Модуль №1
ТЕХНИЧЕСКИЕ АСПЕКТЫ

Эра интернета

Мечтаешь стать супергероем? Добро пожаловать в век Интернета. Владение новыми технологиями позволяет открыть целый мир во всём его разнообразии. Уверены, ты уже испытал на себе «эффект присутствия», когда посредством Интернета мгновенно связывался с людьми по всему миру и был в курсе любых событий. Разве это не удивительно?! Несколько кликов — и в твоём распоряжении любая информация, музыка или фильмы из облачного хранилища данных. А за знаниями совсем не обязательно ехать в столицу — Интернет позволяет создать глобальную научную среду онлайн и получать образование бесплатно.

И постоянно появляется что-то новое. В 2013 году компания Google анонсировала очки с дополненной реальностью, совмещающие окружающий мир и изображение, сгенерированное компьютером. Интернет — это сверхвозможности! Используешь ли ты их?

Представь, что интернет изобрели 1000 лет назад
http://www.youtube.com/watch?v=TMJMjyyEAZU

Изучи Интернет
http://www.igra-internet.ru/

Что даёт интернет

Как насчёт того, чтобы отправиться в кругосветное путешествие? Начни, например, с виртуального маршрута Москва — Владивосток, где под стук колёс из окна поезда тебе откроется увлекательный и незнакомый мир. Любители пеших прогулок могут побродить по улочкам Барселоны или пройти трудным горным маршрутом к Гранд-Каньону. Коллекция «Чудес света» включает самые известные места планеты. Это удивительное собрание объектов всемирного наследния ЮНЕСКО.

Арт-проект Google раскрыл для тебя двери более 200 музеев из 40 стран мира. Из российских музеев здесь представлены Государственный музей изобразительных искусств имени А. С. Пушкина, Русский музей, Государственная Третьяковская галерея, Государственный Эрмитаж и Музей имени Н. К. Рериха.

Ты можешь рассмотреть шедевры мирового искусства в мельчайших деталях, как не смог бы этого сделать даже в музее. А хочешь исследовать исторические архивы, которые невозможно увидеть в реальной жизни? С Интернетом у тебя есть доступ практически к любой информации.

Читай книги, изучай редкие языки, будь в курсе передовых научных публикаций — открывай мир, границы которого стирает Интернет. Теперь тебе доступны образовательные программы любого уровня — от школы и колледжа до лучшего университета. А с проектом «Википедия» ты, конечно, уже познакомился, когда готовился к урокам или писал реферат.

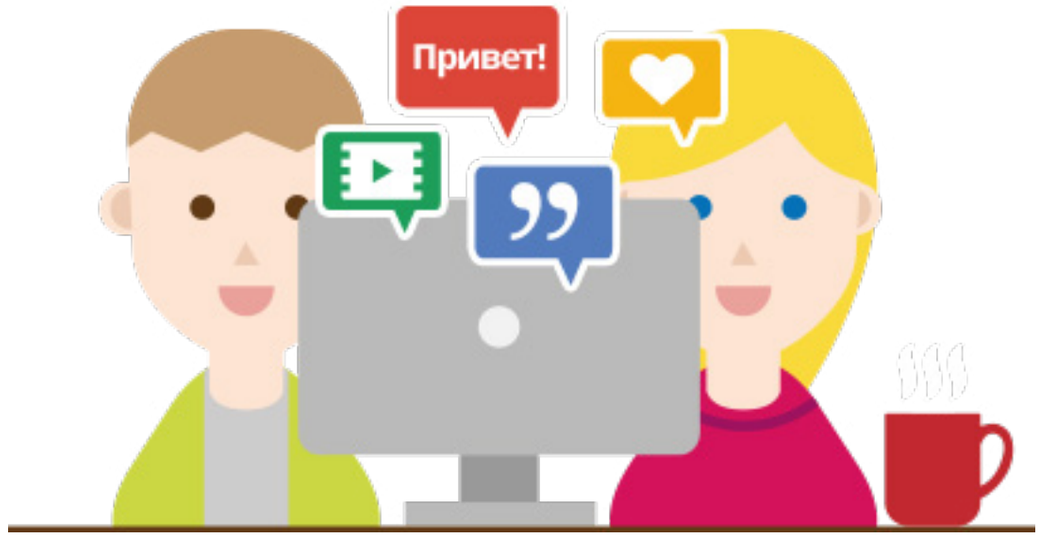
«А развлечения?» — спросишь ты. Конечно! Телеконтент, коллекции фильмов художественного и документального жанров, мультфильмы... А может, лучше купить билет онлайн и пойти с друзьями в кинотеатр?

