Министерство спорта и молодежной политики Республики Бурятия
ГАУ ДПО РБ «Бурятский республиканский институт образовательной политики»
Кафедра воспитания, психологии и дополнительного образования

УРОКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ СРЕДНЕЙ ШКОЛЫ РЕСПУБЛИКИ БУРЯТИЯ

(МЕТОДИЧЕСКОЕ ПОСОБИЕ)

Улан-Удэ
2024

УДК 371.4.485
ББК 78.07
У-71

Обсуждено на заседании кафедры воспитания, психологии и дополнительного образования КВПиДО

Одобрено на заседании Научно-методического совета ГАУ ДПО РБ «БРИОП»

Составитель:
Сандабкина Т. Б., к.п.н., доцент, зав. кафедрой воспитания, психологии и дополнительного образования ГАУ ДПО РБ «БРИОП»

Рецензенты:

Буртонова И. Б., к.п.н., доцент Центра непрерывного повышения профессионального мастерства ГАУ ДПО РБ «БРИОП»

Федоров Н.П., зам.директора МАОУ «Гимназия № 14» г. Улан-Удэ

Оглавление

Пояснительная записка ……..4
Учебно-тематическое планирование уроков «Информационная безопасность»……...……5
Методические материалы для уроков «Информационная безопасность»…….…..17
Методические материалы для классного часа «Информационная безопасность»…….....…..165
Приложение "Наглядный материал «Безопасный интернет»……...….172
Приложение "Интернет-зависимость: шкала оценки зависимость от персонального компьютера, Интернета»……..174
Литература……..……178

Пояснительная записка

Настоящие материалы рекомендованы в помощь в практической деятельности для проведения уроков, классных часов по вопросам информационной безопасности обучающихся школ для администрации общеобразовательных учреждений, специалистам, педагогам, классным руководителям. Разработки уроков ориентированы на проведение уроков по информационной безопасности школьников и безопасному поведению в сети Интернет и отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах.

В основе пособия отражены практические рекомендации и разработки уроков ФГБНУ Институт изучения детства, семьи и воспитания РАО, Центр цифровой трансформации образования ГУ ДПО «ИРО Забайкальского края», МБУ «Центр психолого-педагогической, медицинской и социальной помощи» г. Пермь, Лаборатория знаний.

Данный материал для администрации общеобразовательных учреждений, специалистов, педагогов, классных руководителей - качественный инструмент формирования у детей и подростков культуры безопасного поведения в сети, отвечающий современным требованиям, методическим решениям и проверенной экспертами федерального уровня информацией.

УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ УРОКОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (вариант 1)[1]

Учебно-тематическое планирование для 5 класса

№	Название	Количество часов
1	«Опасный и удивительный мир интернета»	2
2	«Мобильное здоровье. Как пользоваться мобильной связью не причиняя вред своему здоровью»	2
3	«Правила безопасного поведения в сети Интернет»	2
4	«Основные виды киберугроз»	2
5	«Безопасный интернет»	2
6	«Безопасность школьников в сети Интернет»	2
7	«Безопасность в сети Интернет»	2
	Итого	14

Учебно-тематическое планирование для 6 класса

№	Название	Количество часов
1	«Опасный и удивительный мир интернета»	2
2	«Мобильное здоровье»	2
3	«Правила безопасного поведения в сети Интернет»	2
4	«Основные виды киберугроз»	2
5	«Игровой сленг»	2
6	«Моя безопасность в Интернете»	2
7	«Безопасный интернет»	2
8	«Безопасность школьников в сети Интернет»	2
	Итого	16

Учебно-тематическое планирование для 7 класса

№	Название	Количество часов
1	«Интернет-сообщества, виртуальные друзья»	2
2	«Компьютерные игры. Основные понятия»	2
3	«Цифровой потребление»	2
4	«Безопасный интернет. Как правильно себя вести в сети»	2
5	«Урок безопасности в сети Интернет»	2
6	«Безопасность учащихся в сети Интернет»	2
7	«Безопасность в сети Интернет»	2
8	«Безопасность в сети Интернет: правила безопасной работы в сети»	2
	Итого	16

Учебно-тематическое планирование для 8 класса

№	Название	Количество часов
1	«Интернет-сообщества, виртуальные друзья»	2
2	«Компьютерная грамотность. Цифровой этикет»	2
3	«Как не попасть в сети интернет-мошенников»	2
4	«Информационная безопасность школьников»	2
5	«Урок безопасности в сети Интернет»	2
6	«Безопасность школьников в сети Интернет»	2
7	«Безопасность в сети Интернет»	2
8	«Безопасность в сети Интернет: опасные угрозы сети Интернет и методы борьбы с ними»	2
9	«Безопасность в сети Интернет: правила безопасной работы в сети Интернет»	2
	Итого	18

Учебно-тематическое планирование для 9 класса

№	Название	Количество часов
1	«Безопасный интернет»	2
2	«Безопасный Интернет. Информационная культура общения»	2
3	«Безопасность в Интернете»	2
4	«Социальные сети: за и против»	2
5	«Урок безопасности в сети Интернет»	2
6	«Безопасность в сети Интернет»	2
7	«Безопасный Интернет»	2
8	«Безопасность в сети Интернет: Интернет угрозы и методы профилактики»	2
9	«Безопасность в сети Интернет: правила безопасного пользования»	2
	Итого	18

УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ УРОКОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (вариант 2) [3]

Курс представлен в учебном пособии «Информационная безопасность. Безопасное поведение в сети Интернет. 5–6 классы». К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые познавательные ресурсы для 5–6 классов **http://lbz.ru/metodist/authors/ib/5-6.php**

Для школьников 5–6 классов курс включает две части и рассчитан на 30 уроков, которые может реализовать учитель информатики и ОБЗР.

Информационная часть урока организована с использованием материала для анализа учебной информации с демонстрацией работы в сети Интернет на примере использования различных устройств доступа к сети. Практическая часть каждого урока предлагается в форме теста, компьютерного задания, и по итогам курса можно выявить наиболее активных учащихся и поощрить их грамотой за курс.

Курс открывается уроком об информационном обществе. Содержание курса включает темы, сформулированные в форме проблем для их решения, что нужно знать о сети Интернет (Часть 1) и как использовать ее ресурсы при самостоятельной работе (Часть 2).

Введение. Что такое информационное общество?

Часть 1. Что нужно знать? Пространство Интернета на планете Земля
1.1. История создания сети Интернет
1.2. Что такое Всемирная паутина?
1.3. Путешествие по сети Интернет: сайты и электронные
сервисы
1.4. Как стать пользователем Интернета?
1.5. Опасности для пользователей Интернета
1.6. Что такое кибератака
1.7. Что такое информационная безопасность
1.8. Законы о защите личных данных в Интернете
1.9. Сетевой этикет
1.10. Коллекции сайтов для детей
1.11. Электронные музеи

Часть 2. Что нужно уметь? Правила для пользователей сети Интернет
2.1. Правила работы с СМС
2.2. Правила работы с электронной почтой
2.3. Правила работы с видеосервисами
2.4. Правила работы в социальных сетях
2.5. Правила защиты от вирусов, спама, рекламы и рассылок
2.6. Правила защиты от негативных сообщений
2.7. Правила общения в социальной сети
2.8. Правила работы с поисковыми системами и анализ информации
2.9. Правила ответственности за распространение ложной и негативной информации
2.10. Правила защиты от нежелательных сообщений и контактов
2.11. Правила вызова экстренной помощи
2.12. Правила защиты устройств от внешнего вторжения
2.13. Правила выбора полезных ресурсов в Интернете
2.14. Средства работы в Интернете для людей с особыми потребностями

Курс в 5–6 классах реализуется в рамках образовательной Программы формирования ИКТ — компетентности обучающихся согласно ФГОС основного общего образования, а также в рамках изучения предмета ОБЖ.

Варианты учебного планирования:

Вариант 1. Курс проводится как одногодичный в 5 или в 6 классе по выбору образовательной организации. Курс рассчитан на 1 урок в неделю. 30 уроков за учебный год.

Вариант 2. Курс проводится по полугодиям в 5 и 6 классах, по 15 уроков в каждом классе.

Курс разработан для учащихся 7–9 классов и предлагается к изучению как курс по выбору образовательной организации в рамках рамках предметов «Информатика» или ОБЗР. Курс рассчитан на 33 часа и может реализоваться по 11 часов в качестве внеурочного модуля в 7, 8 и 9 классах, или как одногодичный курс в 8 или в 9 классах.

К курсу разработано учебное пособие «Кибербезопасность. 7–9 классы».

К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые электронные документы и ресурсы для 7–9 классов **http://lbz.ru/metodist/authors/ib/7-9.php**

Все электронные ресурсы выложены на основе наличия открытого доступа к ним.

К каждому модулю предлагается практическая работа на компьютерах. По итогам изучения модуля учащимся предлагается тест.

К каждому параграфу предусмотрен набор заданий по теме для обсуждения и выполнения на уроке, в том числе с использованием электронного приложения.

Организация учебной деятельности на уроке включает теоретическую, понятийную часть, с использованием видео материалов и документов в электронном приложении, дискуссию по вопросам к параграфу, выполнение практической части в задании к параграфу на компьютере.

В курсе используется ряд новых терминов, которые сформировались недавно. Кибернетика — это «искусство управления». Теперь можно говорить не только о безопасности в интернете, но и о возможности управления информационным пространством в преступных или негативных целях. Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить *киберпространство*. Теперь преступнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния посягающие на общественную безопасность, включаются в **пятую группу** киберпреступлений.

Количество киберпреступлений, совершаемых в мире, неуклонно растет. Меняется и их качественный состав, и раз- мер причиненного ущерба. Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно. Законодательство большинство стран мира предполагает *уголовную ответственность за совершение преступлений данного вида*.

Пособие включает четыре раздела.

Введение.

Раздел 1. Киберпространство. (11 часов)

Киберпространство. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество. Практикум к разделу 1. Практическая работа на основе онлайн курса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайн платежи».

Тест к разделу 1.

Раздел 2. Киберкультура. (11 часов)

Киберкультура. От книги к гипертексту. Киберкнига.

Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии.

Практикум к разделу 2. Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся).

Тест к разделу 2.

Раздел 3. Киберугрозы (11 часов)

Кибервойны. Киберпреступность. Примеры киберпреступлений. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в киберобществе.

Практикум к разделу 3 Практическая работа на основе онлайн курса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам:

- Защита от вредоносных программ.
- Безопасность аккаунтов. Логины и пароли от электронной почты, социальных сетей и других сервисов.

Тест к разделу 3.

Раздел 4. Проверь себя

Содержит тесты к трем тематическим разделам.

№ урока	Тема урока/параграф учебного пособия	Практическая работа к уроку	Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php
1	Введение. Что такое ин формационное общество	Задания В.1–В.2	В.1. Проведите самооценку и выясните для себя, не вредите ли вы своему здоровью. Не забираете ли для информационной работы слишком много времени в ущерб учебе, творчеству, живому общению со сверстниками? Не появилась ли у вас интернет-зависимость? В.2. Ознакомьтесь с видеоматериалами. Обсудите в группе, какую опасность здоровью может нанести неразумное увлечением общением в сети Интернет — лайкомания. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Лайкомания»
2	**Часть 1. Что нужно знать? Пространство Интернета на планете Земля (15 часов)**	Задание 1.1	1.1. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие угрозы таит в себе Интернет. Сайт «Безопасный Интернет для детей»: http://i-deti.org/video/ - Видеоролик «Угрозы Интернета для детей» - Видеоролик «Мировой опыт защиты детей в Интернете»
3	1.1. История создания сети Интернет	Тест 1. Задания 1.2–1.3	1.2. Ознакомьтесь с видеоматериалами. Обсудите их в группе и ответьте на вопрос: где находится Интернет? Сайт телеканала «Карусель»: https://www.karusel-tv.ru/ Видеоролик «Почемучка. Где находится Интернет?». 1.3. Придумайте кроссворд на базе слова «Интернет»

4	1.2. Что такое Всемирная паутина	Задания 1.4–1.5. Тест 2	1.4. На сайте телеканала «Карусель» посмотрите разделы сайта, используя слова-меню. 1.5. Ознакомьтесь с видеоуроком телеканала «Карусель»: : https://www.karusel-tv.ru/ «Почемучка. Что такое веб-браузер»? Ответьте на вопрос: каким веб-браузером вы пользуетесь?
5	1.3. Путешествие по сети Интернет: сайты иэлектронные сервисы	Задания 1.6–1.9. Тест 3	1.6. Выполните поиск сайта телеканала «Карусель» с помощью поисковой системы Яндекс. Выберите нужную ссылку и перейдите на этот сайт. 1.7. Ознакомьтесь с видеоуроком телеканала «Карусель»: «Почемучка. Поисковая система». Ответьте на вопрос: что такое поисковые системы и для чего они предназначены? 1.8. Познакомьтесь с сайтом «Культура.РФ». Обсудите в группе, какие разделы вы находите наи- более интересными для себя, что понравилось больше всего. 1.9. Ознакомьтесь с детской социальной сетью «Лунтик»: www.luntik.ru, представляющей российские и зарубежные мультфильмы для детей
9	1.7. Что такое информационная безопасность	Задание 1.15 Тест 7	1.15. Ознакомьтесь с видеоматериалами. Составьте личную памятку безопасности при работе в Интернете. Сайт телеканала «Карусель»: https://www.karusel-tv.ru/. Видеоурок «Почемучка. Безопасность при работе в Интернете»
10	1.8. Законы о защите личных данных в Интернете	Задания 1.16–1.18 Тест 8	1.16. Портал «Лига безопасного Интернета». Ознакомьтесь с видеоуроком «Защита персональных данных детей». 1.17. Сайт «Персональныеданные.Дети». Пройдите электронный тест «Что ты знаешь о персональных данных». 1.18. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое конфиденциальность и зачем ее соблюдать в Интернете. Какие угрозы подстерегают в сетевых играх? Сайт «Защита детей. Лаборатория Касперского»: • Фиксики: Фикси-советы: Осторожней в Интернете! — Конфиденциальность: https://kids.kaspersky.ru/entertainment/ficksics/fiksi-sovety-ostorozhnej-v-internete-konfidentsialnost/ • Мультфильм «Приключения робота Каспера — Общение в игре»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-privatnost-akkauntov-2/
№ урока	**Тема урока/параграф учебного пособия**	**Практическая работа к уроку**	**Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php**

