***«Безопасность детей в информационном пространстве"***

***Законы***

 1. [Закон РФ "О защите детей от информации, причиняющей вред их здоровью и развитию"](https://infourok.ru/go.html?href=https%3A%2F%2Fgymn272.spb.ru%2Fdoc%2Finfarm%2Fsafety_zakon.pdf) от 21 декабря 2010 года

2.Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»

3. Классификатор информации, распространение которой запрещено в соответствии с законодательством Российской Федерации

С введением новых образовательных стандартов, современная школа отходит от привычных моделей обучения, ребенок теперь сам должен научиться добывать информацию. И в данном случае Интернет становится просто незаменимым орудием для образования. Однако с другой стороны, психологи и врачи говорят о появлении новой болезни – компьютерной зависимости.

По данным Mediascope, аудитория в октябре 2016 — марте 2017 года достигла 87 млн человек, что составило 71% от всего населения страны. За год российская интернет-аудитория по данным Mediascope увеличилась на 2%. При этом 66 млн человек, или 54% от населения РФ, пользуются интернетом хотя бы 1 раз в месяц через мобильные устройства, а 20 млн человек — 16% от населения страны — только с мобильных устройств.

Российские дети проводят в Интернете значительнобольше времени, чем представители молодого поколения во многих странах Европы и США. Такие данные «Лаборатория Касперского» получила в результате исследования\* «Растим детей в эпоху Интернета», которое было проведено в 2016 году. В опросе приняли участие 3780 семей с детьми от 8 до 16 лет (один взрослый и один ребенок из семьи) в России, США, Великобритании, Германии, Франции, Испании, Италии. В России было опрошено 540 семей.

Так, почти постоянно в Сети находятся более половины всех опрошенных несовершеннолетних пользователей в России (56%), что ниже показателей других стран.

Пользователи младшей возрастной группы (8-10-лет) не так сильно привязаны к Интернету: почти постоянно присутствуют в Сети менее половины российских малышей (40%).

Чем старше дети, тем больше времени они проводят в Интернете. Так, 68% российских подростков (14-16 лет) почти постоянно находятся онлайн. В большинстве исследуемых стран этот показатель ниже.

Дети используют Интернет для общения с друзьями и семьей, развлечений и получения информации. Так, 56% несовершеннолетних пользователей в России говорят, что не могут обойтись без него. И даже по этому показателю Россия обгоняет остальных участников опроса.

«Российские дети пришли в Интернет позже американских и европейских, но по интенсивности и увлеченности Сетью опережают своих ровесников во многих странах, — соглашается с результатами исследования «Лаборатории Касперского» Галина Владимировна Солдатова, директор Фонда Развития Интернет, доктор психологических наук, член-корреспондент РАО. — Сравнение результатов трех исследований Фонда Развития Интернет показывает, что уровень ежедневного использования Интернета детьми практически уже достиг своего максимума: в 2010 году каждый день выходили в сеть 82% подростков, а в 2016-м — уже 92%. При этом около 80% детей проводят в Сети в среднем три часа в день, а каждый седьмой – 8 часов и более. Причем, по данным ВЦИОМ (Всероссийский центр изучения общественного мнения), количество взрослых по показателю ежедневного использования Интернета в 2016 году составляет всего 53%. Эта разница — лишь один из показателей существенного разрыва между поколениями. Именно низкая цифровая грамотность родителей лежит в основе их беспечного отношения к интернет-активностям юного поколения. Взрослым нельзя оставлять детей в одиночку в Сети, а стоит вместе осваивать новый цифровой образ жизни. Это позволит не допускать ненужной в этом возрасте чрезмерной увлеченности Интернетом в ущерб учебе, досугу, спорту, прогулкам и живому общению».

**Опасности, с которыми дети могут столкнуться в Сети**

Доступ к неподходящей информации:

* сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности,
* сайты, размещающие изображения порнографического или иного неприемлемого сексуального контента, к которым дети могут легко получить доступ,
* сайты с рекламой табака и алкоголя;
* сайты, посвященные изготовлению взрывчатых веществ;
* сайты, пропагандирующие наркотики;
* сайты, пропагандирующие насилие и нетерпимость;
* сайты, публикующие дезинформацию;
* сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;
* сайты, позволяющие детям принимать участие в азартных играх онлайн;
* сайты, на которых могут собирать и продавать частную информацию о Ваших детях и Вашей семье.

