

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

*Подготовила воспитатель Елань-Колоновского центра ППМСП
Завьялова И.Г.*



ИНТЕРНЕТ

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



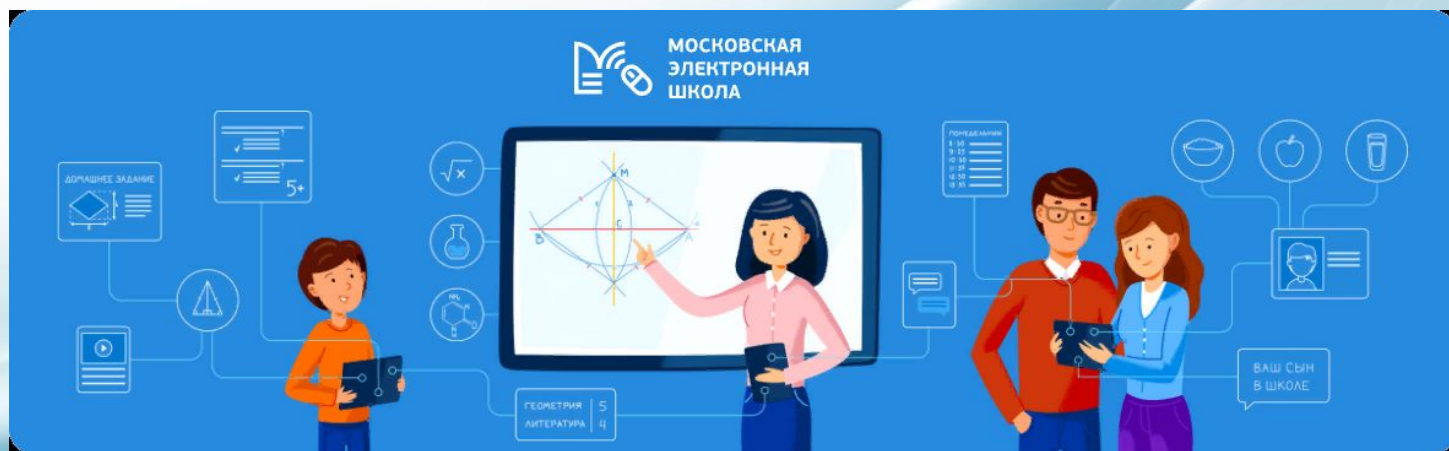
Среднесуточная аудитория Российского Интернета (Рунета) достигла 80,5 млн пользователей, а 66,5 млн. человек выходят в сеть каждый день что составляет 57% населения.



Средний возраст начала самостоятельной работы в Сети - 10 лет и сегодня наблюдается тенденция к снижению возраста до 9 лет;

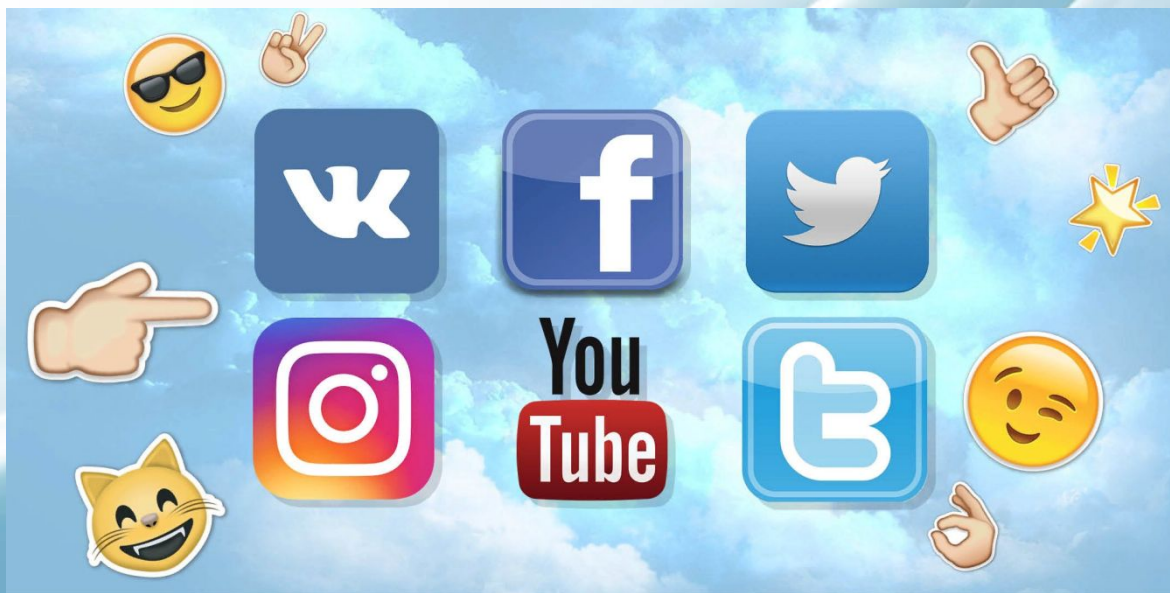


Современные сетевые средства позволяют не только общаться в социальных сетях, но и совместно учиться, познавать новое, создавать авторские информационные продукты. Компьютер в наше время стал для ребенка и «другом», и «помощником», и даже «воспитателем», «учителем».