11	1.9. Сетевой этикет	Задания 1.19–1.20. Тест 9	1.19. Ознакомьтесь с видеоуроком из архива канала Бибигон: «Правила поведения в коллективе/ Сетевой этикет». Ответьте на вопрос: какие правила поведения в коллективе нужно использовать в сообщениях на мобильном телефоне или по электронной почте? 1.20. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие правила нужно соблюдать при общении в Интернете, чтобы не навредить себе. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Овершеринг. Вред репутации»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-overshering-vred-reputatsii/
12	1.10. Коллекции сайтовдля детей	Задания 1.21–1.23	1.21. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое «позитивный контент». Сайт «Безопасный Интернет для детей»: http://i-deti.org/ Знакомимся с Интернетом: http://i-deti.org/video/ 1.22. Ознакомьтесь с разделами интернет-браузера «Гогуль: Играй, Гуляй, Общайся, Учись». 1.23. Проведите путешествие по ресурсам сайта «ВебЛандия». Обсудите в группе, какие из них помогут вам в развитии творчества.
13	1.11. Электронные музеи	Задания 1.24–1.28	1.24. Русский музей в Санкт-Петербурге. Виртуальный филиал: http://www.virtualrm.spb.ru/ru/resources/galleries. Ознакомьтесь с виртуальными экскурсиями. 1.25. Третьяковская галерея в Москве. Электронные коллекции: https://www.tretyakovgallery.ru/collection/ Ознакомьтесь с залами Музея с помощью онлайн-панорамы: https://artsandculture.google.com/partner/the-state-tretyakovgallery 1.26. Музей изобразительных искусств имени А. С. Пушкина в Москве. Электронная коллекция: http://www.artsmuseum.ru/collections/index.php Выберите тематику и посетите электронную экспозицию Музея изобразительных искусств имени А. С. Пушкина. 1.27. Эрмитаж. Виртуальное путешествие: https://www.hermitagemuseum.org/wps/portal/hermitage/panorama?lng=ru Выберите виртуальное путешествие по Эрмитажу. Раздел на сайте «Панорамные туры»: https://polymus.ru/ru/museum/fonds/panoramic/ 1.28. Политехнический музей в Москве. Раздел на сайте «Панорамные туры». Выберите тур на сайте Политехнического музея и ознакомьтесь с его экспозицией на своем компьютере
№ урока	**Тема урока/параграф учебного пособия**	**Практическая работа к уроку**	**Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php**

14–15	Контрольный урок	Контрольное задание к части 1	Скачайте на свой компьютер файл с пособием, представленным «Лабораторией Касперского» в открытом доступе. Распечатайте пособие и выполните в нем задания. Сайт «Лига безопасного Интернета» Практикум «Азбука информационной безопасности» (Лаборатория Касперского): http://ligainternet.ru/upload/docs/docs-for-dowloud/Azbuka_informatsionnoy_bezopasnosti.pdf
	Часть 2. Что нужно уметь? Правила для пользователей сети Интернет (15 часов)		
16	2.1. Правила работы сСМС	Задание 2.1. Тест 10	2.1. Ознакомьтесь с видеоматериалами. Обсудите в группе действия героя, который столкнулся с вымогательством денег через сообщения мнимого друга. Сайт «Защита детей. Лаборатория Касперского»: • Мультфильм «Приключения робота Каспера — Друг Вовка»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-drug-vovka/ • Мультфильм «Приключения робота Каспера — Приватность аккаунтов»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-privatnost-akkauntov/
17	2.2. Правила работы с электронной почтой	Задания 2.2–2.3. Тест 11	2.2. Ознакомьтесь с видеоматериалами. Составьте свою памятку с основными правилами использования электронной почты. Сайт телеканала «Карусель»: https://www.karusel-tv.ru/, видеоурок «Почемучка. Электронная почта». 2.3. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие методы вымогательства денег могут использовать злоумышленники для рассылок на ваш адрес. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Сообщения со взломанных аккаунтов»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-soobshheniya-so-zlomannyh-akkauntov/
18	2.3. Правила работы свидеосервисами	Задания 2.4–2.5. Тест 12	2.4. Ознакомьтесь с системой помощи по работе с видеозаписями в социальной сети ВКонтакте: https://vk.com/support. 2.5. Ознакомьтесь с видеоматериалами. Обсудите в группе, как в компьютерных видеоиграх может быть встроено вымогательство денег. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Покупки в играх»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-pokupki-v-igrah/
№ урока	**Тема урока/параграф учебного пособия**	**Практическая работа к уроку**	**Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php**

19	2.4. Правила работы в социальных сетях	Задания 2.6–2.7. Тест 13	2.6. Ознакомьтесь с кнопкой «Пожаловаться» в социальной сети ВКонтакте. 2.7. Ознакомьтесь с видеоматериалами. Обсудите в группе, кто такие тролли в Интернете и как с ними бороться, как защититься от нежелательных обращений. Сайт «Защита детей. Лаборатория Касперского». Фиксики: Фикси-советы: Осторожней в Интернете! — Тролли: https://kids.kaspersky.ru/entertainment/ficksics/fiksisovetyostorozhnej-v-internete-trolli/
20	2.5. Правила защиты от вирусов, спама, рекламы и рассылок	Задание 2.8. Тест 14	2.8. Ознакомьтесь с видеоматериалами. Обсудите в группе пути распространения вирусов в Интернете и методы борьбы с ними. Сайт «Защита детей. Лаборатория Касперского». Фиксики: Фиксики — Вирус: https://kids.kaspersky.ru/entertainment/ficksics/fiksiki-virus-fixiki/
21	2.6. Правила защиты от негативных сообщений	Задания 2.9–2.10. Тест 15	2.9. Ознакомьтесь с видеоматериалами. Обсудите в группе, какие бывают виды сетевого мошенничества. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Мошенничество в Интернете»: https://kids.kaspersky.ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-moshennichestvo-v-internete/
			2.10. Ознакомьтесь с видеоматериалами. Обсудите в группе, какая опасность может скрываться на сайтах, какие траты денег могут незаметно, но настойчиво предлагаться. Сайт «Защита детей. Лаборатория Касперского»: • Мультфильм «Приключения робота Каспера — Опасности на надежных сайтах»: https://kids.kaspersky.ru/entertainment/opasnosti_na-saitah/ • Фиксики: Фикси-советы: Осторожней в Интернете! — Встроенные покупки: https://kids.kaspersky.ru/entertainment/ficksics/fiksi-sovetyostorozhnej-v-internete-vstroennye-pokupki/
22	2.7. Правила общения в социальной сети	Задания 2.11–2.13. Тест 16	2.11. Ознакомьтесь с видеоматериалами. Обсудите в группе следующие вопросы. Что недопустимо при общении в социальной сети с незнакомцами? Можно ли полностью доверять информации, которую размещают на своих страничках участники социальной сети? Можно ли соглашаться на встречу в реальном мире с незнакомцами из социальной сети? Сайт «Защита детей. Лаборатория Касперского». Фиксики: Фикси-советы: Осторожней в Интернете! — Профили: https://kids.kaspersky.ru/entertainment/ficksics/fiksi-sovetyostorozhnej-v-internete-profili/
№ урока	**Тема урока/параграф учебного пособия**	**Практическая работа к уроку**	**Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php**

			2.12. Вместе с учителем или родителями внимательно прочитайте текст в социальной сети на страницах о системе помощи. • Система помощи в социальной сети ВКонтакте: https://vk.com/support • Система помощи в социальной сети Facebook: https:// www.facebook.com/help/ • Система помощи в социальной сети Одноклассники: https://www.ok.ru/help 2.13. Ознакомьтесь с видеоматериалами. Составьте памятку поведения в социальных сетях на тему информационной безопасности. Сайт телеканала «Карусель»: https://www.karusel- tv.ru/ Видеоурок «Почемучка. Как вести себя в социальных сетях?»
23	2.8. Правила работы с поисковыми система-ми и анализ информа- ции	Задания 2.14–2.15. Тест 17	2.14. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое пиратские сайты и почему они так называются. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Пиратские сайты»: https://kids.kaspersky.ru/ entertainment/multfilmy/priklyucheniya-robota-kaspera-piratskie-sajty/
			2.15. Ознакомьтесь с видеоматериалами. Обсудите в группе, что такое ложная информация и как ее распознать. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Ложная информация»: https://kids.kaspersky.ru/ entertainment/multfilmy/priklyucheniya-robota-kaspera-lozhnaya-informatsiya/
24	2.9. Правила ответ-ственности за распространение ложной и негативной информации	Задания 2.16–2.17	2.16. Ознакомьтесь с законами, представленными на сайте «Безопасный Интернет для детей»: http:// i-deti.org/ в разделе «Законодательство». 2.17. Ознакомьтесь с видеоматериалами. Обсудите в группе, как общество защищает детей в Интернете. Сайт «Безопасный Интернет для детей»: http://i-deti. org/ Как обнаружить ложь и остаться правдивым в Интернете: http://i-deti.org/video/ • Защита персональных данных. Детская безопасность в Интернете: http://i-deti.org/video/
25	2.10. Правила защиты от нежелательных сообщений и контактов	Задание 2.18	**2.18.** Ознакомьтесь с видеоматериалами. Обсудите в группе, какие угрозы подстерегают вас при общении с незнакомцами. Сайт «Защита детей. Лаборатория Касперского»: • Мультфильм «Приключения робота Каспера — Опасность встречи в реале»: https://kids.kaspersky. ru/entertainment/multfilmy/priklyucheniya-robota-kaspera-opasnost-vstrechi-v-reale/
№ урока	**Тема урока/параграф учебного пособия**	**Практи ческая работа к уроку**	**Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php**
			• Мультфильм «Приключения робота Каспера — Никогда не разговаривайте с неизвестными»: https://kids.kaspersky.ru/entertainment/multfilmy/ priklyucheniya-robota-kaspera-nikogda-ne-razgovarivajte-sneizvestnymi/

26	2.11. Правила вызова экстренной помощи	Задание 2.19	2.19. Ознакомьтесь с сайтом «Пространство безопасности. Школа первой помощи». Раздел «Телефоны первой помощи»: http://allsafety.ru/first_aid/telefon.htm Составьте памятку по основным сведениям, которые вы должны сообщить при вызове экстренных служб
	2.12. Правила защиты устройств от внешнего вторжения	Задание 2.20. Тест 18	**2.20.** Ознакомьтесь с видеоматериалами. Обсудите в группе правила подборки паролей. Сайт «Защита детей. Лаборатория Касперского». Мультфильм «Приключения робота Каспера — Пароли»: https://kids.kaspersky.ru/entertainment/priklyucheniya-robota-kaspera-paroli/
27	2.13. Правила выбора полезных ресурсов в Интернете	Задания 2.21–2.23	2.21. Российская государственная детская библиотека: https://rgdb.ru/ Раздел «Национальная электронная детская библиотека»: http://arch.rgdb.ru/xmlui/ Ознакомьтесь с каталогом книг, коллекцией диафильмов, архивом детских журналов.
№ урока	**Тема урока/параграф учебного пособия**	**Практическая работа к уроку**	**Содержание задания/Видеоматериалы http://lbz.ru/metodist/authors/ib/5-6.php**
29–30	Контрольный урок	Контрольное задание к части 2	Выполните задания: • Сайт «Защита детей. Лаборатория Касперского»: https://kids.kaspersky.ru/entertainment/kak-vesti-sebya-v-internete/ Тест-викторина • Сайт «Единый урок безопасности в сети Интернет»: http://xn--d1abkefqip0a2f.xn--d1acj3b/?view=quiz&quiz_id=28 Контрольная работа для младшей группы. • Сайт «Лига безопасного интернета»: http://www.ligainternet.ru/encyclopedia-of-security/parents-andteachers/parents-and-teachers-detail.php?ID=3652 Тест «Безопасный Интернет» • Портал «Персональные данные — дети»: http://xn-80aalcbc2bocdadlpp9nfk.xn--d1acj3b/zadaniya/personalnye_dannye/ Тест «Что ты знаешь о персональных данных?»
			2.22. Аудиохрестоматия: http://audiohrestomatiya.ru/ «Аудиохрестоматия» — это медиапортал, на котором собраны произведения мировой литературы в исполнении известных артистов, а также биографии писателей. Выберите писателя, ознакомьтесь с его биографией. 2.23. Детская электронная библиотека: http://www.deti-book.info/ Прочитайте инструкцию о регистрации в электронной библиотеке. Пройдите регистрацию с помощью учителя или родителей

28	2.14. Средства рабо- ты в Интернете для людей с особыми потребностями	Задания 2.24–2.25	2.24. Ознакомьтесь с сайтом Всероссийского общества слепых. Сайт Всероссийского общества слепых: http://www.vos.org.ru/ 2.25. Для поддержки людей с ограниченными возможностями по зрению специально создан социально-информационный проект Nvda.ru. Бесплатная программа экранного доступа Nvda: https://nvda.ru/ Ознакомьтесь с разделом Web-радио на сайте проекта Nvda.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УРОКОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

РАЗРАБОТКИ УРОКОВ ДЛЯ ОБУЧАЮЩИХСЯ 5-Х КЛАССОВ [1]

УРОК № 1 «Опасный и удивительный мир интернета»

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

Задачи:

a. Уточнение представления детей об Интернет - опасностях.
b. Способствовать осознанию различных Интернет - опасностей и рисков Интернет - зависимости.
c. Оказание помощи в снятии психоэмоционального напряжения.
d. Воспитание умения аргументировать своё мнение.
e. Развитие у детей чувство ответственности за свое здоровье.
f. 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 урока:

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 данныймомент.