Мультиязычная образовательная Академия Хана
http://www.youtube.com/user/KhanAcademyRussian?feature=watch

Научная ярмарка Google
https://www.googlesciencefair.com/ru_ALL/2013/

Я в интернете

Интернет даёт тебе новую степень свободы, не сравнимую ни с чем. Благодаря Интернету ты можешь реализовать себя в любой области, заявить миру о своих увлечениях, талантах и планах на будущее. Разве не вдохновляет пример 16-летнего эксперта по безопасности Android Хиромы Якура и 17-летнего Ора Саги — участника космической программы с собственным проектом беспилотника на Луну?! А вспомни 15-летнего Ариана Манна, создавшего игру, которую выпустила компания Apple? Или онлайн-кондитерскую Аманды Лим, или 15-летнюю Анну Дрованди — президента компании по производству и продаже сыров и йогуртов? Подозревал ли Джастин Бибер, что ролик, выложенный на YouTube, сделает его звездой? Что мешает тебе достигнуть таких же результатов? Начни свой проект, собери своё сообщество! И помни: всегда можно напрямую обратиться за помощью к профессионалам и даже получить финансовую поддержку. Ведь мы уже говорили, что в Интернете нет никаких барьеров и ничего невозможного!



Литературный проект Adora Svitak
http://www.adorasvitak.com/Main.html

Детский волонтёрский проект
http://www.webuilt.org/

Технические аспекты

Интернет стал привычной частью нашей повседневной жизни. Мы используем его не задумываясь, как если бы включали телевизор или микроволновую печь. Клик-клик — всё очень просто. Разработчикам действительно удалось сложные и наукоёмкие технологии сделать дружелюбными для пользователя.

Однако иногда эта простота обманчива, поэтому важно усвоить базовые принципы безопасного использования Интернета.

.....

СОДЕРЖАНИЕ

Программное обеспечение

Для просмотра веб-сайтов используется специальное программное обеспечение — браузер. Различные настройки браузера призваны сделать использование Интернета простым и безопасным.

Например, в браузере Google Chrome опция сохранения паролей упрощает доступ к регулярно посещаемым сайтам. Достаточно один раз ввести логин и пароль, применить функцию «запомнить пароль» — и в дальнейшем браузер будет вводить данную информацию автоматически. Но использовать эту функцию можно только на персональном устройстве, к которому никто, кроме тебя, не имеет доступа.

Функция автозаполнения позволяет единожды ввести имя, адрес, номер телефона, адрес электронной почты и другую контактную информацию, чтобы программа её запомнила и автоматически предлагала при повторном введении учётных данных. Чтобы сохранённой информацией не могли воспользоваться злоумышленники, включай эту опцию браузера только при заполнении неконфиденциальной информации.

В Google Chrome история посещённых страниц сохраняется автоматически. Это удобно, если нужно вернуться обратно на страницу или восстановить события. При работе на общественном компьютере лучше использовать режим инкогнито, при котором история не сохраняется.

Всплывающие окна чаще всего используются для размещения в Сети рекламных сообщений. Google Chrome автоматически блокирует всплывающие окна, чтобы они не загромождали экран. При этом в адресной строке появляется значок:

Браузеры позволяют сохранять файлы из Интернета на локальном диске компьютера. При загрузке файла (например, с расширением EXE, DLL или BAT) браузер запросит подтверждение операции. Это позволяет предотвратить автоматическую загрузку вредоносного программного обеспечения на твой компьютер. Если URL загружаемого файла находится в актуальном списке вредоносных веб-сайтов — браузер выдаст предупреждение.

