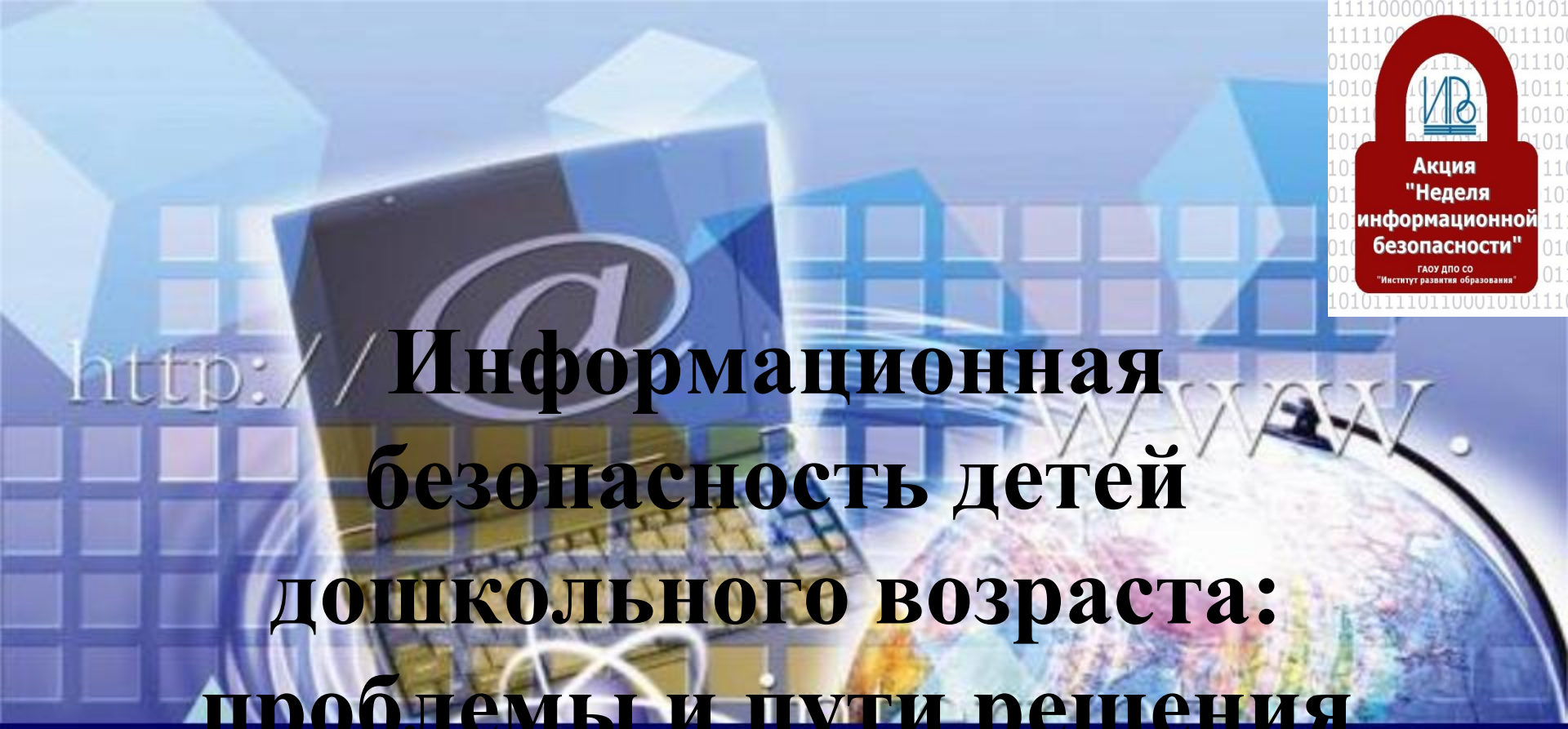


Акция "Неделя информационной безопасности"
ГАОУ ДПО СО "Институт развития образования"

Информационная безопасность детей дошкольного возраста: проблемы и пути решения

Составил:
Ст.воспитатель МБДОУ
«Детский сад № 29 «Теремок»

г. Реж
2017

Информационная безопасность детей

Информационная безопасность - то, о чем говорят чем дальше, тем больше. Сейчас, конечно, зрители уже стали привыкать к возрастной маркировке на экране и все реже путать цифры 12+ или 16+ с погодой. Но тем не менее вопросы еще остаются.

Что такое информационная безопасность ребёнка?

