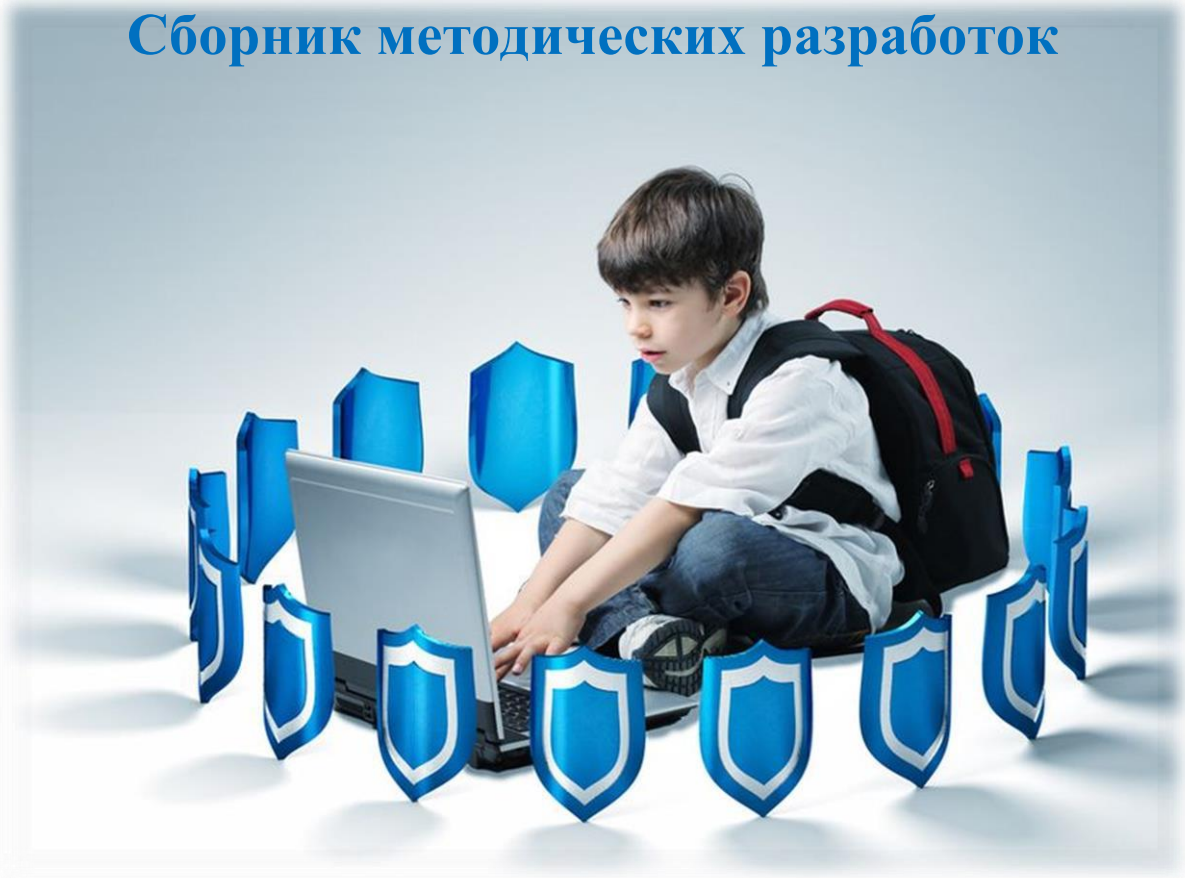
УРОКИ КИБЕРБЕЗОПАСНОСТИ В ШКОЛЕ

(КИБЕРуроки)

Сборник методических разработок



20223.

Уроки безопасности в школе (КИБЕРуроки). Сборник методических разработок

Методические разработки адресованы администрации общеобразовательных учреждений, специалистам, педагогам, классным руководителям для проведения уроков, классных часов по вопросам кибербезопасности. Методические разработки уроков представлены для учащихся в каждой возрастной категории, в том числе для детей с ограниченными возможностями здоровья.

Материалы опубликованы на сайте Муниципального бюджетного учреждения «Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

ОГЛАВЛЕНИЕ

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ С ОВЗ		
78	Киберурок «Информационная безопасность детей с ОВЗ в сети Интернет"	400
79	Киберурок: «Безопасный Интернет. Путешествие с котом Жориком».	403
80	Киберурок: «Предупреждение интернет-зависимости» (для 5-9 класса)	415

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 1-Х КЛАССОВ

1. КИБЕРУРОК

«Как Ваня понял, что онлайн-игра до добра не доведет» Цель: обучение детей правильно оценивать свои и чужие поступки.

Задачи:

1. повысить уровень знаний учащихся о возможностях использования сети Интернет: получение интересной и полезной информации, общение и коммуникация.
2. повысить уровень знаний учащихся об основных опасностях при использовании сети интернет.
3. усвоение детьми правил безопасного использования интернета.
4. повысить уровень осведомленности о возможностях решения неприятных и опасных ситуаций, возникающих в интернете.
5. сформировать систему действий и способов принятия решения при столкновении с неприятными и опасными ситуациями **Ход киберурока:**

Чтение и обсуждение истории

Учитель: Здравствуйте, ребята. Послушайте сказку «Как Ваня понял, что онлайн-игра до добра не доведет» и подумайте, о чем мы сегодня будем говорить на занятии. **Учитель рассказывает историю.**

Сегодня я расскажу вам историю про мальчика Ваню, который очень любил играть в онлайн-игры.

"И зачем вы только этот планшет ему купили! Ещё больше играть будет!", — возмущалась бабушка.

"Планшеты сейчас у каждого ребёнка сейчас есть, и ничего…", — возражал папа.

"А в телефоне всё мелкое, со своими игрушками он зрение испортит!", — добавляла мама.

Бабушка только вздыхала и уходила на кухню. Вначале Ваня играл в игры нечасто, учил уроки, помогал прибираться по дому. Но потом в его любимой игре начался сезон турниров. Вот тут и началось самое интересное! "Ваня, а ты слышал, что скоро в нашей игре турнир будет?", — возбуждённо крикнул Павлик, подбежав к другу.

"Нет, а что такое турнир?" . "Ну ты и тундра!", — удивился Павлик. "Это чемпионат, здесь можно стать мега крутым бойцом!"

" Эх, у меня, наверно, не получится поучаствовать. Не разрешит мне мамка столько играть! А долго надо играть?", — с интересом спросил Ваня.

"Не меньше пяти часов! Дня два будут состязания идти. Надо во всех битвах победить. А это трудно: знаешь, какие там бойцы!", - заявил Павлик.

Ваня пришёл домой с мыслями только об одном: что бы такое придумать, чтоб ему разрешили турнир этот пройти. Ваня даже обещания маме и папе заготовил: хорошо учиться, прибираться в комнате, всегда помогать и всё такое.

Дома была только бабушка. Тётя приболела, и родители уехали её проведать. Два дня их не будет! Ваня был счастлив: бабушка не такая строгая, как мама и папа. Уж теперь турнир точно будет его!

После вкусного обеда Петя вымыл за собой тарелку и, заглядывая бабушке в глаза, тихо спросил: "Бабуля, можно?"

"Что можно?", - спросила бабушка. Ваня отвечал: "Ну, поиграть немного на планшете… У меня турнир сегодня". "Ну, если турнир, то конечно! Но только немного", - улыбнулась бабушка. "Конечно, конечно!", — Ваня, схватив планшет, удобно устроился на диване.

Игра захватила мальчика, он ничего вокруг не видел и не слышал. Битва была сложной. Он осилил только троих бойцов и начал игру сначала, а в дверях детской уже появилась бабушка: "Ванечка, ты же просил немного, а уже целый час прошёл! Ну всё, заканчивай!"

"Бабуля, милая, ну минуточку, последний бой!" - попросил Ваня.

"Пять минут, Ваня, пять минут!" - ответила бабушка.

Но через пять минут Петя даже и не подумал убрать планшет. Он снова проиграл бой и очень разозлился: он хотел стать победителем, но увы не получалось.

И когда бабушка снова заглянула в комнату, мальчик сделал вид, что не слышит её замечания. Да, он знал, что бабушка обидится, но он потом извинится, а сейчас битва — вот самое главное! Бабушка заходила несколько раз, но Ваня или молчал, или просто махал рукой: некогда мне.

В конце концов бабушка не выдержала и спросила:"Ваня, я устала тебе говорить, что пора прекращать свою игру! У тебя уже глаза квадратные! Ты меня слышишь?"

Мальчик молчал. Ваня…

"Да, отстань, ты от меня! «Ваня, Ваня»…"Да как ты разговариваешь со мной", — дрожащим голосом заговорила бабушка.

"Как хочу, так и разговариваю! Это моя квартира, и я здесь хозяин! Не нравится — уходи!", — последние слова мальчик громко выкрикнул, а потом вскочил с дивана и захлопнул дверь своей комнаты перед лицом бабушки.

Он думал, что сейчас бабушка зайдёт его снова ругать, но услышал только тихие шаги за дверью. "Наверно, на кухню пошла, — подумал он, — вот и хорошо. Я как раз доиграю, а потом извинюсь. А сейчас не до этого: битва есть битва!"

Петя весь ушёл в игру. Сколько прошло времени — он не знал. Турнир все ещё не заканчивался, а у планшета села батарея. Мальчик вспомнил, что оставил зарядное устройство в большой комнате.

"Ну и ладно, — сказал сам себе Петя, — схожу за зарядным устройством, зайду на кухню к бабушке, извинюсь и продолжу!"

Петя потянулся: все мышцы из-за того, что он долго сидел в одной позе, затекли. Он открыл дверь своей комнаты и удивился: в коридоре были другие обои, да и всё было по-другому.

"Бабуля здесь за пару часов всё переклеила что ли?", — удивился Иван.

Но когда мальчик вошёл на кухню, то никакой бабушки не было. А была только девочка лет восьми. Она сидела за столом и за обе щёки уплетала конфеты.

"Ты кто?". — спросил Петя.

"Оля", — сказала девочка, — а вы, дядя, наверно, водопроводчик? "Какой водопроводчик? Да и какой я тебе дядя, я тебя только на пару лет старше!",- ответил Ваня.

"Ха-ха! Ну вы и шутник! Я что, похожа на бабушку?". — весело рассмеялась девочка.

"Хватит мне морочить голову, — Ваня разозлился, — ты кто такая, и где моя бабушка?"

"Какая бабушка?". — поинтересовалась девочка.

"Инга Андреевна— моя бабушка! Ты мне объясни, ты как сюда попала, тебя бабушка впустила?", - спросил удивленно Ваня.

"Я здесь живу!". — девочка обиженно поджала губки. Затем, что-то припоминая, добавила: "Инга Андреевна, — где-то я это слышала… А, вспомнила! Мне папа рассказывал. Это моя прабабушка. Он ещё говорил, что она пропала до его рождения. Внук её старший обидел. Он так заигрался на планшете в игру, что никого не видел и не слышал. Его родители — мои бабушка и дедушка — пытались его привести в чувства, врачей вызывали, но всё бесполезно. Даже новую болезнь открыли — «зомбикомп» называется. С тех пор к этому мальчику, а он, кстати, мой дядя, перестали заходить. Врач сказал, что ему даже еда не нужна, ведь он переселился в виртуальный мир. На двери его комнаты даже табличку повесили: «Не входить!».

Ваня пришёл в ужас:

"А бабушка, куда она пропала?". - спросил Ваня.
"Никто не видел её с того вечера. Стоп, а вы не из той комнаты с табличкой? Вы — мой дядя и виртуального мира?", -удивленно спросила Оля.

Петя ничего не ответил. Он выбежал из кухни и влетел в свою комнату. Взглянув на себя в зеркало, он не увидел мальчишку. На него из зеркала смотрел усталый бледный дедушка.

"Что я натворил! — закричал Петя. "Из-за какой-то глупой игры бабушка пропала! Бабушка, моя милая бабушка…" - сквозь слезы бормотал Ваня.

Ваня, рыдая, упал в кровать и от своего бессилия уснул.

Ваня, Ваня… Кто-то осторожно трогал его за плечо. Открыв глаза, Ваня увидел свою бабушку.

"Бабушка, милая, ты вернулась!", - спросил Ваня.

"Да я, никуда и не уходила, на кухне посидела, чтоб тебе не мешать…", - ответила бабушка.

"Ты мне не мешаешь… Бабушка, прости меня, я не хотел тебя обидеть, честно!", - извиняясь проговорил Ваня.

Бабушка улыбнулась и ответила: "Я не сержусь на тебя, Ваня".

А мальчик подумал: «Как хорошо, что это был сон!».

Ваня, бывает, и сейчас может поиграть в какую-нибудь игру. Но теперь он помнит, что это всего лишь игра, а реальный мир намного интересней!

Вопросы для обсуждения:

- Сравните отношение Вани до ... и после...
- Как отнеслась бабушка к поведению Вани?
-Для чего нужно слушаться и прислушиваться к словам старших?

Дети обсуждают варианты поведения в этой ситуации.

Подведение итогов

Учитель еще раз акцентирует внимание детей на ситуации, рассмотренной на классном часе, делает выводы:

1. Слушаться взрослых.
2. Словом и поступком можно обидеть человека.
3. Игры на компьютере, планшете, в телефоне должны быть дозированными по времени.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод. руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Управителева Л.В. Классные часы по нравственному воспитанию в начальной школе. Ярославль, академия развития,2009 - 192с.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29.
7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. https://teremok-1.tvoysadik.ru/site/pub?id=219
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/ 3. https://skazkaplus.ru/russkiye-skazki/kak-petya-ponyal-chto-onlayn-igrydo-dobra-ne-dovedut

2. КИБЕРУРОК

«Как самый маленький гном Вася учился безопасному поведению в сети Интернет»

Цель: обучение детей правильно оценивать свои и чужие поступки.

Задачи:

1. повысить уровень знаний учащихся о возможностях использования сети Интернет: получение интересной и полезной информации, общение и коммуникация.
2. повысить уровень знаний учащихся об основных опасностях при использовании сети интернет.
3. усвоение детьми правил безопасного использования интернета.
4. повысить уровень осведомленности о возможностях решения неприятных и опасных ситуаций, возникающих в интернете.
5. сформировать систему действий и способов принятия решения при столкновении с неприятными и опасными ситуациями **Ход киберурока:**

Чтение и обсуждение сказки

Учитель: Здравствуйте, ребята. Послушайте сказку «Как самый маленький гном Вася учился безопасному поведению в сети Интернет» и подумайте, о чем мы сегодня будем говорить на занятии. **Учитель читает сказку.**

Сегодня я расскажу вам историю про маленького гномика Василия, который на летние каникулы приехал в гости к бабушке и дедушке. На опушке леса в маленьком уютном доме жила небольшая, но очень дружная семья маленьких гномов. Каждое утро дедушка отправлялся на спортивную площадку для занятия спортом. У бабушки были другие заботы: прибрать дом, истопить печь, приготовить обед. А маленький гномик Вася в это время оставался дома один, играл в игрушки и листал книжки. Очень часто он просил у своих бабушки и дедушки купить ему компьютер. И вот в один из вечеров, когда вся семья собиралась за ужином, дедушка сказал: «Мы решили подарить тебе компьютер». Василий очень обрадовался. С этого дня гномик проводил всё своё свободное время возле компьютера. Просьбы бабушки и дедушки не сидеть в интернете он просто не слушал. Стоило бабушке и дедушке утром уйти из дома, гномик сразу же садился за компьютер. В интернете он завёл много друзей, так ему казалось. Но из всех друзей был один друг, как казалось гномику, самый лучший. Он был очень добрый, хороший и Василию очень нравилось с ним общаться. Гномик рассказал своему другу, где он живёт, когда бабушка и дедушка уходят из дома и когда приходят домой. И вот однажды его друг предложил ему встретиться, поговорить и поиграть без компьютера, дома у гномика. Василий согласился, но бабушке и дедушке ничего не сказал. Испугался, что

ему не разрешат. И вот в один из летних дней, когда бабушка и дедушка ушли из дома, в дверь дома постучали. Василий очень радостный побежал открывать дверь, но когда он открыл её, то очень испугался. На пороге его дома стоял волк. От испуга гномик сильно закричал. Его крик услышали бабушка и дедушка, которые сегодня работали в огороде возле дома. Они прибежали домой, и выгнали волка, а гномику сказали: «Всегда надо спрашивать близких взрослых о незнакомых вещах в Интернете. Мы расскажем, что безопасно делать, а что нет. Прежде чем начать дружить с кем-то в Интернете, надо спросить у нас, как безопасно общаться. Никогда не надо рассказывать о себе незнакомым людям, где ты живёшь. Нельзя встречаться без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду». С тех пор маленький гномик большой бабушкин помощник: он собирает хворост для печки, приносит воду из колодца, рвёт вкусные травы для супа. А компьютером пользуется только со взрослыми, и только для того чтобы научиться чему - то хорошему

Завершение занятия

Учитель: Почему Василий перестал дружить с волком? (Потому что волк его обманул). Как вы считаете, ребята, нужно прислушиваться к словам взрослых или близких людей? (Ответы детей). **Используемая литература:**

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод. руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Управителева Л.В. Классные часы по нравственному воспитанию в начальной школе. Ярославль, академия развития,2009 - 192с.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. https://teremok-1.tvoysadik.ru/site/pub?id=219
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. Безопасность детей в Интернете http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html

3. КИБЕРУРОК
«Я имею право на безопасный Интернет» (1-4 классы)

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 систему взаимодействия 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

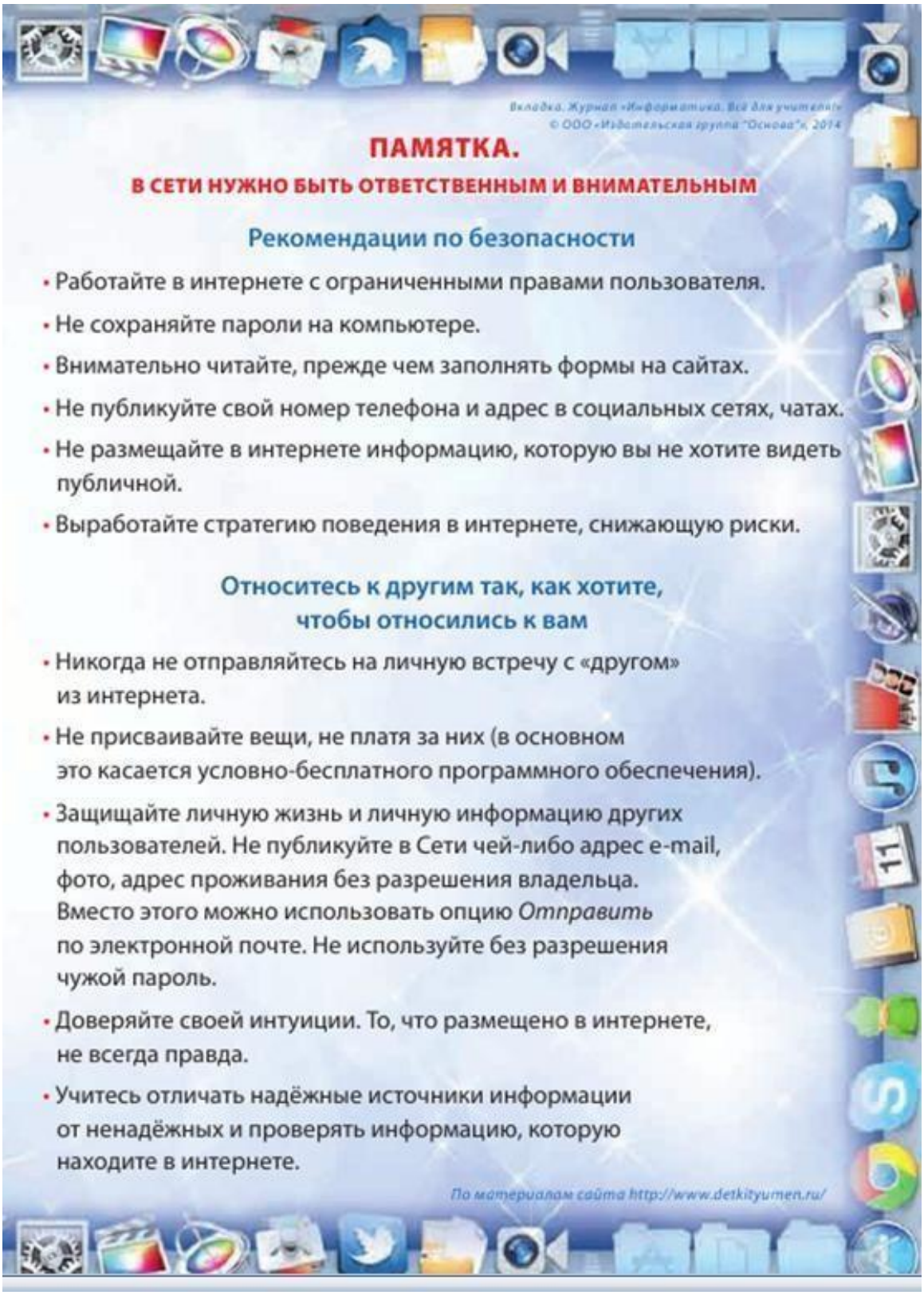
Интернет — такое же общественное место, как и улица (только виртуальное), поэтому:

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.



4. КИБЕРУРОК
«Полезный и опасный Интернет»

Цель: знакомство учащихся с понятием Интернет, его возможностями, опасностями, которые подстерегают их в интернете.

Задачи:

1. Познакомить ребят с понятием Интернет
2. Научить ребят выбирать правильную информацию в интернете, распознавать опасность при переписке с незнакомыми людьми, определять какую информацию о себе можно оставлять в соц. Сетях.
3. Развивать информационную грамотность
4. Воспитывать интерес к получению новых знаний.

Оборудование: Презентация, карточки с вопросами, фломастеры.

Ход киберурока:

1. **Организационный момент**

   Начинается урок,
   Он пойдет ребятам впрок!
   Постарайтесь все понять,
   Хорошо запоминать!

2. **Самоопределение темы и задач**

- Ребята, нам с вами сегодня пришло письмо от семьи Барбоскиных. Вчера они весь день просидели за компьютером: скачивали разные мультики и игры, и их компьютер подхватил вирус. Откуда он взялся они не знают, теперь он пишет на экране только это.

  713И65Н218Т45Е813Р984Н21Е69Т394

- Давайте им поможем! Зачеркните все цифры и из полученных букв составьте слово.
- Ну теперь все понятно! Барбоскины подхватили вирус из Интернета.
- Ребята, как вы думаете, о чем мы сегодня с вами будем говорить? (Называют тему и определят задачи)
- Сегодня мы узнаем, что такое Интернет и почему его называют полезным и опасным.

3. Изучение новой темы

Интернет

Охватил весь белый свет Всемогущий
Интернет.
Отыскать ты можешь мышкой
То, что раньше было в книжках.
Врач, профессор и студент,
Космонавт и президент
Смело в интернет заходят И
ответы в нем находят.

Анатолий Гришин

- Мы с вами живем в век информационных технологий. Компьютеры, планшеты, смартфоны прочно вошли в нашу жизнь практически во все ее сферы.
- У кого дома есть компьютер? Интернет? Как вы им пользуетесь?
- Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в то же время сеть таит в себе много опасностей.
- Знаете ли вы как обезопасить себя в Интернете?
- В 2011 году был принят Федеральный Закон «О защите детей от информации, причиняющей вред их здоровью и развитию», который должен помочь на государственном уровне обеспечить защиту детей от негативных информационных проявлений, в том числе и в Интернете. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительств о и прочие малоприятные явления.
- Тема правильного поведения детей в Интернете - очень важная тема.
- Как вы думаете, ребята, для чего школьникам нужен Интернет?
- Ребята, чтоб интернет был вам другом много лет!
  Будешь знать семь правил этих - смело плавай в интернете!

ПРАВИЛА ИНТЕРНЕТА:

1. **Спрашивай взрослых** Если что-то непонятно страшно или неприятно,
   Быстро к взрослым поспеши, Расскажи и покажи.
   Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
2. **Установи фильтр** Как и всюду на планете,
   Есть опасность в интернете.
   Мы опасность исключаем,
   Если фильтры подключаем.
   Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.
3. **Не открывай файлы**

Не хочу попасть в беду —
Антивирус заведу! Всем,
кто ходит в интернет,
Пригодится наш совет.
Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

4. **Не спеши отправлять SMS**
Иногда тебе в сети
Вдруг встречаются вруны. Ты
мошенникам не верь,
Информацию проверь!
Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.
5. **Осторожно с незнакомцами** Злые люди в Интернете Расставляют свои сети.
С незнакомыми людьми Ты на встречу не иди!
Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
6. **Будь дружелюбен**
С грубиянами в сети
Разговор не заводи.
Ну и сам не оплошай –
Никого не обижай.
Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.
7. **Не рассказывай о себе**
Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото
В интернет не помещай И
другим не сообщай.
Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

4. Физкультминутка

5. Закрепление изученного

- Какие же правила безопасного поведения в сети Интернет? Давайте еще больше узнаем о них с помощью мультфильма «Безопасный интернет»

6. Итог урока. Рефлексия

- У вас на домашнем компьютере установлен Интернет?
- Что вам больше всего нравится в Интернете?
- Как ваши родители воспринимают ваши занятия в Интернете? Почему
- А теперь подведём итоги нашего урока. Используйте для своего ответа следующие фразы:
  - Сегодня на уроке я узнал …
  - Я буду применять полученные знания на…
  - Мне понравился урок …
  - Сегодня на уроке я ничего нового не узнал.

5. КИБЕРУРОК
«10 ПРАВИЛ ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ»

Цель: познакомить учащихся с опасностями, которые подстерегают их в сети Интернет. Систематизировать и обобщить сведения о безопасной работе школьников в сети.

Задачи:

- информирование учащихся о видах информации, способной причинить вред здоровью и развитию младших школьников, а также о негативных последствиях распространения такой информации;
- обучение детей правилам ответственного и безопасного пользования услугами Интернет, в том числе способам защиты от опасных посягательств в сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде);
- профилактика формирования у учащихся Интернет-зависимости и игровой зависимости;
- предупреждение совершения учащимися правонарушений с использованием ИКТ-технологий.

Основные понятия: информация, угроза, безопасность.

Оборудование зависит от места проведения, это может быть, как обычная классная доска, так и электронная доска или компьютер с проектором.

В результате занятия, обучающиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет.

ХОД КИБЕРУРОКА:

В качестве видео-заставки для классного часа можно использовать http://youtu.be/789j0eDglZQ мультфильм «Безопасный интернет — детям!», который разработала студия Mozga.ru.

Учитель: отгадайте загадку: Сетевая
паутина оплела весь
белый свет, не пройти
детишкам мимо. Что же
это?**(**Интернет**)**

Детям предлагают из напечатанных на листах слов составить тему урокабеседы.

Итак, вы замечательно справились с заданием, тема нашего урокабеседы «10 ПРАВИЛ БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ».

Учитель: Мы живем в обществе, и очень многое в нашем поведении обусловлено правилами. Есть правила поведения на улице и в школе, транспорте, правила этикета. Надо ли их выполнять? (Конечно, надо.)

Что происходит, если нарушаются правила? Приведите примеры. (Дети отвечают и приводят примеры.)

Учитель: Среди множества правил существуют особые правила – «ПРАВИЛА БЕЗОПАСНОСТИ». На свете существуют опасности, которые могут не только испортить нам жизнь, но даже отнять её у нас. Чтобы такого не случилось, надо обязательно уметь предвидеть эти опасности и знать способы, как избежать их. Ведь народная мудрость гласит: «Берегись бед, пока их нет!».

Какие вы знаете Правила безопасности, и что будет, если их не соблюдать? (Дети отвечают: правила пожарной безопасности, поведения на дорогах, на воде и др.).

Учитель: Сделаем вывод: чтобы избежать опасных ситуаций, следует слушать советы взрослых и действовать по правилам безопасности.

Учитель: А какие же правила безопасности надо соблюдать при работе в сети Интернет? Интернет — интересный и многогранный мир, который позволяет узнавать много нового, общаться с людьми на разных концах света, играть в игры и делиться с другими своими фотографиями. Как вы думаете, какие опасности могут поджидать нас в Интернет? (Дети отвечают).

Учитель: Давайте выделим основные правила, которые нам надо соблюдать при работе в сети Интернет. «Мы хотим, чтоб Интернет Был вам другом много лет! Будешь знать СЕМЬ правил этих – Смело плавай в Интернете».

Правило 1. Никогда не публикуйте в сети и не сообщайте свое настоящее имя, адрес, школу, класс, номер телефона. Если вы разместите слишком много информации о себе, она может попасть в руки таких незнакомцев, которые захотят вас обидеть. «Если кто-то НЕЗНАКОМЫЙ

Вас попросит рассказать
Информацию о школе,
О друзьях и телефоне, Иль к
страничке доступ дать –
Мы на это НЕТ ответим,
Будем все держать в секрете!»

Правило 2. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернет; под маской виртуального

друга может скрываться злой человек. О подобных предложениях немедленно расскажите родителям. «Злые люди в Интернете Расставляют свои сети.

С незнакомыми людьми
Ты на встречу не иди!»

Правило 3. Не сообщайте никому свои пароли, не посылайте СМС в ответ на письма от неизвестных людей. Будьте осторожны с вложениями и ссылками в сообщениях электронной почты.

«Иногда тебе в сети Вдруг
встречаются вруны.
Обещают все на свете
Подарить бесплатно
детям: Телефон, щенка,
айпод и поездку на курорт.
Их условия не сложны:
СМС отправить можно
С телефона папы, мамы –
И уже ты на Багамах. Ты
мошенникам не верь,
Информацию проверь».

Правило 4. Всегда сообщайте взрослым обо всех случаях в Интернет, которые вызвали у вас смущение или тревогу.

«Если что-то непонятно,
Страшно или неприятно, Быстро
к взрослым поспеши, Расскажи
и покажи.
Есть проблемы в Интернете?
Вместе взрослые и дети
Могут все решить всегда
Без особого труда».

Правило 5. Для того, чтобы избежать встречи с неприятной информацией в Интернет, установите на свой браузер фильтр или попросите сделать это взрослых – тогда ты сможешь смело путешествовать по интересным тебе страницам. «Как и всюду на планете Есть опасность в Интернете. Мы опасность исключаем, Если фильтры подключаем».

Правило 6. Не скачивайте и не открывайте незнакомые файлы, не спросив разрешения родителей или учителей. Если же решили что-то скачать, проверьте файл с помощью антивирусной программы перед

тем, как открыть его. «Не хочу попасть в беду – Антивирус заведу! Всем, кто ходит в Интернет, Пригодится наш совет».

Правило 7. При общении в Интернете вы должны быть дружелюбными с другими пользователями. Ни в коем случае не надо писать и говорить оскорбительные слова, нельзя опубликовывать в сети чужие фотографии и сведения без разрешения хозяина. «С грубиянами в сети Разговор не заводи. Ну и сам не оплошай – Никого не обижай».

Правило 8. Уважайте чужую собственность. Незаконное копирование чужой информации, музыки, фотографий, компьютерных игр и других программ – кража.

Правило 9. Регистрируйтесь в программах, требующих регистрационного имени и заполнения форм, не требующих личных данных.

Правило 10. Помните, что далеко не всё, что мы читаем и видим в интернете -правда. Советуйтесь со взрослыми, прежде чем заходить на незнакомые сайты. Учитель: Ребята, если Вы будете соблюдать эти правила, то Интернет станет для Вас верным помощником, ведь в Интернет можно искать информацию, читать книги, посещать виртуальные музеи, играть, общаться с друзьями и конечно, учиться.

Учитель показывает мультфильм Фиксики: «Интернет» http://www.fixiki.ru/watch/4/7513/

Учитель: А теперь проверим, насколько хорошо Вы усвоили правила безопасного поведения в Интернете. Разделитесь на команды и попробуйте сформулировать основные правила, используя хорошо известные сказки. За каждый правильный ответ команда получает по смайлику J. Победит команда, набравшее больше количество смайликов.

Учитель демонстрирует картинки из сказок, учащиеся формулируют правила.

- «**Красная шапочка»** (Не разговаривай с незнакомцами).
- **«Волк и семеро козлят»** (Под маской виртуального друга может скрываться злой человек).
- **«Золотой ключик, или Приключения Буратино»** (Опасайся мошенников. Не сообщай никому свои пароли, не посылай СМС в ответ на письма от неизвестных людей).
- **Мойдодыр** (Проверяй компьютер на вирусы, пользуйся антивирусными программами).
- **«Сестрица Алёнушка и братец Иванушка**» (При встрече с неприятной (грязной) информацией в сети, выйди из Интернет).

- **«Морозко»** (Будь вежливым при общении в сети, не груби, тогда и к тебе будут относиться так же).

ПОДВЕДЕНИЕ ИТОГОВ

1. О чем мы сегодня говорили на классном часе?
2. Как вы думаете, помогут ли знания, полученные сегодня, в вашей жизни?
3. В наше время есть специальные службы, которые приходят на помощь людям в момент опасности, нам знакомы телефоны этих служб – 01, 02, 03.

Сегодня появилась новая бесплатная всероссийская служба консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи - 8 800 25 000 15.

Домашнее задание. Вспомни правила безопасного поведения в сети Интернет, обсуди их с родителями. Изготовь рисунок-плакат, посвященный одному из этих правил.

6. КИБЕРУРОК «Секрет хорошего настроения» (профилактика гаджет зависимости)

Цель: способствовать формированию навыков хорошего настроения, не прибегая к использованию телефона.

Задачи:

- научить понимать свои эмоции от использования телефона;
- научить анализировать свои мысли и поступки; снять физического и психического напряжения; сформировать навыки саморегуляции.

Продолжительность: 1 академический час.

Возраст: 7-12 лет.

Материалы и оборудование:

- карточки с эмоциями (удовольствие, интерес, радость, восторг, грусть, обида, страх, злость) (*приложение №1*);
- картинка «телефон» (*приложение №1*);
- бумага А4;
- ручка;
- цветные карандаши;
- маленькие кусочки разноцветной бумаги (либо цветной яркий песок, примерно 0,5 ч. ложки);
- кисточка;
- 3 пластиковых стаканчика;
- бумажная или влажная салфетка;
- черный песок (земля) (примерно 0,5ч. ложки); бланк с заданием «незаконченные предложения».

Упражнение «Ласковое имя»

Цель: создать доброжелательную атмосферу, настрой на работу.

Техника проведения: педагог предлагает ребенку поздороваться и назвать свое ласковое имя.

Инструкция: сегодня такой чудесный день, у меня очень хорошее настроение. Чтобы оно было такое же чудесное у тебя, давай поздороваемся друг с другом и назовём, как ласково звучат наши имена. Например, «Здравствуй, мое ласковое имя - Настенька». А как твое имя будет звучать ласково?

Анализ:

- Понравилось упражнение?
- Готов работать дальше?

Упражнение «Мой телефон»

Цель: научитьпонимать свои эмоции от использования телефона.
Материалы и оборудование: картинка «телефон», карточки с эмоциями (приложение №1).
Техника проведения: педагог предлагает ребенку разложить карточки с эмоциями от телефона на положительные и отрицательные.
Инструкция: Перед тобой рисунок телефона и восемь карточек с эмоциями. Распредели эти карточки так, чтобы с правой стороны от рисунка были приятные эмоции, которые ты мог испытывать от пребывания в телефоне, а с левой стороны от рисунка положи неприятные эмоции. Приведи примеры ситуаций с телефоном к каждой эмоции.
Анализ:

- Были трудности в выполнении задания?
- Почему ты так разложил карточки?
- Какое у тебя настроение, когда ты не можешь пользоваться телефоном?
- Какое у тебя настроение без использования телефона, когда ты играешь или занимаешься своими делами?

3. Упражнение «Незаконченные предложения» *Цель:*
*с*формировать навыки саморегуляции.
Материалы и оборудование: бланк с незаконченными предложениями, ручка.
Техника проведения: педагог открывает ребенку секрет о том, что настроение зависит от наших мыслей и поступков. Затем педагог приводит примеры мыслей и поступков, которые создают хорошее или плохое настроение, и вместе с ребенком их записывает.
Инструкция: я хочу тебе открыть «правило-секрет» о нашем настроении. Наше настроение зависит от наших мыслей и поступков. Поэтому, если хочешь, чтобы у тебя было хорошее настроение, думай о хорошем и совершай хорошие поступки, которые будут приносить радость тебе и окружающим. Попробуем применить это правило. Закончи предложения.

Мысли

Я плохой _____	Я справлюсь _____
Я не умею _____	У меня получится_____
Я не справился _____	Я научусь_____
Меня обидели _____	Все будет хорошо_____

Я боюсь _____	Я не буду бояться_____
Поступки	
Я не делаю_____	Я делаю_____
Я не помогаю _____	Я помогаю_____
Я не забочусь _____	Я забочусь_____

Анализ:

- Понравилось упражнение?
- Что нового ты для себя узнал? **4. Упражнение на снятие напряжения**

Цель: снять физическое и психическое напряжение.

Техника проведения: педагог-психолог совместно с ребенком выполняет предложенные упражнения.

Инструкция: после напряженной работы я предлагаю расслабиться и снять напряжение. Для этого мы будем выполнять следующие упражнения, которые ты сможешь применять в повседневной жизни.

1) Физкультминутка. Чтоб коленки не скрипели,
Чтобы ножки не болели,
Приседаем глубоко,
Поднимаемся легко. (приседания 10 раз)
Встали прямо, ноги шире,
Подбоченились руками.
Наклонились в правый бок,
Влево наклонились,
А теперь еще разок,
И остановились.

2) «Успокаивающее дыхание».

Повторяй за мной. Следует вдыхать в течение 5 секунд, затем задержать дыхание на 5 секунд и выдыхать в течение 5 секунд. Каждый последующий вдох мы будем уменьшать время задержки дыхания и увеличим время выдоха на 1 секунду. Начнем.

(Через несколько дыхательных циклов время вдоха должно составлять 5 секунд, а время выдоха - 10. В таком ритме можно подышать 2-3 минуты).

Анализ:

- Как твое самочувствие?
- Какое упражнение понравилось больше? □ Что не получилось? Почему?

5. Упражнение «Наши мысли и поступки».

Цель: научить анализировать свои мысли и поступки, закрепление полученный знаний.

Материалы и оборудование: 3 пластиковых стаканчика, черный песок (земля), разноцветная бумага (разноцветный яркий песок), кисточка, вода, салфетка, карточки с эмоциями (радость, удовольствие, интерес, вина, грусть, обида, страх, злость).

Техника проведения: педагог берет 3 стакана с водой и проводит опыт для визуализации эмоционального состояния.

Инструкция: попробуем увидеть, как работает «правило-секрет». Когда мы чувствуем себя хорошо, у нас все получается, мы всем довольны и всех любим. В это время настроение похоже на чистую воду, и мысли у нас ясные и «чистые» *(показывает стакан с чистой водой).* Положи рядом со стаканчиком карточки с теми эмоциями, которые похожи на твои спокойные мысли.

Когда в голову приходят отличные идеи, то настроение бывает прекрасным, радостным и мысли становятся похожи на салют: они становятся красочными, как вода в этом стакане *(бросаем в первый стакан кусочки разноцветной бумаги и кисточкой их размешивает).* Положи рядом со стаканчиком карточки с теми эмоциями, которые похожи на твое веселое настроение.

Но бывает, что наши мысли грустны и неприятны. Тогда они похожи на темную, мутную воду *(добавляет черный песок (землю) во второй стакан и размешиваем кисточкой).* Положи рядом со стаканчиком карточки с теми эмоциями, которые похожи на твое неприятные мысли.

Чтобы мутная вода стала снова прозрачной, мы можем подождать некоторое время. Песок (земля) осядет на дно, и мы сможем перелить воду в другой стаканчик, чтобы отделить воду от песка (земли). Или процедить воду через салфетку (чтобы песок (земля) остались на ней). Представляя, как совершаешь хорошие поступки и от этого вода (мысли) становится чище. В любом случае осадок остается и так же происходит с любой неприятной эмоцией.

Подумай, чтобы ты сделал с этим осадком? (выбросил, убрал в сторону и т.д.). Выбери карточки, которые характеризует твое состояние после того, как ты избавился от осадка.

Получается, чтобы прогнать неприятных мыслей, нужно подумать и совершить хорошие поступки, чтобы освободить себя от них. То есть, мы увидели, как наше настроение меняется от наших мыслей.

Анализ:

- Бывало ли у тебя грустное настроение? Когда?
- Что ты чувствовал при этом?
- О чем ты думал?
- Как ты выходил из грустного состояния?
- Что же нужно делать, чтобы плохое настроение прошло?

6. Обратная связь

Цель: анализ и закрепление опыта, постановка целей на будущее.

Инструкция:

- Что ты запомнил из сегодняшнего занятия?
- Что понравилось больше всего из сегодняшнего занятия? Почему?
- Что не понравилось? Почему?
- Каким образом можно улучшить свое настроение не используя телефон?
- Какие выводы ты сделал для себя? Какое у тебя настроение? **7. Упражнение «Хороший поступок»**

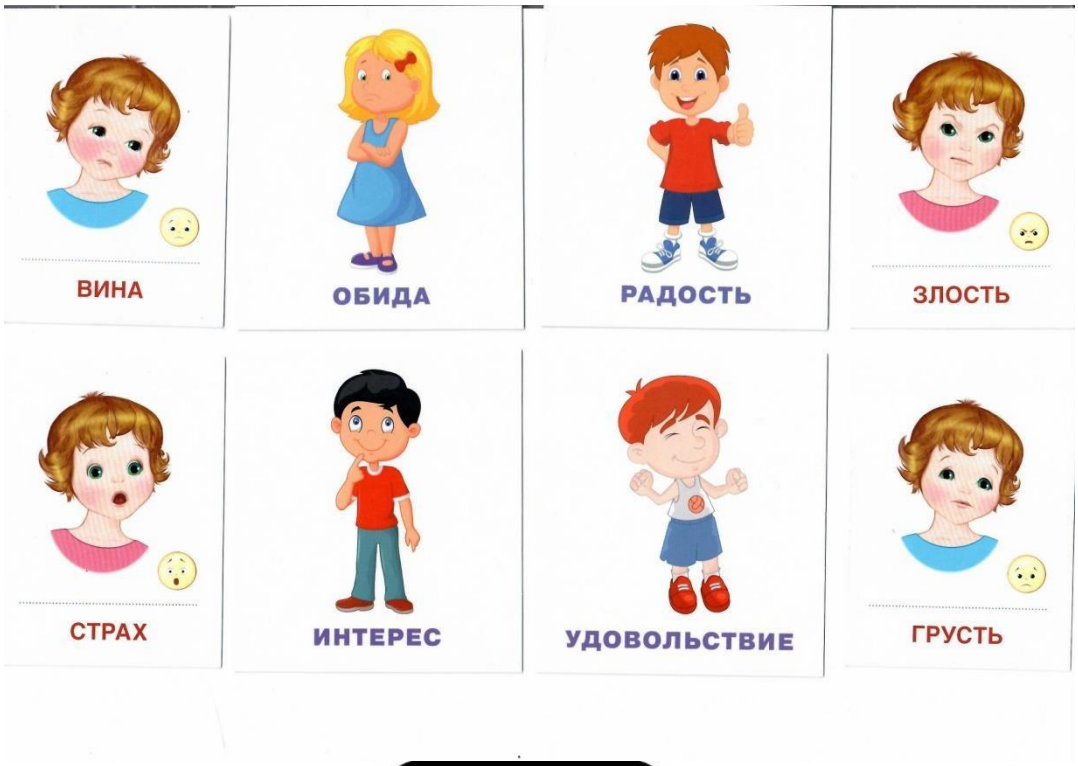
Цель: сформировать позитивное отношение к окружающим.

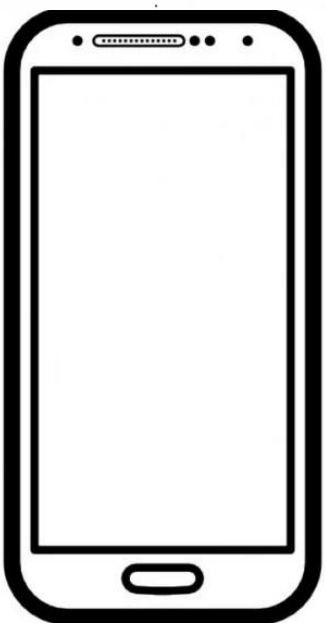
Материалы и оборудование: бумага А4, цветные карандаши.

Техника проведения: педагог предлагает ребенку совместно нарисовать свое настроение.

Инструкция: сегодняшнее занятие подошло к концу. Я предлагаю тебе на прощание сделать хороший поступок поделиться своим настроением. Предлагаю на листе бумаги нарисовать свое настроение и подарить его.

Приложение №1





7. КИБЕРУРОК
«Компьютер: друг или враг» (для 1 класса)

Цель: познакомить с основными устройствами компьютера; с правилами пользования компьютером.

Задачи: формировать у учащихся представления о роли, возможностях и способах использования компьютера в жизни человека;

Оборудование: карточки с названиями устройств компьютера, мультимедиа проектор, компьютер, презентация Power Point, конспект.

Ход киберурока:

Учитель:

Послушайте загадку:

Он рисует, он считает,
Проектирует заводы,
Даже в космосе летает И
дает прогноз погоды.
Миллионы вычислений Может
сделать за минуту,
Догадайтесь, что за гений?
Ну, конечно же …(компьютер)

Учитель:

Сегодня к нам в гости пришел компьютер, он не такой современный как у вас дома, но зато он знает всю историю развития вычислительной техники. Поэтому мы узнаем, как компьютеры изобретались, каковы основные устройства компьютера, а также мы научимся правильно сидеть за компьютером и решим враг нам компьютер или друг. Компьютеры уже давно проникли во все сферы нашего жизненного пространства. Компьютер – это чудо техника.

Беседа с показом слайдов.

1. С глубокой древности людям приходилось считать. Сначала они считали на камнях, ставили зарубки на дощечках, узелки на веревках. Прошло много лет, и люди научились считать на пальцах. На Руси долгое время считали на косточках, раскладывая их в кучки. Затем косточки нанизывали на горизонтальную веревку, так появились счеты. Раньше счеты широко использовались в кассах магазинов.

На протяжении всей истории человек постоянно изобретал различные приспособления, помогающие ему в работе. Во второй половине 20 века люди создали электронные вычислительные машины (ЭВМ), которые выполняли сложные расчеты. ЭВМ занимали много места в помещении, работали медленно. На смену им пришли калькуляторы – маленькие карманные устройства для выполнения вычислений. Но, калькулятор только считал - этого стало человеку недостаточно, и он изобретает персональный компьютер, который мог работать с разной информацией и выполнять сложные расчеты. Одним из самых замечательных изобретений человека является компьютер. С каждым годом они становятся сложнее

2. Компьютер – это сложный электронный прибор, он состоит из разных устройств, работающих вместе. А как вы знаете эти устройства, проверим.

Загадки отгадываем и на доску вывешиваем карточки с отгадками.

Скромный серый колобок,
Длинный тонкий проводок,
Ну а на коробке – Две
или три кнопки.
В зоопарке есть мартышка,
У компьютера есть … (мышка)
Ты – как в море капитан, Пред
тобой горит экран.
Яркой радугой он пышет,
А на нем компьютер пишет И
рисует без запинки
Всевозможные картинки.
Наверху машины всей
Размещается…(дисплей)
Монитор еще называют
ДИСПЛЕЕМ Около дисплея –
Главный блок:
Там бежит электроток
К самым важным микросхемам.
Этот блок зовут…(системным)
По клавишам прыг да скок – Бе-
ре-ги но-го-ток!
Раз-два – и готово:
Отстукали слово!
Вот где пальцам
физкультура! Это вот -
…(клавиатура) Для чего же
этот ящик?
Он в себя бумагу тащит.
И сейчас же буквы, точки, Запятые
– строчка к строчке!
Напечатает картинку
Ловкий мастер –
Струйный …(принтер)

Учитель: Сейчас в принтеры встроены сканеры – устройство, которое, анализируя какой-либо объект, создаёт цифровую копию изображения объекта и помещает его в память компьютера. Процесс получения этой копии называется сканированием. Если принтеры выводят

информацию из компьютера, то сканеры, наоборот, переносят информацию с бумажных документов в память компьютера.

Учитель: Ребята, какое из устройств компьютера главнее? Все важны, но без системного блока компьютер не будет работать. А все остальные устройства подключаются к системному блоку.

Дети читают стихи

Этот вот системный блок,
Для компьютера – как Бог.
Он решает все проблемы,
И содержит микросхемы.
Ум компьютера – процессор.
Самый главный элемент. Он
в машине служит мозгом, И
его важнее нет.
Человеческий язык, Понимать
он не привык.
Наших слов не разбирает,
Буквы в цифры превращает.
Вот тебе теперь известно,
Как работает процессор.