5 принципов конфиденциальности Google
http://www.youtube.com/watch?v=ah5DfJe-0Dk&list=PLD70-B32DF5C50A1D7

Безопасность подключения

Способы доступа в Интернет различаются по степени надёжности. Наиболее уязвимым считается выход в Интернет через общие компьютеры или публичные Wi-Fi-сети. Основной риск — кража пароля от аккаунтов в социальных сетях, от почты или электронных кошельков. Поэтому старайся не использовать платёжные системы и другие важные сервисы при работе с таким подключением.

При заходе на сайт следи, чтобы его адрес начинался с https://. Ещё лучше, если рядом будет стоять иконка замка:

Первое обозначает, что соединение с веб-сайтом зашифровано, второе — что оно защищено и более безопасно. Дополнительная степень защиты — сертификат надёжности. Если у сайта такой сертификат есть, то его индикатор появится на зелёном фоне между значком замка и URL-адресом.

Установив домашний Wi-Fi, обязательно защити сеть паролем, используй собственную комбинацию символов, а не предлагаемую по умолчанию. В настройках доступа выбирай более надёжный протокол WPA2.

Пароли

Идентификатором пользователя в виртуальной среде служит имя (логин), выбранное при регистрации. Логин используется вместе с паролем, который необходим для аутентификации пользователя. Правильная пара «логин — пароль» обеспечивает вход в систему.

Многие сайты (особенно это касается платёжных веб-ресурсов и систем онлайн-банкинга) используют более эффективный способ двухэтапной аутентификации с подтверждением пароля через одноразовый код, который приходит по СМС или электронной почте. Эта опция имеется и у почтового сервиса Gmail. Кража пароля от электронной почты даёт злоумышленникам несанкционированный доступ ко многим ресурсам от имени пользователя, поэтому следует максимально обезопасить свой аккаунт.

Но прежде всего ты должен знать, как самому повысить надёжность пароля:

1. **Идеальный пароль — это комбинация из различных 8 и более букв, цифр, а также знаков пунктуации и символов.**

2. **Используй разные пароли для каждой учётной записи.**

3. **Регулярно меняй свои пароли.**

4. **Для генерации и хранения паролей применяй специальные программы.**

Как выбрать надёжный пароль

http://www.youtube.com/watch?v=QvOlgob5njQ

Защита компьютера от вирусов

Работа в Интернете делает компьютер уязвимым для вредоносных программ — вирусов. Чтобы предотвратить заражение, придерживайся следующих правил:

1. **Регулярно обновляй браузер, операционную систему и антивирусную базу.** Браузер Chrome автоматически обновляется до последней версии при каждом запуске, обеспечивая надёжную защиту без усилий со стороны пользователя.

2. Проверяй **адреса сайтов, не загружай неизвестные файлы** с расширением .exe, .dll, .bat и не переходи по ссылкам из всплывающих окон.

3. Если твои действия привели к **блокировке экрана** подозрительным сообщением, закрой браузер в диспетчере задач или мониторе активности своей операционной системы.

4. **Загружай ПО только с официальных сайтов-разработчиков.**

5. **При неадекватной работе ПО** (устройство медленно работает, появляются всплывающие окна, выполняются непонятные платежи) сразу удали его с помощью последней версии антивирусной программы.

