

*МКУ «Управление образования
Партизанского
муниципального
района*

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ
КАК ОДНА ИЗ ПРИОРИТЕТНЫХ ЗАДАЧ
ГОСУДАРСТВЕННОЙ ПОЛИТИКИ**

Информационная безопасность детей

признана одним из национальных приоритетов современной государственной политики России.

Это четко обозначено в Национальной стратегии действий в интересах детей и Концепции информационной безопасности детей от 2 декабря 2015 года.



НОРМАТИВНАЯ ПРАВОВАЯ БАЗА ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ



**ФЕДЕРАЛЬНОЕ
ЗАКОНОДАТЕЛЬСТВО**

ФЕДЕРАЛЬНЫЙ ЗАКОН №124-ФЗ ОТ 24.07.1998 ГОДА
**«ОБ ОСНОВНЫХ ГАРАНТИЯХ ПРАВ РЕБЁНКА
В РОССИЙСКОЙ ФЕДЕРАЦИИ»**

ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ №2124-1 ОТ 27.12.1991
«О СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ»

ФЕДЕРАЛЬНЫЙ ЗАКОН №38-ФЗ ОТ 13.03.2006 ГОДА
« О РЕКЛАМЕ»

УКАЗ ПРЕЗИДЕНТА РФ ОТ 01.06.2012 ГОДА №761
**« О НАЦИОНАЛЬНОЙ СТРАТЕГИИ ДЕЙСТВИЙ В ИНТЕРЕСАХ
ДЕТЕЙ НА 2012-2017 ГОДЫ»**

ФЕДЕРАЛЬНЫЙ ЗАКОН № 436-ФЗ ОТ 29.12.2010 Г.
**«О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ
ЗДОРОВЬЮ И РАЗВИТИЮ»**

ФЕДЕРАЛЬНЫЙ ЗАКОН № 149-ФЗ ОТ 27.07.2006 Г.
**«ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О
ЗАЩИТЕ ИНФОРМАЦИИ»**



«Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать»

СОЦИОЛОГИЧЕСКИЕ ИССЛЕДОВАНИЯ

По последним данным, в России: средний возраст начала самостоятельной работы в Сети - 7 лет и сегодня наблюдается тенденция к снижению возраста до 5 лет. 88% четырёхлетних детей выходят в сеть вместе с родителями. В 7-9-летнем возрасте дети всё чаще выходят в сеть самостоятельно. К 14 годам совместное, семейное пользование сетью сохраняется лишь для 7% подростков.



Мобильным интернетом сегодня пользуется практически каждый второй ребенок.

- Больше половины пользователей сети в возрасте до 14 лет просматривают сайты с нежелательным содержанием.
- 39% детей посещают порносайты,
- 19% наблюдают сцены насилия,
- 16% увлекаются азартными играми.
- Наркотическими веществами и алкоголем интересуются 14% детей,
- Экстремистские и националистические ресурсы посещают 11% несовершеннолетних пользователей



Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

1. Самая распространенная угроза для детей в Интернете, это обилие откровенных материалов сексуального характера.

Многочисленные видеоролики и снимки с так называемой «жесткой эротикой», в том числе содержащие информацию о сексуальных извращениях, могут дезориентировать ребенка, ранить его психику, вызвать нарушения психосексуального и нравственно-духовного развития, воспрепятствовать построению нормальных социальных, в том числе межполовых и семейных отношений в будущем.





Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

2. При общении в Сети у каждого обязательно появляются **виртуальные знакомые и друзья.**

Кроме своих сверстников и интересных личностей, общение с которыми пойдет на пользу, ребенок может завязать знакомство не только с педофилом и извращенцем, но и с мошенником и хулиганом. Виртуальное хамство и розыгрыши часто заканчиваются киберпреследованием и киберунижением, доставляя объекту травли множество страданий. Для ребенка такие переживания могут оказаться критичными, поскольку он более раним, чем взрослые люди.





Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

2. При общении в Сети у каждого обязательно появляются **виртуальные знакомые и друзья.**

В последние годы получили распространение такие общественно опасные посягательства на личность несовершеннолетнего в сети, как кибербуллинг (cyberbullying) – подростковый виртуальный террор.

Кибербуллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи.



Наиболее опасными видами кибербуллинга считаются **киберпреследование** — **скрытое отслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.**, а также хеппислепинг (Happy Slapping — счастливое хлопанье, радостное избиение) — видеоролики с записями реальных сцен насилия.



Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

3. Опасная для детей информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться на электронных ресурсах, содержащих материалы экстремистского и террористического характера.





Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

4. Особую опасность представляют для незрелой психики несовершеннолетних электронные ресурсы, созданные и поддерживаемые **деструктивными религиозными сектами.**

Главная проблема деструктивных сект в сети – это предоставление ложной информации. Попасть под негативное влияние секты через сайт очень легко – если ребенок читает в сети соответствующий материал,



смотрит видео и фото-информацию, то он уже вступает во взаимодействие с вербовщиком секты, невольно участвует в психологической игре организаторов секты, нередко попадая от них в зависимость.



Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

5. Доверчивость и наивность детей нередко используют в своих целях компьютерные мошенники, спамеры, фишеры.

Несовершеннолетние нередко переходят по присланным им злоумышленниками ссылкам без подозрений, скачивают неизвестные файлы, которые могут оказаться вирусами или содержать незаконную информацию. Недостаточно информированный об опасностях в сети ребенок может сообщить злоумышленнику номер кредитной карточки родителей, пароль от электронного кошелька, свой настоящий адрес и многое другое.





Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

5. Доверчивость и наивность детей нередко используют в своих целях компьютерные мошенники, спамеры, фишеры.

Что сообщают о себе школьники в профиле социальной сети





Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

6. Пропаганда наркотиков, насилия и жестокости, суицидального поведения, аборт, самоповреждений может быть весьма опасной для неокрепшей детской психики.

Ребенок на веру принимает многие сомнительные идеи, особенно если они грамотно изложены. Например, о том, как лучше покончить с собой или от приема каких таблеток «станет веселее», как без обращения к врачу избавиться от нежеланной беременности и т.д. Этим пользуется немало людей, использующих детей в корыстных и иных личных целях.





Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

7. Помимо указанной выше информации в Сети есть немало сомнительных развлечений, таких как онлайн-игры, пропагандирующие секс, жестокость и насилие, требующие немалых финансовых вложений. Дети бывают вовлечены в азартные игры в сети.



Bad Language - Ненормативная лексика
Игра содержит грубые и непристойные выражения.



Discrimination - Дискриминация
Присутствие в продукте сцен или материалов, которые могут порочить или дискриминировать некоторые социальные группы.



Fear - Страх:
Материалы игры могут оказаться страшными и пугающими для маленьких детей.



Gambling - Азартные игры
В игре есть возможность сыграть в азартные игры и сделать ставку, в том числе — реальными деньгами.



Sexual Content – Непристойности
В игре присутствует обнажение и/или встречаются сцены с сексуальными отношениями.



Violence - Насилие
Игра изобилует сценами с применением насилия.



Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

8. Психологами отмечается распространённость в среде пользователей, в том числе несовершеннолетних, случаев болезненного пристрастия к участию в сетевых процессах, так называемой "Интернет-зависимости", проявляющегося в навязчивом желании неограниченно долго продолжать сетевое общение.

