Автор: **Иконникова Людмила Владимировна**,
МАОУ СОШ с.Красный Ключ Нуримановский район Республики Башкортостан
учитель математики и информатики, e-mail: ikonnikova.L.V@mail.ru

образовательный проект на тему:

«Опасности в мире Интернета»

2019

Содержание

Введение

«Они, дети, должны знать, какие опасности подстерегают их в сети и как их избежать».

А. Ю.Кузнецова

Сегодня Интернет играет большую роль в жизни человека, а также оказывает огромное влияние на него. Всеобщая информатизация и доступный Интернет позволяет получать качественное образование дистанционно. Кроме того, не секрет и то, что сегодня для многих детей компьютер стал «и мамой, и папой», единственным другом, и «помощником», и даже «воспитателем», «учителем». Результаты многочисленных исследований свидетельствуют, что пристрастием к виртуальному общению в социальных сетях уже охвачено более половины всех пользователей Интернета. И дети не исключение. Чаще дети путешествуют по страницам Интернета бесконтрольно. Instagram, Одноклассники, В Контакте, YouTube - на слуху у всех. Но дети в виртуальном мире, в отличие от взрослых, совершенно не чувствуют опасности. В Интернете представлены сайты, где все чаще стала появляться «вредная» информация. Он приближает к нам сервисы и серверы, расположенные в разных странах и на разных континентах: всё, что угодно душе, оказывается «на расстоянии клика». Но на таком же расстоянии – то есть совсем рядом!– находятся и ресурсы, которые с легкостью заразят компьютер вирусом, украдут персональные данные, превратят компьютер в «зомби», который без ведома, будет рассылать спам или участвовать в атаках на сайты. Но страшнее всего принятие детьми за чистую монету все то, что они видят по телевизору и в Интернете. Недостаточный уровень медиакультуры не позволяет им вовремя распознать манипулятивные техники, используемые при подаче рекламной и иной информации, проанализировать степень достоверности информации и подлинность ее источников. Самое страшное - страницы в сети, подталкивающие детей к самоубийству. Нельзя забывать и о том, что при работе с компьютером может негативно влиять на физическое, психологическое, духовное здоровье детей. Часто это служит причиной неадекватного поведения психически неустойчивых школьников, представляющих угрозу для людей.

Актуальность проекта

Согласно российскому законодательству информационная безопасность 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 (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»). Так как на высоком уровне остается проблема распространения через Интернет - ресурсы материалов экстремисткой и террористической направленности. 90% распространения и сбыта наркотических и психоактивных веществ происходит бесконтактным путем. Актуальность проблемы можно продемонстрировать следующими фактами:

• число зависимых от интернета, составляет от 2 до 10% пользователей (350 миллионов) по всему миру;

• в 11 версии Международной классификации болезней (МКБ 11) рассматривается вопрос о включении НХЗ, как самостоятельной нозологической единицы;

• в обиход входят такие понятия, как Facebook-депрессия (В России она могла бы называться "Депрессия от "ВКонтакте"), смс-лунатизм, фантомный звонок, веб-серфинг – социальные сети становятся реальным политическим инструментом при организации масштабных акций и флэшмобов .

Я задала ученикам нашей школы вопрос опрос «Как вы относитесь к запрету пребывания детей до 10 лет в интернете?» Ответы свидетельствовали о том, что эта проблема волнует старшеклассников. Большая часть учащихся ответила «Я за запрет». Вывод напрашивался сам проблема безопасности в Интернете актуальна для ребят. Мне стало интересно, а можно ли защитить себя и своих учеников от агрессивного и нелегального контента? Как сделать Интернет безопасным для нас?

Обсуждая эту проблему я пришла к выводу о необходимости разработки данного проекта, так как убеждена в том, что преодолеть нежелательное воздействие компьютера на детей возможно только совместными усилиями учителей, родителей и самих школьников.

Цели и задачи проекта

Цель: понять, как обезопасить себя и учащихся при работе в Интернете; разработка рекомендаций по повышению безопасности в глобальной сети, выпуск памяток по ознакомлению детей с основными правилами безопасного использования Интернета, выпуск познавательного буклета по данной теме.

Задачи:

- Изучить литературу, источников интернета по теме.
- Провести социальный опрос, анкетирование.
- Разработать рекомендации по повышению безопасности в глобальной сети.
- Разработать памятки для детей в сети Интернет.
- Сплотить коллектив детей, родителей, учителей.
- Популяризировать гражданскую позицию участников проекта через реализацию данного проекта.
- Повысить уровень знаний об основных опасностях (негативных ситуациях), которые существуют в сети Интернет, и как их избежать.
- Информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации, информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания).
- Обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия).
- Профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга).
- Предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Объект исследования – опасности в Интернете

Предмет исследования - учащиеся МАОУ СОШ с.Красный Ключ; безопасная работа в социальных сетях: общение и публикации материалов.