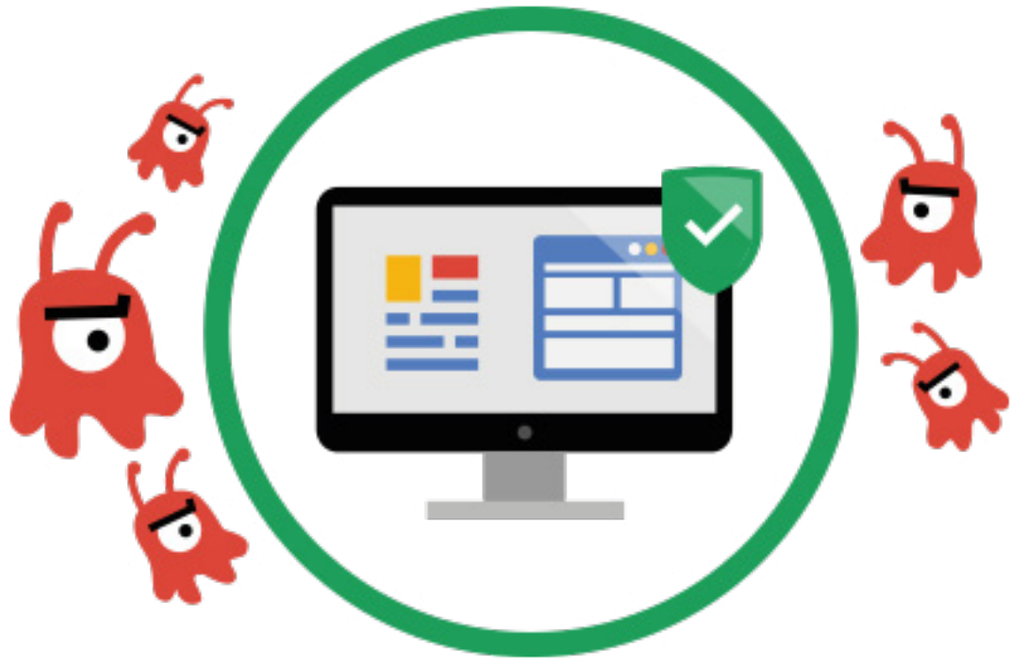
6. **Выбирай зарекомендовавшие себя** антивирусные программы и устанавливай только лицензионные версии.

7. **Установи следующие настройки антивирусной программы:**
   — включи проактивный и поведенческий анализ
   — эти режимы позволяют отловить вредоносные программы, которых ещё нет в антивирусной базе;
   — настрой проверку почтовых сообщений и их вложений;
   — проводи полное сканирование компьютера и подключаемых устройств не реже 1 раза в неделю.

8. Не устанавливай на компьютер сразу **несколько средств защиты**. Программы распознают друг друга как вредоносное ПО и начинают конкурировать или вообще перестают работать.

Как защитить компьютер от атак
http://www.google.ru/goodtoknow/online-safety/device/

Как защитить компьютер и мобильное устройство от злоумышленников
http://www.google.ru/goodtoknow/online-safety/locking/



Конфиденциальность

В Интернете, как в любой публичной сфере, размещение персональных данных должно ограничиваться соображениями конфиденциальности и личной безопасности. Хорошо, когда родители по твоим чекинам могут видеть, что с тобой всё в порядке. Но если информация о твоём местонахождении находится в открытом доступе, ею могут воспользоваться и злоумышленники — например, чекин на отдыхе подскажет, что семья уехала из города и оставила квартиру без присмотра. Поэтому, делясь информацией, не забудь грамотно выставить настройки доступа.

Центр безопасности Google+ наряду с общими настройками защиты данных ввёл специальные настройки для подростков.

При загрузке домашнего видео на YouTube рекомендуется выбрать вариант «Личное» или «Доступно тем, у кого есть ссылка».

Помни, что при общении в чате Gmail или в приложении Google Hangouts ты можешь выключить запись чата.

Технологии безопасности Gmail включают в себя проверку на вирусы, фильтрацию спама, доступ по протоколу HTTPS и двухэтапную аутентификацию.