Учитель:

Что умеет делать компьютер? Как мы его используем? Для чего?

Игра: вывешивается картинка, дети говорят назначение компьютера.

Учитель:

Компьютер – это техническое устройство для хранения и обработки различных видов информации, которая находится в его памяти в закодированном виде. Компьютеры нужны: в магазинах, чтобы подсчитать стоимость товара; на вокзале, в библиотеке, в сберегательном банке компьютер хранит всю информацию о денежных вкладах; в киностудии создаст фильм; архитектору поможет сконструировать макет здания; в автомобильном салоне компьютер создаст модель новой машины.

Компьютер – это незаменимый помощник человека при работе с информацией. Можно назвать его своим другом?

Дети читают стихи.

Оглянись, дружок, вокруг!
Вот КОМПЬЮТЕР – верный друг.
Он всегда тебе поможет:
Сложит, вычтет и умножит!
Может он ребят учить,

Может он станок включить Папе,
дедушке и тете
Он поможет на работе.

Учитель: Да, компьютеры сильно облегчают нашу работу, делают жизнь интересней, но за удобства, комфорт мы вынуждены платить своим здоровьем. Поэтому сейчас поговорим о том, как правильно организовать наше общение с компьютером.

Американские ученые установили, что именно правильная поза является главным гарантом здоровья и безопасности при работе за компьютером. Прежде всего, следует учесть: высота стула должна соответствовать длине голени: тогда ступни ног всей поверхностью будут полностью касаться пола. Максимальная глубина сиденья стула должна составлять 2/3 длины бедра. Очень полезно устроить валик между спинкой стула и поясницей. Это позволит разгрузить поясничный отдел позвоночника. Локти должны быть расположены как можно ближе к телу, поэтому стул должен быть с подлокотниками и высокой спинкой. Нужно сидеть, откинувшись на спинку рабочего кресла, шея должна быть выпрямлена. Расстояние от экрана монитора до глаз должно быть 50-70 см.

Для того, чтобы избежать истощение зрительной системы, следует помнить об одном факторе здоровья глаз: нужно не забывать моргать. Работа за компьютером формирует синдром «застывшего взгляда». Его нужно преодолевать сознательно и чаще моргать, тем самым снижая напряжение с глазных мышц. Ну, и конечно, через каждые 20-25 мин. проводить комплекс упражнений для глаз.

Стрекоза

Вот какая стрекоза - как горошины глаза.
Пальцами делают очки.
Влево - вправо, назад - вперед- Глазами
смотрят вправо- влево.
Ну, совсем как вертолет.
Круговые движения глаз.
Мы летаем высоко.
Смотрят вверх.
Мы летаем низко.
Смотрят вниз.
Мы летаем далеко. Смотрят
вперед.
Мы летаем близко.
Смотрят вниз.

Гимнастика для глаз

1. Закрыть глаза, на счет 1-4, широко раскрыть глаза и посмотреть вдаль на счет 1-6. Повторить 4-6 раз
2. Посмотреть на кончик носа, на счет 1-4 и перевести взгляд вдаль на счет 1-6. Повторить 4-6 раз
3. Голова прямо, медленно выполнять круговые движения глазами вверх – вправо – вниз – влево и в обратную сторону. Затем посмотреть вдаль и в обратную сторону. Затем посмотреть вдаль на счет 1-6. Повторить 4-6 раз
4. Быстро перевести взгляд по диагонали: направо вверх – налево вниз, потом прямо на счет 1-6. Повторить 4-6 раз
5. Затем налево вверх – направо вниз и посмотри вдаль на счет 1-6. Повтори 4-6 раз.

Учитель:

Для достаточной освещенности клавиатуры и рабочего места рекомендуется использовать настольную лампу дополнительно к общему освещению. Лампу ставить слева от монитора, свет не должен ярко светить в глаза. Кроме того, нельзя сидеть за компьютером в полной темноте.

Компьютер не только источник информации, радости: это, прежде всего устройство, воздействующее своими электромагнитными и электростатическими полями на наш организм. Но вся жизнь человека проходит в мире, заполненном разного рода излучениями. Они исходят из космоса, из земли, от любого бытового электроприбора, в том числе и от компьютера. В современных компьютерах излучение абсолютно безопасно и не влияет на здоровье человека. Зато электростатическое поле обладает способностью «заряжать» микрочастицы, пылинки, летающие в воздухе, препятствуют их оседанию. В результате в воздухе повышается количество пыли, что увеличивает риск развития аллергических заболеваний. Поэтому, компьютер может стать врагом, если не соблюдать все меры предосторожности, которые мы рассмотрели.

Учитель: Комнату, где стоит компьютер надо проветривать, поместить в ней много комнатных растений, и даже врачи советуют поставить аквариум. **Детям 7 лет допустимо 30-60 мин в день проводить за компьютером.**

Компьютер – это помощник человека при работе с информацией. Он является незаменимым помощником человека в любой профессии. Для детей инвалидов, которые не могут посещать школу, компьютер является единственным средством получения полноценного образования.

Учитель:

Чтобы для нас компьютер стал другом и помощником, рассмотрим выставку. Для детей созданы увлекательные компьютерные игры, обучающие компьютерные программы, электронные библиотеки.

Работа с выставкой компьютерных игр.

Учитель: Давайте проверим, как вы усвоили названия устройств компьютера:

1. *Устройство для ввода символов (букв, цифр, знаков препинания,)*
2. *Устройство, с помощью которого можно подключиться к сети Интернет.*
3. *Устройство для хранения информации.*
4. *Устройство для ввода информации.*
5. *Устройство вывода информации на экран.*
6. *Устройство ввода в компьютер рисунков, фотографий.*

Учитель: Вот и подошел к концу наш киберурок. Выберете смайлик, соответствующий вашему настроению и прикрепите его на доску. Надеюсь, вы подружились с компьютером, и он станет вам другом и помощником.

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 2-Х КЛАССОВ

8. КИБЕРУРОК
«Как Ваня понял, что онлайн-игра до добра не доведет»

Цель: обучение детей правильно оценивать свои и чужие поступки.

Задачи:

1) повысить уровень знаний учащихся о возможностях использования сети Интернет: получение интересной и полезной информации, общение и коммуникация.
2) повысить уровень знаний учащихся об основных опасностях при использовании сети интернет.
3) усвоение детьми правил безопасного использования интернета.
4) повысить уровень осведомленности о возможностях решения неприятных и опасных ситуаций, возникающих в интернете.
5) сформировать систему действий и способов принятия решения при столкновении с неприятными и опасными ситуациями

Ход киберурока:

Вводная часть:

Упражнение «С миру по нитке»

Один из участников начинает рассказ «Сказка про Интернет», предлагая одно предложение, затем следующий по кругу добавляет к нему свое предложение, следующий – свое, и так до тех пор, пока очередь не дойдет до начавшего. Затем кому-нибудь из группы предлагается вспомнить и рассказать все получившееся целиком. Остальные могут дополнять или поправлять **Основная часть:**

Чтение и обсуждение истории

Учитель: Здравствуйте, ребята. Послушайте сказку «Как Ваня понял, что онлайн-игра до добра не доведет» и подумайте, о чем мы сегодня будем говорить на занятии. **Учитель рассказывает историю.**

Сегодня я расскажу вам историю про мальчика Ваню, который очень любил играть в онлайн-игры.

"И зачем вы только этот планшет ему купили! Ещё больше играть будет!", — возмущалась бабушка.

"Планшеты сейчас у каждого ребёнка сейчас есть, и ничего…", — возражал папа.

"А в телефоне всё мелкое, со своими игрушками он зрение испортит!", — добавляла мама.

Бабушка только вздыхала и уходила на кухню. Вначале Ваня играл в игры нечасто, учил уроки, помогал прибираться по дому. Но потом в его любимой игре начался сезон турниров. Вот тут и началось самое интересное! "Ваня, а ты слышал, что скоро в нашей игре турнир будет?", — возбуждённо крикнул Павлик, подбежав к другу.

"Нет, а что такое турнир?" . "Ну ты и тундра!", — удивился Павлик. "Это чемпионат, здесь можно стать мега крутым бойцом!"

" Эх, у меня, наверно, не получится поучаствовать. Не разрешит мне мамка столько играть! А долго надо играть?", — с интересом спросил Ваня. "Не меньше пяти часов! Дня два будут состязания идти. Надо во всех битвах победить. А это трудно: знаешь, какие там бойцы!", - заявил Павлик.

Ваня пришёл домой с мыслями только об одном: что бы такое придумать, чтоб ему разрешили турнир этот пройти. Ваня даже обещания маме и папе заготовил: хорошо учиться, прибираться в комнате, всегда помогать и всё такое.

Дома была только бабушка. Тётя приболела, и родители уехали её проведать. Два дня их не будет! Ваня был счастлив: бабушка не такая строгая, как мама и папа. Уж теперь турнир точно будет его!

После вкусного обеда Петя вымыл за собой тарелку и, заглядывая бабушке в глаза, тихо спросил: "Бабуля, можно?"

"Что можно?", - спросила бабушка. Ваня отвечал: "Ну, поиграть немного на планшете… У меня турнир сегодня". "Ну, если турнир, то конечно! Но только немного", - улыбнулась бабушка. "Конечно, конечно!", — Ваня, схватив планшет, удобно устроился на диване.

Игра захватила мальчика, он ничего вокруг не видел и не слышал. Битва была сложной. Он осилил только троих бойцов и начал игру сначала, а в дверях детской уже появилась бабушка: "Ванечка, ты же просил немного, а уже целый час прошёл! Ну всё, заканчивай!"

"Бабуля, милая, ну минуточку, последний бой!" - попросил Ваня.

"Пять минут, Ваня, пять минут!" - ответила бабушка.

Но через пять минут Петя даже и не подумал убрать планшет. Он снова проиграл бой и очень разозлился: он хотел стать победителем, но увы не получалось.

И когда бабушка снова заглянула в комнату, мальчик сделал вид, что не слышит её замечания. Да, он знал, что бабушка обидится, но он потом извинится, а сейчас битва — вот самое главное! Бабушка заходила несколько раз, но Ваня или молчал, или просто махал рукой: некогда мне.

В конце концов бабушка не выдержала и спросила: «Ваня, я устала тебе говорить, что пора прекращать свою игру! У тебя уже глаза квадратные! Ты меня слышишь?" Мальчик молчал. Ваня…
"Да, отстань, ты от меня! «Ваня, Ваня»…"Да как ты разговариваешь со мной", — дрожащим голосом заговорила бабушка.
"Как хочу, так и разговариваю! Это моя квартира, и я здесь хозяин! Не нравится — уходи!", — последние слова мальчик громко выкрикнул, а потом вскочил с дивана и захлопнул дверь своей комнаты перед лицом бабушки.

Он думал, что сейчас бабушка зайдёт его снова ругать, но услышал только тихие шаги за дверью. "Наверно, на кухню пошла, — подумал он, — вот и хорошо. Я как раз доиграю, а потом извинюсь. А сейчас не до этого: битва есть битва!"

Петя весь ушёл в игру. Сколько прошло времени — он не знал. Турнир все ещё не заканчивался, а у планшета села батарея. Мальчик вспомнил, что оставил зарядное устройство в большой комнате.

"Ну и ладно, — сказал сам себе Петя, — схожу за зарядным устройством, зайду на кухню к бабушке, извинюсь и продолжу!"
Петя потянулся: все мышцы из-за того, что он долго сидел в одной позе, затекли. Он открыл дверь своей комнаты и удивился: в коридоре были другие обои, да и всё было по-другому.
"Бабуля здесь за пару часов всё переклеила что ли?", — удивился Иван.

Но когда мальчик вошёл на кухню, то никакой бабушки не было. А была только девочка лет восьми. Она сидела за столом и за обе щёки уплетала конфеты.
"Ты кто?". — спросил Петя.
"Оля", — сказала девочка, — а вы, дядя, наверно, водопроводчик? "Какой водопроводчик? Да и какой я тебе дядя, я тебя только на пару лет старше!",- ответил Ваня.
"Ха-ха! Ну вы и шутник! Я что, похожа на бабушку?". — весело рассмеялась девочка.
"Хватит мне морочить голову, — Ваня разозлился, — ты кто такая, и где моя бабушка?"
"Какая бабушка?". — поинтересовалась девочка.
"Инга Андреевна— моя бабушка! Ты мне объясни, ты как сюда попала, тебя бабушка впустила?", - спросил удивленно Ваня.
"Я здесь живу!". — девочка обиженно поджала губки. Затем, что-то припоминая, добавила: "Инга Андреевна, — где-то я это слышала… А, вспомнила! Мне папа рассказывал. Это моя прабабушка. Он ещё говорил,

что она пропала до его рождения. Внук её старший обидел. Он так заигрался на планшете в игру, что никого не видел и не слышал. Его родители — мои бабушка и дедушка — пытались его привести в чувства, врачей вызывали, но всё бесполезно. Даже новую болезнь открыли — «зомбикомп» называется. С тех пор к этому мальчику, а он, кстати, мой дядя, перестали заходить. Врач сказал, что ему даже еда не нужна, ведь он переселился в виртуальный мир. На двери его комнаты даже табличку повесили: «Не входить!».

Ваня пришёл в ужас:

"А бабушка, куда она пропала?". - спросил Ваня.

"Никто не видел её с того вечера. Стоп, а вы не из той комнаты с табличкой? Вы — мой дядя и виртуального мира?", -удивленно спросила Оля.

Ваня ничего не ответил. Он выбежал из кухни и влетел в свою комнату. Взглянув на себя в зеркало, он не увидел мальчишку. На него из зеркала смотрел усталый бледный дедушка.

"Что я натворил!, — закричал Ваня. "Из-за какой-то глупой игры бабушка пропала! Бабушка, моя милая бабушка…" - сквозь слезы бормотал Ваня.

Ваня, рыдая, упал в кровать и от своего бессилия уснул.

Ваня, Ваня… Кто-то осторожно трогал его за плечо. Открыв глаза, Ваня увидел свою бабушку.

"Бабушка, милая, ты вернулась!", - спросил Ваня.

"Да я, никуда и не уходила, на кухне посидела, чтоб тебе не мешать…", - ответила бабушка.

"Ты мне не мешаешь… Бабушка, прости меня, я не хотел тебя обидеть, честно!", - извиняясь проговорил Ваня.

Бабушка улыбнулась и ответила: "Я не сержусь на тебя, Ваня".

А мальчик подумал: «Как хорошо, что это был сон!».

Ваня, бывает, и сейчас может поиграть в какую-нибудь игру. Но теперь он помнит, что это всего лишь игра, а реальный мир намного интересней!

Вопросы для обсуждения:

- Сравните отношение Вани до ... и после...
- Как отнеслась бабушка к поведению Вани?
-Для чего нужно слушаться и прислушиваться к словам старших?

Дети обсуждают варианты поведения в этой ситуации.

Подведение итогов

Учитель еще раз акцентирует внимание детей на ситуации, рассмотренной на уроке, делает выводы:

1. Слушаться взрослых.
2. Словом и поступком можно обидеть человека.
3. Игры на компьютере, планшете, в телефоне должны быть дозированными по времени.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод. руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Управителева Л.В. Классные часы по нравственному воспитанию в начальной школе. Ярославль, академия развития,2009 - 192с.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. https://teremok-1.tvoysadik.ru/site/pub?id=219
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. https://skazkaplus.ru/russkiye-skazki/kak-petya-ponyal-chto-onlayn-igry-dodobra-ne-dovedut

9. КИБЕРУРОК
«Как самый маленький гном Вася учился безопасному поведению в сети Интернет»

Цель: обучение детей правильно оценивать свои и чужие поступки.

Задачи:

1. повысить уровень знаний учащихся о возможностях использования сети Интернет: получение интересной и полезной информации, общение и коммуникация.
2. повысить уровень знаний учащихся об основных опасностях при использовании сети интернет.
3. усвоение детьми правил безопасного использования интернета.
4. повысить уровень осведомленности о возможностях решения неприятных и опасных ситуаций, возникающих в интернете.
5. сформировать систему действий и способов принятия решения при столкновении с неприятными и опасными ситуациями

Ход киберурока:

Вводная часть:

Игра-активатор: ПОЗДОРОВАЙСЯ

Ведущий объявляет, что сейчас все будут здороваться друг с другом, но не совсем привычными способами. По хлопку в ладоши и его команде участники должны поздороваться со всеми, кто стоит рядом. Ведущий хлопает в ладоши и кричит: «Руки!» Все пожимают друг другу руки. Затем ведущий хлопает в ладоши и выкрикивает: «Колени!» Все касаются коленом колена и называют свое имя. Ведущий может выкрикивать все, что удобно в данной аудитории (локти, уши, щеки, лодыжки и т.д.)

Упражнение «Сочини историю»

Один из участников начинает рассказ «Как я правила пользования Интернетом учил….», предлагая одно предложение, затем следующий по кругу добавляет к нему свое предложение, следующий – свое, и так до тех пор, пока очередь не дойдет до начавшего. Затем кому-нибудь из группы предлагается вспомнить и рассказать все получившееся целиком. Остальные могут дополнять или поправлять **Основная часть:**

Чтение и обсуждение сказки

Учитель: Здравствуйте, ребята. Послушайте сказку «Как самый маленький гном Вася учился безопасному поведению в сети Интернет» и подумайте, о чем мы сегодня будем говорить на занятии. **Учитель читает сказку.**

Сегодня я расскажу вам историю про маленького гномика Василия, который на летние каникулы приехал в гости к бабушке и дедушке. На опушке леса в маленьком уютном доме жила небольшая, но очень дружная семья маленьких гномов. Каждое утро дедушка отправлялся на спортивную площадку для занятия спортом. У бабушки были другие заботы: прибрать дом, истопить печь, приготовить обед. А маленький гномик Вася в это время оставался дома один, играл в игрушки и листал книжки. Очень часто он просил у своих бабушки и дедушки купить ему компьютер. И вот в один из вечеров, когда вся семья собиралась за ужином, дедушка сказал: «Мы решили подарить тебе компьютер». Василий очень обрадовался. С этого дня гномик проводил всё своё свободное время возле компьютера. Просьбы бабушки и дедушки не сидеть в интернете он просто не слушал. Стоило бабушке и дедушке утром уйти из дома, гномик сразу же садился за компьютер. В интернете он завёл много друзей, так ему казалось. Но из всех друзей был один друг, как казалось гномику, самый лучший. Он был очень добрый, хороший и Василию очень нравилось с ним общаться. Гномик рассказал своему другу, где он живёт, когда бабушка и дедушка уходят из дома и когда приходят домой. И вот однажды его друг предложил ему встретиться, поговорить и поиграть без компьютера, дома у гномика. Василий согласился, но бабушке и дедушке ничего не сказал. Испугался, что ему не разрешат. И вот в один из летних дней, когда бабушка и дедушка ушли из дома, в дверь дома постучали. Василий очень радостный побежал открывать дверь, но когда он открыл её, то очень испугался. На пороге его дома стоял волк. От испуга гномик сильно закричал. Его крик услышали бабушка и дедушка, которые сегодня работали в огороде возле дома. Они прибежали домой, и выгнали волка, а гномику сказали: «Всегда надо спрашивать близких взрослых о незнакомых вещах в Интернете. Мы расскажем, что безопасно делать, а что нет. Прежде чем начать дружить с кем-то в Интернете, надо спросить у нас, как безопасно общаться. Никогда не надо рассказывать о себе незнакомым людям, где ты живёшь. Нельзя встречаться без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду». С тех пор маленький гномик большой бабушкин помощник: он собирает хворост для печки, приносит воду из колодца, рвёт вкусные травы для супа. А компьютером пользуется только со взрослыми, и только для того чтобы научиться чему - то хорошему **Завершение занятия**

Учитель: Почему Василий перестал дружить с волком? (Потому что волк его обманул). Как вы считаете, ребята, нужно прислушиваться к словам взрослых или близких людей? (Ответы детей).

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод. руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Управителева Л.В. Классные часы по нравственному воспитанию в начальной школе. Ярославль, академия развития,2009 - 192с.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете:
запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

3. https://teremok-1.tvoysadik.ru/site/pub?id=219
4. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. Безопасность детей в Интернете
http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html

10. КИБЕРУРОК
«Я имею право на безопасный Интернет» (1-4 классы)

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 зурока:**

Вводная (подготовительная часть)

Упражнение – активатор: «Тишина»

Группа делится на пары, одному из участников пары дается бумажка, на которой написано нетрудное задание. Пользуясь только жестами, не говоря ни слова, он должен объяснить своему напарнику, что написано на бумажке, и добиться того, чтобы он это выполнил.

Упражнение 2: Игра «Цветок»

Цель: знакомство участников для создания комфортной атмосферы для работы

Описание упражнения: Перед началом упражнения учительприкрепляет цветок, сделанную из цветной бумагибез лепестков на доске (рисунок 1). Учитель раздает каждому ученику стикеры и дает задание участникам придумать себе прозвище («никнеймы»), которыми они пользуются при общении в Интернет пространстве или хотели бы использовать, и написать их на стикерах. Кожнен ученик выходит с стикером , называет никнейм, свое реальнее имя и хобби и наклеивает стикер с никнеймом на цветок, так чтобы стикер стал лепестком цветка. После выполнения упражнения цветок остается для следующего упражнения (Смотрите рисунок 2). **Основная часть:**

- 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 систему взаимодействия 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**

3. Журнал «Основа. Информатика» №1 2014г.
4. .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.

11. КИБЕРУРОК

«Безопасность в сети Интернет» (для 2 класса) Цель:

- познакомить учащихся с опасностями, которые подстерегают их в Интернете и помочь избежать этих опасностей;

- рассказать о вирусах, вредоносных программах, в интернете; - дать знания о том, как себя вести в социальной сети.

Оборудование: памятка учащимся, музыкальное сопровождение, карточки (рефлексия)**,** картинки героев из мультфильма "Маша и Медведь", презентация

Ход урока

I Организационный момент

- Улыбнитесь друг другу, настройтесь на дружную и активную работу на уроке. Я желаю вам, чтобы работа на уроке принесла вам только положительные эмоции!

II Сообщение темы занятия

-Ребята, у нас в гостях герои мультфильма Маша и Медведь.

Маша уже школьница. Она научилась читать и писать. Миша решил сделать ей подарок. А хотите узнать какой? Тогда отгадайте эту загадку.

1.Что за чудо-агрегат
Может делать все подряд - Петь,
играть, читать, считать,
Самым лучшим другом стать? (Компьютер.)

- Давайте познакомим Машу с компьютером. Ведь ей так не терпится научится работать на нём. Поможем ей?
- Сначала нужно его открыть и назвать все его основные части. А в этом нам поможет игра.

1. Игра «Угадай-ка»

На столе он перед нами, на него направлен взор,
подчиняется программе, носит имя... (монитор). Не
зверушка, не летаешь, а по коврику скользишь и
курсором управляешь. Ты – компьютерная... (мышь).

Нет, она – не пианино, только клавиш в ней – не счесть! Алфавита там картина, знаки, цифры тоже есть.

Очень тонкая натура. Имя ей ... (клавиатура). Сохраняет все
секреты «ящик» справа, возле ног, и слегка шумит при этом.
Что за «зверь?». (Системный блок).

Сетевая паутина оплела весь белый свет, не пройти детишкам мимо. Что же это? (Интернет).

- 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).

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

- Ребята, у кого из вас на домашнем компьютере установлен Интернет? Что вам больше всего нравится в Интернете? Как ваши родители воспринимают ваши занятия в Интернете? Почему?
- В современном мире знания вы можете получать из различных источников информации. Какими источниками информации вы пользуетесь чаще всего?
- Как вы думаете, какой источник информации представляет наибольшую опасность для ребенка?
- Определите, о чём пойдёт речь на уроке?

(Интернет. Какие опасности он таит для нас?)

- *Молодцы! Маша, слушая вас даже призадумалась. Ведь оказывается нужно многому учиться.* **2. Изучение нового материала.**

1. *Вступительное слово учителя*

- Ребята, а как вы думаете, нужна ли защита детям от информации и материалов, наносящих вред их благополучию?

Не случайно в 2011 году был принят Федеральный Закон «О защите детей от информации, причиняющей вред их здоровью и развитию», который должен помочь на государственном уровне обеспечить защиту детей от негативных информационных проявлений, в том числе и в Интернете.

Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительств о и прочие малоприятные явления. Учреждён и Международный День безопасного Интернета, который отмечается ежегодно 8 февраля.

-Как вы думаете, ребята, для чего школьникам нужен Интернет? Сегодня мы поговорим об Интернете: выясним - что такое Интернет, назовем положительные и негативные его стороны, определим основные виды опасностей, подстерегающих детей в сети Интернет и составим правила безопасного пользования Интернетом и научим всему нашу гостью Машу.

1) Что такое интернет?

- А в этом нам помогут ребята, которые подготовили небольшие выступления.

1 ученик. Интернет – обширная информационная система, которая стала наиболее важным изобретением в истории человечества.

2 ученик. Интернет - это всемирная электронная сеть информации, которая соединяет всех владельцев компьютеров, подключенных к этой сети. **3 ученик.** 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.

4 ученик. 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.

5 ученик. Что касается Интернета, то кроме чатов там есть форумы, где обсуждаются серьезные вопросы и где можно высказать свою точку зрения.

2) ВЫВОД:

1. ИНТЕРНЕТ - площадка для общения (школьные сайты, блоги, форумы; электронная почта);
2. ИНТЕРНЕТ - источник информации
3. ИНТЕРНЕТ - дистанционное обучение (дистанционные курсы, мастерклассы, консультирование болеющих детей и детей на домашнем обучении);
4. ИНТЕРНЕТ - позволяет участвовать в сетевых конкурсах, олимпиадах, проектах.

Интернет предлагает большое количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. У газет или журналов есть редактор, который проверяет информацию. А Интернет не сможет проверить, насколько правдива размещенная информация.

III ФИЗКУЛЬТМИНУТКА

(поют песенку и выполняют движения)

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

1.На компьютере играли,
Наши глазоньки устали,
А теперь мы отдохнем
И опять играть начнем. (Руки на поясе,
наклоны влево, вправо).

2.Нужно спортом заниматься И
в жару нам, и в мороз,
Если где-то ты не сможешь, То
не хмурь уж ты свой нос.
(Хлопать в ладоши).

3.Мы пропели вам частушки
Хорошо ли, плохо ли,
А теперь мы вас попросим, Чтобы
вы похлопали.

IV. Закрепление изученного

- Пока мы отдыхали, Маша прочла на экране:

1. **Будь осторожен в Интернете.**

-Какие опасности могут подстерегать детей в Интернете? ***1)Чтение стихов о правилах Интернет-безопасности***

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

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

3.Вдруг однажды сам решил
Втайне от родителей
Потихоньку завести
Для общения в сети электронный адрес.
Указал без разрешения
Адрес, улицу и дом, и квартиру в нем.

4.Разместил на сайте ты фотографии семьи. Не
забыл секреты старших - все в анкете указал,
Все, что вспомнил, все, что знал!
Переписываться стал, подписался на рассылку, Фильмы
разные качал.

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

5.И теперь сидишь довольный: стал мгновенно знаменит!
О тебе все знают в школе! Что там в школе и в
районе, Во всем мире знаменит! От друзей секретов
нету - Это всем давно известно.

6.А теперь запомни, друг мой!
Правила не сложные: В Интернете, как и в жизни, Должен
ты всё понимать:
Информацию и фото с мамой вместе размещать.
На рассылку подписаться или мультики скачать,
Должен с нею всё решать!

7.Хочешь с мамой или с папой - это сам ты выбирай.
В Интернете, как и в жизни, **безопасность** соблюдай!

- Маша очень старалась слушать, но у неё ничего не получалось. Давайте ей ещё раз напомним о безопасностях.
- О каких правилах пользования Интернетом говорится в этом стихотворении? Какие еще советы и предложения вы могли бы сами дать своим сверстникам, чтобы их нахождение в сети Интернет было полезным и безопасным?

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

- А Маша побыстрее хочет включить компьютер, который ей подарил Мишка. Но у неё не получается. Нужен ключ к нему. А для этого необходимо ответить на вопрос. Поможем ей? Но сначала поговорим о компьютерных играх.

2.О компьютерных играх

1. Чтение стихотворения учеником

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,
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!
- Ребята, но 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.
-Что мы можем сделать, чтобы не попасть в Интернет зависимость?
(Нужно стать грамотным пользователем, осваивать полезные программы, нужно поменьше играться, а заняться спортом, общаться с друзьями, читать книги и т. п.)
Вы так хорошо работали, что Маша решила отблагодарить вас и предложила вам отдых.

V.Музыкальная пауза

Звучит песня Геннадия Гладкова из мультфильма «38 попугаев».
(Во время музыкальной паузы учащиеся выполняют движения.) Интернет - технологии стали неотъемлемой частью жизни современного человека, особенно популярны они среди детей и молодежи. Однако виртуальное пространство полно опасностей. Угрозы, хулиганство, вымогательство, неэтичное и агрессивное поведение – все это нередко можно встретить.

1.Виртуальное общение

Виртуальное общение не может заменить живой связи между людьми. Человек, погрузившийся в вымышленный мир под чужой маской, постепенно теряет свое лицо, теряет и реальных друзей, обрекая себя на одиночество.

2.Интернет-хулиганство

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

3.Вредоносные программы

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать

скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

4.Недостоверная информация

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной.

4.Онлайновое пиратство

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

5.Материалы нежелательного содержания.

К материалам нежелательного содержания относят материалы, которые распространяют идеи насилия, жестокости, ненормативную лексику. Пусть Интернет будет безопасным не 1 день, а каждый день в году, чтоб мы были уверены в своей защищенности от вредоносных программ и прочих угроз приватности!

VI. Итог урока. Рефлексия.

-А теперь подведём итоги нашего урока. У вас на столе лежат три картинки. Выберите ту, которая соответствует вашему настроению и

подпишите под ней:

- Сегодня на уроке я узнал …
- Я буду применять полученные знания на…
- Мне понравился урок …

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!

-Маша решила поблагодарить вас за работу! А на память об этом уроке она дарит каждому из вас памятку по безопасному поведению в Интернете.

ПАМЯТКА

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.

- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью. - Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате. - Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

Безопасность при хождении по сайтам и по приему электронной почты:

- Не ходите на незнакомые сайты
- Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы
- Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты
- Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи) - Никогда, никому не посылайте свой пароль
- Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

12. КИБЕРУРОК
«Гаджет – кто ты для меня?» (для 2 класса)

Цель: создать условия для развития безопасности в работе с современными электронными устройствами (гаджетами).

Задачи:

1. Образовательные: раскрыть влияние работы с ПК и гаджетами на здоровье человека.
2. Развивающие: развивать коммуникативные навыки и самооценку своей деятельности.
3. Воспитательные: формировать у детей положительные качества личности, культуры общения с ПК и гаджетами.

Планируемые результаты обучения УУД:

- **Познавательные УУД:**находить ответы на вопросы в текстах, иллюстрациях, делать выводы в результате совместной работы класса и учителя, разобрать плюсы и минусы ПК применения, разработать рекомендации по правильной работе с ними.

- **Коммуникативные УУД:** слушать и понимать речь других, уметь выражать свои мысли, доказывать свою точку зрения, договариваться, находить общее решение.
- **Личностные УУД:** самостоятельно делать выводы, умение соблюдать технику безопасности при работе с ПК, оценка собственной деятельности на уроке.
- **Регулятивные УУД:** учиться высказывать свое предположение на основе работы с иллюстрацией, контролировать свою деятельность по ходу выполнения задания и проверка правильности выполнения.

Оборудование: презентация, мультимедийный проектор. **Ход урока:**

1. **Организационный момент**. Прозвенел звонок весёлый Все готовы? Всё готово? Мы сейчас не отдыхаем, Мы работать начинаем.
2. **Мотивация обучающихся**

- О чем мы будем говорить сегодня, вы узнаете, отгадав загадки.

1. Он мелодию сыграет,
Как будильник прозвонит,
На часок-другой смолкает
— И опять заговорит. В
сумочке лежит всегда, А
молчит лишь иногда.
(мобильный телефон) (Слайд)
2. Он как маленький компьютер:
В нем есть игры, интернет.
Тонкий, легкий и удобный,
Называется... (планшет)
3. С ним мы в игры поиграем,
С ним мы тексты набираем,
Он оформит их красиво И
разложит по архивам.
Он работу нам облегчит, Связь
мгновенно обеспечит.
Он рисует и поет, В
Интернет с собой ведет.
Друг что надо! Просто супер!
Персональный наш...(компьютер) 4.
Он умен не по годам
И похож на чемодан. (ноутбук)

- Правильно сегодня мы поговорим с вами о мобильном телефоне, планшете, компьютере, ноутбуке.
- Кто знает, как назвать все эти предметы одним словом? (Гаджеты)
- Гаджеты – небольшие электронные устройства.

3. Целеполагание

- Хочу продолжить нашу беседу с хорошо знакомой нам всем ситуации.

Перемена. Все двигаются. Компания сидит, уткнувшись в телефон.

- Для чего в школе перемена? С пользой ли провели её эти ребята? - Наверно пришла пора научиться, как правильно использовать гаджеты и узнать о них больше информации.

Современные гаджеты стали частью нашей жизни. Мы так привыкли всегда быть на связи, иметь ежеминутный доступ к Интернету, всегда иметь под рукой часы, плеер, фотоаппарат, калькулятор, календарь, что уже не представляем своей жизни без них.

Не задумываемся, что порой эти современные устройства приносят нам не только пользу, но и вред.

- А вы не задумывались, какое значение имеют гаджеты для вас?
- Какова их роль в вашей жизни?
- Наш урок так и называется «Гаджет – кто ты для меня?» - Какие цели и задачи стоят перед нами?
- У кого есть собственный телефон? (компьютер или планшет) Интернет у кого подключен?
- Мы выяснили, что у всех есть мобильный телефон, компьютер или планшет. И большинство из вас пользуются интернетом.

4. Актуализация знаний.

- Вместе давайте постараемся разобраться, когда гаджеты могут быть другом и помощником? Высказываем свои мнения, кто как думает (выслушать ответы детей).

Вывод: телефон может быть другом и помощником. (Слайд)

✓ Сотовый телефон расширяет общение между людьми (звонки друзьям, родственникам, знакомым);

✓ Способствует получению информации через интернет;

✓ гарантирует безопасность (тревожная кнопка, телефон полиции, родителей, МЧС);

✓ выполняет функции фонарика, калькулятора, наручных часов, будильника, музыкального центра)

- А могут ли гаджеты быть врагом, нанести вред нам? (Выслушать ответы детей) (Слайд)

✓ Провоцирует правонарушения, такие как – кражи, оскорбления, угрозы, ложные вызовы полиции, скорой помощи, МЧС.

✓ Отрицательно влияет на здоровье.

- По отчету Парламентской ассамблеи Совета Европы после семи лет активного использования аппарата мобильной связи существенно повышается риск развития опухолей мозга. При этом под активным использованием подразумевается всего 27 минут в сутки. Некоторые российские ученые вообще пришли к выводу, что дети до 16 лет не должны ни в коем случае использовать сотовые телефоны и смартфоны, однако с ними согласны далеко не все. Например, операторы мобильной связи аргументируют безопасность сотовых телефонов тем, что Всемирная организация здоровья не может предъявить конкретных доказательств о вредном воздействии мобильных аппаратов, а сами устройства становятся все безопаснее и год от года снижают уровень электромагнитного воздействия. При этом по статистике каждый десятый пользователь мобильной связи – ребенок. - Вывод. Выслушать мнение детей.

- Ребята, а зачем вам нужны компьютеры, планшеты? Называем и аргументируем в чем польза или вред.

Высказывания детей о пользе и вреде планшета.

Физкультминутка.

Зарядка для глаз

• Жмурки. Крепко-крепко зажмурь глаза на 5 секунд, а затем открой их

• Бабочка. Поморгай глазками, как машет крыльями бабочками – быстро и легко

• Светофор. Поочерёдно закрывай, то левый, то правый глаз, как мигает железнодорожный светофор

• Вверх-вниз. Посмотри сначала вверх, затем вниз, не наклоняя головы

• Часики. Пусть глаза смотрят то вправо, то влево, как часики: "тик-так".

• Массаж. Закрой веки и аккуратно помассируй глаза пальчиками.

Работа по теме урока (продолжение)

- Исследователи из российского центра электромагнитной безопасности утверждают, что электромагнитное излучение от современных коммуникационных устройств оказывает негативное влияние на центральную нервную систему. Причем наиболее подвержен именно детский организм. Анализ групп школьников показал, что дети, регулярно использующие планшеты и смартфоны, отличаются рассеянным вниманием и снижением коэффициента развития интеллекта. Российские санитарные нормы не рекомендуют детям использовать гаджеты с высокочастотным электромагнитным излучением: телефоны, смартфоны, планшеты.

Помимо вреда от непосредственного излучения существуют и дополнительные ***факторы вреда здоровью*** от активного применения планшетов и других подобных устройств:

✓ у детей часами проводящими за сенсорным экраном начинаются проблемы с координацией действий между командами головного мозга и движениями рук. Наблюдались случаи, когда такие ребята не могут даже кинуть мяч по прямой линии, поскольку верхние конечности неадекватно реагируют на сигналы из головы; (Слайд)

✓ постоянное вглядывание в небольшие объекты на экранах смартфонов и планшетов развивает близорукость (особенно у тех, кто близко подносят экран к глазам), а сухость напряженных глаз может приводить к их воспалению и инфицированию; (Слайд)

✓ регулярное применение планшетов и смартфонов вредно для позвоночника (особенно шейного отдела), который у детей еще имеет податливую структуру и быстро искривляется; (Слайд)

- Вывод: телефон, компьютер, интернет могут быть нашим другом, помощником, а также, к сожалению, - и врагом. (Слайд)
- Чтобы современные гаджеты были только нашими друзьями, помощниками, что же нам необходимо делать? (Выслушать высказывания детей)
- Да, ребята, нам необходимо разработать рекомендации по правильной работе с ними и не забывать их выполнять: (Слайд)

Правила пользования мобильным телефоном

1. Чем короче разговор, тем безопаснее для здоровья.
2. Старайтесь носить телефон как можно дальше от жизненно важных органов. Рекомендуется носить телефон в сумке, портфеле, а не в кармане, так как даже в режиме ожидания он продолжает обмениваться данными с сетью.
3. Старайтесь не разговаривать в закрытом пространстве (автомобиле, лифте, поезде, гараже и др.).
4. Не пользуйтесь мобильным телефоном во время грозы. Вероятность попадания молнии в работающий телефон в несколько раз выше попадания в человека.
5. Не пользуйтесь мобильным телефоном во время пересечения проезжей части и управлении транспортным средством.
6. Правило этики: уважайте других людей – выключайте телефон или, по крайней мере, не разговаривайте по телефону в общественных местах и транспорте.

Вывод: мобильный телефон будет нашим помощником, если выполнять эти правила.

- И в конце нашего классного часа мы посмотрим небольшой мультфильм «Смешарики» о Мобильном этикете!

Каждому обучающемуся раздаётся памятка с мобильным этикетом. - Не забудьте поделиться новой информацией со своими близкими и друзьями.

Подведение итогов занятия. Рефлексия.

- Давайте подведем итоги нашего занятия.

Гаджеты – часть нашей жизни. Все-таки они друзья или враги? Обратите внимание на доску. (Доска разделена на 2 части. На одной половине написано – *друг,* на другой – *враг.)*

(Детям раздаются макеты телефонов)

- Прикрепите свои макеты телефонов к той колонке (*друг* или *враг*), какое отношение к телефону вы выбираете. Результат очевиден.
- Что нового для себя вы сегодня узнали?
- Информация была для вас полезной?
- Станете ли вы меньше пользоваться мобильным телефоном, планшетом?
- А что ещё вы хотели бы узнать по этой теме?
- Наше занятие окончено. Всем спасибо. **Список использованной литературы:**

1. Журнал «Счастливые родители» статья «Ребенок и современные гаджеты»
2. Сайт журнала "Здоровье": http://zdr.ru/articles/elektronnue_deti Электронные дети
3. http://shkolazhizni.ru/archive/0/n-34786/ Гаджеты. Что это такое?
4. http://mama.ru/articles/gadzhety-dlya-detei-za-i-protiv Развивающие игры и игрушки
5. http://www.artofcare.ru/top/6665.html Дети и электронные гаджеты: Кто кого?
6. http://www.detiburg.ru/news/health/6148/ Дети и гаджеты: отнять нельзя разрешить – где поставить запятую?
7. http://www.ug.ru/article/676 Дети и гаджеты: спасение или искушение?
8. https://www.youtube.com/watch?v=TfvZN0oBvVg мультфильм «Смешарики» о Мобильном этикете!

Приложение

Правила пользования мобильным телефоном

1. Чем короче разговор, тем безопаснее для здоровья.
2. Старайтесь носить телефон как можно дальше от жизненно важных органов. Рекомендуется носить телефон в сумке, портфеле, а не в кармане, так как даже в режиме ожидания он продолжает обмениваться данными с сетью.
3. Старайтесь не разговаривать в закрытом пространстве (автомобиле, лифте, поезде, гараже и др.).
4. Не пользуйтесь мобильным телефоном во время грозы. Вероятность попадания молнии в работающий телефон в несколько раз выше попадания в человека.
5. Не пользуйтесь мобильным телефоном во время пересечения проезжей части и управлении транспортным средством.
6. Правило этики: уважайте других людей – выключайте телефон или, по крайней мере, не разговаривайте по телефону в общественных местах и транспорте.

Вывод: мобильный телефон будет нашим помощником, если выполнять эти правила.


14 57

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 3-Х КЛАССОВ

13. КИБЕРУРОК
«Как Даша подарком воспользовалась» (для 3 класса)

Цель: обучение детей правильно оценивать свои и чужие поступки.

Задачи:

1. повысить уровень знаний учащихся о возможностях использования сети Интернет: получение интересной и полезной информации, общение и коммуникация.
2. повысить уровень знаний учащихся об основных опасностях при использовании сети интернет.
3. усвоение детьми правил безопасного использования интернета.
4. повысить уровень осведомленности о возможностях решения неприятных и опасных ситуаций, возникающих в интернете.
5. сформировать систему действий и способов принятия решения при столкновении с неприятными и опасными ситуациями

Ход киберурока:

Чтение и обсуждение истории

Учитель: Здравствуйте, ребята. Послушайте реальную историю «Как Даша подарком воспользовалась» и подумайте, о чем мы сегодня будем говорить на занятии. **Учитель читает историю.**

Сегодня я расскажу вам реальную историю про маленькую девочку Дашу.

Жила девочка Даша, и она очень хотела на Новый год компьютер, но пользоваться компьютером Даша не умела. Наконец Дарья дождалась подарка. Компьютер был черного цвета и очень большой. Как-то раз Даша решила зайти с компьютера на страницу в контакте. Зашла, почитала новости, посмотрела фотографии подружек. Подружка Нина была в сети, и Даше захотелось с ней пообщаться. Девочки начали свой разговор смайликами. Даша удивилась, как Нина отправляет такие красивые и необычные смайлики. Даша спросила у Нины: «Как ты, отправляешь такие смайлики?». Нина быстро ответила: «Родители купили». Даше не понравилось, что Нине купили такие милые смайлики, а ей нет. Даша зашла на страницу, где продавались смайлики, и нажала на кнопку «Купить». Чуть позже высветилась таблица, на ней было написано: «Укажите номер своего телефона». И много другой информации» запрашивали, но Даша ничего читать не стала, а просто написала номер своего телефона и начала ждать, когда у неё будут такие смайлики. Даше на телефон пришло смс сообщение: «Вы купили смайлики. Спасибо за покупку!». Через некоторое время Даше

пишет мама смс сообщение: «Ты уже дома?» Даша только начинает отправлять сообщение, а ей высвечивается сообщение: «Недостаточно средств на телефоне». Вечером приходит мама и спрашивает: «Почему ты не ответила на смс сообщение?». Даша отвечает: «Потому что у меня нет денег на телефоне». Мама удивилась: «Так я тебе вчера только деньги на телефон положила!». Даша опустила глаза и рассказала, что случилось.
Больше Даша никогда без разрешения взрослых ничего не покупала!

Завершение занятия

Вопросы для обсуждения:

- Сравните поступок Даши после покупки компьютера?
- Как отнеслась мама к поведению дочери?
- Нина могла остановить каким-образом Дашу?

Дети обсуждают варианты поведения в этой ситуации.

Подведение итогов

Учитель еще раз акцентирует внимание детей на ситуации, рассмотренной на классном часе, делает выводы:

1. Слушаться взрослых.
2. Совершать покупки могут только взрослые члены семьи.
3. Игры на компьютере, планшете, в телефоне должны быть дозированными по времени.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010. 2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод. руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Управителева Л.В. Классные часы по нравственному воспитанию в начальной школе. Ярославль, академия развития,2009 - 192с.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или

объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. https://teremok-1.tvoysadik.ru/site/pub?id=219
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. https://inform183.jimdofree.com/творчество/безопасное-использованиесети-интернет-сказки/

14. КИБЕРУРОК

«Безопасность в интернете. Зачем нам Интернет? Правила поведения во «Всемирной пацтине» (для 3 класса)

Цель: рассказать о пользе Интернета и о правилах поведения во «Всемирной паутине».

Задачи:

1. обобщение знаний детей по теме «Возможности Интернета», сформулировать правила безопасного поведения в Интернете; 2. развитие логического мышления при оценке жизненных ситуаций;
3. воспитание навыков безопасного поведения.

Оборудование: листы бумаги, карандаши, краски, пластилин.

Ход киберурока:

Вступительное слово учителя

Здравствуйте, ребята. Сегодня мы поговорим с вами про Интернет. Интернет – огромная информационная система на планете Земля. Её ещё называют «Всемирная паутина». Как вы думаете, почему? (Она, как паук, связывает между собой все города мира, всех людей мира.)

-Кто из вас заходил хотя бы раз в интернет? Для чего нужен Интернет? Что в нём есть интересного и полезного? (ответы детей)

Творческая работа «Интернет - всемирная паутина»

Учитель: Ребята, а сейчас я вам предлагаю подумать и представить нарисовать интернет – всемирную паутину.

А затем попробуйте это выразить при помощи бумаги, красок, пластилина, пантомимы, звуков или танца.

Дети в течение дести минут работают самостоятельно.

Учитель: Лучше разобраться в том, что происходит в интернете, узнать, что в нем имеется интересного и полезного, а также опасного и неприятного, помогут нам наши герои – Интернешка и Дикуля!

Интернешка родился и прожил всю жизнь в интернете. Он все-все про него знает. А так как он очень добрый, веселый и верный товарищ, то всегда готов прийти на помощь своему другу Дику. Дик – щенок, он стал пользоваться интернетом совсем недавно, после того, как родители подарили ему компьютер. Дику все интересно, но он пока еще не очень

хорошо разбирается в интернете, поэтому ему нужен помощник, чтобы не попадать в неприятные ситуации.

И, конечно, Интернешка расскажет своему другу Дикули о том, сколько всего полезного, важного и интересного есть в интернете! **Интернешка:**

Где найти подружку Олю?
Прочитать, что было в школе?
И узнать про все на свете?
Ну, конечно, в
ИНТЕРНЕТЕ! Там музеи,
книги, игры, Музыка, живые
тигры! Можно все, друзья,
найти В этой сказочной сети.

Учитель: Ребята, вот сайты, на которые можно совершенно безопасно заходить. Здесь много разной полезной и интересной информации: http://www.newart.ru/, www.lukoshko.net, http://www.classmag.ru, http://otlichnyk.ru, http://www.gogul.tv/. Все эти и другие сайты можно найти с помощью поисковой системы. Вы уже пользовался поиском в интернете? Что искали? А теперь послушаем, что Интернешка рассказал Дикули.

Интернешка:

Как не сбиться нам с пути?
Где и что в сети найти? Нам
поможет непременно
Поисковая система.
Ей задай любой вопрос,
Все, что интересно, –
Вмиг ответ она найдет
И покажет честно.
В интернете, в интернете
Пруд пруди всего на свете!
Здесь мы можем
поучиться, Быстро текст
перевести, А в онлайн-
библиотеке Книжку
нужную найти!

Учитель: Однажды друзья Дика поехали проведать своих дальних родственников, он очень расстроился, так как знал, что будет очень скучать без своих друзей... И рассказал о своей беде Интернешке. Что же ему ответил Интернешка? **Интернешка:**

Расстоянья интернету
Совершенно не страшны.
За секунду он доставит
Сообщенье хоть с Луны.
Не печалься, если вдруг
Далеко уехал друг.
Подключаешь интернет –
Расстоянья больше нет!
Электронное письмо Вмиг
домчится до него. Ну, а
видеозвонок
Сократит разлуки срок.