Методы работы: изучение литературы по проблеме; наблюдение, опрос.

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

Ожидаемые результаты:

В ходе работы над проектом **учащиеся научатся:**

- работать с большим объемом информации, выбирать главное, делать выводы;
- работать с аудиторией;
- уважительно относиться друг к другу;
- работать в группе, в коллективе;
- познакомятся с программным обеспечением, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации;
- научатся делать более безопасным и полезным свое общение в Интернете и иных информационно-телекоммуникационных сетях, а именно:
  - критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
  - отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
  - избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
  - распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
  - распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
  - критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
  - анализировать степень достоверности информации и подлинность ее источников;
  - применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Классификация интернет - угроз

1. Контентные риски, которые связаны с потреблением информации, публикуемая в интернете и включающая 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 анарексии 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.

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

- Вредоносное ПО - Рекламное ПО - Шпионское ПО - Браузерный эксплойт

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 - 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. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

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

4. 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.

5. Вредоносное 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.

6. Шпионские 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.

7. Мошенничество.

- спам
- Депрессивные молодежные течения
- Наркотики
- Социальные сети, Знакомства, блоги чаты, секты.
- Экстремизм, нацизм, фашизм.

8. 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.

Способы защиты сети Интернет.

Программы фильтры:

- **KinderGate Родительский Контроль** - это интернет-фильтр для дома, школы и других образовательных учреждений, который обеспечивает полный контроль интернета и надежную защиту от нежелательного контента.
- **Детский интернет-браузер Гогуль** - это программа для ограничения доступа в интернет и фильтрации содержимого веб-ресурсов, для обеспечения безопасности ребёнка и **родительского контроля** детского сёрфинга по сети. Безопасность ребёнка в интернете обеспечивается за счёт каталога **детских сайтов**, проверенных педагогами и психологами, и насчитывающего тысячи детских интернет-сайтов. Гогуль ведёт статистику посещённых сайтов для родительского контроля интернет-сёрфинга ребёнка, а также может ограничивать время пребывания детей в интернет
- **КиберМама** проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет. КиберМама поддерживает следующие возможности:

- ограничение по суммарному времени работы;

- поддержка перерывов в работе;

- поддержка разрешенных интервалов работы;

- возможность запрета интернета;

- возможность запрета игр/программ.

Реализация проекта.

Месяц		Этапы работы над проектом
1	Сентябрь	Изучение литературы, источников интернета по теме. Выявление проблем. Выбор темы проекта
2	Октябрь	**Исследовательский**: социальный опрос, проведение анкетирования, родительского собрания по теме, анализ полученных данных, сбор информации из письменных источников, из Интернета.
3	Ноябрь - Январь	1. Уроки безопасности по теме: «Интернет - польза или вред?», где обсуждались вопросы коммуникации в сети Интернет, особенности работы с информацией в сети и некоторые технические аспекты работы в сети. 2. Просмотр видеоролика и переводенного на русский язык словенского мультсериала «SheepLive» партнёрством «Лига безопасного интернета». 3. Квест «Сетевичок 2019» 4. Уроки безопасности по теме: «Интернет - польза или вред?», где обсуждались вопросы культуры пользователя сети Интернет, защита контента, защита авторских прав, как безопасно и грамотно вести себя в социальных сетях, как общение в социальных сетях сделать полезным. 5. Просмотр видеофильма и презентаций. 6. «Изучи Интернет – управляй им!» – это социально-образовательный проект для школьников. Ознакомление и регистрация. 7. Уроки в 8 – 9 классах на тему «Интернет как глобальная информационная система. Кибербезопасность» 8. Всероссийский «Урок цифры» по теме «Безопасность в Интернете» в 7 – 11 классах. 9. Создание и распространение памятки по теме «Безопасный Интернет» (для детей и взрослых),

		распространение учащимся в школе. 10. Создание буклета для классных уголков в кабинетах школы «Безопасный интернет». 11. Изучение раздела безопасности в сети интернет на сайте школы https://schoolkrskluch.02edu.ru/school/about/information-security/
4	Май	Оформление проекта. Подведение итогов. Обсуждение на итоговом родительском собрании результативности проведенных мероприятий в течение года.