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 наошибку;
- 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 толькопользу.
Чёрный угол- выбирают те, кто считает, что Интернет приносит многовреда.
Зелёный угол – больше пользы, чем вреда (обозначить параметры пользыи вреда).
Оранжевый угол – больше вреда, чем пользы (обозначить параметрыпользы 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 проводившаяв 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 котомкуСмайл -царевичу, и отправился он невесту искать.
Вышел на поисковую строку, кликнул по ссылкам поганым, а они туткак тут: сообщества Змея-искусителя-Горыныча, стрелялки - убивалки Соловья - разбойника, товары заморские купцов шаповских, сети знакомствзазывалок русалочьи… Как же найти-отыскать Смайл - царевну?
Крепко задумался Смайл - королевич, надел щит антивирусный, взялв руки меч - кладенец кодовый, сел на коня богатырского и ступил в трясинунепролазную. 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 помогатьбудет 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.

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 обовсем, 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 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://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.moi-universitet.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

УРОК № 2 «Мобильное здоровье. Как пользоваться мобильной связью непричиняя вред своему здоровью»

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 «Вредмобильника».

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 небольшойанкеты.

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 0,7метра 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, можетнагреваться на 1 - 2 градуса. А ведь это изменения в нормальной работоспособности организма (слайд 7)!!!

Информационное выступление учителя.

Теперь давайте рассмотрим, как воздействует на организм человекамобильный 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 сотовыеи 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.

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)

Обсуждение в группах, разработка памятки по безопасномуиспользованию 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 мобильнымтелефоном.

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 научно- технического 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 минутза 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 полноймере 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?

УРОК № 3
«Правила безопасного поведения в сети Интернет»

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) (5-7минут)
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, вашидействия?

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 впечатном 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. УдачиВам!

УРОК № 4
«Основные виды киберугроз»

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). Некоторымвирусам 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 личнойбезопасности. 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 обновленийпросто не существует;
- огромным количеством сторонних маркетплейсов, где можноскачать 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 : учебно- методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.

УРОК № 5 «Безопасный интернет»

Цель:обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития имнавыков ответственного и безопасного поведения в современнойинформационно-телекоммуникационной среде.

Задачи:

изучение информированность пользователей о безопасной работе в сетиинтернет; знакомство с правилами безопасной работы в сети интернет; ориентирование в информационном пространстве; способствовать ответственному использованию online-технологий;

формирование информационной культуры обучающихся, умения самостоятельнонаходить нужную информацию, пользуясь web-ресурсами; воспитание дисциплинированности при работе в сети.

Обучающиеся должны знать:

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

Обучающиеся должны уметь:

Ответственно относиться к использованию on-line-технологий; работать с web-браузером;

пользоваться информационными ресурсами; искать информацию в сети интернет.

Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный, (демонстрация), практический; частично- поисковый, проблемный, метод мотивации интереса; интерактивная формаобучения (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, онивоспользуются этой возможностью. И ни когда-то, а прямо сейчас (просмотр видеоролика «дети и интернет» – 1 мин.(по выбору)

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

2. Изучение нового материала.

Игра «за или против».

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

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

Учитель предлагает ученикам ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». (Целесообразно заранее нескольким обучающимся подготовить короткие сообщения по темам:

- «интернет-зависимость»,
- «вредоносные и нежелательные программы»,
- «психологическое воздействие на человека через интернет»,
- «материалы нежелательного содержания»,
- «интернет-мошенники»).

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 Интернет

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 простыерекомендации, 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 самостоятельнуюиндивидуальную работу можно поставитьоценки.

Информация о домашнем задании, инструкция о его выполнении:

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

Используемая литература:

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.

УРОК № 6 «Безопасность школьников в сети Интернет»

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, делатьвыводы.

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 кликнете на 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 кибер-преступнику, который будет его переполнять горами спама).

Онлайн-угрозы могут также навредить вашей репутации.

- А теперь давайте перейдем к самому опасному виду угроз,который может принести ущерб не только вашему имуществу, но и жизни

– это оффлайн-угроза. Она включает все то, что может случиться в реальнойжизни. 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 письмедля 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 проведемфизкультминутку.

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

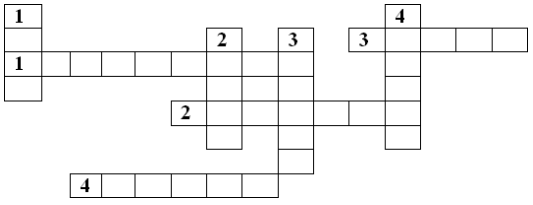
1. Установите комплексную систему защиты.
2. Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.
3. Пользуйтесь браузерами MozillaFirefox, GoogleChrome и AppleSafari.
4. 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.
5. Не отправляйте SMS-сообщения.
6. Очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.
7. 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.
8. Используйте сложные пароли.

9. 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
10. разные значки.
11. Старайтесь не использовать функцию запоминания паролей, которую предлагают многие почтовые ящики и социальные сети.
12. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях .
13. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
14. При регистрации на сайтах, старайтесь не указывать личную информацию
15. Нежелательные письма от незнакомых людей называются
16. «Спам». Если вы получили такое письмо, не отвечайте на него.
17. 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.
18. 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 учетнуюзапись

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.
3.

УРОК № 7 "Безопасность в сети Интернет"

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 приработе 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. Организационныймомент (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 могутоказаться 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 названиеВаших 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 посмотретьвидеоролик «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 УРОКОВ ДЛЯ ОБУЧАЮЩИХСЯ 6-Х КЛАССОВ

УРОК № 1 «Опасный и удивительный мир интернета»

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 урока:

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 данныймомент.

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 наошибку;

- 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 толькопользу.

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

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

Оранжевый угол – больше вреда, чем пользы (обозначить параметрыпользы 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 проводившаяв 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 котомкуСмайл -царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тутка 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, взялв руки меч - кладенец кодовый, сел на коня богатырского и ступил в трясинунепролазную. 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 помогатьбудет 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 обовсем, 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. 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.
2. Солдатова Г.У., Зотова Е.Ю. Зона риска. Российские и европейские школьники: проблемы онлайн-социализации // Дети в информационном обществе. – 2011. – № 7. – С. 46–55.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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://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.moi-universitet.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

УРОК № 2 «Мобильное здоровье»

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 «Вредмобильника».

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 небольшойанкеты.

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;

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 0,7метра 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).

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

Информационное выступление учителя.

Теперь давайте рассмотрим, как воздействует на организм человекамобильный 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.

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)

Обсуждение в группах, разработка памятки по безопасномуиспользованию 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 мобильнымтелефоном.

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 научно- технического 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 полноймере 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 большевсего, вредит, так сказать, по максимуму.
6. И, наконец, избавьтесь от пагубной привычки спать рядом с сотовымтелефоном (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 мобильноготелефона.
3. http://shkolazhizni.ru/archive/0/n-291/ Вредны ли мобильные телефоны. Антон Исаков.
4. http://www.inmoment.ru Сотовые (мобильные) телефоны. ГалинаГатаулина.
5. http://www.ecohome.ru Мобильный телефон не причина вреда если….

12.http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html

Мобильные телефоны вредны?

УРОК № 3 «Правила безопасного поведения в сети Интернет»

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

Задачи:

Обучающие:

1. познакомить с понятием информационной безопасности; рассмотреть различные угрозы информационной безопасности.

Развивающие задачи:

2. совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог; определить план действий для предотвращения угрозы информационной безопасности.

Воспитательные задачи:

3. 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 вреальности): 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, вашидействия?

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 синкейна, 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. УдачиВам!

УРОК № 4 «Виды киберугроз»

Цель: познакомить учеников 6 классов с основными видами киберугроз

Задачи:

- Познакомить и научить различать внешние и внутренние киберугрозы
- Познакомить с основными понятиями и явлениями киберсреды,способными нанести вред не только компьютеру, но и человеку.

- 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). Некоторымвирусам 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 личнойбезопасности. 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 можноскачать 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 : учебно- методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.

УРОК № 5 «Игровой сленг»

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 – разновидностьнелитературной 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 вчераотправил 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 сталнеотъемлемой частью игрового процесса.

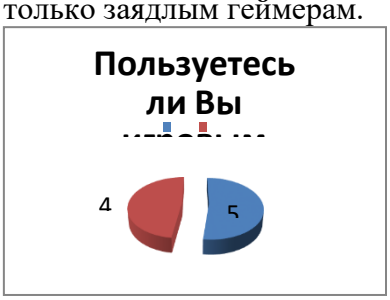
В игровой ситуации игроки вырабатывают стратегию ведения игры, события разворачиваются быстро, и участникам происходящего нужно быстро доносить важную информацию до всех членов группы, и для решения этих задач используется соответствующая форма общения. Как следствие, используемые слова обычно короткие 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?

УРОК № 6 «Моя безопасность в Интернете»

Цель: формирование потребности безопасного использования глобальнойсети.

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 (покол-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 правилбезопасного 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 поведенияв 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 информациюо 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 отнеизвестных 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.
   - A. Попрошу его фото, и потом отправлю своё.
   - B. Посоветуюсь с родителями.
2. В чате тебя обозвали очень грубыми словами.
   - A. Скажу в ответ всё, что я об этом думаю.
   - B. Прекращу разговор с этим человеком.
3. Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.
   - A. Потребую доказательств, что она плохая.
   - B. Сразу откажусь.
4. Пришло сообщение с заголовком «От провайдера». Запрашивают твой логин и пароль для входа в Интернет.
   - A. Вышлю только пароль: они сами должны знать логин.
   - B. 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 личнуюинформацию (адрес, номер телефона, номер школы, любимые места для игри т.д.).

5. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в интернете чем-то, 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.

УРОК № 7 «Безопасный интернет»

Цель:обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития имнавыков ответственного и безопасного поведения в современнойинформационно-телекоммуникационной среде.

Задачи:

изучение информированность пользователей о безопасной работе в сетиинтернет; знакомство с правилами безопасной работы в сети интернет; ориентирование в информационном пространстве; способствовать ответственному использованию online-технологий;

формирование информационной культуры обучающихся, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами; воспитание дисциплинированности при работе в сети.

Обучающиеся должны знать:

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

Обучающиеся должны уметь:

Ответственно относиться к использованию on-line-технологий; работать с web-браузером;

пользоваться информационными ресурсами; искать информацию в сети интернет.

Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный, (демонстрация), практический; частично- поисковый, проблемный, метод мотивации интереса; интерактивная формаобучения (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 иглавного 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 компьютеровполучи 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 нayoutube Http://www.youtube.com/watch?v=3ap1rkr0rce&feature=relmfu
Развлечения и безопасность винтернете Http://www.youtube.com/watch?v=amcsvzxcd9w&feature=bfa&list=pld7
0b 32df5c50a1d7&lf=autoplay остерегайся мошенничества в интернете Http://www.youtube.com/watch?v=xrsnlkvempy&feature=relmfu мир глазами Gmail - защита отспама)

Как не стать жертвой сети интернет? Тема нашего урока «безопасныйИнтернет».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.

5. Интернет имеет неограниченные возможности дистанционногоОбразования. И это хорошо!

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

7. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.

8. Интернет является мощным антидепрессантом.

9. 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 простыерекомендации, 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 поставитьоценки.

УРОК № 8 «Безопасность школьников в сети Интернет»

Цель: познакомить с основными угрозами в сети Интернет иметодах 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 кликнете на 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 кибер- преступнику, который будет его переполнять горами спама).

Онлайн-угрозы могут также навредить вашей репутации.

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

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

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

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

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 письмедля 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

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 дляполной 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 иAppleSafari.

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 Россииз-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как уодного, 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 отправки SMS. При отправке SMS, в лучшем случае, можно лишиться 300-600 рублейна счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

4. Используйте слжные пароли.

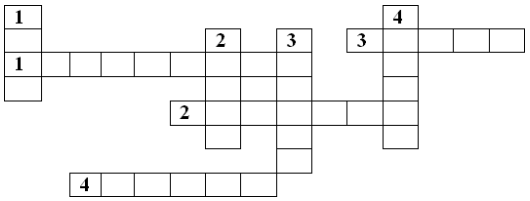
Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти 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 личнуюинформацию
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 сведениябудут 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:

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 учетнуюзапись

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 УРОК №ОВ ДЛЯ ОБУЧАЮЩИХСЯ 7-Х КЛАССОВ

УРОК № 1 «Интернет-сообщества, виртуальные друзья»

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 дляобозначения 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. Правилаформулируются 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:

Психологический настрой. Упражнение «Всемирная паутина» (5минут)

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 иреальных друзей?
3. Обсуждение сходств и различий реальной и виртуальной дружбы.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного. Спасибо всем заработу.

