт. Взрослые сами могут за себя постоять, но дети особенно впечатлительны и подвержены влиянию, и опасности Интернета могут оказать на них пагубное воздействие.

Но имеет ли смысл запрещать детям пользоваться сетью? Нет! Запрещать детям пользоваться сетью - это не выход. Такое поведение не поможет обезопасить ребёнка. Однако и полагаться на волю случая тоже не следует. Все риски, с которыми дети могут встретиться в сети, давно известны, и изучены, и соблюдение некоторых простых правил поможет избежать проблем.

Цели:

- 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: научить

- критически относиться к информационной продукции, распространяемой в сети Интернет;
- отличать достоверные сведения от недостоверных, вредную информацию от безопасной;
- избегать навязывания 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;
- нормам и правилам поведения детей в сети Интернет;
- организовывать безопасную работу дома в Интернете;
- определять угрозы безопасной работе в Интернете.

Ход классного часа:

Повернитесь друг к другу, посмотрите друг другу в глаза, улыбнитесь друг к другу, пожелайте друг другу хорошего рабочего настроения на уроке. Теперь посмотрите на меня. Я тоже желаю вам работать дружно, открыть что-то новое.

Определение темы

Ребята, посмотрев на эту картинку, как вы думаете, о чём сегодня я бы хотела с вами поговорить? Правильно, совершенно верно, но не просто об интернете, а о безопасном интернете. Ребята, а что такое безопасность? Когда мы говорим о безопасности? Вы все знакомы с компьютером и каждый из вас «заходил» в интернет. А что такое Интернет?

Есть такая сеть на свете Ею рыбу не поймать. В неё входят даже дети, Чтоб общаться иль играть.	Информацию черпают, И чего здесь только нет! Как же сеть ту называют? Ну, конечно ж... *(Интернет)*

Современный человек проводит в Интернете очень много времени. Кто-то занят поиском информации, кто-то общается в социальных сетях с друзьями или коллегами. То, что Интернет несет в себе большое количество возможностей — неоспоримо. Но вместе с этим, в глобальной сети скрывается масса потенциальных угроз. Особенно, если за компьютером сидите вы, мои дорогие дети.

Сегодня мы поговорим о том, чем опасен Интернет для вас и каким образом можно снизить уровень этой опасности.

Интернет — это огромнейший поток информации разного рода. Здесь мы можем найти что-то полезное, важное и значимое. Например, можно почитать последние новости, узнать прогноз погоды на неделю, найти много интересного об интересном писателе, скачать и посмотреть интересный фильм, любимую музыку, найти рецепт необычного блюда и многое другое. Но так же, здесь есть и совершенно бесполезные ресурсы и порталы, отнимающие время пользователя. Их мы прицельно рассматривать не будем, так как это личное дело каждого – тратить напрасно свои бесценные часы жизни или нет. Но есть еще одна категория информации в Сети, о которой как раз пойдет речь на нашем уроке. Это материалы, способные нанести вред человеку, особенно маленькому.

Работа в группах *Вы получили электронное письмо.*

«Дорогой друг! Мне нравятся твои комментарии. Видно, что ты умный и добрый человек. У меня к тебе есть интересное предложение. Давай встретимся сегодня в парке в 5 часов вечера. У меня в руках будет игрушка мишки. До встречи! Никому не сообщай о встрече! Это наш маленький секрет».

Посоветуйтесь в группах и и расскажите, как будите действовать прочитав письмо **(обсуждение в группах, выступления).**

Рефлексия

-Кому на уроке было интересно, прикрепите на доску смайлик с улыбкой.
- Кому просто комфортно было на уроке, смайлик с прямой линией.
- Кому было грустно, неинтересно на уроке, прикрепите грустного смайлика.

Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

А сейчас я вручу каждому памятки о правилах безопасного пользования детей интернетом

Памятка о правилах безопасного пользования детей интернетом и мобильной связью

1. Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
2. Прежде чем начать дружить с кем-то в Интернете, поставьте в известность родителей, спросите у них, как безопасно общаться.
3. При регистрации на сайтах старайтесь не указывать личную информацию т.к. она может быть доступна незнакомым людям. Где Вы живете, в какой школе учитесь, номер телефона должны знать только друзья и родственники.
4. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
5. Нежелательные письма от незнакомых людей называются «спам». Если получили такое письмо, не отвечайте на него, покажите его родителям. В случае, если ответите на подобное письмо, отправитель будет знать, что Вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам «спам».
6. Если Вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
7. Необходимо знать, что если публикуете фото- , видеоматериалы, каждый может посмотреть их.

Конспект урока информатики и ИКТ по теме «Безопасный Интернет» (9 класс)

Горячева Татьяна Андреевна,
зам. директора по УВР,
учитель информатики и ИКТ
МБОУ «Средняя общеобразовательная школа №9
с углубленным изучением иностранных зыков
г. Дубны Московской области»
goryachevatatyana@gmail.com

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

- изучить информированность обучающихся о безопасной работе в сети Интернет;
- сформулировать правила безопасной работы в Интернете;
- научить ориентироваться в информационном пространстве;
- способствовать ответственному использованию online-технологий;
- формировать информационную культуру учащихся;
- развивать критическое мышление;

Учащиеся должны знать:

перечень информационных услуг сети Интернет; опасности глобальной компьютерной сети.

Учащиеся должны уметь:

работать с Web-браузером; пользоваться информационными ресурсами; искать информацию в сети Интернет; ответственно относиться к использованию online-технологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Программно-дидактическое обеспечение: презентация «Безопасный Интернет.pptx», видеофайл «Безопасность школьников в сети Интернет (http://videouroki.net/view_post.php?id=376)», тест, информационные плакаты, карточки с адресами Web-ресурсов.

Ссылки на web-ресурсы:

1. Интернешка - онлайн-конкурс по полезному и безопасному использованию интернета и мобильной связи http://www.interneshka.net
2. Азбука цифрового мира http://www.edu.yar.ru/azbuka/password.php#game
3. Лига безопасного интернета http://www.ligainternet.ru/
4. "Основы безопасности детей и молодежи в Интернете" — интерактивный курс по Интерент-безопасности http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/quiz_ks3.htm

Этапы урока:

1. Организация начала урока. Постановка цели урока (3 мин). Постановка темы и главного вопроса урока.
2. Изучение нового материала (26 мин). Просмотр видеоролика. (16 минут). Физкультминутка. Дискуссия в группе.

3. Практическая работа (7 мин). Создание пароля. Закрепление изученного материала (7 мин). Тестирование.
4. Подведение итогов урока (2 мин). Оценка работы учащихся. Информация о домашнем задании.

Оформление доски, высказывания:

Интернет тебе не враг, если знаешь что и как!

Бесплатный сыр бывает в интернет-мышеловках!

В виртуальном мире есть свои правила!

Ход урока

1. Организация начала урока. Постановка цели урока (3 мин).

Приветствие учителя.

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь у вас появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И не когда-то, а прямо сейчас.

- Как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет». Главный вопрос урока: Как сделать работу в сети безопасной?

2. Изучение нового материала (26 мин).

На сегодняшний день мало кто не пользуется Интернетом. Он практически всегда с вами, в том числе на устройствах, которые помещаются в карман. С каждым днем растет число и разнообразие инструментов для работы в глобальной сети: Браузеры, приложения, почтовые клиенты, расширения. Прямо сейчас есть возможность передать сообщение на другой континент, выйти в социальную сеть, найти интересующий факт из биографии писателя. Всегда ли «Интернет» подразумевает что-то полезное и хорошее?

Игра «За или против» (4 мин.). Предлагаю поиграть в игру «За или против».

Вы увидите несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
2. Интернет – это глобальный рекламный ресурс. И это хорошо!
3. Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.
4. Интернет магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.
5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли (16 минут.)

Спасибо за ваши интересные высказывания. Сейчас будем работать в двух группах. Первая группа - У вас на столах есть листы «Чем опасен интернет?». На данных листах зафиксируйте опасности, о которых будет говориться в следующем видеоролике.

Вторая группа будет фиксировать правила безопасной работы в сети у себя в тетрадях.

Просмотр видеоролика. Заполнение листов.

Физ. минутка «Собери рукопожатия» (2 мин.).

Сейчас я вам предлагаю размяться, в течении 10 секунд Вам необходимо пожать руки как можно большего числа других людей.

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Чем он был вызван?

Аналогия с работой в Интернет.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия?

- Ответим на главный вопрос урока – «Как сделать работу в сети безопасной?»

Обсуждение листов «Чем опасен Интернет», формулирование правил безопасного интернета (4 мин).

Вы добавили бы к списку опасностей еще что-то? Как избежать этих опасностей?

Добавить к услышанным проблемам: спам, распространение вирусов, кибербуллинг, инетрнет-зависимость.

3. Практическая работа (7 мин.).

Очень много проблем возникает у людей, при потере пароля от электронной почты. Зачем нужен пароль? И как сделать свой пароль надежным?

Перейдите для практической части за компьютеры *(работа в парах).* В браузере есть закладка на Азбуку цифрового мира. (http://www.edu.yar.ru/azbuka/password.php#game)

Комикс «Зачем нужен пароль». Обсуждение.

Оказывается, Тройка самых популярных в мире паролей выглядит так: «password», «monkey» и «123456»

Простые правила выбора пароля: Длина не менее 8 символов, использование букв обоих регистров, использование букв и цифр, а так же специальных символов.

Почему не желательно выбирать в качестве пароля словарное слово?

(Потому что словарные слова быстрее подбираются киберпреступниками)

Сейчас вам требуется создать качественный пароль. Нажмите на кнопку Начать. После того как вам удастся придумать хороший пароль - запишите его на доске с указанием времени на взлом.

Слайд 5. Посмотрите примеры формирования паролей.

4. Закрепление изученного материала (7 мин.).

Тестирование (7 мин). Проведем небольшое тестирование по теме нашего сегодняшнего урока.

5. Подведение итогов урока (2 мин.).

Я рада, что вы не остались равнодушны к теме безопасного интернета. Спасибо за активное участие (оценка работы группы).

Информация о домашнем задании, инструкция о его выполнении.

Всем: Дать определение понятию «информационная безопасность».

На выбор: 1. Составить информационный лист «Моя безопасная сеть» или

2. Составить памятку «Правила безопасной работы в интернете».

Тестирование к уроку «Безопасный интернет»

Ключ к тесту: a,b,c,e,f; 2-a,c,d; 3-b; 4 - b,c; 5 – c; 6 – c; 7 – d; 8 – c; 9 - a,b,c,d

За каждую отмеченную верную букву 1 балл. Максимум 19 баллов.

За неверно отмеченную букву минус - 0.5 баллов.

«5» - 18-19 баллов

«4» - 14-17.5 ошибки

«3» - 10-13.5 баллов

Тестирование к уроку «Безопасный интернет»

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

a) номер домашнего телефона
b) номер мобильного телефона
c) свой e-mail
d) названия любимых книг, песен
e) номер своей школы, класса
f) свои фотографии
g) никнейм
h) кличку своего домашнего питомца

2. Последствиями сетевой атаки для Вашего компьютера могут быть:

a) неработоспособность программ
b) поломка компьютера
c) кража или уничтожение информации
d) заражение компьютера вредоносными программами

3. Поддельный сайт – это…

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

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

a) откроете файл и ознакомитесь с содержимым
b) сохраните файл на компьютер, затем проверите антивирусной программой и в случае отсутствия вирусов откроете файл
c) 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?

a) переслать его пяти друзьям
b) переслать его не пяти, а десяти друзьям
c) не пересылать такие письма
d) ответить отправителю, что вы больше не хотите получать такие письма

6. Что такое кибербуллинг?

a) мошенничества, совершаемые в сети Интернет
b) размещение в сети Интернет провокационных сообщений с целью вызвать конфликты между участниками беседы
c) 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)?

a) записывать в блокнот
b) сохранять в скрытом файле на компьютере
c) использовать менеджер паролей
d) запоминать
e) наклеить цветные стикеры с паролями на монитор

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

a) крекинг
b) серфинг
c) фишинг
d) биллинг

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

a) по электронной почте
b) при скачивании зараженных файлов из интернет
c) через флеш-накопители
d) при загрузке зараженного веб-сайта

Информационное сообщение на уроке на тему «Безопасность в сети Интернет» в рамках «Единого урока кибербезопасности»

Дудкин Сергей Викторович,
учитель информатики и ИКТ,
МБОУ «Средняя общеобразовательная школа №2
г. Дубны Московской области»
e-mail: sergvict1@yandex.ru

Цель сообщения — повышение уровня информированности обучающихся в области информационной безопасности, ознакомление с правилами ответственного и безопасного поведения в **современной информационно-телекоммуникационной среде.**

I. Безопасность в интернете

1. Общая безопасность в интернете

Интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их.

Какие опасности могут поджидать в интернете

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут использовать самые разные инструменты и методы — например, вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах.

Вирусы

Вирусы могут распространяться с помощью вложенных файлов, ссылок в электронных письмах или в соцсетях, на съемных носителях, через зараженные сайты. Сообщение с вирусом может прислать как посторонний человек, так и знакомый, но уже зараженный участник социальной сети или почтовой переписки.