- это состояние защищённости детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому. Психическому, духовному, нравственному развитию

(Статья 2 ФЗ)

Какая информация является запрещённой для детей, то есть причиняет вред здоровью и развитию детей?

- побуждающая детей к совершению действий, представляющих угрозу жизни и (или) здоровью людей, а так же к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготовляемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

(Статья 5 ФЗ)

На какие группы делится информационная продукция?

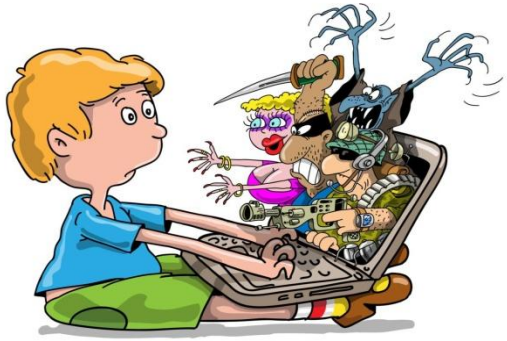
- информационная продукция для детей, не достигших возраста шести лет;
- информационная продукция для детей, достигших возраста шести лет;
- информационная продукция для детей, достигших возраста двенадцати лет;
- информационная продукция для детей, достигших возраста шестнадцати лет;
- информационная продукция, запрещённая для детей.

(статья 6 ФЗ)

Как определить степень опасности информации?

- производитель, распространитель информационной продукции размещают знак и (или) текстовое предупреждение об ограничении её распространения перед началом трансляции телепрограммы, телепередачи, демонстрации фильма при кино- и видео-обслуживании;
- знак информационной продукции демонстрируется в публикуемых программах теле- и радиопередач. В углу кадра, за исключением демонстрации фильма, осуществляемой в кинозале;
- размер знака информационной продукции должен составлять не менее 5% площади экрана, афиши или иного объявления о проведении соответствующего зрелищного мероприятия. Объявления о кино- или видео-показе, а также входного билета, приглашения.

(Статья 12 ФЗ)



ОБРАТИТЕ ВНИМАНИЕ:

– доступ детей к информации, распространяемой посредством информационно-телекоммуникационных сетей (в том числе сети Интернет), предоставляется операторами связи, при условии применения ими средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию (Статья 14 ФЗ)

– содержание и художественное оформление печатных изданий, полиграфической продукции (в том числе тетрадей, дневников, обложек для книг, закладок для книг), аудиовизуальной продукции, иной информационной продукции, используемой в образовательном процессе. Должны соответствовать требованиям настоящего Федерального закона (Статья 15 ФЗ)

– первая и последняя полосы газеты, обложка экземпляра печатной продукции, запрещённой для детей, при распространении для неопределённого круга лиц в местах, доступных для детей, не должны содержать информацию, причиняющую вред здоровью и (или) развитию детей;

– информационная продукция, запрещённая для детей, в виде печатной продукции допускается к распространению в местах, доступных для детей, только в запечатанных упаковках;

– информационная продукция, запрещённая для детей, не допускается к распространению в предназначенных для детей образовательных организациях, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем 100 метров от границ территорий указанных организаций. (Статья 16 ФЗ)

Влияние Интернет

В дошкольном возрасте

доля детей пользователей интернета значительно ниже, чем старших, и составляет в среднем 26% (дети 5-9 лет). Наиболее доступным местом пользования интернета является их дом. Девочки значительно реже, чем мальчики пользуются услугами интернета. Мальчики в большей степени, чем девочки подвергаются информационной опасности, так как чаще пользуются услугами интернета, где не контролируются взрослыми.

Влияние аудио-, идеоинформации

64-70 % детей в свободное время смотрят телевизор, около 50% - играют в компьютерные игры, 20% - смотрят видео, фильмы на дисках, он-лайн. Чем старше возраст детей, тем больше дети играют в игры с элементами насилия, ценят развлекательный характер передач и меньше – нравственные характеристики своих любимых героев. Уровень просмотра развлекательных передач увеличивается, также растет увлеченность компьютерными играми с насилием и наоборот уменьшается доля детей, которые любят своих русских мультипликационных персонажей за нравственные качества .

Чем чаще родители интересуются жизнью ребенка, обсуждают с детьми их интересы, контролируют и говорят о вредном воздействии информации:

- тем меньше дети смотрят телевизор в ночное время, видео и остаются за компьютером ;
- сокращается длительность компьютерных игр у детей;
- меньше интересуются эротикой в Интернете;
- дети понимают, что вредно много смотреть телевизор, видео;
- сокращается число детей, которые положительно относятся к насилию на экране;
- меньше интереса к распространению видеосъемок с насилием;
- меньше интереса к жестоким компьютерным играм.