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 ейочень 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». Зайдяна 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 могутвозникнуть? 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 вобщественных 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 прочиталаполученное 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 телефонпришло 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 верныхвариантов 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 онабесплатная.

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 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-по-кибербезопасности- к/
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-kem-obshchayutsya-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

УРОК № 2 «Компьютерные игры. Основные понятия»

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 – разновидностьнелитературной 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-либопредназначение, 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 сталнеотъемлемой 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?

УРОК № 3 «Цифровое потребление»

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.

2. Просмотр видеоролика “Безопасность платежей в интернете”

https://ligainternet.ru/videouroki/

3. **Учитель:** Интернет-пространство расширяется, и с этим связано развитиекибер-

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 какимпричинам?

Да, глазами преступников не увидишь, и понять, что и как они могутсделать, 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 мясорубкив 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 пригодятсяэти навыки.

Мясорубка – мне ещё нужно осознать то, что я узнал на занятиях, обсудитьс 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 уважайтеприватность 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 ибез 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 неуказываться. Помочь человеку или нет – только ваше дело.

Задание 2. Вам приходит письмо с официального сайта благотворительной организации (детдома, приюта) с просьбой о материальной помощи какой- либо 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, получи500).
Или вам приходит сообщение о смерти дальнего родственника, наследником которого являетесь вы, однако нужно переслать налог нанаследство.

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 винтернете.

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 какую-то 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 нателефон 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. N436-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-по- кибербезопасности-к/
3. Копилочка активных методов обучения https://multiurok.ru/files/keis- po-informatike-bezopasnost-v-seti-internet.html
4. Безопасность детей в Интернете https://www.cism-ms.ru/poleznye- materialy/virtualnye-druzya-s-kem-obshchayutsya-deti-v-sotsialnykh- setyakh/
5. Копилочка активных методов обучения http://www.moi-universitet.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

УРОК № 4 «Безопасный интернет. Как правильно себя вести всети»

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития имнавыков ответственного и безопасного поведения в современнойинформационно-телекоммуникационной среде.

Задачи:

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

Обучающиеся должны знать:

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

Обучающиеся должны уметь:

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

Тип урока: урок изучения нового материала.

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

Этапы урока:

Организация начала урока. Постановка цели урока. Просмотр видеоролика 1. 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 миллионахкомпьютерах во всем мире. Но с другой стороны, миллионы компьютеровполучи доступ к вашему компьютеру. И не сомневайтесь, онивоспользуются этой возможностью. И никогда-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 нayoutube Http://www.youtube.com/watch?v=3ap1rkr0rce&feature=relmfu

Развлечения и безопасность винтернете 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 отспама)

Как не стать жертвой сети интернет? Тема нашего урока «безопасныйИнтернет».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.

11. Интернет 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?»

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 простыерекомендации, 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.

12. 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 самостоятельнуюиндивидуальную работу можно поставитьоценки.

Информация о домашнем задании, инструкция о его выполнении:

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

Используемая литература:

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 поБезопасному использованию интернета;

5) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;

6) http://www.rgdb.ru – российская государственная детскаябиблиотека.

УРОК № 5 «Урок по безопасности в сети Интернет

Цель: формирование информационно-коммуникативнойкомпетенции.

Оборудование: мультимедийный проектор, компьютер, карточки с заданиями.

Организационный моментХод 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 карточек- памяток)*

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Постоянно устанавливай цифровые заплатки, которые автоматически устанавливаются с целью доработки программы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый.Лучше уточни у него, отправлял ли он тебе их.

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

Сети Wi-Fi

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

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

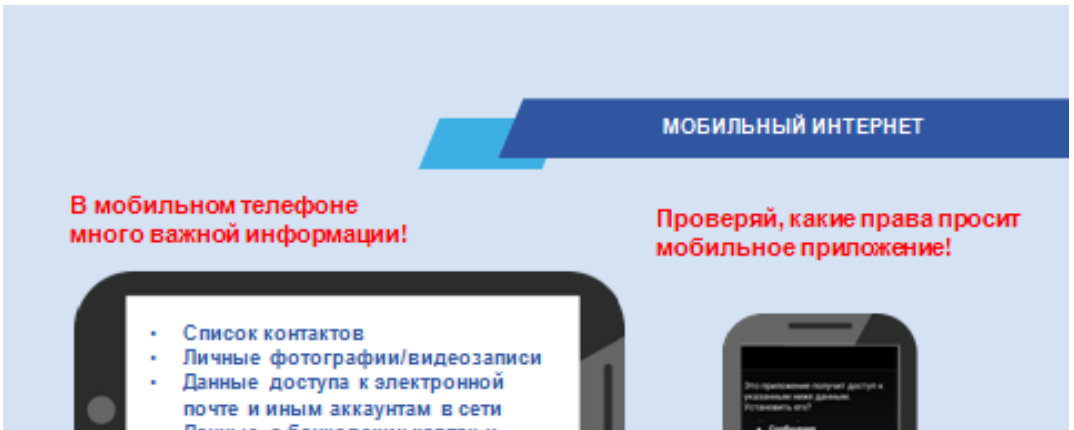
- Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
- Управляй своей киберрепутацией;

- 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 агрессивногоповедения 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 твоегосмартфона;
- Используй антивирусные программы для мобильныхтелефонов;
- Не загружай приложения от неизвестного источника, ведьони 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 услугиактивированы на твоем номере;
- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им непользуешься. Не забывай иногда проверять это.



Online игры

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

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

Цифровая репутация

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

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

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

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

Рефлексия

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

Итог урока

- Сегодня мы попытались разобраться в тех угрозах, которые несёт нам Интернет, а также выявили основные правила безопасности, которые соблюдать в будущем вам будет совсем несложно. Памятки помогут вам в этом. Кроме того, Сетевичок.рф – твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступнымязыком, а при возникновении критической ситуации обратиться за советом.Также вам будет полезен

«Блог школьного Всезнайки» http://www.e-parta.ru - информационно- познавательный портал для подростков. Желаю насыщенной, интересной, а главное, безопасной деятельности в сети Интернет.

Использованные интернет-ресурсы:

1. http://сетевичок.рф/dlya-shkol2. http://www.ligainternet.ru/ 3. http://www.e-parta.ru/

УРОК № 6 «Безопасность учащихся в сети Интернет»

Цель: учащиеся узнают об основных угрозах сети Интернет иметодах 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, делатьвыводы.
- 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 кликнете на 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 кибер-преступнику, который будет его переполнять горами спама). Онлайн-угрозы могут также навредить вашей репутации.

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

Зачастую мошенникам даже не нужно ломать голову над тем, как получить заветную информацию от пользователя – он сам предоставляет ее на тарелочке. Например, при

регистрации в социальной сети и составлении
личного профайла предлагается внести информацию о своем годе рождение, номер телефона, адрес электронной почты, адрес проживания и работы. К сожалению, дети воспринимают такие «требования» как необходимость, и заносят личную информацию во все графы. Это первая и сама главная ошибка! Мы советуем вносить как можно меньше личной информации. Почему? Вот простой пример: ребенок в ожидании долгожданных каникул с родителями и всей семьей в какой- нибудь заморской стране каждый день обновляет свой статус: «Ура, до путешествия осталось три дня!», «Осталось два дня, не могу дождаться!», а на третий-четвертый день, после того, как дни закончились, квартиру обворовывают. Причина в том, что помимо ежедневного обновления статусов ребенок добавил в профиль домашний адрес и фотографии из квартиры, в которой мошенника, а уже и
«домушника», заинтересовал интерьер и домашняя аппаратура.
И, наконец, социальные сети могут быть рассадником людей с более серьезными отклонениями. Создав поддельный профиль ребенка, и втершись в доверие к вам, они могут предложить встретиться, но на встречу уже придет взрослый человек с корыстными или
«больными» планами.

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

1. Алексею на почту пришло сообщение от службы безопасности социальной сети с информацией о том, что аккаунт пытались взломать, и его владельцу необходимо перейти по ссылке в письме для того, чтобы подтвердить персональные данные. Ни на минуту не подумав о подвохе, Алексей переходит по ссылке, затем появляется стартовая страницы соцсети, куда он немедленно вносит пароль и логин. После этого с его профиля начали рассылаться письма довольно странного содержания его друзьям, вместо его фотографий на странице появились непристойные картинки.

2. Однажды в социальной сети девочке пришло сообщение от организаторов конкурса красоты, в котором они предложили ей принять участие. Для участия нужно было отправить несколько фотографий в купальнике, для того чтобы оценить природную красоту будущей конкурсантки. Еще одним условием участия в конкурсе была необходимость перечислить определенную сумму на счет организации в качестве вступительного взноса, после оплаты которого, они свяжутся с девушкой по поводу дополнительной информации о конкурсе, а также времени и месте его проведения.

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

- Сейчас я расскажу вам о том, как обезопасить себя и свой компьютер от сетевых угроз.Но сначала, мы немножко отдохнем и проведем физкультминутку.

Итак, как же бороться с сетевыми угрозами? Приложение 1

А сейчас я предлагаю вам отгадать небольшой кроссворд.
Приложение 2

Итог занятия

- Что нового вы узнали?

Приложение 1

Правила безопасности при использовании социальных сетей

1. Установите комплексную систему защиты.

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-

фильтр и еще пару-тройку модулей дляполной 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 иAppleSafari.

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 Россииз-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как уодного, так и у второго браузера,поэтому лучше ими не пользоваться вовсе.

3. Не отправляйте MS-сообщения.

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 рублейна 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, еголучше не открывать. Подобные письма могут содержать вирусы.
8. При регистрации на сайтах, старайтесь не указывать личную информацию
9. Нежелательные письма от незнакомых людей называются

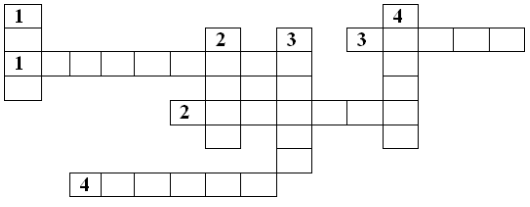
«Спам». Если вы получили такое письмо, не отвечайте на него.

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:

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 учетнуюзапись

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: новаяпрограмма повышения квалификации преподавателей АПКиППРО
//Microsoft в образовании. — [Электронный ресурс]. — Электрон.. 2010 – Режим доступа: http://www.ms-education.ru

УРОК № 7 «Безопасность в сети Интернет»

Цель: расширить представления учащихся о возможностях сетиИнтернет 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 интернет-пользователя».

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

Ход занятия.

1. Экспресс-опрос.

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

Далее в форме беседы выясняем, знают ли ребята, как давно появилсяинтернет 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 онлайн- обучения, расскажем им о том, что в интернете можно не только искать информацию для докладов и презентаций, но и пользоваться всевозможными справочниками, библиотеками, онлайн-тестами и пр. Скорее всего, ребята в качестве недостатка не вспомнят о кибер-преступлениях. Напомним ученикам об этой угрозе и о других опасностях, которые таит в себе всемирная паутина. Предлагаем составить для себя личную «Памятку безопасности интернет-пользователя» и выдаем заранее подготовленную форму.

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 илиадрес 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 трёхвысказываний 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 можетвыглядеть 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».

УРОК № 8 «Безопасность в сети Интернет: правила безопасной работы всети»

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

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

Учащиеся должны знать:

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

Учащиеся должны уметь:

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

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично- поисковый, проблемный, метод мотивации интереса; интерактивная формаобучения (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, онивоспользуются 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 УРОКОВ ДЛЯ ОБУЧАЮЩИХСЯ 8 КЛАССОВ

УРОК № 1 «Интернет-сообщества, виртуальные друзья»

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 дляобозначения 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. Правилаформулируются 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:

Психологический настрой. Упражнение «Всемирная паутина» (5минут)

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 иреальных друзей?
3. Обсуждение сходств и различий реальной и виртуальной дружбы.

Завершение занятия

Учитель: Мы сегодня узнали много нового и интересного. Спасибо всем заработу.

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 ссылкеhttps://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 ейочень 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». Зайдяна 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 могутвозникнуть? Обоснуйте свой ответ.
- Сформулируйте правила, которыми нужно руководствоваться прииспользовании 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 вобщественных 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 прочиталаполученное 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 телефонпришло 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 верныхвариантов 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 онабесплатная.

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 использованияинтернета 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 14.Копилочка активных методов обучения https://sch5nov.schools.by/pages/5-8kludiviti-opasnyj-mir-interneta 9..сборник классных часов безопасность в интернете

http://news.scienceland.ru/2019/04/23/конкурс-задач-по-кибербезопасности- к/
10.Копилочка активных методов обучения
https://multiurok.ru/files/keis-po-informatike-bezopasnost-v-seti-internet.html 17.Безопасность детей в Интернете
12. https://www.cism-ms.ru/poleznye-materialy/virtualnye-druzya-s-kem-obshchayutsya-deti-v-sotsialnykh-setyakh/
13. Копилочка активных методов обучения
14..http://www.moi-universitet.ru/ebooks/kamo/kamo/
15..Материалы сайта «Интернешка» http://interneshka.net/,
16.http://www.oszone.net/6213/
17.Материалы викторины «Безопасность детей в сети интернет
18.http://videouroki.net
19.Копилочка активных методов обучения
20.https://урок.рф/library/klassnij_chas_na_temu_pautina_sotcialnih_setej_181100.html

УРОК № 2 «Компьтерная грамотность. Цифровой этикет»

Цель: повысить компьютерную грамотность взрослого иподрастающего 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 – разновидностьнелитературной 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-либопредназначение, 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 сталнеотъемлемой 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….

