

**Муниципальное общеобразовательное учреждение
«Средняя общеобразовательная школа №1»
города Магнитогорска**



**Методические рекомендации по
разработке
и проведению обучающего семинара
для классных руководителей
«Интернет изнутри»**

Разработчики:

Юдина Е.А. – педагог-психолог,
Фролова Н.Н. – социальный педагог.

г. Магнитогорск

2020 г.

Обучающий семинар для классных руководителей 7-8 классов

по теме: «Интернет изнутри»

Цель: ознакомить педагогов с различными опасностями в сети Интернет и показать, как можно формировать навыки поведения в информационном обществе с целью обеспечения информационной безопасности.

План работы

1. Вводная часть.
2. Нормативно-правовая база по обеспечению информационной безопасности обучающихся.
3. Концептуальные и методологические основы медиаобразования и медиабезопасности.
4. Технология организации медиабезопасности в образовательном учреждении. Опасности, которые подстерегают обучающихся в сети Интернет (причины и угрозы).
5. 10 мифов про Интернет. Памятка для родителей.
6. Интересные факты об Интернете. Упражнение № 1. «Сказка о золотых правилах безопасности в сети Интернет». Памятка для детей.
7. Упражнение № 2. «Реклама в сети Интернет».
8. Упражнение № 3. «Достоинства и недостатки сети Интернет».
9. Упражнение № 4. «Ребусы про глобальную сеть Интернет».
10. Упражнение №5. «Заполни пустоту».
11. Подведение итогов.

Ход семинара

Здравствуйте, уважаемые коллеги. Мы с Вами собрались чтобы обсудить вопросы информационной безопасности в глобальной сети Интернет. Тема нашего обучающего семинара: «Интернет изнутри».

Вводная часть.

(Фролова Н.Н.)

Современное общество основано на использовании информации и знаний. Сегодня невозможно игнорировать повсеместное распространение медиа, различных форм информационных и коммуникационных технологий, или их влияние на нашу частную, экономическую, политическую и общественную жизнь.

Левада-Центром накоплены данные о том, откуда россияне получают информацию, какие каналы информации и с какой используют. Телевидение на сегодняшний день остается главным источником информации для россиян (на начало 2018 года 91% населения отметили, что «хотя бы раз в неделю» или чаще смотрят новости по телевизору). В самой молодой возрастной группе интернет обогнал телевидение как источник информации (более 70% подростков предпочитают получать информацию из интернета).

Почти половина населения (46%) сомневается в своей способности распознать ложь и правду в информационных потоках. Полностью уверены, что могут разобраться в этом лишь 9%. Не существует универсальных комплексных решений, которые могли бы обеспечить аудиторию только качественным контентом. В данном контексте проблема медиабезопасности становится все более актуальной. Как следствие, целесообразно рассматривать организацию медиабезопасности в образовательной организации как одну из ключевых задач медиаобразования.

Данные методические рекомендации с учетом требований действующего законодательства о безопасности детей.

Нормативно-правовые основы медиабезопасности в образовательных организациях

(Фролова Н.Н.)

В современном обществе медиабезопасность обучающихся обеспечивается комплексом законодательных актов.

На международном уровне безопасность в медийном пространстве гарантируется комплексом нормативно—правовых документов:

- Европейская декларация о свободе обмена информацией в интернете 2003 г.;
- Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете; Решение Европейского парламента и Совета ЕС № 276/1999/ о принятии долгосрочного плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносным содержимым в рамках глобальных сетей.

В Российской Федерации информационная безопасность детей, защита их физического, умственного и нравственного развития также обеспечиваются рядом нормативно-правовых актов.

- В соответствии со статьей 14.1 Федерального закона ««Об основных гарантиях прав ребенка в Российской Федерации»» в целях содействия физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и формированию у них навыков здорового образа жизни органы государственной власти Российской Федерации, органы местного самоуправления в соответствии с их компетенцией создают благоприятные условия для осуществления деятельности организаций, образующих социальную инфраструктуру для детей (включая места для их доступа к сети интернет).

- В Федеральном закон № 390-ФЗ «О безопасности» определены направления деятельности по обеспечению безопасности.

- В Федеральном законе № 43 -ФЗ ««О защите детей от информации, причиняющей вред их здоровью и развитию»» представлен перечень информации, запрещенной для распространения среди детей.

На региональном уровне были созданы письма Министерства образования и науки Челябинской области «Об организации работы по медиабезопасности» (Письмо от 27.12.2012 № 15/10422 , Письмо от 12.03.2013 № 05/1633). Безопасность работы с интернетом, обеспечивает приказ Министерства образования и науки Челябинской области от 06.02.2007 № 01 110 «О внедрении контентной фильтрации доступа образовательных учреждений Челябинской области, подключаемых к сети интернет».

