****

****

****

**Опасности в Интернете**

В современном мире среди активных пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир... Но в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента .

****

**Преступники и злоумышленники**

Преступники используют преимущества анонимности для завязывания доверительных и дружеских отношений с неопытными молодыми людьми. Преимущественно контакты с детьми устанавливают в чатах, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции, где незнакомые люди могут привлечь подростка своим вниманием, заботливостью, добротой и даже подарками. Злоумышленники выслушивают проблемы подростков и сочувствуют им, но постепенно вносят в свои беседы оттенок сексуальности или демонстрируют материалы эротического содержания. Преступники могут также обсуждать возможность встречи с детьми в реальной жизни.

**Заражение вредоносными и нежелательными программами**

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом, использовать компьютер для распространения своих копий на компьютеры коллег, друзей, родственников пользователя и по всей остальной глобальной Cети. Под «нежелательным программным обеспечением» понимаются программы, которые выполняют на компьютере некие задачи без согласия на то пользователя. Они могут показывать рекламные сообщения, объявления или собирать личные данные о человеке, его окружении. Необходимо постоянно улучшать защиту компьютера.

**Азартные игры в Интернете**

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

**Онлайновое пиратство**

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом –например, музыки, фильмов, игр или программ – без разрешения правообладателя. Раскрытие личных данных. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Подробное раскрытие личных данных потенциально опасно.

**Интернет-мошенничество и хищение данных кредитной карты**

Интернет-мошенничество может осуществляться с помощью фальшивых электронных писем, в которые включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом будет использована с ущербом для пользователя. Поэтому, посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта и не пользоваться ссылкой, содержащейся в подозрительном электронном письме.

**Неправильное формирование нравственных ценностей**

В Интернете можно встретить материалы нежелательного характера, к которым можно отнести материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, включающие ненормативную лексику. Существуют средства фильтрации нежелательного материала, но фильтры могут только помочь в блокировании только некоторых нежелательных материалов и решить полностью проблему не могут. Поэтому взрослым важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались за советом и помощью.



**Безопасность в Интернете**

Начиная с 1988 года, ежегодно 30 ноября отмечается Международный день защиты информации. Именно в этом году произошла самая первая масштабная компьютерная эпидемия, которая получила название «эпидемия червя Морриса». Червь был назван так в честь своего разработчика Т. Морриса. Тогда появление сетевого червя парализовало работу шести тысяч интернет-узлов США, нанеся ущерб в размере около 96 миллионов долларов.

Благодаря этой эпидемии человечество поняло, как опасно безоговорочно доверять компьютерным сетям.В период перехода к информационному обществу одним из важнейших аспектов деятельности человека становится умение оперативно и качественно работать с информацией. В данный период времени многие области деятельности человека связаны с применением компьютера. Эти машины плотно внедрились в нашу жизнь. Они имеют колоссальные возможности, позволяя тем самым освободить мозг человека для более необходимых и ответственных задач. Компьютер может хранить и обрабатывать очень большое количество информации. А также компьютеры, объединённые в сети, могут предоставлять доступ к колоссальному количес тву самых разнообразных данных.

Информация, находящаяся на электронных носителях играет все большую роль в жизни современного общества. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным и другим данным. Всё увеличивается число компьютерных преступлений, поэтому информация – это ресурс, который нужно защищать. Информационная безопасность — совокупность мер по защите информационной среды общества и человека.

Информационные угрозы безопасности информации можно разделить на преднамеренные

(несанкционированный доступ) и случайные. Преднамеренные угрозы часто называют несанкционированным доступом, атакой, нападением. Эти угрозы связаны с действиями человека. Пример преднамеренной наиболее серьезной угрозы, являющейся типичной для компьютерных систем - распространение компьютерных вирусов. Каждый день появляется до 300 новых вирусов. Вирусы не признают государственных границ, распространяясь по всему миру за считанные часы.

Как обеспечить информационную безопасность? Использование Интернета является безопасным, если

**выполняются три основных правила:**

1. Защитите свой компьютер

· Регулярно обновляйте операционную систему.

· Используйте антивирусную программу.

· Применяйте брандмауэр.

· Создавайте резервные копии важных файлов.

· Будьте осторожны при загрузке новых файлов.

2. Защитите себя в Интернете

· С осторожностью разглашайте личную информацию.

· Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила

· Закону необходимо подчиняться даже в Интернете.

· При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

**Памятка для учащихся «Интернет-этика»**

Если вы хотите стать ответственными пользователями выполняйте правила поведения в сети Интернет:

 Узнайте правила прежде, чем что-нибудь сказать или сделать. Некоторые чаты и форумы имеют специальные

правила, поясняющие, что Вы можете или не имеете права говорить или кто нарушает правила, знание правил

может избавить вас от ненужного дискомфорта.

 Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что вы говорите приемлемые вещи, которые не

приведут к разгоревшемуся конфликту.

 Единственное, в чем вы можете не сомневаться, — это в том, что всѐ, сказанное вами в Интернете, может

вернуться и неотступно преследовать вас.

 Не относитесь критически к другим, особенно новичкам, даже если они нарушают правила. Если вы должны

помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме.

Помните, что и вы когда-то были новичком.

 Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте

киберслухи, не разыгрывайте других, не рассылайте спам.

 Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей -либо

адрес электронной почты без разрешения владельца. Не используйте без разрешения чужой пароль.

 Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).

**Памятка для учащихся «Как не следует вести себя в сети»**

 Печатать ЗАГЛАВНЫМИ БУКВАМИ, что может рассматриваться как крик, провоцирующий спор или

конфликт.

 Размещать ложную информацию или грубые высказывания о другом человеке.

 Отправлять большие вложенные файлы, не спросив разрешения у получателя.

 Общаться к другим в чате по их настоящему имени.

 Рассылать электронную почту рекламного содержания людям, которых Вы не знаете.

 Отклоняться о темы разговора на форуме.

 Не дожидаться своей очереди или не следовать правилам чата или форума.

Памятка для учащихся по безопасному общению в чатах

В Интернете также широко распространены службы для мгновенного обмена сообщениями и онлайн-общения

(Windows Live Messenger, ICQ, IRC, чаты). Эти службы также могут таить в себе опасности при их использовании

детьми, поэтому придерживаться некоторых правил.

1. Не доверяйте никому вашу личную информацию.

2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.

3. Если вам неприятно находится в чате, покиньте его.

4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.

5. Будьте тактичны по отношению к другим людям в чате.