12.http://sterlegrad.ru/sovet/13370-mobilnye-telefony-vredny.html Мобильные телефоны вредны?

УРОК № 3 «Как не попасть в сети Интернет-мошенникам»

Цель: 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 ситуациимошенничества.
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 какимпричинам?

Да, глазами преступников не увидишь, и понять, что и как они могутсделать, 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 мясорубкив 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 пригодятсяэти навыки.

Мясорубка – мне ещё нужно осознать то, что я узнал на занятиях, обсудитьс 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 откажитесьот слежки, не отправляйте смс и сообщения на указанные номера и уважайтеприватность 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 ибез 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 неуказываться. Помочь человеку или нет – только ваше дело.

Задание 2. Вам приходит письмо с официального сайта благотворительной организации (детдома, приюта) с просьбой о материальной помощи какой- либо категории людей/человеку в социально опасном/затруднительном положении.

Как поступить. При желании помочь – проверьте адрес сайта (не дублер лиэто), 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, получи500).
Или вам приходит сообщение о смерти дальнего родственника, наследником которого являетесь вы, однако нужно переслать налог нанаследство.

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 винтернете.

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 тольковы 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.

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 проблемыявляются 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 либоприходит смс для ответа, либо вы автоматически подписываетесь на какую-то телефонную услугу и у вас со счета списывается ежедневно пара десятковрублей. 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 нателефон 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 сообщениеприслал 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 можетстать 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, которыедолжны 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-по- кибербезопасности-к/
3. Копилочка активных методов обучения https://multiurok.ru/files/keis- po-informatike-bezopasnost-v-seti-internet.html
4. Безопасность детей в Интернете https://www.cism-ms.ru/poleznye- materialy/virtualnye-druzya-s-kem-obshchayutsya-deti-v-sotsialnykh- setyakh/
5. Копилочка активных методов обучения http://www.moi-universitet.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

УРОК № 4 «Информационная безопасность школьников»

Цель:обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития имнавыков ответственного и безопасного поведения в современнойинформационно-телекоммуникационной среде.

Задачи:

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

Обучающиеся должны знать:

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

Обучающиеся должны уметь:

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

Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный, (демонстрация), практический; частично- поисковый, проблемный, метод мотивации интереса; интерактивная формаобучения (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 миллионахкомпьютерах во всем мире. Но с другой стороны, миллионы компьютеровполучи доступ к вашему компьютеру. И не сомневайтесь, онивоспользуются 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 нayoutube Http://www.youtube.com/watch?v=3ap1rkr0rce&feature=relmfu

Развлечения и безопасность винтернете

Http://www.youtube.com/watch?v=amcsvzxcd9w&feature=bfa&list=pld7
0b 32df5c50a1d7&lf=autoplay остерегайся мошенничества в интернете Http://www.youtube.com/watch?v=xrsnlkvempy&feature=relmfu мир глазами Gmail - защита отспама)
Как не стать жертвой сети интернет? Тема нашего урока «безопасныйИнтернет». 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. Интернет имеет неограниченные возможности дистанционного Образования.И это хорошо!

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»).

9. 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?»

10. 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.

11. 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 простыерекомендации, 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.

12. 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 поставитьоценки.
Информация о домашнем задании, инструкция о его выполнении:

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

Используемая литература:
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 поБезопасному использованию интернета;
5) http://content-filtering.ru – интернет СМИ «ваш личный интернет»;
6) http://www.rgdb.ru – российская государственная детскаябиблиотека.

УРОК № 5 «Урок по безопасности в сети Интернет

Цель:формирование информационно-коммуникативной компетенции.
Оборудование: мультимедийный проектор, компьютер, карточки с заданиями.
Организационный моментХод 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 карточек- памяток)*

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

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

Сети Wi-Fi

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

(*раздача карточек- памяток)*

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- Используй и обновляй антивирусные программы. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использованияв 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 кWi-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 не анонимных 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 агрессивногоповедения 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 твоегосмартфона;
- Используй антивирусные программы для мобильныхтелефонов;
- Не загружай приложения от неизвестного источника, ведьони 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 услугиактивированы на твоем номере;
- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им непользуешься. Не забывай иногда проверять это.

Online игры

Основные советы по безопасности твоего игрового аккаунта: (*раздачакарточек-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 многолет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

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

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

Рефлексия

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

Итог урока

- Сегодня мы попытались разобраться в тех угрозах, которые несёт нам Интернет, а также выявили основные правила безопасности, которые соблюдать в будущем вам будет совсем несложно. Памятки помогут вам в этом. Кроме того, Сетевичок.рф – твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступнымязыком,а при возникновении критической ситуации обратиться за советом.Также вам будет полезен

«Блог школьного Всезнайки» http://www.e-parta.ru - информационно- познавательный портал для подростков. Желаю насыщенной, интересной, а главное, безопасной деятельности в сети Интернет.

Использованные интернет-ресурсы:

1. http://сетевичок.рф/dlya-shkol2. http://www.ligainternet.ru/ 3. http://www.e-

parta.ru/

УРОК № 6 «Безопасность школьников в сети Интернет»

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, делатьвыводы.
- 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 кликнете на 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 кибер-преступнику, который будет его переполнять горами спама).

Онлайн-угрозы могут также навредить вашей репутации.

- А теперь давайте перейдем к самому опасному виду угроз,который может принести ущерб не только вашему имуществу, но и жизни

– это оффлайн-угроза. Она включает все то, что может случиться в реальной жизни. К ней относятся предложения о встрече от неизвестных «друзей», телефонный шантаж, мошенничество, вымогательство и даже ограбление квартиры или кража другого имущества.

Зачастую мошенникам даже не нужно ломать голову над тем, как получить заветную информацию от пользователя – он сам предоставляет ее на тарелочке. Например, при регистрации в социальной сети и составлении личного профайла предлагается внестии нформацию 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 письмедля 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 содержанияего 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 уодного, 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 сообщениена короткий номер для оплаты, в худшем – на компьютере появитсяужасный 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 защитаинформации:
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 повышенияквалификации преподавателей АПКиППРО //Microsoft в образовании. — [Электронный ресурс]. — Электрон.. 2010 – Режимдоступа: http://www.ms-education.ru.

УРОК № 7 «Безопасность в сети Интернет»

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.

<u>План урока:</u>

- 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 – несколькувысказываний. Попробуйте привести аргументы, отражающие противоположнуюточку 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 опасностиподстерегают 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 своихдрузей? (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 жертвойсетевых 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 вредоносныйкод, (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 угрожатьбезопасности компьютера. – Проверять сохраняемые файлы,скачанные вИнтернете – 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 хорошимзнакомым – Использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки и никому их несообщать. – Никогда не отвечать на спам, не переходить по содержащимся в нем ссылкам, не отписываться от спама и тем – более не пересылать его по цепочке. – Установить программу анти-спам – Не передавать учетные данные логины и пароли по незащищенным каналам связи
Фальшивые Интернет - магазины	– Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в Интернете – Не доверять объявлениям о подозрительно дешевых товарах – Старайтесь делать покупки в – известных и проверенных интернет-магазинах.
Бесплатное скачивание файлов с подпиской	– Не указывать свой мобильный номер на незнакомых сайтах. – Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.
Безопасность при оплате картами в сети	– Заведите отдельную карту для покупок в Интернете. – Используйте для покупок в Интернете только личный компьютер. – Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных. – Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах. – Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете поэлектронной 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 васпорадуется.

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.
Не стремитесь утаивать от родителей круг тем, которые вы обсуждаетв 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 обеспечивалинаилучшую 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 сэлектронной 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 восстановлениясистемы
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 энциклопедияhttp://ru.wikipedia.org/wiki/Компьютерный_вирус
4. Социальная сеть работников образования http://nsportal.ru/
5. База образовательных ресурсов http://obrazbase.ru/inform/uroki-i-meropriyatiya
6. Интернет СМИ «ваш личный интернет» http://content-filtering.ru

УРОК № 8 «Безопасность в сети Интернет. Интернет-угрозы»

Цель урока: изучить опасные угрозы сети Интернет и методы борьбыс ними;

Задачи:

- *Образовательная:* познакомиться с понятием «Интернет»,

«Вирус», изучить приемы безопасности при работе в сети Интернет;

- *Развивающая:* развитие интереса к предмету, информационнойкультуры; 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, индивидуальнаяработа.

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), егоцелей 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 загрузкекомпьютера.
Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения внеинфицированные скрипты.
Макровирусы. Это разновидность компьютерных вирусов разработанных намакроязыках, встроенных в такие прикладные пакеты ПО,как Microsoft Office.
Вирусы, поражающие исходный код. Вирусы данного типа поражаютили 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 WindowsUnix
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 программированияскриптовый 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 жертвойсетевых 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 Chromeи Apple Safari. (Слайд 32)

Большинство червей и вредоносных скриптов ориентированы подInternet 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 могутпредотв 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 игнорируетепредупреждение 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 обсуждаетв 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 популярныхсетевых 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 обеспечивалинаилучшую 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, чемостальные:

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 спросьбой 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 восстановлениясистемы

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 найтиправила 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.

УРОК № 9 «Безопасность в сети Интернет: правила безопасной работы всети»

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

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

Учащиеся должны знать:

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

Учащиеся должны уметь:

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

Тип урока: урок изучения нового материала

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

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

Этапы урока:

6. Организация начала урока. Постановка цели урока. Просмотрвидеоролика. Постановка темыи главного вопроса урока.
7. Изучение нового материала. Дискуссия в группе.

Теоретическоеосвещение вопроса(сообщения учащихся).

8. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденномуматериалу.

9. Закрепление изученного материала. Рекомендации по правиламбезопасной работы.

Тестирование.

10. Подведение итогов урока. Оценка работы группы. Просмотрвидеоролика. Информация одомашнем 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, онивоспользуются 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 сетибезопасной?»

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 закладкибраузера 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 УРОК №ОВ ДЛЯ ОБУЧАЮЩИХСЯ 9-Х КЛАССОВ

УРОК № 1 «Безопасный интернет»

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

Обучающиеся должны знать:

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

Обучающиеся должны уметь:

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

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

Этапы урока:

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

Ход урока

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 миллионахкомпьютерах во всем мире. Но с другой стороны, миллионы компьютеровполучи доступ к вашему компьютеру. (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 нayoutube Http://www.youtube.com/watch?v=3ap1rkr0rce&feature=relmfu

Развлечения и безопасность винтернете Http://www.youtube.com/watch?v=amcsvzxcd9w&feature=bfa&list=pld7 0b 32df5c50a1d7&lf=autoplay остерегайся мошенничества в интернете Http://www.youtube.com/watch?v=xrsnlkvempy&feature=relmfu мир глазами Gmail - защита отспама)

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

Изучение нового материала.

Игра «за или против».

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

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

Интернет – это глобальный рекламный ресурс. И это хорошо!

3. Общение в интернете – это плохо, потому что очень часто подменяет Реальное общение виртуальным.

Интернет является мощным антидепрессантом.

4. 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?»

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.

Закрепление изученного материала.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людямс 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.

УРОК № 2 «Безопасный Интернет. Информационная культура общения»

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

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

Учащиеся должны знать:

перечень информационных услуг сети Интернет; опасности глобальной компьютерной сети.

Учащиеся должны уметь:

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

Тип урока: урок изучения нового материала

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

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

Ссылки на web-ресурсы:

1. Интернешка - онлайн-конкурс по полезному и безопасному использованию интернета и мобильной связи http://www.interneshka.net
2. Азбука цифрового мираhttp
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 иглавного вопроса урока.
2. Изучение нового материала (26 мин). Просмотр видеоролика. (16 минут).Физкультминутка. Дискуссия в группе.
3. Практическая работа (7 мин). Создание пароля. Закреплениеизученного материала(7 мин). Тестирование.
4. Подведение итогов урока (2 мин). Оценка работы учащихся.Информация одомашнем 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,онивоспользуются 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 возможностидистанционного образования .И это хорошо!
2. Интернет – это глобальный рекламный ресурс. И этохорошо!
3. Общение в Интернете – это плохо, потому что оченьчасто подменяет реальное общение виртуальному.
4. Интернет магазины – это плохо, потому что этонаиболее 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 вдвух 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 Вамнеобходимо 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 сетибезопасной?»

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

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

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

Практическая работа (7 мин.).

Очень много проблем возникает у людей, при потере пароля отэлектронной 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.

Закрепление изученного материала (7 мин.).