Зараженными могут быть сайты, специально созданные в целях мошенничества, или обычные ресурсы, но имеющие уязвимости информационной безопасности.

Рекомендации

• Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требование перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Мошеннические письма

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма по определенному сценарию. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль в обмен на небольшую сумму.

Рекомендации

• Внимательно изучите письмо. Проверьте достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.

• Игнорируйте такие письма.

Получение доступа к аккаунтам в социальных сетях и на других сервисах

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, на почтовых и других сервисах. Украденные аккаунты они используют, в частности, для распространения спама и вирусов.

Мошенники могут получить доступ к учетной записи жертвы следующими способами:

• Заставить жертву ввести свои данные на поддельном сайте.

• Подобрать пароль жертвы, если он не сложный.

• Восстановить пароль жертвы с помощью «секретного вопроса» или указанной при регистрации электронной почты.

• Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Как правило, для кражи личных данных используются фишинговые сайты. Фишинг (от англ. **fishing** — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации

• Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

• Никому не сообщайте свой пароль.

• Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.

• Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).

• Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

Похищение данных при использовании бесплатных сетей Wi-Fi

Сейчас мы много общаемся через компьютер или смартфон и часто делаем это в общественных местах — подключившись к Wi-Fi-сети, которая не защищена паролем. Когда никто из окружающих не заглядывает в экран, создаётся ощущение приватности. На самом деле, передача данных через открытую Wi-Fi- очку – это в каком-то смысле разговор в полный голос в людном месте.

Злоумышленники создают сети с распространёнными названиями и просматривают всё, что подключившиеся к ней пользователи делают в интернете: читают и пишут личные сообщения в соцсетях, вводят пароли или данные банковских карт.

Рекомендации

• Используйте мобильный интернет (EDGE, 3G, LTE).

• Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

• Старайтесь посещать только сайты с шифрованием данных (HTTPS – он обычно отмечен зелёным замочком в браузерах).

• Используйте специальные средства защиты — браузеры со специальным безопасным режимом просмотра страниц или программы-защитники, которые разрабатывают антивирусные компании.

2. Безопасность платежей в интернете (для старшеклассников)

Большая часть мошеннических операций в интернете оказываются успешными по тем же причинам, что и в реальной жизни, — из-за таких человеческих качеств, как невнимательность, неосведомленность, наивность, беспечность.

2.1. Распространенные примеры платежного мошенничества

Фиктивные звонки от платежных сервисов

Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Цель звонка — выманить платежные данные, с помощью которых можно украсть деньги с карты или из кошелька.

Рекомендации

• Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.

• Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.

Выманивание смс-пароля незнакомцем

Пользователю может прийти смс от банка или платежного сервиса с паролем для совершения платежа. Сразу после этого звонит человек, который говорит, что ввел этот номер мобильного телефона по ошибке, и просит сообщить код из смс, которое только что пришло пользователю. На самом деле код из смс — это пароль не к счету незнакомца, а к счету пользователя. С помощью пароля злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Рекомендации

• Никому не сообщайте пароли, пин-коды и коды из смс, которые приходят на мобильный номер от банков, платежных сервисов, а также мобильных операторов.

Фальшивые письма от платежных сервисов

Пользователь может получить фальшивое письмо от имени платежного сервиса, своего банка или других платежных сервисов. Например, о том, что его счет заблокирован и для разблокировки необходимо перейти по ссылке и ввести свои данные. Единственная цель таких писем — заставить человека перейти на поддельный (фишинговый) сайт и ввести там свои персональные данные, которые будут украдены. В дальнейшем эти данные могут быть использованы, например, для доступа к счету пользователя. Кроме того, на таком сайте компьютер может быть заражен вирусом.

Рекомендации

• Помните, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.

• Не переходите по ссылкам из таких писем и не вводите свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка, Яндекс.Денег или другого платежного сервиса.

• Перед вводом своих платежных данных на каких-либо сайтах проверяйте адрес сайта в браузере. Например, вместо money.yandex.ru фальшивый сайт может иметь адрес money.yanex.ru.

Фальшивые выигрыши в лотерее

Пользователь может получить сообщение (по телефону, почте или смс), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет. Конечно, никакого обещанного приза пользователь не получит.

Признаки фальшивой лотереи

• Пользователь никогда не принимал участие в этой лотерее и вообще ничего о ней не знает.

• Пользователь никогда не оставлял своих личных данных на ресурсе или в организации, от имени которой приходит сообщение.

• Сообщение составлено безграмотно, с орфографическими ошибками.

• Почтовый адрес отправителя — общедоступный почтовый сервис. Например, gmail.com, mail.ru, yandex.ru.

Бесплатное скачивание файлов

Часто пользователям, которые хотят бесплатно скачать файл или посмотреть видео в хорошем качестве без рекламы, предлагают ввести на сайте мобильный номер. Если так и сделать, может включиться платная смс-подписка и с указанного номера будут списываться деньги.

Рекомендации

• Не указывайте свой мобильный номер на незнакомых сайтах.

• Если подписка уже оформлена, позвоните в службу поддержки оператора мобильной связи и попросите отключить её.

2.2. Платежные данные, которые нельзя раскрывать

Что делать, если

…вы потеряли карту.

Срочно позвоните в банк, попросите ее заблокировать и перевыпустить. Желательно с новым номером. Пока вы не заблокируете карту, любой, у кого она окажется в руках, сможет воспользоваться ею — например, оплатить дорогую покупку в интернет-магазине.

…вам пришло уведомление о платеже, который вы не совершали.

Подайте в банк заявление об отмене операции, где максимально подробно опишите произошедшее. Банк рассмотрит ваше обращение и вернет вам деньги. Не затягивайте с подачей заявления: оно должно быть обработано в срок от 30 до 60 дней с момента совершения операции.

…вы забыли пароль от электронного кошелька.

Зайдите на сайт платежного сервиса и нажмите на ссылку «Восстановить пароль» — система запросит мобильный номер, к которому привязан кошелёк. Указав номер телефона, вы получите смс с кодом для восстановления пароля.

2.3. Безопасность при оплате картами

Обеспечить безопасность своей банковской карты несложно, если придерживаться следующих *рекомендаций:*

• Не сообщайте номер карты другим людям.

• Храните банковскую карту в надежном месте.

• Не держите записанные пароли и коды рядом с картой.

• Заведите отдельную карту для покупок в интернете.

• Используйте для покупок в интернете только личный компьютер.

• Регулярно обновляйте антивирусную защиту компьютера.

• Старайтесь делать покупки в известных и проверенных интернет-магазинах.

• Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.

• Подключите в банке услугу смс-уведомлений, чтобы получать сведения о всех совершаемых платежах.

• Сохраняйте документы об оплате и доставке товаров, полученные по

электронной почте.
• Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.
• Не используйте общественный Wi-Fi при совершении покупок в интернете – данные банковских карт могут быть перехвачены мошенниками.

II. Законы о защите детей в информационной сфере.

Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищѐнности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.);

№ 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 ребѐнке порочные наклонности, сформировать у ребѐнка искажѐнную картину мира и неправильные жизненные установки.)

Разработка урока «Безопасность в Интернете» (9 – 11 классы)

Жевтило Ирина Аскольдовна,
учитель информатики
МБОУ «Лицей «Дубна»
г.Дубны Московской области»

Цель урока: способствовать формированию у обучающихся навыков безопасного и ответственного поведения в современной информационно-телекоммуникационной среде.

Задачи:

образовательные:

- сформировать правила безопасной работы учащихся в Интернете;
- учить ориентироваться в современном информационном пространстве;
- заложить основы правовых знаний работы в Интернете.

развивающие:

- формировать информационную культуру учащихся;
- развивать умение самостоятельно находить нужную информацию пользуясь web-ресурсами;
- развивать критическое мышление.

воспитательные:

- воспитывать ответственность и дисциплинированность учащихся при работе в сети.

Оборудование: компьютерный класс, ПК, мультимедийный проектор.

Ход урока

I. Оргмомент

II. Активизация внимания

Учитель.

Сегодня у нас очень важная тема, те проблемы, о которых мы будем говорить, касаются абсолютно каждого из вас. Посмотрев, на рисунки и попробуйте определить тему нашего урока.

Интернет вошел в нашу жизнь. Интернет наш помощник – помогает нам работать, путешествовать, отдыхать, общаться с друзьями. Интернет наш учитель – помогает получать новые знания, своевременную информацию.

Но путешествие в Интернет похоже на поход неопытного человека в лес. В лесу можно заблудиться, попасть в болото, собрать ядовитые грибы или ягоды, попасть в лапы диких зверей. Но, если человек знает лес, знает, кто в нем обитает, знает растения, которые в нем растут, то поход в лес ничего кроме пользы и удовольствия не принесет.

Так и в Интернете много полезного, нужного и интересного, но на каждой web – странице вас могут поджидать информация, опасная для вашего кошелька, физического или психического здоровья и даже жизни.

Задача нашего урока оценить эти опасности и выработать стратегию поведения в каждом конкретном случае.

III. Новый материал

Группа 1

Вирусы

1. Что делают вирусы на нашем компьютере? (виды вирусов, пути распространения, деструктивные действия)
2. Антивирусные программы (назначение, возможности, советы по безопасности)

Группа 2

Мошенники в Интернете

1. Сайты – двойники
2. Интернет – шантаж
3. Предложение работы на дому и не только
4. «Лохотрон» на проверке безопасности
5. Инвестиционные проекты и финансовые пирамиды

Демонстрируется видеоролик «Безопасность и развлечения в Интернете»

Группа 3

Информация в интернете

1. Безопасное общение. Что такое «скам»?
2. Интернет – зависимость
3. Какие сайты не следует посещать никогда

Демонстрируется видеоролик «Безопасность в Интернете»

Группа 4

Этика и право в Интернете

1. Этические нормы Интернета
2. «Крэкерские» сайты и «ломаные» программы
3. Защита интеллектуальной собственности в России

Просмотр видеоролика «Я и Интернет»
(http://kvestsetevichok.ru/index.php/2015-09-17-14-45-01/videourok

Правила безопасного поведения в сети Интернет

Просмотр видеоролика, подготовленный пресс-службой Совета Федерации Федерального Собрания Российской Федерации, о проведении 30 октября во всех школах страны Единого урока безопасности в сети Интернет (http://kvestsetevichok.ru/index.php/rolik-soveta-federatsii).

IV. Закрепление материала

Учитель.

Давайте проверим, насколько хорошо вы усвоили сегодняшний урок, выполнив тест на компьютере. (Индивидуальная работа учащихся на ПК)

V. Итог урока

VI. Домашнее задание (по выбору учащихся)

1. Запишите в тетрадь основные правила безопасного поведения в сети Интернет
2. Придумать сказку для учащихся младших классов об осторожности в Интернете

VII. Рефлексия

Разработка урока на тему «Безопасность в сети Интернет»

Зеленкова Алена Александровна,
учитель информатики и ИКТ
МБОУ «Гимназия №8 им. академика Н.Н. Боголюбова
г.Дубны Московской области»
Адрес сайта http://s8.goruno-dubna.ru/
e-mail school8@uni-dubna.ru

Цель урока: изучить опасные угрозы сети Интернет и методы борьбы с ними;
Задачи:

- *Образовательная:* познакомиться с понятием «Интернет», «Вирус», изучить приемы безопасности при работе в сети Интернет;
- *Развивающая:* развитие интереса к предмету, информационной культуры; формирование приёмов логического мышления; развитие способность анализировать и обобщать, делать выводы;
- *Воспитательная:* воспитание аккуратности, точности, самостоятельности, привитие навыки групповой работы, сотрудничества;
- *Здоровьесберегающая:* соблюдение санитарных норм при работе с компьютером, соблюдение правил техники безопасности, оптимальное сочетание форм и методов, применяемых на уроке;

Предварительная подготовка учащихся: материал, изученный на предыдущих уроках информатики;
Предварительная подготовка учителя: изучение материала урока, написание конспекта, создание презентации, создание теста, подготовка видеофрагмента;

Дидактические основы урока:
Методы обучения: словесные, наглядные, практические.
Тип урока: объяснение нового материала;
Формы учебной работы учащихся: фронтальная, индивидуальная работа.

Оборудование: ПК, проектор, интерактивная доска (или экран), 12 компьютеров, тетради, презентация «Безопасность в сети Интернет».

План урока:

1. Организационный момент (1-2 мин.);
2. Введение в тему (3-5 мин.);
3. Объяснение нового материала (30-35 мин.);
4. Физкультминутка (1 мин.);
5. Самостоятельная работа (7-10 мин.);
6. Итог урока (2-3 мин.);

Ход урока:

1. **Организационный момент, 1-2 мин.:**
   - ✓ сообщение темы урока (занесение темы в тетрадь), его целей и задач;

✓ краткий план деятельности.

2. Введение в тему, 3-5 мин.:

✓ подготовить детей к восприятию темы;

✓ нацелить на продуктивную работу.