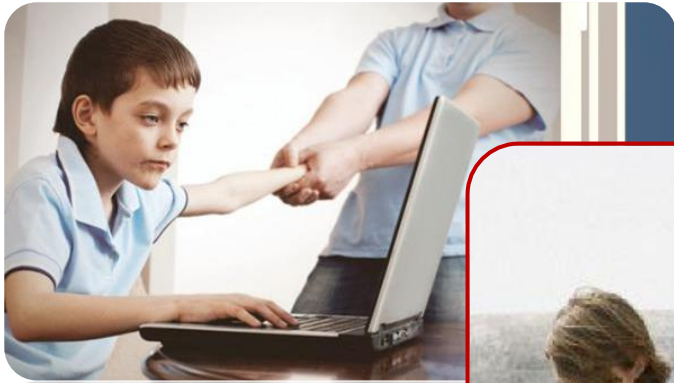
Выделяется 6 основных типов интернет-зависимости:

- 1. Навязчивый веб-серфинг** — бесконечные путешествия по Всемирной паутине, поиск информации.
- 2. Пристрастие к виртуальному общению** и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, избыточность друзей в Сети.
- 3. Игровая зависимость** — навязчивое увлечение компьютерными играми по сети.
- 4. Навязчивая финансовая потребность** — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.
- 5. Пристрастие к просмотру фильмов через интернет**, когда больной может провести перед экраном весь день, не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.
- 6. Киберсексуальная зависимость** — навязчивое влечение к посещению порносайтов и занятию киберсексом.



Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

Интернет-зависимость



Административные и организационные меры, технические и программно-аппаратные средства защиты детей от вредной информации в ОУ Партизанского муниципального района

- Правила использования сети Интернет
- Инструкция по организации контроля использования сети Интернет
- Дополнения в должностные инструкции работников
- Должностная инструкция работника, ответственного за организацию доступа к Интернет
- План мероприятий по обеспечению информационной безопасности обучающихся
- Перечень мероприятий по контролю состояния системы обеспечения информационной безопасности обучающихся
- Назначены ответственные за организацию доступа к сети Интернет
- На официальных сайтах и информационных стендах размещена информация для детей и родителей
- Установлена система фильтрации Интернет-контента «ТЫРНЕТ-ПРОКСИ»

ВСЕРОССИЙСКИЙ ЕДИНЫЙ УРОК ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

С 2014 года в общеобразовательных учреждениях проходит Всероссийский Единый урок по безопасности в сети Интернет, цель которого заключается в воспитании у детей и подростков информационной культуры

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ

СЛОЖНЫЙ ПАРОЛЬ

Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Чем сложнее пароль, тем сложнее взломать твой аккаунт. Помни, что твой пароль можешь знать только ты.



СОВЕТ ВЗРОСЛЫХ

Всегда спрашивай взрослых о непонятных вещах, которые ты встречаешь в Интернете: ты не знаешь, какой пункт выбрать, на какую кнопку нажать, как закрыть программу или окно. Они расскажут тебе, как поступить - что можно делать, а что нет.



ЛИЧНАЯ ИНФОРМАЦИЯ

Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому о том, где работают твои родители и номера их телефонов. Эта информация может быть использована во вред тебе и твоим родителям.



НЕ ОТПРАВЛЯЙ СМС

Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс - не делай этого! Смс на короткие номера могут стоить несколько сотен рублей. Ты потеряешь деньги, которые мог бы потратить на что-то другое.



НЕ ЗАБУДЬ ВЫЙТИ

При использовании чужих компьютеров или мобильных устройств, не забывай выходить из своего ящика электронной почты или профилей в социальных сетях. Иначе, следующий пользователь этого устройства сможет просмотреть твою личную информацию.



ОСТОРОЖНО, НЕЗНАКОМЕЦ!

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения - сразу скажи об этом взрослым! Не все люди являются теми, за кого себя выдают в Интернете!



БЕСПЛАТНЫЙ Wi-Fi

При выходе в Интернет через общественную Wi-Fi сеть, не совершай никаких покупок и оплаты, не проверяй личную электронную почту и не передавай конфиденциальную информацию. Злоумышленники могут похитить ваши пароли и данные.