Концептуальные и методологические основы медиаобразования и медиабезопасности

Современные исследователи в сфере медиа рассматривают медиабезопасность, как деятельность, направленная на защиту интересов гражданского общества от появления и распространения недостоверной информации в сети интернет, способной негативно повлиять на социальные процессы. В узком смысле медиабезопасность - это деятельность по обеспечению личной безопасности пользователя в сети и интернет, которая позволяет ему не только распознавать недостоверную информацию, но и предотвращать распространение вредоносной информации.

С целью минимизации угроз со стороны медиа в исследованиях ученых определяются пути решения проблемы медиабезопасности. На сегодняшний день определены основная теоретическая модель медиабезопасности – медиаобразование.

Медиаобразование как направление в педагогике, выступающее за изучение школьниками закономерностей массовой коммуникации (прессы, телевидения, радио, кино, видео, и т. д.).

Основные задачи медиаобразования: подготовить новое поколение к безопасной жизни в современных информационных условиях, к критическому восприятию различной информации, научить понимать цели и намерения авторов любой информации, осознавать последствия воздействия на психическое здоровье человека, овладевать способами общения на основе невербальных форм коммуникации. Позитивным результатом медиаобразования следует считать медиакомпетентность личности «совокупность ее мотивов, знаний, умений, способностей, способствующих выбору, использованию, критическому анализу, оценке, созданию и передаче медиа текстов в различных видах, формах и жанрах, анализу сложных процессов функционирования медиа в социуме».

Таким образом, медиаобразование выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, значит, является одним из необходимых условий медиабезопасности. Медиаграмотность определяется в международном праве как «грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг» (Рекомендация Комитета министров государствам членам Совета Европы по расширению возможностей детей в новой информационно коммуникационной среде от 27.09.2006).

**Технология организации медиабезопасности в образовательном учреждении.
Опасности, которые подстерегают обучающихся в сети Интернет (причины и угрозы)
(Юдина Е.А.)**

Давайте рассмотрим возможности и опасности сети Интернет:

Доступность и возможности открытой среды (сеть Интернет)	Опасности и риски для пользователей, в т.ч. детей и подростков
Поиск необходимой информации в сети Интернет (Интернет-источник информации)	Психические и психологические расстройства (Интернет-зависимость) Психологическое давление на психику детей и подростков (манипуляции)
Работа, бизнес (Интернет-магазины, онлайн-переводы, реклама)	Контентные риски (сайты, содержащие противоправную и неэтичную информацию) – пропаганда анорексии, суицида и т.д.
Образовательные ресурсы, дистанционное обучение	Азартные игры на деньги (онлайн)
Развлечения (фото, музыка, фильмы, анекдоты, игры...)	Заражение ПК вирусами и уничтожение информации
Средство общения на расстоянии в разных точках страны и мира (социальные сети)	Информация может быть недостоверной, потому что нет редакторов и корректоров
Интернет – возможность справиться с одиночеством (сайты знакомств, форумы)	Хищение персональных данных, паролей и другой информации
Отдых (бронирование авиабилетов, отелей и т.д.)	Интернет-знакомства могут интернет-хулиганством (преследование, буллинг, оскорбления)

С каждым годом дети и подростки все больше времени проводят в Интернете. По данным исследования Фонда Развития Интернет (2013), в среднем 89 % российских детей 12–17 лет, пользующихся Интернетом, выходят в Сеть каждый или почти каждый день в любое время и в любом месте, где есть такая возможность. По сравнению с данными 2010 г. число таких подростков увеличилось. Отметим, что ежедневно пользуется Интернетом лишь половина всех опрошенных взрослых — родителей подростков.

Как часто вы пользуетесь интернетом?

Каждый или почти каждый день

1—2 раза в неделю

1—2 раза в месяц

Реже

Не пользуюсь интернетом



53%

22%

5%

3%

17%



89%

9%

1%

1%

0%

Каждый десятый подросток пользуется Интернетом 1–2 раза в неделю, реже бывают в он-лайн лишь единицы. В выходные дни в Интернете от 5 до 8 часов проводит каждый шестой школьник и только каждый 25-й взрослый.

Психологи выделяют несколько **причин, почему же дети уходят в Интернет:**

- Лень
- Одиночество, отсутствие друзей
- Игры заманивают
- Кажущаяся легкость в общении
- Проблемы в семье
- Неумение занять себя
- Слишком много свободного времени

Почему Интернет затягивает?

Психологи говорят:

«Дети признались, что виртуальная жизнь дает им самое главное - в ней они могут быть теми, кем хотят быть. А если им что-то не нравится – они могут просто нажать кнопку выхода».