Проблема защиты детей в Сети находит самый широкий резонанс и это не случайно. Обратимся к статистике:

- 88% четырёхлетних детей выходят в сеть вместе с родителями

- около 50% детей выходят в Сеть без контроля взрослых.

- 19% детей иногда посещают порносайты, еще 9% делают это регулярно.

- 38% детей, просматривают страницы о насилии

- 16% детей просматривают страницы с расистским содержимым

- 25% пятилетних детей активно используют Интернет.

- 14,5% детей назначали встречи с незнакомцами через Интернет,

- 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем–то встречаются;

- примерно треть вредоносного ПО, существующего в настоящее время, создана детьми до 11 лет. Дети начинают интересоваться разработкой кодов, столкнувшись с проблемами во время игр онлайн.

И это число постоянно растет. А ведь не исключено, что и наши обучающиеся могут оказаться в Интернет - зависимости, которая на сегодняшний день приравнивается к болезни, наравне с алкогольной и наркотической зависимостью.

Можно ли заболеть Интернетом? Ведь Интернет – это не вирус, попавший в кровь? Конечно, можно.

**Опасные молодежные течения**.

Подросший ребенок будет обращаться в сфере его возрастной группы, которая часто так и называется – сложный возраст. Сайты всевозможных фанатов, социальные сети, объединяющие людей с неуравновешенной психикой в разного рода группы депрессивных течений и группы суицидальной направленности, толкают порой детей к суициду (буллициду) – все это нужно заблокировать для ребенка. Также опасение вызывает тот факт, что ряд экстремистских групп используют Интернет для распространения своих идей, пропаганды насилия в отношении национальных меньшинств и иммигрантов. Часто в подростковом возрасте возникает повышенный интерес к своей формирующейся личности. Подростки много времени уделяют своей внешности, пытаются обнаружить у себя часто не существующие косметические дефекты, самостоятельно исправить их. Подписываясь на такие сообщества или группы в социальных сетях как «0 калорий», «Типичная анорексичка» и т.д. ребенок может заинтересоваться и применить на себе опасные диеты и тем самым испортить здоровье.

**Виды информации, причиняющей** **вред здоровью и (или) развитию детей**

К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению **вреда своему здоровью, самоубийству;**

2) способная вызвать у детей желание употребить **наркотические средства,** психотропные и (или) одурманивающие вещества, **табачные изделия, алкогольную и спиртосодержащую продукцию**, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) 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;

4) **отрицающая семейные ценности** и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая **противоправное поведение**;

6) содержащая **нецензурную брань**;

7) содержащая информацию **порнографического характера**.

Общение по Интернету не проходит даром, ни для взрослых, ни для детей. В Сети человек чувствует себя спокойнее, здесь думать о внешности и всем остальном не надо, поэтому коммуникативные и другие умения не имеют значения. Справедливо отмечают, что для некоторых это место, где можно отдохнуть и сбежать от реальной жизни, можно сказать все, что вздумается, не заботясь об ответственности.

В Интернете также есть игры, приложения, которые получили широкое распространение. Например, компьютерная игра «Моя любимая ферма». Вроде бы ничего особенного: ни мутантов, ни крови, ни насилия. Но как она затягивает! Дети, прибегая домой, буквально бросаются за компьютер, чтобы полить огород или поухаживать за животными, зачастую забыв про обед для себя, уроки или помощь по дому. Такие игры привлекают своей массовостью, одновременно в игре может находиться несколько сотен участников, знакомых и незнакомых. Кроме того, играя в компьютерные игры, трудно проиграть состояние, однако очень просто и быстро «проиграть» свой разум. Интернет, к которому вырабатывается нездоровое пристрастие, как, например, в случае с компьютерными играми, поглощает все время и все мысли человека.

