**Урок информатики в средней школе**

**Тема: “ Безопасность детей в интернете ”**

**Цели:** освоить содержание понятия «информационная культура»; знать основные тенденции развития информационного общества; знать особенности формирования информационных ресурсов и формы безопасной работы с ними.

**Ход урока**

**1. Организационный момент**

**2. Актуализация знаний**

-перечислите основные черты современного общества (наращивание информационного объема и сокращение времени на полное обновление всего информационного массива)

- является ли появление компьютера закономерным процессом развития общества? (компьютер разработан для сокращения рутинных действий человека с информацией, поэтому и можно считать этот процесс закономерным)

- почему на уроках информатики основное внимание уделяется информационным технологиям? (уровень оснащения техникой в обществе еще не так высок, поэтому, необходимо постоянно повышать уровень информационной культуры и навыки компьютерных технологий)

**3. Оборудование:** доска, проектор, презентация, мультимедийные материалы.

**4. Особенности урока**

* Беседа-Дискуссия
* Собственно разработанные мультимедийные материалы
* Максимальный охват всех аспектов темы
* Разделение урока на блоки
* Наглядная демонстрация, примеры.
* Получение заочного жизненного опыта

**5. План урока**

* Вводная часть
* Опасности WWW
* Защищённость операционных систем.
* Пути «заражения».
* Защита, борьба, профилактика вирусных угроз
* Защита от нежелательного контента.
* Рекомендации по защите личных данных и поведению в социальных сетях.
* Вывод. Общее подведение итогов.
* Раздача буклетов, заметок.
* Промежуточные и обобщённые тестирования

**5. Теоретический материал урока**

Развитие компьютерных технологий, как и развитие любой отрасли, привлекает внимание не только людей творческих, позитивных, работающих на благо своего государства, но и людей, несущих негативную волну в общество, связанную с развитием вредоносного программного обеспечения и другими противоправными действиями.

Как защитить себя? Лучший способ – это изучить возможные пути «перемещения» нежелательного для пользователя программного обеспечения и контента.

**Вводная часть.**

В настоящее время, уровень интеграции информационных технологий, распространившихся совершенно во все отрасли, зашёл достаточно далеко. Так, что мы уже не можем представить себе жизнь без всевозможных информационных устройств и других «умных» гаджетов. К великому сожалению, информационные технологии и средства их распространения не всегда используются в мирных, познавательных целях. Возрастает уровень интернет-угроз и мошенничества. В связи с этим, необходимо повышать информационную культуру, которая в свою очередь поможет защититься от вирусных угроз, атак и уловок мошенников.

**Опасности WWW**

1. **Интернет-мошенничество**

**Виды Интернет-мошенничества:**

* **Секретные методы заработка**
* **Выигрыш лотереи**
* **Интернет-Магазин**
* **Фишинг** (Phishing)

От английского *fishing* — рыбалка, выуживание. Вид интернет-мошенничества, при котором мошенник пытается выдать себя за организацию или фирму с целью получения доступа к конфиденциальным данным пользователей  
(логин и пароль от кредитных карт, либо соц. сетей).

* **Вишинг** (vishing — voice phishing)

Аналогичен фишингу. Но отличается тем, что в нём каким-либо образом задействуется телефон.

* **Кликфрод.   
  К**онтекстная реклама— один из видов сетевого мошенничества, представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении.
* **Фарминг**

Его смысл состоит в том, что пользователь направляется на другой сайт, но делает это не через левые ссылки, а посредством зараженного компьютера.

* Скандинавские аукционы

Такой аукцион предполагает пользователям сделать минимальные ставки на товары, выставленные с очень низкой стоимостью, приблизительно пара рублей. С каждой ставки снимается определенный процент. Это такой способ покупки вещей с элементами азарта. Естественно, что ничего вы не получите в итоге.

* Ставки на спорт  
  Букмекерские конторы
* Мошенничество с помощью служб знакомств и социальных сетей

**Опрос:**

*Как распознавать фишинговые сайты или сайты-мошенники?*

**Характерные черты сайтов-мошенников**

* Большие, постоянно вылезающие на весь экран окна.
* Автоматически загружающиеся видеоролики, звуки, музыка.
* Большие, яркие, повторяющиеся заголовки.
* Предсказуемые заманчивые предложения и фразы*(“только сейчас”, “успейте до…”)*
* Невозможность сразу зарыть эту веб-страницу.

**Характерные черты фишинговых сайтов**

* Другое доменное имя, при одинаковом дизайне сайта.
* Дизайн дополнен ранее не встречавшимися новыми функциями.
* Дизайн немного изменён(изменены стили).
* Для входа в ваш профиль вас просят ввести больше информации (E-mail, Секретный вопрос и др.), чем в предыдущие посещения.