Учитель: Но не все так гладко и хорошо бывает в этой мировой паутине! В интернете может быть интересно и безопасно. Но для этого нужно знать несколько главных правил. И сегодня на уроке мы познакомимся с ними. Они научат нас делать так, чтобы в интернете с нами ничего плохого не случилось!

Интернешка:
Мы хотим, чтоб интернет Был
вам другом много лет! Будешь
знать семь правил этих – Смело
плавай в интернете!

Учитель: Дикуля много времени проводит в интернете и с ним постоянно случаются разные истории. Послушайте одну из них:

Перед днем рождения своей мамы Дикуля никак не мог придумать, что же ей подарить. Он набрал фразу «подарок для мамы» в поисковике и увидел много интересных сайтов, предлагающих подарки, которые можно оплатить с телефона. Дикуля решил отправить смс-ку! Он сразу же это сделал и очень радовался своей находчивости. Но никакого подарка не получил, а на его телефоне закончились все деньги, и он не мог никому позвонить! Расстроенный Дикуля обратился за помощью к Интернешке.

Интернешка:
Иногда тебе в сети
Вдруг встречаются вруны.
Обещают все на свете
Подарить бесплатно
детям: Телефон, щенка,
айпод И поездку на
курорт.

Их условия не сложны:
SMS отправить можно
С телефона папы, мамы –
И уже ты на Багамах. Ты
мошенникам не верь,
Информацию проверь.
Если рвутся предложить,
То обманом может быть.

Учитель: Да, грустно, что Дика обманули. Но зато и мы с вами, и Дикуля теперь знаем, что надо быть очень осторожными. А что же с подарком для мамы Дикули? Не волнуйтесь, все закончилось хорошо. Интернешка помог Дикули с помощью графической программы нарисовать красивую картинку, куда они вставили мамину фотографию. Они распечатали рисунок на принтере и повесили в красивой рамке на стену. Мама была очень рада!

А вот другая история. Однажды Дикуля делал домашнее задание. Для этого ему надо было разыскать несколько стихотворений и выучить их. Он решил быстро найти их в интернете, переходя по ссылкам с одного сайта на другой. И вдруг что-то начало происходить с компьютером! Компьютер абсолютно перестал слушаться Дикулю. Щенок растерялся и обратился за помощью к Интернешке. Интернешка помог Дикули установить две волшебные программы: антивирус и родительский контроль. Это такие программы, которые мешают вирусам и плохой информации проникать в ваш компьютер.

Интернешка: Вдруг
из щели между строк
Вылезает червячок.
Безобидный он на вид, Но
в себе беду таит.
Может файлы он стирать,
Может деньги воровать,
Предлагает нам обновки,
Вирус – мастер маскировки!
Не хочу попасть в беду,
Антивирус заведу!

Учитель: Дикуля очень общительный и хочет, чтобы у него было много друзей. Однажды он завел себе профиль в сети «Пес-Коннект», где рассказал о своих увлечениях и что ищет себе друзей, и стал ждать писем. И вот какое письмо он получил! Давайте я вам его прочитаю.

«Привет, Дикуля. Я Большая Белая и Пушистая Мальтийская болонка. У меня совсем мало друзей, поэтому я очень хочу познакомиться и подружиться с тобой. Пришли мне, пожалуйста, свой адрес и номер школы, в которой ты учишься. Я очень хочу посмотреть на тебя, поэтому пришли мне еще свою фотографию и фотографию своей семьи. С наилучшими пожеланиями, твой новый друг – Мальтийская болонка».

Как вы думаете, ребята, как надо Дикули отвечать на это письмо? Что может с ним случиться, если он исполнит все просьбы Мальтийской болонки? А давайте спросим Интернешку.

Интернешка:

В интернете, как и в мире,
Есть и добрые, и злые.
Полон разных он людей,
Есть и гений, и злодей. По
портрету не поймешь, От
кого слезу прольешь.
Чтобы вор к нам не
пришел,
И чужой нас не нашел,
Телефон свой, адрес, фото
В интернет не помещай И
чужим не сообщай.

Учитель: Сейчас я вам расскажу продолжение истории про Дикулю и Мальтийскую болонку. Дикуля отправил Мальтийской болонке письмо и все, что она его просила. В ответ болонка начала посылать ему письма, где Дика называла глупым псом, комком шерсти и т. д. Также Мальтийская болонка стала использовать фотографию Дика, представляясь от его имени и знакомясь с другими собаками, и обижать их. Дикуля очень расстроился и попросил Интернешку помочь ему. Интернешка помогает Дикули: он пересылает грубые письма администратору сайта, который блокирует адрес Мальтийской болонки, и Дикуля больше не получает плохих писем. Какое же правило на этот раз нам расскажет Интернешка?

Интернешка: В
интернете злые тролли
Появляются порой.
Эти злюки-задаваки Могут
довести до драки. Им дразнить
людей прикольно, Несмотря,
что это больно. Только полный

их «игнор» Тролля охладит
задор.
Сам же вежлив оставайся, В
тролля ты не превращайся!

Учитель: Ребята, нужно не только не давать информацию о себе чужим людям, но и не встречаться с незнакомцами. Какое правило про эту ситуацию расскажет нам Интернешка?

Интернешка:

Как всем детям интересно
Поиграть с друзьями вместе, В
интернете тоже можно, Нужно
быть лишь осторожным.
И с чужими не играть,
В гости их к себе не звать
И самим не приходить –
Я прошу вас не забыть.

Учитель: Ребята, а было у вас такое, что вы ищете что-то нужное в интернете, а на компьютере появляется совсем не то? А как вы думаете, что надо делать, чтобы этого не случилось? Давайте спросим у Интернешки!

Интернешка:

В интернете сайты есть – Невозможно
глаз отвесть.
Там и игры, и мультфильмы,
И учеба, и кино,
Только вдруг ты там находишь Иногда
совсем не то...
Чтобы не перепугаться И
потом не огорчаться,
Надо фильтр поискать И
компьютер подковать!
Ты родителям скажи:
Фильтры тут всегда нужны!

Учитель: Ребята, а что все-таки делать, если вы встретились с какойто трудностью в интернете: например, к вам пробрался вирус, или вас ктото обижает, или вы отправили SMS на незнакомый номер?

Вы должны обратиться к вашим родителям или учителям! Они могут взять в помощь себе и вам разные компьютерные программы, они всегда помогут решить проблему и защитят от неприятностей! Интернешка все про это знает!

Интернешка:

Если что-то непонятно, Страшно
или неприятно – Быстро к
взрослым поспеши, Расскажи и
покажи.
Есть проблемы в интернете?
Вместе взрослые и дети
Могут все решить всегда
Без особого труда.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного об интернете, о его возможностях и опасностях, о том, какие правила нужно соблюдать, чтобы все было хорошо. Про что эти правила? Сколько их? Какие правила вы запомнили?

Настало время прощаться! Сегодня вы узнали основные правила поведения в интернете! Надеюсь, вы запомните их!

Подведение итогов

Учитель анализирует с ребятами результаты творческих рисунков, работ из пластилина и предлагает организовать в классе небольшую выставку из работ.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55. 4. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И.

Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. Азбука безопасности. В Интернете http://azbez.com/safety/internet
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасность детей в Интернете
5. http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
6. Копилочка активных методов обучения
7. http://www.moi-universitet.ru/ebooks/kamo/kamo/
8. Материалы сайта «Интернешка» http://interneshka.net/, http://www.oszone.net/6213/
9. Материалы викторины «Безопасность детей в сети интернет http://videouroki.net

15. КИБЕРУРОК «Я и мой компьютер» (для 3 класса) 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 киберурока:

1. 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
сканер	до	думает	и	печать
не	компьютер	кормит	бумага	а
человек	но	шифр	решает	принтер

«Компьютер решает, а человек думает»

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

Оглянись, дружок, вокруг! Вот… - верный друг. Он всегда тебе поможет: Сложит, вычтет и умножит. *(компьютер)*	Наверху машины всей .Размещается… - Словно смелый капитан! А на нем горит … *(дисплей, экран)*	Ну а рядом главный блок: Там бежит электроток К самым важным микросхемам. Этот блок зовут … *(системным)*
Это вот - … Вот где пальцам физкультура И гимнастика нужны! Пальцы прыгать там должны! *(клавиатура)*	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)*	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)*
Сетевая паутина Оплела весь белый свет, Не пройти детишкам мимо. Что же это? *(интернет)*		

Дети называют, показывают предметы, определяют их предназначение.

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.

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.

16. КИБЕРУРОК
«Безопасность в сети Интернет» (3 класс)

Цель: познакомить детей с правилами ответственного и безопасного поведения в современной информационной среде. **Задачи:**

- расширить представление детей об интернете;
- формировать основы коммуникативной грамотности, чувства ответственности за своё поведение;
- сформировать у учащихся понятия о принципах безопасного поведения в сети Интернет;
- обеспечить информационную безопасность ребенка при обращении к ресурсам Интернет; воспитывать внимательное отношение к информационным ресурсам.

Ход киберурока. 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, (*Интернет*)

- Для чего нужен интернет?

Интернет – это информационная система, которая стала одним из важнейших изобретений человека.

Интернет - это всемирная электронная сеть информации, которая соединяет всех владельцев компьютеров, подключенных к этой сети. Получив доступ к сети, можно сделать многое.

При помощи Интернета можно связаться с человеком, который находится вдалеке от вас, вы можете переписываться с ним при помощи электронной почты, общаться с ним в «чатах» и даже видеть своего собеседника. Это очень интересно.

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.

Сегодня мы с вами поговорим об Интернете. Тема нашего классного часа «Безопасность в интернете».

Чтобы Интернет стал нам настоящим другом и приносил только пользу и радость, нужно знать несколько несложных, но очень важных правил.

Самое главное правило пользователя Интернета

- Будь внимателен и осторожен!

1 правило: Спрашивай взрослых.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

«Если что-то непонятно
страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.»

2 правило: Антивирус-ваш друг!

Выберите любой антивирус для компьютера, планшета, телефона (платный, бесплатный. Главное, чтобы он был всегда включен. «Не хочу попасть в беду — Антивирус заведу!
Всем, кто ходит в Интернет,
Пригодится наш совет.»

3 правило: Пусть пароли будут сложными и разными!

Простой пароль взломают легко мошенники, для каждого ресурса-свой пароль. Все гаджеты, которые можете потерять защитите графическим ключом или отпечатком пальца.

4 правило: Установи фильтр. (защита от СПАМ*)*

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

«Как и всюду на планете, Есть
опасность в Интернете.
Мы опасность исключаем,
Если фильтры подключаем.»

5 правило: Ни слова о слове СКАЧАТЬ! Не открывай файлы. Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Слово скачать- самый верный способ подцепить вредоносную программу. Опаснее только Скачать бесплатно! Не знаете, что за файл вам прислали? Он необычный или пришёл из неожиданного источника? Удалить!

6 правило: Не спеши отправлять SMS.

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс — не спеши! Сначала проверь этот номер в интернете — безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

«Иногда тебе в Сети Вдруг
встречаются вруны. Ты
мошенникам не верь,
Информацию проверь!»

7 правило: Осторожно с незнакомыми.

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду. «Злые люди в Интернете Расставляют свои сети.
С незнакомыми людьми
Ты на встречу не иди!»

8 правило: Будь дружелюбен.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать. «С грубиянами в Сети Разговор не заводи. Ну и сам не оплошай —
Никого не обижай.»

9 правило: Не рассказывай о себе.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

«Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото
В интернет не помещай
И другим не сообщай.»

10 правило: ВАЙ фай может быть лазейкой мошенников! Не подключайтесь к сети вай-фай в публичных местах: кафе, вокзалах, на улице.

А теперь попробуем сформулировать эти простые правила, опираясь на всем известные фразы из сказок. **Повернись избушка, ко мне передом, 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 - и вам, и другим людям. **Не пей из болотца! Козленочком станешь!**

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 нас от негативных эмоций, а наш компьютер – от вирусов, "червяков" и другого вредоносного программного обеспечения.

Волку дверь не открывайте!

Создатели Интернет позаботились о том, чтобы мы были защищены от тех, кто хочет причинить нам какой-либо вред. У них ничего не получится, если только мы сами не откроем им дверь – не сообщим им наши пароли или другую важную информацию, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям. Но ведь именно так мы поступаем в обычной жизни, когда сначала спрашиваем: "Кто там?", а только потом открываем дверь! Следуй этим правилам каждый раз, когда «выходишь» в Интернет!

Наш классный час подходит к концу. 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!

Рефлексия.

«Продолжи предложение»:

- сегодня я узнал…
- было интересно…
- меня удивило…
- я понял, что…

17. КИБЕРУРОК «В мире гаджетов» (для 3-4 класса)

Цель и задачи урока:

- расширять знания учащихся о компьютере, показать вред и пользу компьютера;
- формировать навыки организации безопасного взаимодействия с гаджетами; познакомить со средствами профилактики вредного воздействия компьютера на человека;
- осуществлять профилактику психологической зависимости от компьютера.

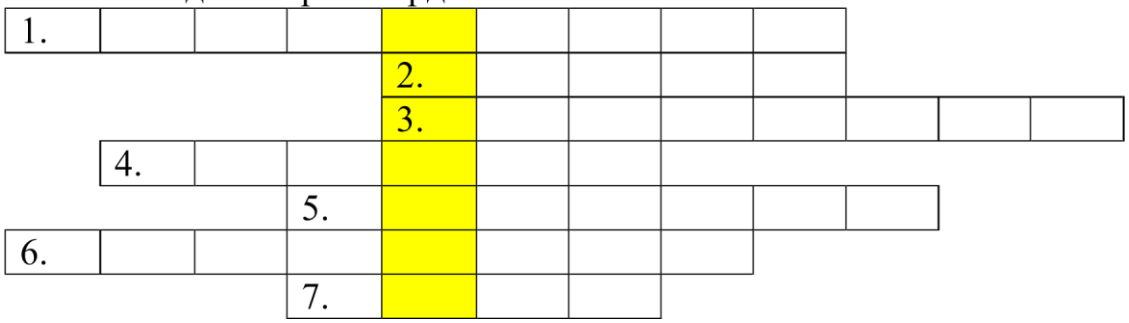
Оборудование: презентация, мультимедиапроектор, памятка по использованию компьютера в домашних условиях.

Ход урока:

I. Организационный момент. Прозвенел звонок веселый.
Мы начать урок готовы.
Будем слушать, рассуждать,
И друг другу помогать.

II. Актуализация знаний учащихся.

1. Разгадайте кроссворд:



1. Этот предмет избавит от бед, Если вдруг вы заблудились Или с пути внезапно сбились. Он даст верный вам совет,

Верен ваш маршрут иль нет,
Оптимальный путь подскажет,
Расстояние укажет.
Стрелка вправо-влево -вверх – Это компас?

Вовсе нет.
Это чудо оператор –
Или просто
(**навигатор.)**

2. Много игр в нём, песен разных, Так же много функций в нём.
Он хороший, клёвый, классный!
А зовут его.... **(айфон)**

3. Если я в игру играю,
То на кнопки нажимаю.
Кнопки, рычаги и хвостик... Догадались?
Это... **(джойстик)**

4. Можно выбросить шкафы, где на полках пыльных,
Строем книжечки стоят в переплётах стильных,
Для жилья освободить метражи законные, Ведь
подарок для тебя – … **(книжка)** электронная!

5. Он мелодию сыграет,
Как будильник прозвонит,
На часок-другой смолкает
– И опять заговорит. В
сумочке лежит всегда, А
молчит лишь иногда.
(Мобильный **телефон)**

6. У меня есть друг карманный, И красивый, и желанный.
С ним, я честно признаюсь, Никогда не расстаюсь.
С ним – беда – мне не беда.
Он поможет мне всегда. И
в любое время года С ним
– невзгоды – ерунда. Все,
что нужно, прочитаю От
него секретов нет Он
всегда мне даст совет.
Если вдруг беда нагрянет

Одиноко вдруг мне станет,
Только пальцем проведи-
Он со мной поговорит.
В жизни он – не заменимый.
Кто же этот друг любимый? **(Смартфон)**
7. Бегает по коврику, Курсором
управляет,
Нажатием на кнопку
Программы открывает. (Компьютерная **мышь)**

1.Н	А	В	И	Г	А	Т	О	р				
				2.А	Й	Ф	О	Н				
				3.Д	Ж	О	Й	С	Т	И	К	
	4.К	Н	И	Ж	К	А						
			5.Т	Е	Л	Е	Ф	О	Н			
6.С	М	А	Р	Т	Ф	О	Н					
			7.м	Ы	Ш	Ь						

Прочитаем получившееся по вертикали слово.
Что получилось?
Что обозначает слово гаджет?

III. Сообщение темы занятия.

Ещё несколько десятков лет назад компьютер был диковинкой, а сегодня он стал доступен обычной семье.
У кого дома есть компьютер?
Кто им пользуется?
А как вы используете компьютер?
Каждое современное предприятие внедряет компьютерные технологии в производственный процесс.
Где вы видели компьютер? (в авиа и железнодорожных кассах, магазинах, поликлинике, на работе у родителей).
В нашем быстро развивающемся обществе каждый день появляются новые приспособления, которые способны облегчить жизнь человека. Их называют гаджеты. Появление гаджетов сильно повлияло на наш мир.Сегодня мы выясним: что такое гаджеты, приносят они человеку пользу или вред, как обезопасить себя при работе с гаджетами.

IV.Работа по теме занятия.

1. Поиск в словаре значения слова гаджет.

Слово «гаджет» пришло к нам от английского «gadget», переводится как «прибор, приспособление». Это - небольшие электронные устройства, которые за последние несколько лет проникли чуть ли не во все сферы нашей жизни. Они слышат, видят, поют, рассказывают, используются как аксессуары к персональному компьютеру, смартфону или другим приспособлениям. Новейшие гаджеты служат как для решения деловых вопросов, так и в целях развлечения. Они могут работать и как самостоятельные устройства, и как приложения к различному оборудованию.

Другие значения слова «гаджет»

Термин «гаджет» имеет и другие значения. Например, гаджетом была названа в свое время первая атомная бомба. В литературе это слово встречается чаще всего в шпионских кинофильмах (сериал о Джеймсе Бонде). Любители мультфильмов могут вспомнить Инспектора Гаджета, сила которого заключается в наборе гаджетов. В начале 20 века гаджетами в английском флоте моряки называли все технические устройства, названия которых они не запомнили, не знали. С точки зрения компьютерной грамотности получается очень удобно, если «в разговоре» употреблять слово «гаджет» всякий раз, когда забыл (или не знаешь) названия нового технического устройства или названия нового приложения. Не совсем грамотно, но, может быть, иногда это лучше, чем говорить, «такая штука, названия которой не знаю ».

2. Какие гаджеты знаете вы? (Высказывания учащихся)

В настоящее время к гаджетам относят любые цифровые аппараты, размеры которых позволяют подсоединить их к персональному компьютеру, смартфону или надеть на руку. Гаджеты компактны и предназначены для выполнения конкретных, узкоспециализированных задач. Отличительной особенностью гаджетов является то, что они являются новинкой, то есть, необычным, креативным решением определенных задач по сравнению с имеющимися стандартными технологиями. Часто гаджеты не могут работать самостоятельно, их основная задача расширять функциональные возможности устройств, к которым они подключены.

Примеры гаджетов:

- планшет, □ iPod,
- MP3-плеер,
- электронная книга,
- цифровой фотоаппарат,
- смартфон,

- коммуникатор,
- масса полезных, а также бесполезных, шуточных, «прикольных» устройств, подключаемых к компьютеру через порт USB, и так далее. ***Смартфо́н (англ. smartphone — умный телефон) — телефон, дополненный функциональностью карманного персонального компьютера.***

Коммуникатор (англ. communicator, PDA phone) — карманный персональный компьютер, дополненный функциональностьюмобильного телефона.

USB гаджеты

Это небольшие приспособления, которые подключаются через USB-порт. Клавиатура, мышь, флешка, принтер, внешний жесткий диск все они подключаются к компьютеру, как правило, через USB.

примеры USB-гаджетов : кружка с подогревателем от USB,

- USB-пепельница, USB мини-холодильник ,
- USB-пылесос для клавиатуры от крошек и пыли,
- USB-коврик для мыши с подогревом,
- USB-коврик для ног с подогревом,
- USB-тапочки с подогревом,
- USB-подсветка для клавиатуры,
- USB-мышь на палец,
- USB-подставка для ноутбука,
- USB-вентилятор и т.д. **iPod**

iPod – небольшое устройство для прослушивания музыки и аудио-файлов в хорошем качестве. iPod предоставляет возможность не только слушать музыку, аудио-книги и аудио-кассеты, но и использовать органайзер, слушать FM-радио, смотреть видео-ролики.

Тест «Какими Вы пользуетесь гаджетами?»

- Планшет iPod
- MP3-плеер
- Электронная книга
- Цифровой фотоаппарат
- Смартфон
- Коммуникатор
- USB-гаджеты (например, USB-коврик)
- Не пользуюсь гаджетами

3. Как вы используете гаджеты? (Высказывания учащихся) Сетевая паутина оплела весь белый свет, не пройти детишкам мимо.

Что же это?

(Интернет). **Анкета**

- Кто в Вашей семье пользуется Интернетом?
- Пользуешься ли ты Интернетом? да нет
- Как долго работаешь в Интернете?
- Какие сайты посещаешь чаще всего?
- Отметь, что тебя привлекает в Интернете игры в режиме **On -line**

-возможность скачивания игр

-чтение книг

-другое

Для того что бы облегчить человеческую жизнь, люди везде используют гаджеты, которые способны помочь, но не всегда они полезны. Гаджеты есть везде! Даже при рождении ребёнка родители приобретают гаджеты, способные развивать или контролировать его, например, радио-няня.

На протяжении жизни гаджеты сменяют друг друга в зависимости от потребностей человека. Если вы собрались в путешествие на автомобиле вам поможет гаджет – GPRS-навигатор, который укажет вам путь.

4.Анкетирование. Анкета

1 Отгадайте-ка, ребятки,
Интересную загадку.
Знает все он и про всех,
Потому что в интернет
Выход нам он предлагает,
Мир огромный открывает
И друзей не забывает, -
Он для нас и телефон, И
плейстейшн и Айфон... А
какой же внешний вид -
экстерьер и габарит
Симпатичен и практичен, Он
ведь друг, и он учитель.
Знают дети с малых лет,
Что зовут его....(планшет)

Как Вы используете планшет?

1.Играю в игры

2. В образовательных целях

3.Во время путешествий

4. Просмотр ТВ, видео
5.Для связи с друзьями, семьей
6.Для чтения
7.Слушаю музыку
8. Узнаю новости

Анкета 2

Есть ли у вас гаджет-зависимость?

Перед вами 11 утверждений. Честно отметьте утверждения, которые касаются вашей жизни.

1. Телефон — это главное устройство в моей жизни. Я не представляю существования без него.
2. Я провожу со своим смартфоном много времени. Гораздо больше, чем уделяю другому занятию.
3. Я конфликтую с близкими, потому что много времени уделяю своему гаджету.
4. С каждым днем я все больше времени провожу с телефоном в руках. При этом не важно, как его использую, возможны игры, общение или чтение.
5. Мой телефон способен поднять мне настроение, когда он рядом, мне спокойнее.
6. Если я не могу пользоваться смартфоном, я начинаю нервничать.
7. Мне постоянно хочется использовать мой смартфон, при каждом удобном случае я беру его в руки.
8. У меня не получается сократить время использования. У меня постоянно появляется повод вновь взять в руки устройство.
9. Я врал окружающим людям о том, сколько времени я провел за своим телефоном.
10. Я часто откладываю важные дела, чтобы заняться чем-то не очень полезным на смартфоне.
11. Я использую телефон только при необходимости.

Если результат составил:

От 0 до 4 пунктов, то нет повода для беспокойства, у вас нет зависимости.

От 5 пунктов и более — это повод задуматься о зависимости.

К врачу стоит обращаться, если 9 из 10 пунктов соответствуют вашей жизни. Не стоит списывать частые звонки и контакты с помощью смартфона на работу. Конечно, есть профессии, которые связаны с общением, но стоит проследить, что люди часто начинают зависеть не от звонков клиентов, а от игр или регулярной проверки социальных сетей.

5. Как сохранить своё здоровье при общении с компьютером, чтобы он всегда оставался нам добрым другом и помощником и не приносил вреда?

Он быстрее человека
Перемножит два числа,
В нем сто раз библиотека
Поместиться бы смогла,
Только там открыть возможно Сто
окошек за минуту.
Угадать совсем несложно, Что
загадка про… (компьютер).

Компьютерные игры. С недавних пор это словосочетание прочно вошло в нашу жизнь, каждый, кто имеет компьютер наверняка смог почувствовать их притягательность С каждым скачком в области компьютерных технологий растет количество людей, которых в народе называют "компьютерными фанатами" или "гамерами" (от английского "game" - игра).

Основной деятельностью этих людей является игра на компьютере, круг социальных контактов у них очень узок, вся другая деятельность направлена лишь на выживание, на удовлетворение физиологических потребностей, а главное - на удовлетворение потребности в игре на компьютере. В обществе формируется целый класс людей-фанатов компьютерных игр. Общение с этими людьми показывает, что многим из них увлечение компьютером отнюдь не идет на пользу, а некоторые серьезно нуждаются в психологической помощи.

Какие необходимо соблюдать правила, работая с компьютером? ***Составление правил работы с гаджетами(компьютером).***

Обсуждение с учащимися. (Учащиеся предлагают правило, оно обрабатывается)

Правила использования компьютера (гаджета):

* Стол с компьютером следует поставить сбоку от окна так, чтобы свет падал слева, подальше от источников тепла. Хорошо, если будет присутствовать и искусственное освещение (лампа)
* В помещениях, где работают компьютеры , полезно ставить цветы и аквариумы, испаряющие воду и повышающие влажность воздуха
* Долгое сидение у монитора грозит здоровью головными болями, слезотечением, резью в глазах, снижением остроты зрения.
* Сидеть за компьютером нужно правильно: спину выпрямить, опереться на спинку кресла, плечи не опускать. Стопы упираются в пол.
* Соблюдайте правила техники безопасности при работе с компьютером.

***** Не играйте в компьютерные игры перед сном.

***** Через 20-30 минут работы на компьютере необходимо делать перерыв.

* Время работы на компьютере не более 1,5 - 2 часа в день *** Разучивание гимнастики для глаз.**

Офтальмологическая пауза или гимнастика для глаз

Закрываем мы глаза, вот какие чудеса. *(Закрывают оба глаза.)*

Наши глазки отдыхают, упражнения выполняют. *(Продолжают стоять с закрытыми глазами)*

А теперь мы их откроем, через речку мост построим.*(Открывают глаза, взглядом рисуют мост)*

Нарисуем букву о, получается легко. *(Глазами рисуют букву о)*

Вверх поднимем, глянем вниз, (*Глаза поднимают вверх, опускают вниз* Вправо, влево повернем, *(Глаза смотрят вправо- влево)*

Заниматься вновь начнем.

В зависимости от того, как мы сами ведём себя с ним, компьютер может быть хорошим и плохим, вредным и полезным. В руках знающего пользователя он совершенно безопасен — подобно тому, как дрессированный тигр рядом с опытным укротителем ведёт себя послушнее комнатной киски.

Разгадывание кроссворда.

1. Он умен не по годам И
похож на чемодан.
(Ноутбук)

2. У дисковода-папы
Под крышей - мама-плата, Но
дочки с ними не живут – У
людей нашли приют.
Умненькие дочки
Запоминают строчки,
Запоминают все, что есть,
Что может с них компьютер счесть.
Все дочки-девочки равны,
Лишь отличаются они
Объемом памяти и платьем,
И в этом девичье их счастье!
Зовут красавиц просто - Стешки, А
по компьютерному - .(флешки)

3. Нет, она – не пианино,
только клавиш в ней – не счесть!
Алфавита там картина, знаки,
цифры тоже есть.
Очень тонкая натура. Имя
ей ...(Клавиатура) .

4. Корпус компьютера. В нем
что-то хранится, Что
компьютеру пригодится. Корпус
из пластика, стали, стекла, В нем
материнская плата жила, А также
процессор, ОЗУ, дисковод...
Что это за корпус, скажите, народ? (Системный блок)

5. Думать, делать помогает,
жить компьютер заставляет
И заботлива, как мама,
Что это? - Виртуальная.. . (программа)

6. На столе он перед нами, на
него направлен взор,
подчиняется программе, носит
имя... (Монитор) .

7. Он круглый и блестящий,
С пластинкою похож,
Но меньше он, изящней, И
современней все ж.
На нем хранится много
Всего, что ты захочешь.
Вот вставишь в дисковод его,
Читаешь все, что хочешь. (Диск)

8. Столбик черный, как-то
странно, Может бегать по
экрану.
Посмотри на монитор,

Кто там бегает? (Курсор)

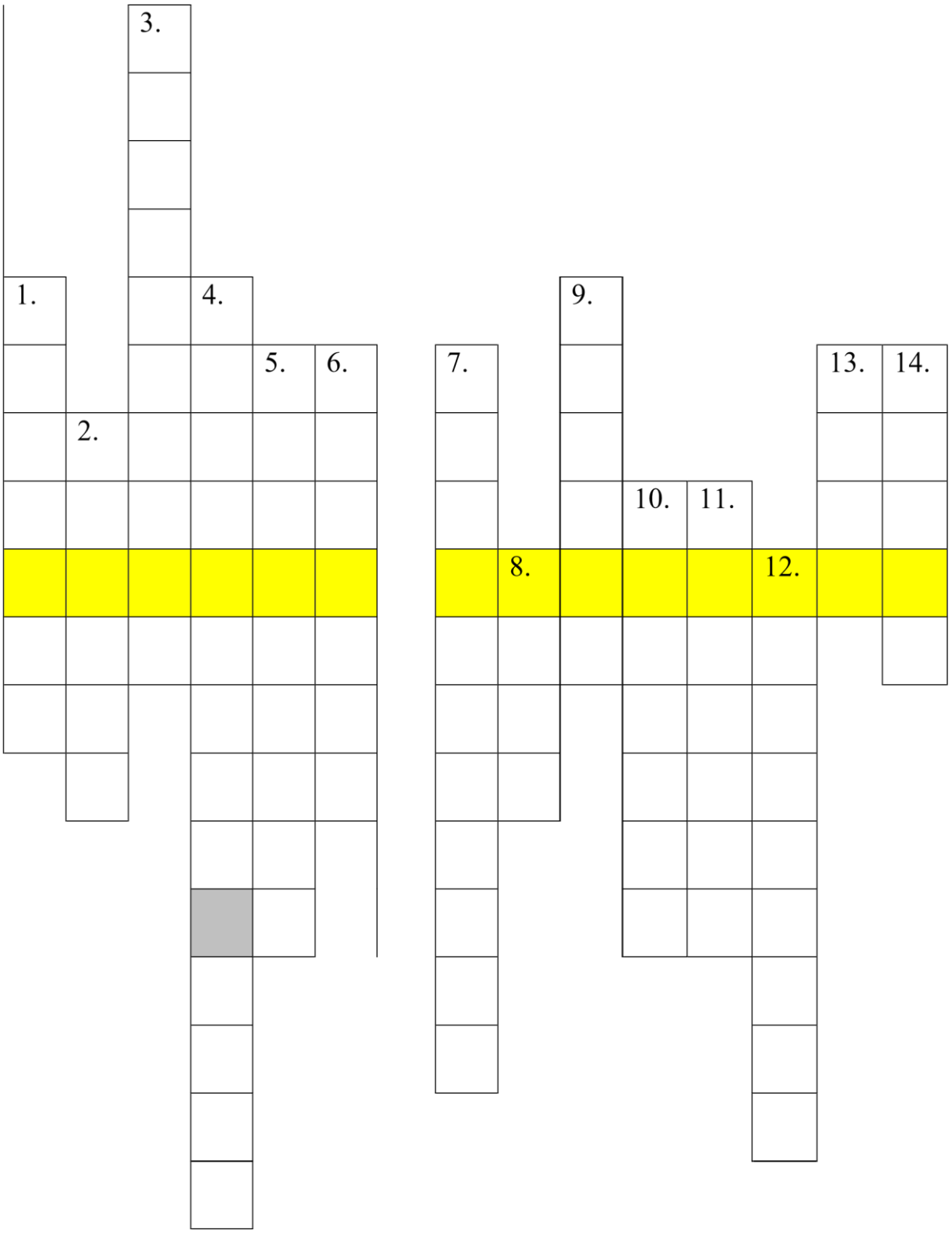
9. Бывает струйный,
лазерный бывает. Его всегда
печатать заставляют.
Он на бумагу распечатает что нужно. Печатник
этот всем нам очень нужен. (Принтер)

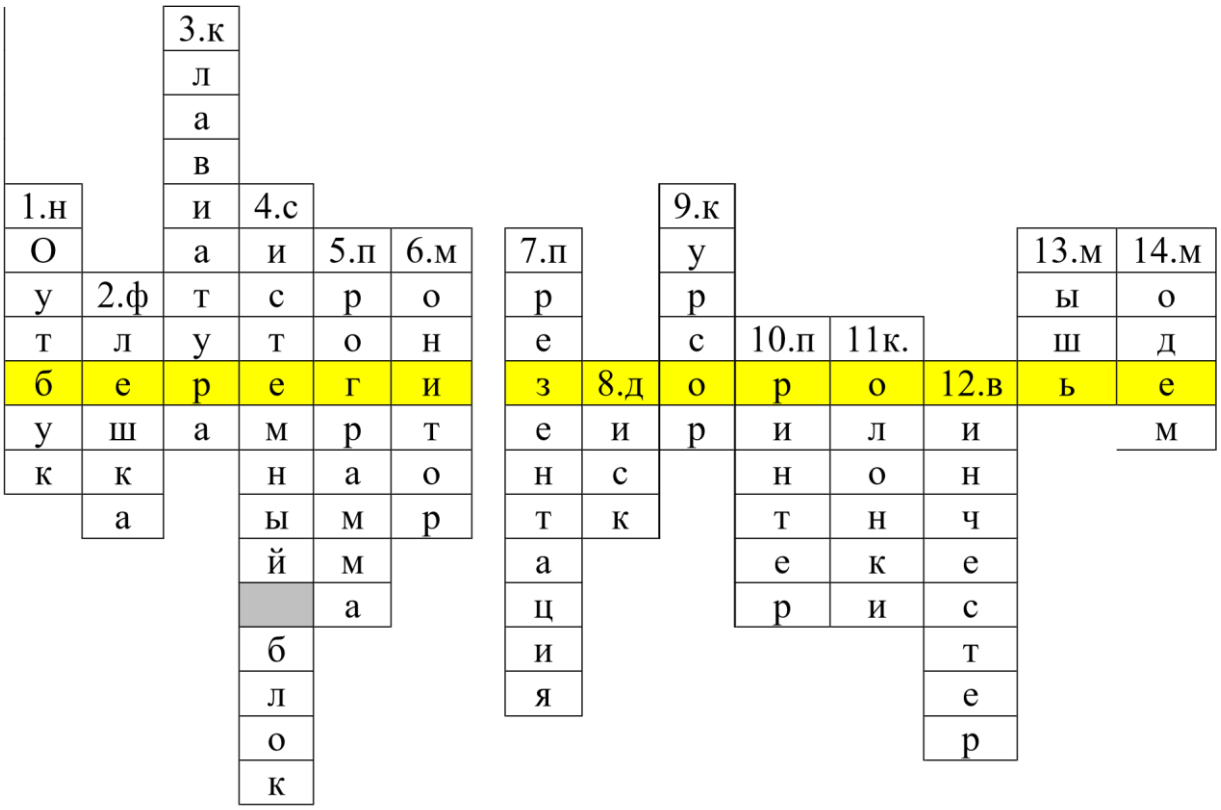
10. Если что-то отключить, То
компьютер замолчит,
Тугоухий, как медведь -
Ничего не сможет спеть (Колонки)

11. Жесткий диск так
называют. Кто название
отгадает?
Копятся данные в этом устройстве, Запоминать
— его главное свойство. (Винчестер)

12. Не зверушка, не летаешь, а
по коврику скользишь и
курсором управляешь. Ты –
компьютерная... (Мышь) .

13. С телефонами он дружен И
для связи очень нужен,
Ведь к компьютерным сетям Доступ
разрешает нам.
Там где он, там нет проблем! И
зовется он… *(Модем.)*


3.
1.
4.
9.
5.
6.
7.
13.
14.
2.
10.
11.
8.
12.



6. Выступление медсестры.

Синдромы современности

Изначально гаджеты и интернет технологии были созданы с целью облегчить, и даже улучшить нашу жизнь, экономить время, но учёные бьют тревогу. Всё больше людей заражаются новой, прежде невиданной болезнью, порожденной техническим прогрессом. Опасную болезнь, являющую собой особую форму психической и психологической зависимости, западные исследователи назвали ***гаджетоманией*** или ***гаджет- аддикцией***. Психологи детально изучают данную проблему и выделяют психологические и физиологические симптомы гаджет - аддикции. Смартфоны давно уже превратились в популярнейшие и необходимые гаджеты, которые позволяют оперативно выходить в интернет, слушать музыку, смотреть кино и читать книги, помимо совершения звонков.

Ученые предупреждают, что это может привести к нарушениям зрения, а также сильным головным болям.

Почему же компьютеры и гаджеты опасны для зрения?

Они являются источниками так называемого синего света и повреждают зрительный аппарат.

Врачи, обследующие школьников, всё чаще замечают, что у детей ухудшается слух. В ухудшении слуха виноваты так называемые наушники - затычки. Для слуха опасны как высокие, так и низкие частоты. Максимальный уровень шума, который способен выносить человек в

течение восьми часов без вреда для здоровья, - 65 децибел. Как правило, в плеере громкость - 100 децибел и больше, даже самые современные наушники не способны выдать меньше. Врачи Национального японского института физиологических наук утверждают, что чем больше слушать плеер в метро, тем хуже наш мозг начинает распознавать обычные звуки, не только в ухе, но даже в мозге происходят нейрофизиологические изменения.

Туннельный синдром, возникающий в результате частых и длительных разговоров по мобильному телефону, характеризуется болями в кисти, которые вызывают защемление нерва в запястном канале.

Синдром, условно названный *«смартфонный палец»* грозит любителям сидеть в интернете посредством мобильного телефона. Всё чаще люди начинают жаловаться на болезненность в запястье и большом пальце руки.

Гаджетомания – навязчивая потребность к приобретению электронных устройств, в которых нет необходимости. Гаджетоманы - наркоманы прогресса. Они убивают своё время, нервы и семейное благополучие, тратят большое количество денег и в итоге расплачиваются собственным здоровьем. Эта своего рода чума 21 века опасна ещё и тем, что выглядит внешне вполне безобидно и проявляет разрушительные свойства почти незаметно для окружающих.

Основными симптомами гаджет - аддикции являются: ○ хорошее самочувствие или состояние эйфории при использовании прибора

○ невозможность оторваться от прибора или от покупки новой ○ «игрушки»

○ невозможность контролировать затраты, связанные с использованием прибора

○ ощущение пустоты и депрессии без прибора или регулярного обновления гаджетов

○ пренебрежение семьёй и друзьями ○ проблемы с работой или учёбой

Гаджетомания сказывается и на физическом уровне:

○ сухость в глазах ○ разрушается психика ○ головные боли ○ бессонница

○ поражение нервных стволов правой руки, связанное с ○ перенапряжением мышц ***6.Что полезно, что вредно?*** Работа в группах.

Распределить функции на две группы.

Польза: Вред:

* вызывает интерес к новой технике

* развивает творческие способности
* полностью захватывает сознание ребёнка
* устраняет страх ребенка перед новой техникой
* отрицательно влияет на физическое развитие детей
* повышает состояние нервозности и страха при стремлении во что бы то ни стало добиться победы
* формирует психологическую готовность к овладению компьютерной грамотности
* содержание игры провоцирует проявления детской агрессии, жестокости * позволяет развивать воображение ребёнка, моделируя совершенно новые ситуации, даже из области будущего и нереального
* воспитывает внимательность, сосредоточенность
* обязывает ребёнка действовать в темпе, задаваемом программой * снижает интеллектуальную активность детей за счет развлекательного содержания игры
* позволяет лучше и быстрее освоить понятия цвета, формы, величины
* помогает овладеть чтением и письмом
* ухудшает зрение ребёнка
* способствует возникновению нарушения осанки
* развивает элементы наглядно-образного и логического мышления
* тренирует внимание и память
* развивает быстроту действий и реакций
* способствует развитию гиподинамии
* воспитывает целеустремлённость

Проверка : группы по очереди называют функцию и колонку, в которую её отнесли.

V.Итог занятия. Рефлексия Чему научились на занятии?

Что особенно отложилось в памяти? Исполнение частушек:

Мы частушки сочиняем
И всем классом их поем, На компьютере играем,
В интернете все живем.

***

Есть компьютер в нашем классе
И проектор тоже,
Презентациям и тестам

Обучить вас можем.
***
Друг компьютер или враг,
Обсуждали бурно,
Обошлось хоть и без драк,
Но многим стало дурно.
***
Стало дурно от того,
Что компьютер – это зло:
От него глаза болят,
Файлы вирусы едят.
Появляется ярлык,
Открываю его вмиг, Эх,
играть не надлежит:
Троянский вирус здесь
лежит. *** В интернете не
сиди
Целыми часами, А
то деньги убегут
С твоими, брат, мечтами. ***
В интернете я сидела,
На экран всю ночь глазела, Думала,
что пять минут,
Но дети в школу уж
идут! *** Разрешили
поиграть
Часик-два, а я – все пять!
Теперь, как крот, слепой
хожу, Дверь свою не нахожу.
***
В паутинке посидеть
Хотела пять минуточек, Но
успела поседеть –
Теперь мне не до шуточек. ***
Мы оспаривать не станем Положительный
эффект,
Разве лучше всем нам станет,
Если вход закрыт в инет?
*** В наше время в

интернете Много
информации: Сочиненья,
рефераты – Увлеченья
нации. ***
Мой компьютер – это класс,
В интернете я сейчас.
Посидел хоть и немного,
Накопал всего и много. ***
Я открыла фотошоп,
Загрузила фотку,
Пять минут работы -
И я уже красотка.
***
Если было б в старину
Это чудо-юдо,
То не знали б ничего
Мы про кризис, люди!

Рекомендация книг

Библиотекарь знакомит учащихся с представленными на выставке книгами и электронными пособиями и о возможностях их использования.

Использованная литература:

1. Википедия, свободная энциклопедия, “Всё о гаджетах”, http://ru.wikipedia.org.
2. Интернет журнал Keit, “Что такое гаджет-зависимость?”, http://keit.ru/2008_06/chto_takoe_gadzhetzavisimost.
3. Интернет журнал Здоровье, “Диагноз: гаджет-зависимость”, http://www.zdr.ru/hots /2008/05/30/diagnoz-gadzhet-zavisimost/index.html. 4. “Гаджет-аддикция. Новый вид психологической зависимости”, 5. http://www.qoop.ru/pages/5030.html. Леонтьев В.П. Компьютерная энциклопедия. М., 2002.
6. http://www.ru.all.biz/img/ru/catalog/1205886.jpeg
http://www.3ezhika.ru/mamaladushka/chitalka/stixi/pro-kompyuter-stixizagadki/
http://otkliki.by/vse-dlja-detej-detskoe-detskie/sovremennye-zagadki-dlja-detej
http://nsportal.ru/nachalnaya-shkola/raznoe/2015/06/16/chastushki-

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 4-Х КЛАССОВ

18. КИБЕРУРОК
«Как Даша подарком воспользовалась»

Цель: обучение детей правильно оценивать свои и чужие поступки.

Задачи:

1. повысить уровень знаний учащихся о возможностях использования сети Интернет: получение интересной и полезной информации, общение и коммуникация.
2. повысить уровень знаний учащихся об основных опасностях при использовании сети интернет.
3. усвоение детьми правил безопасного использования интернета.
4. повысить уровень осведомленности о возможностях решения неприятных и опасных ситуаций, возникающих в интернете.
5. сформировать систему действий и способов принятия решения при столкновении с неприятными и опасными ситуациями

Ход киберурока:

Вводная часть:

Упражнение – активатор: «БРОУНОВСКОЕ ДВИЖЕНИЕ»

Сначала участников группы просят закрыть глаза и представить, что каждый человек – маленький атом, а атомы, как известно, способны соединяться и образовывать молекулы, которые представляют собой достаточно устойчивые соединения. Далее следуют слова ведущего: «Сейчас вы откроете глаза и начнете беспорядочное движение в пространстве.

По моему сигналу (вид сигнала оговаривается) вы объединитесь в молекулы, число атомов в которых я также назову. Когда будете готовы, откройте глаза». Участники начинают свободное перемещение в пространстве и, услышав сигнал ведущего, объединяются в молекулы по 2, 3, 4, 5, 6, 7 и т.д. атомов. Подвигавшись некоторое время цельным соединением, молекулы вновь распадаются на отдельные атомы. Затем ведущий снова дает сигнал, и участники снова объединяются и т.п.

Если последним числом атомов в молекуле будет 2, то упражнение служит хорошим способом деления группы на пары для последующей работы.

Упражнение «С МИРУ ПО НИТКЕ»

Один из участников начинает рассказ «Жил бвл Интернет….», предлагая одно предложение, затем следующий по кругу добавляет к нему свое предложение, следующий – свое, и так до тех пор, пока очередь не дойдет

до начавшего. Затем кому-нибудь из группы предлагается вспомнить и рассказать все получившееся целиком. Остальные могут дополнять или поправлять рассказывающего.

Основная часть:

Чтение и обсуждение истории

Учитель: Здравствуйте, ребята. Послушайте реальную историю «Как Даша подарком воспользовалась» и подумайте, о чем мы сегодня будем говорить на занятии. **Учитель читает историю.**

Сегодня я расскажу вам реальную историю про маленькую девочку Дашу.

Жила девочка Даша, и она очень хотела на Новый год компьютер, но пользоваться компьютером Даша не умела. Наконец Дарья дождалась подарка. Компьютер был черного цвета и очень большой. Как-то раз Даша решила зайти с компьютера на страницу в контакте. Зашла, почитала новости, посмотрела фотографии подружек. Подружка Нина была в сети, и Даше захотелось с ней пообщаться. Девочки начали свой разговор смайликами. Даша удивилась, как Нина отправляет такие красивые и необычные смайлики. Даша спросила у Нины: «Как ты, отправляешь такие смайлики?». Нина быстро ответила: «Родители купили». Даше не понравилось, что Нине купили такие милые смайлики, а ей нет. Даша зашла на страницу, где продавались смайлики, и нажала на кнопку «Купить». Чуть позже высветилась таблица, на ней было написано: «Укажите номер своего телефона». И много другой информации» запрашивали, но Даша ничего читать не стала, а просто написала номер своего телефона и начала ждать, когда у неё будут такие смайлики. Даше на телефон пришло смс сообщение: «Вы купили смайлики. Спасибо за покупку!». Через некоторое время Даше пишет мама смс сообщение: «Ты уже дома?» Даша только начинает отправлять сообщение, а ей высвечивается сообщение: «Недостаточно средств на телефоне». Вечером приходит мама и спрашивает: «Почему ты не ответила на смс сообщение?». Даша отвечает: «Потому что у меня нет денег на телефоне». Мама удивилась: «Так я тебе вчера только деньги на телефон положила!». Даша опустила глаза и рассказала, что случилось.

Больше Даша никогда без разрешения взрослых ничего не покупала! **Завершение занятия** ***Вопросы для обсуждения:***

- Сравните поступок Даши после покупки компьютера?
- Как отнеслась мама к поведению дочери?
- Нина могла остановить каким-образом Дашу?

Дети обсуждают варианты поведения в этой ситуации.

Подведение итогов

Учитель еще раз акцентирует внимание детей на ситуации, рассмотренной на классном часе, делает выводы:

1. Слушаться взрослых.
2. Совершать покупки могут только взрослые члены семьи.
3. Игры на компьютере, планшете, в телефоне должны быть дозированными по времени.

Используемая литература:

9. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010. 10. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод. руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.

11. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
12. Управителева Л.В. Классные часы по нравственному воспитанию в начальной школе. Ярославль, академия развития,2009 - 192с.
13. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
14. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 15. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
16. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

4. https://teremok-1.tvoysadik.ru/site/pub?id=219
5. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
6. https://inform183.jimdofree.com/творчество/безопасное-использованиесети-интернет-сказки/

19. КИБЕРУРОК

«Безопасность в интернете. Интернет: вред или польза» (для 4 класса)

Цель: рассказать о пользе Интернета и о правилах поведения во «Всемирной паутине».