Сегодня наш урок посвящен теме «Безопасность в сети Интернет». (Слайд 1)

Примечание. Учащиеся записывают в тетрадь основные определения самостоятельно по ходу лекции.

(Слайд 2) *Интернет* – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)

Молодцы!

3. Объяснение нового материала (27-30 мин.):

А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом (Слайд 3):

1. Вредоносные программы
2. Кража информации
3. Халатность сотрудников
4. Хакерские атаки
5. Финансовое мошенничество
6. Спам
7. Аппаратные и программные сбои

Как вы видите, угроз достаточно много и все они связаны между собой, например, из-за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.

Но, конечно же, лидером среди угроз являются вирусы. Давайте посмотрим, что такое вирусы, и какими они бывают. (Слайд 4)

☠ **Компью́терный ви́рус** — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

Классификация (Слайд 5)

В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы на следующие группы.

По поражаемым объектам (Слайд 6-11)

Файловые вирусы. Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)

Загрузочные вирусы. Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.

Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.

Макровирусы. Это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.

Вирусы, поражающие исходный код. Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а так же VCL и ActiveX компоненты.

По поражаемым операционным системам и платформам (Слайд 12-13)

- DOS
- Microsoft Windows
- Unix
- Linux

По технологиям, используемым вирусом (Слайд 14-17)

Полиморфные вирусы. Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.

Стелс-вирусы. Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)

Руткит. Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

По языку, на котором написан вирус (Слайд 18-19)

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык
- и др.

По дополнительной вредоносной функциональности (Слайд 20-24)

Бэкдоры. Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе

Шпионы. Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Ботнеты. Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

(Слайд 25-26) Каждый день появляются все новые и новые вирусы. Вам необходимо знать, что создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273).

(Слайд 27) Также в нашей стране существует доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.

4. Физкультминутка (1 мин)

Но сначала, мы немножко отдохнем и проведем физкультминутку. (Слайд 28)

Мы все вместе улыбнемся,
Подмигнем слегка друг другу,
Вправо, влево повернемся
И кивнем затем по кругу.
Все идеи победили,
Вверх взметнулись наши руки.
Груз забот с себя стряхнули
И продолжим путь науки.

Итак, как же бороться с сетевыми угрозами? (Слайд 29)

1. Установите комплексную систему защиты. (Слайд 30)

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

2. Будьте осторожны с электронной почтой (Слайд 31)

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

3. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari. (Слайд 32)

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

4. Обновляйте операционную систему Windows. (Слайд 33)

Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

5. Не отправляйте SMS-сообщения. (Слайд 34)

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

6. Пользуйтесь лицензионным ПО. (Слайд 35)

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.

Лицензионные программы избавят Вас от подобной угрозы!

7. Используйте брандмауэр. (Слайд 36)

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

8. Используйте сложные пароли. (Слайд 37)

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года.

Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

9. Делайте резервные копии. (Слайд 38)

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.

10. Функция «Родительский контроль» обезопасит вас. (Слайд 39)

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз. (Слайд 40).

5. Самостоятельная работа (7-10 мин.);

Закрепление материала - компьютерное тестирование.

А теперь, давайте проверим, насколько внимательно вы сегодня слушали данный материал.

- ✓ Займите места за компьютером.
- ✓ Загрузите программу My Test Student.
- ✓ Выберите файл «Безопасность в сети Интернет»

Тест содержит 10 вопросов, в каждом вопросе есть только один правильный ответ.

По результатам теста, вы увидите окно со своим результатам. Оценка, которую поставит вам компьютер, и будет вашей оценкой за сегодняшний урок.

Тест:

1. Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

A. Административному кодексу
B. Трудовому кодексу
C. Уголовному кодексу
D. Гражданскому кодексу

2. Какой классификации вирусов на сегодняшний день не существует?

A. По поражаемым объектам
B. По поражаемым операционным системам и платформам
C. По количеству поражаемых файлов
D. По дополнительной вредоносной функциональности

3. Какой из приведенных паролей является более надежным

A. 123456789
B. qwerty
C. annaivanova
D. 13u91A_Ivanova

4. Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:

A. Установить несколько антивирусных программ
B. Удалить все файлы, загруженные из сети Интернет
C. Своевременно обновлять антивирусные базы
D. Отключить компьютер от сети Интернет

5. Какой из браузеров считается менее безопасным, чем остальные:

A. Mozilla Firefox

B. Internet Explorer
C. Google Chrome
D. Opera

6. Какие действия не рекомендуется делать при работе с электронной почтой?

A. Отправлять электронные письма
B. Добавлять в свои электронные письма фотографии
C. Открывать вложения неизвестной электронной почты
D. Оставлять электронные письма в папке Отправленные

7. Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?

A. Отправить SMS сообщение
B. Выполнить форматирование жесткого диска
C. Перезагрузить компьютер
D. Не отправлять SMS сообщение

8. Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?

A. Трудовому кодексу РФ
B. Доктрине информационной безопасности РФ
C. Стратегии развития информационного общества РФ
D. Конвенции о правах ребенка

9. Зачем необходимо делать резервные копии?

A. Чтобы информация могла быть доступна всем желающим
B. Чтобы не потерять важную информацию
C. Чтобы можно было выполнить операцию восстановления системы
D. Чтобы была возможность распечатать документы

10. Что необходимо сделать, если на сайте в Интернет, вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?

A. Перезагрузить компьютер
B. Отформатировать жесткий диск
C. Закрыть сайт и выполнить проверку ПК
D. Выключить компьютер.

6. Итог урока (2-3 мин.);

- ✓ Выставление оценок.
- ✓ Домашнее задание.

Ребята, домашнее задние у вас будет тоже связано с нашей темой. Разделимся на группы – вы сидите за компьютерами и по номеру компьютера мы и определим, какая группа будет готовить материал:

1. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.
2. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»
3. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

Разработка урока «Безопасность в сети Интернет»

Зеленкова Алена Александровна,
учитель информатики и ИКТ
Гимназия №8 им. академика Н.Н. Боголюбова
Адрес сайта http://s8.goruno-dubna.ru/
e-mail school8@uni-dubna.ru

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

- изучить информированность пользователей о безопасной работе в сети Интернет; познакомить с правилами безопасной работы в Интернете; учить ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;
- формировать информационную культуру учащихся; умение самостоятельно находить нужную информацию пользуясь web-ресурсами;
- развивать критическое мышление;
- воспитывать дисциплинированность при работе в сети.

Учащиеся должны знать:

- перечень информационных услуг сети Интернет;
- опасности глобальной компьютерной сети.

Учащиеся должны уметь:

- работать с Web-браузером;
- пользоваться информационными ресурсами;
- искать информацию в сети Интернет;
- ответственно относиться к использованию online-технологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Программно-дидактическое обеспечение: презентация «Безопасный Интернет.pptx», видеофайлы «Дети и Интернет.flv», «Учите детей общаться.flv», тест, информационные плакаты, карточки с адресами Web-ресурсов.

Этапы урока:

1.Организация начала урока. Постановка цели урока. Просмотр видеоролика. Постановка темы и главного вопроса урока.
2.Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения учащихся).
3.Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.
4.Закрепление изученного материала. Рекомендации по правилам безопасной работы.

Тестирование.

5.Подведение итогов урока. Оценка работы группы. Просмотр видеоролика. Информация о домашнем задании.

Ход урока

1. Организация начала урока. Постановка цели урока (3 мин).

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь у вас появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И не когда-то, а прямо сейчас.

- Внимание, видеоролик!

(Просмотр видеоролика «Дети и Интернет» – 1 мин.)

- Как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет».

Главный вопрос урока: Как сделать работу в сети безопасной?

2. Изучение нового материала (18 мин).

Игра «За или против» (5 мин.).

Для начала, предлагаю поиграть в игру «За или против». Вы увидите несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

- Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
- Интернет – это глобальный рекламный ресурс. И это хорошо!
- Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.
- Интернет магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.
- В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли (8 мин.)

- Какие опасности подстерегают нас? Какие виртуальные грабли лежат у нас на пути? Посмотрим, что на это скажет Таня, которая подробно познакомилась с этой проблемой дома (сообщение учащегося по темам: «Интернет-зависимость», «Вредоносные и нежелательные программы», «Онлайновое пиратство»).

- Как уберечься от недостоверной информации? Кто такие интернет-мошенники? Расскажет Владимир (сообщение учащегося по темам: «Как уберечься от недостоверной информации?», «Материалы нежелательного содержания», «Интернет-мошенники»).

- Общение в Интернете. Какое оно? Послушаем Мариям (сообщение учащегося по теме «Преступники в Интернете», «Интернет-дневники»).

Физ. минутка «Собери рукопожатия» (2 мин.).

Участникам предлагается в течении 10 секунд пожать руки как можно большего числа других людей.

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Чем он был вызван?

Аналогия с работой в Интернет.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия?

- Ответим на главный вопрос урока – «Как сделать работу в сети безопасной?»

3. Практическая работа (7 мин.).

- Что можно? Что нельзя? К чему надо относиться осторожно?

Давайте посмотрим, что об этом можно прочитать на web-страницах и попробуем сформулировать правила безопасной работы.

- У вас на столах лежат карточки с адресами web-страниц, которые я предлагаю вам сегодня посетить. Данный ресурс добавлен в закладки браузера Opera в папку «Безопасный Интернет». Познакомьтесь с информацией ресурса и сформулируйте правила безопасной работы в сети.

Резюмируем (обсуждение найденной информации). Какие правила безопасной работы вы выбрали, посещая web-сайты?

4. Закрепление изученного материала (12 мин).

- Я тоже для вас приготовила несколько советов.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Повернись, избушка, ко мне передом, а к лесу задом!

Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет общение будет приносить пользу.

Не пей из колодца!

Даже когда мы испытываем жажду, мы не будем пить из грязной лужи. Также и в среде Интернет, случайно оказавшись в месте, которое производит отталкивающее впечатление агрессивного и замусоренного, лучше покинуть его, переборов чувство любопытства. Это защитит вас от негативных эмоций, а ваш компьютер – от вредоносного программного обеспечения.

Волку дверь не открывайте!

У интернет-мошенников ничего не получится, если только мы сами не откроем им дверь – не сообщим им наши пароли, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям.

5. Подведение итогов урока (5 мин.).

Я рада, что вы не остались равнодушны к теме безопасного интернета. Спасибо за активное участие (оценка работы группы).

Каждый год, проходит День безопасного Интернета. Его цель – способствовать безопасному и более ответственному использованию онлайн-технологий и мобильных телефонов среди детей и молодежи по всему миру. Впервые он проводился в 2004 году, и с тех пор число его участников постоянно растет. Для его проведения был образован Российский Оргкомитет, в состав которого вошли представители практически всех ведущих общественных, некоммерческих и других организаций, деятельность которых связана с развитием Интернета. В рамках проведения Дня безопасного Интернета прошел конкурс на лучший видеоролик. Ролик, занявший 1 место, вы видели в начале урока.

- В завершении нашего урока предлагаю посмотреть еще одну интересную конкурсную работу (просмотр видеоролика «Учите детей общаться.pptx» - 0, 35 сек.).

Конспект урока "Безопасный интернет"

Клокова Ольга Михайловна,
учитель Информатики и ИКТ
МБОУ «Лицей «Дубна» г.Дубны
Московской области», http://licdubna.ucoz.ru/
Адрес сайта: http://liceum-dubna.ucoz.ru/SaitInform/index.html
e-mail: olgak4371@yandex.ru

Аннотация

Статья представляет собой конспект урока "Безопасный интернет". Данный урок был проведён с учащимися 9-11 классов лицея «Дубна», в рамках всероссийского проекта проведения во всех школах страны Единого урока безопасности в сети Интернет.

При разработке и проведении урока были использованы методические материалы по проведению всероссийского урока безопасности школьников в сети Интернет, размещённые на сайте http://www.сетевичок.рф

Статья может быть полезна учителям-предметникам и классным руководителям при проведении уроков, посвящённых проблеме безопасности в Интернете.

Цель проведения занятия – повышение информационной грамотности учащихся, обеспечение ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Содержание

Введение

Современное общество и виртуальная реальность тесно связаны друг с другом. Подростки проводят большую часть времени в Интернет и не мыслят себя без него. Массу преимуществ и колоссальные возможности даёт возможность пользоваться Интернетом, но как и в реальной жизни, жизнь в киберпространстве сопряжена с целым рядом рисков.