Ребенок, включенный в процесс познания, оказывается незащищенным от потоков информации. Давайте задумаемся, почему мы не оставим ребенка с незнакомым человеком? Правильно, мы не знаем его целей, а с неизвестной информацией в Интернете, мультипликационным фильмом, книгой, авторов и целей которой мы не знаем, оставляем. Не комментируем, не обсуждаем, не возвращаемся к увиденному и прочитанному. Мы учим детей защищаться от плохого человека, вести себя в критической ситуации, возникающей в период стихийных бедствий. Но, не учим главному!...

Недостоверная, неэтичная, непристойная, деструктивная информация, исходящая от основных источников информации, а также от средств информационного воздействия, оказывает определенное влияние на получателя информации – ребенка. Когда мы радуемся, что ребенок, сидящий за компьютером, рядом с нами, мы не задумываемся над тем, что ребенок виртуально далеко от нас. Кто в этот момент управляет им? Кто манипулирует?

Мы, взрослые, отстаем от информационной грамотности детей, не подозревая, какой опасности они подвергаются. Многие не знают и не интересуются содержанием сайтов, которые посещает ребенок, в какие компьютерные игры играет, какую музыку слушает.

И так, какие же существуют **Угрозы, подстерегающие ребенка в Глобальной сети?**

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержанием!

1. Депрессивные молодежные течения

Ребенок может поверить, что шрамы – лучшее украшение, а суицид – всего лишь способ избавления от проблем.

2. Порнография

Опасна избыточной информацией и грубым, часто извращенным, натурализмом. Мешает развитию естественных эмоциональных привязанностей.

3. Наркотики

Интернет пестрит новостями о “пользе” употребления марихуаны, рецептами и советами изготовления “зелья”.

4. Сайты знакомств, социальные сети, блоги и чаты

К сожалению уже было много случаев, когда педофилы выдавали себя за одного из детей или выдуманных персонажей, чтобы войти к ним в доверие и завести пошлые или открыто сексуальные беседы с ними или даже договориться о личной встрече.

5. Секты

Виртуальный собеседник не схватит за руку, но ему вполне по силам “проникнуть в мысли” и повлиять на взгляды на мир.

6. Экстремизм, национализм, фашизм

Все широкие возможности Интернета используются представителями экстремистских течений для того, чтобы заманить в свои ряды новичков.

Дети и подростки, в силу возраста не обладают способностью фильтровать качество информации. У них не сформированы критерии различия, они не видят опасностей и не осознают рисков, принимают всю информацию, не понимая, что она может быть противозаконной, неэтичной, недостоверной, вредоносной. Информационное воздействие становится главным рычагом управления людьми.

Педагоги способны быть проводниками детям в мир знаний, но, в то же время не допустить, чтобы неустойчивая подростковая психика подвергалась информационному насилию, подготовить сознание детей к противодействию негативным информационным воздействиям, формировать информационную безопасность (навыки критического мышления), развивать способности к самоблокированию информации, учить отличать качественную информацию от некачественной. Проблема защиты детей от информации напрямую связана с темой образования.

Формирование у обучающихся умений работать с информацией и, следовательно, умений обеспечения ее безопасности, является важной задачей образования.

Что такое **информационная безопасность**? 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.

Мы считаем, что самым эффективным механизмом информационной безопасности несовершеннолетних может стать работа по формированию осознанного самостоятельного умения учащихся выбирать безопасную информацию. Лучший фильтр, который может обеспечить безопасность ребенка в сети и решить многие другие проблемы, – в голове самого ребенка, а взрослому нужно только настроить этот фильтр.

Необходимо учитывать, что в настоящее время информационная безопасность – важнейший компонент национальной безопасности, информационная безопасность становится одним из элементов национальной, общественной и личной безопасности. Соответственно, приступая к планированию занятия по информационной безопасности, важно помнить, что задача педагогов и родителей не закрыть детям мир информации, а научить брать из этого многогранного мира лучшее!

10 самых распространенных мифов о детских онлайн-рисках (ЮдинаЕ.А.)

(журнал «Дети в информационном обществе», №9, издается Фондом Развития Интернет с 2009 года, научная поддержка: факультет психологии МГУ имени М.В. Ломоносова и Федеральный институт развития образования МОН РФ. Информационная поддержка: Министерство образования и науки Российской Федерации. <http://detionline.com/assets/files/journal/9/world-research9.pdf>)

1. Цифровые дети знают все

Утверждение, что дети знают о компьютерах и интернете больше, чем их родители, — сильное преувеличение. Только 36% школьников в возрасте от 9 до 16 лет согласились с утверждением «Я знаю об интернете больше, чем мои родители». 31% опрошенных сказали, что это «отчасти правда», два из трех 9-10-летних школьников отметили, что это «совсем не правда». За разговорами о цифровых аборигенах утрачивается осознание необходимости совершенствовать компьютерные навыки младших школьников.