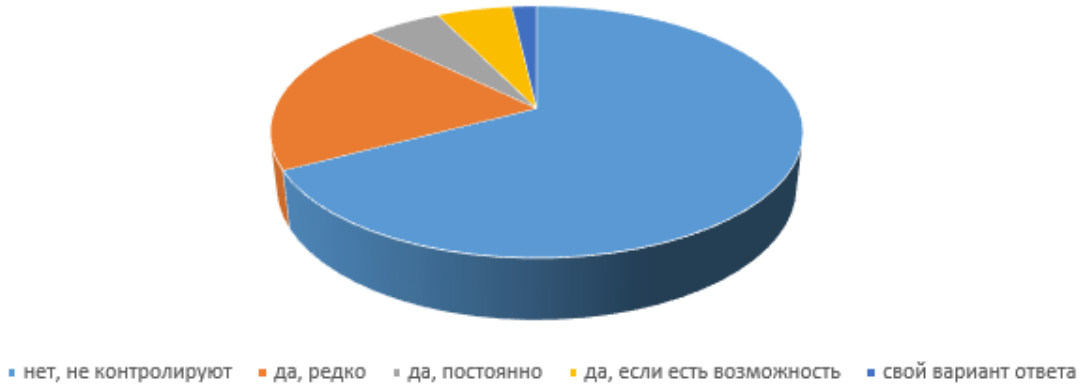
Результаты анкетирования учащихся

В опросе приняли участие 110 учащихся среднего и старшего звена, по ответам на вопросы выяснилось, что большинство учащихся находятся в сети без контроля старших практически весь день, в основном используя ноутбук или телефон, просматривая на youtube видеоролики, редко кто читает книги. Решают свои проблемы в основном чаще с друзьями, чем с родителями. Однако есть семьи, в которых родители ограничивают время нахождения своих детей за компьютером

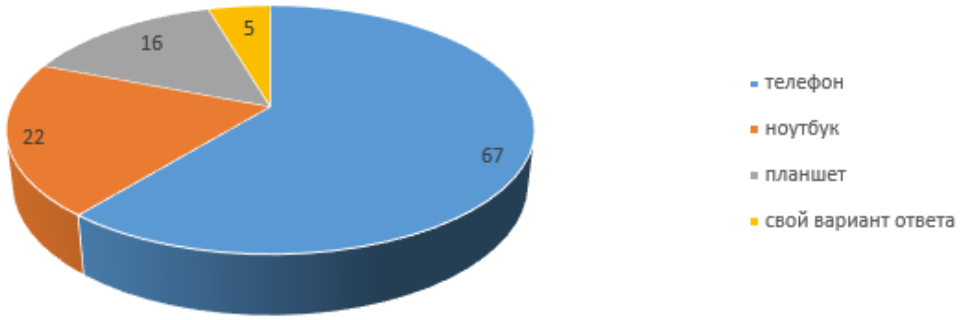
Подробный анализ представлен ниже в диаграммах.

1.Скажи, пожалуйста, имеешь ли ты возможность выходить в Интернет? Если да, то сколько времени в день ты проводишь в сети?

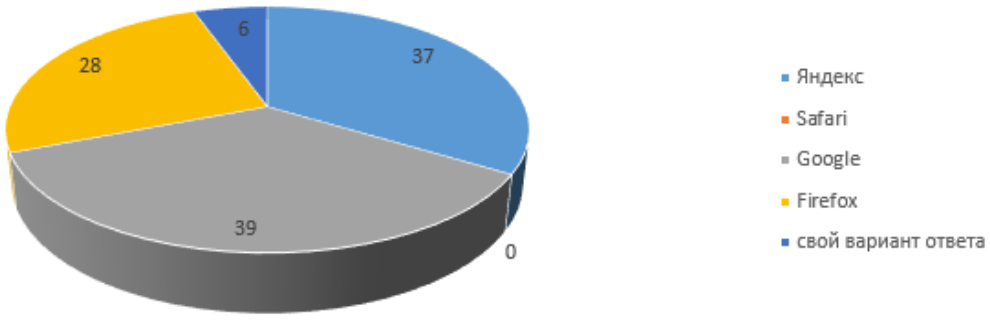
2.Если ты выходишь в Интернет, то контролируют ли тебя родители (бабушки / дедушки, старшие братья / сестры и др.)?