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

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,d3а 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»

Какую персональную информацию не следуетпубликовать 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

Последствиями сетевой атаки для Вашего компьютера могут быть:

- неработоспособность программ

- поломка компьютера
- кража или уничтожение информации
- заражение компьютера вредоносными программами

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

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

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

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 получатьтакие письма

Что такое кибербуллинг?

a) мошенничества, совершаемые в сети Интернет

b) размещение в сети Интернет провокационных сообщений сцелью вызвать конфликты между участниками беседы

c) любые сообщения или публикации в сети, размещаемые сцелью запугать, оскорбить илииначе притеснить другого

Как надо хранить свои пароли (например, от электронной почтыили профиля в социальной сети)?

d) записывать в блокнот

e) сохранятьв скрытом файле накомпьютере

f) использовать менеджер паролей

g) запоминать

h) наклеить цветные стикеры с паролямина монитор

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

i) крекинг

j) серфинг

k) фишинг

l) биллинг

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

a) по электронной почте

b) при скачивании зараженных файлов изинтернет

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 нихнеобходимо 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 илипочтовой 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 незначительноевознаграждение, 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- точку – это в каком-то смысле разговор в полный голос в людном месте.

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

Рекомендации

- Используйте мобильный интернет (EDGE, 3G, LTE).
- Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.
- Старайтесь посещать только сайты с шифрованием данных (HTTPS – он обычно отмечен зелёным замочком в браузерах).
- Используйте специальные средства защиты — браузеры со специальным безопасным режимом просмотра страниц или программы-защитники, которые разрабатывают антивирусные компании.

2. Безопасность платежей в интернете (для старшеклассников)

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

2.1. Распространенные примеры платежного мошенничества

Фиктивные звонки от платежных сервисов

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

Рекомендации

- Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.
- Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.

Выманивание смс-пароля незнакомцем

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

Рекомендации

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

Фальшивые письма от платежных сервисов

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

Рекомендации

- Помните, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.
- Не переходите по ссылкам из таких писем и не вводите свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка,

Яндекс.Денег или другого платежного сервиса.

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

Фальшивые выигрыши в лотерее

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

Признаки фальшивой лотереи

- Пользователь никогда не принимал участие в этой лотерее и вообще ничего о ней не знает.
- Пользователь никогда не оставлял своих личных данных на ресурсе или в организации, от имени которой приходит сообщение.
- Сообщение составлено безграмотно, с орфографическими ошибками.
- Почтовый адрес отправителя — общедоступный почтовый сервис. Например, gmail.com,mail.ru, yandex.ru.

Бесплатное скачивание файлов

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

Рекомендации

- Не указывайте свой мобильный номер на незнакомых сайтах.
- Если подписка уже оформлена, позвоните в службу поддержки оператора мобильной связи и попросите отключить её.

2.2. Платежные данные, которые нельзя раскрывать Что делать, если

…вы потеряли карту.

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

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

…вы забыли пароль от электронного кошелька.

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

2.3. Безопасность при оплате картами

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

- Не сообщайте номер карты другим людям.
- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.

•Заведите отдельную карту для покупок в интернете.

•Используйте для покупок в интернете только личный компьютер.

•Регулярно обновляйте антивирусную защиту компьютера.

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

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

•Подключите в банке услугу смс-уведомлений, чтобы получать сведения овсех 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.)

УРОК № 3 «Безопасность в Интернете»

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 информационномпространстве;
- заложить основы правовых знаний работы в Интернете.

развивающие:

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

воспитательные:

- воспитывать ответственность и дисциплинированность

учащихсяпри работе в сети.

Оборудование: компьютерный класс, ПК, мультимедийныйпроектор.

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, путираспространения, деструктивные действия)
2. Антивирусные программы (назначение, возможности, советыпо 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 Интернет
е» 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 поведенияв сети Интернет
2. Придумать сказку для учащихся младших классов обосторожности в Интернете

Рефлексия

УРОК № 4 "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; бейджикис указанием имен участников; аудитория, оформленная по типу ТВ-студии.

Предварительная анкета:

1 Как вы относитесь к социальным сетям?2 В каких социальных сетяхвы 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 засоциальные сети?

Три однозначных плюса социальных сетей. Три однозначных минусасоциальных 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 средствкоммуникации

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 часовв 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, узнатьу 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 виртуальнос 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, япостоянно 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 противоречиямимежду потребностью в признании их взрослыми со стороны окружающих исобственной 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,чато
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 удочкуИнтернет-дружбы.

Ведущий: Мы получили достаточное количество положительных ответов, но и не меньше отрицательных. Чем больше будет развиваться цивилизация, тем способы общения между

людьми тоже будут усовершенствоваться. Человечество всегда находится в поиске новых формобщения….
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

УРОК № 5 «Урок по безопасности в сети Интернет»

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 карточек- памяток)*

- Используй современные операционные системы, имеющиесерьёзный 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, ане 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 использованияв работе или учебе;
- Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- Используй 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, тозлоумышленники 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 не анонимных 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 знаки 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. Тыточно знаешь, где они будут в конечном итоге?
- Необходимо обновлять операционную систему твоегосмартфона;
- Используй антивирусные программы для мобильныхтелефонов;
- Не загружай приложения от неизвестного источника, ведьони 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 многолет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

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

- Подумай, прежде чем что-то публиковать и передавать усебя 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 можеткого-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 делатьвообще?
- Как вы себя теперь будете вести в социальных сетях?
- Стоит ли вступать в бой-противостояние с кибер-хулиганами?

Итог урока

- Сегодня мы попытались разобраться в тех угрозах, которые несёт нам Интернет, а также выявили основные правила безопасности, которые соблюдать в будущем вам будет совсем несложно. Памятки помогут вам в этом. Кроме того, Сетевичок.рф – твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком,а при возникновении критической ситуации обратиться за советом. Также вам будет полезен

«Блог школьного Всезнайки» http://www.e-parta.ru - информационно-познавательный портал для подростков. Желаю насыщенной, интересной, аглавное, безопасной деятельности в сети Интернет.

Использованные интернет-ресурсы:

1. http://сетевичок.рф/dlya-shkol2. http://www.ligainternet.ru/ 3. http://www.e-parta.ru/

УРОК №6 «Безопасность в сети Интернет»

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 – несколькувысказываний. Попробуйте привести аргументы, отражающие противоположнуюточку зрения.

1. Интернет имеет неограниченные возможности дистанционногообразования. 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 своихдрузей? (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 жертвойсетевых 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 (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 – серфингпо 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 вИнтернете – 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 толькохорошим знакомым – Использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки и никому их не сообщать. – Никогда не отвечать на спам, не переходить посодержащимся внем ссылкам, не отписываться от спама и тем более не пересылать его по цепочке. – Установить программу анти-спам Не передавать учетные данные логины и пароли по незащищенным каналам связи
Фальшивые Интернет магазины	– Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в Интернете – Не доверять объявлениям о подозрительно дешевых товарах – Старайтесь делать покупки в известных и проверенных интернет- магазинах.
Бесплатное скачивание файлов с подпиской	– Не указывать свой мобильный номер на незнакомых сайтах. – Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить – отключить её.

Безопасность при оплате картами в сети	– Заведите отдельную карту для покупок вИнтернете. – Используйте для покупок в Интернете только личный компьютер. – Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протоколобеспечивает безопасную передачуданных. – 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 просматривайтев интернет-банке историювыполненных 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. Витоге, 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.), чтобызлоумышленники 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 завас 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 обсуждаетв 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 томчисле вирусов) преследуется в России согласно…

- Административному кодексу
- Трудовому кодексу
- Уголовному кодексу
- Гражданскому кодексу

Какой из приведенных паролей является более надежным

- о. 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 электроннойпочтой?

- 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 длядальнейшей 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 восстановлениясистемы
- 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-i-meropriyatiya
11. Интернет СМИ «ваш личный интернет» http://content-filtering.ru

УРОК № 7 "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

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, электроннойпочте и мобильной связи.
Здесь же можно задать свой вопрос, если ответ на страницах сайта не найден. Для этого существует форма обратной связи, и все операторынаходятся 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 аккаунтумобильный номер, а несекретный 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 своегокошелька или банковской карты.
- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.

- Заведите отдельную карту для покупок в интернете.
- Используйте для покупок в интернете только личный компьютер.
- Регулярно обновляйте антивирусную защиту компьютера.
- Старайтесь делать покупки в известных и проверенных интернет-магазинах.
- Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.
- Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет

Пользователи должны научиться грамотно пользоваться Интернетом и электронными устройствами

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- критически относиться к информационной продукции;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

УРОК № 8 «Безопасность в сети Интернет. Интернет-угрозы. Методыпрофилактики»

Цель урока: изучить опасные угрозы сети Интернет и методыборьбы с ними;

Задачи:

- *Образовательная:* познакомиться с понятием «Интернет»,

«Вирус», изучить приемы безопасности при работе в сети Интернет;

- *Развивающая:* развитие интереса к предмету, информационнойкультуры; 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, индивидуальнаяработа.

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), егоцелей 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. Рейтингсамых 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 внеинфицированные скрипты.

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

Вирусы, поражающие исходный код. Вирусы данного типа поражаютили 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 WindowsUnix

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 программированияскриптовый 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 жертвойсетевых угроз.

7. 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 Chromeи Apple Safari. (Слайд 32)

Большинство червей и вредоносных скриптов ориентированы подInternet 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 второгобраузера,поэтому лучше ими не пользоваться вовсе.

4. Обновляйте операционную систему Windows. (Слайд 33)

Постоянно обновляйте операционную систему Windows. Корпорация Microsoftпериодически 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 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, вхудшем – 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 игнорируетепредупреждение 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 обсуждаетв 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 популярныхсетевых 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 обеспечивалинаилучшую 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, чемостальные:

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 спросьбой 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 восстановлениясистемы

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 найтиправила 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.

УРОК № 9 «Безопасность в сети Интернет. Правила безопасногопользования»

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

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

Учащиеся должны знать:

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

Учащиеся должны уметь:

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

Тип урока: урок изучения нового материала

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

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

Этапы урока:

11. Организация начала урока. Постановка цели урока. Просмотрвидеоролика. Постановка темыи главного вопроса урока.
12. Изучение нового материала. Дискуссия в группе. Теоретическоеосвещение вопроса(сообщения учащихся).
13. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденномуматериалу.
14. Закрепление изученного материала. Рекомендации по правиламбезопасной работы.

Тестирование.

15. Подведение итогов урока. Оценка работы группы. Просмотрвидеоролика. Информация одомашнем 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, онивоспользуются 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 сетибезопасной?»

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 закладкибраузера 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.).

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КЛАССНОГО ЧАСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» [1]

Цель: создание условий для повышения уровня грамотности учащихся в вопросах информационной безопасности, расширение знаний учащихся о кибербезопасности и киберугрозах, формирование навыков их распознавания и оценки рисков, их минимизация

Задачи:

- ознакомить учащихся с нормативно-правовой базой;
- ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия;
- выявить и обсудить основные правила обеспечения информационной безопасности в сети Интернет, научиться выявлять риски и минимизировать их;
- закрепить полученные знания путем выполнения творческого задания.

Ожидаемые результаты: повышение уровня осведомленности учащихся о проблемах информационной безопасности при использовании сети Интернет, умение оценивать потенциальные риски и минимизировать их.

В ходе урока «Информационная безопасность» в среднем звене целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

- Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.);
- №252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребѐнке порочные наклонности, сформировать у ребѐнка искаженную картину мира и неправильные жизненные установки.)

Важно ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (https://politech47.mskobr.ru/files/informaciya_o_liniyah_pomowi_v_slu chae_internet-ugroz.pdf).

Линия помощи в случаях Интернет-угроз «Горячая линия». На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия».

Линия помощи «Дети онлайн». 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 8 800 250 00 15 (с 9 до 18 по рабочим дням, время московское)
- по электронной почте helpline@detionline.com •
- на сайте www.detionline.com

Возможны следующие формы проведения урока: урок - пресс-

конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами и т.д.

В качестве примера для учащихся 5-7 классов предлагается урок - беседа «10 правил безопасности в Интернете».

Каждый современный человек, ежедневно проводит время в интернете. Но интернет - это не только источник информации и возможность общаться на расстояние, но и угроза информационной безопасности. Вы можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломать злоумышленники.

Правила безопасности в интернете.

1) Используйте надежный пароль. Перво и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль. Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль.

Генератор паролей создается, чтобы помочь вам с придумыванием устойчивых к взлому и легко запоминающихся паролей.

Часто бывает: вы зарегистрировались где-нибудь,а там просят: «введите пароль». В спешке приходится вводить что-нибудь типа qwerty или 12345. Последствия могут быть фатальными для вашего аккаунта: при попытке взлома такие пароли проверяются в первую очередь. Чтобы этого не происходило, надо создавать сложный пароль, желательно состоящий из букв разного регистра и содержащий цифры и другие символы. Для создания таких паролей существуют специальные программы. Но, на наш взгляд, гораздо легче набрать наш адрес и просто выбрать понравившийся пароль.

Советы:

Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания. Не используйте пароль, связанный с теми данными, которые могут быть о вас известны, например, ваше имя или дату рождения. Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими.

Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне.

Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надежности. 2) Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.

6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем - получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.

7) Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.

8) Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.

10) Периодически меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля. Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте.