Задачи:

4. обобщение знаний детей по теме «Возможности Интернета», сформулировать правила безопасного поведения в Интернете; 5. развитие логического мышления при оценке жизненных ситуаций;

6. воспитание навыков безопасного поведения.

Оборудование: листы бумаги, карандаши, краски, пластилин.

Ход киберурока:

Вступительное слово учителя

Здравствуйте, ребята. Сегодня мы поговорим с вами про Интернет. Интернет – огромная информационная система на планете Земля. Её ещё называют «Всемирная паутина». Как вы думаете, почему? (Она, как паук, связывает между собой все города мира, всех людей мира.)

-Кто из вас заходил хотя бы раз в интернет? Для чего нужен Интернет? Что в нём есть интересного и полезного? (ответы детей)

Творческая работа «Интернет - всемирная паутина»

Учитель: Ребята, а сейчас я вам предлагаю подумать и представить нарисовать интернет – всемирную паутину.

А затем попробуйте это выразить при помощи бумаги, красок, пластилина, пантомимы, звуков или танца.

Дети в течение десяти минут работают самостоятельно.

Учитель: Лучше разобраться в том, что происходит в интернете, узнать, что в нем имеется интересного и полезного, а также опасного и неприятного, помогут нам наши герои – Интернешка и Дикуля!

Интернешка родился и прожил всю жизнь в интернете. Он все-все про него знает. А так как он очень добрый, веселый и верный товарищ, то всегда готов прийти на помощь своему другу Дику. Дик – щенок, он стал пользоваться интернетом совсем недавно, после того, как родители подарили ему компьютер. Дику все интересно, но он пока еще не очень хорошо разбирается в интернете, поэтому ему нужен помощник, чтобы не попадать в неприятные ситуации.

И, конечно, Интернешка расскажет своему другу Дикули о том, сколько всего полезного, важного и интересного есть в интернете!

Интернешка:

Где найти подружку Олю?
Прочитать, что было в школе?
И узнать про все на свете?
Ну, конечно, в
ИНТЕРНЕТЕ! Там музеи,
книги, игры, Музыка, живые
тигры! Можно все, друзья,
найти В этой сказочной сети.

Учитель: Ребята, вот сайты, на которые можно совершенно безопасно заходить. Здесь много разной полезной и интересной информации: http://www.newart.ru/, www.lukoshko.net, http://www.classmag.ru, http://otlichnyk.ru, http://www.gogul.tv/. Все эти и другие сайты можно найти с помощью поисковой системы. Вы уже пользовался поиском в интернете? Что искали? А теперь послушаем, что Интернешка рассказал Дикули.

Интернешка:

Как не сбиться нам с пути?
Где и что в сети найти? Нам
поможет непременно
Поисковая система.
Ей задай любой вопрос,
Все, что интересно, –
Вмиг ответ она найдет
И покажет честно.
В интернете, в интернете Пруд
пруди всего на свете!
Здесь мы можем поучиться,
Быстро текст перевести, А
в онлайн-библиотеке
Книжку нужную найти!

Учитель: Однажды друзья Дика поехали проведать своих дальних родственников, он очень расстроился, так как знал, что будет очень скучать без своих друзей... И рассказал о своей беде Интернешке. Что же ему ответил Интернешка? **Интернешка:**

Расстоянья интернету
Совершенно не страшны.
За секунду он доставит

Сообщенье хоть с Луны.
Не печалься, если вдруг
Далеко уехал друг.
Подключаешь интернет –
Расстоянья больше нет!
Электронное письмо Вмиг
домчится до него. Ну, а
видеозвонок
Сократит разлуки срок.

Учитель: Но не все так гладко и хорошо бывает в этой мировой паутине! В интернете может быть интересно и безопасно. Но для этого нужно знать несколько главных правил. И сегодня на уроке мы познакомимся с ними. Они научат нас делать так, чтобы в интернете с нами ничего плохого не случилось!

Интернешка:

Мы хотим, чтоб интернет Был
вам другом много лет! Будешь
знать семь правил этих – Смело
плавай в интернете!

Учитель: Дикуля много времени проводит в интернете и с ним постоянно случаются разные истории. Послушайте одну из них:

Перед днем рождения своей мамы Дикуля никак не мог придумать, что же ей подарить. Он набрал фразу «подарок для мамы» в поисковике и увидел много интересных сайтов, предлагающих подарки, которые можно оплатить с телефона. Дикуля решил отправить смс-ку! Он сразу же это сделал и очень радовался своей находчивости. Но никакого подарка не получил, а на его телефоне закончились все деньги, и он не мог никому позвонить! Расстроенный Дикуля обратился за помощью к Интернешке.

Интернешка:

Иногда тебе в сети
Вдруг встречаются вруны.
Обещают все на свете
Подарить бесплатно
детям: Телефон, щенка,
айпод И поездку на
курорт.
Их условия не сложны:
SMS отправить можно

С телефона папы, мамы –
И уже ты на Багамах. Ты
мошенникам не верь,
Информацию проверь.
Если рвутся предложить,
То обманом может быть.

Учитель: Да, грустно, что Дика обманули. Но зато и мы с вами, и Дикуля теперь знаем, что надо быть очень осторожными. А что же с подарком для мамы Дикули? Не волнуйтесь, все закончилось хорошо. Интернешка помог Дикули с помощью графической программы нарисовать красивую картинку, куда они вставили мамину фотографию. Они распечатали рисунок на принтере и повесили в красивой рамке на стену. Мама была очень рада!

А вот другая история. Однажды Дикуля делал домашнее задание. Для этого ему надо было разыскать несколько стихотворений и выучить их. Он решил быстро найти их в интернете, переходя по ссылкам с одного сайта на другой. И вдруг что-то начало происходить с компьютером! Компьютер абсолютно перестал слушаться Дикулю. Щенок растерялся и обратился за помощью к Интернешке. Интернешка помог Дикули установить две волшебные программы: антивирус и родительский контроль. Это такие программы, которые мешают вирусам и плохой информации проникать в ваш компьютер.

Интернешка: Вдруг
из щели между строк
Вылезает червячок.
Безобидный он на вид, Но
в себе беду таит.
Может файлы он стирать,
Может деньги воровать,
Предлагает нам обновки,
Вирус – мастер маскировки!
Не хочу попасть в беду,
Антивирус заведу!

Учитель: Дикуля очень общительный и хочет, чтобы у него было много друзей. Однажды он завел себе профиль в сети «Пес-Коннект», где рассказал о своих увлечениях и что ищет себе друзей, и стал ждать писем. И вот какое письмо он получил! Давайте я вам его прочитаю.

«Привет, Дикуля. Я Большая Белая и Пушистая Мальтийская болонка. У меня совсем мало друзей, поэтому я очень хочу познакомиться

и подружиться с тобой. Пришли мне, пожалуйста, свой адрес и номер школы, в которой ты учишься. Я очень хочу посмотреть на тебя, поэтому пришли мне еще свою фотографию и фотографию своей семьи. С наилучшими пожеланиями, твой новый друг – Мальтийская болонка».

Как вы думаете, ребята, как надо Дикули отвечать на это письмо? Что может с ним случиться, если он исполнит все просьбы Мальтийской болонки? А давайте спросим Интернешку.

Интернешка:

В интернете, как и в мире,
Есть и добрые, и злые.
Полон разных он людей,
Есть и гений, и злодей.
По портрету не поймешь,
От кого слезу прольешь.
Чтобы вор к нам не пришел,
И чужой нас не нашел,
Телефон свой, адрес,
фото В интернет не
помещай И чужим не
сообщай.

Учитель: Сейчас я вам расскажу продолжение истории про Дикулю и Мальтийскую болонку. Дикуля отправил Мальтийской болонке письмо и все, что она его просила. В ответ болонка начала посылать ему письма, где Дика называла глупым псом, комком шерсти и т. д. Также Мальтийская болонка стала использовать фотографию Дика, представляясь от его имени и знакомясь с другими собаками, и обижать их. Дикуля очень расстроился и попросил Интернешку помочь ему. Интернешка помогает Дикули: он пересылает грубые письма администратору сайта, который блокирует адрес Мальтийской болонки, и Дикуля больше не получает плохих писем. Какое же правило на этот раз нам расскажет Интернешка?

Интернешка: В
интернете злые тролли
Появляются порой.
Эти злюки-задаваки Могут
довести до драки. Им дразнить
людей прикольно, Несмотря,
что это больно. Только полный
их «игнор» Тролля охладит
задор.

Сам же вежлив оставайся, В
тролля ты не превращайся!

Учитель: Ребята, нужно не только не давать информацию о себе чужим людям, но и не встречаться с незнакомцами. Какое правило про эту ситуацию расскажет нам Интернешка?

Интернешка:

Как всем детям интересно
Поиграть с друзьями вместе, В
интернете тоже можно, Нужно
быть лишь осторожным.
И с чужими не играть,
В гости их к себе не звать
И самим не приходить –
Я прошу вас не забыть.

Учитель: Ребята, а было у вас такое, что вы ищете что-то нужное в интернете, а на компьютере появляется совсем не то? А как вы думаете, что надо делать, чтобы этого не случилось? Давайте спросим у Интернешки!

Интернешка:

В интернете сайты есть – Невозможно
глаз отвесть.
Там и игры, и мультфильмы,
И учеба, и кино,
Только вдруг ты там находишь Иногда
совсем не то...
Чтобы не перепугаться
И потом не огорчаться, Надо
фильтр поискать И
компьютер подковать!
Ты родителям скажи:
Фильтры тут всегда нужны!

Учитель: Ребята, а что все-таки делать, если вы встретились с какойто трудностью в интернете: например, к вам пробрался вирус, или вас ктото обижает, или вы отправили SMS на незнакомый номер?

Вы должны обратиться к вашим родителям или учителям! Они могут взять в помощь себе и вам разные компьютерные программы, они всегда помогут решить проблему и защитят от неприятностей! Интернешка все про это знает!

Интернешка:

Если что-то непонятно, Страшно
или неприятно – Быстро к
взрослым поспеши, Расскажи и
покажи.
Есть проблемы в интернете?
Вместе взрослые и дети
Могут все решить всегда
Без особого труда.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного об интернете, о его возможностях и опасностях, о том, какие правила нужно соблюдать, чтобы все было хорошо. Про что эти правила? Сколько их? Какие правила вы запомнили?

Настало время прощаться! Сегодня вы узнали основные правила поведения в интернете! Надеюсь, вы запомните их!

Подведение итогов

Учитель анализирует с ребятами результаты творческих рисунков, работ из пластилина и предлагает организовать в классе небольшую выставку из работ.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55. 4. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или

объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. Азбука безопасности. В Интернете http://azbez.com/safety/internet
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасность детей в Интернете
5. http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
6. Копилочка активных методов обучения
7. http://www.moi-universitet.ru/ebooks/kamo/kamo/
8. Материалы сайта «Интернешка» http://interneshka.net/, http://www.oszone.net/6213/
9. Материалы викторины «Безопасность детей в сети интернет http://videouroki.net

20. КИБЕРУРОК
«Безопасное использование интернет.» (для 4 класса)

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 киберурока:

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.

21. КИБЕРУРОК
«Урок кибер безопасности в Интернете» (для 4 класса)

Цель урока:

Создание условий для обеспечения информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационнотелекоммуникационной среде.

Задачи:

- Ознакомить детей с основными угрозами, которые подстерегают пользователя в сети Интернет, объяснить правила общения в социальных сетях, в чатах и на форумах.
- 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=vi

deodwl&utm_content=all&utm_term=20151011bezopasnost

Комбинированный урок:

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

1. Мотивационная беседа

Ход занятия

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	Когда кто-то об этом просит. Сообщать с осторожностью людям, которым вы доверяете. Во всех случаях.
телефона?	

4. 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.

22. КИБЕУРОК
«Единый урок кибербезопасности в сети Интернет» (для 4 класса)

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

6. Подключен ли твой мобильный телефон к Интернету?

а) да б) нет

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

а) да

б) нет

8. В каких целях ты используешь Интернет?

а) поиск информации

б) общение с друзьями

в) игры

*г) другое (напиши свой ответ)*_____ 9. Знаешь ли ты какие сайты таят опасность?

а) да

б) нет

10. 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)Нистагмам

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 какойнибудь 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 агрессивнонастроенные 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!!!

23. КИБЕРУРОК

«Современные угрозы в цифровом мире» (для 4 класса) Цели:

- показать детям, какие опасности может таить Интернет;
- дать советы по безопасному поведению в сети Интернет;
- формировать положительное отношение к таким качествам характера, как самостоятельность, любознательность;
- развивать навыки участия в дискуссии;
- побуждать детей к самовыражению, саморазвитию.

Задачи:

- расширить представление детей об интернете;
- формировать основы коммуникативной грамотности, чувства ответственности за своё поведение;
- сформировать у учащихся понятия о принципах безопасного поведения в сети Интернет;
- обеспечить информационную безопасность ребенка при обращении к ресурсам Интернет;
- воспитывать внимательное отношение к информационным ресурсам.

Форма: беседа

Оснащение и методическое обеспечение: учительский компьютер, интерактивная доска, памятки по правилам безопасности в интернете.

Ход урока:

1. Организационный момент. (Слайд 1)

2. Постановка учебной задачи.

Сегодня мы затронем насущную тему для всех подростков. И начну наш классный час с такой загадки – ответ на которую вы все знаете. **(Слайд 2-3)**
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, (*Интернет*)
Учитель. А что такое **интернет**? (Слайд 4).
И тема нашего классного часа «Современные угрозы в цифровом мире.
Урок медиабезопасности» (Слайд 5)

(Слайд 6) Интернет – огромная информационная система на планете Земля. Её ещё называют «Всемирная паутина». Как вы думаете, почему? (Она, как паук, связывает между собой все города мира, всех людей мира.) **Учитель:** Кто из вас заходил хотя бы раз в интернет? Для чего нужен Интернет? Что в нём есть интересного и полезного? (ответы детей).

3.Основная часть.

1. Учитель: Что же нам даёт интернет? (Слайд 7-22)

1.В Интернете можно найти ответ на любой вопрос.

Интернет – это справочное бюро.

2. Отправить быстро письмо в другой город, другую страну, общаться по видеосвязи – **это почтальон.**

3. Найти и прочитать книгу – **это библиотека.**

4. Посмотреть фильм – **это кинотеатр.**

5. Поиграть одному или с друзьями – **это игротека.**

6. Обучаться дома, получая задание из школы или института – **это учитель.**

7. Узнать погоду на несколько дней вперед в любой точке планеты – **это прогноз погоды.**

8. Заказать и купить любой товар – **это магазин.**

2. Учитель: "Ребенок дома, за компьютером - значит, все в порядке, он в безопасности". Так считают многие родители. И ошибаются. Детей эры поисковых систем и социальных сетей опасности подстерегают не только на улице. Через мониторы компьютеров угроз на них обрушивается отнюдь не меньше. Одна из опасностей - **кибербулинг**: запугивание, психологический и физический террор - до чувства страха и подчинения. Конечно, Интернет не только источник угроз, он открывает большие возможности для общения и саморазвития. Чтобы Интернет приносил пользу, а не вред, вам

необходимо научиться правилам безопасного пользования Сетью так же, как вас учат не переходить дорогу на красный свет светофора. Интернет это полезная и интересная вещь, если правильно ею пользоваться, но у всякой медали есть своя оборотная сторона. В виртуальном мире нас подстерегает множество опасностей, о которых мы не имеем ни малейшего понятия. Поэтому надо знать основные правила работы в Интернет и соблюдать их. (Слайд 23)

Учитель: Давайте посмотрим видеоролик «Безопасность детей в сети интернет» и потом ещё раз назовём правила безопасного пользования Интернетом. (Слайд 24)

3. Учитель. Чтобы Интернет стал нам настоящим другом и приносил только пользу и радость, нужно знать несколько несложных, но очень важных правил.

Самое главное правило пользователя Интернета

- Будь внимателен и осторожен!

-А познакомиться с этими правилами нам поможет следующий видеосюжет. (Просмотр видео «Безопасный интернет»). (Слайд 25) **Учитель.** А запомнить их вам помогут вот эти стихи. Мы хотим, чтоб интернет Был вам другом много лет! Будешь знать семь правил этих — Смело плавай в интернете!

1. **Спрашивай взрослых**

Если что-то непонятно
страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

Установи фильтр

Как и всюду на планете, Есть
опасность в интернете.
Мы опасность исключаем,
Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете. **Не открывай файлы** *Не хочу попасть в беду — Антивирус заведу!*

Всем, кто ходит в интернет,
Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

Не спеши отправлять SMS

Иногда тебе в сети
Вдруг встречаются вруны. Ты
мошенникам не верь,
Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте. **Осторожно с незнакомцами** *Злые люди в Интернете Расставляют свои сети. С незнакомыми людьми Ты на встречу не иди!*

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

Будь дружелюбен

С грубиянами в сети
Разговор не заводи. Ну
и сам не оплошай -
Никого не обижай.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

Не рассказывай о себе

Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото
В интернет не помещай И
другим не сообщай.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

4.Учитель. Ребята, внимательно рассмотрите эту картинку. Глядя на неё, что вы можете сказать?

- (Мама и папа оттаскивают дочку от компьютера);
- Как вы думаете, почему? - (Потому что он много времени проводит за компьютером.)
- Как называют людей, которые бесконечно сидят в интернете, в поисках чего-то. Они уже свою жизнь не представляют без интернета, они зависимы от интернета.? - (**Это интернет - зависимые люди**.)

 Сегодня интернет зависимостью страдают 1,5% от общего числа пользователей интернета. Официальная медицина не признаёт такой диагноз. Но люди действительно психически расстроены.Они впадают в истерику, депрессию, если не побывали на просторах интернета. Многие люди уже зависимы от интернета и просто не понимают этого. В чём это проявляется? (Слайд 30 - 32)

5.Способы избавления от компьютерной зависимости (Слайд №33-34)

1.Любовь к ЗОЖ.

2.Общение с живой природой.

Реальный мир намного ярче виртуального, в нем есть много интересных и захватывающих вещей.

3.Увлечение прикладным творчеством (оригами, квиллинг).

4.Психолог.

Соберитесь с силами и сходите к профессиональному психологу, они неоднократно встречаются с этой проблемой и знают оптимальные способы борьбы с ней.

5.Близкие люди (родственники).

6. Учитель: И ещё несколько советов, которые помогут вам не попасть в паутину сети Интернета.

Возможные опасности, с которыми сопряжен доступ детей к Интернету:

- **Неприемлемые материалы.** В Интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий;
- **Неприятности, связанные с нарушением законов или финансовыми потерями.** У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов;
- **Разглашение конфиденциальной информации.** Детей и даже подростков могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол, и информация о семье могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации;
- **Проблемы технологического характера.** По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, “червь”, “троянский конь”, “зомби” или другой код, разработанный со злым умыслом.

4.Рефлексия (Слайд №35)

«Продолжи предложение»:

- сегодня я узнал…
- было интересно…
- меня удивило…
- мне захотелось…

5.Итог. (Слайд №36-37)

СИТУАЦИИ

1.Вы всегда мечтали иметь программу «Фотошоп». Наконец-то вы нашли её в Интернете и скачали. Активируя программу в компьютере, уже перед завершением процесса, вы прочитали следующее сообщение: «Для получения бесплатного сообщения с кодом введите номер вашего мобильного телефона». Как вы поступите?

2.Находясь в Интернете, вы открыли очень важную для вас страничку. Но компьютер тут же отреагировал: «Этот файл угрожает безопасности вашего

компьютера, содержит троянскую программу». Каковы ваши дальнейшие действия?

3.На сайте «Одноклассники» вы познакомились с классным парнем (или классной девчонкой). Через некоторое время «новый друг» просит встречи с вами на «нейтральной территории». Опишите ваши действия.

4.Для скачивания файла в Интернете потребовали введения ваших личных данных. Как вы поступите?

Вывод.

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна! Станет Интернет другом вам или врагом - зависит только от вас. Самое главное, что теперь вы знаете всё об интернете. Решать вам! Памятки о правилах безопасного пользования интернетом и рекомендации, остаются вам.

Список использованной литературы:

1.Лопатин Д.В., Королева Н.Л., Анурьева М.С., Пузанова Я.М., Остапчук К.И. Проблема безопасности школьников в сети Интернет // Вестник Тамбовского университета. Серия Естественные и технические науки. Тамбов, 2017. Т. 22. Вып.1

2.Рекомендации "Безопасный Интернет". Н. И. Баскакова. Тамбов: ТОИПКРО, 2011

Приложение

Правила безопасного пользования 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, так как она может быть доступна незнакомым людям. Где Вы живёте, 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 фотографии, видеоматериалы, каждый может посмотреть их.
8. Никогда не нажимайте незнакомые ссылки.

Безопасность при хождении по сайтам и по приему электронной почты:

- Не ходите на незнакомые сайты
- Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы
- Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты
- Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи) - Никогда, никому не посылайте свой пароль
- Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

Рекомендуем!

Школьный Яндекс - это полнофункциональная поисковая система для школьников.

Рекомендации подросткам, как избежать интернет – зависимости.

1. Используйте реальный мир для общения.
2. Ищите друзей в реальности. Виртуальный мир дает только иллюзию принадлежности к группе и не развивает никаких действительных навыков общения.
3. Наполняйте жизнь положительными событиями, поступками.
4. Имейте собственные четкие взгляды, убеждения.
5. Избегайте лживости и анонимности в виртуальной реальности.
6. Научитесь контролировать собственное время и время за компьютером.
7. Найдите любимое занятие, увлечение, хобби в реальной жизни.
8. Больше гуляйте, проводите время на свежем воздухе, займитесь спортом.
9. Прислушивайтесь к советам родителей, если они говорят, что вы слишком много времени проводите за компьютером.

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 5-Х КЛАССОВ

24. КИБЕРУРОК
«Опасный и удивительный мир интернета» (для 5 класса)

Цель: Актуализировать знания детей о различных Интернет -опасностях, предупреждение формирования Интернет - зависимости у детей.

Задачи:

1. Уточнение представления детей об Интернет - опасностях.
2. Способствовать осознанию различных Интернет - опасностей и рисков Интернет - зависимости.
3. Оказание помощи в снятии психоэмоционального напряжения.
4. Воспитание умения аргументировать своё мнение.
5. Развитие у детей чувство ответственности за свое здоровье. 6. Способствовать осознанию детьми и подростками своих ценностей.

Оборудование: листы, цветные карандаши (фломастеры), классная доска (маркерная доска), опорные слова для рефлексии, цветные листы бумаги или картона для обозначения 4-х углов.

Ход киберурока:

Вступительное слово учителя. Психологический настрой. Упражнение «Статус» (5 минут)

Здравствуйте, ребята. Каждому участнику предлагается озвучить свой «сетевой статус» - предложение, обозначающее его эмоциональное состояние на данный момент. Это может быть цитата из книги, стихотворение или просто описание того, что подросток чувствует в данный момент.

Правила поведения на занятии (3 минуты) Примерные формулировки правил поведения на занятии:

«МОЖНО»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу «НЕЛЬЗЯ»:
- перебивать говорящего товарища, выкрикивать с места; - смеяться над чужим мнением;
- смеяться над ошибками. И другие.

Правила формулируются самими учащимися, рисуются символы.

Разминка. **Упражнение «Четыре угла» (5 минут)**

Участникам предлагается обсудить, какие положительные или негативные моменты Интернет привносит в нашу жизнь. Предлагается выбрать один из четырёх углов в зависимости от мнения и аргументировать своё мнение.

Красный угол – становятся те, кто считает, что Интернет приносит только пользу.

Чёрный угол - выбирают те, кто считает, что Интернет приносит много вреда.

Зелёный угол – больше пользы, чем вреда (обозначить параметры пользы и вреда).

Оранжевый угол – больше вреда, чем пользы (обозначить параметры пользы и вреда).

Аргументируем ответы каждой группы

Учитель: А сейчас послушайте сказку "О золотых правилах безопасного поведения в Интернет"

СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл - царевич - королевич, который правил славным городом. И была у него невеста – прекрасная Смайл - царевна - Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл - царевич, возводя город , заботился об охране своих границ

и обучая жителей города основам безопасности жизнедеятельности в Интернет - государстве.

И не заметил он, как Интернет-паутина всё-таки затянула Смайл царевну в свои коварные сети. Погоревал – да делать нечего: надо спасать невесту.

Собрал он королевскую – дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл -царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки - убивалки Соловья - разбойника, товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл - царевну?

Крепко задумался Смайл - королевич, надел щит антивирусный, взял в руки меч - кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, и остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл - царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей, разомкнувшихся Смайл - царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

Учитель: Ребята, вот о каких правилах в сети интернет идет разговор.

1. Спрашивай взрослых

Если что-то непонятно, страшно или
неприятно, Быстро к взрослым поспеши,
Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете.
Они расскажут, что безопасно делать, а что нет.

2. Установи фильтр Как и всюду на планете, Есть опасность в интернете. Мы опасность исключаем, Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

3. Не открывай файлы Не хочу попасть в беду — Антивирус заведу! Всем, кто ходит в интернет, Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

4. Не спеши отправлять SMS

Иногда тебе в сети,
Вдруг встречаются вруны. Ты
мошенникам не верь,
Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами Злые люди в Интернете, Расставляют свои сети. С незнакомыми людьми Ты на встречу не иди!

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Будь дружелюбен

С грубиянами в сети,
Разговор не заводи.
Ну и сам не оплошай –
Никого не обижай.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

7. Не рассказывай о себе

Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото,
В интернет не помещай, И
другим не сообщай.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего, сама начнёт обучаться и помогать

будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образования.

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Учитель: Какова мораль этой сказки? (ответы детей). **Мозговой штурм**

Какие опасности я знаю в интернете? С чем я лично сталкивался (или боюсь столкнуться)? - оскорбления,

- вирусы,
- мошенники,
- постоянное пребывание в сети,
- неадекватные люди,
- угрозы, преследования и т.д.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного об интернете, о его возможностях и опасностях, о том, какие правила нужно соблюдать, чтобы все было хорошо. Про что эти правила? Сколько их? Какие правила вы запомнили?

Настало время прощаться! Сегодня вы узнали основные правила поведения в интернете! Надеюсь, вы запомните их! Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

Памятки о правилах безопасного пользования интернетом остаются вам.

Приложение 1.

Памятка по безопасному поведению в Интернете

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью. - Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате. - Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.

2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55. 4. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
2. сборник классных часов безопасность в интернете http://bpk.ucoz.ru/Files/Grant/8_sbornik_metodicheskikh_razrabotok_klassn ykh_chas.pdf
3. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасность детей в Интернете http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
5. Копилочка активных методов обучения http://www.moiuniversitet.ru/ebooks/kamo/kamo/
6. Материалы сайта «Интернешка»

http://interneshka.net/,http://www.oszone.net/6213/

7. Материалы викторины «Безопасность детей в сети интернет http://videouroki.net

25. КИБЕРУРОК
«Мобильное здоровье. Как пользоваться мобильной связью не причиняя вред своему здоровью» (для 5 класса)

Цель: Сформировать у обучающихся 5-6 классов понятие рационального использования средств мобильной связи не причиняя вред физиологическому, эмоциональному и психологическому здоровью. **Задачи**:

1. Повысить уровень информированности о сущности безопасного использования мобильного телефона.
2. Содействовать развитию навыков оценки и самооценки степени опасности бесконтрольного пользования мобильным телефоном.
3. Мотивировать на более безопасное для здоровья использование мобильного телефона.

Оборудование:

Презентация Power Point, экран, мультимедийный проектор, компьютер с возможностью выхода в интернет, анкета «Ты и мобильный телефон», тест «Вред мобильника».

Ход занятия с кратким описанием этапов и деятельности учащихся и учителя на каждом из них:

1. Информирование о теме встречи, проведение анкетирования.

Дорогие ребята, сегодня мы с вами поговорим о влиянии на организм мобильного телефона. Давайте сначала проверим, что вы знаете об этом и проведем анкетирование. Вам предлагается ответить на 8 вопросов небольшой анкеты.

Анкета для учащихся «Ты и мобильный телефон»

1. Сколько времени в день ты разговариваешь по телефону?

а) не больше 30 минут; в) больше 1 часа;

б) от 30 мин. до 1часа; г) больше 3 часов.

2. Где ты носишь мобильный телефон?

а) в сумке; в) в кармане;

б) на шее; г) другое.

3. Когда ты спишь, телефон лежит –

а) рядом с кроватью; в) далеко от кровати.

б) под подушкой; 4. Сколько тебе было лет, когда у тебя появился мобильник?

_____

5. Знаешь ли ты о вредном влиянии мобильного телефона на организм человека?

_____

6. Сколько времени в сутки ты пользуешься мобильным интернетом?

_____

7. Как ты думаешь, сколько времени можно пользоваться телефоном без вреда для здоровья? _____

8. Знаешь ли ты, что телефон в режиме Bluetooth излучает больше вредных электромагнитных волн, чем в обычном режиме?

а) да; в) не задумывался об этом.

б) нет;

2. Демонстрация и обсуждение слайдов презентации. Слайд 1.

За последние 20 лет мобильные телефоны плотно вошли в нашу жизнь. Где бы ни был человек, он просто обязан оставаться на связи 24 часа в сутки, если не хочет пропустить важные события в своей жизни. Вот только о влиянии телефона на здоровье человека мало кто задумывается. А ведь согласно статистике операторов сотовой связи:

- около 70% пользователей разговаривают по телефону более 30 минут в день; (слайд 2)
- 30% людей имеют по 2 сотовых и регулярно их используют; (слайд 3)
- 40% наших сограждан на ночь кладет телефон на расстояние менее 0,7 метра от головы, а ведь даже не звонящий аппарат постоянно связывается с базовой станцией; (слайд 4)
- только 20% пользователей знают, что влияние мобильного телефона на человека может быть чрезвычайно вредным (слайд 5).

3.Результаты анкетирования следующие:

- Больше _____ из опрошенных учащихся пользуются мобильным телефоном большую часть дня, и не задумываются о вредном облучении. ___% на ночь кладут телефон под подушку, и почти все опрошенные носят телефон в кармане (слайд 6).
- Многие из вас считают, что мобильный телефон абсолютно безвреден для здоровья, но хочу привести общеизвестный факт: в западных странах уровень влияния телефона на здоровье человека определяется не плотностью потока мощности как у нас, а температурой, на которую нагреваются участки тела человека при разговоре по мобильному телефону. То есть, Вам что-либо говорят следующие данные - уровень электромагнитного излучения возле головы при разговоре составляет около 1 Ватта на 1см2??? Или понятней будет сказать, что та область головы, к которой Вы прикладываете трубку в процессе разговора,

может нагреваться на 1 - 2 градуса. А ведь это изменения в нормальной работоспособности организма (слайд 7)!!!

4. Информационное выступление учителя.

Теперь давайте рассмотрим, как воздействует на организм человека мобильный телефон. О вреде сотовых телефонов для здоровья человека говорят уже много времени, но как-то без должного энтузиазма, - пока это вроде не особо и вредно, а дальше посмотрим.

Все предостережения сводятся к рекомендациям поменьше говорить по мобильному телефону. Однако недавно этот застарелый вопрос поднял главный санитарный врач России Геннадий Онищенко. Он настоятельно рекомендовал ограничить использование мобильных телефонов подростками в возрасте до 18 лет. Ведь согласно последним фактам сотовые телефоны действительно снижают иммунитет, изменяют психику и увеличивают биологический возраст человека. И это уже не просто "страшилка": медики утверждают, что по степени опасности сотовые и радиотелефоны можно смело приравнять к сигаретам и алкоголю.

Учёными была обследована группа людей в возрасте 30-40 лет, которые пользуются сотовым телефоном 15-25 минут в день на протяжении 2-4 лет. Выяснилось, что столь длительное облучение электромагнитным излучением приводит к нарушению всех основных функций мозга: мышления, памяти, внимания. Исследователи изучали состояние хрусталика глаза, а также нервной системы.

В результате выяснилось, что мобильные телефоны вызывают невосстанавливаемые изменения в обследуемых органах и подкорковых структурах головного мозга. А биологический возраст активных пользователей превышает календарный в среднем на 6-8 лет. То есть, если человеку 12 лет, и он часто говорит по мобильному телефону, в графе возраст он смело может писать 18 лет.

5. Осмысление, (слайд 8)

«Позволить добровольно облучать собственный мозг микроволнами мобильных телефонов – это самый большой биологический эксперимент над человеческим организмом"

(Шведский нейрохирург-профессор Лейф Селфорд). Как вы понимаете это высказывание?

(учащиеся высказывают своё мнение)

6. **Обсуждение в группах, разработка памятки по безопасному использованию телефона.**

-Что же делать, чтобы обезопасить себя от вредного воздействия мобильного телефона?

Ребятам предлагается провести обсуждение по группам и разработать памятки со своими правилами безопасного пользования мобильным телефоном.

7. Заключительный этап, (слайд10).

После работы в группах ребята зачитывают памятки со своими правилами безопасного пользования мобильным телефоном.

Итак, подведём итог. Для того чтобы не стать жертвой научнотехнического прогресса постарайтесь соблюдать следующие правила:

1. **Ограничить время и частоту** использования сотового телефона. Всё-таки нужно помнить, что мобильник – это не стационарный телефон, по которому можно было говорить часами. Более **2-3 минут за один вызов** и более **10-15 минут в день** разговаривать по мобильнику **не следует:**
2. Стараться по возможности **не использовать телефон в тех местах, где наблюдается плохой приём** (лифт, подземные помещения, транспорт и т. д.), так как при плохом приёме мобильный телефон пытается найти антенну-передатчик, и из-за этого его излучение (свойства и воздействия которого на человека до сих пор ещё в полной мере не изучены) многократно усиливается.
3. Реже использовать мобильный телефон в закрытых помещениях (машина, дом, лифт), так как излучаемые им волны могут отражаться стенами и покрытиями, что в несколько раз усиливает облучение.
4. Имейте в виду, что беспроводной способ передачи данных от одного мобильника к другому, разработанный под маркой Bluetooth, прибавляет мобильному телефону дополнительную силу излучения.
5. Не прикладывайте мобильный телефон к уху в тот момент, когда он находится в процессе поиска оператора сети (это бывает при самом включении и при плохом приёме). В этот момент он излучает больше всего, вредит, так сказать, по максимуму.
6. И, наконец, избавьтесь от пагубной привычки спать рядом с сотовым телефоном (тем более класть включённый, работающий (а, значит, постоянно излучающий!!!) мобильник под ПОДУШКУ!)

ОБЯЗАТЕЛЬНО ВЫКЛЮЧАЙТЕ ТЕЛЕФОН ПЕРЕД СНОМ!

Ну, а если вы привыкли использовать телефон в качестве будильника, то лучше отложить его в дальний угол вашей спальни. Это не только значительно снизит риск вашего облучения телефоном во время безмятежного сна, но и намного повысит вероятность вашего успешного

пробуждения. Ведь для того, чтобы выключить телефон-будильник, вам обязательно придётся подняться с постели.

Хотя стоит заметить, что встроенный в большинство современных мобильных телефонов будильник срабатывает и в том случае, если вы выключите телефон, и это, безусловно, простое и мудрое решение разработчиков. Так что совсем не обязательно доставать с чердака старый бабушкин будильник.

Используемая литература

1. http://www.elsmog.ru/index.php/mobtel/mobtel2.html Мобильный телефон вреднее курения.
2. http://www.shhitmobil.com.ua/clauses/show5 Вред мобильного телефона.
3. http://shkolazhizni.ru/archive/0/n-291/ Вредны ли мобильные телефоны. Антон Исаков.
4. http://www.inmoment.ru Сотовые (мобильные) телефоны. Галина Гатаулина.
5. http://www.ecohome.ru Мобильный телефон не причина вреда если….
6. http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html Мобильные телефоны вредны?

26. КИБЕРУРОК «Правила безопасного поведения в сети Интернет» (для 5 класса)

Цель: Формирование представления об информационной безопасности, формирование навыков ответственного и безопасного поведения Интернет среде

Задачи:

1. **Обучающие:**
   - познакомить с понятием информационной безопасности; рассмотреть различные угрозы информационной безопасности.
2. **Развивающие задачи:**
   - совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог; определить план действий для предотвращения угрозы информационной безопасности.
3. **Воспитательные задачи:**
   - воспитывать ответственность за свои действия и информационную культуру личности.

Необходимое оборудование: Экран, мультимедийный проектор, компьютер с возможностью выхода в интернет, раздаточный материал (карточки с заданиями на каждую группу).

Ход занятия с кратким описанием этапов и деятельности учащихся и учителя на каждом из них:

Организационный этап (1-2 минуты):

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.

Мотивационный этап (определение темы и цели занятия) (5-7 минут)

Перед тем как нам двигаться дальше предлагаю послушать, подумать и дать правильный ответ.

Он знает всё и даже больше, И к нам
на помощь поспешит. Любой вопрос,
пусть очень сложный, Мгновенно с
лёгкостью решит. Плетёт свою он
паутину, Хотя, по сути, не паук.
Он видит всё. Вы догадались?
*А, ну-ка, что это за друг? (*Интернет)

Я прошу обратить ваше внимание на 1 слайд на экране**.** О чем нам могут рассказать данные картинки

Обучающиеся разгадывают загадку, отвечают на вопросы учителя и определяют тему занятия и цель занятия. (1 слайд презентации)

- «Безопасность в Интернете» или «Угрозы в интернете, защита от угроз»,

«Правила безопасного поведения в сети Интернет»

- Научиться правилам безопасного поведения и общения в Интернете

Деятельностный этап (20-23 мин)

Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.

Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Информационная безопасность - это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам

Работа с презентацией

Ребята активно слушают, добавляют информацию по данным вопросам, вступают в обсуждение.

После обсуждения, учащиеся класса делятся на группы по 5 человек, на экране перед ребятами появляются задания, на которые ребята должны дать правильные

1. Перед ребятами на слайде 2 ситуация 1.

«Можно ли отправлять SMS или давать свой номер телефона, чтобы получить код доступа к игре или подарку?

Ребята в группах обсуждают и дают ответ, аргументировав его.

2. Слайд 3, ситуация 2.

Стоит ли сообщать в интернете своим виртуальным друзьям (незнакомым в реальности): фамилию, имя, адрес проживания, номер школы, место отдыха?

Ребята в группах обсуждают и дают ответ, аргументировав его.

3. Слайд 4,ситуация 3.

На ваш почтовый адрес пришло письмо с неизвестного адреса, ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его. **4.**

Слайд 5, ситуация 4.

Виртуальный друг предложил встретиться, ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

5. Слайд 6, ситуация 5.

Вы встретились с дразнилками и оскорблениями в Интернете, ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

6. Слайд 7, ситуация 6.

При открытии сайта Вы увидели, что являетесь 1000 посетителем и Вам положен подарок. Для этого предлагается пройти по ссылке, Ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

7. **Слайды 8-15. Работа с правилами поведения в сети Интернет.** Ребятам предлагаются задания они появляются на слайдах и раздаются в печатном виде каждой группе для удобства в работе. Решив задания, ребята узнают правила поведения.
8. **Слайды 16-18, ребятам необходимо отгадать ребусы.**

Классу выдается бланк где ребята записывают сообща те правила поведения в сети Интернет, которые узнали на уроки. У ребят получится памятка, которую можно закрепить на уголке безопасности.

Итогово-рефлексивный этап (8-10 мин):

Синквейн.

Первая строка — тема синквейна, заключает в себе одно слово (обычно существительное или местоимение), которое обозначает объект или предмет, о котором пойдет речь.

Вторая строка — два слова (чаще всего прилагательные или причастия), они дают описание признаков и свойств выбранного в синквейне предмета или объекта.

Третья строка — образована тремя глаголами или деепричастиями, описывающими характерные действия объекта.

Четвертая строка — фраза из четырёх слов, выражающая личное отношение автора синквейна к описываемому предмету или объекту.

Пятая строка — одно слово-резюме, характеризующее суть предмета или объекта.

Ребята, большое спасибо вам за интересную и важную информацию. Я уверена, что вы стали более грамотными в вопросах безопасности, и ваше путешествие по сети будет приносить вам пользу и радость познания в процессе обучения и вашем дальнейшем интеллектуальном развитии. Удачи Вам!

27. КИБЕРУРОК

«Основные виды киберугроз» (для 5 класса) Цель:

познакомить учеников 5 классов с основными видами киберугроз **Задачи:**

1. Познакомить и научить различать внешние и внутренние киберугрозы
2. Познакомить с основными понятиями и явлениями киберсреды, способными нанести вред не только компьютеру, но и человеку.
3. Научить основным навыкам личной безопасности и необходимости сохранения персональных данных.

Оборудование: ноутбук, проектор для презентации,

Ход занятия

1. Приветствие. Добрый день, ребята! Сегодня я расскажу вам что такое «Киберугрозы» и что современным пользователям телефонов, ноутбуков и других гаджетов нужно делать, чтобы не стать жертвой этих угроз.
2. Лекция-презентация «Основные виды киберугроз».

В настоящее время все киберугрозы принято разделять на внешние и внутренние. Причины и источники внешних угроз находятся вне компьютеров пользователей, как правило, в глобальной сети. Внутренние угрозы зависят исключительно от самих пользователей, программного обеспечения и оборудования. Сегодня на уроке мы подробно обсудим основные виды внешних угроз.

К внешним угрозам относят:

• вирусы;
• спам;
• фишинг;
• удаленный взлом;
• DoS/DDoS-атаки;
• хищение мобильных устройств.

Основная опасность киберугроз в скорости их изменения.

Вирусы скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Чтобы вирусы проникли в компьютер, достаточно всего лишь открыть вложение в электронном письме (при этом совершенно не обязательно, чтобы письмо было отправлено неизвестным адресатом, хорошо известный компаньон также может прислать вирус, если ранее его компьютер был заражен). Некоторым вирусам достаточно уже того, что компьютер просто подключен к локальной сети, к которой подключен и зараженный компьютер. Для распространения значительного числа вирусов используют съемные накопители информации (флешки, мобильные жесткие диски и оптические носители). Использование нелицензионного (пиратского) программного обеспечения может привести к потере данных пользовательских аккаунтов, к блокировке устройства, где установлена нелегальная программа. В настоящее время создатели вирусов используют их в основном для получения финансовой выгоды.

Еще более опасно, если вирус троянской программы перехватит данные банковского счета. Вирусы могут нарушить работоспособность компьютеров и программ, уничтожить файлы, используя для своих целей трафик, каналы связи, рассылая спам. Наиболее опасным вирусом является

кибероружие, которое направлено в некоторых случаях на уничтожение промышленной инфраструктуры. Появление вирусов Duqu, Stuxnet, Gauss, Flame обошлось не в один миллион долларов.

Спам не только вызывает раздражение у пользователей, но и забивает каналы связи, расходует трафик, отвлекает от работы, вынуждая людей искать важную корреспонденцию среди рекламы. В конечном счете, все это приводит к финансовым потерям. Помимо этого, спам также является одним из распространенных каналов внедрения троянских программ и вирусов.

Фишинг, в отличие от спама, нацелен на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код. Большую опасность представляет также удаленный взлом компьютеров, за счет которого злоумышленники могут получать возможность читать и редактировать документы, хранящиеся на файл-серверах и в компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, которые следят за всеми действиями конкурентов и собирают определенную информацию, вплоть до незаметного аудио- и видеонаблюдения через микрофоны ноутбуков и штатные веб-камеры.

Еще одна зона риска в Интернете — это угрозы для личной безопасности. Она связана с появлением мобильных устройств. Пользователь вынужден выдавать организаторам транзакций большой объем личной информации, которая может быть использована ему во вред.

Особого внимания для пользователей продукции Android заслуживают Android-трояны, распространенность которых обусловлена основными проблемами Android:

- повсеместным использованием старых версий операционных систем со слабой системой безопасности;
- разнообразием мобильных устройств, для ряда которых обновлений просто не существует;
- огромным количеством сторонних маркетплейсов, где можно скачать фальшивые и зараженные приложения.

Пользователи продукции Apple тоже не могут чувствовать себя в полной безопасности. Угрозу несут в себе и новые технологии, особенно в случае отсутствия их профессиональной киберзащиты.

В 2022 г. на информационные ресурсы нашей страны было совершено свыше 100 млн кибератак, что почти в 1,5 раза превысило показатели 2021 г. Для надежной защиты собственной критической информационной инфраструктуры в России создана Государственная система обнаружения,

предупреждения и ликвидации последствий компьютерных атак. Но не только государство, но и каждый из нас с вами может стать жертвой злоумышленников. О том, как распознать интернет-оферты и как с ними бороться мы поговорим с вами на следующем уроке, а теперь «проверка знаний».

Проверка

Литература. Вангородский, С. Н. Основы кибербезопасности : учебнометодическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.

28. КИБЕРУРОК
«Безопасный интернет» (для 5 класса)

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; частичнопоисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

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=pld70b 32df5c50a1d7&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. И нтернет 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»).

Физкультурная 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_room a.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.

5. 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:

2. Дать определение понятию «информационная безопасность». 3. Составить информационный лист «моя безопасная сеть».

Используемая литероатура:

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.

29. КИБЕРУРОК

«Безопасность школьников в сети Интернет»

(для 5 класса)

Аннотация

На уроке учащиеся знакомятся с основными Интернет - угрозами, полученные знания применяют при определении Интернет - угрозы в предложенных ситуациях, решении кроссворда.

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 Интернет можно 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);

- фи шинг - 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 киберпреступнику, 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

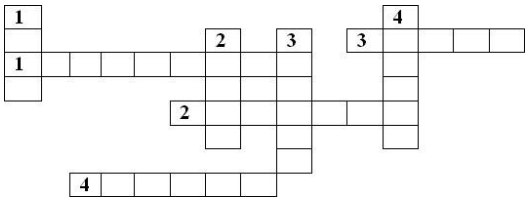
9. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.

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

Кроссворд



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:**
5. Программа, которая осуществляет защиту компьютера от вирусов
6. Интернет-угроза
7. Вредоносное программное обеспечение
8. 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.

30. КИБЕРУРОК
"Безопасность в сети Интернет" (для 5 класса)

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**

1. Организационный момент (3 мин.)

На доске написана тема "Безопасность в сети Интернет". Оформление кабинета плакатами, отражающими тему урока.

- 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)
   - Ответы на поставленные вопросы
   - Защита работ
6. Рефлексия (5 мин.)

Синквейн: основное понятие - Интернет

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 6-Х КЛАССОВ

31. КИБЕРУРОК
«Опасный и удивительный мир интернета» (для 6 класса)

Цель: Актуализировать знания детей о различных Интернет -опасностях, предупреждение формирования Интернет - зависимости у детей.

Задачи:

1. Уточнение представления детей об Интернет - опасностях.
2. Способствовать осознанию различных Интернет - опасностей и рисков Интернет - зависимости.
3. Оказание помощи в снятии психоэмоционального напряжения.
4. Воспитание умения аргументировать своё мнение.
5. Развитие у детей чувство ответственности за свое здоровье. 6. Способствовать осознанию детьми и подростками своих ценностей.

Оборудование: листы, цветные карандаши (фломастеры), классная доска (маркерная доска), опорные слова для рефлексии, цветные листы бумаги или картона для обозначения 4-х углов.

Ход киберурока:

Вступительное слово учителя. Психологический настрой. Упражнение «Статус» (5 минут)

Здравствуйте, ребята. Каждому участнику предлагается озвучить свой «сетевой статус» - предложение, обозначающее его эмоциональное состояние на данный момент. Это может быть цитата из книги, стихотворение или просто описание того, что подросток чувствует в данный момент.

Правила поведения на занятии (3 минуты) Примерные формулировки правил поведения на занятии:

«МОЖНО»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу «НЕЛЬЗЯ»:
- перебивать говорящего товарища, выкрикивать с места; - смеяться над чужим мнением;

- смеяться над ошибками. И другие.

Правила формулируются самими учащимися, рисуются символы.

Разминка. **Упражнение «Четыре угла» (5 минут)**

Участникам предлагается обсудить, какие положительные или негативные моменты Интернет привносит в нашу жизнь. Предлагается выбрать один из четырёх углов в зависимости от мнения и аргументировать своё мнение.

Красный угол – становятся те, кто считает, что Интернет приносит только пользу.

Чёрный угол - выбирают те, кто считает, что Интернет приносит много вреда.

Зелёный угол – больше пользы, чем вреда (обозначить параметры пользы и вреда).

Оранжевый угол – больше вреда, чем пользы (обозначить параметры пользы и вреда).