Наибольший урон учебе, дружеским и семейным отношениям наносит увеличение времени, проведенного в он-лайн, и, как следствие, оттеснение реальной жизни на второй план. У современного человека есть много возможностей приятно провести время, но он ищет все новые и новые. Сеть в этом ряду занимает свое особое место. Сеть не вызывает физиологической зависимости, но вызывает психологическую, особенно у детей и подростков.

Проблемой игромании в России врачи занимаются последние десятилетие. Но с каждым годом она становится острее. В основном врачи работают с подростками от 12 лет, но среди пяти - шестилетних детей уже есть такие, которые мыслят компьютерными категориями. Среди пациентов в основном мальчики. Агрессивность и инстинкт охотника, свойственные мужской натуре, разрастаются на благодатной почве компьютерных игр. А еще игра - это сильные ощущения. Поэтому именно дети, которым в жизни не достает позитивных эмоций, общения с родителями, чаще всего становятся жертвами компьютера. Виртуальный мир дает искаженное представление о мире реальном. И тем самым играет с ним злые шутки. Так, игрок усваивает, что можно прыгнуть с большой высоты и не разбиться. Можно войти в огонь и не сгореть. И мчащаяся на полном ходу машина в виртуальном мире не опасна. А в итоге ребенок привыкает не особо реагировать на такую же машину в мире реальном, что влечет за собой последствия, связанные с летальным исходом.

Одна из новейших Интернет - угроз – так называемы «киберсуицид» или согласованные самоубийства. По Интернету подростки и молодые люди договариваются о совместном самоубийстве. В Сети довольно много сайтов, где подробно описаны и проиллюстрированы способы свести счеты с жизнью. Подростки, которых интересует подобный опыт, говорят о том, что вместе уйти из жизни проще, чем поодиночке, в сети находят поддержку своим суицидальным наклонностям, вступая в контакт с единомышленниками, которые как и они сами, думают о самоубийстве.

В социальных сетях через программы мгновенного обмена сообщений ребенок может стать жертвой педофилов. Преступники представляются сверстниками и выманивают у детей адрес или маршрут следования из школы. Пострадать ребенок может и от поведения других детей. В России набирает обороты киберхулиганство: подростки снимают на видео сцены унижения или избиения сверстника и выкладывают этот ролик в Интернет. Так об этом факте узнают десятки, а то и сотни ровесников жертвы, и начинается его настоящая травля.

Еще одной из проблем, подстерегающих в сети Интернет, является пропаганда жестокости, экстремизма и нетерпимости. Когда информация экстремистского содержания попадает в руки взрослого, знающего разницу между добром и злом, в руки полностью сформировавшейся личности это, в большинстве случаев, не принесет серьезного вреда, и совершенно другое дело, когда сайты экстремистского, националистического содержания попадают на глаза детей, личность которых еще только проходит этап становления. Что произойдет с психикой ребенка, например, после просмотра ролика казни людей боевиками ИГИЛ, которые были доступны в сети в течение 2-х дней?

Ни для кого не секрет, что широкие возможности Интернета уже давно и активно используют экстремистские и террористические организации по всему миру. Существенную проблему сетевая деятельность террористов представляет и для России. Так, за последнее время МВД России выявило в Сети 148 сайтов террористической и экстремисткой направленности: в российском сегменте Всемирной паутины – более 70 сайтов. Очень известны случаи, когда школьницы, девочки – подростки общаются с боевиками, представителями ИГИЛ через социальные сети. Так, 16-летняя жительница Москвы, в данный момент осужденная, 2 года общалась по сети с возлюбленным из Дагестана. При этом девушка не вела себя замкнуто в школе, училась на 4 и 5. Когда молодой человек приехал к ней в Москву, она за сутки успела принять ислам и совершить бракосочетание по мусульманскому обряду. В тот же день девушка вместе с молодым человеком уехала в Дагестан. Когда их задержали, было выяснено, что пара собиралась уехать в Сирию и вступить в ряды Исламского государства.

Это были психологические аспекты опасности интернет-пространства, теперь информационная сторона.