2. Сегодня каждый создает собственный контент

В течение месяца, предшествовавшего опросу, только каждый пятый школьник использовал сайты обмена файлами или создал аватар и лишь половина из них что-либо написала в блоге. Чем младше дети, тем менее они склонны создавать сами. И поскольку социальные сети облегчают доступ к массовому контенту, дети их используют главным образом именно для чтения и скачивания, а не для создания собственных текстов.

3. Дети до 13 лет не могут использовать социальные сети, поэтому беспокоиться не о чем

С 38 процентами 9-12-летних школьников, имеющих профиль в социальных сетях, становится очевидно, что возрастные ограничения здесь не работают. Дети при регистрации указывают более старший возраст — и все. И даже если провайдер установил соответствующие настройки по безопасности, малолетних пользователей все равно невозможно вычислить. Некоторые из младших школьников открывают свободный доступ к своему профилю, в котором сообщают личные данные, некоторые общаются с незнакомыми им в реальной жизни людьми. Что с этим делать? Следует ли провайдерам еще усилить системы безопасности или же снять возрастные ограничения, чтобы не приучать детей лгать - этот вопрос все еще остается открытым.

4. Все смотрят в сети порно

Масштаб этого явления совсем не так велик, как многие думают. В течение года, предшествовавшего опросу, около четверти школьников смотрели порно в сети или в оффлайне и только один из семи делал это именно в сети (среди подростков эта цифра составила четверть). Даже если учесть, что далеко не каждый опрошенный сообщил о себе правду, очевидно, что шум в прессе вокруг порнографии в сети не имеет под собой достоверных оснований.

5. В сети есть киберхулиганы (буллеры) и жертвы

Большинство (60%) тех, кто занимался буллингом, сам был его жертвой. Причем не важно, в онлайн это было или в реальной жизни. В сети доля таких детей составляет 40%. И те, кто сам занимается буллингом, и их жертвы имеют общие черты — такие дети, как правило, особенно ранимы и психологически уязвимы, чем и объясняется склонность к порочному поведению.

6. В сети дети общаются с незнакомцами

И этот миф не подтвердился — 87% школьников сказали, что общаются с теми, кого знают в реальной жизни. 4 из 10 опрошенных сообщили, что среди их онлайн-знакомых есть люди, которых они знают только по переписке, однако они являются друзьями их родственников или знакомых. Однако четверть школьников общается в онлайн с людьми, которые не принадлежат к их социальному кругу, а 9% признались, что встречались в реальной жизни с теми, с кем познакомились по интернету. Мало кто из европейских детей ходил на эту встречу в одиночестве или встречался с кем-то старше себя. Реальный негативный опыт такого общения имели лишь 1% опрошенных. Такие встречи редки, но опасны, поэтому важно оградить детей от них, не ограничивая при этом те широкие возможности для общения, которые предоставляет интернет.

7. Риски реальной жизни перекочевали в онлайн

Наши данные подтверждают это утверждение, но только отчасти. Дети, которые сообщают о том, что подвержены различным видам рисков в реальной жизни, более склонны сталкиваться с ними и в онлайн. Однако нельзя сказать, что те, кто меньше встречается с рисками реальной жизни, огражден от них и в виртуальном мире. Онлайн-риски непредсказуемы, и мы по-прежнему не знаем все те факторы, которые могут их усиливать. Важно учитывать и те и другие виды рисков применительно к индивидуальной ситуации.

8. Поместите компьютер в общую комнату и многие проблемы решатся сами собой

Почти половина (53%) школьников выходят в сеть, бывая у друзей, 49% — в своей комнате и 33% — через мобильные телефоны и другие портативные устройства. Так что этот совет уже устарел. Лучше посоветовать родителям время от времени обсуждать с детьми, что и как они делают в сети, или выходить в интернет вместе с ними.

9. Компьютерная грамотность снижает онлайн-риски

Как раз наоборот — более высокий уровень компьютерной грамотности ассоциируется с большим риском. Все просто — чем больше дети используют компьютер, тем выше цифровая грамотность. И чем искуснее школьник использует компьютер, тем шире его возможности, а более широкие возможности связаны с увеличением риска. Почему возможности и риски взаимосвязаны? Во-первых, защищен влечений, он невольно сталкивается с рисками, поскольку онлайн-среда в принципе предназначена не для детей (только один из факторов риска — избыток всплывающих окон). Но в то же время с опытом работы в сети появляется все больше навыков, позволяющих снизить риски.

10. Дети могут обойти системы защиты

На самом деле только 28% опрошенных школьников сказали, что они могут изменить настройки фильтров. В большинстве своем дети считают, что то, что делают их родители в отношении их интернет-безопасности, полезно (27% — что «очень полезно», 43% — «немного полезно»). Тем не менее, почти половина школьников считает, что действия родителей ограничивают их свободу в интернете, а почти треть в той или иной степени игнорирует родительские запреты (7% — «часто игнорируют», 29% — «иногда игнорируют»).

