Муниципальное бюджетное учреждение дополнительного образования «Дом детского творчества» поселка Псебай муниципального образования Мостовский район

Проект

по теме: «БЕЗОПАСНЫЙ ИНТЕРНЕТ»

Автор проекта:
педагог дополнительного образования
Нестеренко Г.Н.
Учащиеся объединения «Клуб-Ок+»
Группа 2.2
Проект среднесрочный
Дата проведения проекта:
01.11.2023г. - 01.02.2024г.

п. Псебай.

Введение:

В настоящее время Интернет стал неотъемлемой частью повседневной жизни. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учебы. Здесь можно общаться со своими друзьями в режиме онлайн, можно найти новых друзей, вступать в сообщества по интересам.

Интернет представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей.

Небезопасное поведение в сети Интернет может нанести вред и взрослым, и детям. Как показали исследования, наиболее растущим сегментом пользователей Интернета являются школьники. В этом возрасте взрослые играют определяющую роль в обучении детей безопасному использованию Интернета.

Родители и педагоги могут помочь детям сформировать понимание и осознание разумного поведения, а также неограниченного доступа к Интернету.

Интернет может быть безопасным и полезным для обучения, отдыха и общения с друзьями. Но, как и реальный мир, *«Сеть»* может быть опасна: в ней появились своя преступность, хулиганство, вредительство, и прочие малоприятные явления.

Цель проекта: расширить представления о физической и информационной безопасности личности в современном информационном обществе

Задачи проекта:

Для учащихся:

Обучающие:

-Узнать о вреде бесконтрольного использования компьютера и интернета.

Развивающие:

-развитие познавательного интереса и правильного использования интернета;

Воспитательные:

- воспитание бережного отношения к своему физическому и психическому здоровью.

Для педагога:

- Овладеть методом проектов как технологией.
- Сформировать предметно-развивающую среду для проекта, оформить проект наглядным материалом по изучаемой теме.

Этапы проекта:

Подготовительный этап:

Определить цель и задачи, определить направления работы. Составить план выполнения проекта. Создание анкет подбор материала к ним.

Анкетирование родителей «Основы безопасности в сети Интернет»

Основной этап: реализация проекта.

Заключительный этап: анализ проведенной работы, подведение итогов, анкетирование родителей «Итоги работы по безопасности Интернета», подготовка презентации «Безопасный интернет».

Предполагаемый результат:

Учащиеся имеют элементарные представления о влияние компьютера на здоровье ребенка; о безопасности в сети Интернет.

Родители стали понимать значимость проблемы, сопровождать ребёнка за работой с компьютером.

Гипотеза: я предполагаю, что «Интернет и дети - друзья», если использовать его, соблюдая правила безопасности.

Участники проекта подготовили анкету (Приложение1.) и провели анкетирование.

Результаты анкетирования показали:

1. Дома у всех имеется компьютер
2. Компьютером пользуются все члены семьи
3. 65% детей имеют доступ к интернету
4. 50% родителей не следят за тем, на какие сайты заходят дети
5. 95% родителей не установлены программы, которые фильтруют содержание сайтов
6. 70% родителей ответили, что дети больше часа времени проводят в сети Интернет
7. 45% родителей беседуют с ребёнком о безопасности в сети Интернет
8. 10% родителей ответили, что ребенок заходит в образовательные сайты.

Участники проекта подготовили информацию «10 интересных фактов о кибербезопасности, о которых вы не знали» (Приложение 2)
Памятки:
«Чем вреден компьютер» (Приложение 3)
«Советы по безопасности в сети интернет для родителей» (Приложение 4)
«БезОпасный интернет детям» (Приложение5)

А так же подготовили презентацию « Безопасный интернет» (Приложение 6)

Заключение

Интернет может быть очень опасным, но в тоже время, нельзя не упомянуть о том, что Интернет сегодня является необходимостью. И здесь,

как и в реальной жизни, всё зависит от самого человека. Если у него есть чувство меры в «отношениях с Интернетом» и не возникает нездоровая Интернет-зависимость, то такое достижение человечества, как Интернет вполне достойно всяческого уважения.