Рекомендации для родителей

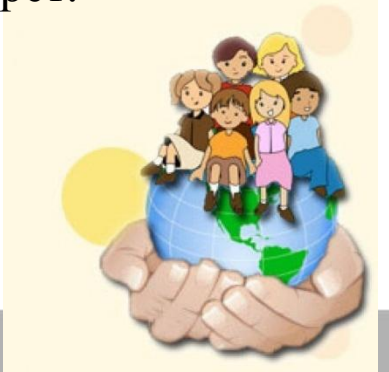
•Всю работу по противодействию негативной информации необходимо начинать как можно с более младшего возраста ребенка.

• Чем больше родитель уделяет внимания своему ребенку, тем меньше риск негативного влияния отрицательной информации, которую ребенок получает через телевидение, интернет, музыку, которую он слушает и др. источники.

• Ребенок, имеющий какие-либо увлечения, который ходит в различные секции, кружки, имеет меньше вредных привычек, ведет более здоровый образ жизни и он меньше подвержен воздействию негативной информации. Поэтому постарайтесь организовать досуг ребенка.

•Обезопасить ребенка от негативного влияния СМИ, Интернет, аудио - и видеопродукции очень сложно в одиночку, работа должна проходить комплексно, с участием различных сторон, окружающих ребенка. Не стесняйтесь обращаться за помощью к психологу, к социальному педагогу, администрации детского сада и другим. Но детскому саду будет легче, если родители сами будут проявлять инициативу.

•Очень большое влияние на психологическое состояние ребенка оказывает семейное окружение. Почаще разговаривайте с ребенком, постарайтесь узнавать его проблемы, давайте ему советы как поступить в той или иной ситуации. Ни в коем случае не порицайте ребенка, если он открыл вам свой какой-то негативный поступок. Этим Вы можете его оттолкнуть, и в следующий раз он не расскажет вам свой секрет.



Рекомендации по профилактике негативного воздействия современных информационных технологий на развитие ребенка:

- Регулируйте просмотр детьми телевидения
- Заблокируйте каналы, несущие негативную информацию
- Прячьте модемы, когда уходите по делам
- Ежедневно просматривайте «историю» в интернете
- Не допускайте сквернословия
- Проверьте круг общения ребенка

Какие же угрозы содержит Интернет?

Советы по обеспечению безопасности ребенка в Интернет

Данные рекомендации были составлены на основе информации, размещенной на сайтах различных IT-компаний и образовательных сайтах. Также были включены рекомендации школьных учителей информатики

Инфографика по вопросам безопасности в Интернете


bezpeka.kyivstar.ua
А ВЫ ЗНАЕТЕ, КАК ПОВЫСИТЬ УРОВЕНЬ БЕЗОПАСНОСТИ РЕБЕНКА В ИНТЕРНЕТЕ?
23:59
***
Поставьте пароли для разных пользователей
кеш
Проверьте и очистите историю браузера
Установите надежный антивирус
Установите программу родительского контроля
Безопасность ребенка зависит от ваших знаний.
Расскажите детям о безопасности в Интернете!


bezpeka.kyivstar.ua
14% детей время от времени присылают платные SMS
17% детей готовы предоставить информацию о себе и своей семье
22% детей время от времени попадают на сайты «для взрослых»
28% детей готовы без колебаний прислать свою фотографию незнакомцам
А чем ваш ребенок занимается в Интернете?

Десять правил безопасности для детей в Интернете*

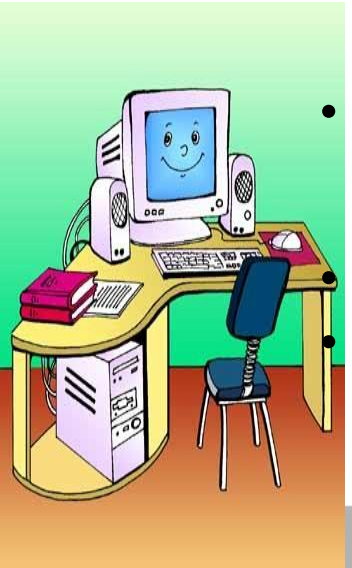
1. Посещайте сеть вместе с детьми, поощряйте их делиться опытом использования Интернета
2. Научите детей доверять интуиции - если их в Интернете что-либо беспокоит, пусть сообщают вам
3. Помогите ребенку зарегистрироваться в программах, требующих регистрационного имени и заполнения форм, не используя личной информации (имя ребенка, адрес электронной почты, номер телефона, домашний адрес). Для этого можно завести специальный адрес электронной почты
4. Настаивайте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки
5. Объясните детям, что в Интернете и реальной жизни разница между правильным и неправильным одинакова

6. Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают
7. Скажите детям, что далеко не все, что они читают или видят в Интернете, - правда, приучите их спрашивать вас, если они не уверены
8. Контролируйте действия детей с помощью современных программ, которые отфильтруют вредное содержимое, помогут выяснить, какие сайты посещает ребенок и что он там делает
9. Настаивайте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ - кража
10. Научите детей уважать других, убедитесь, что они знают о том, что правила хорошего тона действуют везде - даже в виртуальном мире

* Рекомендации Министерства образования Республики Беларусь

В помощь Родителям

- Kaspersky Internet Security 2014
- Kaspersky CRYSTAL
- KinderGate Родительский Контроль - программный продукт, предназначенный для домашних пользователей и позволяющий контролировать использование сети Интернет несовершеннолетними детьми.
- Outpost Security Suite - комплексная защита сетевых угроз, включающая в себя антивирус, брандмауэр, антиспам и т.д.
- Rejector - простой инструмент для родительского контроля и не только. Бесплатен.
- SkyDNS - бесплатный интернет-сервис на основе службы DNS для блокировки доступа к опасным, вредоносным сайтам и сайтам не подходящим для просмотра несовершеннолетними.
- Time Boss Родительский Контроль - простая программа для родительского контроля, ограничивающая влияние компьютера на ребенка.



Детский браузер Гогуль

- Интернет Цензор - бесплатный интернет-фильтр, обеспечивающий блокировку потенциально нежелательных сайтов и ресурсов сети интернет

Азбука Интернет - опасностей

А

Агрессивные сайты - пропагандируют ксенофобию, терроризм, и аутоагрессивной направленности (суицид, on-line суицид, суицидальные договоры, информационные ресурсы о применении средств для суицида с описанием дозировки и степени их летальности);

Аддиктивный фанатизм - религиозный (сектантство), политический (партийный), национальный, спортивный, музыкальный и т. д.)

В

Веб-серфинг навязчивый - блуждания во Всемирной Сети информационный поиск в удалённых базах данных (посещение новостных сайтов, чтение информации на форумах, блогах, просмотр и прослушивание информации в различных форматах). На каждом сайте обязательно есть ссылки, ведущие на другие ресурсы, а на сайтах, на которые мы попадаем, также имеются гиперссылки и т. д. Веб-сёрфинг затягивает пользователя, отвлекая от учёбы и других дел, поскольку, попав в информационный поток, утрачивается ощущение времени.

Вирус компьютерный — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Вишинг – технология Интернет-мошенничества с целью кражи конфиденциальной информации с помощью Интернет-телефонии и автонабирателей. Абоненту предлагается перезвонить по городскому номеру, где звучит сообщение о необходимости сообщения информации личного пользования

Г

Гемблинг он-лайн - гиперувлечённость индивидуальными и/или сетевыми онлайн-играми

Геджит-аддикция - пристрастие к обладанию конкретным мобильным прибором, устройством, имеющим выход в Интернет: сотовым телефоном, смартфоном, коммуникатором, мини-компьютером, КПК и зависимость от его использования.

Гриферы - Интернет-хулиганы мешают игрокам (в особенности начинающим) спокойно играть, всячески вредя их персонажам, блокируя функции игры и создавая невыносимые условия для Сетевой команды в целом и, подвергая травле и преследованиям, отдельных игроков.

К

Кибербуллинг – одна из форм преследования детей и подростков с использованием цифровых технологий. Иногда для этого создаются целые сайты, на которых размещаются компрометирующие преследуемого ребёнка материалы. Если Ваш ребёнок стал внезапно получать многочисленные электронные сообщения агрессивного содержания от неизвестных людей, если его начали преследовать и запугивать, значит, он подвергся кибербуллингу. Сложность фильтрации подобных сообщений, невозможность контроля, регулярность атак (может достигать 24 часов в сутки) и анонимность преследователей делают запугивание особенно сильным, нанося психологическую травму ребёнку.