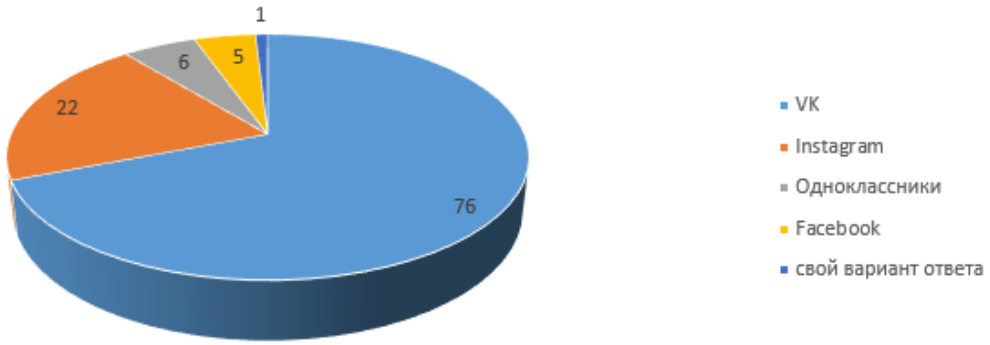
3.Какое устройство ты чаще всего используешь для выхода в Интернет? Укажи название



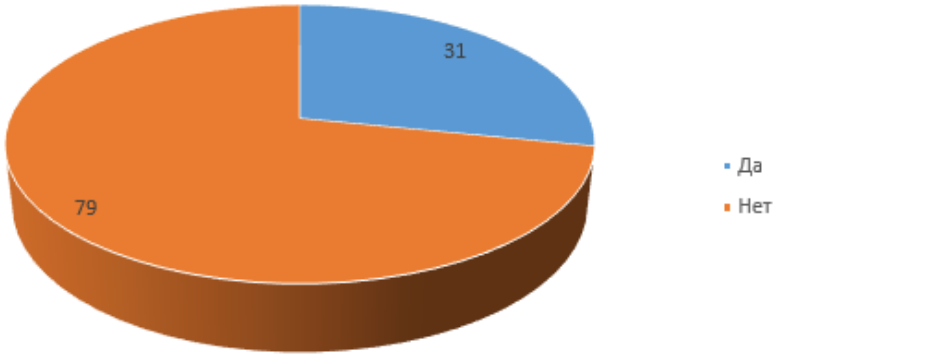
4.Какой браузер ты чаще всего используешь для поиска информации в сетиИнтернет?



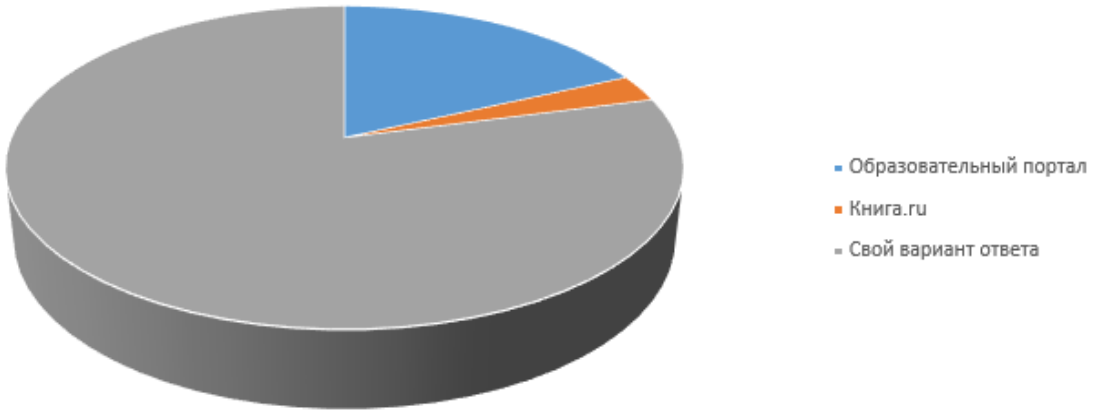
5.Есть ли у тебя страницы в социальных сетях?Если да, какой из социальных сетей ты уделяешь больше внимания?



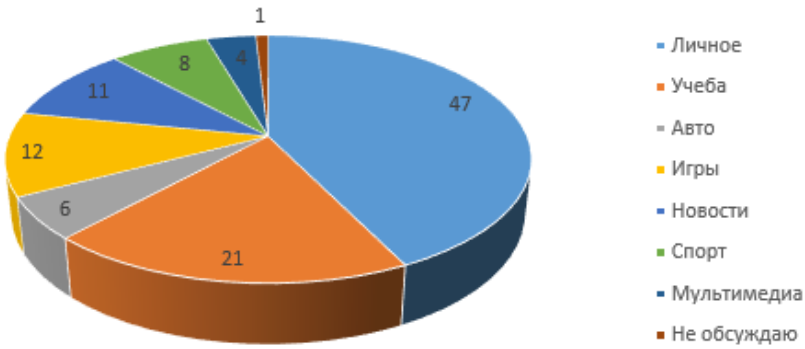
6. Читаешь ли ты книги?