Проблема безопасного интернета становится всё более актуальной проблемой, так как год от года возрастает количество киберпреступлений. Неслучайно, что в соответствии с решением парламентского слушания Совета Федерации от 12 марта 2014 года было принято решение о проведении во всех школах Российской Федерации 30 октября 2015 Единого урока по безопасности в сети и квест по цифровой грамотности среди детей и подростков "Сетевичок 2015"

Проблемы современной жизни в киберпространстве

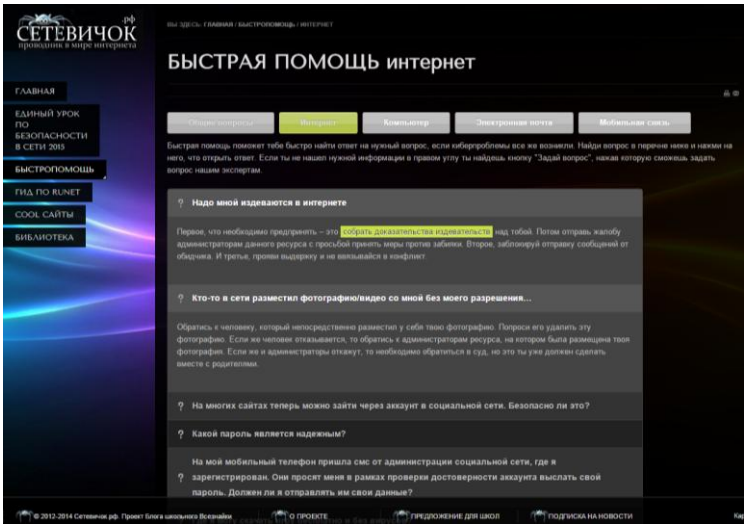
Какие опасности могут подстерегать пользователей Интернета?

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Для этого они могут использовать вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах, смс-мошенничество.

Мошенникам удаётся достичь своих целей, так как они манипулируют такими человеческими качествами как доверчивость, невнимательность и неосведомлённость. Осведомлён – значит вооружён! Надо знать о возможных действиях мошенников, быть готовым не поддаваться провокации с их стороны и в случае атаки дать отпор, действовать грамотно.

Наиболее злободневные вопросы

Множество вопросов возникает у пользователей сети Интернет, когда они сталкиваются с проблемами. И есть много ресурсов, посвящённых безопасности в сети. Наиболее часто возникающие вопросы по разрешению проблем, возникающих у подростков, разработчики сайта «Сетевичок» собрали в раздел «Быстропомощь» (http://xn--b1afankxqj2c.xn--p1ai/vopros/elektronnaya-all)



На этом ресурсе отдельно рассматриваются общие вопросы безопасности, вопросы, посвящённые Интернету, компьютеру, электронной почте и мобильной связи.

Здесь же можно задать свой вопрос, если ответ на страницах сайта не найден. Для этого существует форма обратной связи, и все операторы находятся офлайн. Можно оставить сообщение и получить ответ на него в ближайшее время.

Памятка для пользователей

Как уберечь компьютер от заражения вирусом

- Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.
- Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключайте к своему компьютеру непроверенные съемные носители.
- Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные

- Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).
- Никому не сообщайте свой пароль.

- Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.
- Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).
- Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.
- Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

Как не попасться на удочку смс-мошенников

- Не отправляйте смс на незнакомые телефонные номера, за оправку таких смс могут взимать плату.
- Переводите деньги только на известные телефонные номера.
- Не вводите телефонный номер на незнакомых сайтах.

Как избежать мошенничества при платежах

- Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.
- Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.
- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.
- Заведите отдельную карту для покупок в интернете.
- Используйте для покупок в интернете только личный компьютер.
- Регулярно обновляйте антивирусную защиту компьютера.
- Старайтесь делать покупки в известных и проверенных интернет-магазинах.
- Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.
- Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет

Пользователи должны научиться грамотно пользоваться Интернетом и электронными устройствами:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет;
- 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 доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- критически относиться к информационной продукции;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Будь внимателен! Стань грамотным потребителем цифровой эпохи!

Конспект классного часа
"Информационная безопасность детей в сети Интернет"

Комарова Ольга Владимировна,
учитель начальных классов,
«МБОУ г.Дубны Московской области,
лицей №6 имени академика Г.Н.Флёрова»

Цель:

углубить представление учащихся о влиянии **компьютера** на детей, ознакомить с признаками зависимости от компьютера, воспитывать уважение к собственному здоровью.

Ожидаемые результаты:

- формирование культуры ответственного, этичного и безопасного использования Интернета;
-повышение осведомленности детей о позитивном контенте сети Интернет, полезных возможностях глобальной сети для образования, развития, общения;
- повышение уровня осведомленности детей о проблемах безопасности при использовании детьми сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз. Опасности интернета - правда или ложь?
- разработка памяток «Свод правил поведения в сети Интернет».

Оборудование: презентация, памятки.

Ход классного часа

I. Орг. момент. Введение.

II. Просмотр социального мультфильма «Безопасный интернет»

Беседа после просмотра. Определение темы занятия, целеполагание (учащиеся класса пытаются сформулировать тему классного часа, определить цели).

Классный руководитель:

- Да, тема нашего сегодняшнего классного часа – это «**Информационная безопасность** детей в сети Интернет».Слайд1

Интернет, как и все в жизни, имеет две стороны - черную и белую. Помимо преимуществ, интернет принес определенные неудобства. Для некоторых интернет, по силе своего воздействия и привязанности, не уступает алкоголю или никотину.

Сейчас медики обсуждают вопрос, не расширить ли раздел Международной классификации болезней, а именно, болезней зависимости. Пока в него входят наркомания, алкоголизм, табакокурение. В последние годы сюда добавились врачебная зависимость и обжорство. Теперь речь идет и о виртуальной наркомании. Сегодня наряду со взрослыми все больше детей пользуются интернетом для общения, поиска информации, игр, загрузки мультимедиа.

1) Беседа:

- Что же такое информационная безопасность? (учащиеся дают свои определения).

Учитель выводит определение на 2, 3 слайд.

- Слышали ли вы когда-нибудь о понятии «безопасный интернет»?
- Учат ли вас родители on-line-этикету?

2) Учитель предлагает учащимся класса разработать памятку «Свод правил поведения в сети **Интернет**».

Учащиеся прописывает свод правил поведения в Интернете, обсуждают и фиксируют плюсы и минусы использования Интернета. слайды 4-10.

Возможные правила:

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
2. Используйте нейтральное экранное имя, не выдающее никаких личных сведений: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
3. Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
4. Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

5. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений
6. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
7. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.

Плюсы использования Интернета (слайд 11) :

- Оперативность получения любой информации;
- Общение
- Участие в международных конкурсах;
- Получения дополнительного образования;
- Обеспечение досуга;
- Формирование информационной компетентности, включающей умение работать с информацией.

Минусы использования Интернета (слайд 12):

- Беспорядочная недостоверная информация.
- Ухудшение здоровья: потеря зрения (компьютерный зрительный синдром) ; гиподинамия; искривление осанки; психические и интеллектуальные нарушения развития.
- Вредная информация (асоциальные сайты),нецензурная лексика;

III. Рефлексия. (слайды 13,14):

Учащиеся подводят итоги классного часа. Каждый ученик заканчивает предложение на выбор:
- Классный час был мне полезен, потому что…
- Я сегодня узнал…
- Теперь я буду…

Приложение.

Памятка для обучающихся начальной школы

Ты должен это знать:

- Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
- Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
- Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься и номер твоего телефона должны знать только родители и друзья.
- Никогда не отправляй свои фотографии людям, которых не знаешь лично. Компьютерный друг мог говорить о себе неправду. Ты ведь не хочешь, чтобы у незнакомого человека была твоя фотография, с которой он сможет сделать все, что захочет.
- Не встречайся с людьми, с которыми познакомился в Интернете, без родителей. Многие люди выдают себя не за тех, кем являются на самом деле.
- Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов - читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.
- Если тебя кто-то расстроил или обидел, обязательно расскажи об этом родителям.

Полезные ссылки:

1) ***http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon_ metsa.html*** – о правилах безопасного поведения в сети Интернет с элементами интерактива;
2) ***http://www.nachalka.com/node/948*** - учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;
3) ***http://content-filtering.ru/aboutus/*** - информационно-аналитический ресурс «Ваш личный Интернет».

Разработка урока «Безопасность в сети Интернет» (8-10 класс)

Моисеева Светлана Эдуардовна,
учитель математики и информатики
МБОУ «Средняя общеобразовательная школа №10
г.Дубны Московской области»,
http://school10.dubna.ru
e-mail: *shkr_68@mail.ru*

Разработка предназначена, в первую очередь, учителям информатики и классным руководителям для проведения данного урока в 8-10 классах.

Данный урок направлен на то, чтобы сделать "всемирную паутину" безопасной для детей и научить их правильно вести себя в Интернет-пространстве.

Класс: 8-10 классы

Цель урока: изучение опасных угроз сети Интернет и методы борьбы с ними; предотвращение возможных негативных последствий использования Интернета.

Задачи:

- ознакомление с возможными угрозами сети Интернет;
- приобретение навыка выявления мошеннических манипуляций над пользователем;
- выработка тактики безопасного поведения пользователя в сети;
- обучение ответственному использованию online-технологий;
- воспитание дисциплинированности при работе в сети.

Тип урока: урок изучения нового материала.

План урока:

7. Организационный момент (1-2 мин.);
8. Актуализация знаний (7 мин.);
9. Объяснение нового материала (30-35 мин.);
10. Самостоятельная работа (7-10 мин.);
11. Итог урока (2-3 мин.);

Ход урока:

7. Организационный момент, 1-2 мин.:

–сообщение темы урока (занесение темы в тетрадь), его целей и задач;

–краткий план деятельности.

8. Актуализация знаний (7-10 мин)

–Что такое Интернет?

–Какова польза от сети Интернет?

–Как вы думаете, опасен ли Интернет? Если да, то какой вред от использования Интернета?

Сегодня наш урок посвящен теме «Безопасность в сети Интернет».

Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

Рассматривая возможности Интернета, следует выделить его положительное влияние (формирование социализации, обучение решению жизненно важных проблем, предоставления выбора «виртуального» социального окружения («виртуальных» сообществ) и пр.). Но на ряду с этим, существуют риски негативного влияния: воздействие на состояние физического и психического здоровья пользователя (например, прямое влияние на зрение и опосредованное – на формирование психологической Интернет-зависимости, нарушение осанки, малоподвижный образ жизни, замкнутость поведения).

Вообще в настоящее время использование Интернета порождает гораздо больше проблем, нежели радужных перспектив.

Одна из проблем – обеспечение информационной безопасности в сети.

На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Игра «за или против».

Учитель предлагает игру «за или против». На слайде – несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!

2. Интернет – это глобальный рекламный ресурс. И это хорошо!

3. Общение в интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.

4. Интернет является мощным антидепрессантом.

5. В интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Учитель предлагает ученикам ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответы учащихся)

9. Объяснение нового материала (25-30 мин.):

А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом:

8. Вредоносные программы
9. Кража информации
10. Халатность сотрудников
11. Хакерские атаки
12. Финансовое мошенничество
13. Спам
14. Аппаратные и программные сбои

Как вы видите, угроз достаточно много и все они связаны между собой, например, из-за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.

Итак, как же бороться с сетевыми угрозами?

Опасности в сети Интернет, пути их преодоления

п/п	**Проблема**	**Способы преодоления**
	Вирусы **Компью́терный ви́рус** — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).	– Установка антивирусной программы. Сегодня актуальны так называемые «комплексные системы защиты», предназначенные для полной защиты вашего компьютера – Новые вирусы появляются ежедневно, поэтому необходимо регулярно обновлять базы сигнатур, лучше всего настроить программу на автоматическое обновление – Осуществлять веб – серфинг по проверенным сайтам – Блокировать всплывающие окна

		– Внимательно проверять доменное имя сайта – Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера. – Проверять сохраняемые файлы, скачанные в Интернете – Установить запрет открытия вложений электронной почты от неизвестных и подозрительных адресатов, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения.
	Спам, мошеннические письма	– Сообщать свой основной адрес электронной почты только хорошим знакомым – Использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки и никому их не сообщать. – Никогда не отвечать на спам, не переходить по содержащимся в нем ссылкам, не отписываться от спама и тем более не пересылать его по цепочке. – Установить программу анти-спам – Не передавать учетные данные — логины и пароли — по незащищенным каналам связи
	Фальшивые Интернет - магазины	– Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в Интернете – Не доверять объявлениям о подозрительно дешевых товарах – Старайтесь делать покупки в известных и проверенных интернет-магазинах.
	Бесплатное скачивание файлов с подпиской	– Не указывать свой мобильный номер на незнакомых сайтах. – Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.
	Безопасность при оплате картами в сети	– Заведите отдельную карту для покупок в Интернете. – Используйте для покупок в Интернете только личный компьютер. – Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных. – Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах. – Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте. – Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Опасности общения в социальных сетях

п/п	Проблема	Способы преодоления
	Проблема конфиденциальности	– Размещая информацию о себе в социальных сетях, необходимо помнить, что ее может увидеть большое количество людей, в том числе родителей, работодателей и др. В итоге, личная жизнь становится достоянием общественности.
	Взлом страницы мошенниками и злоумышленниками	– Использовать сложные логин и пароль и никому их не сообщать
	Страницы – фэйки, страницы – двойники	– Необходимо ограниченно сообщать личную информацию о себе (не указывать домашний адрес, номер телефона, номер паспорта, и др.), чтобы злоумышленники не смогли воспользоваться ею в своих целях.
	Интернет – зависимость	– Планировать время, проводимое в Интернете, и строго следовать этому, соблюдать санитарные нормы
	Зависть и агрессия	– Делиться успехами с самыми близкими: теми, кто искренне за вас порадуется.