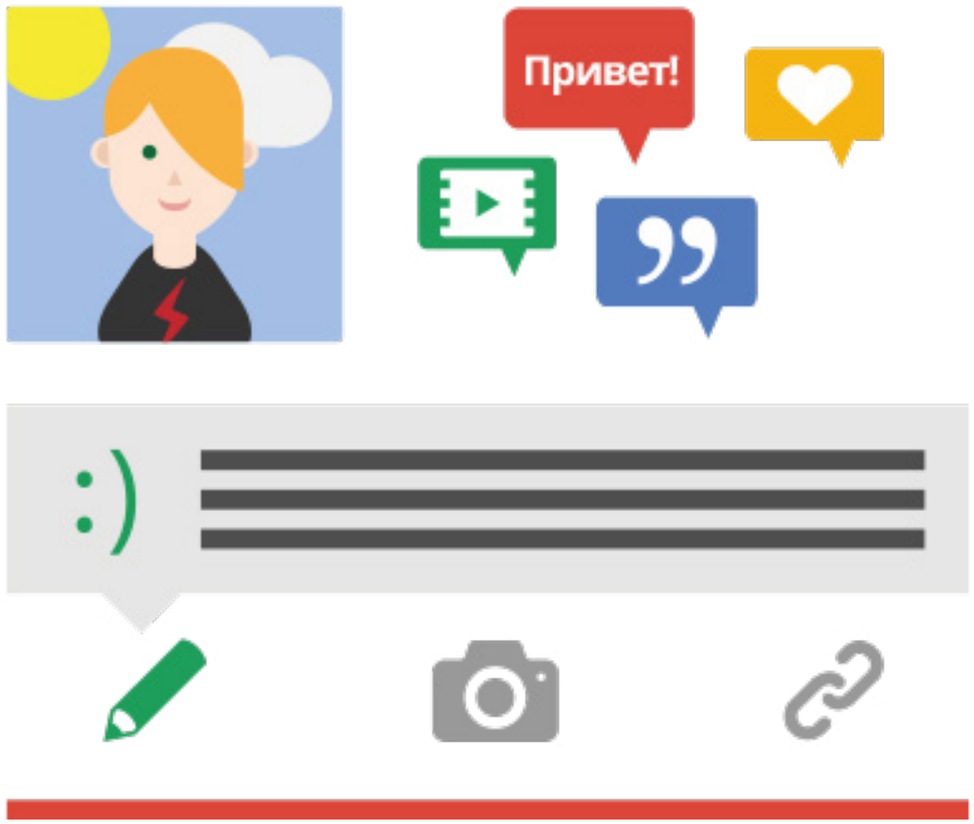
При попадании конфиденциальных данных в панораму улиц на картах Google (Street View) ты можешь отправить запрос на «размытие» изображения.

Несмотря на общедоступность, блоги в Blogger имеют опцию ограничения доступа читателей.

Отправка геоданных:
вы сможете в любой момент включить и отключить отправку геоданных, если захотите делиться своими координатами в Google+, сохранять историю местоположений или использовать эту функцию для других целей.

Сервис «Я в Интернете» от Google позволяет отслеживать информацию о тебе в Сети и управлять публикацией другими пользователями твоих личных

Инструменты безопасности и конфиденциальности Google
http://www.google.ru/goodtoknow/online-safety/security-tools/



Защита от хищения личных данных

Киберзлоумышленники крадут личные данные, чтобы использовать их в преступных целях. Не дай мошенниками провести тебя!

1. **Не передавай пароли, личные и финансовые данные** через электронную почту, сообщения чата или всплывающие окна сайта.

2. **Не переходи по обманчиво знакомым ссылкам из подозрительных сообщений** — введи URL самостоятельно или воспользуйся закладками.

3. Никому **не передавай свой пароль** и помни, что официальный сайт никогда не затребует таких сведений.

4. **При вводе учётных данных следи, чтобы URL сайта** начинался с **https://**, а в адресной строке платёжной системы или банка обязательно стоял значок замка.

5. **Всегда** сообщай о подозрительных письмах или попытках мошенничества.

Технологии защиты личной информации в Интернете
http://www.google.ru/goodtoknow/protection/identity/

Как не допустить хищения личных данных
http://www.google.ru/goodtoknow/online-safety/identity-theft/

Выводы

Интернет — глобальный источник информации и знаний. Это уникальная платформа для общения, творчества, создания собственных проектов и самореализации.

Используя по максимуму возможности Интернета, постарайся свести к минимуму риски, связанные с хищением личных данных и заражением компьютера вирусами.

Для этого выбирай безопасные способы подключения к Сети. Следи за надёжностью и секретностью своего пароля.

Установи на компьютер лицензионную антивирусную программу и грамотно выстави параметры защиты.

С помощью настроек конфиденциальности, которые имеют все сервисы Google, ограничь доступ к своей личной информации и будь внимателен, с кем, как и чем ты делишься.

Сообщай о попытках мошенничества и помни, что родители, учителя и специалисты службы технической поддержки всегда готовы прийти к тебе на помощь.