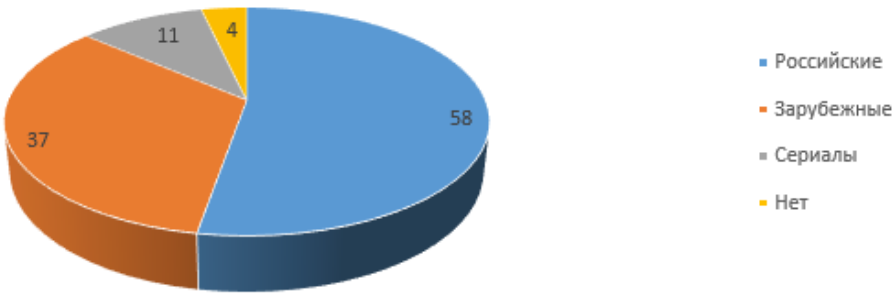
7. Какие интернет-ресурсы содержат интересующие тебя книги?



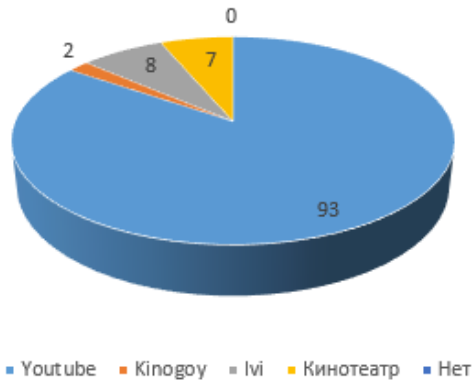
8. Какие темы ты чаще всего обсуждаешь в социальных сетях? Назови, наиболее обсуждаемые.



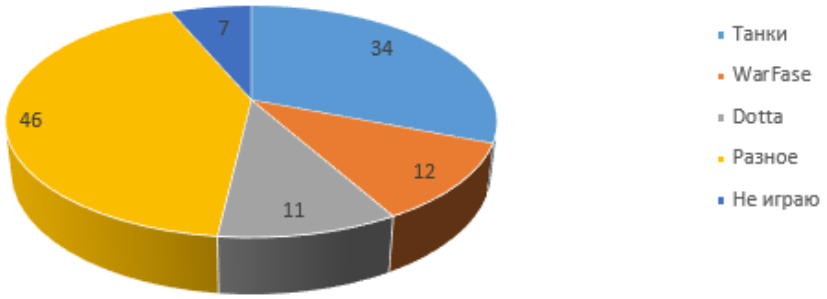
9. Какие фильмы из тех, которые ты смотрел, тебе запомнились более других?



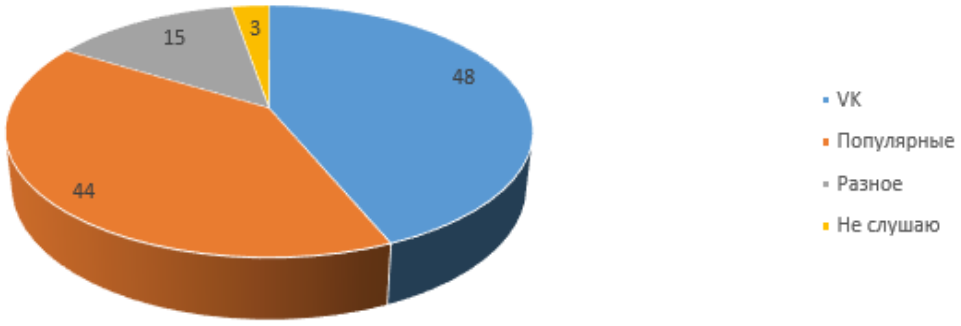
10. Какие интернет-ресурсы содержат интересующие тебя фильмы?

