

# Правила безопасности в сети Интернет

Не рассказывать о себе и друзьях незнакомым людям в сети Интернет



Не встречаться со знакомыми из сети Интернет без предупреждения родителей



Не отправлять смс для получения доступа к информации без ведома взрослых

При регистрации придумывать сложный логин и пароль, не говорить их никому



подготовила: Трегубова К.В.  
Преподаватель КИК

# Рекомендации по медиабезопасности.

## Пункт 1:

Как можно **больше общайтесь** со своим ребенком, чтобы избежать возникновения Интернет- зависимости. Приобщайте ребенка к культуре и спорту, чтобы он не стремился заполнить свободное время компьютерными играми. Помните! Не существует детей, которых бы не интересовало ничего, кроме компьютера. Помните! «Ребенку для полного и гармоничного развития его личности необходимо расти в семейном окружении, в атмосфере счастья, любви и понимания».

## Пункт 2:

Существуют определенные механизмы контроля пользования Интернетом, например:

- размещать компьютер в общих комнатах, или быть рядом, когда дети пользуются Интернетом;
- совместное с ребенком пользование Интернетом;
- устанавливать специальные системы фильтрации данных, самостоятельно закрывающие доступ к определенной информации. Критерии фильтрации задает взрослый, что позволяет устанавливать определенное расписание пользования интернетом.



### **Пункт 3:**

Возможные Соцсети, в которых могут сидеть Ваши дети – это Вконтакте, Одноклассники, Facebook, Фотострана, MySpace. Также обратите внимание на ресурс «Мой Мир» на почтовом сайте Mail.

При общении в Сети у ребенка завязываются виртуальные отношения с новыми «знакомыми» и «друзьями», которые кажутся безобидными, поскольку Интернет-друг является как бы «ненастоящим». Предупредите своего ребенка, что под именем «нового друга» может скрываться мошенник или извращенец. Виртуальное хамство и розыгрыши часто заканчиваются киберпреследованием и киберунижением, доставляя объекту травли множество страданий.

### **Пункт 4:**

Научите детей не оставлять в публичном доступе личную информацию: контакты, фото, видео. Запомните принцип Интернет: «Все, что вы выложили, может быть использовано против вас». Желательно оставлять только электронные способы связи. Например, специально выделенный для подобного общения e-mail или номер icq.

### **Пункт 5:**

Станьте «другом» Вашего ребенка в Соцсетях. Это Вам поможет контролировать *виртуальные отношения* ребенка с новыми «знакомыми» и «друзьями». Объясните ему, что Другом должен быть только тот, кто хорошо известен.



### **Пункт 6:**

Контролируйте время, которое Ваш ребенок проводит в Интернете. Длительное времяпрепровождение в Сети может быть связано с «заигрываниями» со стороны педофилов, особенно в блогах, социальных сетях.

### **Пункт 7:**

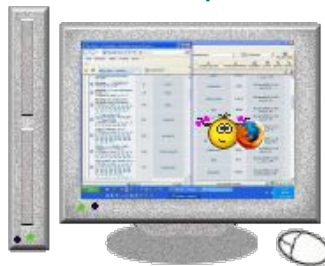
Несмотря на моральный аспект, периодически читайте электронную почту ребенка, если вы видите, что после прочтения почты Ваш ребенок расстроен, растерян, запуган.

### **Пункт 8:**

Главное средство защиты от мошенника, педофила – ребенок должен твердо усвоить, что *виртуальные знакомые должны оставаться виртуальными*. То есть – никаких встреч в реальном мире с теми друзьями, которых он обрел в Интернете. По крайней мере, без родительского присмотра.

### **Пункт 9:**

Средство защиты от хамства и оскорблений в Сети – игнорирование пользователя - ни в коем случае не поддаваться на провокации. Объясните ребенку, как пользоваться настройками приватности; как блокировать нежелательного «гостя»: добавить пользователя в «черный список», пожаловаться модератору сайта.



### **Пункт 10:**

Избежать неприятного опыта с покупками в Интернет-магазинах можно, придерживаясь нескольких правил: проверьте «черный список», читайте отзывы в Интернете. Вас должна насторожить слишком низкая цена товара, отсутствие фактического адреса и телефона продавца на сайте, стопроцентная предоплата.