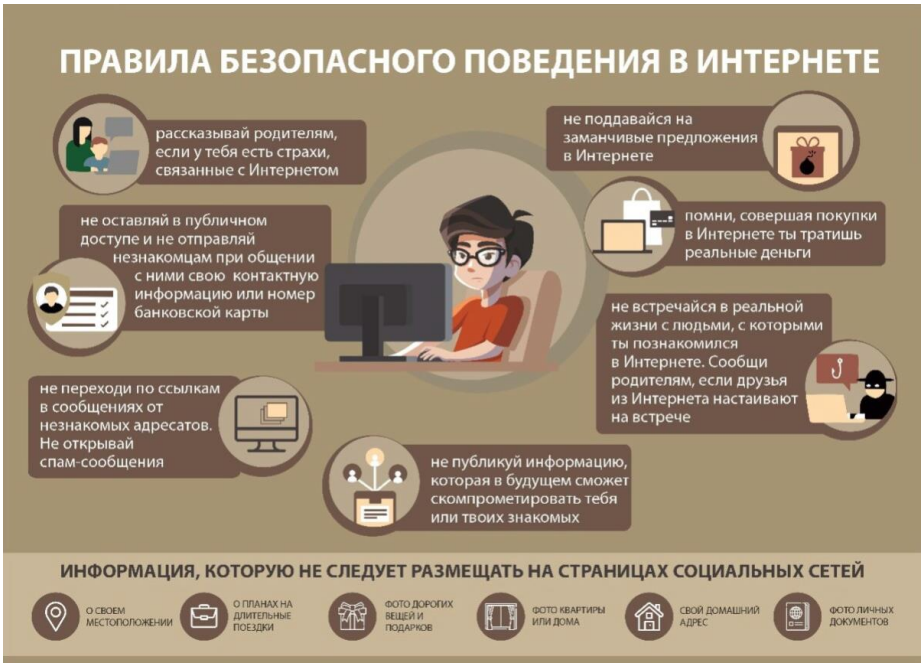
Варианты работы с этой информацией

1. **Обсуждение и дополнение основных 10 правил.**

Учащимся предлагается обсудить и дополнить эти основные правила с учетом уже имеющегося у них опыта работы в интернете.

2. **Рисуем инфографику**

Учащимся предлагается нарисовать плакат в стиле современной инфографики, где размещаются основные правила безопасной работы в сети Интернет.



В качестве примера для учащихся 8-9 классов предлагается занятие в формате семинара «Киберугрозы современности: главные правила их распознавания и предотвращения»

1. **Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете**

   У каждого ученика на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый ученик должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные ученики зачитывают свои листовки, остальные могут добавлять правила. Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит учеников перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников. Проводится обсуждение ответов.

Анализируя исследования, проводимые «Лаборатории Касперского» можно выделить 3 группы серьезных киберугроз:

1. Шпионское программное обеспечение и другие вредоносныепрограммы.
2. Спамы;
3. Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске. После обсуждения листовок на доске должен быть записаны основные правила защиты от киберугроз.

2. Практикум «Угроза 419»

Цель: формирование навыков распознавание спама в «нигерийских письмах».

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419». «Нигерийские письма» - вид мошенничества, получивший наибольшее развитие с появлением спама. Называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов. С появлением интернета «Нигерийские письма» стали нарицательным понятием. Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится, у него выманиваются всё большие суммы денег на сборы, взятки и т. д. В худших вариантах жертве предлагается полулегально прибыть в Нигерию, где его либо арестовывали за незаконное прибытие в страну и у него вымогаются деньги за освобождение, либо похищали с целью получения выкупа.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде. Сделка подаётся как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям. Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.

Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности

«Нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама.

Подавляющее большинство «нигерийского» спама идет на английском языке, но в 2004-2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни.

«Нигерийские письма» являются дидактическим инструментом для формирования навыков распознавания спама и фишинговых атак.

Учитель делит аудиторию на 4 группы. Каждой группе выдает конверт, в котором содержится образец «нигерийского письма» и задание:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.
3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными.

После того, как группы выполнят задание, начинается коллективное обсуждение. Вопросы для обсуждения:

1. Как можно распознать «нигерийское письмо»?
2. Как вы думаете кто авторы «нигерийских писем»?
3. Какую цель преследуют авторы «нигерийских писем»?
4. Можно ли считать безвредными «нигерийские письма»?

Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение. Учитель на доске записывает главные особенности «Нигерийских писем», которые нашли ученики, дополняет, систематизирует. Подведение итогов занятия.

Карточка 1

«Меня зовут Бакаре Тунде, я брат первого нигерийского астронавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским астронавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым. Несмотря ни на что мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами. Вечно ваш, доктор Бакаре Тунде, ведущий специалист по астронавтике».

Карточка 2

«Дорогой друг,

Я послан к вам по поводу моего покойного клиента, фамилия которого совпадает с вашим. Хотя мы еще не встречались друг с другом и раньше, но я верю, что судьба свела нас на ссылка на purpose.It будет лучше, мы утверждаем, и использовать деньги, чем позволить Ecobank

топ- чиновников делиться и отвлекать его в своих соответствующих частных счетов, как заброшенный месторождения. Если закон не мог по конституции банка предоставить их должностными лицами право на наследование месторождения умершего клиента, вы и у меня больше прав, потому что умерший может быть ваш дальний родственник, так как он является гражданином вашей страны. Прежде всего, я работал на него в течение многих лет, поэтому я верю, что он будет счастлив с нашим расположением, чтобы претендовать на фонд особенно когда противоположное состояние деньги незнакомым выступает в подобных старший staffs.You Ecobank, должны понимать, что в финансовых возможностей учреждения, подобные этой, общей, но не слышал. Люди вкладывают свои деньги в финансовые институты и некоторые из этих счетов являются либо закодированы или конфиденциально ссылка на operated.Normally, когда нечто подобное происходит в финансовом учреждении, сообщается в управлении. Он не опубликованы и соответствующие финансовые учреждения только информирует адвокат своего клиента в зависимости от обстоятельств может быть и ждет реальный наследник, чтобы показать. По истечении указанного периода определяется банком получателя, чтобы придумать, руководство отправляет деньги своим «долгом Re-преобразования Департамента и закрытия счета.

Теперь вопрос в том, кто управляет «Долг Re-преобразования Департамента", а кто управления? Ответ прост: они председателей, управляющих директоров и членов Правления. Эти люди разделили деньги, и никто не задает вопросы. На самом деле, такой вопрос даже не обсуждается вне заседаний совета директоров. Если мое расположение обращаюсь к вам, и я получить ваше согласие работать в качестве партнеров в передаче фонда, я буду начинать с необходимой правовой процесс, как покойный адвокат. В сущности, мне нужно будет быть предоставлена информация ниже, так что я могу начать с правовой процесс создания ближайших родственников с умершим;

1. Ваше полное имя
2. Возраст
3. Адрес
4. Частная Телефон
5. Профессия
6. Национальность
7. Другой адрес электронной почты ссылка на yahoo.com, ссылка nahotmail.com.

После этого, я должен подготовить и отправить Вам образцы письмо- заявку, которая будет представлена в банке, положив претендовать на его балансе US $ 10,500,000.00. Фонд может быть оплачен на банковский счет, вы будете назначать в установленном порядке или по видам чек кассира обращается в ваше имя и пользу.

Хотя трудно точно оценить время, которое потребуется, чтобы заключить этот вопрос, но я уверен, что весь процесс не займет до 10 рабочих дней с момента вы официально обратиться с банком transfer.I фонда " м предлагается 40% от общего фонда как вознаграждение за вашу помощь, моя будет составлять 50%, и мы будем дарить 9% (US $ 945 000) для благотворительной организации нашего выбора в то время как 1% (US $ 105,000) будет установлена в сторону, с учетом всех прочих расходов, которые могут возникнуть в процессе transfer.I фонда надеемся, что вы оцените это предложение, как я взял многие вещи во внимание, прежде чем предлагать такое соотношение обмена.

Наконец, я хочу, чтобы вы знали, что я столкнулся с трудностями, пытаясь отправить это письмо к вам, как простой сообщении. Именно поэтому я прикрепил его. Поэтому мой скромный совет, который вы открываете новый адрес электронной почты либо в ссылка на hotmail.com, ссылка на yahoo.com и ссылка на Gmail.com содействовать нашей электронной корреспонденции. Вы также можете связаться со мной через номер +22890945333.
С наилучшими пожеланиями, Г-н Джонсон Slami Esq.»

Карточка 3

«Уважаемый Добрый день!
Я юрист, г-н Карл Алекс Хендерсон Юрист в семье покойного президента Мусу Yaradua, мне было поручено семья в поисках хорошей инвестицией в вашей стране, предпочтительно недвижимость, я должен был обеспечивать конфиденциальность и доверие в этой сделке, так что вы находитесь в лучшем положении, знать больше, чем меня на этом инвестиции.

Деньги наличными $25,2 млн., Муса Yaradua семей хотят инвестировать эти деньги в вашу страну с вашей поддержкой, и мы обнаружили, что этот план, чтобы переместить его с помощью дипломатических средств. Пожалуйста, это очень конфиденциальная и совершенно секретной, я буду лететь вниз, чтобы посмотреть вам в лицо подписывать документы, необходимые для инвестиций, как только вы получите фонд.

Мы предлагаем 10% от общей суммы за вашу помощь в этом проекте, в то время как 5% будет использоваться для любых непредвиденных расходов, которые могут возникнуть при переводе средств.
Я с нетерпением ждем вашего ответа на это письмо. Если вы примете мое предложение, я хотел бы иметь следующую информацию ниже, чтобы начать процесс.
1. Ваше полное имя:
2. Ваш номер телефона:
3. Ваш возраст:
4. Ваш пол:
5. Род занятий:
6. Вашей страны:
С уважением, Адвокат г-н Карл Алекс Хендерсон
Сотовые +2348020574082
факс +23417641464»

Карточка 4

«From: Prince Joe Eboh
Date: Wednesday, April 21, 2004
12:53 PMSubject: TRANSFER
Принц Джо Эбох
Уважаемый господин,/госпожа, Надеюсь, что это послание найдет Вас в хорошем здравии. Я - Принц Джо Эбох, Председатель “Комитета заключения контрактов”, “Нигерийской Комиссии Развития Дельты (NDDC)”, являющейся филиалом нигерийской Национальной Нефтяной Корпорации (NNPC). Нигерийская Комиссия Развития Дельты (NDDC) была создана покойным Главой государства, генералом Сани Абача, который умер 18-ого июня 1998 года, для управления прибылью, образующейся от продаж нефти и ее субпродуктов.

Предполагаемый ежегодный доход на 1999 год составил свыше 45 миллиардов долларов США, сведения об этом содержаться в отчете Генерального аудитора Федеративной республики Нигерия (FMF A26 ONE 3B Параграф “D”) за ноябрь 1999 года.

Я - Председатель Комитета заключения контрактов, и мой комитет исключительно ответственен за то, как и куда должны распределяться денежные средства. Во всех случаях мы действуем от имени Федерального правительства Нигерии. Мой Комитет заключает контракты с иностранными подрядчиками для разработки нефтяных месторождений в районе дельты Нигера.

Так случилось, что в одном из контрактов нам удалось сэкономить US$25,000,000. Но, из-за существования некоторых внутренних законов, запрещающих государственным служащим в Нигерии открытие иностранных счетов, мы не имеем возможности перевести эти деньги за границу.

Однако, эти деньги US$25,000, 000 могут быть оформлены в форме оплаты иностранному подрядчику, поэтому мы хотели бы использовать ваш счет в банке как держателя бенефициария фонда. Мы также достигли соглашения, о том, что Вам будет предоставлена награда за содействие в этой операции в размере 20 % полной суммы, переданной как нашему иностранному партнеру, в то время как 5 % будут сохранены на непредвиденные расходы, которые обе стороны понесут в ходе реализации этой сделки, а остаток в 75 % будет сохранен для членов комитета.

Если Вы решите принять наши условия, Вы должны послать мне немедленно детали вашего счета или открыть новый счет в банке, куда мы сможем осуществить перевод денег в сумме US$25,000, 000 , держателем которой вы будете, до тех пор, пока мы не прибудем в вашу страну за нашей долей. Для нас не важно, каким бизнесом вы занимаетесь. Все, что нам необходимо, это название вашей компании, ваш личный номер телефона / факса, полное имя, адрес и детали вашего счета в банке, на который будет осуществлен перевод через Apex Bank .

Отметьте, что эта сделка, как ожидается, должна будет реализована в пределах 21 рабочего дня со дня, когда мы предоставим все необходимые сведения Федеральному Министерству финансов, которое одобрит необходимое валютное распределение для перемещения этих средств на ваш счет. Пожалуйста, рассматривайте вышесказанное как конфиденциальные сведения.

Прошу Вас ответить мне как можно скорее.

Спасибо за ваше сотрудничество. Искренне ваш, Принц Джо Эбох»

Занятие завершается ответом на вопрос «Как и для чего нужно знать основные правила безопасной работы в Интернете?».

ПРИЛОЖЕНИЕ 1 НАГЛЯДНЫЙ МАТЕРИАЛ «БЕЗОПАСНЫЙ ИНТЕРНЕТ» [1]

Материалы для учащихся средних классов к «Уроку безопасного Интернета» https://ligainternet.ru/wp-content/uploads/2022/10/materialy-dlya-uchashhixsya-srednix-klassov-k-uroku-bezopasnogo-interneta.pdf

Интернет-зависимость

ЕСЛИ ТЫ ХОЧЕШЬ ИЗБЕЖАТЬ ИНТЕРНЕТ-ЗАВИСИМОСТИ, ТО ПРИДЕРЖИВАЙСЯ ПРАВИЛ:

- Сократи время использования гаджетов и компьютера.
- Не бери в руки телефон минимум за час до того, как планируешь лечь спать. Интернет, соцсети или игры могут вызвать яркие эмоции, которые помешают уснуть.
- Не ешь за компьютером и не используй телефон во время еды. Отвлекись от них ненадолго, лучше пообщайся с родственниками или друзьями.
- Старайся на выходных использовать компьютер и гаджеты как можно меньше. В Интернете или в играх очень легко «зависнуть» и весь день пролетит незамеченным, а ты потом будешь сожалеть о потерянном свободном времени.