Аргументируем ответы каждой группы

Учитель: А сейчас послушайте сказку "О золотых правилах безопасного поведения в Интернет"

СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл - царевич - королевич, который правил славным городом. И была у него невеста – прекрасная Смайл - царевна - Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл - царевич, возводя город , заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет - государстве.

И не заметил он, как Интернет-паутина всё-таки затянула Смайл царевну в свои коварные сети. Погоревал – да делать нечего: надо спасать невесту.

Собрал он королевскую – дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл -царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки - убивалки Соловья - разбойника, товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл - царевну?

Крепко задумался Смайл - королевич, надел щит антивирусный, взял в руки меч - кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, и остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл - царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей, разомкнувшихся Смайл - царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

Учитель: Ребята, вот о каких правилах в сети интернет идет разговор.

1. Спрашивай взрослых

Если что-то непонятно, страшно или неприятно,
Быстро к взрослым поспеши, Расскажи и
покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете.
Они расскажут, что безопасно делать, а что нет.

2. Установи фильтр Как и всюду на планете, Есть опасность в интернете. Мы опасность исключаем, Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

3. Не открывай файлы Не хочу попасть в беду — Антивирус заведу! Всем, кто ходит в интернет, Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

4. Не спеши отправлять SMS

Иногда тебе в сети,
Вдруг встречаются вруны. Ты
мошенникам не верь,
Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли

отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами Злые люди в Интернете, Расставляют свои сети. С незнакомыми людьми Ты на встречу не иди!

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Будь дружелюбен

С грубиянами в сети,
Разговор не заводи.
Ну и сам не оплошай –
Никого не обижай.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

7. Не рассказывай о себе

Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото,
В интернет не помещай, И
другим не сообщай.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образования.

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Учитель: Какова мораль этой сказки? (ответы детей). **Мозговой штурм**

Какие опасности я знаю в интернете? С чем я лично сталкивался (или боюсь столкнуться)? - оскорбления,
- вирусы,
- мошенники,
- постоянное пребывание в сети,
- неадекватные люди,
- угрозы, преследования и т.д.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного об интернете, о его возможностях и опасностях, о том, какие правила нужно соблюдать, чтобы все было хорошо. Про что эти правила? Сколько их? Какие правила вы запомнили?

Настало время прощаться! Сегодня вы узнали основные правила поведения в интернете! Надеюсь, вы запомните их! Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

Памятки о правилах безопасного пользования интернетом остаются вам.

Приложение 1.

Памятка по безопасному поведению в Интернете

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью. - Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате. - Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

Используемая литература:

9. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
10. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
11. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55. 12. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.

13. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
14. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 15. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
16. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

4. Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
5. сборник классных часов безопасность в интернете http://bpk.ucoz.ru/Files/Grant/8_sbornik_metodicheskikh_razrabotok_klassnykh_chas.pdf
6. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасность детей в Интернете http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
5. Копилочка активных методов обучения http://www.moiuniversitet.ru/ebooks/kamo/kamo/
6. Материалы сайта «Интернешка» http://interneshka.net/,http://www.oszone.net/6213/
7. Материалы викторины «Безопасность детей в сети интернет http://videouroki.net

32. КИБЕРУРОК «Мобильное здоровье» (для 6 класса)

Цель: Сформировать у обучающихся 6 классов понятие рационального использования средств мобильной связи не причиняя вред физиологическому, эмоциональному и психологическому здоровью. **Задачи**:

1. Повысить уровень информированности о сущности безопасного использования мобильного телефона.
2. Содействовать развитию навыков оценки и самооценки степени опасности бесконтрольного пользования мобильным телефоном.
3. Мотивировать на более безопасное для здоровья использование мобильного телефона.

Оборудование:

Презентация Power Point, экран, мультимедийный проектор, компьютер с возможностью выхода в интернет, анкета «Ты и мобильный телефон», тест «Вред мобильника».

Ход занятия с кратким описанием этапов и деятельности учащихся и учителя на каждом из них:

2. Информирование о теме встречи, проведение анкетирования.

Дорогие ребята, сегодня мы с вами поговорим о влиянии на организм мобильного телефона. Давайте сначала проверим, что вы знаете об этом и проведем анкетирование. Вам предлагается ответить на 8 вопросов небольшой анкеты.

Анкета для учащихся «Ты и мобильный телефон»

1. Сколько времени в день ты разговариваешь по телефону?

а) не больше 30 минут; в) больше 1 часа;

б) от 30 мин. до 1часа; г) больше 3 часов.

2. Где ты носишь мобильный телефон?

а) в сумке; в) в кармане;

б) на шее; г) другое.

3. Когда ты спишь, телефон лежит –

а) рядом с кроватью; в) далеко от кровати.

б) под подушкой; 4. Сколько тебе было лет, когда у тебя появился мобильник?

_____

5. Знаешь ли ты о вредном влиянии мобильного телефона на организм человека?

_____

6. Сколько времени в сутки ты пользуешься мобильным интернетом?

7. Как ты думаешь, сколько времени можно пользоваться телефоном без вреда для здоровья? _____

8. Знаешь ли ты, что телефон в режиме Bluetooth излучает больше вредных электромагнитных волн, чем в обычном режиме?

а) да; в) не задумывался об этом.

б) нет;

2. Демонстрация и обсуждение слайдов презентации. Слайд 1.

За последние 20 лет мобильные телефоны плотно вошли в нашу жизнь. Где бы ни был человек, он просто обязан оставаться на связи 24 часа в сутки, если не хочет пропустить важные события в своей жизни. Вот только о влиянии телефона на здоровье человека мало кто задумывается. А ведь согласно статистике операторов сотовой связи:

- около 70% пользователей разговаривают по телефону более 30 минут в день; (слайд 2)
- 30% людей имеют по 2 сотовых и регулярно их используют; (слайд 3)
- 40% наших сограждан на ночь кладет телефон на расстояние менее 0,7 метра от головы, а ведь даже не звонящий аппарат постоянно связывается с базовой станцией; (слайд 4)
- только 20% пользователей знают, что влияние мобильного телефона на человека может быть чрезвычайно вредным (слайд 5).

3.Результаты анкетирования следующие:

- Больше _____ из опрошенных учащихся пользуются мобильным телефоном большую часть дня, и не задумываются о вредном облучении. ___% на ночь кладут телефон под подушку, и почти все опрошенные носят телефон в кармане (слайд 6).
- Многие из вас считают, что мобильный телефон абсолютно безвреден для здоровья, но хочу привести общеизвестный факт: в западных странах уровень влияния телефона на здоровье человека определяется не плотностью потока мощности как у нас, а температурой, на которую нагреваются участки тела человека при разговоре по мобильному телефону. То есть, Вам что-либо говорят следующие данные - уровень электромагнитного излучения возле головы при разговоре составляет около 1 Ватта на 1см2??? Или понятней будет сказать, что та область головы, к которой Вы прикладываете трубку в процессе разговора, может нагреваться на 1 - 2 градуса. А ведь это изменения в нормальной работоспособности организма (слайд 7)!!!

4. Информационное выступление учителя.

Теперь давайте рассмотрим, как воздействует на организм человека мобильный телефон. О вреде сотовых телефонов для здоровья человека говорят уже много времени, но как-то без должного энтузиазма, - пока это вроде не особо и вредно, а дальше посмотрим.

Все предостережения сводятся к рекомендациям поменьше говорить по мобильному телефону. Однако недавно этот застарелый вопрос поднял главный санитарный врач России Геннадий Онищенко. Он настоятельно рекомендовал ограничить использование мобильных телефонов подростками в возрасте до 18 лет. Ведь согласно последним фактам сотовые телефоны действительно снижают иммунитет, изменяют психику и увеличивают биологический возраст человека. И это уже не просто "страшилка": медики утверждают, что по степени опасности сотовые и радиотелефоны можно смело приравнять к сигаретам и алкоголю.

Учёными была обследована группа людей в возрасте 30-40 лет, которые пользуются сотовым телефоном 15-25 минут в день на протяжении 2-4 лет. Выяснилось, что столь длительное облучение электромагнитным излучением приводит к нарушению всех основных функций мозга: мышления, памяти, внимания. Исследователи изучали состояние хрусталика глаза, а также нервной системы.

В результате выяснилось, что мобильные телефоны вызывают невосстанавливаемые изменения в обследуемых органах и подкорковых структурах головного мозга. А биологический возраст активных пользователей превышает календарный в среднем на 6-8 лет. То есть, если человеку 12 лет, и он часто говорит по мобильному телефону, в графе возраст он смело может писать 18 лет.

5. Осмысление, (слайд 8)

«Позволить добровольно облучать собственный мозг микроволнами мобильных телефонов – это самый большой биологический эксперимент над человеческим организмом"

(Шведский нейрохирург-профессор Лейф Селфорд). Как вы понимаете это высказывание?

(учащиеся высказывают своё мнение)

6. Обсуждение в группах, разработка памятки по безопасному использованию телефона.

-Что же делать, чтобы обезопасить себя от вредного воздействия мобильного телефона?

Ребятам предлагается провести обсуждение по группам и разработать памятки со своими правилами безопасного пользования мобильным телефоном.

7. Заключительный этап, (слайд10).

После работы в группах ребята зачитывают памятки со своими правилами безопасного пользования мобильным телефоном.

Итак, подведём итог. Для того чтобы не стать жертвой научнотехнического прогресса постарайтесь соблюдать следующие правила:

7. **Ограничить время и частоту** использования сотового телефона. Всё-таки нужно помнить, что мобильник – это не стационарный телефон, по которому можно было говорить часами. Более **2-3 минут за один вызов** и более **10-15 минут в день** разговаривать по мобильнику **не следует:**
8. Стараться по возможности **не использовать телефон в тех местах, где наблюдается плохой приём** (лифт, подземные помещения, транспорт и т. д.), так как при плохом приёме мобильный телефон пытается найти антенну-передатчик, и из-за этого его излучение (свойства и воздействия которого на человека до сих пор ещё в полной мере не изучены) многократно усиливается.
9. Реже использовать мобильный телефон в закрытых помещениях (машина, дом, лифт), так как излучаемые им волны могут отражаться стенами и покрытиями, что в несколько раз усиливает облучение.
10. Имейте в виду, что беспроводной способ передачи данных от одного мобильника к другому, разработанный под маркой Bluetooth, прибавляет мобильному телефону дополнительную силу излучения.
11. Не прикладывайте мобильный телефон к уху в тот момент, когда он находится в процессе поиска оператора сети (это бывает при самом включении и при плохом приёме). В этот момент он излучает больше всего, вредит, так сказать, по максимуму.
12. И, наконец, избавьтесь от пагубной привычки спать рядом с сотовым телефоном (тем более класть включённый, работающий (а, значит, постоянно излучающий!!!) мобильник под ПОДУШКУ!)

ОБЯЗАТЕЛЬНО ВЫКЛЮЧАЙТЕ ТЕЛЕФОН ПЕРЕД СНОМ!

Ну, а если вы привыкли использовать телефон в качестве будильника, то лучше отложить его в дальний угол вашей спальни. Это не только значительно снизит риск вашего облучения телефоном во время безмятежного сна, но и намного повысит вероятность вашего успешного пробуждения. Ведь для того, чтобы выключить телефон-будильник, вам обязательно придётся подняться с постели.

Хотя стоит заметить, что встроенный в большинство современных мобильных телефонов будильник срабатывает и в том случае, если вы выключите телефон, и это, безусловно, простое и мудрое решение

разработчиков. Так что совсем не обязательно доставать с чердака старый бабушкин будильник.

Используемая литература

7. http://www.elsmog.ru/index.php/mobtel/mobtel2.html Мобильный телефон вреднее курения.
8. http://www.shhitmobil.com.ua/clauses/show5 Вред мобильного телефона.
9. http://shkolazhizni.ru/archive/0/n-291/ Вредны ли мобильные телефоны. Антон Исаков.
10. http://www.inmoment.ru Сотовые (мобильные) телефоны. Галина Гатаулина.
11. http://www.ecohome.ru Мобильный телефон не причина вреда если….
12. http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html Мобильные телефоны вредны?

33. КИБЕРУРОК

«Правила безопасного поведения в сети Интернет» (для 6 класса)

Цель: Формирование представления об информационной безопасности, формирование навыков ответственного и безопасного поведения Интернет среде

Задачи:

4. **Обучающие:**
   - познакомить с понятием информационной безопасности; рассмотреть различные угрозы информационной безопасности.
5. **Развивающие задачи:**
   - совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог; определить план действий для предотвращения угрозы информационной безопасности.
6. **Воспитательные задачи:**
   - воспитывать ответственность за свои действия и информационную культуру личности.

Необходимое оборудование: Экран, мультимедийный проектор, компьютер с возможностью выхода в интернет, раздаточный материал (карточки с заданиями на каждую группу).

Ход занятия с кратким описанием этапов и деятельности учащихся и учителя на каждом из них:

Организационный этап (1-2 минуты):

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.

Мотивационный этап (определение темы и цели занятия) (5-7 минут)

Перед тем как нам двигаться дальше предлагаю послушать, подумать и дать правильный ответ.

Он знает всё и даже больше, И к нам
на помощь поспешит. Любой вопрос,
пусть очень сложный, Мгновенно с
лёгкостью решит. Плетёт свою он
паутину, Хотя, по сути, не паук.
Он видит всё. Вы догадались?
*А, ну-ка, что это за друг? (*Интернет)

Я прошу обратить ваше внимание на 1 слайд на экране**.** О чем нам могут рассказать данные картинки

Обучающиеся разгадывают загадку, отвечают на вопросы учителя и определяют тему занятия и цель занятия. (1 слайд презентации)

- «Безопасность в Интернете» или «Угрозы в интернете, защита от угроз», «Правила безопасного поведения в сети Интернет»
- Научиться правилам безопасного поведения и общения в Интернете

Деятельностный этап (20-23 мин)

Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.

Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Информационная безопасность - это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам

Работа с презентацией

Ребята активно слушают, добавляют информацию по данным вопросам, вступают в обсуждение.

После обсуждения, учащиеся класса делятся на группы по 5 человек, на экране перед ребятами появляются задания, на которые ребята должны дать правильные

1. Перед ребятами на слайде 2 ситуация 1.

«Можно ли отправлять SMS или давать свой номер телефона, чтобы получить код доступа к игре или подарку?

Ребята в группах обсуждают и дают ответ, аргументировав его.

2. Слайд 3, ситуация 2.

Стоит ли сообщать в интернете своим виртуальным друзьям (незнакомым в реальности): фамилию, имя, адрес проживания, номер школы, место отдыха?

Ребята в группах обсуждают и дают ответ, аргументировав его.

3. Слайд 4,ситуация 3.

На ваш почтовый адрес пришло письмо с неизвестного адреса, ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

4. Слайд 5, ситуация 4.

Виртуальный друг предложил встретиться, ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

5. Слайд 6, ситуация 5.

Вы встретились с дразнилками и оскорблениями в Интернете, ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

6. Слайд 7, ситуация 6.

При открытии сайта Вы увидели, что являетесь 1000 посетителем и Вам положен подарок. Для этого предлагается пройти по ссылке, Ваши действия?

Ребята в группах обсуждают и дают ответ, аргументировав его.

7. **Слайды 8-15. Работа с правилами поведения в сети Интернет.** Ребятам предлагаются задания они появляются на слайдах и раздаются в печатном виде каждой группе для удобства в работе. Решив задания, ребята узнают правила поведения.
8. **Слайды 16-18, ребятам необходимо отгадать ребусы.**

Классу выдается бланк где ребята записывают сообща те правила поведения в сети Интернет, которые узнали на уроки. У ребят получится памятка, которую можно закрепить на уголке безопасности.

Итогово-рефлексивный этап (8-10 мин):

Синквейн.

Первая строка — тема синквейна, заключает в себе одно слово (обычно существительное или местоимение), которое обозначает объект или предмет, о котором пойдет речь.

Вторая строка — два слова (чаще всего прилагательные или причастия), они дают описание признаков и свойств выбранного в синквейне предмета или объекта.

Третья строка — образована тремя глаголами или деепричастиями, описывающими характерные действия объекта.

Четвертая строка — фраза из четырёх слов, выражающая личное отношение автора синквейна к описываемому предмету или объекту.

Пятая строка — одно слово-резюме, характеризующее суть предмета или объекта.

Ребята, большое спасибо вам за интересную и важную информацию. Я уверена, что вы стали более грамотными в вопросах безопасности, и ваше путешествие по сети будет приносить вам пользу и радость познания в процессе обучения и вашем дальнейшем интеллектуальном развитии. Удачи Вам!

34. КИБЕРУРОК

«Виды киберугроз» (для 6 класса) Цель:

познакомить учеников 6 классов с основными видами киберугроз **Задачи:**

4. Познакомить и научить различать внешние и внутренние киберугрозы
5. Познакомить с основными понятиями и явлениями киберсреды, способными нанести вред не только компьютеру, но и человеку.
6. Научить основным навыкам личной безопасности и необходимости сохранения персональных данных.

Оборудование: ноутбук, проектор для презентации,

Ход занятия

3. Приветствие. Добрый день, ребята! Сегодня я расскажу вам что такое «Киберугрозы» и что современным пользователям телефонов, ноутбуков и других гаджетов нужно делать, чтобы не стать жертвой этих угроз.

4. Лекция-презентация «Основные виды киберугроз».

В настоящее время все киберугрозы принято разделять на внешние и внутренние. Причины и источники внешних угроз находятся вне компьютеров пользователей, как правило, в глобальной сети. Внутренние угрозы зависят исключительно от самих пользователей, программного обеспечения и оборудования. Сегодня на уроке мы подробно обсудим основные виды внешних угроз.

К внешним угрозам относят:

• вирусы;
• спам;
• фишинг;
• удаленный взлом;
• DoS/DDoS-атаки;
• хищение мобильных устройств.

Основная опасность киберугроз в скорости их изменения.

Вирусы скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Чтобы вирусы проникли в компьютер, достаточно всего лишь открыть вложение в электронном письме (при этом совершенно не обязательно, чтобы письмо было отправлено неизвестным адресатом, хорошо известный компаньон также может прислать вирус, если ранее его компьютер был заражен). Некоторым вирусам достаточно уже того, что компьютер просто подключен к локальной сети, к которой подключен и зараженный компьютер. Для распространения значительного числа вирусов используют съемные накопители информации (флешки, мобильные жесткие диски и оптические носители). Использование нелицензионного (пиратского) программного обеспечения может привести к потере данных пользовательских аккаунтов, к блокировке устройства, где установлена нелегальная программа. В настоящее время создатели вирусов используют их в основном для получения финансовой выгоды.

Еще более опасно, если вирус троянской программы перехватит данные банковского счета. Вирусы могут нарушить работоспособность компьютеров и программ, уничтожить файлы, используя для своих целей трафик, каналы связи, рассылая спам. Наиболее опасным вирусом является кибероружие, которое направлено в некоторых случаях на уничтожение промышленной инфраструктуры. Появление вирусов Duqu, Stuxnet, Gauss, Flame обошлось не в один миллион долларов.

Спам не только вызывает раздражение у пользователей, но и забивает каналы связи, расходует трафик, отвлекает от работы, вынуждая людей

искать важную корреспонденцию среди рекламы. В конечном счете, все это приводит к финансовым потерям. Помимо этого, спам также является одним из распространенных каналов внедрения троянских программ и вирусов.

Фишинг, в отличие от спама, нацелен на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код. Большую опасность представляет также удаленный взлом компьютеров, за счет которого злоумышленники могут получать возможность читать и редактировать документы, хранящиеся на файл-серверах и в компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, которые следят за всеми действиями конкурентов и собирают определенную информацию, вплоть до незаметного аудио- и видеонаблюдения через микрофоны ноутбуков и штатные веб-камеры.

Еще одна зона риска в Интернете — это угрозы для личной безопасности. Она связана с появлением мобильных устройств. Пользователь вынужден выдавать организаторам транзакций большой объем личной информации, которая может быть использована ему во вред.

Особого внимания для пользователей продукции Android заслуживают Android-трояны, распространенность которых обусловлена основными проблемами Android:

- повсеместным использованием старых версий операционных систем со слабой системой безопасности;
- разнообразием мобильных устройств, для ряда которых обновлений просто не существует;
- огромным количеством сторонних маркетплейсов, где можно скачать фальшивые и зараженные приложения.

Пользователи продукции Apple тоже не могут чувствовать себя в полной безопасности. Угрозу несут в себе и новые технологии, особенно в случае отсутствия их профессиональной киберзащиты.

В 2022 г. на информационные ресурсы нашей страны было совершено свыше 100 млн кибератак, что почти в 1,5 раза превысило показатели 2021 г. Для надежной защиты собственной критической информационной инфраструктуры в России создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. Но не только государство, но и каждый из нас с вами может стать жертвой злоумышленников. О том, как распознать интернет-оферты и как с ними бороться мы поговорим с вами на следующем уроке, а теперь «проверка знаний».

Проверка

Литература. Вангородский, С. Н. Основы кибербезопасности : учебнометодическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа,
2019.

35. КИБЕРУРОК
«Игровой сленг» (для 6 класса)

Цель: повысить компьютерную грамотность взрослого и подрастающего поколения **Задачи:**

1. Познакомиться с понятием сленга.
2. Формировать навык цифрового этикета.
3. Профилактика кибербуллинга.

Оборудование: ноутбук, проектор для презентации,

Ход занятия

Здравствуйте! Сегодня мы с вами поговорим на тему «Что такое игровой сленг»? А вы знаете значение слова «сленг»?

Сленг – это разновидность речи, используемой преимущественно в устном общении отдельной относительно устойчивой социальной группой, объединяющей людей по признаку профессии или возраста.

Из этого определения следует, что сленг – разновидность нелитературной речи, к которой относятся:

1) профессионализмы,
2) вульгаризмы,
3) жаргонизмы,
4) лексика неформальных молодежных объединений и молодежной среды, часто называют сленгом.

Функции сленга:

У каждого слова и выражения, используемого в языке, есть какое-либо предназначение, и ничто не существует в языке просто так. Для чего же нужен сленг?

1) Сленг делает речь более краткой. (Сравним два выражения: Я вчера отправил другу письмо на электронную почту, на которое он не ответил- Я вчера отправил другу письмо на мыло, которое он проигнорил).
2) Сленг служит опознавательным знаком того, что этот человек принадлежит к данной социальной среде. Свой сленг есть у футбольных болельщиков, студентов, школьников и программистов и прочее.

Компьютерный сленг — разновидность сленга, используемого как профессиональной группой специалистов, так и пользователями компьютеров.

История появления слов из компьютерного сленга

В 80-х гг. XX в. компьютер стал доступен обычным людям. Его способности систематизировать и быстро находить нужные данные стали активно использовать в разных сферах, не связанных с наукой. Будучи довольно молодой, компьютерная отрасль еще не успела сформировать специфическую терминологию. И названия новым деталям и программам стали придумывать те, кто их создавали - вчерашние школьники и студенты. Не имея достаточного образования (не у кого было учиться - они первопроходцы), ребята называли многие приборы и команды по своему вкусу. Так что эти слова больше напоминали жаргон, чем профессиональные термины.

Особенности игрового сленга

Игровой сленг - условный язык, при помощи которого игроки в различных играх обмениваются информацией. Возникновение игрового сленга связывают с появлением массовых онлайн-игр, где он стал неотъемлемой частью игрового процесса.

В игровой ситуации игроки вырабатывают стратегию ведения игры, события разворачиваются быстро, и участникам происходящего нужно быстро доносить важную информацию до всех членов группы, и для решения этих задач используется соответствующая форма общения. Как следствие, используемые слова обычно короткие и информационно ёмкие. Это объясняется тем, что в игре победу или поражение определяют секунды, и быстрый обмен информацией становится важной задачей для игроков.

Игровой сленг является подмножеством компьютерного сленга, который не является грубым, таким же, как например жаргон панков, хиппи или блатной язык. Причиной является то, что профессия или увлечение, связанное с компьютерами, относится к высокоинтеллектуальным. Эмоциональность сленга особенно проявляется в оценке уровня игры другого человека. То есть, если игрок играет плохо, то его могут назвать целым рядом обидных выражений (нуб, рак), если же хорошо, то одобрительным (топовый). Эти эмоции могут проявляться к другим элементам (игровым предметам, навыкам и др.).

Краткость слов игрового сленга характеризуется тем, что слова обычно состоят из одного, двух, максимум трёх слогов.

Игровой сленг в настоящее время стал неотъемлемой частью речи учеников, которые не могут обойтись без таких сленговых слов, как: «комп», «виснуть», «клава», «винда».

По результатам опроса, проведённого в одной из школ, выяснилось, что более половины современных школьников активно пользуются словами, которые хорошо известны только заядлым геймерам.

В процессе общения ученики обмениваются различной информацией не только между собой, но и со своими родителями и учителями. Взрослые, к сожалению, не всегда могут понять то, что говорит современный ребёнок. А от уровня взаимопонимания очень зависит воспитание детей.

Сейчас вам предлагается групповая работа – кроссворд. Посмотрим, насколько хорошо вы знаете слова, которые часто используют любители видеоигр, и понимаете ли вы значение этих слов.

Приложение №1.

Мини-словарь игрового компьютерного сленга.

Слово	**Значение слова**
Ачивка	внутриигровое достижение
Босс	особенно сильный, уникальный противник
Донат	1) добровольное пожертвование, 2) покупка в игре за реальные деньги
Комбо	несколько сложных действий, выполненных подряд и без ошибок
Крафтинг	Создание предметов
Лаг	задержка между действием пользователя и откликом игры
Лутбокс	контейнер со случайным призом
Нуб	новичок
Скилл	Мастерство игрока
Спидран	Крайне быстрое прохождение
Стелс	скрытное прохождение
Хардкор	очень сложный уровень прохождения игры
Чекпоинт	точка сохранения
Читер	игрок, получивший преимущество нечестным путем

Используемая литература

1. http://www.elsmog.ru/index.php/mobtel/mobtel2.html Мобильный телефон вреднее курения.
2. http://www.shhitmobil.com.ua/clauses/show5 Вред мобильного телефона.
3. http://shkolazhizni.ru/archive/0/n-291/ Вредны ли мобильные телефоны. Антон Исаков.
4. http://www.inmoment.ru Сотовые (мобильные) телефоны. Галина Гатаулина.
5. http://www.ecohome.ru Мобильный телефон не причина вреда если….
6. http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html Мобильные телефоны вредны?

36. КИБЕРУРОК
«Моя безопасность в Интернете» (для 6 класса)

Цель: формирование потребности безопасного использования глобальной сети. **Задачи:**

- Познакомить ребят с потенциальными угрозами, исходящими из Интернета.
- Разработать нормы и правила поведения детей в сети Интернет.
- Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности.

Оборудование: бланки (по кол-ву уч-ся) с тестовой работой, листы А4 (по кол-ву уч-ся), карандаши, фломастеры, ручки.

Видео-презентация **Ход занятия**

- Здравствуйте, ребята! Рада вас видеть! **1. Упражнение «Встаньте все те, кто…»** - является пользователем Интернета?
- у кого есть своя страничка в социальных сетях?
- много времени проводит в социальных сетях?
- у кого друзей в соц. сетях больше, чем в реальной жизни?
- использует Интернет, чтобы узнать что-то новое, интересное о мире и людях?
- считает, что Интернет – это свободное пространство, в котором по своему усмотрению можно делать все, что пожелаешь?
- у кого были какие-либо неприятные случаи, связанные с Интернетом?
- считает, что Интернет приносит вред физическому здоровью?
- считает, что Интернет приносит вред психическому здоровью?
- Итак, многие из вас являются активными пользователями Интернета.
- Тема занятия: **« Моя безопасность в Интернете»**
- Здесь и сейчас мы будем работать над тем, как обезопасить себя, пользуясь Интернет-ресурсами.

2. Основные угрозы, исходящие из Интернета

Миллионы людей по всему миру являются активными пользователями интернета. Всемирная Сеть способствует приобретению новых знаний, помогает в учебной деятельности, даёт возможность узнать и научиться, с помощью видео-ресурсов, разным видам деятельности. Здесь можно, не выходя из дома, совершать покупки, читать книг и СМИ, научную информацию, посещать Интернет-библиотеку. Интернет дает возможность вам участвовать в различных конкурсах и олимпиадах, проектах. Создавать свои проекты, сайты.

В Интернете большую популярность приобрели социальные сети. Такая форма общения очень удобна. Имея аккаунт в социальной сети, мы можем общаться со своими близкими и друзьями, которые находятся далеко от нас, делиться новостями из своей жизни, личными фото, видео, находить интересных людей и новых знакомых.

- Всемирная паутина может нести опасность.
- Как вы думаете, какие угрозы могут исходить из Сети Интернета?
- С какими из них вы уже столкнулись сами? Или ваши знакомые, друзья?
- Как вы отреагировали?

(1. Нежелательные контакты, грубость, оскорбления

2. Мошенничество, ненужные покупки

3. Информация, не соответствующая возрасту

4. Угроза заражения вредоносными программами

5. Интернет-зависимость

6. Сайты, призывающие к терроризму, экстремизму, суициду;

7. Последствия предоставления личной информации и др.)

3. Работа в группах - обсуждение ситуаций, выработка правил безопасного использование Интернета.

Ситуация №1

«Новый друг, в данных которого указан тот же возраст, что и у тебя, предложил тебе встретиться»

Ситуация №2

«В чате тебя оскорбили, унизили»

Ситуация №3

«Знакомый предложил разослать оскорбительную информацию о вашем однокласснике (однокласснице)»

Ситуация №4

«Ваш одноклассник, играя в онлайн-игры, перестал общаться с друзьями» - *Какую угрозу несет данная ситуация?*

- *Что бы вы предложили делать в данной ситуации?*
- *Итак, давайте сформулируем правила, как избежать данных ситуаций или правильно (без вреда для себя и окружающих) отреагировать на них.(Ребята самостоятельно формулирую правила безопасного поведения в Интернете).*

В России средний возраст самостоятельной работы в Интернете около 10 лет. 30% несовершеннолетних проводят в Сети более 3х часов в день (при норме 2 час в неделю). Самые востребованные сайты – социальные сети. Нередко увлечение сетевыми играми перерастает в игровую зависимость.

Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних. **4. Личная страничка в Интернете**

- Предлагаю каждому создать свою собственную страницу в социальной сети. Каждый заполняет свою страницу так, как он желает нужным. Необходима фотография – нарисовать себя или свой портрет, как вы себя видите. Желательно в деталях. Рядом с рисунком у вас есть возможность заполнить контактную информацию, свои интересы и увлечения, что для вас ценно в жизни, адреса, телефоны, лучших друзей имена и др.
- Заодно подумайте над приватностью, хотите ли вы показать информацию о себе присутствующим здесь.
- Давайте обсудим, должны ли быть настройки приватности в нашей социальной сети?

5. Выработка правил поведения в Интернете

- Итак, давайте разработаем правила поведения в сети Интернет. Закончите предложение:

- ✓ Помните о (*что в интернете общаемся, так, как и в реальности – соблюдаем нормы воспитанного человека)*
- ✓ Позаботьтесь об (*антивирусной защите своего компьютера)*
- ✓ Никогда не *(не показывайте свои личные данные)*
- ✓ Всегда *(помните, что незаконное копирование продуктов труда других людей (музыки, игр, программ и т.д) считается плагиатом (умышленное присвоение авторства чужого произведения)*
- ✓ Думайте (прежде, чем *открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием)*
- ✓ Не верьте (*всему, что вы видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым)*
- ✓ Запомните (*Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями лично)*

6. ТЕСТ на знание правил поведения в Интернете

- Ребята, я предлагаю вам проверить себя, на сколько вы готовы правильно реагировать различные ситуации, которые могут возникнуть при использовании Интернет-ресурсов.

1. Новый друг, в данных которого указан тот же возраст, что и у тебя, предложил тебе обменяться фотографиями.

А. Попрошу его фото, и потом отправлю своё.

В. Посоветуюсь с родителями.

2. В чате тебя обозвали очень грубыми словами.

А. Скажу в ответ всё, что я об этом думаю.

В. Прекращу разговор с этим человеком.

3. Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.

А. Потребую доказательств, что она плохая.

В. Сразу откажусь.

4. Пришло сообщение с заголовком «От провайдера».

Запрашивают твой логин и пароль для входа в Интернет.

А. Вышлю только пароль: они сами должны знать логин.

В. Отмечу письмо как Спам.

Посчитай, сколько получилось ответов «А» и сколько «В».

4 «А» - Тебе ещё многому надо научиться.

3 «А» и 1 «В» - Внимательно прочитай эту памятку.

2 «А» и 2 «В» - Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «В» - Ты почти справился, но есть слабые места.

4 «В» - Молодец! К Интернету готов!

7. Итог

Приложение

ПРАВИЛА БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В ИНТЕРНЕТЕ 1. Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире.

2. Незаконное копирование продуктов труда других людей (музыки, игр, программ и т.д) считается плагиатом (умышленное присвоение авторства чужого произведения).

3. Не верьте всему, что вы видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым.

4. Нельзя сообщать другим пользователям интернета свою личную информацию (адрес, номер телефона, номер школы, любимые места для игр и т.д.).

5. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в интернете чемто, что требует указания идентификационного имени пользователя, тогда выберите это имя вместе со взрослыми, чтобы убедиться, что оно не содержит никакой личной информации.

6. Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями лично.

7. Нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.

37. КИБЕРУРОК
«Безопасный интернет» (для 6 класса)

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; частичнопоисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Этапы урока:

6. Организация начала урока. Постановка цели урока. Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html Постановка темы и главного вопроса урока.
7. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).

8. Практическая работа. Поиск информации в сети интернет. Дискуссия по найденному материалу.

9. Закрепление изученного материала. Рекомендации по правилам безопасной работы в интернет. Тестирование.

10. Подведение итогов урока. Оценка работы группы.

Домашнее задание. **Ход урока**

3. 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=pld70b 32df5c50a1d7&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? **4. Изучение нового материала.**

Игра «за или против».

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

6. И нтернет имеет неограниченные возможности дистанционного Образования. И это хорошо!

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

8. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.

9. Интернет является мощным антидепрессантом.

10. 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»).

Физкультурная 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?»

6. 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_room a.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.

7. 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.

8. 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:

4. Дать определение понятию «информационная безопасность».
5. Составить информационный лист «моя безопасная сеть».

Используемая литероатура:

Ссылки на web-ресурсы:

3) http://www.kaspersky.ru – антивирус «лаборатория касперского»;

4) 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;

7) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;

8) http://www.rgdb.ru – российская государственная детская библиотека.

38. КИБЕРУРОК
«Безопасность школьников в сети Интернет»
(для 6 класса)

Цель: познакомить с основными угрозами в 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 Интернет можно 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);

- фи шинг - 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 киберпреступнику, 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)

3. 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.

4. *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 12. 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.

13. 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.

14. 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.

15. 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.

16. Старайтесь не использовать функцию запоминания паролей, которую предлагают многие почтовые ящики и социальные сети.

17. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях .

18. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

19. При регистрации на сайтах, старайтесь не указывать личную информацию

20. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.

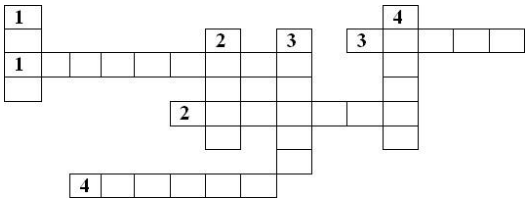
21. Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки. Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.

22. Не добавляйте в друзья в социальных сетях всех подряд.

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

Приложение 2

Кроссворд



По вертикали:

9. Массовая почтовая рассылка без согласия получателей
10. Личная информация о пользователе
11. Указатель перехода на одну из страниц сайта 12. Вид интернет - мошенничества **По горизонтали:**

13. Программа, которая осуществляет защиту компьютера от вирусов
14. Интернет-угроза
15. Вредоносное программное обеспечение
16. 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.

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 7-Х КЛАССОВ

39. КИБЕРУРОК

«Интернет-сообщества, виртуальные друзья» (для 7 класса)

Цель:

1. Ознакомиться с особенностями и возможностями интернет-групп.
2. Изучение особенностей виртуальной дружбы. **Задачи:**
1. Введение в тему «Социальных сетей».
2. Понимание особенностей социальных сетей, сообществ. Приобретение популярности в сети интернет.

Оборудование: клубок нити, кейс-задания в конвертах на 4 команды. листы, цветные карандаши (фломастеры), классная доска (маркерная доска),

опорные слова для рефлексии, цветные листы бумаги или картона для обозначения 4-х углов.

Организационный момент

Учитель: Предварительно класс делится на 4 подгруппы. Распределившись на команды, ребята садятся.

Вступительное слово учителя

Здравствуйте, ребята. Обсуждение правил работы на занятии. Правила формулируются самими учащимися. **Правила поведения на занятии (3 минуты)**

Примерные формулировки правил поведения на занятии: «можно»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу «нельзя»:
- перебивать говорящего товарища, выкрикивать с места; - смеяться над чужим мнением;
- смеяться над ошибками. И другие.

Ход Киберурока:

Психологический настрой. Упражнение «Всемирная паутина» (5 минут)

Учитель одной рукой держит конец нитки, кидает клубок случайному участнику и говорит, что его с ним связывает (например, «Мы с Машей любим уроки психологии»). Каждый учащийся, получая клубок в руки, оставляет себе нить и бросает клубок следующему. В итоге у каждого участника в руке должна оказаться нить.

Учитель задает вопросы детям:

1. Чем похожа наша паутина на Всемирную паутину Интернета?
2. Легко нам попасть сюда? Легко освободиться?
3. Какие есть плюсы и минусы социальных сетей?

Учитель: Социальные сети активно вошли в нашу жизнь и на сегодняшний день захватывают все больше свободного времени и личного пространства людей, особенно подростков. В этом виртуальном мире каждый находит для себя что-то нужное и ненужное, интересное и бесполезное.

В связи с этим возникает отдельная проблема – безопасность. Любая социальная сеть – это база, в которую вы вносите персональные данные. При этом многие пользователи слишком откровенны, они с охотой публикуют полную информацию о себе. А зря. Злоумышленники могут использовать

такие данные. Согласно опросу, проведенному среди студентов, 37% публикуют на своей странице в социальной сети свои персональные данные.

Учитель: Из каждой подгруппы приглашаются выйти по 1 представителю для выбора кейс-задания.

Организационный момент

Из каждой подгруппы вышли по 1 представителю для выбора кейс-задания. С выбранными заданиями представители сели на свои места. На выполнение кейс-задания дается 10-15 минут. По истечение предложенного времени, каждая подгруппа разбирает выбранный кейс и дает правильные ответы.

Мозговой штурм

Учитель задает вопросы ребятам, на которые необходимо дать ответы.

1.Больше друзей в Интернете или в жизни? Почему?

2.Какие плюсы и минусы большого количества виртуальных друзей и реальных друзей?

3.Обсуждение сходств и различий реальной и виртуальной дружбы.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного. Спасибо всем за работу.

Приложение 1.

Кейс - задания в конвертах для 4 команды.

Задание 1. Инструкция. Дайте краткий ответ.

Задание. Вам пришло письмо на электронную почту следующего содержания: «Для подтверждения того, что Вы являетесь настоящим пользователем «Вконтакте», перейдите по ссылке https://vvk.com/id47073790». Стоит ли переходить по ссылке и почему? Обоснуйте свой ответ.

Правильный ответ. Переходить по ссылке нельзя. Данный адрес не является официальным адресом сайта «Вконтакте», так как в адресе имеется лишняя буква v — vvk.com. Если при переходе по этой ссылке вести свой логин и пароль, то мошенник получит доступ к вашим персональным данным.

Задание 2. Инструкция. Прочитайте описание ситуации и дайте развернутые ответы на поставленные вопросы.

Задание. Гуляя по торговому центру, Таня увидела платье, которое ей очень понравилось, но оно было дорогим. Девочка решила проверить, сколько это платье стоит в интернет-магазине. Не задумываясь, она подключилась к одной из обнаруженных открытых сетей «FreeWiFi». Зайдя на сайт интернет-магазина, девочка обнаружила точно такое же платье её размера, но по цене в 3 раза дешевле. Обрадовавшись, Таня оформила онлайн-покупку, введя номер банковской карты и трехзначный код с обратной стороны карты. После этого она авторизовалась в социальной сети и своей радостной новостью поделилась с подружкой.

- Какие ошибки совершила Таня?
- Какие негативные последствия совершенного ею поступка могут возникнуть? Обоснуйте свой ответ.
- Сформулируйте правила, которыми нужно руководствоваться при использовании общественной Wi-Fi сети.

Правильные ответы. 1. Подключившись к общественной Wi-Fi сети, Таня передала конфиденциальные данные: ввела номер и код с банковской карты, авторизовалась в социальной сети – ввела логин и пароль.

2. Негативные последствия совершенного поступка: злоумышленники с применением введенного Таней логина и пароля могут «взломать» её страницу в социальной сети, тем самым узнать личную информацию, от лица Тани просить у «друзей» деньги, шантажировать саму Таню и т.д. Кроме того, так как при оплате покупки Таня ввела трехзначный код с карты, то теперь ее картой могут воспользоваться мошенники, оплачивая свои покупки в Интернете.

3. Правила: не доверять сетям с подозрительными названиями (FreeInternet или FreeWiFi), не совершать онлайн-покупки и банковские переводы в общественных сетях, не передавать конфиденциальную информацию, не вводить логины и пароли от различных сайтов.

Задание 3. Инструкция. Прочитайте описание ситуации и дайте развёрнутые ответы на поставленные вопросы.

Задание. Мама Кати, придя на работу, обнаружила, что забыла дома свой мобильный телефон. С рабочего телефона она позвонила Кате с просьбой принести ей его на работу. Закончив разговор, Катя услышала, что в соседней комнате на мамин мобильный телефон пришло СМС-сообщение. Так как у Кати с мамой были доверительные отношения, девочка прочитала

полученное СМС-сообщение. Катя заметила, что сообщение пришло от неизвестного отправителя. Оно содержало следующий текст: «Доброго времени суток! По вашим паспортным данным найдены страховые начисления в размере 47 руб. Подробности на сайте: http://snils-gost.online». Девочка, не задумываясь о последствиях, перешла по ссылке. В открывшемся окне браузера не было никакой информации о паспортных данных мамы, и Катя его закрыла. Через пару минут на мобильный телефон пришло СМС-сообщение от сотового оператора: «Ваш баланс менее 5 рублей». Заподозрив, что исчезновение средств связано с переходом по ссылке из СМС-сообщения, Катя испугалась и побежала на работу к маме.

Какие ошибки допустила Катя?
Какие последствия могут возникнуть в результате действий Кати? Обоснуйте свой ответ.
Составьте рекомендацию для детей, в которой будет содержаться описание признаков СМС-мошенничества и правил поведения при встрече с ними.

Правильные ответы: 1. Прочитала сообщение, адресованное не ей, перешла по подозрительной ссылке.
2. Переход по ссылке может привести к тому, что 1) произойдет списание денег со счета, 2) в телефон будут загружены вирусы, которые прекратят нормальную работу устройства и скачают все персональные данные, 3) при подключении телефона к компьютеру произойдет заражение и этого устройства.
3. Признаки СМС-мошенничества: номер от неизвестного отправителя; номер очень короткий; в сообщении содержится информация о выигрыше, для получения которого необходимо перейти по указанной ссылке; требование обратного звонка; просьба о помощи, связанной с переводом денег. Правила поведения: никогда не перезванивать и не переводить деньги; удалить СМС-сообщение; перезвонить своему мобильному оператору для решения «проблемы»; установить антивирусную программу на телефон.

Задание 4. Инструкция. Выберите из предложенных несколько верных вариантов ответа.

Задание. Разработчик игры «Stoon» потратил пять лет на её создание. Когда «Stoon» вышел в прокат, мальчик Лёня очень захотел приобрести эту игру. Придя в магазин, он обнаружил, что у неё высокая стоимость, поэтому

решил обратиться в Интернет за помощью. В сети перейдя по первой ссылке, Лёня увидел надпись: «Игра «Stoon» бесплатная и скачать её можно по данной ссылке ниже». Из представленных ниже вариантов выберите тот, который Вы предложили бы Лёне.

Правильные ответы: 1. Скачать игру с данного сайта, так как там она бесплатная.

2. Попросить денег у родителей и купить в магазине.

3. Продолжить искать игру в интернете с возможностью купить её со скидкой.

Правильные ответы: б и в.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55. 4. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta

2. сборник классных часов безопасность в интернете
http://news.scienceland.ru/2019/04/23/конкурс-задач-по-кибербезопасностик/
3. Копилочка активных методов обучения https://multiurok.ru/files/keis-po-informatike-bezopasnost-v-seti-internet.html
4. Безопасность детей в Интернете
5. https://www.cism-ms.ru/poleznye-materialy/virtualnye-druzya-s-kemobshchayutsya-deti-v-sotsialnykh-setyakh/
6. Копилочка активных методов обучения
7. http://www.moi-universitet.ru/ebooks/kamo/kamo/
8. Материалы сайта «Интернешка» http://interneshka.net/,
9. http://www.oszone.net/6213/
10. Материалы викторины «Безопасность детей в сети интернет
11. http://videouroki.net
12. Копилочка активных методов обучения
13. https://урок.рф/library/klassnij_chas_na_temu_pautina_sotcialnih_setej_181100.html

40. КИБЕРУРОК
«Компьютерные игры. Основные понятия» (для 7 класса)

Цель: повысить компьютерную грамотность взрослого и подрастающего поколения **Задачи:**

4. Познакомиться с понятием сленга.
5. Формировать навык цифрового этикета.
6. Профилактика кибербуллинга.

Оборудование: ноутбук, проектор для презентации,

Ход занятия

Здравствуйте! Сегодня мы с вами поговорим на тему «Что такое игровой сленг»? А вы знаете значение слова «сленг»?

Сленг – это разновидность речи, используемой преимущественно в устном общении отдельной относительно устойчивой социальной группой, объединяющей людей по признаку профессии или возраста.

Из этого определения следует, что сленг – разновидность нелитературной речи, к которой относятся:

1) профессионализмы,
2) вульгаризмы,
3) жаргонизмы,
4) лексика неформальных молодежных объединений и молодежной среды, часто называют сленгом.

Функции сленга:

У каждого слова и выражения, используемого в языке, есть какое-либо предназначение, и ничто не существует в языке просто так. Для чего же нужен сленг?

1) Сленг делает речь более краткой. (Сравним два выражения: Я вчера отправил другу письмо на электронную почту, на которое он не ответил- Я вчера отправил другу письмо на мыло, которое он проигнорил).
2) Сленг служит опознавательным знаком того, что этот человек принадлежит к данной социальной среде. Свой сленг есть у футбольных болельщиков, студентов, школьников и программистов и прочее.

Компьютерный сленг — разновидность сленга, используемого как профессиональной группой специалистов, так и пользователями компьютеров.

История появления слов из компьютерного сленга

В 80-х гг. XX в. компьютер стал доступен обычным людям. Его способности систематизировать и быстро находить нужные данные стали активно использовать в разных сферах, не связанных с наукой. Будучи довольно молодой, компьютерная отрасль еще не успела сформировать специфическую терминологию. И названия новым деталям и программам стали придумывать те, кто их создавали - вчерашние школьники и студенты. Не имея достаточного образования (не у кого было учиться - они первопроходцы), ребята называли многие приборы и команды по своему вкусу. Так что эти слова больше напоминали жаргон, чем профессиональные термины.

Особенности игрового сленга

Игровой сленг - условный язык, при помощи которого игроки в различных играх обмениваются информацией. Возникновение игрового сленга связывают с появлением массовых онлайн-игр, где он стал неотъемлемой частью игрового процесса.

В игровой ситуации игроки вырабатывают стратегию ведения игры, события разворачиваются быстро, и участникам происходящего нужно быстро доносить важную информацию до всех членов группы, и для решения этих задач используется соответствующая форма общения. Как следствие, используемые слова обычно короткие и информационно ёмкие. Это объясняется тем, что в игре победу или поражение определяют секунды, и быстрый обмен информацией становится важной задачей для игроков.

Игровой сленг является подмножеством компьютерного сленга, который не является грубым, таким же, как например жаргон панков, хиппи или блатной язык. Причиной является то, что профессия или увлечение, связанное с компьютерами, относится к высокоинтеллектуальным. Эмоциональность сленга особенно проявляется в оценке уровня игры другого человека. То есть, если игрок играет плохо, то его могут назвать целым рядом обидных выражений (нуб, рак), если же хорошо, то одобрительным (топовый). Эти эмоции могут проявляться к другим элементам (игровым предметам, навыкам и др.).