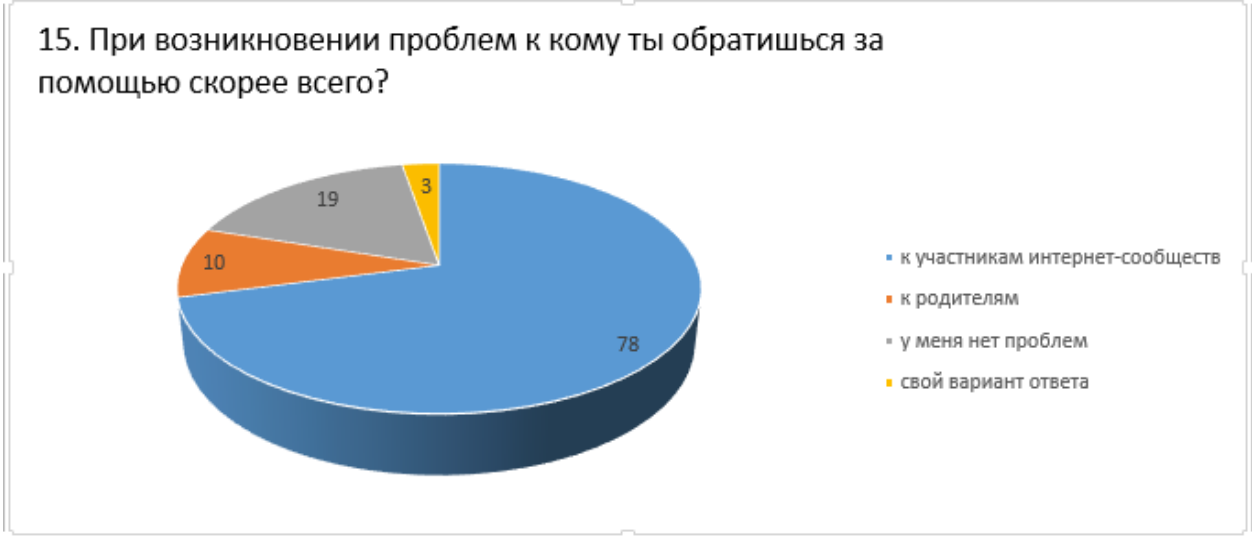


11. Играешь ли ты в компьютерные / on-line / или иного формата игры? Если да, то какие игры, по твоему мнению, наиболее захватывающие / увлекательные?



12. На каких интернет-ресурсах ты находишь интересующую тебя музыку?





Рекомендации для детей и родителей по безопасному использованию Интернета.

По результатам анкетирования я решила найти возможные способы защиты для детей и родителей при работе с интернетом. Один из способов это установка программ фильтров. Мы разработали рекомендации и инструкции для родителей. А также провели родительское собрание, на котором познакомили родителей со способами защиты в сети Интернет. А учащимся напомнили правила пользования сетью Интернет и сделали памятки для безопасного использования сетью.

Правила пользования Интернет 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 веб-содержимого. 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. 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.

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

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

3. 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.

4. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.

5. 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.

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

1. Научите ваших детей уважать собеседников в Интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернете и в реальной жизни;
2. Скажите им, что никогда не стоит встречаться с друзьями из Интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
3. Объясните, что **далеко не все, что можно увидеть в Интернете – правда**. При сомнениях, пусть лучше уточнит у вас.

10. Компьютер с подключением к Интернету должен находиться в общей комнате.

11. Приучите себя знакомиться с сайтами, которые посещают ваши дети.

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

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!
4. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari!

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.

7. Если хочешь скачать картинку или мелодию, но тебя просят отправить смс – не спеши! Сначала проверь этот номер в Интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

8. Не используйте в качестве паролей набор цифр: 1234, дату вашего рождения и т.п. «Легкие» пароли быстро взламываются, и Вы можете стать жертвой злоумышленников. Не передавайте свой пароль посторонним лицам.

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.

Заключение

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 ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки.

Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к скрытым угрозам.

Работая с Интернетом, соблюдая все рекомендации по безопасности, мы во многом реализовали данный проект. Тем самым подтвердив нашу гипотезу: «Интернет и дети - друзья», если использовать его, соблюдая правила безопасности.

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

Сфера применения (практическая значимость проекта)

Данный проект может быть реализован как дополнительный курс по изучению темы «Информационная безопасность», так и как основной курс по данной теме в дистанционной форме.

Литература

1.Домбровский В., Ломтев И., Городбин А. Проект «Мы в интернет-безопасности» // Молодой ученый. — 2016. — №8.1. — С.

2.http://stopcrack.narod.ru/- сайт посвящен всем тем, кто интересуется проблемами компьютерной безопасности в интернет.

3.http://www.compdoc.ru/secur/internet/securpolicy/glava5_2.shtml- сайт посвящен Политике безопасности при работе в Интернете.