ПО ДАННЫМ ИССЛЕДОВАНИЙ В РОССИИ:

80% ШКОЛЬНИКОВ не могут обойтись без смартфона

80% ШКОЛЬНИКОВ страдают нарушением зрения

80% ШКОЛЬНИКОВ страдают искривлением позвоночника

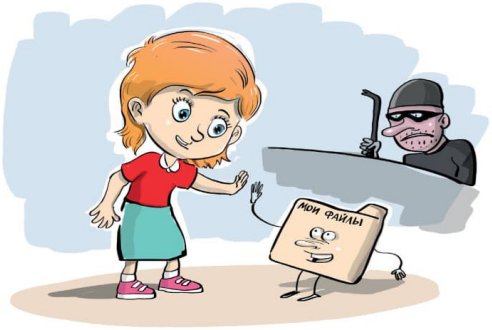
3-4% ВЫПУСНИКОВ полностью здоровы

6

Персональные данные

КАК ЗАЩИТИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

1. **Придумывай и используй разные сложные пароли для почтовых ящиков, соцсетей и других сайтов.** Пароль восстановить проще, чем вернуть украденные деньги.
2. **Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.**
3. **Не отмечай местоположение** своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.
4. **Не ставь в браузере «разрешить» всплывающим окнам.** Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ и соглашаться на какое-либо действие.
5. **Проверь, чтобы твои аккаунты не были доступны с чужих устройств.** В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.
6. **Закрой доступ к своим страницам в социальных сетях.** Включи настройки конфиденциальности.



МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!

12

ПРИЛОЖЕНИЕ 2

ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ШКАЛА ОЦЕНКИ ЗАВИСИМОСТЬ [2]

Шкала оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему

Вопросы предъявляются в случайном порядке. Оценка производится в баллах в соответствии с выбранным респондентом вариантом ответа. Набранные баллы группируются в 4 субшкалы, в зависимости от набранных по ним баллов выводится итоговая оценка.

№	Вопросы	Варианты ответов и баллы			
		нико-гда	редко	часто	все-гда
	Субшкала 1 – Влечение				
1	Ваш ребенок в свободное от других занятий время мечтает только о том, чтобы побыстрее сесть за компьютер или взять в руки мобильное устройство	0	1	2	3
2	Ваш ребенок при возможности выбирать между разными вариантами проведения досуга останавливает свой выбор на взаимодействии с компьютером или мобильным устройством	0	1	2	3
3	Как только появляется малейшая возможность сесть за компьютер или взять в руки мобильное устройство, ваш ребенок немедленно делает это	0	1	2	3
4	Ваш ребенок готов без разбора посещать любые сайты, играть в любые игры, пользоваться любыми программами, лишь бы только пользоваться компьютером или мобильным устройством	0	1	2	3
5	Вы замечали, что приступив к работе с компьютером или с мобильным устройством, ваш ребенок становится подвижным, возбужденным, у него дрожат руки, он пишет друзьям много сообщений, не обращая особого внимания на их смысл	0	1	2	3
6	Вы замечали, что если ребенок некоторое время (несколько дней, месяц) не мог воспользоваться компьютером или мобильным устройством, то снова получив его в свое распоряжение, он стал проводить за ним намного больше времени, чем прежде	0	1	2	3
	Минимальное число баллов – 0, максимальное – 18, группа риска –9 и более, достоверно присутствует патологическое влечение – 12 иболее				
	Субшкала 2 – Утрата контроля				
7	Если ваш ребенок сел за компьютер или взял в руки мобильное устройство, чтобы поработать пять минут, он неизбежно просидит за ним час или два	0	1	2	3
8	Ваш ребенок ведет себя так, словно играет на компьютере или работает с мобильным устройством, хотя ни компьютера, ни планшета у него в настоящее время нет	0	1	2	3
9	Ваш ребенок использует для работы с Интернет одновременно два или более устройств, хотя в этом нет технической необходимости*	0	1	2	3
10	Ваш ребенок использует для работы с Интернет одновременно две или более программ, хотя в этом нет технической необходимости**	0	1	2	3
11	Ваш ребенок пользуется малейшей возможностью, чтобы продлить время взаимодействия с компьютером или мобильным устройством	0	1	2	3

12	Ваш ребенок всегда мечтает о приобретении нового компьютера или мобильного устройства, даже если его собственное – новое и ультрасовременное	0	1	2	3
	* – исключаются случаи, когда использование второго устройства является технически необходимым или оправданным, например, при получении на смартфон пароля для доступа к сетевым сервисам ** – исключаются случаи, когда использование второй программы является технически необходимым или оправданным, например,				
	использование программ-переводчиков или при импорте/экспорте содержимого из одного программного продукта в другой, при конвертации файлов				
	Минимальное число баллов – 0, максимальное – 18, группа риска –9 и более, достоверно присутствует утрата контроля – 12 и более				
	Субшкала 3 – Абстинентный синдром				
13	Вы замечали, что у вашего ребенка, лишенного возможности взаимодействовать с компьютером или мобильным устройством***, меняется настроение, появляются головные боли, боли в мышцах, раздражительность, тревога****	0	2	4	6
14	Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится возбужденным, суетливым, он потеет, у него дрожат руки, он ищет компьютер (телефон) или замену им вплоть до пульта от телевизора или детской игрушки****	0	2	4	6
15	Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, совершает акты вандализма, рвет книги, ломает мебель, отказывается от еды, угрожает самоубийством****	0	2	4	6
16	Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится угнетенным, грустным, малоподвижным, монотонным, говорит тихим голосом, заявляет о бессмысленности своего существования****	0	2	4	6
17	Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится гневливым и агрессивным, сердитым и злым, лезет в драку и/или сам причиняет себе боль или повреждения, в том числе – опасные****	0	2	4	6
18	Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится демонстративным и капризным, жалуется на боли в разных частях тела, на удушье, головокружения, падает в обмороки, испытывает приступы страха, паники****	0	2	4	6

*** - подразумевается, что лишение контакта с компьютером или мобильным устройством носит продолжительный характер

**** - чтобы ваш ответ был утвердительным, достаточно наличия одного из перечисленных в вопросе симптомов

Минимальное число баллов – 0, максимальное – 36, группа риска – 12 и более, достоверно присутствует абстиненция – 18 и более

	Субшкала 4 – Рост толерантности и	поглощенность активностью	
№	Вопросы	Варианты ответов и баллы	
		Нет	Да
19	Ваш ребенок тратит на взаимодействие с компьютером и/или мобильным устройством в среднем более2 часов в день и это время день заднем увеличивается*****	0	6
20	Ваш ребенок, если его не ограничивать, проводит за компьютером или с мобильным устройством все свое время, в ущерб посещению школы, питанию, ночному сну	0	6
21	Создаваемые вашим ребенком в Сети виртуальные образы (в социальных сетях, на форумах, в чатах, в сетевых играх) значительно отличаются от реального (в том числе – по возрасту, полу)	0	6
22	У вашего ребенка отмечается резкое сужение круга интересов, фиксация на игре или сетевой активности, сопровождавшиеся эмоциональной вовлеченностью, поглощенностью своими игровыми успехами или накоплением виртуальных друзей на своей странице в социальной сети	0	6
23	У вашего ребенка отмечается перенос в сферу сетевой активности большинства социальных контактов и многих социальных и даже биологических по своей природе действий, в частности – творческой активности, просмотра кинофильмов и прослушивания музыки, установления дружеских и партнерских отношений, вплоть до виртуальных сексуальных контактов	0	6
24	У вашего ребенка в связи с много-часовой ежедневной сетевой активностью, требующей значительных психических и физических усилий, отмечались выраженное переутомление, формирование астеноневротических реакций (заикания, тиков, обморочных состояний, энуреза, хронической головной боли и других)	0	6

***** - исключаются случаи, когда работа за компьютером или с мобильным устройством объективно является необходимой (например, для получения высоких результатов в учебе, спорте или хобби); включаются игры, посещение сайтов развлекательной тематики, социальных сетей и т.д.

Минимальное число баллов – 0, максимальное – 36, группа риска – 12 и более, достоверно присутствует рост толерантности и поглощенность активностью – 18 и более

Варианты ответов респонденту после завершениятестирования

Вариант 1. Шкала “влечение” – меньше 9 баллов, шкала “утрата контроля” – меньше 9 баллов, шкала “абстинентный синдром” – меньше 12 баллов, шкала “рост толерантности и поглощенность” – меньше 12 баллов.

Ответ 1. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка не выявлено признаков интернет–аддикции. Если продолжаете сомневаться, обратитесь с ребенком к врачу для очной консультации.

Вариант 2. Шкала “влечение” – больше 9, но меньше 12 баллов и/или шкала “утрата контроля” – больше 9, но меньше 12 баллов, шкала “абстинентный синдром” – меньше 12 баллов, шкала “рост толерантности и поглощенность” – меньше 12 баллов.

Ответ 2. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка не выявлено достоверных признаков

интернет–аддикции, однако имеется значительный риск ее формирования. Пожалуйста, обратитесь с ребенком к врачу, на данном этапе возможна успешная профилактика дальнейшего развития зависимости.

Вариант 3. Шкала “влечение” – больше 12 баллов и/или шкала “утрата контроля” – больше 12 баллов, шкала “абстинентный синдром” – меньше 12 баллов, шкала “рост толерантности и поглощенность” – меньше 12 баллов.

Ответ 3. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка с высокой вероятностью имеется интернет–зависимость, предположительно I стадии. Пожалуйста, обратитесь с ребенком к врачу для верификации диагноза и разработки индивидуальной программы лечения и реабилитации.

Вариант 4. Шкала “влечение” – больше 12 баллов и/или шкала “утрата контроля” – больше 12 баллов, шкала “абстинентный синдром” – больше 12, но меньше 18 баллов и/или шкала “рост толерантности и поглощенность” – больше 12, но меньше 18 баллов.

Ответ 4. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка с высокой вероятностью имеется интернет–зависимость, предположительно I стадии с намечающимся переходом во II стадию. Пожалуйста, обратитесь с ребенком к врачу для верификации диагноза и разработки индивидуальной программы лечения и реабилитации.

Вариант 5. Шкала “влечение” – больше 12 баллов и/или шкала “утрата контроля” – больше 12 баллов, шкала “абстинентный синдром”

– больше 18 баллов и/или шкала “рост толерантности и поглощенность” – больше 18 баллов.

Ответ 5. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему у вашего ребенка с высокой вероятностью имеется интернет–зависимость, предположительно II стадии. Пожалуйста, обратитесь с ребенком к врачу для верификации диагноза и разработки индивидуальной программы лечения и реабилитации.

Вариант 6. Шкала “влечение” – меньше 12 баллов и шкала “утрата контроля” – меньше 12 баллов, шкала “абстинентный синдром”– больше 12 баллов и/или шкала “рост толерантности и поглощенность” – больше 12 баллов.

Ответ 6. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, относительно состояния вашего ребенка получены противоречивые данные, не поддающиеся интерпретации. Пожалуйста, понаблюдайте за ребенком внимательно несколько дней и повторите тестирование или обратитесь с ребенком к врачу для очной консультации

ЛИТЕРАТУРА

1. Департамент образования Администрации г. Перми Муниципальное бюджетное учреждение «Центр психолого-педагогической, медицинской и социальной помощи» г. Пермь, 2022.
2. Пережогин, Л.О. Интернет-зависимость : предпосылки формирования, клиническая картина, лечение и профилактика : методические рекомендации / Л. О. Пережогин, А. А. Федонкина. - М.:ФГБУ “НМИЦ ПН им. В.П. Сербского» Минздрава России, 2024. – 33 с.
3. Цветкова, М.С. Информационная безопасность. 2–11 классы : методическое пособие для учителя / М. С. Цветкова. — М.: БИНОМ. Лаборатория знаний, 2020. — 64с.— ISBN 978-5-9963-5730-7.
4. Методический сборник для подготовки и проведения классного часа для школьников по вопросам информационной безопасности / А. К. Балагурова. – Чита: ГУ ДПО «ИРО Забайкальского края», 2022. – 42 с.

ИНТЕРНЕТ-РЕСУРСЫ

1. Безопасный Интернет : материалы для учащихся начальных классов к «Уроку безопасного Интернета» : [презентация] // Лига безопасного Интернета : [сайт]. –URL:https://ligainternet.ru/wp-content/uploads/2022/10/materialy-dlya-uchashhixsya-nachalnyx-klassov-k-uroku-bezopasnogo-interneta.pdf(дата обращения: 19.08.2024)
2. Методические рекомендации по проведению уроков безопасного Интернета в школах : [презентация] // Лига безопасного Интернета : [сайт].–URL: https://ligainternet.ru/wp-content/uploads/2022/10/metodicheskie-rekomendacii-po-provedeniyu-urokov-bezopasnogo-interneta-v-shkolax.pdf (дата обращения: 19.08.2024)

Практическое пособие

Составитель:
Сандабкина Туяна Баировна

УРОКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ СРЕДНЕЙ ШКОЛЫ РЕСПУБЛИКИ БУРЯТИЯ

В АВТОРСКОЙ РЕДАКЦИИ

Технический редактор
Доржиева Алтана Шагдаровна