Краткость слов игрового сленга характеризуется тем, что слова обычно состоят из одного, двух, максимум трёх слогов.

Игровой сленг в настоящее время стал неотъемлемой частью речи учеников, которые не могут обойтись без таких сленговых слов, как: «комп», «виснуть», «клава», «винда».

По результатам опроса, проведённого в одной из школ, выяснилось, что более половины современных школьников активно пользуются словами, которые хорошо известны только заядлым геймерам.

В процессе общения ученики обмениваются различной информацией не только между собой, но и со своими родителями и учителями.
Взрослые, к сожалению, не всегда могут понять то, что говорит современный ребёнок. А от уровня взаимопонимания очень зависит воспитание детей.
Сейчас вам предлагается групповая работа – кроссворд. Посмотрим, насколько хорошо вы знаете слова, которые часто используют любители видеоигр, и понимаете ли вы значение этих слов.

Приложение №1.
Мини-словарь игрового компьютерного сленга.

Слово	**Значение слова**
Ачивка	внутриигровое достижение
Босс	особенно сильный, уникальный противник
Донат	1) добровольное пожертвование, 2) покупка в игре за реальные деньги
Комбо	несколько сложных действий, выполненных подряд и без ошибок
Крафтинг	Создание предметов
Лаг	задержка между действием пользователя и откликом игры
Лутбокс	контейнер со случайным призом
Нуб	новичок
Скилл	Мастерство игрока
Спидран	Крайне быстрое прохождение
Стелс	скрытное прохождение
Хардкор	очень сложный уровень прохождения игры
Чекпоинт	точка сохранения
Читер	игрок, получивший преимущество нечестным путем

Используемая литература

1. http://www.elsmog.ru/index.php/mobtel/mobtel2.html Мобильный телефон вреднее курения.
2. http://www.shhitmobil.com.ua/clauses/show5 Вред мобильного телефона.

3. http://shkolazhizni.ru/archive/0/n-291/ Вредны ли мобильные телефоны. Антон Исаков.
4. http://www.inmoment.ru Сотовые (мобильные) телефоны. Галина Гатаулина.
5. http://www.ecohome.ru Мобильный телефон не причина вреда если….
6. http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html Мобильные телефоны вредны?

41. КИБЕРУРОК
«Цифровое потребление» (для 7 класса)

Цель:

1. Формирование и развитие навыков поведения в опасных ситуациях, связанных с Интернет-мошенничеством.

Задачи:

1. Познакомить с видами Интернет мошенничества.
2. Формировать навыки эффективного поведения в ситуации мошенничества.
3. Развивать навыки достойного отказа.
4. Способствовать снятию психоэмоционального напряжения, вызванного использованием сетью Интернет.
5. Актуализировать у детей и подростков полученных знаний. 6. Развивать навыки поведения в опасных ситуациях.

Оборудование: карточки с ситуациями, таблички с названиями опасностей в Интернете, скриншоты страниц с опасными предложениями, картинки с изображением чемодана, корзины, мясорубки.

Организационный момент

Организационный момент

Учитель: Предварительно класс делится на 4 подгруппы. Распределившись на команды, ребята садятся.

Ход занятия

1. Приветствие, психологический настрой (3 минуты)

- Поприветствуем друг друга разными способами по условному сигналу: хлопком ладонь к ладони, плечом и т.д.

Правила поведения на занятии (3 минуты)

Примерные формулировки правил поведения на занятии: «можно»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу «нельзя»:
- перебивать говорящего товарища, выкрикивать с места; - смеяться над чужим мнением; - смеяться над ошибками. И другие.

Ход классного часа

2. Просмотр видеоролика “Безопасность платежей в интернете” **https://ligainternet.ru/videouroki/**

3. **Учитель:** Интернет-пространство расширяется, и с этим связано развитие кибер-мошенничества. Если люди уже научились распознавать мошенников в реальной жизни, и уже не «ведутся» на обычные шутки, то мошенников в интернете распознать гораздо сложнее. Как вы считаете, по каким причинам?

Да, глазами преступников не увидишь, и понять, что и как они могут сделать, непросто.

В кибер-пространстве мошенники работают по нескольким направлениям.

Учитель: Из каждой подгруппы приглашаются выйти по 1 представителю для выбора кейс-задания.

Организационный момент

Из каждой подгруппы вышли по 1 представителю для выбора кейс-задания. С выбранными заданиями представители сели на свои места. На выполнение кейс-задания дается 10-15 минут. По истечение предложенного времени, каждая подгруппа разбирает выбранный кейс и дает правильные ответы.

4. Упражнение «Чемодан. Корзина. Мясорубка»

Участники выбирают картинки чемодана, мусорной корзины или мясорубки в зависимости от полезности полученных знаний и отработанных навыков по теме безопасности в сети Интернет (или располагаются по принципу «Четыре (три) угла» в соответствии с размещёнными там картинками чемодана, корзины и мясорубки.

Чемодан – знания, умения и навыки были полезными, я возьму их с собой и буду пользоваться.

Мусорная корзина – ничего для меня не было полезным, мне не пригодятся эти навыки.
Мясорубка – мне ещё нужно осознать то, что я узнал на занятиях, обсудить с кем-то.

Завершение занятия

Учитель: Ребята, наше занятие подошло к концу. Будьте внимательны и соблюдайте правила безопасности в интернете.

Приложение 1.
Кейс - задания в конвертах для 4 команды.

Задание 1. Денежные «мышеловки»
1) «узнай местоположение по номеру телефона»
Задание. Вам предлагается зарегистрировать программу распознавания либо бесплатно, либо со взносом определенной суммы; программа часто оказывается обыкновенным вирусом. В любом случае, человек что-то теряет – деньги со своего счета или же информацию со своих аккаунтов, связанных с компьютером или телефоном. Либо незадачливого «шпиона» начинают терроризировать звонками и электронными письмами.

Как поступить. Правоохранители предупреждают, что узнать местоположение можно только с согласия абонента, либо по запросу в полиции (от оператора). Иные варианты не действуют. Поэтому откажитесь от слежки, не отправляйте смс и сообщения на указанные номера и уважайте приватность своих ближних.

2) «беспроцентный кредит»
Задание. Пользователю, желающему взять кредит, предлагают предоставить его быстро, легко и в любом объеме, если на счет мошенников будет перечислена круглая сумма. Действия преступников строятся как зеркальное отражение закона: к людям выезжают сотрудники, заполняются необходимые документы (получается согласие в том, что все добровольно и без претензий). Итог – ни денег, ни кредита.

Как поступить. Кредиты лучше не брать вообще; при необходимости сделайте заем у кого-нибудь из друзей или знакомых. При отсутствии возможности возьмите кредит в известном банке, придя лично в его филиал.

Задание 2. Денежные «мышеловки»

2.1. «Магазин на диване»

Задание. Вам предлагается приобрести желаемый товар по привлекательной цене (раз в 5 ниже среднестатистической), а возможно и вовсе бесплатно – вроде конфискат, вам делают подарок. Или к вам попадает журнал с товарами от известного магазина. Есть предложение – получить за заказ на ЭН-ную сумму ценный приз.

2.2. «Попрошайничество»

2.2. "Помощь в трудной жизненной ситуации"

Задание 1. К вам на почту поступает письмо с просьбой о материальной помощи, т.к. автор письма студент/начинающий/в сложной ситуации/денег нет, кушать нечего. На вас никто не давит, желаемая сумма может не указываться. Помочь человеку или нет – только ваше дело.

Задание 2. Вам приходит письмо с официального сайта благотворительной организации (детдома, приюта) с просьбой о материальной помощи какойлибо категории людей/человеку в социально опасном/затруднительном положении.

Как поступить. При желании помочь – проверьте адрес сайта (не дублер ли это), на кого оформлены реквизиты для перечисления денег. Позвоните в организацию (посетите ее), уточните номер счета и достоверность размещенной информации.

Задание 3. Денежные «мышеловки»

3.1. «Увеличение дохода»

Задание. Вы получаете письмо, где указывается, что денежный сайт предлагает эффективный способ удвоения капитала, (отправь 100 р, получи 500).

Или вам приходит сообщение о смерти дальнего родственника, наследником которого являетесь вы, однако нужно переслать налог на наследство.

Как поступить. Ни в коем случае ничего не высылайте; проверьте, действительно ли у вас был четвероюродный внучатый дядя из Канады, и ждите адвоката. Все юридические вопросы решаются с глазу на глаз, а не в интернете.

3.2. «Техподдержка»

Задание. вам приходит письмо с уведомлением, что аккаунт на каком-либо сайте взломан, или может быть заблокирован или удален (и т.д.), чтобы этого не случилось, необходима оплата (даже когда вы даже не регистрировались на сайте).

Как поступить: не оплачивать, не переходить по ссылкам (можете подхватить вирус) и не вводить данные. Зайдите на сайт с проверенного адреса, обновите страницу, можете обратиться к администратору сайта с вопросом.

Если все же успели ввести пароль, сразу же смените его.

Задание 4. Денежные «мышеловки»

4.1. «Лотерея»

Задание. Вам приходит письмо о крупном выигрыше: вы выиграли деньги/машину/что-то еще, приз будет выслан/счет активирован, как только вы переведете некоторую сумму (пошлина, транспортные расходы и тд.). Вы не участвовали в конкурсе – неважно. Даже не слышали о нем – тем более. Это очень интересно, просыпается азарт – получить нечто, при этом ничего не делая.

Как поступить. Вспомните, принимали ли вы участие, знаете ли организацию, откуда у нее ваши контакты; не знаете ответа на вопрос – забудьте о сообщении и ничего не переводите.

6) отправка смс

Ситуация первая. «Ваш аккаунт блокирован, подтвердите смс… вы выиграли, отправьте смс… помоги выиграть в голосовании…, получи доступ к сайту…» Стоимость СМС - в 5-10 раз больше обычной.

4.2. "Шантаж"

Задание. В эту категорию относятся все сообщения насчет «нелегального доступа к услугам сайта», спама с вашей страницы, угроз выложить в сеть какие-либо материалы, где главным условием избавления от проблемы являются ваши действия по отправлению денежных средств шантажисту.

Как поступить. Можете написать провайдеру о спаме с угрозами, либо в техподдержку сайта, услугами которого вы якобы пользуетесь. Любую угрозу можно заскринить, распечатать и обратиться в полицию.

5. "Механический ущерб"

5. 1."Вирусы"

Задание. «Вы реальный человек – введите свой номер телефона». Вам либо приходит смс для ответа, либо вы автоматически подписываетесь на какуюто телефонную услугу и у вас со счета списывается ежедневно пара десятков рублей. Если вы получили сообщение со ссылкой на скачивание открытки, музыки, картинки или какой-нибудь программы, не спешите открывать её. Перейдя по ссылке, вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Как поступить. Внимательно читать всю информацию, особенно мелким шрифтом, со страниц, в частности - внизу сайта. Если не помогло, немедленно обратитесь в салон связи отключать услугу. Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто-то из знакомых вам людей, убедитесь в этом, позвонив оппоненту. Если отправитель вам не знаком, не открывайте письмо.

Помните, что установка антивирусного программного обеспечения на компьютер или мобильное устройство повышает вашу безопасность.

5.2. "Сайты-фейки"

Задание. Вы заходите на сайт, на котором вы уже зарегистрированы, по ссылке, но вам надо заново вводить почту и пароль от нее.

Как поступить. Проверьте адрес сайта и перейдите по проверенной ссылке.

6. "Работа в интернете"

Задание. Интернет является одним из способов заработка, но человек может стать жертвой мошенников: когда он выполнит работу по переводу текста или написанию реферата, то может остаться без обещанной платы.

Как поступить. Собираясь работать в сети, помните, что главный принцип – сначала оплата (хотя бы половинная), потом – работа.

Учитель предлагает ребятам поиграть в большую ролевую игру «Опасности сети Интернет»

- Учащимся раздаются роли (таблички с названиями опасностей в Интернете). На внешней стороне таблички написана приемлемая роль (например СМС, электронное письмо, Друг, Реклама, Интересный сайт, Антивирус, но с обратной стороны (невидимой для окружающих) на многих из них написана истинная роль, которую нужно будет грамотно сыграть: вирусы, спам, вредоносные ПО (программное обеспечение), Интернет-хам (тролль), поддельный сайт, Интернет-мошенник (попрошайка), Незнакомец, который хочет заманить куда-нибудь, вызвать на встречу и другие. Несколько ребят играют роль пользователей, которые должны взаимодействовать с остальными (носителями пользы и вреда в Интернет-пространстве) и грамотно принимать или отсеивать поступающую информацию.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29.
7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.

8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
2. сборник классных часов безопасность в интернете http://news.scienceland.ru/2019/04/23/конкурс-задач-покибербезопасности-к/
3. Копилочка активных методов обучения https://multiurok.ru/files/keispo-informatike-bezopasnost-v-seti-internet.html
4. Безопасность детей в Интернете https://www.cism-ms.ru/poleznyematerialy/virtualnye-druzya-s-kem-obshchayutsya-deti-v-sotsialnykhsetyakh/
5. Копилочка активных методов обучения http://www.moiuniversitet.ru/ebooks/kamo/kamo/
6. Материалы сайта «Интернешка» http://interneshka.net/, http://www.oszone.net/6213/
7. Материалы викторины «Безопасность детей в сети интернет https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
8. Копилочка активных методов обучения http://save.nios.ru/sites/save.nios.ru/files/materialy/yurina_vneklassnoe_meropriyatie_4.moshennichestvo_v_seti.pdf

42. КИБЕРУРОК
«Безопасный интернет. Как правильно себя вести в сети»
(для 7 класса)

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; частичнопоисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Этапы урока:

11. Организация начала урока. Постановка цели урока. Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html Постановка темы и главного вопроса урока.
12. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).
13. Практическая работа. Поиск информации в сети интернет. Дискуссия по найденному материалу.
14. Закрепление изученного материала. Рекомендации по правилам безопасной работы в интернет. Тестирование.
15. Подведение итогов урока. Оценка работы группы. Домашнее задание.

Ход урока

5. 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=pld70b 32df5c50a1d7&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? **6. Изучение нового материала.**

Игра «за или против».

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

отражающие Противоположную точку зрения.

11. И нтернет имеет неограниченные возможности дистанционного Образования.

И это хорошо!

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

13. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.

14. Интернет является мощным антидепрессантом.

15. 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»).

Физкультурная 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?»

9. 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_room a.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.

10. 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.

11. 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:

6. Дать определение понятию «информационная безопасность». 7. Составить информационный лист «моя безопасная сеть».

Используемая литероатура:

Ссылки на web-ресурсы:

5) http://www.kaspersky.ru – антивирус «лаборатория касперского»;

6) 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;

9) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;

10) http://www.rgdb.ru – российская государственная детская библиотека.

43. КИБЕРУРОК
«Урок по безопасности в сети Интернет (для 7 класса)

Цель: формирование информационно-коммуникативной компетенции. Оборудование: мультимедийный проектор, компьютер, карточки с заданиями. Организационный момент Ход урока**:**

- 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 карточекпамяток)*

- 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 карточекпамяток)*

- 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 карточекпамяток)*

- 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 - информационнопознавательный 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/

44. КИБЕРУРОК
«Безопасность учащихсяч в сети Интернет»
(для 7 класса)

Цель: учащиеся узнают об основных угрозах сети Интернет и методах борьбы с ними; **Задачи:**

- познакомиться с понятием «Интернет», «Интернет-угроза»; - изучить приемы безопасности при работе в сети Интернет. - формирование приёмов логического мышления;
- развитие способности анализировать и обобщать, делать выводы.
- воспитание аккуратности, точности, самостоятельности; - привитие навыка групповой работы, сотрудничества.
- оптимальное сочетание форм и методов, применяемых на занятии.

Ход урока:

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 Интернет можно 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);
- фишинг - 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 киберпреступнику, который будет его переполнять горами спама).

Онлайн-угрозы могут также навредить вашей репутации.

45.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)

5. 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.

6. 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 23. 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.

24. 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.

25. 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.

26. 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.

27. Старайтесь не использовать функцию запоминания паролей, которую предлагают многие почтовые ящики и социальные сети.

28. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях .

29. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

30. При регистрации на сайтах, старайтесь не указывать личную информацию

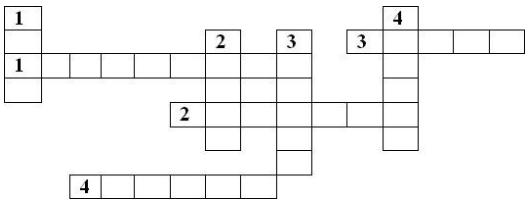
31. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.

32. 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. 33. Не добавляйте в друзья в социальных сетях всех подряд.

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

Приложение 2

Кроссворд



По вертикали:

17. Массовая почтовая рассылка без согласия получателей
18. Личная информация о пользователе
19. Указатель перехода на одну из страниц сайта 20. Вид интернет - мошенничества **По горизонтали:**

21. Программа, которая осуществляет защиту компьютера от вирусов
22. Интернет-угроза
23. Вредоносное программное обеспечение
24. 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

45. КИБЕОРУРОК «Безопасность в сети Интернет» (для 7 класса).

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

Задачи:

2. Выяснить первоначальные представления учащихся о назначении и возможностях сети Интернет.
3. Формировать культуры ответственного, этичного и безопасного использования Интернета.

4. Повысить осведомленность детей о позитивном контенте сети Интернет, полезных возможностях глобальной сети для образования, развития, общения.

5. Расширить осведомленность детей о проблемах безопасности при использовании детьми сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.

6. Совместно составить «Памятку безопасности интернетпользователя».

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 словассоциаций 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. **2. Создание проблемной ситуации.**

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 онлайнобучения, 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 киберпреступлениях. 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.

1. 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.

3. 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».

46. КИБЕРУРОК
«Безопасность в сети Интернет: правила безопасной работы в сети» (для 7 класса)

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 onlinetехнологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частичнопоисковый, 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.).

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 8 КЛАССОВ

47. КИБЕРУРОК

«Интернет-сообщества, виртуальные друзья» (для 8 класса) Цель:

1. Ознакомиться с особенностями и возможностями интернет-групп.
2. Изучение особенностей виртуальной дружбы. **Задачи:**
1. Введение в тему «Социальных сетей».
2. Понимание особенностей социальных сетей, сообществ. Приобретение популярности в сети интернет.

Оборудование: клубок нити, кейс-задания в конвертах на 4 команды. листы, цветные карандаши (фломастеры), классная доска (маркерная доска), опорные слова для рефлексии, цветные листы бумаги или картона для обозначения 4-х углов.

Организационный момент

Учитель: Предварительно класс делится на 4 подгруппы. Распределившись на команды, ребята садятся.

Вступительное слово учителя

Здравствуйте, ребята. Обсуждение правил работы на занятии. Правила формулируются самими учащимися.

Правила поведения на занятии (3 минуты)

Примерные формулировки правил поведения на занятии: «можно»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу «нельзя»:
- перебивать говорящего товарища, выкрикивать с места; - смеяться над чужим мнением;
- смеяться над ошибками. И другие.

Ход Киберурока:

Психологический настрой. Упражнение «Всемирная паутина» (5 минут)

Учитель одной рукой держит конец нитки, кидает клубок случайному участнику и говорит, что его с ним связывает (например, «Мы с Машей любим уроки психологии»). Каждый учащийся, получая клубок в руки,

оставляет себе нить и бросает клубок следующему. В итоге у каждого участника в руке должна оказаться нить. **Учитель задает вопросы детям:**

1. Чем похожа наша паутина на Всемирную паутину Интернета?
2. Легко нам попасть сюда? Легко освободиться?
3. Какие есть плюсы и минусы социальных сетей?

Учитель: Социальные сети активно вошли в нашу жизнь и на сегодняшний день захватывают все больше свободного времени и личного пространства людей, особенно подростков. В этом виртуальном мире каждый находит для себя что-то нужное и ненужное, интересное и бесполезное.

В связи с этим возникает отдельная проблема – безопасность. Любая социальная сеть – это база, в которую вы вносите персональные данные. При этом многие пользователи слишком откровенны, они с охотой публикуют полную информацию о себе. А зря. Злоумышленники могут использовать такие данные. Согласно опросу, проведенному среди студентов, 37% публикуют на своей странице в социальной сети свои персональные данные.

Учитель: Из каждой подгруппы приглашаются выйти по 1 представителю для выбора кейс-задания.

Организационный момент

Из каждой подгруппы вышли по 1 представителю для выбора кейс-задания. С выбранными заданиями представители сели на свои места. На выполнение кейс-задания дается 10-15 минут. По истечение предложенного времени, каждая подгруппа разбирает выбранный кейс и дает правильные ответы.

Мозговой штурм

Учитель задает вопросы ребятам, на которые необходимо дать ответы.

1.Больше друзей в Интернете или в жизни? Почему?

2.Какие плюсы и минусы большого количества виртуальных друзей и реальных друзей?

3.Обсуждение сходств и различий реальной и виртуальной дружбы.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного. Спасибо всем за работу.

Приложение 1.

Кейс - задания в конвертах для 4 команды.

Задание 1. Инструкция. Дайте краткий ответ.

Задание. Вам пришло письмо на электронную почту следующего содержания: «Для подтверждения того, что Вы являетесь настоящим

пользователем «Вконтакте», перейдите по ссылке https://vvk.com/id47073790». Стоит ли переходить по ссылке и почему? Обоснуйте свой ответ.

Правильный ответ. Переходить по ссылке нельзя. Данный адрес не является официальным адресом сайта «Вконтакте», так как в адресе имеется лишняя буква v — vvk.com. Если при переходе по этой ссылке вести свой логин и пароль, то мошенник получит доступ к вашим персональным данным.

Задание 2. Инструкция. Прочитайте описание ситуации и дайте развернутые ответы на поставленные вопросы.

Задание. Гуляя по торговому центру, Таня увидела платье, которое ей очень понравилось, но оно было дорогим. Девочка решила проверить, сколько это платье стоит в интернет-магазине. Не задумываясь, она подключилась к одной из обнаруженных открытых сетей «FreeWiFi». Зайдя на сайт интернет-магазина, девочка обнаружила точно такое же платье её размера, но по цене в 3 раза дешевле. Обрадовавшись, Таня оформила онлайн-покупку, введя номер банковской карты и трехзначный код с обратной стороны карты. После этого она авторизовалась в социальной сети и своей радостной новостью поделилась с подружкой.

- Какие ошибки совершила Таня?
- Какие негативные последствия совершенного ею поступка могут возникнуть? Обоснуйте свой ответ.
- Сформулируйте правила, которыми нужно руководствоваться при использовании общественной Wi-Fi сети.

Правильные ответы. 1. Подключившись к общественной Wi-Fi сети, Таня передала конфиденциальные данные: ввела номер и код с банковской карты, авторизовалась в социальной сети – ввела логин и пароль.

2. Негативные последствия совершенного поступка: злоумышленники с применением введенного Таней логина и пароля могут «взломать» её страницу в социальной сети, тем самым узнать личную информацию, от лица Тани просить у «друзей» деньги, шантажировать саму Таню и т.д. Кроме того, так как при оплате покупки Таня ввела трехзначный код с

карты, то теперь ее картой могут воспользоваться мошенники, оплачивая свои покупки в Интернете.
3. Правила: не доверять сетям с подозрительными названиями (FreeInternet или FreeWiFi), не совершать онлайн-покупки и банковские переводы в общественных сетях, не передавать конфиденциальную информацию, не вводить логины и пароли от различных сайтов.

Задание 3. Инструкция. Прочитайте описание ситуации и дайте развёрнутые ответы на поставленные вопросы.

Задание. Мама Кати, придя на работу, обнаружила, что забыла дома свой мобильный телефон. С рабочего телефона она позвонила Кате с просьбой принести ей его на работу. Закончив разговор, Катя услышала, что в соседней комнате на мамин мобильный телефон пришло СМС-сообщение. Так как у Кати с мамой были доверительные отношения, девочка прочитала полученное СМС-сообщение. Катя заметила, что сообщение пришло от неизвестного отправителя. Оно содержало следующий текст: «Доброго времени суток! По вашим паспортным данным найдены страховые начисления в размере 47 руб. Подробности на сайте: http://snils-gost.online». Девочка, не задумываясь о последствиях, перешла по ссылке. В открывшемся окне браузера не было никакой информации о паспортных данных мамы, и Катя его закрыла. Через пару минут на мобильный телефон пришло СМС-сообщение от сотового оператора: «Ваш баланс менее 5 рублей». Заподозрив, что исчезновение средств связано с переходом по ссылке из СМС-сообщения, Катя испугалась и побежала на работу к маме.

Какие ошибки допустила Катя?
Какие последствия могут возникнуть в результате действий Кати? Обоснуйте свой ответ.
Составьте рекомендацию для детей, в которой будет содержаться описание признаков СМС-мошенничества и правил поведения при встрече с ними.

Правильные ответы: 1. Прочитала сообщение, адресованное не ей, перешла по подозрительной ссылке.
2. Переход по ссылке может привести к тому, что 1) произойдет списание денег со счета, 2) в телефон будут загружены вирусы, которые прекратят нормальную работу устройства и скачают все персональные

данные, 3) при подключении телефона к компьютеру произойдет заражение и этого устройства.

3. Признаки СМС-мошенничества: номер от неизвестного отправителя; номер очень короткий; в сообщении содержится информация о выигрыше, для получения которого необходимо перейти по указанной ссылке; требование обратного звонка; просьба о помощи, связанной с переводом денег. Правила поведения: никогда не перезванивать и не переводить деньги; удалить СМС-сообщение; перезвонить своему мобильному оператору для решения «проблемы»; установить антивирусную программу на телефон.

Задание 4. Инструкция. Выберите из предложенных несколько верных вариантов ответа.

Задание. Разработчик игры «Stoon» потратил пять лет на её создание. Когда «Stoon» вышел в прокат, мальчик Лёня очень захотел приобрести эту игру. Придя в магазин, он обнаружил, что у неё высокая стоимость, поэтому решил обратиться в Интернет за помощью. В сети перейдя по первой ссылке, Лёня увидел надпись: «Игра «Stoon» бесплатная и скачать её можно по данной ссылке ниже». Из представленных ниже вариантов выберите тот, который Вы предложили бы Лёне.

Правильные ответы: 1. Скачать игру с данного сайта, так как там она бесплатная.

2. Попросить денег у родителей и купить в магазине.

3. Продолжить искать игру в интернете с возможностью купить её со скидкой.

Правильные ответы: б и в.

Используемая литература:

9. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010. 10. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.

11. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55. 12. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-

психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
13. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
14. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 15. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.
16. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

14. Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
15. сборник классных часов безопасность в интернете
http://news.scienceland.ru/2019/04/23/конкурс-задач-по-кибербезопасностик/
16. Копилочка активных методов обучения https://multiurok.ru/files/keis-po-informatike-bezopasnost-v-seti-internet.html 17. Безопасность детей в Интернете
18. https://www.cism-ms.ru/poleznye-materialy/virtualnye-druzya-s-kemobshchayutsya-deti-v-sotsialnykh-setyakh/
19. Копилочка активных методов обучения
20. http://www.moi-universitet.ru/ebooks/kamo/kamo/
21. Материалы сайта «Интернешка» http://interneshka.net/,
22. http://www.oszone.net/6213/
23. Материалы викторины «Безопасность детей в сети интернет
24. http://videouroki.net
25. Копилочка активных методов обучения
26. https://урок.рф/library/klassnij_chas_na_temu_pautina_sotcialnih_setej_181100.html

48. КИБЕРУРОК
«Компьтерная грамотность. Цифровой этикет» (для 8 класса)

Цель: повысить компьютерную грамотность взрослого и подрастающего поколения **Задачи:**

7. Познакомиться с понятием сленга.
8. Формировать навык цифрового этикета.
9. Профилактика кибербуллинга.

Оборудование: ноутбук, проектор для презентации,

Ход занятия

Здравствуйте! Сегодня мы с вами поговорим на тему «Что такое игровой сленг»? А вы знаете значение слова «сленг»?

Сленг – это разновидность речи, используемой преимущественно в устном общении отдельной относительно устойчивой социальной группой, объединяющей людей по признаку профессии или возраста.

Из этого определения следует, что сленг – разновидность нелитературной речи, к которой относятся:

1) профессионализмы,
2) вульгаризмы,
3) жаргонизмы,
4) лексика неформальных молодежных объединений и молодежной среды, часто называют сленгом.

Функции сленга:

У каждого слова и выражения, используемого в языке, есть какое-либо предназначение, и ничто не существует в языке просто так. Для чего же нужен сленг?

1) Сленг делает речь более краткой. (Сравним два выражения: Я вчера отправил другу письмо на электронную почту, на которое он не ответил- Я вчера отправил другу письмо на мыло, которое он проигнорил).
2) Сленг служит опознавательным знаком того, что этот человек принадлежит к данной социальной среде. Свой сленг есть у футбольных болельщиков, студентов, школьников и программистов и прочее.

Компьютерный сленг — разновидность сленга, используемого как профессиональной группой специалистов, так и пользователями компьютеров.

История появления слов из компьютерного сленга

В 80-х гг. XX в. компьютер стал доступен обычным людям. Его способности систематизировать и быстро находить нужные данные стали активно использовать в разных сферах, не связанных с наукой. Будучи довольно молодой, компьютерная отрасль еще не успела сформировать специфическую терминологию. И названия новым деталям и программам стали придумывать те, кто их создавали - вчерашние школьники и студенты. Не имея достаточного образования (не у кого было учиться - они первопроходцы), ребята называли многие приборы и команды по своему вкусу. Так что эти слова больше напоминали жаргон, чем профессиональные термины.

Особенности игрового сленга

Игровой сленг - условный язык, при помощи которого игроки в различных играх обмениваются информацией. Возникновение игрового сленга связывают с появлением массовых онлайн-игр, где он стал неотъемлемой частью игрового процесса.

В игровой ситуации игроки вырабатывают стратегию ведения игры, события разворачиваются быстро, и участникам происходящего нужно быстро доносить важную информацию до всех членов группы, и для решения этих задач используется соответствующая форма общения. Как следствие, используемые слова обычно короткие и информационно ёмкие. Это объясняется тем, что в игре победу или поражение определяют секунды, и быстрый обмен информацией становится важной задачей для игроков.

Игровой сленг является подмножеством компьютерного сленга, который не является грубым, таким же, как например жаргон панков, хиппи или блатной язык. Причиной является то, что профессия или увлечение, связанное с компьютерами, относится к высокоинтеллектуальным. Эмоциональность сленга особенно проявляется в оценке уровня игры другого человека. То есть, если игрок играет плохо, то его могут назвать целым рядом обидных выражений (нуб, рак), если же хорошо, то одобрительным (топовый). Эти эмоции могут проявляться к другим элементам (игровым предметам, навыкам и др.).

Краткость слов игрового сленга характеризуется тем, что слова обычно состоят из одного, двух, максимум трёх слогов.

Игровой сленг в настоящее время стал неотъемлемой частью речи учеников, которые не могут обойтись без таких сленговых слов, как: «комп», «виснуть», «клава», «винда».

По результатам опроса, проведённого в одной из школ, выяснилось, что более половины современных школьников активно пользуются словами, которые хорошо известны только заядлым геймерам.

В процессе общения ученики обмениваются различной информацией не только между собой, но и со своими родителями и учителями. Взрослые, к сожалению, не всегда могут понять то, что говорит современный ребёнок. А от уровня взаимопонимания очень зависит воспитание детей.

Сейчас вам предлагается групповая работа – кроссворд. Посмотрим, насколько хорошо вы знаете слова, которые часто используют любители видеоигр, и понимаете ли вы значение этих слов.

Приложение №1.

Мини-словарь игрового компьютерного сленга.

Слово	**Значение слова**
Ачивка	внутриигровое достижение
Босс	особенно сильный, уникальный противник
Донат	1) добровольное пожертвование, 2) покупка в игре за реальные деньги
Комбо	несколько сложных действий, выполненных подряд и без ошибок
Крафтинг	Создание предметов
Лаг	задержка между действием пользователя и откликом игры
Лутбокс	контейнер со случайным призом
Нуб	новичок
Скилл	Мастерство игрока
Спидран	Крайне быстрое прохождение
Стелс	скрытное прохождение
Хардкор	очень сложный уровень прохождения игры
Чекпоинт	точка сохранения
Читер	игрок, получивший преимущество нечестным путем

Используемая литература

7. http://www.elsmog.ru/index.php/mobtel/mobtel2.html Мобильный телефон вреднее курения.
8. http://www.shhitmobil.com.ua/clauses/show5 Вред мобильного телефона.
9. http://shkolazhizni.ru/archive/0/n-291/ Вредны ли мобильные телефоны. Антон Исаков.

10. http://www.inmoment.ru Сотовые (мобильные) телефоны. Галина Гатаулина.
11. http://www.ecohome.ru Мобильный телефон не причина вреда если….
12. http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html Мобильные телефоны вредны?

49. КИБЕРУРОК

«Как не попасть в сети Интернет-мошенникам»

(для 8 класса) Цель:

1. Формирование и развитие навыков поведения в опасных ситуациях, связанных с Интернет-мошенничеством.

Задачи:

1. Познакомить с видами Интернет мошенничества.
2. Формировать навыки эффективного поведения в ситуации мошенничества.
3. Развивать навыки достойного отказа.
4. Способствовать снятию психоэмоционального напряжения, вызванного использованием сетью Интернет.
5. Актуализировать у детей и подростков полученных знаний. 6. Развивать навыки поведения в опасных ситуациях.

Оборудование: карточки с ситуациями, таблички с названиями опасностей в Интернете, скриншоты страниц с опасными предложениями, картинки с изображением чемодана, корзины, мясорубки.

Организационный момент

Организационный момент

Учитель: Предварительно класс делится на 4 подгруппы. Распределившись на команды, ребята садятся.

Ход занятия

1. Приветствие, психологический настрой (3 минуты)

- Поприветствуем друг друга разными способами по условному сигналу: хлопком ладонь к ладони, плечом и т.д.

Правила поведения на занятии (3 минуты)

Примерные формулировки правил поведения на занятии: «можно»:

- не вставать с места при ответе;

- высказывать любое своё мнение и отстаивать его;
- уважать мнение своих товарищей;
- не бояться ошибиться, так как каждый человек имеет право на ошибку;
- помогать своему товарищу «нельзя»:
- перебивать говорящего товарища, выкрикивать с места; - смеяться над чужим мнением; - смеяться над ошибками. И другие.

Ход классного часа

2. Просмотр видеоролика “Безопасность платежей в интернете” **https://ligainternet.ru/videouroki/**

3. **Учитель:** Интернет-пространство расширяется, и с этим связано развитие кибер-мошенничества. Если люди уже научились распознавать мошенников в реальной жизни, и уже не «ведутся» на обычные шутки, то мошенников в интернете распознать гораздо сложнее. Как вы считаете, по каким причинам?

Да, глазами преступников не увидишь, и понять, что и как они могут сделать, непросто.

В кибер-пространстве мошенники работают по нескольким направлениям.

Учитель: Из каждой подгруппы приглашаются выйти по 1 представителю для выбора кейс-задания.

Организационный момент

Из каждой подгруппы вышли по 1 представителю для выбора кейс-задания. С выбранными заданиями представители сели на свои места. На выполнение кейс-задания дается 10-15 минут. По истечение предложенного времени, каждая подгруппа разбирает выбранный кейс и дает правильные ответы.

4. Упражнение «Чемодан. Корзина. Мясорубка»

Участники выбирают картинки чемодана, мусорной корзины или мясорубки в зависимости от полезности полученных знаний и отработанных навыков по теме безопасности в сети Интернет (или располагаются по принципу «Четыре (три) угла» в соответствии с размещёнными там картинками чемодана, корзины и мясорубки.

Чемодан – знания, умения и навыки были полезными, я возьму их с собой и буду пользоваться.

Мусорная корзина – ничего для меня не было полезным, мне не пригодятся эти навыки.

Мясорубка – мне ещё нужно осознать то, что я узнал на занятиях, обсудить с кем-то.

Завершение занятия

Учитель: Ребята, наше занятие подошло к концу. Будьте внимательны и соблюдайте правила безопасности в интернете.

Приложение 1.

Кейс - задания в конвертах для 4 команды.

Задание 1. Денежные «мышеловки»

1) «узнай местоположение по номеру телефона»

Задание. Вам предлагается зарегистрировать программу распознавания либо бесплатно, либо со взносом определенной суммы; программа часто оказывается обыкновенным вирусом. В любом случае, человек что-то теряет – деньги со своего счета или же информацию со своих аккаунтов, связанных с компьютером или телефоном. Либо незадачливого «шпиона» начинают терроризировать звонками и электронными письмами.

Как поступить. Правоохранители предупреждают, что узнать местоположение можно только с согласия абонента, либо по запросу в полиции (от оператора). Иные варианты не действуют. Поэтому откажитесь от слежки, не отправляйте смс и сообщения на указанные номера и уважайте приватность своих ближних.

2) «беспроцентный кредит»

Задание. Пользователю, желающему взять кредит, предлагают предоставить его быстро, легко и в любом объеме, если на счет мошенников будет перечислена круглая сумма. Действия преступников строятся как зеркальное отражение закона: к людям выезжают сотрудники, заполняются необходимые документы (получается согласие в том, что все добровольно и без претензий). Итог – ни денег, ни кредита.

Как поступить. Кредиты лучше не брать вообще; при необходимости сделайте заем у кого-нибудь из друзей или знакомых. При отсутствии возможности возьмите кредит в известном банке, придя лично в его филиал.

Задание 2. Денежные «мышеловки»

2.1. «Магазин на диване»

Задание. Вам предлагается приобрести желаемый товар по привлекательной цене (раз в 5 ниже среднестатистической), а возможно и вовсе бесплатно – вроде конфискат, вам делают подарок. Или к вам попадает журнал с товарами от известного магазина. Есть предложение – получить за заказ на ЭН-ную сумму ценный приз.

2.2. «Попрошайничество»
2.2. "Помощь в трудной жизненной ситуации"

Задание 1. К вам на почту поступает письмо с просьбой о материальной помощи, т.к. автор письма студент/начинающий/в сложной ситуации/денег нет, кушать нечего. На вас никто не давит, желаемая сумма может не указываться. Помочь человеку или нет – только ваше дело.

Задание 2. Вам приходит письмо с официального сайта благотворительной организации (детдома, приюта) с просьбой о материальной помощи какойлибо категории людей/человеку в социально опасном/затруднительном положении.

Как поступить. При желании помочь – проверьте адрес сайта (не дублер ли это), на кого оформлены реквизиты для перечисления денег. Позвоните в организацию (посетите ее), уточните номер счета и достоверность размещенной информации.

Задание 3. Денежные «мышеловки»
3.1. «Увеличение дохода»
Задание. Вы получаете письмо, где указывается, что денежный сайт предлагает эффективный способ удвоения капитала, (отправь 100 р, получи 500).
Или вам приходит сообщение о смерти дальнего родственника, наследником которого являетесь вы, однако нужно переслать налог на наследство.

Как поступить. Ни в коем случае ничего не высылайте; проверьте, действительно ли у вас был четвероюродный внучатый дядя из Канады, и ждите адвоката. Все юридические вопросы решаются с глазу на глаз, а не в интернете.

3.2. «Техподдержка»

Задание. вам приходит письмо с уведомлением, что аккаунт на каком-либо сайте взломан, или может быть заблокирован или удален (и т.д.), чтобы этого не случилось, необходима оплата (даже когда вы даже не регистрировались на сайте).

Как поступить: не оплачивать, не переходить по ссылкам (можете подхватить вирус) и не вводить данные. Зайдите на сайт с проверенного адреса, обновите страницу, можете обратиться к администратору сайта с вопросом. Если все же успели ввести пароль, сразу же смените его.

Задание 4. Денежные «мышеловки»

4.1. «Лотерея»

Задание. Вам приходит письмо о крупном выигрыше: вы выиграли деньги/машину/что-то еще, приз будет выслан/счет активирован, как только вы переведете некоторую сумму (пошлина, транспортные расходы и тд.). Вы не участвовали в конкурсе – неважно. Даже не слышали о нем – тем более. Это очень интересно, просыпается азарт – получить нечто, при этом ничего не делая.

Как поступить. Вспомните, принимали ли вы участие, знаете ли организацию, откуда у нее ваши контакты; не знаете ответа на вопрос – забудьте о сообщении и ничего не переводите.

6) отправка смс

Ситуация первая. «Ваш аккаунт блокирован, подтвердите смс… вы выиграли, отправьте смс… помоги выиграть в голосовании…, получи доступ к сайту…» Стоимость СМС - в 5-10 раз больше обычной.

4.2. "Шантаж"

Задание. В эту категорию относятся все сообщения насчет «нелегального доступа к услугам сайта», спама с вашей страницы, угроз выложить в сеть какие-либо материалы, где главным условием избавления от проблемы являются ваши действия по отправлению денежных средств шантажисту.

Как поступить. Можете написать провайдеру о спаме с угрозами, либо в техподдержку сайта, услугами которого вы якобы пользуетесь. Любую угрозу можно заскринить, распечатать и обратиться в полицию.

5. "Механический ущерб"

5. 1."Вирусы"

Задание. «Вы реальный человек – введите свой номер телефона». Вам либо приходит смс для ответа, либо вы автоматически подписываетесь на какуюто телефонную услугу и у вас со счета списывается ежедневно пара десятков рублей. Если вы получили сообщение со ссылкой на скачивание открытки, музыки, картинки или какой-нибудь программы, не спешите открывать её. Перейдя по ссылке, вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Как поступить. Внимательно читать всю информацию, особенно мелким шрифтом, со страниц, в частности - внизу сайта. Если не помогло, немедленно обратитесь в салон связи отключать услугу. Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто-то из знакомых вам людей, убедитесь в этом, позвонив оппоненту. Если отправитель вам не знаком, не открывайте письмо.

Помните, что установка антивирусного программного обеспечения на компьютер или мобильное устройство повышает вашу безопасность.

5.2. "Сайты-фейки"

Задание. Вы заходите на сайт, на котором вы уже зарегистрированы, по ссылке, но вам надо заново вводить почту и пароль от нее.

Как поступить. Проверьте адрес сайта и перейдите по проверенной ссылке.

6. "Работа в интернете"

Задание. Интернет является одним из способов заработка, но человек может стать жертвой мошенников: когда он выполнит работу по переводу текста или написанию реферата, то может остаться без обещанной платы.

Как поступить. Собираясь работать в сети, помните, что главный принцип – сначала оплата (хотя бы половинная), потом – работа.

Учитель предлагает ребятам поиграть в большую ролевую игру «Опасности сети Интернет»

- Учащимся раздаются роли (таблички с названиями опасностей в Интернете). На внешней стороне таблички написана приемлемая роль (например СМС, электронное письмо, Друг, Реклама, Интересный сайт, Антивирус, но с обратной стороны (невидимой для окружающих) на многих из них написана истинная роль, которую нужно будет грамотно сыграть: вирусы, спам, вредоносные ПО (программное обеспечение),
Интернет-хам (тролль), поддельный сайт, Интернет-мошенник (попрошайка), Незнакомец, который хочет заманить куда-нибудь, вызвать на встречу и другие. Несколько ребят играют роль пользователей, которые должны взаимодействовать с остальными (носителями пользы и вреда в Интернет-пространстве) и грамотно принимать или отсеивать поступающую информацию.

Используемая литература:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.
2. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: метод.руководство/ под ред. Г.У. Солдатовой. – М.: Федеральный институт развития образования, 2012. – 48с.
3. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
4. Солдатова Г.У., Зотова Е.Ю., Чекалина А.И., Гостимская О.С. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете / под ред. Г.У. Солдатовой. – М., 2011.
5. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.
6. Солдатова Г.У., Рассказова Е.И. Из-за интернета я не ел и не спал. Зависимость или новый образ жизни?// Дети в информационном обществе.– 2011. – № 9. – С. 22–29. 7. Солдатова Г.У., Рассказова Е.И. Как им помочь. Ребенок в интернете: запрещать, наблюдать или объяснять? // Дети в информационном обществе.– 2012. – № 10. – С. 26–33.

8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"

Список использованных ресурсов

1. Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
2. сборник классных часов безопасность в интернете http://news.scienceland.ru/2019/04/23/конкурс-задач-покибербезопасности-к/
3. Копилочка активных методов обучения https://multiurok.ru/files/keispo-informatike-bezopasnost-v-seti-internet.html
4. Безопасность детей в Интернете https://www.cism-ms.ru/poleznyematerialy/virtualnye-druzya-s-kem-obshchayutsya-deti-v-sotsialnykhsetyakh/
5. Копилочка активных методов обучения http://www.moiuniversitet.ru/ebooks/kamo/kamo/
6. Материалы сайта «Интернешка» http://interneshka.net/, http://www.oszone.net/6213/
7. Материалы викторины «Безопасность детей в сети интернет https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta
8. Копилочка активных методов обучения http://save.nios.ru/sites/save.nios.ru/files/materialy/yurina_vneklassnoe_meropriyatie_4.moshennichestvo_v_seti.pdf

50. КИБЕРУРОК
«Информационная безопасность школьников» (для 7 класса)

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; частичнопоисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Этапы урока:

16. Организация начала урока. Постановка цели урока. Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html Постановка темы и главного вопроса урока.
17. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).
18. Практическая работа. Поиск информации в сети интернет. Дискуссия по найденному материалу.
19. Закрепление изученного материала. Рекомендации по правилам безопасной работы в интернет. Тестирование.
20. Подведение итогов урока. Оценка работы группы. Домашнее задание.

Ход урока

7. 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=pld70b 32df5c50a1d7&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? **8. Изучение нового материала.**

Игра «за или против».

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

отражающие Противоположную точку зрения.

16. И нтернет имеет неограниченные возможности дистанционного Образования.

И это хорошо!

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

18. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.

19. Интернет является мощным антидепрессантом.

20. 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»).

Физкультурная 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?»

12. 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_room a.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.

13. 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.

14. 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:

8. Дать определение понятию «информационная безопасность». 9. Составить информационный лист «моя безопасная сеть».

Используемая литероатура:

Ссылки на web-ресурсы:

7) http://www.kaspersky.ru – антивирус «лаборатория касперского»;

8) 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;

11) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;

12) http://www.rgdb.ru – российская государственная детская библиотека.

51. КИБЕРУРОК
«Урок по безопасности в сети Интернет
(для 8 класса)

Цель: формирование информационно-коммуникативной компетенции. Оборудование: мультимедийный проектор, компьютер, карточки с заданиями. Организационный момент Ход урока**:**

- 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 карточекпамяток)*

- 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 карточекпамяток)*

- 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 карточекпамяток)*

- 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 - информационнопознавательный 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/

52. **КИБЕРУРОК**

«Безопасность школьников в сети Интернет» (для 8 класса)

Цель: актуализируют знания об основных угрозах сети Интернет и методах борьбы с ними; **Задачи:**

- познакомиться с понятием «Интернет», «Интернет-угроза»; - изучить приемы безопасности при работе в сети Интернет.
- формирование приёмов логического мышления;
- развитие способности анализировать и обобщать, делать выводы.
- воспитание аккуратности, точности, самостоятельности; - привитие навыка групповой работы, сотрудничества.
- 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 Интернет можно 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);
- фи шинг - 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 киберпреступнику, 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 ✓ 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.
- ✓ 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.
- ✓ 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.
- ✓ 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.

- ✓ Старайтесь не использовать функцию запоминания паролей, которую предлагают многие почтовые ящики и социальные сети.
- ✓ Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях .
- ✓ Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- ✓ При регистрации на сайтах, старайтесь не указывать личную информацию
- ✓ Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.
- ✓ 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. ✓ Не добавляйте в друзья в социальных сетях всех подряд.

Использованы материалы:

1. Мельников В.П. Информационная безопасность и защита информации:
2. учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр
3. «Академия», 2010. – 336 с.
4. 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.

53. КИБЕРУРОК
«Безопасность в сети Интернет» (для 8 класса)

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

1. ознакомление с возможными угрозами сети Интернет;

2. приобретение навыка выявления мошеннических манипуляций над пользователем;
3. выработка тактики безопасного поведения пользователя в сети; 4. обучение ответственному использованию online-технологий;
5. воспитание дисциплинированности при работе в сети.

Тип урока: урок изучения нового материала. **План урока:**

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

Ход урока:

Организационный момент, 1-2 мин.:

- сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- краткий план деятельности.

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)

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

Проблема	**Способы преодоления**
Вирусы **Компьютерный вирус** 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 интернетмагазинах.
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

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).