### **Пункт 11:**

Для защиты компьютера от вирусов установите специальные для этого программы и периодически обновляйте их. Объясните ребенку, что нельзя сохранять на компьютере неизвестные файлы, переходить по ссылкам от незнакомцев, запускать неизвестные файлы с расширением \*.exe, так как большая вероятность, что эти файлы могут оказаться вирусом или трояном.



# ГЛОССАРИЙ

- **Медиаграмотность** – грамотное использование инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.
- **Медиаобразование** выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, способствует осознанному участию детей и подростков в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества.
- Согласно российскому законодательству, **информационная безопасность (медиабезопасность) детей** - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе - распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.
- **Интернет-зависимость (как вид нехимической зависимости)** – это навязчивая потребность в использовании Интернета, сопровождающаяся социальной дезадаптацией и выраженными психологическими симптомами. Патология проявляется в разрушении обычного образа жизни, смене жизненных ориентиров, проявлении депрессии, нарастании социальной изоляции. Происходит социальная дезадаптация, нарушаются значимые общественные связи.
- **Гэмблинг (игромания)** - патологическая склонность к **азартным играм**. Заключается в частых повторных эпизодах участия в азартных играх, которые доминируют в жизни человека и ведут к снижению социальных, профессиональных, материальных и семейных ценностей.
- **Виктимизация детей** – это процесс функционального воздействия насильственных отношений на ребенка, в результате чего ребенок превращается в жертву насилия, т.е. приобретает виктимные физические, психологические и социальные черты и признаки. Обычно «виктимизацию» определяют как действия, предпринятые одним человеком или несколькими людьми с намерением воздействовать, дискриминировать, нанести физический ущерб или причинить психологическую боль другому человеку.
- **Киберпреступления** – формы: от мошеннических махинаций и нарушений авторских прав до распространения детской порнографии, пропаганды педофилии, торговли детьми.
- 



- Киднеппинг (от [англ. kidnap](#) «похищать») — противоправные умышленные действия, направленные на тайный или открытый, либо с помощью [обмана](#), захват человека, изъятие его из естественной микросоциальной среды, перемещение с его места жительства с последующим удержанием помимо его воли в другом месте. Большей частью совершается из корыстных побуждений и имеет целью получение [выкупа](#) от родственников или близких к похищенному лиц, а также принуждение этих лиц к выполнению необходимых для похитителей действий.
- Кибербуллинг – нападение с целью нанесения психологического вреда, которое осуществляется через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на веб-сайтах, а также посредством мобильной связи.
- Виды кибербуллинга:
- Киберпреследование – скрытое отслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.
- Хеппислеппинг (Happy Slapping – счастливое хлопанье, радостное избиение) – видеоролики с записями реальных сцен насилия.
- Кибервандализм – хулиганство в Сети.
- Суицид, самоубийство, (от [лат. sui caedere](#) — убивать себя) — целенаправленное лишение себя жизни, как правило, добровольное, и самостоятельное (в некоторых случаях осуществляется с помощью других людей).
- Буллицид – доведение до самоубийства путем психологического насилия.
- Спам ([англ. spam](#)) — массовая [рассылка](#) коммерческой, политической и иной [рекламы](#) или иного вида сообщений (информации) лицам, не выразившим желания их получать.
- Троян - [вредоносная программа](#), распространяемая людьми. В отличие от [вирусов](#) и [червей](#), которые распространяются самопроизвольно.
- Фишинг - вид [интернет-мошенничества](#), целью которого является получение доступа к конфиденциальным данным пользователей — [логинам](#) и паролям. Это достигается путём проведения [массовых рассылок электронных писем](#) от имени популярных [брендов](#), а также личных сообщений внутри различных сервисов, например, от имени банков ([Ситибанк](#), [Альфа-банк](#)), сервисов ([Rambler](#), [Mail.ru](#)) или внутри [социальных сетей](#) ([Facebook](#), [Вконтакте](#), [Одноклассники.ru](#)). В письме часто содержится прямая ссылка на [сайт](#), внешне неотличимый от настоящего, либо на сайт с [редиректом](#). После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к [аккаунтам](#) и банковским счетам.