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая несложные правила, вы сможете избежать популярных сетевых угроз. (Слайд 40).

10. Самостоятельная работа (7-10 мин.);

Тест:

1. *Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…*
   A. Административному кодексу
   B. Трудовому кодексу
   C. Уголовному кодексу
   D. Гражданскому кодексу
2. *Какой из приведенных паролей является более надежным*
   A. 123456789
   B. qwerty
   C. annaivanova
   D. 13u91A_Ivanova
3. *Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:*
   A. Установить несколько антивирусных программ
   B. Удалить все файлы, загруженные из сети Интернет
   C. Своевременно обновлять антивирусные базы
   D. Отключить компьютер от сети Интернет
4. *Какие действия не рекомендуется делать при работе с электронной почтой?*
   A. Отправлять электронные письма
   B. Добавлять в свои электронные письма фотографии
   C. Открывать вложения неизвестной электронной почты

D. Оставлять электронные письма в папке Отправленные

5. *Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?*
   A. Отправить SMS сообщение
   B. Выполнить форматирование жесткого диска
   C. Перезагрузить компьютер
   D. Не отправлять SMS сообщение
6. *Зачем необходимо делать резервные копии?*
   A. Чтобы информация могла быть доступна всем желающим
   B. Чтобы не потерять важную информацию
   C. Чтобы можно было выполнить операцию восстановления системы
   D. Чтобы была возможность распечатать документы
7. *А что для вас является "безопасным интернетом?"* _____

_____

_____

11. Итог урока (2-3 мин.):

– Выставление оценок.
– Домашнее задание.

И помните, интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – сеть тоже может быть опасна!

12. Использованы материалы:

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр «Академия», 2008. – 336 с.
2. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус
3. Социальная сеть работников образования http://nsportal.ru/
4. База образовательных ресурсов http://obrazbase.ru/inform/uroki-i-meropriyatiya
5. Интернет СМИ «ваш личный интернет» http://content-filtering.ru

Классный час по теме
"Безопасность в сети Интернет" (5 класс)

Наумов Максим Вячеславович,
учитель русского языка и литературы
МБОУ«Средняя общеобразовательная школа №9
с углубленным изучением иностранных языков
города Дубны Московской области»
e-mail:bet25@mail.ru

Цели:

Методическая: показать актуальность данной темы

Учебная: обучение информационной безопасности в Интернете

Воспитательная: развитие самоконтроля учащихся и воспитание внимательного отношения к информационным ресурсам

Задачи:

- Ознакомить учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет и научить избегать их
- Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности и освоить практические навыки работы в сети Интернет
- Отработка навыков и умений: сравнения информации, критического анализа; выделения главных мыслей и грамотного их изложение восприятия и усвоения услышанного
- Расширение кругозора учащихся
- Формирование информационной культуры

Оснащение и методическое обеспечение:

- Листы А3;
- Цветные карандаши;

1. Видеофильмы:Видеоролик о безопасности в сети Интернет, подготовленный пресс-службой Совета Федерации Федерального Собрания Российской Федерации (1:20)
http://vmeste-rf.tv/broadcastRelease/77305.do?setMobile=true
2. «Остерегайся мошенничества в Интернете» (2:52)
(https://www.youtube.com/watch?v=AMCsvZXCd9w)
3. «Развлечение и безопасность в Интернете» (2:02)
https://www.youtube.com/watch?v=3Ap1rKr0RCE
4. «Как обнаружить ложь и остаться правдивым» (2:21)
https://www.youtube.com/watch?v=5YhdS7rrxt8

Этапы урока	Деятельность учителя и учащихся
1. Организационный момент (3 мин.)	*На доске написана тема "Безопасность в сети Интернет". Оформление кабинета плакатами, отражающими тему урока.* - Здравствуйте, ребята! - Рад Вас приветствовать! Все готовы к работе? */Да!!/*
2. Постановка проблемы урока. Формулировка темы урока. (5 мин.)	- Ребята поднимите руки те, у которых дома есть компьютер, подключенный к Интернету. - Я вижу, что большинство учащихся класса пользуются Интернетом. А что же такое Интернет для детей? Это хорошо или плохо? */Ответы детей/* -Однозначно ответить на этот вопрос мы не можем. Интернет для

	нас - это огромный ресурс, в котором мы сможем найти много полезной информации, как для обучения, так и для саморазвития. Но в Интернете очень много информации, которая нацелена на категорию граждан, которые не могут еще осознать правильность выбора того или иного ресурса, и могут оказаться в различной, может даже трудной жизненной ситуации. И часто страдает самая уязвимая Интернет-аудитория – это дети! -Как вы думаете, о чем мы сегодня поговорим? */О безопасности во Всемирной сети/*
3. Решение проблемы урока. Развитие знаний. (6 мин.)	- Какая же опасность нас может подстерегать в интернете? Давайте посмотрим видеоролик и обсудим его. */Просмотр видеоролика о безопасности в сети Интернет, подготовленный пресс-службой Совета Федерации Федерального Собрания Российской Федерации/* - Что произошло с девочкой? - Как обманулась девочка? И кто ее обманул? - Нам в конце урока нужно будет ответить на главный вопрос: **Как обезопасить себя в сети Интернет? Что можно? Что нельзя? К чему надо относиться осторожно? Обо всем этом мы сегодня поговорим и сделаем выводы.**
4. Применение знаний. (15 мин)	1. **Разделение на группы и постановка проблемных вопросов** Для работы я вас разделил на три команды. Придумайте название Ваших команд! 2. **Первой команде** предлагается посмотреть видеоролик «Развлечение и безопасность в Интернете» (2:02) и подготовить ответы на вопросы Карточки 1: /Смотрим видеоролик/ **Карточка 1** - Ловушки для новичков: Как избежать риска при первом попадании в сеть? Вам необходимо описать действия человека при первом… - регистрация в социальной сети - вам первый написал незнакомый человек - на экран выскочило мигающее окно и не закрывается - случайно нажали на рекламный баннер Вам необходимо дать развернутый ответ, как поступить в данной ситуации и оформить его на листе А3, который находится у Вас на столе. 3. **Второй команде** предлагается посмотреть видеоролик «Как обнаружить ложь и остаться правдивым» и подготовить ответ на вопросы **Карточки 2:** /*Смотрим видеоролик*/ **Карточка 2:** Дайте 10 советов, чтобы обезопасить себя в сети Интернет. Свой ответ необходимо представить в виде стенгазеты. 4.**Третьей команде** предлагается посмотреть видеоролик «Остерегайся мошенничества в Интернете» (2:52) и подготовить ответы на вопросы **Карточки 3**: */Смотрим видеоролик/* **Карточка 3:** - Что такое фишинг? - Как распознать фишинг? - Признаки фишингового мошенничества. Свой ответ необходимо представить в виде стенгазеты. */Учащиеся готовят ответы/*

5. Защита работы и оценивание (15 мин)	1. Ответы на поставленные вопросы 2. Защита работ
6. Рефлексия (5 мин.)	Синквейн: основное понятие - Интернет

Внеклассное мероприятие на тему
«Единый урок кибербезопасности»

Пащенко Елена Юрьевна,
учитель начальных классов
МБОУ «Средняя общеобразовательная школа № 7
с углубленным изучением отдельных предметов
г. Дубны Московской области»

Подготовила и провела: Пащенко Елена Юрьевна
Класс:4
Дата:28.10.2015г.
Технологии:
- групповые
- игровые

Тип занятия: закрепление полученных знаний.
Вид занятия: клубный час
Форма занятия: фронтальная и индивидуальная.
Цели: создать условия для самостоятельной познавательной деятельности.
Задачи:

1. Ознакомить детей с основными угрозами, которые подстерегают пользователя в сети Интернет, объяснить правила общения в социальных сетях, в чатах и на форумах.
2. Научить детей основным правилам безопасности при использовании сети Интернет.

Оборудование:
* портативный персональный компьютер (ноутбук),
* проектор мультимедиа.
* видеоролик (рекомендован Министерство образования и науки Российской Федерации)
http://videouroki.net/view_post.php?id=376&utm_source=jc&utm_medium=email&utm_campaign=videodwl&utm_content=all&utm_term=20151011bezopasnost

Ход урока

1. **Заполнение анкеты и определение темы**

- Заполните, пожалуйста, анкету, и скажите, на какую тему мы сегодня будем говорить.

Анкета для учащихся

1. Есть ли у тебя компьютер?
а) да б) нет
2. Как часто ты занимаешься за компьютером?
а) каждый день б) один раз в неделю
в) другое (напиши свой ответ) _____
3. Если занимаешься, то сколько времени ты проводишь за компьютером в день?
а) один час б) два часа
в) другое (напиши свой ответ) _____
4. Подключен твой компьютер к Интернету?
а) да б) нет
5. Ты выходишь в Интернет
а) самостоятельно б) самостоятельно, но под контролем родителей
в) вместе с родителями
6. Стоит ли на твоем компьютере Фильтр (запрет на посещение нежелательных и опасных сайтов)?
а) да б) нет
7. Есть ли у тебя мобильный телефон?

а) да б) нет

8. Подключен ли твой мобильный телефон к Интернету?

а) да б) нет

9. Подключен ли твой мобильный телефон к безопасному (детскому) Интернету ?

а) да б) нет

10. В каких целях ты используешь Интернет?

а) поиск информации б) общение с друзьями в) игры

*г) другое (напиши свой ответ)*_____

11. Знаешь ли ты какие сайты таят опасность?

а) да б) нет

12. Сколько тебе лет?

а) до 10 лет б) 10-12 лет

12. Насколько ваши родители информированы о том, что вы делаете в интернете?

а) Очень много б) Много в)Средне г)Немного д) Нисколько

13. Какие странички в интернете у вас есть

а)В контакте б) Одноклассники в)Инстаграм г) Фейсбук

д) другое (напиши свой ответ) _____

-На какую же тему мы с вами поговорим? (Безопасность и Интернет)

2. Актуализация ранее полученных знаний.

- У каждого из нас в доме есть компьютер и интернет. И мы уже не представляем свою жизнь без них. Давайте с вами поиграем. Я буду задавать вопросы , а вы будете отвечать только **да** или **нет**. Если ваш ответ **да,** то вы поднимаете правую руку, если ваш ответ **нет**, то поднимаете левую руку. Поняли? (подняли правую руку) .

1.Помогает ли интернет в нашей жизни? (Да)

2. Дает нам интернет новые знания? (Да)

3. Можем ли мы получить эти знания на разных сайтах? (Да)

4. Все ли сайты в интернете безопасны? (Нет)

5. Можно ли использовать сеть Интернет безо всяких опасений? (Нет)

6. Может ли общение в социальных сетях принести вам какой-нибудь вред? (Да)

3. Просмотр ролика

- На все вопросы вы дали правильные ответы. Но как же можно нанести себе вред через интернет? (дают различные ответы). Посмотрим с вами ролик и узнаем, верно, ли мы сказали. Просмотр ролика http://videouroki.net/view_post.php?id=376&utm_source=jc&utm_medium=email&utm_campaign=videodwl&utm_content=all&utm_term=20151011bezopasnost

4. Обсуждение увиденного.

- Так как же можно нанести себе вред через интернет? (дают свои варианты).Вам снова понадобятся ваши руки.

- ***Компьютерные вирусы – могут вызвать поломку компьютера?(Да)***
- ***Могут ли вредоносные программы украсть вашу переписку с друзьями? (Да)***
- ***Можно ли скачивать игры с неизвестных сайтов? (Нет)***
- ***Можно ли открывать письма от неизвестного вам человека, если он предлагает перейти по определенной ссылке, чтобы посмотреть фотографии, картинки и т.д.? (Нет)***
- ***Нужно ли советоваться с родителями, если незнакомый вам человек предлагает совершить какие-либо действия (скачать игру, посмотреть видеоролик и т.д.?(Да)***

4.Составление памятки. Рефлексия.

- Сейчас поделитесь на команды. Каждая команда составит памятку для безопасной работы в интернет.(Составляют, рассказывают). Вот какая единая памятка у нас получилась.

1. Никому и никогда не разглашай свои пароли. Они – твой главный секрет. Придумай свой уникальный пароль, о котором никто не сможет догадаться. Не записывай пароли на бумажках, не храни их в открытом доступе. Не отправляй свои пароли по электронной почте.

2. При регистрации на сайтах и в социальных сетях старайся не указывать личную информацию (номер телефона, адрес места жительства, школы, место работы родителей и другое) – она может быть доступна всем, даже тем, кого ты не знаешь!

3. Старайся не размещать фото, на которых изображена твоя семья, школа, дом и другие личные данные.

4.Старайся не встречаться с теми, с кем ты знакомишься в Интернете.

5.В Интернете и социальных сетях старайся общаться только с теми, с кем ты лично знаком. Подумай и посоветуйся с родителями, прежде чем добавить незнакомого человека к себе в список «друзей».