4.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

5. Приветствие Министерства образования и науки РФ участникам Единого урока безопасности в сети

6. Единый урок по безопасности в сети – http://mosmetod.ru/urok-bezopasnosti-v-seti-internet.html

7. В рамках Единого урока по безопасности в сети проводится Международный квест по цифровой грамотности среди детей и подростков "Сетевичок" - http://kvestsetevichok.ru/

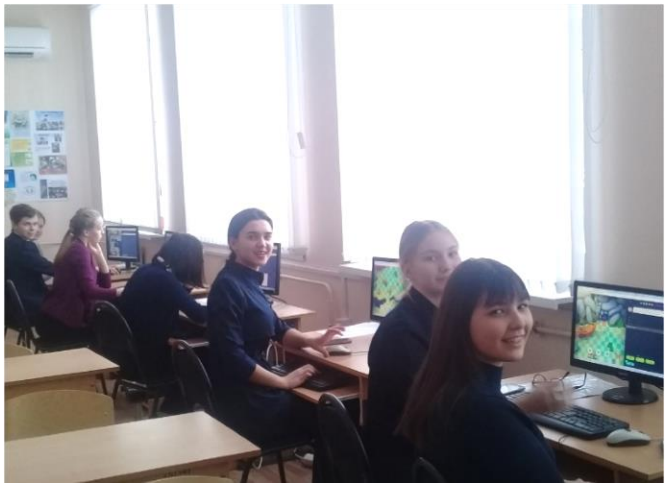
8. Безопасность школьников в сети Интернет - https://www.youtube.com/watch?v=9OVdJydDMbg&feature=youtu.be

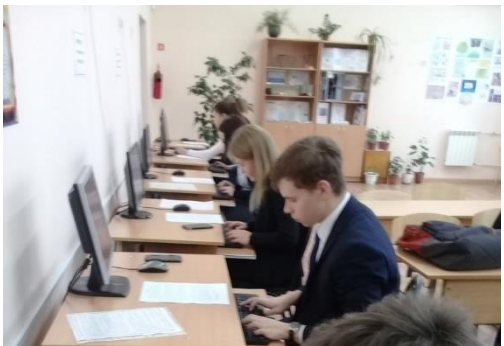
9. Социальный ролик "Безопасный интернет детям" - https://www.youtube.com/watch?v=MtoFtrgO4VQ, https://www.youtube.com/watch?v=pEN0U8VhGTs,

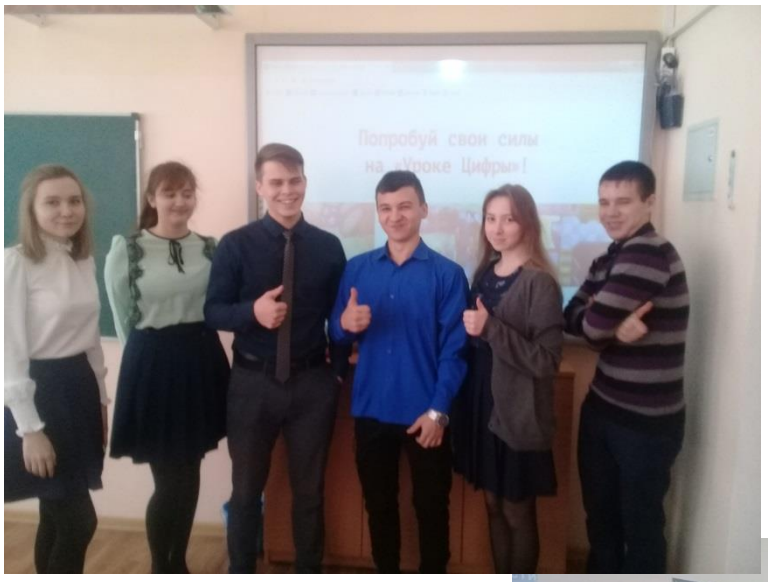
https://www.youtube.com/watch?v=33_NpShyx6s,
https://www.youtube.com/watch?v=dIecaaaVNoU,
https://www.youtube.com/watch?v=Iv1H--114IE,
https://www.youtube.com/watch?v=WdqplwEx4IQ.
10. Всероссийский онлайн-чемпионат «Изучи интернет – управляй им!» - http://интернет-чемпионат.рф/
11. https://schoolkrskluch.02edu.ru/school/about/information-security/

