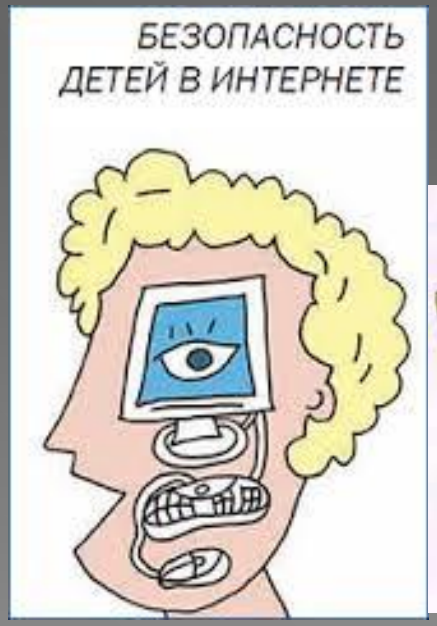
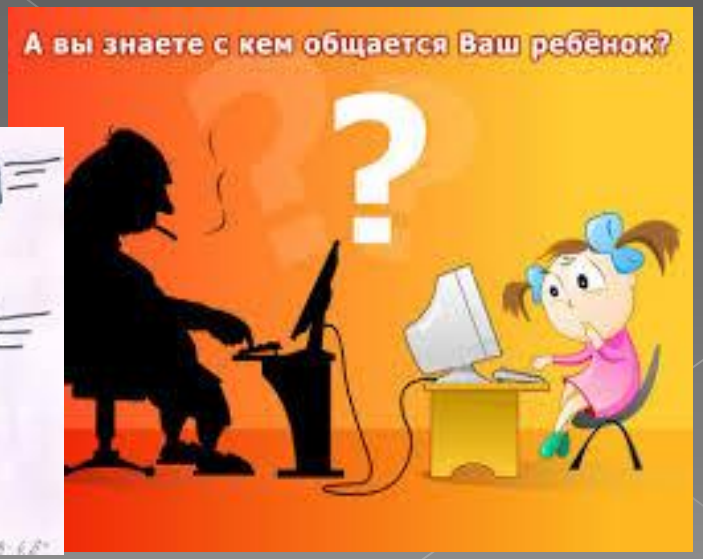
Презентация на тему : Безопасность в сети интернет.

Выполнила учащаяся
8 а класса
Мелина Надежда

XXI век – это не только век новых технологий, прогресса, но и век информационных войн. Общество постепенно включатся в виртуальный мир, поддается соблазнам Интернета, компьютеризируется и не противится процессу увеличения компьютеров в своей жизни. Теперь практически каждый современный человек знает, что такое компьютер, использует его на работе, дома. Современный мир компьютерных технологий позволяет нам решать невероятно большое количество задач, помогает нам обрабатывать огромное количество информации за считанные минуты, секунды. Современная скорость развития компьютерных комплектующих уже не только решает математические, графические задачи. Сегодня мы без особого труда можем обработать видео и аудио информацию, создание видеороликов. Компьютер широко используют от кассиров до
аниматоров и так далее.
Несмотря на нестабильность и не очень высокий жизненный уровень в нашей стране, люди все-таки понимают необходимость использования компьютерной техники.





- **Методы защиты информации сегодня.** Существуют несколько видов защиты информации. Защита выбирается в зависимости от оборудования, возможностей и совместимости . Рассмотрим некоторые из них. Одним из средств физической защиты являются **системы архивирования и дублирования информации**. В локальных сетях, где установлены один-два сервера, чаще всего система устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании.

Наиболее часто встречающиеся угрозы при работе в Интернет:

1. Угроза заражения вредоносным программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы. Эти методы довольно часто используется хакерами для распространения троянских вирусов;
2. Доступ к нежелательному содержимому. Это насилие, наркотики, страницы подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию;
3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи;
4. Поиск развлечений (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег.
5. Неконтролируемые покупки.

Никогда	Всегда
Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы без разрешения родителей	Всегда будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть
Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями	Всегда спрашивай у родителей разрешения посидеть в чате
Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах	Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями
Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера	Всегда держи информацию о пароле при себе, никому его не говори
Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые	Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман
	Всегда держись подальше от сайтов "только для тех, кому уже есть 18". Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой

Если ты услышишь или увидишь, что твои друзья заходят в «небезопасные зоны», напомни им о возможных опасностях и посоветуй, как им правильно поступить.

Будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в «небезопасную зону» или загрузить на свой компьютер вирус или программу-шпион.

Если вы получили оскорбляющие сообщения, расскажите об этом родителям.

Всегда принимайте помощь от взрослых или друзей, разбирающихся в вопросах безопасного Интернета. Мама и папа могут не знать ответов на все интересующие вас вопросы.

- **Влияние компьютера и интернета на здоровье человека**

Плюсы Минусы

Развитие коммуникационных способностей Ухудшение здоровья:

болезни глаз,

искривление позвоночника,

ожирение,

гастрит,

утомляемость,

раздражительность,

Развитие навыков ИКТ Зависимость

Появление друзей Нервные срывы

Умение легко и непосредственно общаться Расшатанная психика

Понимание других людей (развитие толерантности) Принятие компьютерной действительности за реальность

Потеря навыков письма на бумаге

На сегодняшний день известно как минимум 3 основных вида воздействия компьютера на здоровье человека.

- **Вывод:**
- В настоящее время, например, средства электронной почты, используются не только для общения между людьми, а для передачи контрактов и конфиденциальной финансовой информации. Web сервера используются не только для рекламных целей, но и для распространения программного обеспечения и электронной коммерции. Электронная почта, доступ к Web серверу, электронная коммерция, VPN требуют применения дополнительных средств для обеспечения конфиденциальности, аутентификации, контроля доступа, целостности и идентификации.