Кибергруминг. Обретение доверия ребёнка с целью использования его в сексуальных целях. Преступники хорошо разбираются в психологии детей и подростков, прекрасно ориентируются в их увлечениях и интересах. Устанавливая контакты в социальных сетях или на форумах с детьми, находящимися в подавленном психологическом состоянии, они проявляют сочувствие, предлагают поддержку, обсуждают с ребёнком беспокоящие его вопросы, постепенно смещая их в сексуальную плоскость, а затем предлагают перевести отношения в реалых.

Кибероniомания – не контролируемые покупки в Интернет-магазинах, без необходимости их приобретения и учета финансовых возможностей, навязчивое участие в онлайн-аукционах.

Киберкомуникативная зависимость- общение в чатах, участие в телеконференциях).

Киберсексуальная зависимость - непреодолимое влечение к обсуждению сексуальных тем на эротических чатах и телеконференциях, посещению порнографических сайтов и занятий киберсексом

Л

Лудомания он-лайн - гиперувлечённость азартными играми в виртуальных казино

С

Спам (англ. spam) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать.

Секстинг – новый вид развлечений: фотографирование себя в обнажённом виде на камеру телефона с последующей пересылкой снимков друзьям через MMS-сообщения.

Ф

Фишинг – это технология *Интернет-мошенничества с целью кражи конфиденциальной информации (имён и паролей доступа, данных кредитных карт и Интернет-кошельков и т. д.). Почтовый фишинг – получение письма с требованием сообщения каких-либо личных данных. Онлайн-фишинг – копирование дизайна и доменных имён сайтов и Интернет-магазинов с целью обмана покупателя.* **Комбинированный фишинг** – создание поддельного сайта, где жертва самостоятельно заполняя формы, сообщает мошенникам конфиденциальные сведения или использования программ-шпионов key-loggers, фиксирующих информацию, введённую с клавиатуры и пересылающих её на адреса мошенников

Фарминг – перенаправление трафика с загружаемого веб-узла на фальшивый клон сайта, который первоначально хотел посетить пользователь. Заражение происходит при открытии почтового сообщения или посещения веб-сервера. При наборе адреса банка происходит активация исполнимого файла с последующим перенаправлением пользователя на фальшивый веб узел.

Х

Хакерство как пристрастие работы за компьютером - борьба за свободное распространение и доступность информации, самоутверждение, ощущение собственной силы, увлечённость процессом, недостаток познавательной активности при обучении, принадлежность к «хакерской культуре», зависимое поведение.

Ч

Червь сетевой — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

Поддержка центров информационной безопасности, которые помогут настроить и мобильные устройства и компьютер, прийти на помощь по организации безопасного Интернета дома.

Центр детской безопасности в информационном обществе «Не Допусти!» (Центр безопасного Интернета в России) – комплексный проект по защите детей в современном мире с использованием передовых технологий информационного общества

Билайн реализует программу «Безопасный Интернет», которая сочетает информационный и технологический подходы защиты мобильных Телефонов.

МТС реализует различные инструменты безопасности при работе в сети Интернет. На Портале Безопасности МТС размещена актуальная информация о киберугрозах и мошенничестве в глобальной Сети и эффективных способах их предотвращения. Для абонентов разработаны различные услуги информационной безопасности, включая антивирусные программы, инструменты защиты от нежелательных звонков и смс-сообщений и механизмы защиты детей.

Мегафон - российский оператор мобильной связи - проводит в российских общеобразовательных школах уроки «Мобильной грамотности». В рамках занятий специалисты компании рассказывают школьникам о мобильном этикете и потенциальных угрозах.

Факультет психологии Московского государственного университета имени М.В. Ломоносова является одним из ведущих психологический центров. Специалисты факультета совместно с экспертами Фонда Развития Интернет поддерживают линию помощи “Дети Онлайн”, в рамках которой консультируют детей и взрослых по вопросам безопасного использования Интернета.

Фонд Развития Интернет проводит специальные исследования, которые посвящены изучению психологии цифрового поколения России. Особое внимание уделяется проблемам безопасности детей и подростков в Интернете.

Национальный Детский Фонд разрабатывает и реализует актуальные социальные проекты, направленные на воспитание, развитие и поддержку различных детских аудиторий. Национальный детский фонд является социальным партнером проекта «Смешарики» – одного из популярных российских мультипликационных брендов.

Факторы зависимости

1. Сильное влечение к ПК.
2. Нарушение способности контроля самого себя.
3. Смена физиологического состояния.
4. Желание увеличить время.
5. Отказ от других альтернатив в пользу ПК.
6. Невозможность прекратить занятия.

«Постарайтесь шагать рядом с ребёнком по дороге жизни – и ему не нужно будет удирать в виртуальный мир.»