**ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ**

**ПО БЕЗОПАСНОСТИ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ**



**Уважаемые родители!**

            *Если ваши дети пользуются Интернетом, вы, без сомнения, беспокоитесь о том, как уберечь их от неприятностей, которые могут подстерегать в путешествии по этому океану информации. Значительное распространение материалов, предназначенных только для взрослых или неприемлемых для детей по какой – либо другой причине, может легко привести к неприятным последствиям. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. Кроме того, в Сети нередко встречаются люди, которые пытаются с помощью Интернета вступать в контакт с детьми, преследуя опасные для ребенка или противоправные цели.*

Всѐ большее количество детей получает возможность работать в Интернете. На сегодняшний день он предоставляет огромное количество неконтролируемой информации. Подростки ищут свое место в мире и пытаются обрести собственную независимость. В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта. Подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах.

Следует понимать, что подключаясь к сети Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать.

**Классификация интернет-угроз**
Во Всемирной паутине существует следующие виды опасности для юных пользователей:
•    суицид-сайты;
•    наркосайты (интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья»);
•    сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
•    сайты порнографической направленности;
•    сайты знакомств (виртуальное общение разрушает способность к реальному общению, у подростков теряются коммуникативные навыки);
•    сайты, пропагандирующих насилие и девиантные формы поведения;

•  интернет-аферисты (мошенники, онлайн-игроки и пр.), прививающие детям склонность к азартным играм, выманивающие у детей конфиденциальную информацию о родителях и уровне материальной обеспеченности семьи.
•    секты (виртуальный собеседник может повлиять на мировоззрение подростка).

•   угроза заражения вредоносным ПО. Ведь для распространения вредоносного ПО и

проникновения в компьютеры используется целый спектр методов. Среди таких методов

можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители

информации или скачанные из Интернет файлы. Например, программное обеспечение для

мгновенного обмена сообщениями сегодня являются простым способом распространения

вирусов, так как очень часто используются для прямой передачи файлов.

**Советы по безопасности**

* Ограничьте часы работы подростка в Интернет.
* Не забывайте беседовать с детьми об их друзьях в Интернет. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями.
* Родительский контроль может не только блокировать доступ к нежелательным для детей

сайтам, но ограничивать использование Интернет по времени суток, дням недели или

длительности сеанса. Существует множество программ и фильтров, которые помогут вам

контролировать открытие нежелательной информации и время, которое можно проводить

в Интернете. Вам помогут сделать это антивирусные программы и сами браузеры. Так например, Internet Explorer включает компонент Content Advisor, а Kaspersky Internet Security компонент «Родительский контроль», программа-фильтр «NetPolice», программа-фильтр «Интернет Цензор».

* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.
* Приучите себя знакомиться с сайтами, которые посещают подростки.
* Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей.
* Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
* Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между

полами.

* Необходимо прививать ребенку интерес к активным играм и физическим упражнениям, а также приобщать ребенка к домашним делам.
* Необходимо следить, чтобы игра на компьютере не подменяла реальное общение со

сверстниками, друзьями и близкими. Приглашать чаще друзей ребенка в дом.

Следует объяснить детям, что нужно критически относиться к полученным из Интернет материалам, ведь опубликовать информацию в Интернет может абсолютно любой человек.

* Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения с детьми.
* Постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка.
* В конце-концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.
* **Обратите внимание на подозрительные хеш-теги:** #f53 #f57 #f58 #d28 #морекитов #тихийдом #хочувигру #млечныйпуть #хочувигру #хочу\_в\_игру #ждуинструкцию #млечныйпуть, «Киты плывут вверх», «Разбуди меня в 4.20», «Рина», «Няпока», «50 дней до моего...», «домкитов», «150звёзд».

*В интерактивном мире дети могут быть так же беззащитны, как и в реальном. Поэтому важно сделать все возможное, чтобы защитить их.*

**Электронные ресурсы по теме «Безопасный Интернет»**

 http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html - личная

безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать

посещение Интернета для детей полностью безопасным.

 http://www.ifap.ru/library/book099.pdf - информация для родителей: памятки,

советы, рекомендации от компании Microsoft

 http://www.interneshka.net/children/index.phtml - советы детям, педагогам и

родителям, полезные ссылки.

 http://www.intemet-kontrol.ru/ - .Защита детей от вредной информации в сети

интернет.

 http://azbez.com/safety/intemet. - Азбука безопасности.