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?" **Итог урока (2-3 мин.):**

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! **Использованы материалы:**

2. 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.
3. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус
4. Социальная сеть работников образования http://nsportal.ru/
5. База образовательных ресурсов http://obrazbase.ru/inform/uroki-imeropriyatiya
6. Интернет СМИ «ваш личный интернет» http://content-filtering.ru

54. КИБЕРУРОК
«Безопасность в сети Интернет. Интернет-угрозы»
(для 8 класса)

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)

Компьютерный вирус — 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 также 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:

2. 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

3. 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

4. Какой из приведенных паролей является более надежным A. 123456789

B. qwerty

C. annaivanova

D. 13u91A_Ivanova

5. 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

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

A. Mozilla Firefox

B. Internet Explorer

C. Google Chrome

D. Opera

7. 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

8. 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

9. 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

10. 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

11. 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.); 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:

2. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.

3. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»

4. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

55. КИБЕРУРОК
«Безопасность в сети Интернет: правила безопасной работы в сети» (для 8 класса)

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 onlinetехнологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частичнопоисковый, 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:**

6. Организация начала урока. Постановка цели урока. Просмотр видеоролика. Постановка темы и главного вопроса урока.
7. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения учащихся).

8. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.

9. Закрепление изученного материала. Рекомендации по правилам безопасной работы.

Тестирование.

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

Ход урока

6. 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?

7. 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?»

8. 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?

9. 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.

10. 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.).

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 9-Х КЛАССОВ

56. КИБЕРУРОК
«Безопасный интернет» (для 9 класса5)

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;

частичнопоисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Этапы урока:

21. Организация начала урока. Постановка цели урока. Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html Постановка темы и главного вопроса урока.

22. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).

23. Практическая работа. Поиск информации в сети интернет. Дискуссия по найденному материалу.

24. Закрепление изученного материала. Рекомендации по правилам безопасной работы в интернет. Тестирование.

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

Ход урока

9. 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=pld70b 32df5c50a1d7&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?

10. Изучение нового материала.

Игра «за или против».

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

21. И нтернет имеет неограниченные возможности дистанционного Образования.

И это хорошо!

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

23. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.

24. Интернет является мощным антидепрессантом.

25. 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»).

Физкультурная 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?»

15. 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_room a.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.

16. 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.

17. 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:

10. Дать определение понятию «информационная безопасность». 11. Составить информационный лист «моя безопасная сеть».

Используемая литероатура:

Ссылки на web-ресурсы:

9) http://www.kaspersky.ru – антивирус «лаборатория касперского»;

10) 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;

13) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;

14) http://www.rgdb.ru – российская государственная детская библиотека.

57. КИБЕРУРОК
«Безопасный Интернет. Информационная культура общения»
(для 9 класса)

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 onlinetехнологий;
- 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; частичнопоисковый, 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

Приложение 1.

Тестирование к уроку «Безопасный интернет»

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

- номер домашнего телефона ○ номер мобильного телефона ○ свой e-mail ○ названия любимых книг, песен ○ номер своей школы, класса ○ свои фотографии
- никнейм
- кличку своего домашнего питомца

2. Последствиями сетевой атаки для Вашего компьютера могут быть:

- неработоспособность программ ○ поломка компьютера ○ кража или уничтожение информации
- заражение компьютера вредоносными программами

3. Поддельный сайт – это…

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

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

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

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

d) переслать его пяти друзьям

e) переслать его не пяти, а десяти друзьям

f) не пересылать такие письма

g) 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

3. 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

Приложение 2.

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

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 программызащитники, 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 смсподписка 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 интернетмагазинах.
- 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.);

Федеральный закон Российской Федерации № 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 ребёнке порочные наклонности, сформировать у ребёнка искажённую картину мира и неправильные жизненные установки.)

58. КИБЕРУРОК
«Безопасность в Интернете» (для 9 класса)

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

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. **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).

Закрепление материала Учитель.

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

Итог урока

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

Рефлексия

59. КИБЕРУРОК
"Социальные сети: за и против" (для 9 класса)

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 Интернетдружбы.

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

60. КИБЕРУРОК
«Урок по безопасности в сети Интернет
(для 9 класса)

Цель: формирование информационно-коммуникативной компетенции. Оборудование: мультимедийный проектор, компьютер, карточки с заданиями. **Организационный момент Ход урока:**

- 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 карточекпамяток)*

- 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 карточекпамяток)*

- 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 - информационнопознавательный 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/

61. КИБЕРУРОК
«Безопасность в сети Интернет» (для 9 класса)

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

1. ознакомление с возможными угрозами сети Интернет;
2. приобретение навыка выявления мошеннических манипуляций над пользователем;
3. выработка тактики безопасного поведения пользователя в сети; 4. обучение ответственному использованию online-технологий;
5. воспитание дисциплинированности при работе в сети.

Тип урока: урок изучения нового материала. **План урока:**

- Организационный момент (1-2 мин.);

- Актуализация знаний (7 мин.);
- Объяснение нового материала (30-35 мин.);
- Самостоятельная работа (7-10 мин.);
- Итог урока (2-3 мин.);

Ход урока:

Организационный момент, 1-2 мин.:

- сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- краткий план деятельности.

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)

Объяснение нового материала (25-30 мин.):

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

- Вредоносные программы
- Кража информации
- Халатность сотрудников
- Хакерские атаки
- Финансовое мошенничество
- Спам
- 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

	Проблема	**Способы преодоления**

	Вирусы **Компьютерный вирус** 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 интернетмагазинах.
	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

	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).

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

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

○ Административному кодексу ○ Трудовому кодексу ○ Уголовному кодексу ○ Гражданскому кодексу

Какой из приведенных паролей является более надежным

○ A. 123456789 ○ qwerty

○ annaivanova ○ 13u91A_Ivanova

Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо: ○ Установить несколько антивирусных программ ○ Удалить все файлы, загруженные из сети Интернет ○ Своевременно обновлять антивирусные базы ○ Отключить компьютер от сети Интернет

Какие действия не рекомендуется делать при работе с электронной почтой? ○ Отправлять электронные письма ○ Добавлять в свои электронные письма фотографии ○ Открывать вложения неизвестной электронной почты ○ Оставлять электронные письма в папке

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

○ Отправить SMS сообщение

○ Выполнить форматирование жесткого диска ○ Перезагрузить компьютер ○ Не отправлять SMS сообщение

Зачем необходимо делать резервные копии? ○ Чтобы информация могла быть доступна всем желающим ○ Чтобы не потерять важную информацию

○ Чтобы можно было выполнить операцию восстановления системы

○ Чтобы была возможность распечатать документы *А что для вас является "безопасным интернетом*

Итог урока (2-3 мин.):

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! **Использованы материалы:**

7. 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.
8. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус
9. Социальная сеть работников образования http://nsportal.ru/
10. База образовательных ресурсов http://obrazbase.ru/inform/uroki-imeropriyatiya
11. Интернет СМИ «ваш личный интернет» http://content-filtering.ru

62. КИБЕРУРОК

"Безопасный интернет" (для 9 класса)

Аннотация

Данный урок разработан для учащихся 9-11 классов. 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

Разработка 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

1. Введение.
2. Проблемы современной жизни в киберпространстве.
3. Наиболее злободневные вопросы.
4. Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет.

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.

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 интернетмагазинах.
- 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.

63. КИБЕРУРОК
«Безопасность в сети Интернет. Интернет-угрозы. Методы профилактики» (для 9 класса)

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:

7. Организационный момент (1-2 мин.);
8. Введение в тему (3-5 мин.);
9. Объяснение нового материала (30-35 мин.);
10. Физкультминутка (1 мин.);
11. Самостоятельная работа (7-10 мин.); 12. Итог урока (2-3 мин.);

Ход урока:

4. **Организационный момент, 1-2 мин.:**

- ✓ сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- ✓ краткий план деятельности.

5. **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!

6. **Объяснение нового материала (27-30 мин.):**

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

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.

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

Компьютерный вирус — 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 также 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.

6. 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).

7. 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:

12. 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

13. 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

14. Какой из приведенных паролей является более надежным

A. 123456789

E. qwerty

F. annaivanova

G. 13u91A_Ivanova

15. 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

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

A. Mozilla Firefox

B. Internet Explorer

C. Google Chrome

D. Opera

17. 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

18. 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

19. 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

20. 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

21. 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.

7. Итог урока (2-3 мин.); 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:

5. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.

6. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»

7. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

64. КИБЕРУРОК
«Безопасность в сети Интернет. Правила безопасного пользования» (для 9 класса)

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 onlinetехнологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частичнопоисковый, 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:**

11. Организация начала урока. Постановка цели урока. Просмотр видеоролика. Постановка темы и главного вопроса урока.
12. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения учащихся).

13. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.

14. Закрепление изученного материала. Рекомендации по правилам безопасной работы.

Тестирование.

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

Ход урока

11. 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?

12. 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?»

13. **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?

14. **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.

15. 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.).

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 10 КЛАССОВ

65. КИБЕРУРОК
«Безопасность в сети интернет. Обучение навыкам поведения в Интернете» (для 10 класса)

Цель: обучение навыкам поведения в Интернет сети, навыкам уверенного поведения (умение сказать: «Нет!»), развитие способности к стрессоустойчивости, поиск и использование внутренних ресурсов.

Задача: защитить детей от информации, распространяемой в сети Интернет, причиняющей вред их здоровью, физическому, психическому, духовному и нравственному развитию.

Вступительное слово ведущего (1 минута).

Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями в социальных сетях, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Мы получили доступ к практически любой информации, хранящейся на миллионах компьютерах во всем мире. Но с другой стороны, миллионы компьютеров получили доступ к вашему компьютеру, а, значит, к каждому из вас. И не сомневайтесь, они пользуются этой возможностью. И никогда-то, а прямо сейчас. Поэтому очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.

Ведущий задает участникам вопрос: «Как вы считаете подвергаетесь ли вы опасности, когда пользуетесь интернетом? Если да, то какой?» Ответы фиксируются на доске. Резюме. ***Упражнение № 1 «Игра «Весы».*** Работа в мини группах по 3-5 чел.

Участникам группы необходимо, привести по 7-10 примеров положительных и отрицательных возможностей интернета.

Выступления групп, резюме, рефлексия.

Интернет – это безграничный мир информации. Он дал людям много положительных возможностей:

– главное преимущество этого ресурса – огромные возможности поиска разнообразной информации.

– коммуникативные возможности (расстояние между людьми сегодня резко сократилось, появилось больше возможностей для общения, быстрого обмена информацией);

– развлекательные (игры, видео и т.д.).

Однако, кроме хорошего, в виртуальном мире присутствует много негативного.

- Мошенничество (доступ к паролям, конфиденциальной информации
и т.д.)

- Появление интернет-зависимости (интернет-сёрфинг, пристрастие к виртуальному общению и к виртуальным знакомствам)

-Так же существует риск Вовлечение в деструктивные группы (экстремистские, сектантсткие, аутоагрессивные, антироссийский антисемейные)

- Негативные интернет-явления (кибербуллинг, троллинг и др.)

Упражнение 2. «Что такое аффирмация»

Для выполнения задания ведущий объясняет ребятам понятие «аффирмация», «мотиватор», «демотиватор».

Аффирмация (от лат. *affirmatio* — подтверждение) — краткая фраза, содержащая вербальную формулу, которая при многократном повторении закрепляет требуемый образ или установку в подсознании человека, способствуя улучшению\ухудшению его психоэмоционального фона и стимулируя положительные\отрицательные перемены в жизни.

Мотиватор - то, что мотивирует, побуждает человека к определённому поведению

Демотива́тор (демотивационный постер) — разновидность настенного плаката. Демотиватор пародирует мотиваторы(плакаты, предназначенные для создания рабочего настроения), используя схожие с мотиваторами изображения, но с подписями, формально направленными на создание атмосферы обречённости и бессмысленности человеческих усилий.

Формат демотиватора включает базовое изображение в рамке, обрамлённое относительно широкими, чаще всего чёрными, полями и снабжённое по нижнему более широкому полю лозунгом, выполненным крупным белым или жёлтым шрифтом. Помимо слогана многие демотивационные постеры содержат текст-пояснение, выполненное мелким шрифтом, так или иначе оттеняющее смысловое наполнение изображения и/или слогана.

Ведущий показывает картинки «демотиваторы» и предлагает преобразовать их в мотиваторы Например:

Демотиватор	Мотиватор

	
Во всем виновато осень…	*- Какая классная все-таки весна! -* *Ты что! У всех осень.*
	- Мне все-равно, что у всех. Весна, говорю, классная

Упражнение 3. «Создай свой мотиватор»

Для выполнения задания ведущий вводит понятие «самопомощь». Далее ведущий предлагает, воспользовавшись своими телефонами, планшетами, выбрать фотографию, которая служит напоминанием о самом счастливом моменте жизни (можно предложить нарисовать на листе бумаги предмет, сюжет, явление природы и т.п.). Ребята вспоминают когда было сделано это фото, почему именно этот сюжет напоминает о счастье, насколько сильными были эмоции в тот момент. Затем участникам предлагается придумать фразу (вспомнить цитату), которая бы отражала это эмоциональное состояние.

В конце упражнения ведущий дает домашнее задание: оформить на компьютере свой мотиватор и раместить его на своей социальной страничке.

Упражнение 4. «Придумай предложение»

Предлагалось выполнить еще одно упражнение, которое помогает переключить свои эмоции с негативных на позитивные.

Учащимся предлагается несколько цепочек слов: «учеба — желание — успех», «ссора — решение — дружба», «проблема — помощь — родной человек». Им надо придумать как можно больше предложений с этими словами. При составлении предложений слова можно менять местами.

Упражнение 5. «Сейчас у меня нет…»

Участникам тренинга предлагается написать список того, чего на данный момент в их жизни нет. На выполнение дается пять минут.

В списке у ребят оказались желанные, но недоступные им сейчас вещи: компьютер, модный телефон, своя комната, собака и т.д.

Затем ведущий предлагает посмотреть на свою жизнь с другой стороны, задавая вопрос «Вы сейчас здоровы? Значит, чего еще у вас нет? (болезни). Ребятам предлагается продолжить список с данной точки зрения: чего нет плохого (ссоры с другом, пустого холодильника, грязной одежды, школы за 10 км. от дома, платного обучения, жестоких родителей и т.д.). Желательно, чтобы список-продолжение был длиннее, чем составленный на первом этапе. ***Упражнение 6. «Предложи альтернативу».***

Ведущий акцентирует внимание детей на том, почему не стоит обсуждать со сверстниками игры и сайты деструктивного характера, подводит к выводу о том, что «запретный плод – сладок».

Ведущий ставит перед участниками тренинга вопросы: Что делать, если ты узнал, что твой сверстник ведет себя деструктивно (играет в «плохие» игры, начал курить, принимать алкоголь или ПАВ, связался с «дурной» компанией)? Что делать, если твой сверстник предлагает тебе подобное?

В ходе обсуждения ребята вспоминают правила «Как сказать: «Нет!» и отрабатывают навыки ведения диалога без отрицания.

Например,:

Вместо «Это плохая игра. Не играй в нее!», предложи альтернативу «Давай поиграем в футбол».

Вместо «Не кури! Это вредно», предложи альтернативу «Я занимаюсь в бассейне, пойдем со мной».

66. КИБЕРУРОК

«Безопасность в Интернете. Формирование навыков безопасного и ответственного поведеняи в сети» (для 10 класса)

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

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.

Новый материал

Группа 1

Вирусы

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

Мошенники в Интернете

6. Сайты – двойники
7. Интернет – шантаж
8. Предложение работы на дому и не только
9. «Лохотрон» на проверке безопасности
10. 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

4. Этические нормы Интернета
5. «Крэкерские» сайты и «ломаные» программы
6. 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).

Закрепление материала Учитель.

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

Итог урока

Домашнее задание (по выбору учащихся)

3. Запишите в тетрадь основные правила безопасного поведения в сети Интернет

4. Придумать сказку для учащихся младших классов об осторожности в Интернете

Рефлексия

67. КИБЕРУРОК

«Безопасность в сети Интернет. Опасные угрозы и методы борьбы с ними» (для 10 класса)

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

1. ознакомление с возможными угрозами сети Интернет;
2. приобретение навыка выявления мошеннических манипуляций над пользователем;
3. выработка тактики безопасного поведения пользователя в сети; 4. обучение ответственному использованию online-технологий;
5. воспитание дисциплинированности при работе в сети.

Тип урока: урок изучения нового материала. **План урока:**

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

Ход урока:

Организационный момент, 1-2 мин.:

- сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- краткий план деятельности.

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)

Объяснение нового материала (25-30 мин.):

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

- Вредоносные программы
- Кража информации
- Халатность сотрудников
- Хакерские атаки
- Финансовое мошенничество
- Спам
- 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

	Проблема	**Способы преодоления**
	Вирусы **Компьютерный вирус** 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 интернетмагазинах.
	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

	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).

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

8. 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

9. Какой из приведенных паролей является более надежным

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

10. 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

11. 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

12. 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

13. 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

---

14. А что для вас является "безопасным интернетом?" **Итог урока (2-3 мин.):**

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! **Использованы материалы:**

12. 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.

13. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус

14. Социальная сеть работников образования http://nsportal.ru/

15. База образовательных ресурсов http://obrazbase.ru/inform/uroki-imeropriyatiya

16. Интернет СМИ «ваш личный интернет» http://content-filtering.ru **Киберурок "Безопасный интернет"**

Аннотация

Данный урок разработан для учащихся 9-11 классов. 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

Разработка 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

5. Введение.
6. Проблемы современной жизни в киберпространстве.
7. Наиболее злободневные вопросы.
8. Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет.

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.

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 интернетмагазинах.
- 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!

68. КИБЕРУРОК
«Безопасность в сети Интернет» (для 10 класса)

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 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:

13. Организационный момент (1-2 мин.);
14. Введение в тему (3-5 мин.);
15. Объяснение нового материала (30-35 мин.);
16. Физкультминутка (1 мин.);
17. Самостоятельная работа (7-10 мин.); 18. 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. **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!

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

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

15. Вредоносные программы
16. Кража информации
17. Халатность сотрудников
18. Хакерские атаки
19. Финансовое мошенничество
20. Спам
21. 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)

Компьютерный вирус — 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 также 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.

8. 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).

9. **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:

22. 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

23. 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

24. Какой из приведенных паролей является более надежным

A. 123456789
H. qwerty
I. annaivanova
J. 13u91A_Ivanova

25. 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

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

A. Mozilla Firefox
B. Internet Explorer

C. Google Chrome

D. Opera

27. 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

28. 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

29. 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

30. 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

31. 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.

8. Итог урока (2-3 мин.); 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:

8. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.

9. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»

10. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

69. КИБЕРУРОК
«Безопасность в сети Интернет. Правила пользования»
(для 10 класса)

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 onlinetехнологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частичнопоисковый, 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:**

16. Организация начала урока. Постановка цели урока. Просмотр видеоролика. Постановка темы и главного вопроса урока.
17. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения учащихся).

18. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.

19. Закрепление изученного материала. Рекомендации по правилам безопасной работы.

Тестирование.

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

Ход урока 16. 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?

17. 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?»

18. **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?

19. **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.

20. 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.).

70. КИБЕРУРОК:
«Чтобы я делал, если бы не было сети Интернет» (для 10 класса)

Цель киберурока: сформировать представления об альтернативных способах проведения досуга вне сети интернет.

Форма проведения: фотокросс.

Используемые термины:

Фотокросс – это творческие соревнования в условиях временных, тематических и инструментальных ограничений.

Кросс – это объект для съемки (вещь, чувство, ситуация, процесс, сюжет или какой-либо другой объект материальной или нематериальной природы).

Процедура проведения

Подготовительный этап. В ходе подготовительного этапа все участники делятся на команды, в каждой команде не менее 5 человек, количество команд не более 5. Организаторам необходимо убедиться в технической оснащенности участников (наличие устройств с функцией фотографирования). На данном этапе озвучиваются правила участия в фотокроссе, ограничения по времени проведения.

Правила участия в фотокроссе общее время прохождения всех этапов – не более часа; команда не должна покидать территории образовательной организации; каждую команду в ходе выполнения заданий фотокросса сопровождает педагогический работник; фотографировать разрешается все, что, на взгляд участников, соответствует тематике кросса, задания; в каждой команде должен быть выбран капитан из числа обучающихся, который будет отвечать за взаимодействие с организаторами фотокросса и координировать деятельность всей команды.

Основной этап. Обучающимся необходимо передвигаться по кабинетам (в маршрутных листах каждой команды указана информация о месте старта). Команды необходимо направлять таким образом, чтобы они находились на разных локациях, в разное время.

В каждом кабинет, ответственный за организацию, выдает капитану задание:

Задание локации № 1

Предполагаемая локация организована в спортзале или кабинете со спортивным инвентарем. Тема фотографии: «Наши Олимпийские игры!» Текст задания: «Сделайте интересные групповые фотографии на спортивную тематику. На фотографии должен быть запечатлен момент

занятия спортом. Оригинальность и нестандартный подход приветствуется».

Задание локации № 2

Тема фотографии: «Весна – время ловить улыбки!» Текст задания: «Сделайте фотографию так, чтобы на ней не было людей, но была весна и повод для улыбки».

Задание локации № 3

Тема фотографии: «Я – ты – мы!» Текст задания: «При помощи фотографии надо показать друзей, или запечатлеть момент, который воплощает дружбу». ***Задание локации № 4.***

Предполагаемая локация в библиотеке или в кабинете литературы. Тема фотографии: «Селфи с книгой» Текст задания: «Сделайте креативное фото с интересной книгой, а может вам удастся изобразить героев или передать основную мысль произведения?» ***Задание локации № 5.***

Тема фотографии: «Вне сети» Текст задания: «Сделайте самую креативную фотографию, где вы отобразите мир без интернета». На финише участники должны сдать свои работы (фотографии) в электронном виде. Вместе с кадрами участники сдают маршрутные листы с подписанными наименованиями файлов с фотографиями по каждому заданию.

Подведение итогов. Подведение итогов фотокросса проводит жюри из числа педагогических работников, принявших участие в организации и проведении мероприятия. При подведении итогов учитывается скорость выполнения, мастерство и оригинальность. **Критерии оценок фотографий:**

– соответствие снимка теме задания;

– оригинальность идеи;

– качество выполненных заданий.

Общая оценка за Фотокросс выставляется команде путем сложения оценок за все конкурсные снимки.

Жюри вправе исключить из зачета кадры, грубо нарушающие правила или общепринятые этические нормы.

При равном количестве баллов лучшее место присуждается участнику, пришедшему на финиш раньше.

После того, как победители будут объявлены и награждены, обучающимся предлагается завершить фотокросс **флешмобом** «Сделай свой выбор в пользу разнообразной и насыщенной жизни!» (Групповое фото с шарами и иным реквизитом).

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ УЧАЩИХСЯ 11 КЛАССОВ

71. КИБЕРУРОК

«Безопасность в Интернете» (для 11 классов)

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

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

Мошенники в Интернете

11. Сайты – двойники
12. Интернет – шантаж
13. Предложение работы на дому и не только
14. «Лохотрон» на проверке безопасности
15. 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

7. Этические нормы Интернета
8. «Крэкерские» сайты и «ломаные» программы
9. 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)

5. Запишите в тетрадь основные правила безопасного поведения в сети Интернет

6. Придумать сказку для учащихся младших классов об осторожности в Интернете

VII. Рефлексия

Киберурок "Безопасный интернет"

Аннотация

Данный урок разработан для учащихся 9-11 классов. 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

Разработка 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

9. Введение.
10. Проблемы современной жизни в киберпространстве.
11. Наиболее злободневные вопросы.
12. Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет.

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.

Проблемы современной жизни в киберпространстве

Какие опасности могут подстерегать пользователей Интернета?

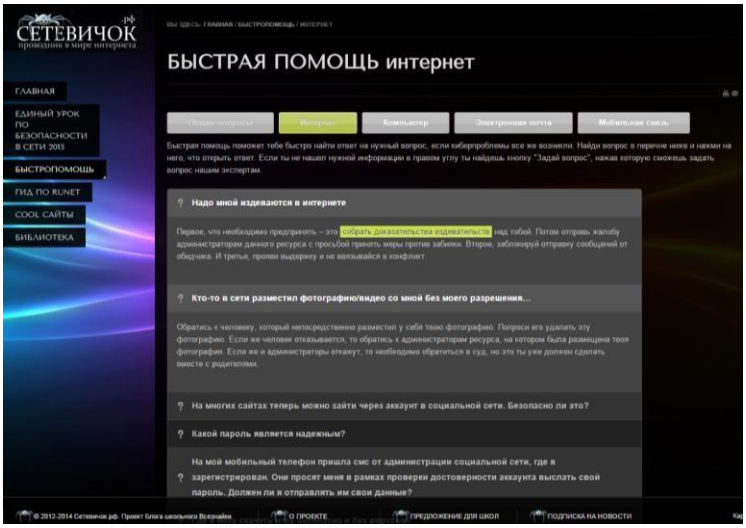
В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Для этого они могут использовать вирусное программное обеспечение (или

«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 интернетмагазинах.

- 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!

72. КИБЕРУРОК
«Безопасность в сети Интернет» (для 11 класса)

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.);
7. **Ход урока:**

Организационный момент, 1-2 мин.:

- ✓ сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- ✓ краткий план деятельности.

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!

Объяснение нового материала (27-30 мин.):

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

- Вредоносные программы
- Кража информации
- Халатность сотрудников
- Хакерские атаки
- Финансовое мошенничество
- Спам
- 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)

Компьютерный вирус — 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 также 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.

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 – флешкарте, 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).

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 своими результатами. 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…*** ○ Административному кодексу ○ Трудовому кодексу ○ Уголовному кодексу ○ Гражданскому кодексу
2. ***Какой классификации вирусов на сегодняшний день не существует?***
   - ○ По поражаемым объектам
   - ○ По поражаемым операционным системам и платформам ○ По количеству поражаемых файлов ○ По дополнительной вредоносной функциональности
3. ***Какой из приведенных паролей является более надежным*** ○ 123456789 ○ qwerty ○ annaivanova ○ 13u91A_Ivanova
4. ***Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:***
   - ○ Установить несколько антивирусных программ ○ Удалить все файлы, загруженные из сети Интернет ○ Своевременно обновлять антивирусные базы ○ Отключить компьютер от сети Интернет
5. ***Какой из браузеров считается менее безопасным, чем остальные:***
   - ○ Mozilla Firefox ○ Internet Explorer ○ Google Chrome ○ Opera
6. ***Какие действия не рекомендуется делать при работе с электронной почтой?***
   - ○ Отправлять электронные письма ○ Добавлять в свои электронные письма фотографии ○ Открывать вложения неизвестной электронной почты ○ Оставлять электронные письма в папке Отправленные
7. ***Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?***
   - ○ Отправить SMS сообщение

- Выполнить форматирование жесткого диска
- Перезагрузить компьютер ○ Не отправлять SMS сообщение

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

- Трудовому кодексу РФ ○ Доктрине информационной безопасности РФ ○ Стратегии развития информационного общества РФ ○ Конвенции о правах ребенка ***9. Зачем необходимо делать резервные копии?***
- Чтобы информация могла быть доступна всем желающим ○ Чтобы не потерять важную информацию
- Чтобы можно было выполнить операцию восстановления системы
- 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?

- Перезагрузить компьютер ○ Отформатировать жесткий диск ○ Закрыть сайт и выполнить проверку ПК ○ Выключить компьютер. **Итог урока (2-3 мин.); 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:

11. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.

12. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»

13. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

73. КИБЕРУРОК

«Урок медиабезопасности

«Предупреждён – значит вооружён» (для 11 класса)

Цель: Способствовать формированию знаний о правилах безопасного поведения в совре- менной информационной среде, в частности – сети Интернет.

Задачи:

Заставить задуматься о своем месте в этом мире.

Познакомить видами Интернет-угроз и противоправных посягательствах в сети Интер нет.

Познакомить студентов с правилами медиабезопасности, с сайтами помощи в случае Интернет-угроз.

Сформировать чувство ответственности за свое пребывание в Интернет, за воспитание будущих поколений.

Продемонстрировать методику проведения подобных занятий для учащихся

- **Оборудование:** анкеты, памятки, презентация, видеофрагменты («Безопасность в Интернете», «Развлечения и безопасность в Интернете», социальный ролик «Безопасный Интернет-детям!»), проектор, ПК.

Используемые понятия:

- **«Интернет-угроза»** - действие в сети Интернет, которое причиняет вред пользователю Интернета путем опубликования или пересылки некоей информации, а также Интернет- коммуникация, направленная на причинение вреда собеседнику в Сети.
- **«Секта»** - религиозная организация.
- **«Вербовка»**, «Вербовать» - найти желающего на выполнение каких-либо работ.
- **«Киберунижение»** – распространение унижающей достоинство человека информации (изображение, видео, текста) в Интернете, а также использование Интернета для оскорблений и травли.
- **«Экстремистские группировки»** - организованные группы людей, занимающиеся преступной и опасной для людей деятельностью (например: убийство, нанесение тяжких теле сных повреждений, массовые беспорядки, терроризм)
- **Терроризм** – массовое устрашение либо уничтожение людей.

Ход киберурока.

1. Организационный момент.

- Добрый день, ребята! Нашу встречу с вами я хочу начать со следующего стихотворения: Ты есть, я есть, он есть, А жизнь у каждого своя.

И ей цена – достоинство и честь, Есть возраст переходных лет, Какой бы сложной не была она. Для многих начинается рассвет, А кто-то погружается во тьму.

Ты есть, я есть, он есть,

Лишь вместе мы сумеем зло пресечь И сохранить достоинство, чтоб жить.

2. Сообщение темы, цели, задач занятия.

- Сегодня наш урок называется «Урок медиабезопасности». Как вы полагаете, о чем мы на этом уроке поговорим? *(ответы)*

А кто может сказать, что такое медиабезопасноть? *(ответы)*

Слово «медиабезопасность» сочетает в себе два термина – медиаграмотность и информационная безопасность.

В международном праве «***Медиаграмотность*** - грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг». В российском законодательстве «***Информационная безопасность детей*** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию». Такие понятия появились благодаря инициативе Уполномоченного при Президенте РФ по правам ребенка Павла Астахова, который сказал:

«*Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медаграмот- ности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать*».

Я думаю, что каждый хочет жить в мире и безопасности, а это значит, что на душе будет радостно и спокойно. Мы не зря поднимаем сегодня этот вопрос. Как было бы здорово, если бы каждый человек соблюдал все правила приличия, был бы всегда доброжелателен. Но, к сожалению, так не бывает. И очень часто по чьей-то вине, нарушается мир другого человека. С 1 сентября 2012 г. вступил в силу закон **«О защите детей от информации, причиняющий вред их здоровью и развитию»**. В связи с этим, каждый пользователь должен знать о правилах ответственного и безопасного

поведения в современной информационной среде, способной нанести вред физическому и психическому здоровью человека.

Не многие знают, что более 80% вербовочного процесса детей, подростков и молодых людей проходит через Интернет! Сегодня мы рассмотрим наиболее распространённые виды Интернет-угроз, через которые злоумышленники воздействуют на человека, а так же узнаем о способах защиты от противоправных посягательств в сети Интернет и мобильной сотовой связи. Ведь недаром поговорка гласит: **«Предупреждён – значит вооружён».**

3. Работа по теоретической части занятия.

Интернет – это не только пространство для поиска информации, ведения личной переписки, знакомства с новыми людьми и общения, это еще и источник опасности, которую можно предотвратить.

Для это нужно быть осведомленным о видах угроз, исходящих из Сети. Какие угрозы встречаются наиболее часто? Прежде всего:

- Угроза заражения вредоносным ПО.
- Доступ к нежелательному содержимому. Это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убий- ствам, страницы с националистической или откровенно фашистской идеологией и многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера;
- Контакты с незнакомыми людьми с помощью чатов, электронной почты или социальных сетей. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить молодежь выдать личную информацию. • Неконтролируемые покупки в Интернет-магазинах.

Подростки и молодые люди в возрасте 18-20 лет являются наиболее уязвимой группой и подвергаются наибольшей опасности. Они стремятся исследовать свою сексуальность, уйти из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то, что общение в Интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Наиболее уязвимыми для злоумышленников являются следующие категории молодых людей:

- новички в Интернете, не знакомые с сетевым этикетом;

- недружелюбные пользователи;
- те, кто стремится попробовать все новое, связанное с острыми ощущениями;
- активно ищущие внимания и привязанности;
- бунтари;
- одинокие или брошенные;
- любопытные;
- испытывающие проблемы с сексуальной ориентацией;
- те, кого взрослые могут легко обмануть;
- те, кого привлекает субкультура, выходящая за рамки понимания их родителей. Современный Интернет называют большой душеловкой? Как она работает? Мошенниче- ство в Интернете существует столько же, сколько и сама Всемирная Сеть. На просторах Интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. Из года в год злоумышленники придумывают всё новые и новые уловки, направленные на то, чтобы обмануть своих потенциальных жертв. В отличие от таких интернет-угроз, как вирусы, троянские программы, программы-шпионы, СМС-блокеры, спам и др…, мошенничество примечательно тем, что мишень злумышленника – не компьютер, а человек у которого, как известно, свои слабости (н-р, страх, любопытство, легковерность…). Человек в наше время стал товаром. Рынок живого товара сейчас догоняет обороты наркотиков. Поэтому, только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной.

По статистике, число детей и подростков – пользователей Интернета в России составляет около 14 млн. человек, из которых две трети выходят в Интернет ежедневно. Возраст начала самостоятельной работы в Сети для российских детей сейчас составляет 10 лет. Примерно 30% детей, пользующихся Интернетом, проводят в Сети ежедневно более трех часов в день. Чтобы узнать, какова картина наших пользователей Интернета, проведем анонимное анкетирование. У каждого из вас есть анкета. Заполните ее. (заполняют и сдают). А теперь проанализируйте свои ответы: если вы получили больше ответов «ДА», то вам следует задуматься над тем, что вы подвергаетесь серьезной опасности не только стать жертвой угроз

Интернета, но и иметь серьезную степень Интернет-зависимости.

Как Вы думаете, какие угрозы в сети Интернет существуют для Вас? *(ответы).* ***Верно. Рассмотрим некоторые из них.***

При общении в Сети у каждого обязательно появляются виртуальные знакомые и друзья. Такая форма общения очень часто привлекает

преступников, т.к. различия кибербпреступлений от традиционных реальных преступных посягательств обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время. Так очень легко завладеть вниманием собеседника, применяя приемы психологического воздействия, так называемый кибербуллинг - это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе). (*видеофрагмент «Безопасность в Интернете»*).

Наиболее опасными видами кибербуллинга являются **киберпреследование** - скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д., а также **хеппислепинг** — видеоролики с записями реальных сцен насилия.

Встречается в виртуальной среде и так называемый **буллицид** – доведение человека до самоубийства путем психологического насилия.

Для безопасности несовершеннолетнего особую угрозу представляют личные встречи с виртуальными знакомыми в реальной жизни, о которых никто может ничего не знать.

Опасная для молодежи информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться ***на электронных ресурсах, содержащих материалы экстремистского и террористического характера.*** Не случайно сегодня очень часто возникает вопрос об участии молодых людей славянской, национальности никогда не бывавших в восточных странах, в незаконных террористических организациях и готовящих террористические акции на территории России. Одной из причин такой ситуации – это вовлечение этой части молодежи в незаконные действия путем Интернет-вербовки.

Особую опасность представляют для незрелой психики несовершеннолетних ***электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами.***

Вот один из примеров: Оксана познакомилась в соц сетях с обаятельной девушкой. Разговорились, девушка пригласила Оксану прийти на вечеринку «Истинных сестер»: «У нас так здорово, мы так дружны и очень интересно проводим время». Оксана согласилась и через несколько дней попала в сомнительную компанию, где надо было в обнаженном виде совершать странные обряды. Но члены секты под угрозой смерти запретили Оксане об

этом кому-нибудь рассказывать. Оксана стала замкнутой и задумчивой, перестала хорошо учиться, с родителями почти не разговаривала. Ее постоянно мучил вопрос: как покинуть секту?

Доверчивость и наивность детей нередко используют в своих целях компьютерные ***мошенники, спамеры, фишеры.*** Несовершеннолетнего пользователя взрослые преступники могут с использованием электронных ресурсов втянуть ***в совершение антиобщественных, противоправных, в том числе уголовно-наказуемых деяний.*** Известны случаи вовлечения подростков через Интернет:

- в действия, носящие оскорбительный и клеветнический характер;
- в экстремистскую деятельность;
- в преступную деятельность по изготовлению и сбыту наркотических средств и психотропных веществ и склонению к их потреблению несовершеннолетних, незаконному обороту оружия, взрывных устройств и взрывчатых веществ, сильнодействующих или ядовитых веществ в целях сбыта.

Вам следует знать, что указанные общественно опасные деяния, независимо от того, совершаются ли они с применением традиционных способов и средств или с использованием информационно-телекоммуникационных сетей, уголовно наказуемы, в том числе для подростков, достигших установленного законом возраста уголовной ответственности (16 лет, а за отдельные виды преступлений – с 14 лет). ***1. Пропаганда наркотиков, насилия и жестокости, суицидального поведения, самоповреждений*** может быть весьма опасной для неокрепшей подростковой психики. Согласно Конвенции ООН о правах ребенка такие действия есть не что иное, как ***криминальная, в том числе коммерческая эксплуатация ребенка.***

2. Киберунижение и кибертравля. Они чаще встречаются в социальных сетях, на форумах и в чатах; для кибертравли используются также электронная почта и онлайн-мессенджеры (например, Аська, СМСки). Опасность распространения унижающей человека информации заключается в том, что в отличие от «обычного» унижения, сцены, изображающие сам процесс унижения, распространяются на неограниченный круг лиц. Таким образом, такие видео или фото могут быть доступны будущим друзьям и знакомым даже в случае переезда в другой город. Еще одна опасность заключается в том, что на данный момент удалить все экземпляры унижающих текстов или изображений из Интернета почти невозможно – ничто не мешает кому-то сохранить их на своем компьютере и опубликовать в Сети повторно даже через несколько лет.

Это не полный перечень тех опасностей, которые могут подстерегать вас в Интернете. Самое главное уметь применять элементарные правила безопасности в Интернете. (*видеофрагмент «Развлечения и безопасность в Интернете»*). Чтобы знать, как поступить, предлагаем вам свод правил поведения в Интернете (*памятки для студентов*).

А что делать, если вы уже подверглись угрозе со стороны Интернетмошенников или стали членом Интернет-клубов сомнительного характера, или у вас проявляются признаки Интернет-зависимости? В этом случае есть возможность обратиться в службу «Горячей линии» Центра безопасного Интернета в России. На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия». Горячая линия принимает сообщения по следующим категориям противоправного контента:

- сексуальная эксплуатация несовершеннолетних;
- вовлечение детей в сексуальную деятельность (grooming);
- расизм, национализм, иные формы ксенофобии;
- киберунижение и кибертравля;
- сцены насилия над детьми;
- пропаганда и распространение наркотиков; - пропаганда и публичное оправдание терроризма.

Отправка сообщения на «Горячую линию» производится анонимно и бесплатно. При этом могут быть не только текстовые формы обращения, но и пересылка ссылок на нежелательные ресурсы, которые могут быть оценены специалистами и закрыты.

Еще одним средством помощи детям и их родителям в области Интернет-угроз является линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на «Линию помощи» можно по телефону или через Интернет (все сведения у вас есть в правилах). На «Линии помощи» психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда развития Интернет, прошедшие специальную подготовку по психологическому и информационному консультированию по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

В ряде случаев сотрудники «Линии помощи» перенаправляют поступивший запрос или рекомендует позвонившим самим обратиться в другие организации, с которыми сотрудничает служба «Дети онлайн». К ним относятся: специализированные телефоны доверия, горячие Линии (в

частности, Горячая Линия по приему сообщений о детской порнографии Фонда «Дружественный Рунет»), службы психологической и социальной помощи, органы МВД (в частности, управление «К», которое занимается расследованиями в области кибер- преступности).

В Оренбургской области работают также региональные службы помощи и детские телефоны доверия.

Владение правилами медиабезопасности являются важной составляющей каждого человека, так как вы все в будущем кто-то учитель, а кто-то родитель. На вас будет лежать ответственность за воспитание будущих поколений. Чтобы ваши дети росли в безопасности, научите их самым элементарным правилам пользования сетью, расскажите о возможных угрозах и будьте всегда рядом, если у него возникают какие-то проблемы.
(*видеофрагмент*

«Социальный ролик «Безопасный Интернет – детям!»).

В этом могут помочь специальные программы контентной фильтрации, т.е. программы, фильтрующие сайты и ресурсы Интернета на наличие нежелательной информации и ограничивающие возможность их просмотра. На рынке программных ресурсов на сегодняшний день существует множество программ выполняющих, так называемую функцию Родительского контроля. Наибольшей популярностью пользуются антивирусные программы, содержащие такую функцию. Они удобны тем, что позволяют защитить компьютер не только от вредоносных программ, но и ограничить время пребывания в сети и доступ ребенка к нежелательным сайтам. Это такие продукты как Антивирус Касперского Security или Crystal, Dr Web Security и другие. Есть и программы, созданные специально для ограничения контента.

6. Итог

Современный мир, который вас окружает, сложен и труден. Нужно быть очень умным, осторожным, сообразительным, чтобы жить в нем. Безопасность в этом мире зависит от каждого из нас, прежде всего, от отношения к самому себе.

Природа создала всё для того, чтобы человек был счастлив. Деревья, яркое солнце, чистую воду, плодородную почву. И нас людей – сильных, красивых, здоровых, разумных. Человек рождается для счастья.

5. Рефлексия.

И в заключении я попрошу тех, кому этот урок стал интересным, полезным и кто считает, что Интернет должен стать для нас другом, хором сказать «***Я за безопасный Интернет!***». Всем спасибо.

Приложение 1.

Анкета для учащихся:

№ п/п	Вопрос	Да	Нет
1.	Часто ли вы замечаете, что находитесь в Интернете дольше запланированного времени?		
2.	Часто ли вы откладываете свои домашние дела из-за необходимости находиться в Интернете?		
3.	Используете ли вы смайлики в обычной, не электронной переписке?		
4.	Думаете ли вы, что без Интернета ваша жизнь стала бы скучна и неинтересна?		
5.	Находите ли вы себя усиленно думающим: «Чего бы еще поискать в Сети?»		
6.	Читая книгу, ищите ли вы полосу прокрутки с правой стороны, чтобы прокрутить текст?		
7.	Вы быстрее вспоминаете адрес своей странички в Интернете, чем номер мобильного телефона?		
8.	Часто ли вы говорите себе: «Еще несколько минут и выхожу», находясь в Интернете?		

Приложение 2.

Памятка для Учащихся:

Основные правила безопасности в Интернете

Вы должны это знать:

* При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
* Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
* Если вы получили нежелательное письмо от незнакомых людей, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
* Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
* Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя по отношению к вам неподобающим образом, сообщите об этом.
* Если вас кто-то расстроил или обидел, расскажите родителям. Родители самые близкие люди, они вас выслушают, помогут и защитят.

* Не желательно размещать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
* Не размещайте фото или видеоматериалы, содержащую изображение других лиц, без их согласия. Помните, если вы публикуете фото или видео в Интернете — каждый может посмотреть их.
* Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
* Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
* Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
* Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
* Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Памятка по безопасному поведению в Интернете

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

•По возможности не сообщайте свои личные данные: имя, номер телефона, адрес проживания или учебы, любимые места отдыха или проведения досуга. Помните, что всё, что вы о себе сообщите в социальных сетях, чатах или форумах, может быть доступно, прочтено и использовано любым человеком в мире: Интернет прозрачен и глобален.

•Никогда не сообщайте в открытых источниках конфиденциальные данные: пароли или номера кредитных карт, пин-коды и другую финансовую информацию.

•При регистрации на интернетстраницах используйте нейтральное имя, а если потребуется выбрать пароль, используйте комбинацию из строчных и заглавных букв и цифр, по возможности сложную.

•Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу. И советуйтесь по сложным ситуациям, когда вы сталкиваетесь с чем-то необычным.

•Используйте защитные программы, антивирусы, фильтры электронной почты, программы для блокирования спама и нежелательных сообщений. •Будьте сдержаны и, по возможности, вежливы в интернет-общении. Прекращайте лю бые контакты с теми, кто начинает задавать вам вопросы раздражающие, личного характера или содержащие сексуальные намеки. Обязательно расскажите об этом родителям.

74. КИБЕРУРОК
«Информационная безопасность» (для 11 класса)

Цель: формирование представления об информационной безопасности.

Задачи: обучающие:

- познакомить с понятием информационной безопасности
- рассмотреть различные угрозы информационной безопасности развивающие:
- совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог
- определить план действий для предотвращения угрозы информационной безопасности

воспитывающие:

- воспитывать ответственность за свои действия **План урока:**

1. Организационный момент
2. Подготовка учащихся к усвоению нового материала
3. Теоретическая часть. Изучение нового материала
4. Практическая часть. Первичное закрепление знаний 5. Домашнее задание 6. Итог урока.

Оборудование и методические материалы: Мультимедийный проектор, ПК на РМУ, презентация, набор карточек, памятка для обучающихся.

Ход урока

Организационный момент

Подготовка к усвоению нового материала

Тема урока «Информационная безопасность».

Цель урока: Формирование представления об информационной безопасности.

Теоретическая часть. Изучение нового материала

- Что такое «информационная безопасность»?

Дети высказывают свое мнение, как они понимают этот термин. Обобщая, учитель сообщает определение, которое записывается в тетрадь

Информационная безопасность - это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам.

- Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Дети делают свои предположения и определяются 7 направлений:

1. Кража личных данных, утечка информации
2. Вирусы, черви, трояны
3. Спам
4. Хакеры
5. Авторское право, нелицензионное ПО
6. Мошенничество
7. Дезинформация

Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Давайте разделимся на группы и установим, какие действия нужно предпринять, чтобы обезопасить себя от таких воздействий. *Работа группами по карточкам, обсуждение - 10 минут, затем представители от каждой группы сообщают всем свои методы защиты (принимая или оспаривая), учитель принимает участие в обсуждении - разрабатывается памятка* ***Кража личных данных, утечка информации*** ○ старайтесь не «светить» номер кредитки в Сети;

- совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;
- отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные.

Итог урока

Учитель подводит итог урока, выставляет оценки.

Набор карточек 1

группа Утечка или кража личных данных.

Суть: Ваша персональная информация может оказаться в чужих руках, что грозит печальными последствиями, вплоть до серьезного последствия.

Факты: Если у вас есть кредитная карта и банковский счет, то весьма собланительно выгляди- дит перспектива оплаты услуг Internet-магазинов в режиме on-line. Действительно, это ведь так удобно! Таким образом, в Европе за прошлый год счета «облегчились» на 533 млн $.

Защита:

2 группа Вирусы.

Суть: На ваш компьютер могут напасть вредоносные программы, уничтожающие данные или приводящие к неработоспособности всего компьютера.

Факты: Вирусов стоит бояться и в оффлайновой жизни, но на просторах Internet распространение вирусов может выливаться в настоящие эпидемии. Коварные создатели вредоносных программ используют почтовые сообщения. Приходится быть осторожными с программами, которые вы скачиваете из Internet. Защита:

3 группа Спам.

Суть: Ваш почтовый ящик начинает переполняться несанкционированными рекламными сообщениями, делая практически невозможной нормальную обработку электронной почты. Факты: Ленивые и неудачные торговцы, вместо того, чтобы заняться повышением уровня своих товаров и услуг, стремятся делать бизнес на некачественной рекламе.

Защита:

4 группа Хакеры.

Суть: В ваш компьютер могут проникнуть из Internet с целью кражи личной информации либо для использования вашего компьютера в качестве плацдарма для дальнейших атак.

Факты: Всего лишь пару лет можно было успокоить домашних пользователей, что хакерам нужен доступ только на крупные, мощные машины – теперь времена изменились. Даже информация о подключении к Internet-провайдеру (телефон+логин+пароль) – лакомая добыча для хакера. Защита:

Приложение 1.

Вирусы, черви, трояны

- приобретите хороший антивирусный пакет, установите его в режиме максимальной без- опасности, и своевременно обновляйте; ***Спам***
- не сообщайте посторонним ваш адрес электронной почты, особенно тот, который
- предоставлен провайдером или особенно важен для вас;
- пользуйтесь почтовыми серверами с установленными фильтрами. ***Хакеры***
- никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
- отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
- старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;
- просматривайте чаще системный реестр на предмет подозрительных записей;
- обязательно делайте резервные копии данных на дискеты или CD R/RW; Авторское право, нелицензионное ПО
- укрепление законодательной базы;

• пресекайте попытки воровства вашего творчества;
• используйте только лицензионное ПО. Мошенничество (денежное надувательство).
• просто будьте более скептичными и менее доверчивыми. Дезинформация.
• разумный скептицизм плюс ее проверка в других средствах массовой информации.