6.Не используй веб-камеру при общении с незнакомыми людьми, помни о необходимости сохранять дистанцию с незнакомыми людьми.

7. Уважай собеседников в Интернете. Никогда и ни при каких обстоятельствах не угрожай другим, не размещай агрессивный и провокационный материал. Будь дружелюбен. Не груби.

8. Не вступай в незнакомые сообщества и не распространяй по чей-либо просьбе информационные, провокационные и агрессивно-настроенные материалы и сообщения.

9.Не ленись и перепроверяй информацию в других поисковиках или спроси у родителей.

10. Помни, что существуют сайты, непредназначенные для детей, не заходи на сайты «для тех, кто старше 18 лет», на неприличные и агрессивно настроенные сайты. Если ты попал на такой сайт по ссылке, закрой свой браузер, используя клавиши "ctrl+alt+delete".

11. Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать.

12. Если тебе показалось, что твои друзья отправляют тебе «странную» информацию или программы, переспроси у них, отправляли ли они тебе какие-либо файлы. Иногда мошенники могут действовать от имени чужих людей.

13. Не загружай файлы, программы или музыку без согласия взрослых – они могут содержать вирусы и причинят вред компьютеру.

14. Попроси родителей установить на компьютер антивирус и специальное программное обеспечение, которое будет блокировать распространение вирусов.

5. Итог

- О чем мы сегодня говорили?
- Вы узнали, что - то сегодня новое? Полученная информация станет полезной для вас?
- О чем бы вы хотели рассказать своим друзьям?

Разместите, эту памятку на своей страничке и сделайте, что бы ее могли увидеть и распространить дальше все ваши друзья.

И тогда, я уверена, кибер мошенникам будет не так просто вас обмануть!!!

«БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ».
Сценарий классного часа (7 класс).

Салтыкова Татьяна Юрьевна,
учитель русского языка и литературы
МБОУ ««Средняя общеобразовательная школа №9
с углубленным изучением иностранных языков
г. Дубны Московской области»
Собственный сайт http://artansa.jimdo.com/

Цель: расширить представления учащихся о возможностях сети Интернет и об опасностях, которые скрывает эта сеть.

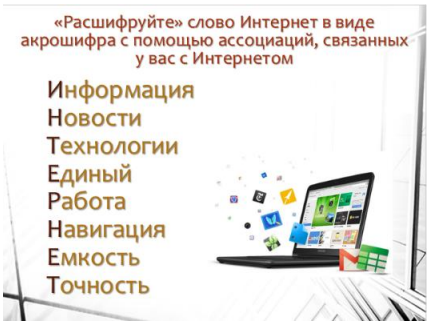
Задачи:

1. Выяснить первоначальные представления учащихся о назначении и возможностях сети Интернет.
2. Формировать культуры ответственного, этичного и безопасного использования Интернета.
3. Повысить осведомленность детей о позитивном контенте сети Интернет, полезных возможностях глобальной сети для образования, развития, общения.
4. Расширить осведомленность детей о проблемах безопасности при использовании детьми сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.
5. Совместно составить «Памятку безопасности интернет-пользователя».

Оборудование: презентация с встроенным в нее видеороликом, раздаточные карточки для персональной работы и работы в группах (см. ход занятия).

Ход занятия.

1. Экспресс-опрос.



Учитель предлагает ученикам расшифровать с помощью слов-ассоциаций понятие ИНТЕРНЕТ. Можно выполнять задание в заранее сформированных группах. В результате выполненной работы можно составить общий акрошифр и проанализировать имеющиеся представления детей о возможностях интернета.

Далее в форме беседы выясняем, знают ли ребята, как давно появился интернет и как это произошло. Напоминаем им, что изначально этот способ взаимодействия людей был создан американскими военными и для военных нужд. В декабре 1969 г. военными разработчиками была создана экспериментальная сеть APRANET, соединившая четыре узла – четыре американских университета в разных городах. За несколько лет сеть постепенно охватила все Соединённые Штаты. В 1973 г. сеть стала международной. В 1983 г. с помощью протокола TCP/IP стало возможно подключаться к Интернету с помощью телефонной линии. В конце 90-х гг. Стало возможным передавать по сети не только текстовую, но и графическую информацию, и мультимедиа. В России первая сеть появилась в 1990 г.

2. Создание проблемной ситуации.

В этом году мы отмечаем 25-летие российской сети. И сегодня абсолютное большинство наших сограждан в той или иной степени являются пользователями интернета. Многие из вас

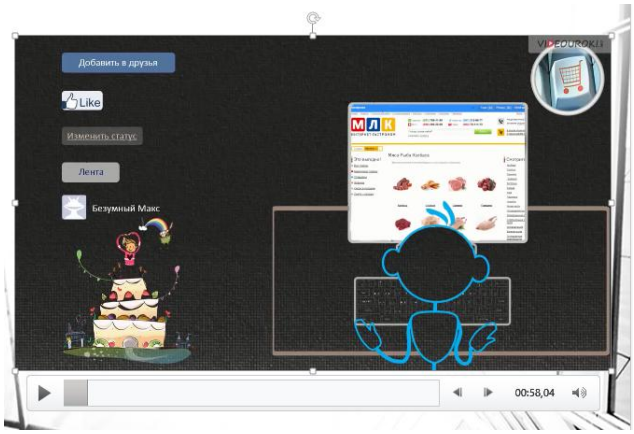
уже не представляют себе жизнь без ежедневного выхода в глобальную паутину. Давайте подумаем, какие достоинства и какие недостатки имеет сегодняшний интернет.

(Ученики работают в группах, заполняя таблицу)

Недостатки интернета	***Достоинства интернета.***

Как вариант, можно предложить разделиться на две команды: «защитников» и «нападающих». Затем выполненное задание обсуждается. Обратим внимание, где окажутся онлайн-игры, и сделаем акцент на том, что нередко игра как способ развлечься, отдохнуть от учёбы или работы становится самоцелью, забирая время, предназначенное для других жизненных процессов. Если ребята забудут про возможности онлайн-обучения, расскажем им о том, что в интернете можно не только искать информацию для докладов и презентаций, но и пользоваться всевозможными справочниками, библиотеками, онлайн-тестами и пр. Скорее всего, ребята в качестве недостатка не вспомнят о кибер-преступлениях. Напомним ученикам об этой угрозе и о других опасностях, которые таит в себе всемирная паутина. Предлагаем составить для себя личную «Памятку безопасности интернет-пользователя» и выдаем заранее подготовленную форму.

3. Просмотр видеоролика и составление «Памятки безопасности интернет-пользователя»



Во время просмотра ролика (подготовлен сайтом videouroki, длительность почти 16 мин.) ребята заполняют собственные памятки. По окончании фильма сравниваем написанное, обсуждаем каждый пункт и дополняем пропущенное.

Примерная памятка может выглядеть таким образом:

Памятка для безопасности интернет-пользователя

1. Никогда не вводи данные кредитных карт или банковских счетов.
2. Не сиди дольше 2,5 ч за компьютером.
3. Не переходи по непроверенным ссылкам.
4. Не вводи регистрационные данные на неизвестных сайтах.
5. Не вступай в общение с незнакомыми людьми.
6. Не публикуй свои личные данные, фото, номер телефона или адрес в соцсетях.

4. Рефлексия

В качестве рефлексии, осознавания полученной информации учениками и выявления их отношения к риску и «подводным течениям» интернета предложим ребятам сформулировать своё мнение по поводу трёх высказываний об интернете:

«Интернет несет читателю тонны мусора и крупинки золотого песка, и умение выбрать самое интересное становится весьма востребованным талантом». (*Марта Кетро)*

«Интернет... Он не сближает. Это скопление одиночества. Мы вроде вместе, но каждый один. Иллюзия общения, иллюзия дружбы, иллюзия жизни…» (*Януш Вишневский "Одиночество в Сети")*

«Интернет – парадокс: он сближает людей, находящихся далеко, но отдаляет от тех, которые находятся рядом». *(Из статусов в соцсетях)*

Подводя итог занятию, предложим ребятам в виде схемы изобразить те моменты, о которых они должны помнить, входя в сеть. Эта схема может выглядеть так:

В заключение учитель говорит: «Интернет, как и многие другие явления нашей жизни, безусловно, полезен, но вместе с тем он таит в себе и опасность при неумеренном, неосторожном или неграмотном использовании. Я очень надеюсь, что вы будете умеренны, осторожны и достаточно образованны в использовании безграничных возможностей всемирной паутины и не запутаетесь в её сетях, как известная героиня сказки Корнея Ивановича Чуковского».

Разработка урока «Безопасность школьников в сети Интернет» (5-8 классов)

Федосеева Марина Сергеевна,
учитель информатики
МБОУ «Гимназия №3 г. Дубны Московской области»,
http://school3.uni-dubna.ru
e-mail: meri_lin@bk.ru

Аннотация

Разработка урока для учащихся 5-8 классов «Безопасность в сети Интернет». На уроке учащиеся знакомятся с основными Интернет - угрозами, полученные знания применяют при определении Интернет - угрозы в предложенных ситуациях, решении кроссворда.

Содержание

Тема занятия: «Безопасность в сети Интернет»

Класс: 5 - 8 класс

Цель: к концу урока учащиеся узнают об основных угрозах сети Интернет и методах борьбы с ними;

Задачи:

Образовательная:

- познакомиться с понятием «Интернет», «Интернет-угроза»;
- изучить приемы безопасности при работе в сети Интернет.

Развивающая:

- формирование приёмов логического мышления;
- развитие способности анализировать и обобщать, делать выводы.

Воспитательная:

- воспитание аккуратности, точности, самостоятельности;
- привитие навыка групповой работы, сотрудничества.

Здоровьесберегающая:

- оптимальное сочетание форм и методов, применяемых на занятии.

Ход занятия:

Тема нашего урока «Безопасность в сети Интернет». (Слайд 1)

Интернет – глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов. (Слайд 2)

На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. (Слайд 3)

Однако многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)

Молодцы!

Угрозы, исходящие из сети Интернетможно разделить на онлайн и оффлайн. (Слайд №4)

Давайте начнем с первой группы угроз – онлайн угрозы. Онлайн угрозы – любые проблемы, которые опасны для вашего компьютера.

К ним, во-первых, относятся различные категории компьютерных вредителей и вирусов, которые могут просочиться на ваш компьютер во время путешествия по просторам социальных сетей. Для этого порой достаточно нажать на ссылку, содержащуюся в письме от «мнимого» друга. Например, получив письмо или найдя сообщение на стене следующего содержания: «Нашел твою фотку!» или «Ты тут неплохо получилась!», или «Смотри какой котеночек!». Заинтересовавшись содержанием письма, вы кликнетена ссылку, которая переведет вас на загадочный сайт, попутно загружающий на компьютер всевозможные зловредные программы. Среди них могут быть:

- программы-шпионы (будут отслеживать все ваши действия на компьютере, вводимую информацию с целью ее похищения).

Если вы осуществляете покупки или занимаетесь онлайн-банкингом на этом компьютере, то такие программы могут похитить пароли и логины для онлайн-банкинга и данные о вашей кредитной карточке, включая ее номер, ПИН и имя владельца);
- винлокеры(программы, которые перекрывают картинкой весь экран и предлагаю заплатить определенную сумму от 100 до 500 рублей, чтобы разблокировать ваш компьютер.Очень часто винлокеры используют картинку порнографического содержания и угрозы сообщить о вас в полицию, как любителе запрещенного порно, когда вы таковым не являетесь);
- подписка на «премиальные» номера (когда вы решите загрузить какую-либо бесплатную программу, типа сервиса для обмена мгновенными сообщениями ICQ или любую другую программу, последнее, что он будет читать, это условия соглашения при загрузке дистрибутива. А они могут зачастую содержать пункт об обязательной подписке на платные сервисы. Таким образом, вы задолжаете сайту денег, которые по закону вы будете должны вернуть);

- фи́шинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.
- попадание в базы рассылки спама (если ваш электронный адрес появится в открытом доступе, то он с легкостью может попасть к кибер-преступнику, который будет его переполнять горами спама).

Онлайн-угрозы могут также навредить вашей репутации.

- А теперь давайте перейдем к самому опасному виду угроз, который может принести ущерб не только вашему имуществу, но и жизни – это оффлайн-угроза. Она включает все то, что может случиться в реальной жизни. К ней относятся предложения о встрече от неизвестных «друзей», телефонный шантаж, мошенничество, вымогательство и даже ограбление квартиры или кража другого имущества.

Зачастую мошенникам даже не нужно ломать голову над тем, как получить заветную информацию от пользователя – он сам предоставляет ее на тарелочке. Например, при регистрации в социальной сети и составлении личного профайла предлагается внести информацию о своем годе рождение, номер телефона, адрес электронной почты, адрес проживания и работы. К сожалению, дети воспринимают такие «требования» как необходимость, и заносят личную информацию во все графы. Это первая и сама главная ошибка! Мы советуем вносить как можно меньше личной информации. Почему? Вот простой пример: ребенок в ожидании долгожданных каникул с родителями и всей семьей в какой-нибудь заморской стране каждый день обновляет свой статус: «Ура, до путешествия осталось три дня!», «Осталось два дня, не могу дождаться!», а на третий-четвертый день, после того, как дни закончились, квартиру обворовывают. Причина в том, что помимо ежедневного обновления статусов ребенок добавил в профиль домашний адрес и фотографии из квартиры, в которой мошенника, а уже и «домушника», заинтересовал интерьер и домашняя аппаратура.