**Профилактика зависимости от компьютерных игр**

* Личный пример родителей, если вы разрешаете играть подростку некоторое время в день, то вы и сами не должны просиживать у компьютера больше времени.
* Список совместных дел, игр, развивающих уличных состязаний. Все должно быть спланировано, чтобы не оставалось свободной минуты.
* Использовать компьютер как награду, для эффективного воспитания, в качестве поощрения.
* Важно четко контролировать те игры, в которые играет подросток. Вы должны знать что это за игра и отслеживать любые отклонения в поведении подростка после того, как он поиграл в игру. Могут наблюдаться раздражительность, возбужденность, бессонница. Все это указывает на то, что либо было превышено время игры, либо игра не подходит подростку.
* Отдавать предпочтение развивающим играм и сайтам. Обсуждать с подростком те игры, в которые ему было бы по вашему мнение полезнее играть.
* Лечение «красотой» реальности: познать мир, музеи, театры, парки, путешествия, общение с интересными собеседниками.
* Установка специальных сетевых фильтров и специализированного ПО, позволяющего контролировать и лимитировать общение подростка с компьютером.

**Советы родителям**

* Резко отнимать или запрещать компьютерные игры подростку, который уже втянулся — нельзя. Делать это стоит последовательно, лучше подготовиться вместе с психологом.
* Можно пройти различные тесты в интернете, чтобы оценить компьютерную зависимость вашего ребенка и вас самих.
* Психологи склонны утверждать, что любая компьютерная зависимость носит временный характер. Но стоит ли ждать этого «насыщения».
* Не все игры плохо влияют на психику, некоторые способствуют развитию познавательных и моральных качеств. Тут решающее значение приобретает то, какие игры выбираются.
* Проанализируйте вашу собственную систему ценностей в отношении воспитания детей.
* Будьте честными. Все подростки весьма чувствительны ко лжи.
* Оценивайте уровень развития подростка.
* Избегайте длинных объяснений или бесед.
* Развивайте в своих детях следующие качества:

-уверенность, базирующуюся на собственном сознании самооценки;

-понимание достоинств и недостатков в себе самом и окружающих;

-интеллектуальную любознательность и готовность к исследовательскому риску;

-уважение к доброте, честности, дружелюбию, сопереживанию, душевному мужеству;

-привычку опираться на собственные силы и готовность нести ответственность за поступки;

-умение находить общий язык и радость в общении с людьми всех возрастов.