***Предлагается*** [***пройти экспресс тестирование по теме***](Интернет-мошенничество.swf)

1. **Опасный контент**

* Провокационные материалы
* Секты
* Экстремистские материалы
* Самоубийства
* Насилие
* Наркотические и психотропные вещества
* Контент для взрослых
* И т.п.

1. **Недостоверная информация**

Не вся информация в интернете верна. Пользуйтесь проверенными сайтами и источниками.

**Защищённость различных операционных систем(ОС)**

**Существующие (наиболее распространённые) ОС:**

* Family Window OS  
  Семейство ОС систем Виндовс
* OS \*nix/ Unix  
   разновидности ОС Linux

**Разграничение прав доступа или многопользовательский режим**

***Family Window OS/Семейство ОС систем Виндовс***. Существует разделение на пользователей с разным разграничением прав доступа (Guest/Гость, Administrator/Администратор). Однако, обычные пользователи этого не знают и работают от имени *Administrator’a.* Что даёт пользователю и всем программам, включая вирусы, полновластно вносить изменения в файловую систему(ФС) и ОС.

***OS \*nix/ Unix, разновидности ОС Linux***. Работа непосредственно из-под учётной записи *СуперПользователя/root(Администратора)* невозможна; пользователь всегда работает с ограниченными правами, а запуск учётной записи root производится только для выполнения отдельных действий, команд, и для каждого такого запуска требуется ввод пароля *СуперПользоватля* или текущего пользователя для подтверждения полномочий. Так Unix разграничивает права доступа*(SELinux, AppArmor),* что не даёт возможности вредоносным программам или вирусам вести свою деятельность.

Это как входная дверь в вашем доме.

В Unix когда вам нужно кого-то *впустить(установить программу, выполнить команду*) или *выпустить*(*деинсталляция*), или *войти самим(вход от Администратора, работа в root консоли* ), вы *открываете* и закрываете за собой дверь*(право доступа*). Каждое такое открытие двери таит в себе опасность: впустить к себе в дом(ОС) кого-то незнакомого или не того(вирус).

Таким образом, работая имени Администратора в OS Windows, вы оставляете эту дверь всегда открытой.

**Вывод:**

* Unix более безопасна.
* ОС \*nix распространяются по свободной некоммерческой лицензии(Free Ware), кроме Mac OS.
* Много пользователей \*nix вносят свой вклад в разработку и улучшение, повышение безопасности.
* Под ОС\*nix написано крайне мало вирусов.

*Опрос на проверку безопасности.*

* *Кто-нибудь пользуется ОС Unix?*
* *Вы ведёте контроль учётных записей Windows, и не работаете от имени Администратора?*

***Предлагается*** [***пройти экспресс тестирование по теме***](ОС.swf)

**Пути «заражения»**

* **Загрузка вредоносных файлов с сети интернет.**

Давайте узнаем и разграничим безопасность файлов, загруженных из сети интернет на три группы.

1. *Безопасные.* Это офисные и мультимедийные файлы. Допустимые расширения:
   * .doc/.docx
   * .ppt/.pptx/.pps
   * .mp3
   * .wma
   * .flac
   * .wav
   * .mp4
   * .fly
2. *Условно безопасные.* Файлы, которые потенциально заражены.
   * *.zip*
   * *.rar*
3. *Опасные.* 
   * *.exe*
   * *.com*
   * *.bat*
   * *.shell*

* **Интернет-серфинг**

Звучит пугающе, не правда ли? Как же это происходит, что при обычном просмотре интернет страниц к нам на ПК попадают вирусы? Всё дело в *JavaScript’ax.* JavaScript – это межплатформенный, объектно-ориентированный язык программирования, базирующийся на объектном представлении браузера, применяемый для использования наибольшей интерактивности. На нём пишутся *JavaScript’ы*(сценарии и скрипты). Они подгружают вредоносные файлы на наш компьютер независимо от наших действий.

Обратимся к статистике атак через Web:

По сравнению с 2011 годом, в 2012 году количество атак через веб-браузер за год увеличилось с 946 393 693 до 1 595 587 670.

* **Спам**

Спам приходит к нам на E-mail. Но не будем про него говорить, а просто посмотрим специально снятый нами видеоролик, который в наглядном примере демонстрирует сущность спама.

[*Мультимедиа (Включается видеоролик про спам.)*](Спам%20и%20борьба%20с%20ним.mp4)

* **Нелицензионное/Пиратское программное обеспечение(ПО)**

Ни для кого не секрет, что люди решившие сэкономить на покупки лицензий покупают или скачивают нелицензионный контент, который как и ввиду своего низкого качества, так и в его *сомнительном содержании* может нанести вред вашему ПК.