Памятка для родителей

Десять правил безопасности для детей в Интернете*



1. Посещайте сеть вместе с детьми, поощряйте их делиться опытом использования Интернета
2. Научите детей доверять интуиции - если их в Интернете что-либо беспокоит, пусть сообщают вам
3. Помогите ребенку зарегистрироваться в программах, требующих регистрационного имени и заполнения форм, не используя личной информации (имя ребенка, адрес электронной почты, номер телефона, домашний адрес). Для этого можно завести специальный адрес электронной почты
4. Наставляйте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки
5. Объясните детям, что в Интернете и реальной жизни разница между правильным и неправильным одинакова
6. Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают
7. Скажите детям, что далеко не все, что они читают или видят в Интернете, - правда, приучите их спрашивать вас, если они не уверены
8. Контролируйте действия детей с помощью современных программ, которые отфильтруют вредное содержимое, помогут выяснить, какие сайты посещает ребенок и что он там делает
9. Наставляйте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ - кража
10. Научите детей уважать других, убедитесь, что они знают о том, что правила хорошего тона действуют везде - даже в виртуальном мире



Безопасный интернет!

Памятка родителям для защиты ребенка от нежелательной информации в сети

Объясните своему ребенку, что:

- при общении использовать только имя или псевдоним (ник);
- номер телефона, свой адрес, место учебы нельзя никому сообщать;
- не пересылать свои фотографии;
- без контроля взрослых не встречаться с людьми, знакомство с которыми завязалось в Сети.

Обязательно расскажите о правах собственности, о том, что любой материал, выставленный в Сети, может быть авторским. Неправомерное использование такого материала может быть уголовно наказуемым.

Поясните, что в сети, несмотря на кажущуюся безнаказанность за какие-то проступки, там действуют те же правила, что и в реальной жизни: хорошо - плохо, правильно - неправильно.

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

Научите детей следовать нормам морали, быть воспитанными даже в виртуальном общении.



Внимательно относитесь к вашим детям!

Интересные факты об Интернете.

(ЮдинаЕ.А.)

1. Смайликам уже более тридцати лет.

Первым, повсеместно используемым смайликом был символ :-) который говорил о веселом, игривом тоне высланного сообщения. Его автором считается американский информатик Скотт Фальман, который первым выслал смайлик в послании к Интернету в 1982 году.

2. Просмотреть все ролики на YouTube невозможно.

Каждую минуту на сервисе YouTube появляется около ста часов новых видеоматериалов. Чтобы посмотреть все фильмы, которые добавили на этот сайт только в течение одного дня, вам понадобится более шестнадцати лет.

3. Интернет под облаками.

При подъеме на гору Эверест, вы можете пользоваться высокоскоростным доступом в сеть. Более того, Интернет доступен даже на вершине самой высокой горы в мире.

4. Веб-камера появилась благодаря... кофе.

Первая в истории веб-камера была установлена в Кембриджском университете в 1991 году на... кофеварке. Благодаря ей работники университета могли подсмотреть сварился ли их кофе или нет. Ленъ — это двигатель прогресса :-) Устройство, которое записывало изображение с разрешением 128x128 пикселей, подключили к сети в 1993 году. Восемь лет спустя, знаменитая кофеварка была продана на интернет-аукционе за сумму около 204 000 рублей.

5. Ключи от Интернета.

Это звучит почти невероятно: в мире есть семь очень тщательно отобранных человек, которые хранят так называемые «ключи от Интернета». Это электронные карты, содержащие шифр, который позволяет в буквальном смысле слова перезагрузить весь Интернет. В случае глобальной хакерской атаки «стражи Интернета» будут немедленно доставлены на военную базу в США, где они активируют свои ключи и тогда глобальная сеть будет отключена.

6. Быстро растущая популярность.

Через четыре года после изобретения Интернета им пользовалось около 50-т миллионов человек. Для сравнения, на создание такой аудитории пользователей телефонов понадобилось 75 лет, радио — 38 лет, телевизоров — 13 лет, а игры AngryBirds, внимание, всего 35 дней.

7. Тонны спама.

Во всем мире существует почти четыре миллиарда действующих электронных почтовых ящиков. Ежедневно с них отправляется около 190 миллиардов сообщений. Согласно проведенным исследованиям, 80 процентов этих сообщений может быть простым спамом. Интересна также история появления слова спам, которое берет свое начало от названия торговой марки мясных консервов «Spam», ставшей известной своей назойливой рекламой.

Упражнение 1. «Сказка о золотых правилах безопасности в сети Интернет»

Я расскажу сегодня сказку,
Про волшебство, про интернет,
Про то, как люди без оглядки,
Бросают все в обмен на сеть.