Попробуйте представить Ваш день без Интернета! Это вряд ли у Вас получится! Значит, несмотря на эту огромную ложку дёгтя-угрозы, опасности, Интернет - это весьма и весьма полезная штука. Работая с Интернетом, соблюдая все рекомендации по безопасности, Вы подтвердите нашу гипотезу: «Интернет и дети - друзья».

И еще. Гарантированную помощь в случае интернет-угрозы и интернет-насилия, можно получить по номеру всероссийского детского телефона доверия (8–800–2500015).

Литература

Для написания данной работы были использованы ресурсы Сети Интернет.

1. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет.[Электронный ресурс] URL:http://www.ifap.ru/library/book331.pdf

2. Безопасность детей в Интернете URL:http://www.microsoft.com/rus/childsafety

3. Дети и интернет, какие опасности скрывает всемирная паутина. / Методическое пособие для родителей. URL:http://www.pandia.ru/text/77/115/462.php

4.Детская безопасность в Интернете. [Электронный ресурс]. URL:http://www.debotaniki.ru/2012/09/detskayabezopasnostvinternete/

5.Полезный и безопасный Интернет. Правила безопасного использования Интернета для детей младшего школьного возраста: Методическое руководство / Под ред. Г. У Солдатовой. - М., 2012. КиберЛенинка:https://cyberleninka.ru/article/n/bezopasnost-v-seti-internet

Приложение 1.

Анкета для родителей «Безопасный интернет для детей»

Есть ли у Вас дома компьютер или телефон с подключением к интернету?

☐ Да

☐ Нет

Кто пользуется компьютером у Вас дома?

☐ Только родители

☐ Только ребенок

☐ Все члены семьи

Имеет ли Ваш ребенок доступ к сети Интернет?

☐ Да

☐ Нет

Следите ли Вы за тем, на какие сайты заходит ребенок? Каким образом?

☐ Да

☐ Нет

Установлены ли у Вас программы, которые фильтруют содержание сайтов?

☐ Да

☐ Нет

Сколько Ваш ребенок проводит времени в сети Интернет?

☐ До 1 часа

☐ Больше 1 часа

☐ Не пользуется Интернетом

Беседуете ли вы с ребёнком о безопасности в сети Интернет?

☐ Да

☐ Нет

На какие сайты заходит Ваш ребенок?

☐ Образовательные

☐ Социальные сети

☐ Разные

Спасибо за участие в анкетировании!

Приложение 2.

10 интересных фактов о кибербезопасности, о которых вы не знали

Кибербезопасность - одна из самых важных тем в IT-индустрии. Она охватывает множество аспектов: от противодействия вредоносному программному обеспечению до защиты конфиденциальной информации. Вот 10 интересных фактов, связанных с кибербезопасностью, о которых вы, возможно, не знали.

1. В США ежегодно происходят более 300 000 кибератак на малые и средние предприятия
2. В мире ежегодно теряют около 600 миллиардов долларов из-за киберпреступности
3. Самым распространенным паролем в 2022 году был "123456"
4. Более 95% утечек данных происходят из-за человеческого фактора, такого как слабый пароль или недостаточная защита устройства
5. Каждую секунду на планете происходит более 5 000 попыток взлома устройств
6. Более 90% электронной почты - спам. Однако, только 0,06% от них содержат вредоносный код
7. Каждую минуту в мире происходит более 1 100 000 атак на устройства подключенные к интернету в поисках уязвимостей в системах
8. Средняя стоимость нарушения безопасности данных в 2022 году составила $ 4,2 млн
9. Более 80% сайтов имеют уязвимости, которые могут быть использованы для кибератак
10. Специалисты по кибербезопасности считают, что в будущем рынок кибербезопасности вырастет до $ 300 миллиардов в 2024 году

Эти факты показывают, что кибербезопасность является критически важной областью в IT-индустрии.

Она важна не только для бизнеса, но и для обычных пользователей, которые хранят на своих устройствах личные данные и конфиденциальную информацию.