Приложение 1

Фотоотчет

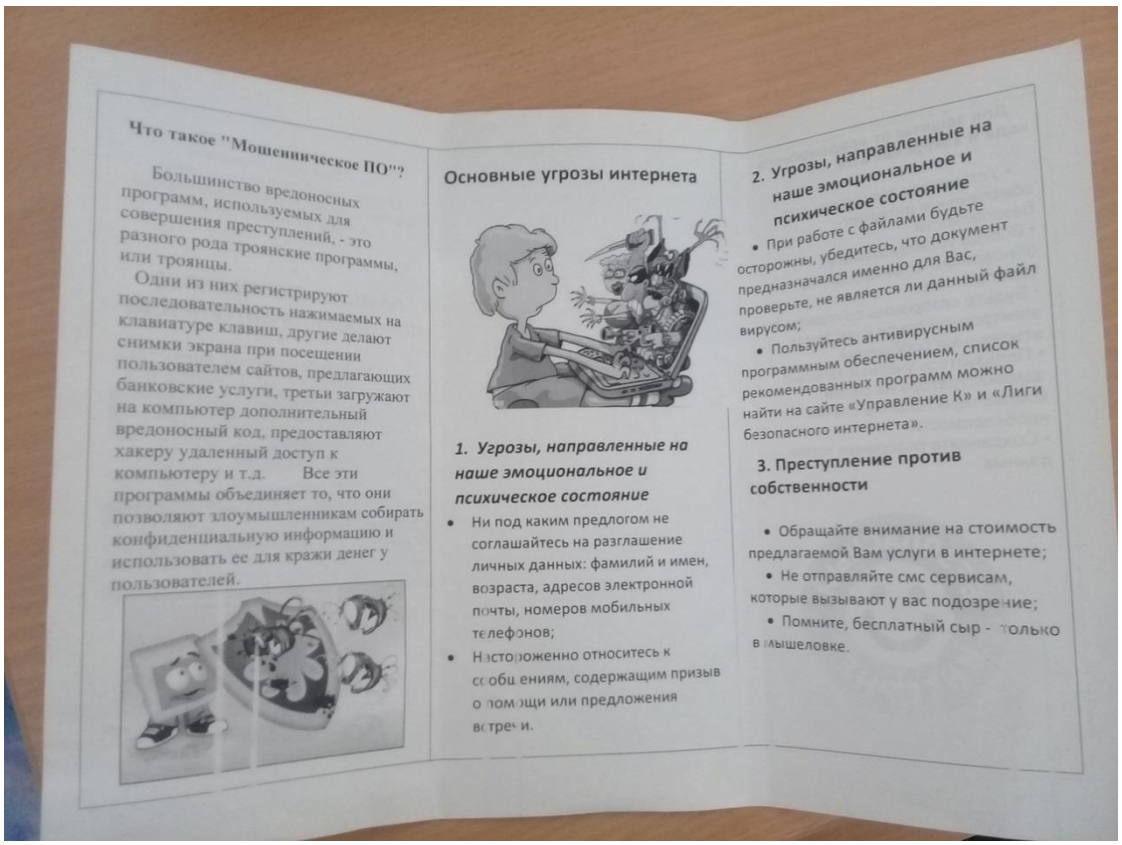






Приложение 2

Буклет и памятки



Что такое "Мошенническое ПО"?

Большинство вредоносных программ, используемых для совершения преступлений, - это разного рода троянские программы, или троянцы.

Одни из них регистрируют последовательность нажимаемых на клавиатуре клавиш, другие делают снимки экрана при посещении пользователем сайтов, предлагающих банковские услуги, третьи загружают на компьютер дополнительный вредоносный код, предоставляют хакеру удаленный доступ к компьютеру и т.д. Все эти программы объединяет то, что они позволяют злоумышленникам собирать конфиденциальную информацию и использовать ее для кражи денег у пользователей.

Основные угрозы интернета

1. Угрозы, направленные на наше эмоциональное и психическое состояние

- Ни под каким предлогом не соглашайтесь на разглашение личных данных: фамилий и имен, возраста, адресов электронной почты, номеров мобильных телефонов;
- Настороженно относитесь к сообщениям, содержащим призыв о помощи или предложения встречи.

2. Угрозы, направленные на наше эмоциональное и психическое состояние

- При работе с файлами будьте осторожны, убедитесь, что документ предназначался именно для Вас, проверьте, не является ли данный файл вирусом;
- Пользуйтесь антивирусным программным обеспечением, список рекомендованных программ можно найти на сайте «Управление К» и «Лиги безопасного интернета».

3. Преступление против собственности

- Обращайте внимание на стоимость предлагаемой Вам услуги в интернете;
- Не отправляйте смс сервисам, которые вызывают у вас подозрение;
- Помните, бесплатный сыр - только в мышеловке.