ЗАЩИТИ КОМПЬЮТЕР

Попроси родителей или сам установи систему фильтрации SkyDNS на сайте www.skydns.ru. Она защитит тебя от потери денег и кражи паролей, а также будет блокировать большую часть рекламы, ускоряя загрузку страниц в Интернете.



РЕКОМЕНДАЦИИ ДЛЯ СПЕЦИАЛИСТОВ ОРГАНИЗАЦИЙ ОБРАЗОВАНИЯ, РАБОТАЮЩИХ С ДЕТЬМИ

Если раньше взрослые старались предостеречь детей от опасностей, которые подстерегают их на улице, то сегодня возникла проблема безопасности ребёнка в киберпространстве. Для того, чтобы обеспечить эту безопасность необходимо в первую очередь самим хорошо знать эту зону.

Педагогам в рамках своих уроков необходимо как можно больше применять современных информационных технологий и сразу предостерегать своих учеников о возможном их негативном влиянии.

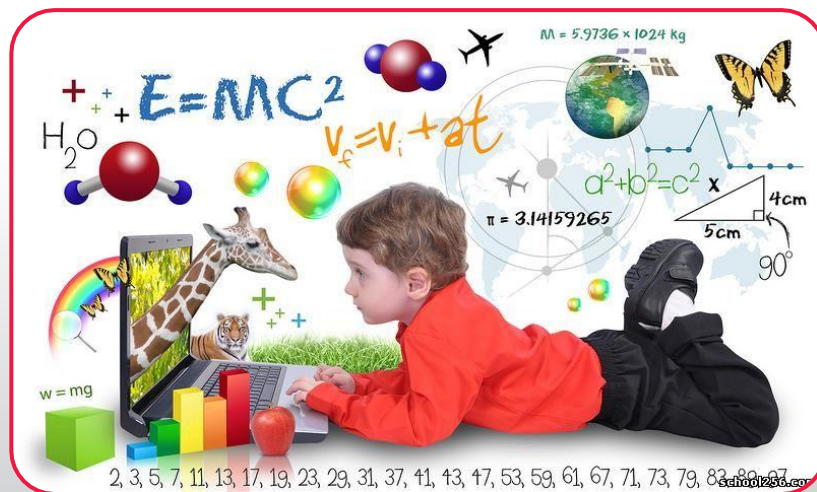
В воспитательной работе уделять внимание воспитанию информационной культуры учащихся.

Проводить уроки медиаобразования, на которых давать самые необходимые знания по соблюдению безопасности в информационном пространстве

УРОКИ МЕДИАБЕЗОПАСНОСТИ

Медиаграмотность- это грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации, привития коммуникативных навыков, позитивное и ответственное использование информационных и коммуникационных технологий и услуг.

Цель проведения уроков медиабезопасности – обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде



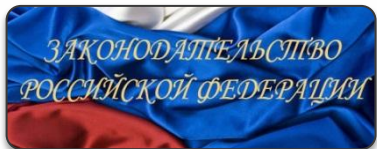
ЗАДАЧИ УРОКОВ МЕДИАБЕЗОПАСНОСТИ



Информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних



Информирование учащихся о способах незаконного распространения такой информации



Ознакомление учащихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации



Обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации



Профилактика формирования у детей интернет-зависимости и игровой зависимости



Предупреждение совершения детьми правонарушений с использованием информационно-телекоммуникационных технологий

Не стоит думать, что Интернет – это безопасное место, в котором дети могут чувствовать себя защищенными.

В Интернете необходимо следовать основным правилам так же, как правилам дорожного движения при вождении.

При этом использование только средств воспитательной работы без организации действенного контроля – это практически бесполезное занятие. Точно так же как и использование репрессивных средств контроля без организации воспитательной работы. Только в единстве данных средств можно помочь детям чувствовать себя в безопасности и оградить их от влияния злоумышленников.



Спасибо за внимание!

Бушуева Е.В.,
специалист по информационным
и коммуникационным технологиям