- Рассмотрим, как можно защитить информацию из своего файла от посторонних глаз, защитить файл от изменений.

Демонстрируется презентация.

Создание текстового файла, который требует пароль при открытии

1. Необходимо нажать в строке меню Сервис / Параметры
2. Появится окно Параметры, выбрать вкладку Безопасность
3. В поле Пароль для открытия файла ввести пароль, нажать Ок
4. Появится окно о подтверждении 5. Внимание!!! Не забудьте свой пароль!

Создание текстового файла, который не позволяет вносить изменения

1. Необходимо нажать в строке меню Сервис / Защитить документ
2. Появится справой стороны панель Защита документа
3. В поле Ограничение на редактирование поставить галочку и указать вариант только чтение
4. Нажать кнопку да, включить защиту.

IV. Практическая часть. Первичное закрепление знаний

Создайте файлы:

• Работа 1, который требует пароль для открытия
• Работа 2, который не позволяет вносить изменения в файл Обучающиеся создают и сохраняют файлы с необходимым условием **V. Домашнее задание**

- Выучить записи в тетради. Ознакомить друзей с памяткой.

Приложение 2.

Памятка для обучающихся *БУДЬ БДИТЕЛЕН!*

Утечка или кража личных данных.

- *старайтесь не «светить» номер кредитки в Сети;*
- *совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;*
- *отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные* ***Вирусы.***
- *приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;* ***Спам.***

- *не сообщайте посторонним ваш адрес электронной почты, особенно тот, который предоставлен провайдером или особенно важен для вас;*
- *пользуйтесь почтовыми серверами с установленными фильтрами.*

Хакеры.

- *никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;*
- *отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;*
- *старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;*
- *просматривайте чаще системный реестр на предмет подозрительных записей;*
- *обязательно делайте резервные копии данных на дискеты или CD R/RW.*

Нарушение авторского права.

- *укрепление законодательной базы;*
- *пресекайте попытки воровства вашего творчества.*

Вероятность дезинформации.

- *разумный скептицизм плюс ее проверка в других средствах массовой информации.*

Денежное надувательство.

- *просто будьте более скептичными и менее доверчивыми.*

75. КИБЕРУРОК
«Безопасность в сети Интернет» (для 11 класса)

Цель урока: Познакомить с приемами безопасной работы в сети Интернет.
Задачи: Образовательные: Находить нужную информацию в сети Интенет, научить применять полученные знания в проектной деятельности.
Развивающие: Развивать умение анализировать и систематизировать имеющуюся информацию.
Воспитательные: развивать навыки работы в группе, формировать сознательность и внимание к информационно безопасности, прививать навыки безопасного использования сети Интернет.
Оборудование: компьютер с доступом в Интернет, видеопроектор, экран
План урока:

6. Организационный момент
7. Вступление в тему
8. Плюсы и минусы Интернета

9. Советы безопасности
10. Работа в группах
11. Подведение итогов **Ход урока:**

1) Организационный момент.

2) Вступление в тему

Слово учителя: 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 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.

В повседневной жизни каждый из вас сталкивался с Интернетом. А давайте попробуем выяснить, что же такое Интернет? (*ученики дают определение*).

Интернет – всемирная глобальная компьютерная сеть для хранения и передачи информации. Просмотр видеоролика: «Знакомство с Интернетом»: http://www.youtube.com/ watch?v=DOaxn1JB7vE

Что из этого вы уже знали? Что было новым для вас? (*ответы учащихся*) Для чего вы используете Интернет? (*ответы учащихся*) Всегда ли безопасно использовать всемирную сеть? **3) Плюсы и минусы Интернета**

Давайте немного подумаем, сейчас на доске у нас появятся высказывания, вы должны привести аргументы за или против.

Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования.
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 электрон ной почты, номер мобильного телефона). И это хорошо!

Какие опасности подстерегают нас в сети?

(*Интернет-зависимость, вредоносные и нежелательные программы, психологическое воздействие на человека, материалы нежелательного содержания, Интернет-мошенники и др.) Давайте посмотрим, как нам уберечься от этих угроз*).

4) Советы безопасности

Перед тем как приступить к групповой работе (по 2 человека) давайте посмотрим с вами несколько видеороликов про безопасность в сети интернет, они вам помогут в дальнейшем в составлении памятки.

Учащимся предлагается к просмотру 3 видеоролика (по 2 мин.). Во время просмотра ребята должны подумать, какие советы они включили бы в свою памятку по безопасности в Интернете.

Просмотр видеоролика «Развлечения и безопасность в Интернете»: http://www.youtube. com/watch?v=3Ap1rKr0RCE

Просмотр видеоролика: «Остерегайся мошенничества в Интернете»: http://www.youtube. com/watch?v=AMCsvZXCd9w

Просмотр видеоролика «Как обнаружить ложь и остаться правдивым в Интернете»: http://www.youtube.com/watch?v=5YhdS7rrxt8

Какие советы кажутся вам наиболее актуальными? Давайте составим вашу собственную памятку по безопасному общению в Интернете.

Работа в группе. Составление слайда «ПАМЯТКА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ».

5) Подведение итогов

Итогом урока станет памятка по безопасному поведению в сети интернет. В конце урока учащиеся высказывают свои мнения о значении Интернета и вопросов информационной безопасности.

Приложение 1.

ПАМЯТКА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ

1. **Преступление против собственности**
   - Обращайте внимание на стоимость предлагаемой Вам услуги в интернете.
   - Не отправляйте смс сервисам, которые вызывают у вас подозрение. - Помните, бесплатный сыр - только в мышеловке.
2. **Угрозы, направленные на наше эмоциональное и психическое состояние**
   - •Ни под каким предлогом не соглашайтесь на разглашение личных данных: фамилий и имен, возраста, адресов электронной почты, номеров мобильных телефонов.
   - Настороженно относитесь к сообщениям, содержащим призыв о помощи или предложения встречи.
3. **Угрозы, направленные на наше эмоциональное и психическое состояние**
   - При работе с файлами будьте осторожны, убедитесь, что документ предназначался имен но для Вас, проверьте, не является ли данный файл вирусом.

- Пользуйтесь антивирусным программным обеспечением, список рекомендованных про грамм можно найти на сайте «Управление К» и «Лиги безопасного интернета».

76. КИБЕРУРОК
«Безопасность в сети Интернет. Нормы поведения в сети» (для 11 класса)

Цель: обратить внимание учащихся на возможные угрозы в сети Интернет, повысить грамотность учащихся в вопросах безопасности в сети, формировать общепринятые нормы поведения в сети. **Задачи:**

1. Знакомство учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
2. Выработка правила безопасного поведения в сети.
3. Выработка необходимости использования в сети общепринятых нравственных норм поведения.

Оборудование: компьютер, проектор, интерактивная доска, памятка учащимся;

Ожидаемые результаты:

- повышение уровня осведомленности учащихся о проблемах безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.
- формирование культуры ответственного, этичного и безопасного использования Интернета.

План и этапы урока:

1. Введение
2. Объявление темы. Постановка задач
3. Просмотр социального ролика «Безопасный интернет – детям»
4. Сказка о золотых правилах безопасного поведения в Интернет
5. Физкультминутка
6. Рефлексия

Ход урока 1.

Введение.

Создание проблемной ситуации

А сейчас я предлагаю вам отгадать загадки, чтобы понять, о чем пойдет речь на уроке.

Игра «Угадай-ка».

Что за чудо-агрегат Может делать все подряд -
Петь, играть, читать, считать,
Самым лучшим другом стать? (*компьютер.*)

На столе он перед нами, на него направлен взор, подчиняется программе, носит имя... (*монитор*).

Не зверушка, не летаешь, а по коврику скользишь и
курсором управляешь. Ты – компьютерная... (*мышь*).
Нет, она – не пианино, только клавиш в ней – не счесть! Алфавита там картина, знаки, циф- ры тоже есть.
Очень тонкая натура. Имя ей ... (*клавиатура*). Сохраняет все
секреты «ящик» справа, возле ног, и слегка шумит при этом.
Что за «зверь?». (*системный блок*).
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*) **2. Объявление темы.**

Постановка задач.

Как вы думаете, о чём мы сегодня будем говорить?

Правильно, мы с вами поговорим об интернете, точнее о безопасности в интернете. Мы живём в эпоху Интернета, без которого, увы, сейчас трудно справиться. Интернет заменил у нас многое. Это нам облегчило жизнь. Сейчас всего лишь при помощи одного небольшого устройства мы можем обмениваться мгновенными сообщениями, покупать книги или музыку, получать любую необходимую информацию и многое другое. Интернет ворвался в нашу жизнь.

У кого дома есть компьютер? Как вы им пользуетесь?

А у кого дома есть Интернет?

А как вы думаете, какая опасность может подстерегать пользователей интернета? (*ответы детей*).

Мы можем найти в интернете любую информацию, но некоторые сайты могут быть заражены, и наш компьютер может «заболеть».

Поэтому постарайтесь запомнить основные правила безопасного интернета.

3. Просмотр социального ролика «Безопасный интернет – детям»

(Этот ролик создала Студия Mozga.ru, приняла участие в конкурсе «Безопасный интернет - детям!», проведённом Mail.ru.) https://www.youtube.com/watch?v=789j0eDglZQ&feature=youtu.be

4. А сейчас послушайте сказку о золотых правилах безопасного поведения в Интернет СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл-царевичкоролевич, который правил славным городом.

И была у него невеста – прекрасная Смайл-царевна-Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город, заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве.

И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети.

Погоревал – да делать нечего: надо спасать невесту.

Собрал он королевскую – дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайлцаревичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловьяразбойника, товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл- царевну?

Крепко задумался Смайл-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, и остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей, разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. Спрашивай взрослых

Если что-то непонятно, страшно или неприятно,
быстро к взрослым поспеши, Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Установи фильтр

Как и всюду на планете, Есть опасность в интернете. Мы опасность исключаем, Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете. **3. Не открывай файлы** *Не хочу попасть в беду — Антивирус заведу!*
Всем, кто ходит в интернет, Пригодится наш совет.
Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус! **4. Не спеши отправлять SMS** *Иногда тебе в сети, Вдруг встречаются вруны. Ты мошенникам не верь, Информацию проверь!*
Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами *Злые люди в Интернете, Расставляют свои сети. С незнакомыми людьми Ты на встречу не иди!*
Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Будь дружелюбен *С грубиянами в сети, Разговор не заводи. Ну и сам не оплошай – Никого не обижай.*
Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

7. Не рассказывай о себе
Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес,
фото, В интернет не помещай, И другим не сообщай.
Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образования.

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Учитель: Какова мораль этой сказки? А сейчас немного отдохнём и поиграем.

5. Физкультминутка Игра «Вирусы»

Цель игры: Эмоциональная разрядка, снятие напряжения.

Вспомогательные материалы: Листы А4 двух цветов и лента, которой можно будет обозначить линию, разделяющую две команды.

Процедура проведения: Листы А4 нужно скомкать и сделать из них снежки двух разных цветов. Снежки одного цвета обозначают, например, вирусы, спам, зараженные файлы, снежки другого цвета – безопасная информация, безопасные файлы. Участники делятся на две команды так, чтобы расстояние между командами составляло примерно 3 м. В руках каждой команды снежки двух цветов, которые они, по команде ведущего, бросают другой команде. Задача: как можно быстрее закидать противоположную команду снежками, при этом успевая откидывать все «опасные» снежки и сохранять у себя все «безопасные». Ведущий засекает 10 секунд и, услышав команду «Стоп!», участники должны прекратить игру. Выигрывает та команда, на чьей стороне оказалось меньше «опасных» и больше «безопасных» снежков. Перебегать разделительную линию запрещено.

Учитель: Ребята, давайте попробуем почувствовать на себе вирусную атаку и постараться защититься от нее! Правила будут такие. Вам нужно разбиться на 2 команды. Но сначала из листочков бумаги черного и белого цвета сделаем снежки! Каждый должен сделать по 2 снежка белого и черного цвета. Черные снежки – «опасные», а белые – «безопасные». По моей команде начинаем бросать друг в друга снежки! Задача одной команды – как можно быстрее закидать противоположную команду снежками.

Также задача каждой команды – успеть откидывать все черные снежки и сохранять у себя белые.

Сейчас я вручу каждому памятку с правилами. Прочитайте правила и постарайтесь их выполнять (вручение памяток).

6. Рефлексия

Подведём итог нашего урока. Прочитайте предложение и продолжите. Мне было интересно узнать…

Мне понравилось… Меня удивило… Мне захотелось…

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

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

Памятки о правилах безопасного пользования интернетом остаются вам.

Приложение 1.

Памятка по безопасному поведению в Интернете

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.
- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.
- Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

77. КИБЕРУРОК

«Моя безопасность в сети» (для 11 класса)

Цель занятия: формирование культуры безопасного и эффективного использования цифровых ресурсов и устройств, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности.

Структура занятия

Часть 1. Мотивационная (до 5 минут).

Педагог.

Ребята, сегодня наше занятие посвящено кибербезопасности. Жизнь современного человека трудно представить без цифровых сервисов и приложений. Мы используем их для решения самых разных повседневных задач. При этом онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Именно поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Также сфера кибербезопасности активно развивается, поэтому это ещё и перспективное направление для профессионального развития. **Педагог.**

В продолжение занятия предлагаю вам погрузиться в настоящее состязание кибермошенников и специалистов по информационной безопасности. Мы проведем командную игру и научимся противостоять киберугрозам, разберём типичные сценарии атак и узнаем, как пользователи могут себя защищать.

Часть 2. Основная (до 20 минут).

Описание игры «Кибербезопасность».

Класс делится на две команды – «Кибермошенники» и «Специалисты по информационной безопасности» (как вариант, можно предложить разделить класс на несколько команд - специалистов по информационной безопасности; в этом варианте педагог сам озвучивает все карточки с киберугрозами).

Каждая команда получает набор карточек с возможными действиями (*см. дополнительные материалы*). Механика игры:

1.Педагог выбирает одну из карточек угроз (в любой последовательности) и озвучивает её.

2.Задача команды «Кибермошенники» — подобрать из набора карточек с действиями те, что злоумышленники типично используют в такой ситуации.

3.Задача команды «Специалисты по информационной безопасности» – оставить план защиты из своего набора карточек-действий и описать модель поведения пользователя.

На обсуждение отводится 3–5 минут.

4.«Кибермошенники» презентуют свой вариант плана «нападения», а «специалисты по информационной безопасности» – план защиты.

5.Педагог оценивает, отражена ли атака (при необходимости используя ключи к ситуациям, в которых представлены примерные планы атаки и защиты), если да, то присваивает балл команде «специалистов по ИБ».

Возможен вариант выбора команды экспертов из числа детей, которые будут качественно оценивать планы действий команд и при необходимости дополнять их.

Тематики заданий из сферы кибербезопасности, которые встречаются в игре:

- фишинговые ссылки;
- социальная инженерия;
- защита личной информации;
- защита профиля.

Карточки-угрозы, карточки-действия для команды

«Кибермошенники» и «Специалисты по информационной безопасности», ключи к ситуациям *представлены в Приложении к сценарию и дополнительных материалах.*

Пример проведения одного тура игры «Кибербезопасность».

Педагог.

Итак, герой нашей истории молодой ученый Алексей, который давно ведёт свой профиль, у него много подписчиков, интересные и полезные научно-популярные публикации — потерять аккаунт для него будет обидно.

Первая угроза: кибермошенники пытаются совершить кражу профиля Алексея через взлом логина/пароля. **Педагог.**

Команда «Кибермошенников» из своих карточек–действий составляет план атаки. Вам нужно отобрать те действия, которые злоумышленники типично используют в такой ситуации (можете добавить свои варианты действий).

Команда «Специалистов по информационной безопасности» составляет из своих карточек план защиты. Ваша задача – собрать эффективную при такой угрозе модель поведения для пользователя (можете добавить свои варианты действий).

Работа в группе 3–5 минут. **Педагог.**

Время для обсуждения закончилось, давайте дадим слово каждой группе и узнаем, какие планы получились у команд. Слово команде «кибермошенников».

(Ответ представителей команды «кибермошенников».) **Педагог.**

Теперь время ответить на атаку, вторая команда, вам слово.

(Ответ представителей команды «специалистов по информационной безопасности».) **Педагог.**

С учетом планов команд я могу объявить победителей этого тура *(Педагог комментирует ответы команд, при необходимости используя ключ с примерными планами атак и защиты, и называет команду-победителя первого тура.).*

Следующие туры проходят по такой же схеме. Количество туров педагог определяет самостоятельно.

Методический комментарий.

Игра может проходить и в формате, когда все обучающиеся играют роль специалистов по информационной безопасности.

В таком варианте педагог озвучивает угрозу и выводит на экран примерный план атаки кибермошенников (из ключа к ситуациям, представленным в приложении).

Задача – всем вместе найти вариант отражения атаки и обезопасить профиль молодого ученого Алексея. **Педагог.**

Теперь вы знаете чуть больше о том, как действуют мошенники онлайн и как можно предусмотреть риски. Это была отличная тренировка для вас. Предлагаю вам из тех полезных правил для пользователя, что мы сегодня услышали и из тех, что вы можете назвать самостоятельно, составить список – топ-5 полезных привычек кибербезопасности, которые каждый из нас может начать придерживаться с сегодняшнего дня.

Обучающиеся предлагают полезные привычки кибербезопасности, педагог модерирует составление списка. **Педагог.**

Спасибо вам за ваши идеи и комментарии, предлагаю подвести итоги занятия.

Часть 3. Заключение (до 5 минут).

Педагог.

Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK и популярного российского певца Егора Крида. ***Демонстрация видео с Е. Кридом.***

Приложение

Карточки-угрозы
кража профиля пользователя через взлом логина/пароля
манипуляция, чтобы пользователь самостоятельно передал свои данные
получение доступа к сохраненным личным данным/данным банковской карты
продуманное мошенничество на основе доступной информации о человеке
мошенничество через подменные/анонимные профили
мошенничество на основе утечки данных пользователя на сторонних ресурсах

Набор карточек для группы «Специалисты по информационной безопасности»

- Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
- Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
- Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
- Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
- Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
- Не переходите по ссылкам от малознакомых людей.
- Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
- Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.

- Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
- Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
- Не поддавайтесь агрессии и не ведитесь на провокации.
- Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
- Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
- Защищайте всю информацию, даже если думаете, что она не важна.
- Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

Набор карточек для группы «Кибермошенники»

- Проследить за открытой информацией в профиле, изучить подробности жизни человека.
- Спровоцировать на эмоции, вызвать интерес у пользователя, использовать приём ограниченного времени.
- Начать торопить пользователя, чтобы не дать разобраться в происходящем.
- Разослать спам-сообщение друзьям пользователя.
- Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
- Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
- Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.

- Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.
- Представиться сотрудником технической поддержки и выманить конфиденциальные данные или склонить к выполнению сомнительных действий.
- Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
- Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
- Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Ключи к ситуациям угрозы (примерные планы атаки и защиты)

Угроза: кража профиля пользователя через взлом логина/пароля.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Начать торопить пользователя, чтобы не дать разобраться в происходящем.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.
4. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

3. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.

4. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Угроза: манипуляция, чтобы пользователь самостоятельно передал свои данные.

Пример атаки:

1. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
2. Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

1. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
2. Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
3. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Угроза: получение доступа к сохраненным личным данным/данным банковской карты.

Пример атаки:

1. Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
2. Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.

3. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
2. Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
3. Не переходите по ссылкам от малознакомых людей.
4. Защищайте всю информацию, даже если думаете, что она не важна. **Угроза:** продуманное мошенничество на основе доступной информации о человеке.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
3. Разослать спам-сообщение друзьям пользователя. **Пример защиты:**

1. Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
2. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
3. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
4. Не поддавайтесь агрессии и не ведитесь на провокации.

Угроза: мошенничество через подменные/анонимные профили.

Пример атаки:

1. Проследить за открытой информацией в профиле, изучить подробности жизни человека.

2. Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме:
например, сообщить о штрафе или о том, что родственник попал в беду.

3. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.

4. Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.

2. Не поддавайтесь агрессии и не ведитесь на провокации.

3. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

4. Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.

5. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Угроза: мошенничество на основе утечки данных пользователя на сторонних ресурсах.

Пример атаки:

1. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации). 2. Разослать спам-сообщение по друзьям пользователя.

Пример защиты:

1. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

2. Не переходите по ссылкам от малознакомых людей.

3. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.

4. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля. 5. Защищайте всю информацию, даже если думаете, что она не важна.

РАЗРАБОТКИ КИБЕРУРОКОВ ДЛЯ ДЕТЕЙ С ОВЗ

78. КИБЕРУРОК
«Информационная безопасность детей с ОВЗ в сети Интернет"

Цель: Познакомить ребят с понятием информационная безопасность в сети интернет.

Задачи:

- Познакомить с правилами поведения в сети интернет.
- Объяснять детям вред и пользу интернета.
- Воспитывать уважение к собственному здоровью.

Ход урока:

Учитель: Здравствуйте ребята! Тема нашего занятия сегодня – «Информационная безопасность детей в сети Интернет».

Интернет, как и все в жизни, имеет две стороны - черную и белую Давайте попробуем найти плюсы и минусы. На доске собираются плюсы и минусы Беседа:

Учитель: Что же такое информационная безопасность?

Дети дают свои определения.

Учитель: Что же может случиться в реальной жизни через беззаботное виртуальное поведение ребенка?

Дети дают свои определения.

Учитель: Слышали ли вы когда-нибудь о понятии «безопасный интернет»? Ответы детей.

Учитель: Давайте мы все вместе попробуем разработать памятку «Свод правил поведения в сети Интернет». Вам уже известно, что такое памятка?

Полезные памятки, касающиеся, ЗОЖ мы с вами размещаем в книжечке здоровья.

Возможные правила: Зачитывает Учитель.

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, любимые места отдыха или проведения досуга.
2. Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
3. Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
4. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

5. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
6. 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.

Учитель: При использовании интернета есть свои плюсы это:

- Оперативность получения любой информации;
- Общение: Вконтакте, Одноклассники, и другие социальные сервисы и форумы…
- Участие в международных конкурсах, это конкурсы где мы с вами публикуем свои поделки и за что получаем дипломы и свидетельства. Получения дополнительного образования;
- Формирование информационной компетентности, включающей умение работать с информацией. Поясняю каждый пункт.

Так же есть и минусы, это:

- Беспорядочная недостоверная информация.
- Ухудшение здоровья: потеря зрения (компьютерный зрительный синдром),
- гиподинамия; искривление осанки; психические и интеллектуальные нарушения развития.
- Вредная информация (асоциальные сайты): религиозные секты; экстремистские сайты; нецензурная лексика;
- Психологическое давление: маньяки; мошенники; подростковая агрессия. Поясняю каждый пункт.

Рефлексия.

Ученики подводят итог беседы. Каждый ученик заканчивает предложение на выбор:

- Польза интернета, это….
- Вред интернета, это …..

Спасибо за внимание.

В интернете нашла «сказку о золотых правилах безопасности в интернете», можно продолжить разговор на следующем занятии, как закрепление беседы.

Ты должен это знать:

1. Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
3. Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься и номер твоего телефона должны знать только родители и друзья.
4. Никогда не отправляй свои фотографии людям, которых не знаешь лично.
5. 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.
6. Не встречайся с людьми, с которыми познакомился в Интернете, без родителей. Многие люди выдают себя не за тех, кем являются на самом деле.
7. Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов

79. КИБЕРУРОК: «Безопасный Интернет. Путешествие с котом Жориком».

Цели:

1. Обогатить знания детей о работе и функциях служб спасения.
2. Познакомить детей с компьютером, с его составными частями.
3. Обеспечение информационной безопасности воспитанников путем привития им навыков ответственного и безопасного поведения в сети Интернет.
4. Активизировать познавательную деятельность, логическое мышление.

Задачи:

1. Расширять и закреплять знания детей о спецслужбах, номерах телефонов для их вызова.
2. Научить детей пользоваться компьютером.
3. Закрепить правила безопасной работы в Сети Интернет
4. Развивать логическое мышление, внимание, умение прогнозировать свое поведение в сети Интернет;
5. Воспитывать дисциплинированность при работе в сети; умение работать в сотрудничестве с товарищами в ходе занятия.

Ход занятия:

Здравствуйте, ребята! Вы знаете, кто я? Я знаменитый кот Жорик. А знаменит я тем, что я веду борьбу с вредоносными объявлениями в интернете, с разными мошенниками на различных сайтах. Я хочу вас пригласить в интересное путешествие, где вы узнаете правила безопасности в сети интернет.

Наше путешествие я хочу начать с очень доброго стихотворения.

Как можно чаще улыбайся.
И радость всем свою дари. С
улыбкой лёгкой просыпайся,
От счастья в облаках пари.
Жизнь так прекрасна, улыбайся.
И засмеётся мир с тобой.
Как можно чаще улыбайся.
Встречай улыбкой день любой.

Улыбнитесь друг другу, настройтесь на дружную и активную работу. Я желаю вам, чтобы работа принесла вам только положительные эмоции!

Сегодня у нас с вами необычное мероприятие. Игра-квест!

- Кто знает, что такое квест?

- *Это приключенческая игра, в которой вы, главные герои, следуете по маршруту и в процессе игры решаете головоломки и задачи.*

Наше путешествие пройдет по маршруту, которое состоит из 5 станций.

- Надеюсь, что мы все сегодня узнаем, кто из нас по праву могут считаться самыми внимательными, самыми сообразительными, самыми эрудированными, кого из вас мы можем назвать «Знатоками».

А тему квеста вы узнаете, если отгадаете загадку.

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)

Итак, ребята, тема нашего путешествия - квеста «Интернет».

И мы с вами отправляемся в путешествие. вперед на станцию номер 1.

СТАНЦИЯ 1. ТЕЛЕФОНЫ.

Оборудование и оформление: Классный кабинет, стационарный телефон, сотовый телефон, карточки с номерами экстренных служб.

Здравствуйте, ребята. Присаживайтесь.

Посмотрите. Что у меня стоит на столе?

Ответы детей.

(стоит стационарный телефонный аппарат) А
что у меня в руке?

Ответы детей.

(в руке сотовый телефон)

Правильно. И это *(показывает на стационарный телефон*) и это *(показывает на сотовый телефон)* называется телефоном.

Что означает слово ТЕЛЕФОН?

ТЕЛЕ означает ДАЛЕКО, а ФОН означает ЗВУК. Это означает что, с помощью этого аппарата мы можем слышать звук на далеком расстоянии.

Вот этот стационарный телефон, им можно пользоваться только, находясь в помещении, его нельзя взять с собой. И это было очень неудобно. Представьте, вам срочно понадобилось позвонить. Вы находитесь, например, на улице. И приходится бегать искать телефон либо в здании каком – нибудь, либо искать на улице телефон – автомат Это занимало много времени. И тогда ученые придумали новый вид телефона, он называется мобильный. Слово МОБИЛЬНЫЙ означает ПЕРЕНОСНОЙ,

Этот телефон можно носить с собой и общаться, где бы вы не находились.
Ребята, а вы умеете правильно разговаривать по телефону?
Предлагаю вам разыграть сценку «Разговор по телефону»
(Два участника команды должны показать, как разговаривают по телефону два товарища.)
С чего начинается разговор, если звоните вы?
Если звонят вам?
Какие вежливые слова употребляют при общении?
Как правильно завершить разговор?
У каждого телефона есть свой номер, это позволяет позвонить именно тому человеку, с которым вы хотите поговорить.
А что нужно делать, если вы ошиблись номером и позвонили не туда?
А какие номера должен знать каждый в нашей стране?
Ответы детей.
Верно, каждому человеку необходимо знать телефоны экстренных служб.
Какие это службы? *Ответы детей.*
- пожарная охрана
- полиция
- скорая помощь
- аварийная газовая служба - служба спасения.

Эти службы работают круглосуточно, поэтому и днем, и ночью мы можем обратиться к ним за помощью.

Пожарная охрана (Единая спасательная служба МЧС России)

Когда люди неаккуратно обращаются с огнем, возникает пожар - сгорают вещи, квартиры, дома, леса, а главное гибнут люди. На помощь приходит пожарная служба. Пожарные быстро тушат огонь, ведь они специально обучены, и в их машинах есть специальные инструменты для тушения пожара: топор, лопата, шланг, огнетушитель, а главное – вода в большом количестве.

Назовите причины пожара. (игра со спичками, неисправные электроприборы, короткое замыкание, оставленная без присмотра газовая плита, курение)

Что же делать, если в доме начался пожар?

Нужно вызвать пожарную охрану!

По какому номеру мы можем вызвать пожарную охрану?

Телефон пожарной службы «01», а с сотового телефона «101».

Полиция.

Полиция — занимается борьбой с преступностью и правонарушениями, охраной порядка, а также личной безопасностью граждан.

В каких случаях вам может потребоваться помощь полицейских? (если вы стали свидетелем преступления; если вы видите, что кто-то нарушает порядок; если кто-то чужой хочет проникнуть в вашу квартиру; если кто-то предлагает вам конфеты, посмотреть мультфильмы, сниматься в кино или покататься в машине)

Что же нужно делать, чтобы не стать объектом преступления? (всегда закрывать квартиру изнутри, когда вы дом; не ходить поздно вечером без взрослых по улице; не разговаривать с незнакомыми людьми на улице или по телефону, не сообщать ничего о себе или своих близких)

Представьте, вы выходите из лифта и видите, что в соседней квартире взломана и открыта настежь дверь. Куда надо обращаться?

Правильно, в полицию!

Звонить туда нужно по телефону, набрав номер «02» с домашнего телефона или «102» с сотового телефона.

Скорая помощь.

Скорая помощь – это медицинская служба, которая приходит на помощь незамедлительно. Скорая помощь оснащена специальным транспортом, как и все службы спасения.

А в каких случаях мы должны вызвать скорую помощь? (если произошел несчастный случай: травма, отравления; высокая температура, обморок, сильная боль в животе или в груди и др.)

Что же нужно делать, чтобы нам не понадобилась вмешательство скорой помощи? А правильнее сказать, чего делать не надо? (не создавать ситуаций опасных для здоровья: не толкаться, не взбираться на окна, не бегать по мокрому полу, не трогать лекарства и другие вещества, которые могут вызвать отравления, соблюдать элементарные правила гигиены и др.)

Вы можете вспомнить случаи из своей жизни, когда вы сильно заболели? (рассказы детей). А случалось болеть так, что с вашей болезнью не могла справиться мама? Что делать? (вызвать «скорую помощь»). По какому телефону?

Нужно позвонить по номеру «03» с домашнего телефона или «103» с сотового телефона.

Служба газа.

Ежедневно люди используют природный газ в своих бытовых целях. Это тепло батарей, всегда горячая вода в кранах.

Газ — бесцветный, без запаха, легковоспламеняющийся, легче воздуха. От пламени он мгновенно вспыхивает и начинает гореть. Если газ заполнит помещение, то даже от малейшей искорки может произойти сильный взрыв. Поэтому очень опасна его утечка.

Чтобы вовремя почувствовать утечку газа, в него добавляют вещество с резким запахом.

В случае утечки природного газа немедленно необходимо вызывать аварийную газовую службу. Как мы можем узнать, что произошла утечка? (По запаху)

По какому номеру мы можем вызвать газовую службу?

Этот номер 04 с домашнего телефона, 104 с мобильного телефона. Также функционирует короткий единый номер вызова экстренных служб – 112.

Звонящего перенаправят на линию скорой помощи, полиции, аварийной службы, МЧС, службы газа,

Звонить в службу спасения можно с мобильного телефона.

Вызвать экстренных службы можно:

- с городского или мобильного телефона,
- даже если на счету вашего мобильного телефона нет средств,
- если SIM-карта заблокирована,
- если в телефоне вообще нет SIM-карты.

Звонок в экстренные службы является бесплатным.

Ребята, очень часто представителям этих служб приходиться выезжать по «ложным» звонкам. Я думаю, вы уже взрослые и вам не нужно объяснять, что просто так, чтобы побаловаться, по этим номерам звонить нельзя. Ведь это баловство может стоить кому-то жизни.

А теперь мы проверим, как вы запомнили номера экстренных служб.

1. Если вдруг в квартиру ломится чужой,
Говорит плохие, странные слова,
Угрожает и стучится в дверь ногой,
Ты в полицию звони быстрей «102»
2. Разгорается огонь Где-то там вдали,
Доставай-ка телефон
И звони «101»
3. Если вдруг произошла с тобой беда,
Если дома появился сильный дым,
Не теряйся и не бойся никогда –
Набери по телефону «101»
4. Коль сестренке стало плохо

Не теряйся никогда
Ты скорее вызывай
Врача по номеру «103»
5. Если в кухне пахнет газом
Вызывай подмогу сразу
Очень быстро набери
Ты с мобильного «104»
6. Если вдруг ты дома сильно захворал,
Простудился или ногу поломал,
В тот же миг по телефону набери
Этот номер скорой помощи «103»
7. Если ты пришел с прогулки,
Шапку снял и вдруг в квартире
Обнаружил запах газа, Набирай
ты «104».
8. Если в дом стучится вор, Ну а дома ты один,
Набирай скорее номер «102»
Все ребята молодцы. Продолжайте свое путешествие. До свидания.
СТАНЦИЯ 2. КОМПЬЮТЕР.
Оборудование и оформление: компьютерный класс, компьютеры. Добрый день, ребята. Вы пришли на станцию, название которой вы узнаете, если отгадаете загадку. *Презентация «Мой друг – компьютер»* http://900igr.net/prezentacija/informatika/moj-drug-kompjuter-135623/ogljanis-druzhok-vokrug-2.html
Он рисует, он считает,
Проектирует заводы,
Даже в космосе летает, И
дает прогноз погоды.
Миллионы вычислений
Может сделать за минуту.
Догадайся, что за гений?
Ну, конечно же… - компьютер
Ребята, как по-другому модно назвать это устройство? *(Машина для обработки информации)*
Ребята, а для чего нам нужен компьютер?
Ответы детей,
Из чего же состоит компьютер?
1. Посмотрите, перед вами коробка. *(показывает на системный блок)* Что это такое?

Перед вами главный блок:
Там бежит электроток
К самым важным микросхемам.
Этот блок зовут …
(системным)
Ребята, а если вытащить все устройства из системного блока, оставить одну коробку, то как назовем ее? *(Корпус)*
2. А что это за телевизор? *(показывает на монитор)*
Наверху машины всей
Размещается… - (дисплей) Словно
смелый капитан!
А на нем горит … (экран)
(дисплей, экран)
Как по-другому называется дисплей? На что похож его экран *(Монитор, на экран телевизора).* Монитор показывает, что происходит с компьютером.
3. А как называется эта доска с кнопочками перед монитором? *Ответы детей.*
Это вот - … (клавиатура) Вот
где пальцам физкультура И
гимнастика нужны!
Пальцы прыгать там должны!
Что мы вводим с клавиатуры? (Разные символы) Все эти символы видны на мониторе компьютера.
4. А вот это что такое? *(показывает на мышку) Ответы детей.*
В зоопарке есть зайчишка, У
компьютера есть… мышка
Эта мышка… не простая,
Эта… мышка вот какая:
Скромный серый коробок,
Длинный тонкий проводок,
Ну а на коробке – Две
или три кнопки.
Ребята, мышь – это устройство для ввода информации.
5. К компьютеру еще присоединяют печатное устройство. Кто знает, как оно называется? 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)
Вот теперь ребята вы познакомились с устройством компьютера. Кто мне может сказать, что является самым главным из всех этих устройств?
Системный блок. Это мозги компьютера. В нем заложены все программы. Без него компьютер работать не будет.
Все молодцы. Все справились с заданиями. И вас уже ждут на следующей станции. До свидания.
3. СТАНЦИЯ ВИРУСЫ. БЕЗОПАСНОСТЬ.
Оборудование: классный кабинет, ноутбук, интерактивны доска.
Здравствуйте, ребята. Вы знаете, как называется это устройство*?(ноутбук)*
Правильно, это тоже компьютер, только все его части собраны в одном корпусе. Для чего это сделано? Чтобы можно было брать с собой в дорогу или переносить с места на место. Давайте поищем что-нибудь интересное в интернете.
Звучит музыкальный трек «Вирус».
Ой, что это такое? Ребята, вы знаете?.*Ответы детей.*

Оказывается, ребята, не все сайты в интернете безопасны. Есть такие сайты, которые могут заразить ваш компьютер вирусом. Что же такое компьютерный вирус.

Как мы с вами можем заразиться вирусом гриппа или другим вирусом, компьютер тоже может подхватить вирус и заболеть.

Вирус- вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Если компьютер подхватит вирус, он перестанет работать и его тоже нужно будет лечить и придется нести его к компьютерному доктору, это специалисты, их называют программистами. Поэтому, так же, как и человеку, которому делают прививку от различных вирусов, на компьютер надо устанавливать противовирусные программы или как их называют АНТИВИРУС. И тогда ваш компьютер будет работать без поломок.
*Презентация «Безопасный интернет»*https://nsportal.ru/nachalnaya-shkola/vospitatelnaya-rabota/2015/12/05/bezopasnyy-internet *(слайды 1-6)*

Ребята, а вы знаете, какие еще опасности нас могут подстерегать в интернете? *Ответы детей.*

В сети интернет нужно работать очень осторожно. На улице мы часто встречаем хулиганов, которые обижают, обманывают и совершают плохие поступки. Есть такие хулиганы и в интернете. Мы их только не видим .
Иногда тебе в сети.
Могут встретиться вруны.
Обещают всё на свете:
Подарить бесплатно детям
Телефон, щенка, айпод И
поездку на курорт.
Их условия не сложны:
СМС отправить можно
С телефона папы, мамы –
И уже ты на Багамах. Ты
мошенникам не верь,
Информацию проверь!
Самое главное правило пользователя интернета — Будь внимателен и осторожен!
Презентация слайды 7-16
1 правило! Всегда спрашивай родителей о незнакомых вещах в Интернете.
Они расскажут, что безопасно делать, а что нет:
Если что-то непонятно,
страшно или неприятно, Быстро
к взрослым поспеши, Расскажи
и покажи.
2 правило! Установи фильтр.
Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой интернет фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

Как и всюду на планете, Есть
опасность в Интернете. Мы
опасность исключаем,
Если фильтры подключаем.

3 правило! Не открывай файлы.
Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус! Не хочу попасть в

беду — Антивирус заведу! Всем, кто ходит в Интернет, Пригодится наш совет.

4 правило! Не спеши отправлять SMS.
Если хочешь скачать картинку или мелодию, но тебя просят отправить смс — не спеши! Сначала проверь этот номер в интернете — безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.
5 правило! Осторожно с незнакомыми.
Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду. Злые люди в Интернете
Расставляют свои сети. С незнакомыми людьми Ты на встречу не иди!

6 правило! Будь дружелюбен.
Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать:

С грубиянами в Сети
Разговор не заводи. Ну
и сам не оплошай —
Никого не обижай.
7 правило! Не рассказывай о себе.
Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!
Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото
В интернет не помещай И
другим не сообщай.

Помните, что интернет — это полезное и прекрасное средство в помощи обучения, общения или отдыха. Но не стоит забывать о том, что и виртуальный мир несет в себе не только положительное, но и отрицательное.
Учитесь правильно и с пользой пользоваться бесконечными возможностями всемогущим интернетом.

Всем большое спасибо за работу. А теперь вас ждут на следующей станции.

СТАНЦИЯ 4. СПОРТИВНАЯ.

Оборудование: интерактивная доска

Здравствуйте ребята. Вы пришли на станцию музыкально – спортивная.

Вы много уже узнали на других станциях про компьютеры и интенет. В этом классе у нас тоже есть компьютер, который соединен с экраном на стене. Это устройство называется интерактивная доска.

С помощью этого устройства вы сможете смотреть на экране в увеличенном виде, что отображается на нашем ноутбуке. Вот посмотрите, сейчас мы включим видео про компьютер.

Видео Фиксипелки

*Компьютер*https://www.youtube.com/watch?v=PaRrbFwq6LQ

А сейчас мы посмотрим видеоклип про кукутиков и фиксиков и выполним физкультминутку ПОМОГАТОР.

Видео « Кукутики и фиксики.

*Помогатор».*https://www.youtube.com/watch?v=HcpPlAQDtyI

Молодцы, ребята. А теперь отправляйтесь на последнюю станцию.

СТАНЦИЯ 5. ЗАГАДОЧНАЯ *(классный кабинет)* Добрый

день, ребята. Присаживайтесь.

На этой станции мы с вами проверим, что вы сегодня усвоили за время вашего путешествия. Я вам буду загадывать загадки или задавать вопросы, а вы должны отвечать. Только спрашивать буду тех, кто будет правильно сидеть и поднимать руку, а не кричать с места. Будьте внимательны. Сетевая паутина

Оплела весь белый свет.

Не пройти детишкам мимо.

Что же это? (Интернет)

Он мелодию сыграет,

Как будильник прозвонит, На

часок-другой смолкает — И

опять заговорит.

В сумочке лежит всегда,

А молчит лишь иногда. (мобильный телефон)

Он быстрее человека Перемножит

два числа,

В нем сто раз библиотека

Поместиться бы смогла,

Только там открыть возможно Сто

окошек за минуту.

Угадать совсем несложно,
Что загадка про... (компьютер)
По ковру зверек бежит,
То замрет, то закружит,
Коврика не покидает,
Что за зверь, кто угадает? (компьютерная мышь)
На доске по строчечке Разместились кнопочки.
Догадайтесь мальчики, Как здесь тыкать
пальчиком?
(клавиатура)
Он похож на раскладушку, Заменяет
мне подружку.
Не обидит, не обманет,
Вместе с ним весь мир в кармане. Обожает
интернет
Мой технический брюнет.
(ноутбук)
Он маленький и тонкий очень, В
нем как в компьютере экран. Я в
игры разные играю,
Устроившись с ним на диван.
(планшет)
С телевизором два брата,
Но для разных дел, ребята.
Не догадались до сих пор?
К компьютеру подключен...
(Монитор)
Монитор — всего полдела. Чтоб
работа закипела,
Чтобы диски ты смотрел,
Чтоб без связи не сидел,
Чтоб компьютер нам помог,
Должен быть… *(Системный блок.)*
Был он матричным сначала, Но
жизнь на месте не стояла:
Лазерным бесшумным став,
Печатал быстро, не устав.
Чтоб иметь и текст, и фото
Без проблем и без заботы,

Вы к компьютеру купите
Новый, очень нужный…*(Принтер.)*
Какие все ребята молодцы. Справились со всеми загадками.
ПОДВЕДЕНИЕ ИТОГОВ,
Вот и закончилось наше с вами путешествие.
Вам понравилось наше путешествие? *Ответы детей.*
Ребята, что вы полезного узнали сегодня? *Ответы детей.*
Какая из станций для вас была сегодня наиболее интересной? Ответы детей.
А теперь подведем итоги и узнаем, кого мы с вами можем по праву назвать знатоками.
Всем спасибо за работу. Все молодцы.
Используемые источники информации:

1. Ведущий образовательный портал России «Инфоурок»
1.1 https://infourok.ru/vospitatelnoe-zanyatie-sluzhbi-kotorie-vsegda-na-strazhe-3147854.html
1.2 https://infourok.ru/konspekt-klassnogo-chasa-po-teme-bezopasniy-internetv-nachalnoy-shkole-klass-2286288.html
2. Международный образовательный портал «MAAM.RU»
2.1 https://www.maam.ru/detskijsad/konspekt-zanjatija-po-informacionoibezopasnosti-bezopasnyi-internet-starshaja-grupa.html
2.2https://www.maam.ru/detskijsad/konspekt-rechevogo-razvitija-deteidoshkolnogo-vozrasta-posredstvom-organizaci-tvorcheskoi-gostinoi-temakompyuternyi-virus.html
3. Социальная сеть работников образования «nsportal.ru» https://nsportal.ru/npo-spo/informatsionnaya-bezopasnost/library/2016/11/15/urok-bezopasnyy-internet
4. https://riddle.su/pro_internet.html
5. https://riddle.su/zagadki_pro_gadgety.html

Адрес публикации: https://www.prodlenka.org/metodicheskie-razrabotki/397816-korrekcionnovospitatelnoe-zanjatie-dlja-dete

80. КИБЕРУРОК:
«Предупреждение интернет-зависимости» (для 5-9 класса)

Цель:

- расширить представления обучающихся о влиянии компьютера и интернет- зависимости, о здоровом образе жизни.

Задачи:

- ознакомление с представлениями о понятиях «интернет-зависимость»,

«компьютерная зависимость»;

- объяснение причин возникновения зависимости;
- повышение осведомлённости обучающихся о потенциальных рисках при использовании интернета и способов защиты от сетевых угроз.

Оборудование: памятки о правилах безопасности в сети интернет.

Ход урока Ведший:

- Ребята в настоящее время Интернет представляет собой «окно в мир», которое открывает нам много интересного. Мы можем найти любую необходимую информацию, пообщаться с друзьями, поиграть в разнообразные игры, совершить покупки и т. д. Поднимите, пожалуйста, руки у кого дома есть интернет?
- Как часто вы им пользуетесь? Находитесь ли в каких-либо социальных сетях? *(ответы детей)* Ведущий:
- Интернет с каждым днём всё больше развивается, сфера его услуг расширяется и больше привлекается людей, которые уже не могут без него обойтись. Назовите достоинства интернета и компьютера. *(ответы детей)*

Хорошо, но, кроме достоинств интернета, есть и достаточно значительные недостатки. У многих людей возникает интернетзависимость. Особенно этой зависимостью страдают дети и подростки, особенно те, у которых кроме интернета нет никаких увлечений. В России уже многие люди подвержены этой зависимости. Зарубежные учёные утверждают, что каждый пятый пользователь интернета подвержен компьютерной зависимости. Даже появился такой термин - «компьютерный синдром». И опасен он тем, что, люди теряют чувство реальности, уходят в виртуальный мир.

Были случаи, когда детей даже увозила скорая помощь, когда они очень долго сидели за компьютером, не ориентировались во времени и реальности. Им казалось, что они сами герои своих игр и для них нет ничего невозможного. Некоторые подростки пропускали из-за этого школу, не принимали долгое время пищу, они теряли в весе, у них искривлялся позвоночник, портилось зрение и мн. др. Даже отмечены смертельные случаи подростков, просидевших в интернете боле 12 часов.

- Чувствуете ли вы, что вы тоже затянуты в виртуальный мир? А есть у вас друзья, которые жить не могут без компьютера? *(ответы детей)*

Ведуший:

- А знаете ли вы, что, когда вы подключились к интернету, миллионы компьютеров получают доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. Среди пользователей есть мошенники, которые могут воспользоваться вашими данными в своих корыстных целях. И даже безобидная смс-ка может стоить вам огромных денег. У вас на партах лежат памятки, давайте ознакомимся с их содержимым. *(дети читаю по очереди советы и правила безопасности в сети интернет)*

Ведущий

- Ребята, давайте теперь сформулируем недостатки, а точнее, чем опасно частое увлечение интернетом и компьютером. Предлагаю желающим выходить к доске и записывать ваши умозаключения, а я вам помогу. Если очень долго сидеть близко у компьютера и долго смотреть на экран, что может в итоге произойти? А если вы дали кому-то свои персональные данные? *(ведущий разбирает с детьми различные ситуации, и все вместе формулируют выводы)*

- ухудшение зрения;
- нарушение осанки, появление сколиоза;
- возникновение психологических проблем;
- появляется состояние нервозности при желании добиться победы;
- возникает агрессия, в случае неудачи, и пр.;
- не исключена возможность нарваться на мошенников и др.

Ведущий

- Видите какие страшные причины компьютерной зависимости нас могут ожидать. А происходит это тогда, когда человек не может найти себе интересы или друзей по интересам, или слишком замкнут. Обычно такие дети начинают активно искать друзей в интернете. Но, если у вас есть интересы, например, любимое хобби, или вы занимаетесь спортом, у вас не будет столько свободного времени, которое вы уделяете интернету.
- Скажите, чем вы любите заниматься в свободное время, каким видом спорта, есть ли у вас интересы? *(дети вместе с ведущим обсуждают возможные интересы и увлечения)*
- Чем вы предполагаете заниматься в будущем?

Я надеюсь, что вы задумаетесь теперь о том, стоит ли проводить много времени в интернете или за компьютером вообще. И знайте, какими

вырастут ваши дети, зависит только от вас самих! У человека всегда есть выбор и возможность сделать свою жизнь интереснее не только в виртуальной реальности.

Рефлексия.

Учащиеся подводят итоги киберурока, читают на листочках начало предложения и заканчивают предложение на выбор:

- Я сегодня узнал (а)...
- Если у меня попросят в интернете адрес… - В дальнейшем я буду...
- Классный час был мне полезен, потому что..