* **Офисные документы Word, Power Point, Open Office**

Могут в себе содержать вредоносные файлы в виде дополнений –*макросов.*

*Макрокоманда* или *макрос* — программный алгоритм действий, записанный пользователем. Помимо выполнения набора встроенных в приложение команд, он позволяет производить обработку внешних файлов, загрузку и передачу файлов и данных через интернет, чтение и изменение настроек ОС. Так, как макросы могут содержать и команды, представляющие опасность, ПК мы рекомендуем отключать поддержку макросов для документов с сомнительным содержимым.

* **Троян – Вирусы.**

Вирусы трояны -вредоносные программы, распространяемые злоумышленниками, с целью контроля действий удалённого компьютера.

Наибольшую опасность представляют вирусы-трояны, о работе которых, вы даже не догадываетесь/подозреваете!

Вот наиболее опасные и распространённые из них:

* Flame
* Stuxnet
* DUQU
* Red October
* Gauss

Вирусы-трояны разделяют на две группы:

* Вирусы, которые собирают какие-либо данные.
* Вирусы устраивающие атаки(DDoS)

С первой группой всё просто. Вирусы-трояны могут собирать:

* вашу личную информацию:
  + в маркетинговых целях,($$$Реклама,)
  + для осуществления мошеннических действий
  + либо передавая её правительству.
* Или вести сбор информации коммерческого и документального характера, которые обнаружились в промышленных и топливно-энергитических компаниях Ирана, Израэля, Саудовской Аравии, Сирии, Судане и ряде других стран.

А вторая группа, вирусы-трояны, осуществляющие распределительные атаки, посредством отправки запросов сотнями тысяч компьютеров на сервер, веб-сайт, либо частный компьютер.

Которые можно продемонстрировать примером из фильма «Матрица»: где агент Смит и все его копии являются заражёнными компьютерами, а Нео атакуемым компьютером, отказ которого ведёт к краху всей системы. (затемнение экрана)

Наибольшая опасность этих вирусов заключается даже не в их разрушительной способности и способности сбора различного рода информации, а в широте распространения!

[*Мультимедиа*](Троян%20-%20Вирусы.mp4)

**Способы защиты, борьбы, профилактики**

* **Установка Антивирусного ПО**
* Виды антивирусных программ по степени доступности:
  + Платные:
    - Kaspersky Lab.
    - ESET Nod 32
    - Comodo
  + Бесплатные:
    - Avast
    - Dr. Web
    - AVZ
* «Грамотная» настройка ПО
* **Сетевой брандмауэр**

**Windows Firewall**

* Smartscreen
* **Обновления программного обеспечения**
* **Обновления антивирусных программ**
* **Обновления программного обеспечения операционных систем**
* **Использование дополнительного ПО Расширений и плагинов**

**FireFox Extensions**

* **No Script** (Блокирует JavaScript, Java и другие плагины)
* **Request Policy**(управление межсайтовыми запросами)
* **RefControl и UaControl**
* **Adblock Plus** (блокирует баннеры и рекламу)
* **HTTPS Everywhere**форсированное использования HTTPS на сайтах,   
  которые его поддерживают, но не ставят основным

**FireFox Extensions**

* **Safe Preview.** Позволяет узнать безопасность сайта по ссылке в режиме предпросмотра.

Включает в себя следующий список антивирусных онлайн сервисов:

* + Google Advistory
  + McAfee
  + Norton Safe Web
  + WOT
  + Avast!
  + Trust Wave
  + Dr. Web online check!

**WOT Extensions** (**Web of Trust**). Отображает репутацию web-сайта, составленную пользователями интернета и оценивающуюся по 4 критериям уровня репутации сайта:

* Доверие. Доверяете ли вы этому сайту? Безопасно ли его использовать? Делает ли он то, что обещает? Сайт может получить низкие оценки по этому критерию в случае риска кражи личности, Интернет-аферы, мошенничества с кредитными картами, фишинга, жульничества с лотереей, вирусов, рекламного или шпионского ПО. Рейтинг «неудовлетворительно» может быть выставлен если на сайте слишком много рекламы или всплывающих окон.
* Надежность продавца. Является ли сайт безопасным для купли и продажи, а также любых деловых операций? Сайт рискует получить низкий рейтинг в случае мошенничества или неприятного опыта покупки.
* Конфиденциальность. Можно ли доверять владельцу сайта, сообщать свой адрес электронной почты и загружать файлы? Если на сайте есть спам, рекламное или шпионское ПО, то он получит низкие оценки от пользователей по этому критерию.
* Безопасность для детей: Нет ли на сайте неподходящих для детей материалов (сцен секса или насилия)? Не поощряет ли он опасные или противозаконные действия?