Представьте... В некотором царстве, Интернет - государстве жил-был Смайл-царевич-Тьютор-Королевич, который правил славным городом СоцОБРАЗом. И была у него невеста – прекрасная Смайл-царевна-Он-лайн-Королевна, день и ночь проводившая в виртуальных забавах. Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город СоцОБРАЗ, заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети. Погоревал – да делать нечего: надо спасать невесту. Собрал он рать королевскую-СоцОбразову – дружину дистанционную и организовал "Регату" премудрую. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать. Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: порно-сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья-разбойника, товары заморские купцов шоповских, сети знакомств-зазывалок русалочьих... Как же найти-отыскать Смайл-царевну? Крепко задумался Тьютор-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясиину непролазную. Долго бродил он, отбиваясь от реклам шоповских зазывающих и спамов завлекающих. И остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне, мохом заросшим: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.



Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказания безопасные!»




Всегда помни своё Интернет-королевское имя (E-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)!





Не поддавайся ярким реклам-указателям и не ходи тропками путанными на подозрительные сайты: утопнуть в трясиине можно!




Если пришло письмо о крупном выигрыше – это «Лохотрон-грамма»: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах – в «Регате...», например!

 Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!

 Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы Web 2.0: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званых!

 Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!

 Не скачивай нелицензионные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернет!

Залилась сочувственными слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего СоцОБРАЗа, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образовательные.

Информационная памятка для обучающихся о безопасном поведении и использовании сети Интернет (Фролова Н.Н.)

(В соответствии с письмом Министерство образования и науки Российской Федерации, Департамент государственной политики в сфере общего образования от 14 мая 2018 г. № 08-1184 «О направлении информации»).

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в Сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться на твоём персональном компьютере
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением
5. Ограничь физический доступ к компьютеру для посторонних.
6. Используй внешние носители информации, такие как флешка, Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников.
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд WESA, что обозначало словосочетание Wireless Fidelity ””, которое переводится как « беспроводная точность »

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура Wi-Fi. Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает « высокая точность »

Да, бесплатный интернет доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие то номера
2. Используй и обновляй антивирусные программы и брандмауер.
Тем самым ты обезопасишь себя от закачки вируса на твоё устройство

3. При использовании Wi-Fi отключи функцию « Общий доступ к файлам и принтерам » . Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту

5. Используй только защищенное соединение через HTTPS, а не HTTP , е. при наборе веб адреса вводи именно « https:// »

6. В мобильном телефоне отключи функцию « Подключение к Wi Fi автоматически » . Не допускай автоматического подключения устройства к сетям Wi Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы

3. Защищай свою репутацию держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее

5. Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить твое местоположение

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Так же кроме передачи простого текста, имеется возможность передавать файлы

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге

2. Не указывай в личной почте личную информацию. Например, лучше выбрать « музыкальный_фанат@ » или « рок2013 » вместо « тема13 »

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS

4. Выбери сложный пароль. Для каждого почтового ящика должен быть с вой надежный, устойчивый к взлому пароль

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. Не открывай файлы и другие вложения в письмах, даже они пришли от твоих друзей. Лучше уточни у них, отправляли ли они эти файлы.

8. После окончания работы на почтовом сервисе перед закрытием После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Юдина Е. А.

Уважаемые коллеги, перед вами на столах представлены памятки, которые мы после прочтения сказки клеиваем обучающимся в дневники.

Памятка для детей



Дорогие коллеги! Сейчас мы хотели бы предложить вам несколько упражнений, которые можно проводить в рамках обучения информационной безопасности. (Юдина Е. А.)

Упражнение № 2. «Реклама» (Работа в группах.)

Интернет как среда и средство потребления не может существовать без рекламы. Многие бесплатные сервисы живут за счет рекламы, без которой не было бы ни бесплатных почтовых ящиков, ни социальных сетей, ни поисковиков.

Однако реклама в Интернете может быть довольно навязчивой и даже опасной. Например, она может содержать в себе искаженную или ложную информацию. Иногда баннеры могут вести на опасные сайты.

У вас на столах лежат листы с анонсами к сказкам, необходимо найти к какой именно сказке относится каждая реклама.