Чем вреден компьютер для здоровья?
Почему вредно для здоровья долго находиться перед компьютером?
ЗАДУМАЙТЕСЬ НАД ФАКТОМ:
Мелькающее изображение вызывает нагрузку на зрение, неменяющаяся поза приводит к нарушениям костно-мышечного аппарата ребёнка, малоподвижный образ жизни способствует появлению избыточного веса.
ЧТО ПРЕДПРИНЯТЬ:
• Правильно установите монитор относительно источника света.
• Подберите мебель в соответствии с ростом малыша (лучше ту, которая регулируется по высоте).
• Увеличивайте физическую нагрузку ребёнка.
www.uchmag.ru


Дисциплина за компьютером
Всё чаще и чаще компьютер становится причиной ссор и обид в семье, особенно между детьми. Можно ли этого избежать, если в доме всего один компьютер?
ЗАДУМАЙТЕСЬ НАД ФАКТОМ:
Борьба за место у компьютера приводит к негативу в семье – обидам, недопониманию, нездоровому соперничеству, а иногда и более страшным последствиям.
ЧТО ПРЕДПРИНЯТЬ:
Начните формировать информационную культуру всей семьёй. Если ребёнку установлено ограничение времени пользования компьютером, установите это ограничение и себе. Переключайтесь на другой интересный вид совместной деятельности.
www.uchmag.ru

Советы по безопасности в сети Интернет для родителей

Соблюдайте время нахождения ребенка в сети интернет.

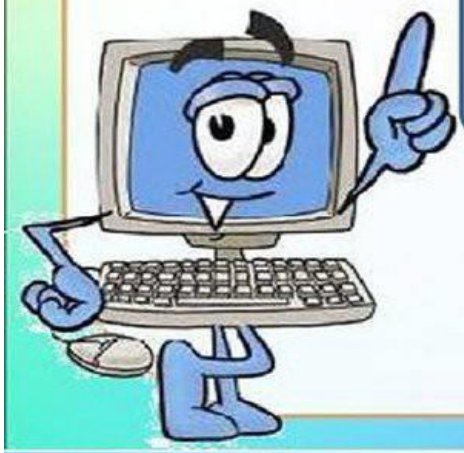
Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

Используйте средства блокирования нежелательного контента, как дополнение к стандартному Родительскому контролю.

Научите детей не загружать файлы, программы или музыку без вашего согласия.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.



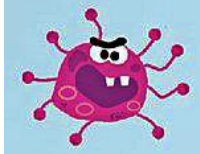
Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.

БезОпасный Интернет - детям!

ИНТЕРНЕТ - это безграничный мир информации, здесь ты найдешь много интересного и полезного для учёбы, в интернете можно общаться со знако-мыми и даже заводить друзей.

Интернет бывает разным:
Другом верным иль опасным.
И зависит это все от тебя лишь одного.
Если будешь соблюдать правила ты разные-
Значит для тебя общение
В нем будет безопасное!
Будь послушен и внимательно
Прочти, запомни основательно
Правил свод, что здесь изложен,
Для детишек он не сложен!

Иногда тебе в сети
Вдруг встречаются вруны.
Обещают все на свете
Подарить бесплатно детям:
Телефон, щенка, айпод
И поездку на курорт.
Их условия не сложны:
SMS отправить можно
С телефона папы, мамы –
И уже ты на Багамах.
Ты мошенникам не верь,
Информацию проверь.
Если рвутся предложить,
То обманом может быть.



Вдруг из щели между строк
Вылезает червячок.
Безобидный он на вид,
Но в себе беду таит.
Может файлы он стирать,
Может деньги воровать,
Предлагает нам обновки,
Вирус – мастер маскировки!
Не хочу попасть в беду,
Антивирус заведу!

В интернете, как и в мире,
Есть и добрые, и злые.
Полон разных он людей,
Есть и гений, и злодей.
По портрету не поймешь,
От кого слезу прольешь.
Чтобы вор к нам не пришел,
И чужой нас не нашел,
Телефон свой, адрес, фото
В интернет не помещай
И чужим не сообщай.