И, наконец, социальные сети могут быть рассадником людей с более серьезными отклонениями. Создав поддельный профиль ребенка, и втершись в доверие к вам, они могут предложить встретиться, но на встречу уже придет взрослый человек с корыстными или «больными» планами.

Задание «О какой Интернет - угрозе идет речь?» (Слайд №5-6)

1. *Алексею на почту пришло сообщение от службы безопасности социальной сети с информацией о том, что аккаунт пытались взломать, и его владельцу необходимо перейти по ссылке в письме для того, чтобы подтвердить персональные данные. Ни на минуту не подумав о подвохе, Алексей переходит по ссылке, затем появляется стартовая страницы соцсети, куда он немедленно вносит пароль и логин. После этого с его профиля начали рассылаться письма довольно странного содержания его друзьям, вместо его фотографий на странице появились непристойные картинки.*
2. *Однажды в социальной сети девочке пришло сообщение от организаторов конкурса красоты, в котором они предложили ей принять участие. Для участия нужно было отправить несколько фотографий в купальнике, для того чтобы оценить природную красоту будущей конкурсантки. Еще одним условием участия в конкурсе была необходимость перечислить определенную сумму на счет организации в качестве вступительного взноса, после оплаты которого, они свяжутся с девушкой по поводу дополнительной информации о конкурсе, а также времени и месте его проведения.*

Как вы видите, угроз достаточно много и все они связаны между собой, например, из-за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.

- Сейчас я расскажу вам о том, как обезопасить себя и свой компьютер от сетевых угроз.

Но сначала, мы немножко отдохнем и проведем физкультминутку.

Итак, как же бороться с сетевыми угрозами? Приложение 1

А сейчас я предлагаю вам отгадать небольшой кроссворд. Приложение 2

Итог занятия

- Что нового вы узнали?

Приложение 1

Правила безопасности при использовании социальных сетей

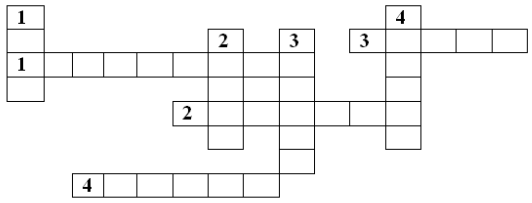
1. Установите комплексную систему защиты.
   Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.
2. Пользуйтесь браузерами MozillaFirefox, GoogleChrome и AppleSafari.
   Большинство червей и вредоносных скриптов ориентированы под InternetExplorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.
3. Не отправляйте SMS-сообщения.
   Очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправкиSMS.
   При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.
4. Используйте сложные пароли.

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

5. Старайтесь не использовать функцию запоминания паролей, которую предлагают многие почтовые ящики и социальные сети.
6. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях .
7. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
8. При регистрации на сайтах, старайтесь не указывать личную информацию
9. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.
10. Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки. Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
11. Не добавляйте в друзья в социальных сетях всех подряд.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз.

Приложение 2



По вертикали:

1. Массовая почтовая рассылка без согласия получателей
2. Личная информация о пользователе
3. Указатель перехода на одну из страниц сайта
4. Вид интернет - мошенничества

По горизонтали:

1. Программа, которая осуществляет защиту компьютера от вирусов
2. Интернет-угроза
3. Вредоносное программное обеспечение
4. Секретный набор символов, который защищает вашу учетную запись

Использованы материалы:

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр «Академия», 2010. – 336 с.
2. Безопасный компьютер и Интернет для детей: новая программа повышения квалификации преподавателей АПКиППРО //Microsoft в образовании. — [Электронный ресурс]. — Электрон.. 2010 – Режим доступа: http://www.ms-education.ru.

Разработка внеклассного занятия «Я имею право на безопасный Интернет» (1-4 классы)

Федосеева Марина Сергеевна,
учитель информатики
МБОУ «Гимназия №3 г. Дубны Московской области»,
http://school3.uni-dubna.ru
e-mail: meri_lin@bk.ru

Аннотация

Разработка внеклассного занятия для учащихся 1-4 классов «Я имею право на безопасный Интернет». На внеклассном занятии учащиеся знакомятся с основными Интернет – угрозами.

Содержание

Тема занятия: «Я имею право на безопасный Интернет»

Класс: 1 - 4 класс

Цель: познакомить учащихся с понятиями «интернет», «сеть».

Задачи:

- ✓ сформировать понятия «интернет», «всемирная паутина»
- ✓ познакомить с основными правилами безопасного пользования Интернетом
- ✓ развивать наглядно-образное мышление, память, внимание, познавательный интерес
- ✓ воспитывать информационную культуру

Ход занятия

- Ребята, как вы проводите свободное время дома? Чем любите заниматься?
- А кто знает где используют компьютер?
- А где мы берем информацию, игры… на наш компьютер?
- Как вы думаете, о чем сегодня будет идти речь на уроке?
- Сетевая паутина оплела весь белый свет, не пройти детишкам мимо. Что же это? (*Интернет*).
- Ребята, что такое интернет?

Ролик «Безопасный Интернет – детям!»

- Интернет давно стал неотъемлемой частью жизни современного человека. Все чаще от окружающих можно услышать: «Не знаю, посмотрю в интернете» или «Отправь мне по интернету». Что же такое интернет?

Интернет обширная информационная система, которая стала наиболее важным изобретением в истории человечества. Хотя сеть интернет построена на основе компьютеров, программ и линий связи, в действительности она представляет собой системувзаимодействия людей и информации.

Интернет - это всемирная электронная сеть информации, которая соединяет всех владельцев компьютеров, подключенных к этой сети. Сеть Интернет представляет собой информационную систему связи общего назначения. Получив доступ к сети, можно сделать многое.

При помощи Интернета можно связаться с человеком, который находится, например, в Австралии или Америке. Если компьютер вашего друга подключен к Интернету, вы можете переписываться с ним при помощи электронной почты, общаться с ним в «чатах» и даже видеть своего собеседника.

В Интернете собрана информация со всего мира. Там можно отыскать словари, энциклопедии, газеты, произведения писателей, музыку. Можно посмотреть фильмы, теле - и радиопередачи, найти массу программ для своего компьютера.

Что касается Интернета, то кроме чатов там есть форумы, где обсуждаются серьезные вопросы и где можно высказать свою точку зрения. Так что Интернет дает очень большие возможности для самоутверждения, самовыражения.

Физкультминутка

- Но интернет приносит не только пользу, но и таит в своей «паутине» много опасностей!

Интернет бывает разным:
Другом верным иль опасным.
И зависит это все
От тебя лишь одного.

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

-Какие же опасности таит в себе интернет?

Ролик «Безопасный и полезный Интернет»

- А сейчас расскажите соседу по парте правила работы за компьютером.
- Продолжите фразу:

Сегодня на уроке я узнал…

Я запомнил такие правила работы за компьютером…

Вы очень хорошо сегодня поработали на уроке и я приготовила для ваших родителей памятки о безопасности ребенка в интернете. Передайте их своим родителям и вместе с ними соблюдайте эти правила.

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

Литература

1. Журнал «Основа. Информатика» №1 2014г.
2. .http://сетевичок.рф

ПАМЯТКА.

ВИРТУАЛЬНЫЕ МОШЕННИКИ И ДРУГИЕ ИНТЕРНЕТ-ПРЕСТУПНИКИ

Интернет — такое же общественное место, как и улица (только виртуальное), поэтому:

1. Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в интернете.
2. Никогда не высылай свои фотографии без родительского разрешения. Их могут использовать против тебя или твоих родных.
3. Если ты хочешь поучаствовать в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
4. Никогда не соглашайся прийти в гости к человеку, с которым ты познакомился в интернете.

Интернет-этика. Киберхулиганы и грубияны в интернете

На самых разных сайтах, форумах и чатах ты можешь столкнуться с людьми, которые ради собственного развлечения могут обидеть тебя или прислать неприятную картинку, поэтому:

1. Помни: ты не виноват, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей — просто прекрати общение.
2. Если тебе угрожают по интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз — испугать тебя и обидеть. К таким поступкам взрослыми предусмотрены специальные меры.
3. Никогда не общайся с людьми, которые обижают других.
4. Всегда советуйся с родителями или взрослыми во всех указанных случаях.

Вкладка. Журнал «Информатика. Всё для учителя!»

ПАМЯТКА.

В СЕТИ НУЖНО БЫТЬ ОТВЕТСТВЕННЫМ И ВНИМАТЕЛЬНЫМ

Рекомендации по безопасности

- Работайте в интернете с ограниченными правами пользователя.
- Не сохраняйте пароли на компьютере.
- Внимательно читайте, прежде чем заполнять формы на сайтах.
- Не публикуйте свой номер телефона и адрес в социальных сетях, чатах.
- Не размещайте в интернете информацию, которую вы не хотите видеть публичной.
- Выработайте стратегию поведения в интернете, снижающую риски.

Относитесь к другим так, как хотите, чтобы относились к вам

- Никогда не отправляйтесь на личную встречу с «другом» из интернета.
- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).
- Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в Сети чей-либо адрес e-mail, фото, адрес проживания без разрешения владельца. Вместо этого можно использовать опцию *Отправить* по электронной почте. Не используйте без разрешения чужой пароль.
- Доверяйте своей интуиции. То, что размещено в интернете, не всегда правда.
- Учитесь отличать надёжные источники информации от ненадёжных и проверять информацию, которую находите в интернете.

По материалам сайта http://www.detkityumen.ru/

Единый урок по безопасности в сети Интернет

Цыброва Ирина Александровна,
учитель информатики
МБОУ «Гуманитарно-эстетическая гимназия №11
г. Дубны Московской области»,
school11@uni-dubna.ru
e-mail: iraalex81@mail/ru

Аннотация

Предлагаемый конспект урока посвящен безопасности в сети Интернет. В данной статье рассматриваются некоторые опасности в сети Интернет и методы их защиты.

Конспект урока адресован, в первую очередь, классным руководителям, учителям-предметникам и педагогам дополнительного образования, занимающими формированием информационно-коммуникационной культуры у детей и подростков, а также может быть полезна широкому кругу читателей, заинтересованному в воспитании подрастающего поколения.

Ключевые слова: безопасность, компьютерный вирус, методы защиты, сети, мобильный телефон, социальные сети, кибербуллинг, игры.

Форма проведения: урок с применением ИКТ.

Цель: формирование информационно-коммуникативной компетенции.

Оборудование: мультимедийный проектор, компьютер, карточки с заданиями.

Ход урока:

Организационный момент

- Здравствуйте, ребята! Сегодня наш урок посвящён безопасности. Безопасность нужна всегда и везде. Мы соблюдаем правила безопасности на улице, в школе, в транспорте и т.д., но важно соблюдать несложные правила при работе с компьютером, а именно в сети Интернет. Вот об этом и поразмышляем!

Вводная беседа

- С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы.

Опрос: Какие компьютерные угрозы Вы встречали в своём личном опыте или знаете о них? *(школьники делятся своим опытом)*

- Итак, давайте разбираться далее.

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ (*раздача карточек-памяток)*

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Постоянно устанавливай цифровые заплатки, которые автоматически устанавливаются с целью доработки программы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Работа с памятками *(кто из ребят применял данные методы в своей практике)*

Сети Wi-Fi

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-Fi: (*раздача карточек-памяток)*

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- Используй и обновляй антивирусные программы. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
- Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- Ипользуй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Физпауза

- Выполняем движения по моей команде со словом «безопасно», если я говорю «вирус» - движение выполнять не нужно! Итак, руки вверх – безопасно, руки на плечи – безопасно, руки вниз – вирус и т.д.

- Продолжаем нашу беседу:

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Опрос: в каких социальных сетях вы зарегистрированы? Чем они вас привлекают? Что полезного вы находите в них?

Основные советы по безопасности в социальных сетях: (*раздача карточек-памяток)*

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификации пользователя является обязательной.

Основные советы по безопасной работе с электронными деньгами: (*раздача карточек-памяток)*

- Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
- Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
- Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;
- Не вводи свои личные данные на сайтах, которым не доверяешь.

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом: (*раздача карточек-памяток)*

- Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
- Управляй своей киберрепутацией;
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
- Соблюдай свой виртуальную честь смолоду;
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
- Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Основные советы для безопасности мобильного телефона: (*раздача карточек-памяток)*

- Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Необходимо обновлять операционную систему твоего смартфона;
- Используй антивирусные программы для мобильных телефонов;
- Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

- После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
- Периодически проверяй какие платные услуги активированы на твоем номере;
- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Основные советы по безопасности твоего игрового аккаунта: (*раздача карточек-памяток)*

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
- Не указывай личную информацию в профайле игры;
- Уважай других участников по игре;
- Не устанавливай неофициальные патчи и моды;
- Используй сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Цифровая репутация

(опросить ребят о их осведомлённости в этом вопросе, нужно ли беречь свою репутацию, зачем это нужно, как это сделать?)