	АНОНС		Название произведения
1	То, что неспособна разрушить женская зависть, то, что неспособна сохранить братская преданность, то, что скрывают тьма и печальная мгла, способна воскресить настоящая любовь! Смотрите сагу о настоящей любви этой весной во всех кинотеатрах страны!	1	«Красная шапочка»
2	Она чиста и наивна! Он одинок и очень опасен! Этим летом их пути пересекутся под пологом темного леса. Сможет ли юность и храбрость противостоять силе и опыту? Вы узнаете во всех кинотеатрах страны!	2	«Три поросенка»
3	На что вы способны ради любви? Оставьте семью? Отказаться от самого дорогого? Вынести нестерпимую боль? Умереть ради любимого человека? Узнай истинную цену любви этой весной во всех кинотеатрах страны!	3	«Колобок»
4	Когда вы одиноки, когда никто не верит в ваш талант, когда весь мир против вас, приходится находить в себе силы, чтобы двигаться навстречу своей мечте! Однажды у вас вырастут крылья... И это случится очень скоро: этим летом во всех кинотеатрах страны!	4	«Волк и семеро козлят»
5	Он выходит на охоту... Его не остановят ни дубовая дверь, ни железный засов, ни каменные стены. Только сила братской любви способна победить зло во плоти! Три героя против кровожадного врага! Смотрите эпическую битву добра со злом этой весной!	5	«Лисичка-сестричка со скалочкой»
6	У нее было все, о чем может мечтать женщина: дом, семья, семеро детей. Однако враг обманом проник в ее дом и осквернил семейный очаг. Вы узнаете, на что способна мать ради своих детей! Этим летом во всех кинотеатрах страны!	6	«Сказка о мертвой царевне и семи богатырях»
7	Он молод и весел, ему тесно в стенах родительского дома. Впереди его ждут отвязные летние приключения: песни, танцы и, конечно, новые друзья! Однако всем ли можно довериться на этом пути? Какова цена беззаботности? Вы узнаете этой	7	«Золушка»

	зимой во всех кинотеатрах страны!		
8	Она мечтала о бальном платье и новых туфлях, а ей доставались обноски старших сестер. Она мечтала вальсировать со сказочным принцем, а ее заставляли танцевать со старой метлой. Но однажды ее жизнь кардинально изменится! Чудо случится этой зимой во всех кинотеатрах страны!	8	«Синяя борода»
9	Что делать, если у тебя за душой нет ни гроша, а хочется красивой и яркой жизни? Отчаянная авантюристка вступает в рискованную игру. Ты мне — я тебе! Однако к чему приводит жадность? Вы узнаете этой зимой во всех кинотеатрах страны!	9	«Гадкий утенок»
10	Выходя замуж, подумайте, хорошо ли вы знаете своего будущего супруга? Переступая порог старого замка, задайтесь вопросом, сможете ли вы вернуться назад? Открывая запретную дверь, решите, готовы ли вы увидеть то, что скрыто за ней? Этим летом вы узнаете самую страшную тайну во всех кинотеатрах страны!	10	«Русалочка»

На обратной стороне листа вы можете прочитать правильные ответы.

Правильные ответы:

1	«Сказка о мертвой царевне и семи богатырях»
2	«Красная Шапочка»
3	«Русалочка»
4	«Гадкий утенок»
5	«Три поросёнка»
6	«Волк и семеро козлят»
7	«Колобок»
8	«Золушка»
9	«Лисичка-сестричка со скалочкой»
10	«Синяя борода»

Вывод: к рекламе в Интернете стоит относиться осторожно: не нужно кликать на все красивые баннеры, а информацию, представленную в рекламных сообщениях, стоит перепроверять.

Упражнение № 3. «Достоинства и недостатки сети Интернет» (Командная игра).

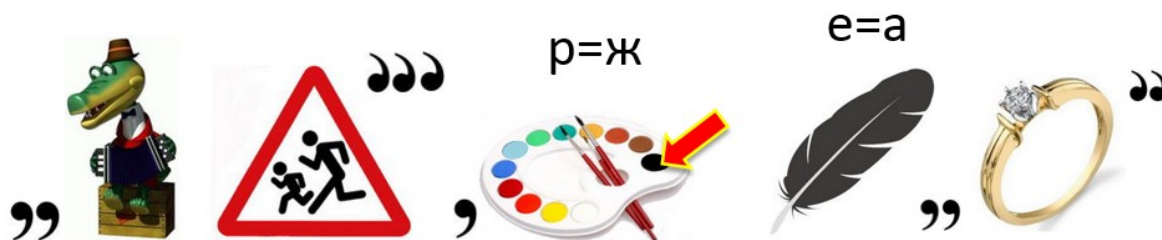
Команда из предложенных карточек выбирает достоинства воздействия компьютера и Интернета на ребёнка, а так же недостатки.

- Растет технически грамотным.
- Чувствует себя увереннее с любой техникой.
- Развивает логическое мышление.
- Увеличивает скорость реакции, принятие решения.
- Учится концентрировать внимание.
- Учится визуально воспринимать объекты.
- Получает возможность общаться с друзьями, живущими далеко.
- Имеет возможность получить любую нужную ему информацию.
- Ухудшение зрения.
- Электромагнитное излучение.

- Появление дерматитов различной сложности.
- Развитие сколиоза. Возникновение психологических проблем.
- Повышает состояние нервозности и страха при стремлении, во что бы то ни стало добиться победы.
- Содержание игр провоцирует проявление детской агрессии, жестокости.
- Обязывает ребенка действовать в темпе, задаваемом программой.
- Способствует развитию гиподинамии.