**Защита от нежелательного контента.**

**использование функции антивируса Eset Nod 32.**

**Расширения FireFox:**

* + [**Blocksi**](https://addons.mozilla.org/ru/firefox/addon/blocksi/?src=search)
  + [**BlockSite**](https://addons.mozilla.org/ru/firefox/addon/blocksite/?src=search)

**Другие программы:**

* + NetPolice
  + Crawler Parental Control 1.1
  + Spector Pro 6.0
  + ParentalControl Bar 5.22
* **Подключение дополнительного пакета услуг от провайдера**

Например, пакеты услуг Ростелеком’a:

* + Детский интернет
  + Функция «ребёнок в доме».
  + Антивирусного программного обеспечения
* **По возможности, использовать зашифрованный протокол HTTPS**

Передаваемые по нему данные, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита этих данных

* **Будьте внимательны!**

Как можно чаще смотрите на адресную строку веб браузера. В большинстве случае, только так вы сможете отличить фишинговый сайт от настоящего.

Делайте это внимательно! Посмотрите на этот адрес:  
<http://www.odnoklassniki.ru.user.name/profileviewlyirb?&5498464571>

Ведёт ли он на настоящий сайт «одноклассники.ру»?

Вовсе нет! Он ведёт на сайт ***www.user.name/,*** где ***odnoklassniki.ru.*** является субдоменным именем.

* **Делайте резервные копии данных**
  + Образ системы
  + Точки восстановления

**Программы для резевных копий**

* + Acronis
  + Norton

**Облачные сервисы  
 хранения:**

* SkyDrive
* Яндекс Диск
* Drop Box
* **Принимайте необходимые меры предосторожности, пользуясь точками открытого доступа Wi-Fi**

Трафик, передающийся через точки открытого доступа может быть перехвачен, а закрытые точки доступа могут быть взломаны.

**Рекомендации по поведению в социальных сетях**

* При регистрации в социальных сетях не указывайте свои ФИО, дату рождения, ваши фотографии. Заменяйте их оригинальным НикНейм’ом(Прозвище) и аватаром(картинкой), известным вашим друзьям.
* Не публикуйте свои личные данные на веб сайтах так, как их индексируют специальные поисковые боты и формируют базу данных.
* Необходимо учитывать, что после публикации информации или других данных в сети, их трудно или практически невозможно удалить.
* Добавляйте в свой круг общения только лично известных вам людей.
* Не открывай письма от незнакомых людей. И уж тем более не переходи по содержащимся в них ссылкам и не скачивай файлы.
* Твой новый приятель, с которым ты познакомился в интернете, может не являться тем, за кого себя выдаёт.
* В целях безопасности, не рекомендуется встречаться с людьми, с которыми ты знаком только по переписке.
* Не вся информация в интернете верна. Пользуйтесь проверенными сайтами и источниками.
* Уважайте своих собеседников. Для интернета есть свой сетевой этикет – нетикет.
* Не видитесь на провокации под видом каких-либо конкурсов – это мошенничество.
* При сёрфинге по социальным сетям в точках открытого доступа (сети Wi-Fi), во избежание взлома, рекомендуем менять пароли.
* Также, рекомендуем создавать сложные пароли, состоящие из более чем 10 знаков, содержащих буквы и спецсимволы.

**Вывод по уроку*.***

Мы узнали основы информационной безопасности:

* Опасности Всемирной Паутины
* О путях «заражения»
* О защищённости операционных систем
* Необходимые методы борьбы, защиты и профилактики
* Про антивирусное ПО
* Рекомендации по поведению в социальных сетях
* Научились отличать фишинговые и мошеннические сайты

***Таким образом****, используя вышесказанный комплекс мер противодействия и систем зашиты, мы можем максимально защититься от вирусных атак, угроз, всевозможных мошеннических действий и нежелательного контента. Что позволит наиболее комфортно пользоваться сетью Интернет и информационными технологиями в целом.*

***В завершение урока для закрепления материала предлагается*** [***пройти итоговое тестирование.***](Итоговое%20тестирование.swf)

## 6. Использованные материалы.

## Автор работы не использовал какие-либо внешние источники информации в чистом виде. Написанный материал по сути является обобщением и анализом общеизвестных сведений, по характеру сравнимых с аксиомами. В случае возникновения каких-либо вопросов, автор готов указать конкретные ссылки на авторитетные, печатные либо электронные, источники информации.

## Все мультимедийные материалы: интерактивные элементы и тесты, видеоролики, презентация - являются личными разработками автора.

## 7. Куратор работы: Ольга Владимировна Пискунова. Учитель математики, информатики МБОУ СОШ с. Балтай.

## 8. Дополнительная информация.

## Предлагаем вам ознакомится с реально проведённым уроком, размещённом на веб-ресурсе “youtube”:

## <http://www.youtube.com/watch?feature=player_detailpage&v=G1skoUbaf2E>

## Дополнительная контактная информация:

## E-mail:

## Skozobow.Roman@yandex.ru