Мы хотим, чтоб интернет
Был вам другом много лет!
Будешь знать семь правил этих –
Смело плавай в интернете!

В интернете сайты есть –
Невозможно глаз отвесть.
Там и игры, и мультфильмы,
И учеба, и кино,
Только вдруг ты там находишь
Иногда совсем не то...
Чтобы не перепугаться
И потом не огорчаться,
Надо фильтр поискать
И компьютер подковать!
Ты родителям скажи:
Фильтры тут всегда нужны!

Как всем детям интересно
Поиграть с друзьями вместе,
В интернете тоже можно,
Нужно быть лишь осторожным.
И с чужими не играть,
В гости их к себе не звать
И самим не приходить –
Я прошу вас не забыть.

Приложение 6.

Транскрипт к презентации «Безопасный интернет»

Слайд 1.

Проблема безопасности сети Интернет для детей

Сегодня трудно представить себе жизнь без компьютера. В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Стремительное развитие и распространение информационных технологий приводит к тому, что постоянно увеличивается число детей, которые используют компьютер в школе, на уроках информатики и для подготовки домашних заданий, а также проводят за ним часть своего свободного времени.

Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а также получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

Однако бурное развитие Интернета несет также существенные издержки. Современная научно - образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно - образовательных ресурсов.

Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются с ресурсами, содержащими неэтичный и агрессивный материал. Терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры материала, с которым могут соприкоснуться дети и подростки.

Слайд 2.

1 сентября 2012 года вступил в силу ФЕДЕРАЛЬНЫЙ ЗАКОН N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

Он направлен на защиту детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности.Как ожидалось, закон должен был способствовать формированию гармоничной и психологически устойчивой личности каждого ребенка, бережному и грамотному воспитанию детей на идеях добра и справедливости.

Бесконтрольное распространение нежелательной информации противоречит целям образования и воспитания молодежи. Однако, полностью отказываться от благ информационных технологий бессмысленно.

Слайд 3.

Классификация интернет–угроз

Контентные риски.

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

Неподобающий контент.

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Незаконный контент.

В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

Электронная безопасность.

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн - мошенничество и спам.

Вредоносные программы.

Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы - шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.

Спам.

Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный

интернет - трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

Кибермошенничество.

Кибермошенничество - это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким - либо образом использует личную информацию пользователя, с целью получить материальную прибыль.

Коммуникационные риски.

Коммуникационные риски связаны с межличностными отношениями интернет - пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Рекламные программы.

Рекламные программы - нежелательное программное обеспечение, содержащее рекламу. Рекламные программы поставляется в сочетании с программными продуктами, как правило, бесплатными или условно-бесплатными. В дальнейшем, при использовании программного продукта пользователю принудительно показывается реклама, которая может содержать нежелательную информацию.

Кроме того бесконтрольно всплывающие рекламные окна раздражают и, в некоторых случаях, снижают производительность системы. Также, рекламные системы могут собирать конфиденциальную информацию о компьютере и пользователе, такую как IP-адрес компьютера, список часто посещаемых пользователем сайтов, поисковые запросы, прочие данные, которые можно использовать при проведении последующих рекламных кампаний.

Вредоносное программы.

Вредоносные программы (вирусы) - любое программное обеспечение, специально созданное для причинения ущерба отдельному компьютеру или компьютерной сети. Вредоносные программы устанавливаются без Вашего разрешения и влияют на работу Вашего компьютера. Наиболее распространенными видами вредоносных программ являются компьютерные вирусы, которые чаще всего, проникают на компьютер через Интернет или по электронной почте.

Шпионские программы.

Шпионская программа – это несанкционированно установленный программный продукт, целью которого является скрытое отслеживание

поведения пользователя в сети. Также, подобные программы используются для сбора различных типов личной информации, например привычка пользования Интернетом и посещаемые сайты.

Мошенничество.

Интернет-мошенничество-вид мошенничества с использованием Интернета. Оно может включать в себя сокрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства. Интернет-мошенничество не считается отдельным преступлением, а включает ряд незаконных действий, совершаемых в киберпространстве. Однако оно отличается от кражи, поскольку в этом случае жертва добровольно и сознательно предоставляет преступнику информацию, деньги или имущество.