Как мы видим, существует как положительное, так и отрицательное воздействие компьютера и Интернета на ребёнка. Но это не говорит о 100%-ом запрете пользования Интернетом, просто всё должно быть дозировано и под строгим контролем взрослого.

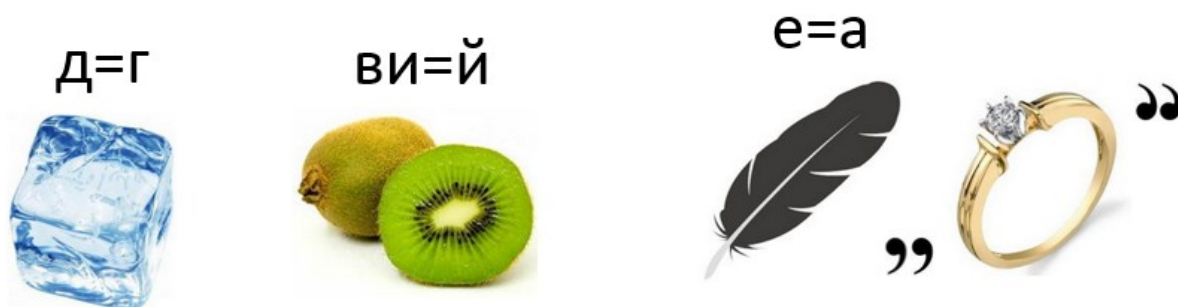
Упражнение № 4. «Ребусы про глобальную сеть Интернет».



Ответ: Надежный пароль



Ответ: Антивирусная программа



Ответ: Легкий пароль

--	--	--	--	--	--	--	--	--

1. Заменить первую букву слова на первую букву русского алфавита.

--	--	--	--	--	--	--	--	--

2. Заменить все буквы «е» на буквы «и».

--	--	--	--	--	--	--	--	--

3. Поменять местами пятую и седьмую буквы.

--	--	--	--	--	--	--	--	--

4. Поменять местами пятую и шестую буквы.

--	--	--	--	--	--	--	--	--

5. Заменить пятую букву слова на третью букву русского алфавита.

--	--	--	--	--	--	--	--	--

6. Заменить последнюю букву слова на букву «у».

--	--	--	--	--	--	--	--	--

7. Добавить букву «с» в конец слова.

--	--	--	--	--	--	--	--	--

Ответ: Антивирус

В конце игры важно обратить внимание игроков на обучающий момент игры, получить обратную связь, что являлось новым, а что учащиеся уже знали об интернет безопасности.

Упражнение № 4. «Заполни пустоту»

В конце нашего занятия мы предлагаем вам рассмотреть картинку: пустая комната.



Вопросы для рассуждения:

- какое впечатление у вас от этой фотографии?
- какие эмоции она вызывает?
- какие ассоциации появляются у вас, когда вы смотрите на эту пустую комнату?
- если бы вы оказались там, что бы вы сделали?
- можно ли жить в этой комнате?

Впечатление от этой фотографии могут быть как отрицательными: там пусто, неуютно, хочется заполнить чем-то; так и положительным: что-то новое, чистое, пространство для творчества.

Какую аналогию можно провести между этой фотографией и воспитанием детей, какие выводы сделать?

- Жизнь ребёнка не может быть пустой, она обязательно будет наполнена эмоциями, событиями. Без этого, как без мебели в комнате ребёнок жить не может.

-Если просто запретить ребёнку играть в компьютер, он будет ощущать пустоту (это касается не только освободившегося времени, ему будет не хватать ярких эмоций), и эту пустоту он попытается чем-то заполнить. Будет ли он её заполнять чем-то положительным или чем-то отрицательным, зависит и от родителей. Нужно направить ребёнка в правильное русло.

Сегодня и мы с вами постараемся «заполнить пустоту» нашего обучающего (ребёнка). Напишите, пожалуйста, те способы, которыми можно это сделать и прикрепите.

Варианты:

- ✓ внимание к ребёнку
- ✓ объятия
- ✓ интересные занятия
- ✓ посещение кружков
- ✓ посещение театра, кинотеатра
- ✓ посещение парков развлечения
- ✓ прогулки
- ✓ пикники
- ✓ рыбалки
- ✓ настольные игры
- ✓ хэндмэйд
- ✓ разговоры по душам

Надеюсь, что предоставленная информация, помогающая узнать об опасностях в Интернете и о том, как им противостоять, будет в дальнейшем полезна Вам и Вашим детям!

И в заключении хочется пожелать: ***Пусть путешествие по океану информации в Сети будет для вас приятным, увлекательным, полезным, а главное безопасным!***

Подведение итогов.

: <https://sch1mgn.educhel.ru/activity/rip/bib/post/617412>