**Список терминов**
•    Аккаунт (англ.- account) - учетная запись, регистрационная запись.
•    Антивирус — пакет компьютерных программ, останавливающий проникновение вирусов на ваш компьютер, осматривающий содержимое компьютера на предмет наличия вирусов. Антивирус также лечит компьютер и удаляет вирусы.
•    Администраторы, модераторы сайта — специальные сотрудники сайта, которые следят за исполнением установленных на сайте правил.
•    Базы данных (БД) - специальное программное обеспечение, предназначенное для организации хранения и доступа к данным (информации). Используются при создании программных решений для автоматизации сайта.
•    Браузер — программа, позволяющая просматривать страницы в сети Интернет. Самые популярные Opera, Mozilla Firefox, Google Chrome, Internet Explorer.
•    Виртуальный собеседник (англ. chatterbot) — это компьютерная программа, которая создана для имитации речевого поведения человека при общении с одним или несколькими пользователями.
•    Всемирная паутина – это все веб-сайты Интернета
•    Домен (англ. domain), Доменный адрес (англ. domain name) - Область пространства иерархических имен сети Интернет, которая обозначается уникальным доменным именем, обслуживается набором серверов доменных имен (DNS)  Для каждого зарегистрированного доменного имени определен единственный Администратор. Это более практичный аналог IP-адреса. Доменная адресация возникла в Интернет для удобства пользователей: легче запомнить доменный адрес (например, www.microsoft.com), чем четыре числа IP-адреса. Доменный адрес может содержать латинские буквы, цифры, точки и некоторые другие знаки.
•    Доменный почтовый ящик, в который поступает почта, приходящая на любые возможные адреса домена (все-что-угодно@ваш-домен).
•    Интерне́т (англ. Internet, МФА: [ˈɪn.tə.net][1]) — всемирная система объединённых  компьютерных сетей для хранения и передачи информации.
•    Игнор — игнорирование, занесение в черный список.
•    Логин (от английского log in — «входить в») — это имя, которое вы выбираете для регистрации в системе или имя, которое система вам сама присваивает. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого.
•    Он-лайн игры —игровой процесс основан на взаимодействии с другими игроками и игровым миром, требующий постоянного подключения к Интернету.
•    Интернет-магазин (Электронный магазин";, "Сетевой магазин"; и т.д.),  - это интерактивный сайт, в котором: рекламируются товары и услуги, принимаются заказы на товары и услуги, посетителю, предлагаются различные варианта оплаты заказанных товаров и услуг, возможна их мгновенная оплата через Интернет.
•    Пароль — набор символов, известный только одному пользователю, необходимый для авторизации (для «входа») на сайте.
•    Персональная страница (персональный сайт) - совокупность Web-страниц, с содержанием, описывающим сферу интересов какого-либо человека (группы лиц), обычно созданная им самим.
•    Посетители - количество уникальных посетителей побывавших на страницах вашего ресурса.
•    Почтовый ящик - дисковое пространство на почтовом сервере, выделенное для хранения, отправки писем пользователя и т.д. (приходящих на его адрес и подлежащих отправке).
•    Псевдонимы (алиасы) - доменные имена, которые указывают на один и тот же web-проект.
•    Регистратор домена - юридическое лицо,оказывающее услуги по регистрации доменных имен и обеспечивающее передачу в Реестр.
Регистрация домена (доменного имени) - 1) Внесение имени и соответствующего ему IP-адреса в базу данных DNS-сервера. Регистрация в доменах верхнего уровня обычно платная. Регистрация доменов нижнего уровня обычно бесплатна и выполняется провайдером. 2) Закрепление определенного доменного имени за физическим или юридическим лицом, путем внесения соответствующей информации в регистрационную базу данных организации, координирующей распределение доменных имен.
•    Родительский контроль — это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение через Интернет. Цель таких средств — обеспечить безопасность ребенка в Интернете, и эти инструменты иногда называют семейными настройками и настройками семейной безопасности. Windows 7, Windows Vista, Xbox 360, Xbox Live, Bing и другие продукты Microsoft включают встроенные настройки семейной безопасности
•    Сайт (от англ. website: web — «паутина, сеть» и site — «место», буквально «место, сегмент, часть в сети») — совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединённых под одним адресом (доменным именем или IP-адресом).
•    Сервер (Web-сервер) -1) Компьютер или специализированное устройство в сети со специальным программным обеспечением, обеспечивающий доступ многих пользователей к расположенной на нем информации и функционирование любых необходимых сервисов Интернет: http (сайт), E-mail (электронная почта), конференции, ftp и т.п. Для размещения сайта в Интернет необходим веб-сервер с поддержкой как минимум сервиса http. 2) Сайт, крупный информационный ресурс Интернета.
•    Спам (англ. spam) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать.
•    Социальные сети — сайты в Интернете, на которых пользователи заводят свои странички для общения с друзьями. Одна из обычных черт социальных сетей — система «друзей» и «групп». Самые популярные русскоязычные: ВКонтакте, Одноклассники, Мой Мир, Мой Круг, ЖЖ и др.
•    Трафик (traffic) - поток (объем) информации, проходящей через канал связи, приходящийся на сайт. Может быть исходящим и входящим.
•    Тролли, троллинг — (от англ. trolling — «ловля на блесну») — размещение в Интернете провокационных сообщений с целью вызвать конфликты между субъектами, взаимные оскорбления.
•    Файлы, скачивание. Вся информация в компьютере сохраняется в виде файлов. Это могут быть текстовые файлы, музыкальные, видео, графические, мультимедийные и проч. Файлы можно создавать, копировать, пересылать (например, по электронной почте), выкладывать на сайт для скачивания, скачивать, то есть сохранять на свой компьютер.
•    Фишинг (от английского fish — «ловить рыбу»)- вид мошенничества в интернете, когда у пользователя пытаются узнать логины и пароли.
•    «Черный список сайтов» (black list), или как еще его называют "скам лист". представляет собой список сайтов, проектов или людей, которые проводят мошеннические операции в сети или не выполняют взятые на себя обязательства. В такие "черные списки" (black list), никогда не помешает заглянуть человеку, прежде чем начать с кем-то сотрудничать или пользоваться каким-либо сервисом..
•    Хостинг (hosting) - Услуга по предоставлению интернет-сервера и обеспечению его круглосуточной работоспособности. В большинстве случаев предоставляется виртуальный сервер (т.н. виртуальный хостинг), т.е. программное обеспечение, обеспечивающее работу необходимых Вам сервисов, но работающее на одной аппаратной платформе с другими подобными виртуальными серверами..
•    Хостинг-провайдер (hosting provider) - организация, профессионально занимающаяся предоставлением услуг Хостинга.
•    Электро́нная по́чта (англ. email, e-mail, от англ. electronic mail) — технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, вложение, ящик, доставка и другие), так и характерные особенности — простоту использования, достаточную надёжность и в то же время отсутствие гарантии доставки.