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в

сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации: (*раздача карточек-памяток)*

- Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
- Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Рефлексия

- Какие вы знаете компьютерные угрозы?
- Что такое цифровая репутация и как её сберечь?
- Как пользоваться электронными деньгами и стоит ли это делать вообще?
- Как вы себя теперь будете вести в социальных сетях?
- Стоит ли вступать в бой-противостояние с кибер-хулиганами?

Итог урока

- Сегодня мы попытались разобраться в тех угрозах, которые несёт нам Интернет, а также выявили основные правила безопасности, которые соблюдать в будущем вам будет совсем несложно. Памятки помогут вам в этом. Кроме того, Сетевичок.рф – твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. Также вам будет полезен «Блог школьного Всезнайки» http://www.e-parta.ru - информационно-познавательный портал для подростков. Желаю насыщенной, интересной, а главное, безопасной деятельности в сети Интернет.

Использованные интернет-ресурсы:

1. http://сетевичок.рф/dlya-shkol
2. http://www.ligainternet.ru/
3. http://www.e-parta.ru/

Конспект внеклассного мероприятия на тему «Урок кибер – безопасности в Интернете»

Чуринова Марина Борисовна,
учитель начальных классов
МБОУ «Средняя общеобразовательная школа № 7
с углубленным изучением отдельных предметов
г. Дубны Московской области»

Подготовила и провела: Чуринова М.Б
Класс: 4
Цель урока:
Создание условий для обеспечения информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.
Задачи:

8. Ознакомить детей с основными угрозами, которые подстерегают пользователя в сети Интернет, объяснить правила общения в социальных сетях, в чатах и на форумах.
9. Научить детей основным правилам безопасности при использовании сети Интернет.

Оборудование:
* портативный персональный компьютер (ноутбук),
* проектор мультимедиа.
* видеоролик(рекомендован Министерство образования и науки Российской Федерации)
http://videouroki.net/view_post.php?id=376&utm_source=jc&utm_medium=email&utm_campaign=videodwl&utm_content=all&utm_term=20151011bezopasnost
Комбинированный урок:

- беседа;
- видеофильм;
- игра;
- презентация материалов;
- дискуссия

Ход занятия

1.**Мотивационная беседа**
Откуда люди могут получать информацию?
Один мудрец давал совет:
«Полезно наблюдать,
Все впечатления копить, -
И будешь много знать».
- Сегодня на мы последуем совету мудреца, познакомимся с правилами работы в Интернете.

2.**Проблемная ситуация**
Как вы считаете, Интернет – наш друг или враг? Давайте обсудим:
- **Игра «Что такое хорошо и что такое плохо».**
(Одна группа детей указывает положительные стороны Интернета, другая - отрицательные стороны.)
- Интернет помогает нам общаться, узнавать новое, делать покупки, заключать сделки, но он может быть опасным.

3. **Видео – урок « Полезный и безопасный Интернет»**

Основные правила безопасного использования сети Интернет вспомним вместе с Интернешкой и Митясиком.
(Просмотр видео-урока)
http://videouroki.net/view_post.php?id=376&utm_source=jc&utm_medium=email&utm_campaign=videodwl&utm_content=all&utm_term=20151011bezopasnost
Прежде, чем «пойти гулять» по просторам Интернета вспомните правила!

4. **Викторина «Безопасность в Интернете» (Презентация)**

Что такое «сетевой этикет»?	Правила поведения на уроке. Правила дорожного движения. Правила поведения в Интернете.
Что запрещено в Интернете?	Играть в игры Запугивать других пользователей. Общаться с друзьями.
Как распространяются компьютерные вирусы?	Через мышку. Посредством электронной почты. Через клавиатуру.
Всегда ли можно быть уверенным, что электронное письмо получено от указанного отправителя?	Нет, потому что данные отправителя легко подделать. Да. Да, если отправитель вам знаком.
Зачем нужен брандмауэр?	Он защищает компьютер от вирусов. Обеспечивает защиту важных документов, хранящихся в компьютере. Не даёт незнакомцам проникнуть в компьютер и просматривать файлы и документы.
Что надо сделать, если на экране компьютера появилось непонятное сообщение?	За советом обратиться к родителям, к учителю Нажать кнопку «ОК» или «Да». Никогда больше не пользоваться Интернетом.
В ящик входящей почты пришло «письмо счастья». Вас просят переслать его пяти друзьям. Как правильно поступить?	Переслать всем друзьям. Переслать только пяти друзьям. Не пересылать никому.
В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой домашний адрес и номер телефона?	Когда кто-то об этом просит. Сообщать с осторожностью людям, которым вы доверяете. Во всех случаях.

5. Итоги занятия.
- О чем же мы говорили? К какому выводы пришли?
- Помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями, но, как и реальный мир, Сеть таит опасности. Учитесь их избегать. О том, что вы узнали на уроке, обязательно расскажите друзьям и родителям.

Ролевая интерактивная игра
"Социальные сети: за и против" (9 класс)

Щецова Ольга Владимировна,
учитель информатики
«МБОУ г.Дубны Московской области
лицей №6 имени академика Г.Н.Флёрова»

Тема: «Социальные сети: за и против»
Класс: 9
Цели:
1. Формирование у подростков навыков адекватного общения в социальных сетях.
2. Развитие навыков аргументировано доказывать свою точку зрения; развитие умения безопасного использования сети Интернет, развитие коммуникативных качеств.
3. Воспитание активной позиции у обучающихся.
Форма проведения: ролевая интерактивная игра
Технологии: интерактивное общение, ИКТ-технологии, технология диалогового общения.
Оборудование: экран, проектор, ноутбук, колонки; стулья по количеству участников; бейджики с указанием имен участников; аудитория, оформленная по типу ТВ-студии.

Предварительная анкета:
1 Как вы относитесь к социальным сетям?
2 В каких социальных сетях вы состоите?
3 Сколько времени в день вы уделяете социальным сетям?
4 Сколько у вас друзей в социальных сетях?
5 Вы их всех лично знаете?
6 Влияют ли социальные сети на вашу жизнь?
7 Развивает ли вас как-либо общение в социальных сетях?
8 Вы за социальные сети?
Три однозначных плюса социальных сетей.
Три однозначных минуса социальных сетей.

Ход мероприятия:

Звучит музыка. Входит ведущий.
Эпиграф: Мы знаем - время растяжимо. Оно зависит от того, какого рода содержимым вы наполняете его.
Н.Заболоцкий
Ведущий: Добрый день! Я рада приветствовать вас на ток-шоу. Тема программы «Социальные сети: за и против».
Ведущий: На сегодняшний день Интернет – это самый колоссальный источник информации, который знало человечество. Но его возможности, такие, как оперативность, быстрота и доступность связи между пользователями на дальних и близких расстояниях, позволяют использовать интернет не только как инструмент для познания, но и как инструмент для общения.
Видеофрагмент (ты знаешь, что такое социальные сети? ты зарегистрирован в социальных сетях? для чего?)
Ведущий: В наши дни дети впервые заходят в Интернет, едва научившись ходить, а страницы в социальных сетях они создают раньше, чем идут в школу. К сожалению, является фактом, что научиться пользоваться гаджетами детям легче, чем развить физиологические навыки. По данным ученых, среди детей от 2 до 5 лет только каждый 10-й умеет завязывать шнурки, в то время, как каждый 5-й сможет запустить приложение в смартфоне.

Ведущий: Наш корреспонденты готов вам представить данные мировой статистики. Попросим _____ их озвучить.

Корреспондент: По статистике: в 2011 году около 96% населения планеты имели доступ к социальным сетям с помощью разных средств коммуникации
Для того чтобы получить 50 миллионов пользователей:
– радио понадобилось 38 лет
– телевидению – 13 лет
– Интернету – 4 года
– iPod – 3 года
– facebook – более 200 млн. пользователей меньше, чем за год
– Вконтакте – более 100 млн. пользователей за 1 месяц;
Наибольшее время в социальных сетях проводят пользователи из России – в среднем 9,8 часов в месяц, что вдвое больше мирового показателя, равного 4,5 часам.
Ведущий: Социальные сети настолько многогранны, что каждый находит в них что-то нужное и ненужное, интересное и бесполезное. В социальных сетях есть свои + и свои -.
Именно об этом мы и поговорим.
Ведущий: Что же о социальных сетях думаете вы? Давайте посмотрим результаты анкетирования обучающихся вашего класса.
(результаты диагностики на экране)
Но всё ли так прекрасно, как хотелось бы?
«ЗА»
Ведущий: Приглашаем в студию нашего первого гостя _____
1. Как вы относитесь к социальным сетям? (положительно)
2. В каких социальных сетях вы зарегистрированы? (Одноклассники, Вконтакте)
3. Влияют ли социальные сети на вашу жизнь? (конечно, у меня есть возможность быстро получать нужную информацию. Например, узнать у одноклассников домашнее задание, если я забыл записать его в школе).
4. Что бы вы предпочли общение в социальных сетях или реальное? Почему? (я застенчивый человек, поэтому общаться виртуально с друзьями мне легче, в то же время есть возможность просматривать фотографии, просмотр видеофильмов, прослушивание музыки)
«ПРОТИВ»
Ведущий: Мама _____ тоже пришла сегодня к нам.
Встречайте _____
1. Как вы относитесь к тому, что свое свободное время ваша дочь (сын) проводит в социальных сетях? (против)
2. Почему? (потеря времени, вред здоровью, размещение личной информации, которая может быть использована в преступных целях, открытый доступ к негативной информации).
3. Знаете ли вы, с кем общается виртуально ваша дочь? (да знаю, я постоянно интересуюсь ее жизнью).
4. Как вы контролируете ее? (ограничиваю время, прошу показать друзей на страничке…)
Ведущий: А что думают по этому поводу зрители? Кто хочет высказать свое мнение?
Ведущий: Я предлагаю двум гостям нашей студии подойти к доске и написать в колонку одному положительные особенности виртуального общения, другому – отрицательные.
Ведущий: Я обращаюсь к психологу в нашей студии _____
Ведущий: Почему на ваш взгляд, так велика популярность социальных сетей среди подростков?
Психолог 1:
Развитие ребенка в подростковом возрасте характеризуется сложными поведенческими проявлениями, вызванными противоречиями между потребностью в признании их взрослыми со стороны окружающих и собственной неуверенностью в этом; характеризуется стремлением подростка к общению со сверстниками. Для детей Интернет в первую очередь не источник информации, как для взрослых, а средство общения. Социальная сеть - дает много

возможностей для самораскрытия, саморекламы, самопрезентации.
Ведущий: Насколько сильно влияние социальных сетей на психику человека?
Прошу ответить вас _____
Психолог 2:
Согласно недавнему исследованию ряда ученых влияние крупнейших социальных сетей в мире с каждым годом все более усиливается. Выражается не столько в количестве людей, которые в них состоят, сколько в проценте людей, которые сегодня уже не могут без них прожить.
В том случае, когда по различным причинам доступ в социальную сеть на некоторый промежуток времени такому человеку будет отрезан, он начинает нервничать из-за невозможности проверки последних обновлений. При этом организм человека испытывает достаточно сильный продолжающийся психологический стресс, что в короткие сроки приводит к повышению раздражительности и агрессии.
Пока работают ребята у доски, интерактивный опрос зрителей.
Тест. «Интернет –омут»
1. Ты являешься пользователем социальных сетей, форумов, чатов?
2. Ты испытываешь недостаток реального общения?
3. У тебя более 50 друзей в Интернете?
4. Ты добавляешь в друзья незнакомых людей?
5. Ты играешь в онлайн игры с незнакомыми людьми?
6. Ты общаешься в Интернете со своими одноклассниками, соседями и реальными друзьями?
Вывод: если у тебя, хотя бы 3 положительных ответа, значит, ты можешь попасться на удочку Интернет-дружбы.
Ведущий: Мы получили достаточное количество положительных ответов, но и не меньше отрицательных. Чем больше будет развиваться цивилизация, тем способы общения между людьми тоже будут усовершенствоваться. Человечество всегда находится в поиске новых форм общения….
У каждого есть своя точка зрения и право ее высказать... В этом и заключается, по моему мнению, само существо интернета: у каждого свое мнение, свои интересы, свои потребности, каждый действует согласно своим убеждениям.
Всего доброго. Оставайтесь с нами.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Методические разработки педагогов образовательных учреждений г.Дубны Московской области в рамках проведения всероссийского урока кибербезопасности «Безопасный интернет. Уроки кибербезопасности в школе», Дубна, 2015, 77 с.

Муниципальное бюджетное учреждение
«Центр развития образования города Дубны Московской области»

141980, г. Дубна, Московская область, ул. Мира, д.1.
Тел.: 8 (496) 214-02-50