Еще одна опасность, подстерегающая в *Интернете-это интернет-зависимость.*

Признаки Интернет- зависимости:

- Навязчивые бесконечные путешествия по Всемирной паутине.
- Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки.
- Избыточность знакомых и друзей в Сети.
- Игровая зависимость — навязчивое увлечение компьютерными играми. 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.

Слайд 4.

Способы защиты сети Интернет

Программы фильтры

- Можно установить специальные программы-фильтры на компьютер, которые будут совершать:
- ограничение по суммарному времени работы;
- поддержку перерывов в работе;
- поддержку разрешенных интервалов работы;
- возможность запрета интернета
- возможность запрета игр/программ.

Слайд 5.

Правила пользования Интернетом для родителей

Не разрешайте ребенку предоставлять личную информацию через Интернет.

Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность - отличный способ защиты. Не выкладывайте фотографии ребенка на веб-страницах или публичных форумах.

Оградите ребенка от ненадлежащего контента.

Научите его, как следует поступать при столкновении с подозрительным материалом, расскажите, что не нужно нажимать на ссылки в электронных сообщениях от неизвестных источников, открывать различные вложения. Такие ссылки могут вести на нежелательные сайты, или содержать вирусы, которые заразят Ваш компьютер. Удаляйте с Вашего компьютера следы информации, которую нежелательно обнаружить Вашему ребенку.

Ребенок должен понять, что его виртуальный собеседник может выдавать себя за другого человека.

Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. И 10-летний друг Вашего ребенка по чату в реальности может оказаться злоумышленником. Поэтому **запретите** ребенку назначать встречи с виртуальными знакомыми.

Рекомендации для родителей

Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернета;

Объясните детям, что если в Интернете что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

Составьте список правил работы детей в Интернет и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда и без оговорок.

Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями, использовании онлайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.

Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию,

например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.

Объясните своему ребенку, что, как и в реальной жизни и в Интернете нет разницы между неправильными и правильными поступками;

Научите ваших детей уважать собеседников в Интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернете и в реальной жизни;

Скажите им, что никогда не стоит встречаться с друзьями из Интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают;

Объясните, что далеко не все, что можно увидеть в Интернете – правда. При сомнениях, пусть лучше уточнит у вас.

— Компьютер с подключением к Интернету должен находиться в общей комнате.
— Приучите себя знакомиться с сайтами, которые посещают ваши дети.

Используйте современные программы, которые предоставляют возможность фильтрации содержимого сайтов, контролировать места посещения и деятельность там.

Слайд 6.

Правила пользования Интернетом для детей.

1. Всегда спрашивай родителей, взрослых о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
2. Нежелательно размещать персональную информацию в интернете. Персональная информация — это ваше имя, фамилия, возраст, номер мобильного телефона, адрес электронной почты, домашний адрес и адрес школы, в которой Вы учитесь.
3. Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!
   Слайд 7.
4. Пользуйтесь браузерами Яндекс, Opera, Google Chrome и Safari!
   Слайд 8.
5. Контролируйте работу за компьютером. Неограниченное использование компьютера может привести к физическим (глазным, гиподинамия, остеохондроз) и психологическим заболеваниям (Интернет-зависимость). Через каждые 20 минут работы выполни зарядку для глаз.

6. Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми познакомились в Интернете.
   Слайд 9.
7. Не используйте в качестве паролей набор цифр: 1234, дату вашего рождения и т.п. «Легкие» пароли быстро взламываются, и Вы можете стать жертвой злоумышленников.
8. Не передавайте свой пароль посторонним лицам.
   Слайд 10.
9. Используйте на компьютерах лицензионное программное обеспечение, антивирусные программы и своевременное обновляйте их, для того что бы защитить компьютер от вирусов и вредоносных программ. Обновление необходимо для пресечения проникновения новых вредоносных программ на Ваш компьютер.
   Слайд 11. Спасибо за внимание!