• **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, флеш-карты и диски, 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. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов. Не верьте письмам присланным от лица администрации каких- либо сервисов в Интернете с просьбой выслать им пароль вследствие его утери или еще по какой причине (им проще поменять его и выслать вам новый);

• Ни в коем случае **не запускайте файлы** присланные вам с помощью почты и мессенджеров, социальных сетей без предварительной проверки на вирусы, например с помощью антивируса с последним обновлением). Стоит очень хорошо подумать, прежде чем запускать что-то пришедшее "оттуда", вот один из самых примитивных способов: В социальной сети методом социальной инженерии, "хакер" прикидывается девчонкой и вступает с жертвой в разговор, заинтресовав разговором, он под каким - либо предлогом устроит обмен фотографиями, только жертва ему пошлет нормальную фотографию, а "хакер" пошлет обыкновенный троян со стандартной иконкой от jpg файлов и кучей пробелов, но его последние 3 символа все таки будут запускными. Как только жертва подаст команду, троян выполнит свое черное дело, заразив систему и распаковав из своего тела небольшую фотографию. Жертва скорее всего не сразу догадается, о том что произошло, ну а последствия могут быть очень серьезными...

• **Доступ к нежелательному содержимому**. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики, порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, в то числе и реклама.

**Это надо знать каждому!**

1. Многие сайты созданы специально для получения данных о посещающих их людях…. Стоит задумываться, какие сайты могут заслуживать вашего доверия, а какие нет, потому что веб сервер, используя множественные ошибки операционной системы от Microsoft, может делать с вашим компьютером практически все, что угодно. Без проблем может выкачать у вас любой файл, и вы даже об этом можете так никогда и не узнать, что конфиденциально важная информация стала достоянием общественности.

2. Ни в коем случае не нужно забывать о таких элементарных вещах как обычный антивирус, что - то вроде Dr.Web, AVP и т.д. Имея последние обновления антивирусов можно предупредить заражение компьютера каким-либо трояном или вирусом.

4. Самое опасное, что может ожидать вас в Интернете, это конечно обыкновенная почта, иногда несущая в себе "смерть". Уже достаточно давно, в компьютерном мире, существуют вирусы и трояны, которые распространяются с огромной скоростью, посредством интернета и электронной почты. Последние из них, например I LoveYou, за считанные дни вывел из строя десятки тысяч компьютеров. Вирус считывал вашу адресную книгу и отправлял от вашего имени письмо содержащее в себе некоторый текст и скрипт который оседал в вашей системе, используя ошибки в почтовом клиенте Outlook Express базового пакета Microsoft автоматически запускает файлы, которые идут с письмом, не надо иметь много фантазии, чтобы понять, чем это грозит.

5. Не стоит забывать о снифферах, с помощью которых ваши пароли могут стать достоянием общественности. Чтобы защитить конфиденциальную информации нужно использовать программы шифрования трафика, такие как PGPNet, которая входит в комплект программы PGP Freeware.

**Как обезопасить себя и свой компьютер?**

1. Перво-наперво, как и со всеми операционными системами нужно установить самый последний update выпущенный производителем ОС (так называемые service pack и хот фиксы к нему

2. Выключить все неиспользуемые сервисы (особенно это касается Internet Services, таких как FTP, WWW, сервиса удаленного управления реестром и др.).

3. Установите файловую систему NTFS, которая позволяет разграничить доступ к каждому файлу, находящемуся у вас на диске.

4. Удалить все упоминание о пользователе Guest(Гость) или группе Everyone в установках пермишенс на корневую и системную директории, запретить локальный и сетевой вход, для всех пользователей оставив только используемых на данной машине, и желательно запретить доступ по сети для пользователя Администратор.

5. Не использовать для повседневной работы пользователя Администратор, проводить аудит, если есть возможность, всех действий Администратора и периодически проверять их на наличие несанкционированных.

6. Установить фильтрацию TCP/IP пакетов оставив открытыми только используемые порты (например, для того, чтоб работал www сервер достаточно оставить открытым только 80 порт).

**Вывод:** Интернет прочно вошел в нашу жизнь, и вопросы психологической, нравственной и антитеррористической безопасности важны сегодня, как никогда. В России около 8 миллионов 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.