Что подростки делают в интернете?

Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Кроме того, подростки активно используют поисковые машины. В этом возрасте Интернет становится частью социальной жизни детей: в Интернете они знакомятся и проводят время, ищут информацию, связанную с учебой или увлечениями.



Какие же опасности ждут школьника в сети?

- Сайты, разжигающие национальную рознь и расовое неприятие
- Депрессивные молодежные течения
- Пропаганда наркотиков
- Сайты знакомств
- Секты
- Контентные риски
- Электронная безопасность
- Вредоносные программы
- Спам
- Кибермошенничество
- Киберпреследования



Вредоносные сайты и вирусы

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты.

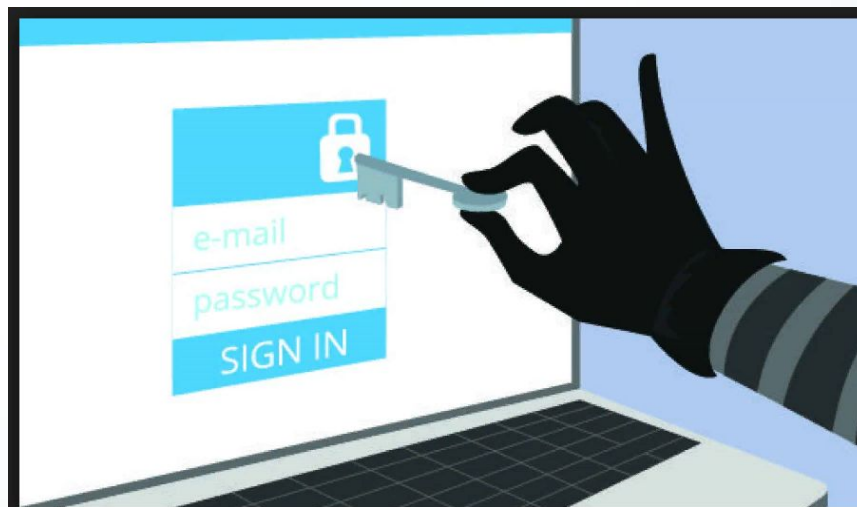


Защита от вирусов

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



ПОЛУЧЕНИЕ ДОСТУПА К АККАУНТАМ В СОЦИАЛЬНЫХ СЕТЯХ И ДРУГИХ СЕРВИСАХ



Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах.



Защита от взлома аккаунта

- Использовать сложные пароли (сложные пароли 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 сообщать свой пароль.
- Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.
- Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).
- Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.



Борьба с сетевыми угрозами

- *Установите комплексную систему защиты!*
Они включают в себя антивирус, фаерволл, антиспам – фильтр и еще пару – тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому настройте программу на автоматическое обновление.
- *Будьте осторожны с электронной почтой!* 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.
- *Пользуйтесь надежными браузерами!*
- *Постоянно обновляйте операционную систему Windows!*



Борьба с сетевыми угрозами

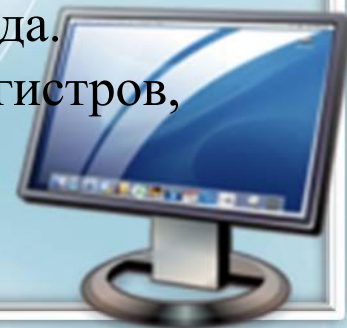
- *Никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.*



- *Пользуйтесь лицензионным программным обеспечением!*
- *Используйте сложные пароли!*

В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — 2-4 часа, но чтобы взломать семисимвольный пароль, потребуется 2-4 года.

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



СПАСИБО ЗА ВНИМАНИЕ

Использованы материалы:

- 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.
- Википедия – свободная энциклопедия
http://ru.wikipedia.org/wiki/Компьютерный_вирус
- Безопасный компьютер и Интернет для детей: новая программа повышения квалификации преподавателей АПКиППРО //Microsoft в образовании. — [Электронный ресурс]. — Электрон. дан. – сор. 2008 – Режим доступа: <http://www.ms-education.ru>.
- <http://pedsovet.su/>

