**1. Общие сведения о методической разработке**

**Автор методической разработки:** Матвеец Ольга Владимировна, учитель математики БОУ г. Омска «Гимназия № 76»

 **Тема методической разработки:** Безопасность детей в сети Интернет.
 **Форма проведения:** собрание-практикум для родителей

 **Место проведения:** классный кабинет

 **Целевая группа:** родители обучающихся 8 класса

 **Цель занятия:** формирование внимательного и ответственного отношения родителей к безопасности детей в сети Интернет.

 **Задачи:**

- повысить родительскую медиаграмотность;

- привлечь родителей к решению проблемы безопасности детей в сети Интернет;

 - выделить совместно с родителями основные риски, с которыми могут столкнуться дети в сети Интернет;

 - выработать совместно с родителями правила, которые помогут защитить детей от опасностей сети Интернет.

 **Планируемые результаты:**

 В ходе практикума родители:

- узнают, какие риски существуют в сети Интернет и как обезопасить детей от этих рисков;

- смогут сформулировать основные правила безопасной работы детей в сети Интернет;

- осознают необходимость защиты детей от рисков, встречающихся в сети Интернет;

 **Регламент работы и формы организации деятельности родителей:** родительское собрание-практикум состоит из этапов: 1) мотивация на деятельность, 2) формулировка проблемы, 3) поиск способов решения проблемы, 4) решение проблемы, 5) рефлексия. Для организации деятельности родителей используется анкетирование, просмотр видеоролика, мозговой штурм, работа в группах. Результат работы: каждому родителю - буклет «Интернет безопасность вашего ребенка», детям - памятка «10 правил личной Интернет безопасности» в классный уголок.

 Время проведения практикума – 60 минут.

 **Ресурсы для проведения занятия:**

Приложение № 1 «Основные риски сети Интернет»

Приложение № 2 «Основные правила безопасности детей в сети Интернет»,

Приложение № 3 буклет для родителей «Интернет безопасность вашего ребенка»

Видеоролик

**2. Сценарный план проведения**

 **1. Мотивация на деятельность (10 мин)**

 **Цель:** выработать на личностном уровне готовность родителей к последующей деятельности.

*Вступительное слово учителя:*

*-* Уважаемые родители, сегодня мы с вами собрались, чтобы обсудить проблему медиаграмотности. Медиаграмотность – это грамотное использование детьми, родителями и их преподавателями инструментов, обеспечивающих доступ к информации. А поскольку большую часть информации современные дети черпают в сети Интернет, то и разговор наш пойдет о правилах поведения в сети Интернет.

*Школьный психолог предлагает родителям ответить на вопросы:*[3]

 1) Как вы думаете, в ваше отсутствие дети имеют доступ в Интернет?

 2) Сколько времени ваш ребенок проводит за компьютером?

 3) Каким сайтам и компьютерным играм он отдает предпочтение?

 4) Сколько друзей у ваших детей в социальных сетях?

 5) Есть ли среди этих друзей те, с которыми ваши дети не знакомы лично?

 6) Легко ли ваш ребенок принимает в друзья незнакомого человека?

 7) Знает ли ваш ребенок, что не следует встречаться с онлайн друзьями?

 8) Считаете ли вы, что Интернет представляет угрозу?

Психолог зачитывает ответы детей на аналогичные вопросы. Проводится сравнительный анализ ответов детей и родителей, делается вывод, о том, сколько времени ребенок проводит в Интернете, о том, что родители знают об общении ребенка в сети Интернет, о его предпочтениях.

**2. Формулировка проблемы (8 мин)**

**Цель:** сформулировать проблему, связанную с ответственностью родителей за безопасность детей в сети Интернет.

*Создание проблемной ситуации:* просмотр видеоролика[1].
 *Беседа учителя с родителями:*

- Видеоролик заканчивается фразой: «Первоочередная роль в информационной безопасности ребенка лежит на родителях и педагогах».

- Сформулируйте, какая существует проблема у родителей? (Как родителям обеспечить информационную безопасность ребенка?)

- Чтобы определить пути решения этой серьезной проблемы, нам надо будет во время нашей встречи:

1) Выделить основные риски, которые могут появляться у детей при работе в сети Интернет
2) Разработать свод правил, которые помогут защитить детей от опасностей в сети Интернет.

**3. Поиск способов решения проблемы (30 мин)**

**Цель**: выделить совместно с родителями основные риски, с которыми могут столкнуться дети в сети Интернет, и разработать правила, которые помогут защитить их.

Для выполнения работы родители делятся на 5 групп по 4-5 человек.

*Задание родителям № 1:*Во время просмотра видеоролика вы услышали о некоторых угрозах, подстерегающих наших детей в сети Интернет. Обсудите в группе и запишите на листах не менее 5 угроз, которые, на ваш взгляд, действительно подстерегают детей в сети Интернет (каждую угрозу записывайте на отдельном листе А4).

 Ответы родителей учитель фиксируется на доске по группам рисков.

- Как можете назвать каждую группу рисков? (Родители предлагают свои версии)

 *Появилось 5 групп Интернет – рисков[5*] *(Приложение 1)*

1. Потребительские риски
2. Электронные риски
3. Контентные риски
4. Коммуникационные риски
5. **Интернет-зависимость**

*Задание родителям № 2:* каждой группе разработать правила, как избежать один из Интернет-рисков (риски определяются путем жребия для каждой группы).

*Презентация* и обсуждение правил Интернет безопасности, разработанных каждой группой.

*Задание для родителей № 3:* используя *Приложение 2,* выберите 10 основных правил, которые необходимо соблюдать каждому ребенку в сети Интернет для личной безопасности. Коллективное обсуждение и оформление памятки для детей «10 правил личной Интернет безопасности». Размещение памятки в классном уголке.

**4. Решение проблемы (10 мин)**

*Выступление школьного психолога*[9]:

***-*** Как же помочь ребенку, если он уже столкнулся с Интернет-угрозой? Очень часто дети боятся признаться, что с ними приключилась беда. Но есть ряд признаков, по которым можно определить, что с ребенком что-то случилось:

* ребенок стал раздражительным, избегает общения;
* вы заметили на компьютере материалы сомнительного содержания;
* вы обнаружили среди Интернет-друзей ребенка новых знакомых, которых вы не знаете и о которых ребенок не может ничего рассказать.

- Если вас стало что-то настораживать в поведении ребенка, то Вам необходимо поговорить с ним или обратиться к психологам (например, в службу “[Дети Онлайн](https://www.sites.google.com/site/kyrsbez/29)“).

- Ни в коем случае не обвиняйте своих детей, даже, если они уже ведут общение со злоумышленником. Обратитесь в местное отделение правоохранительных органов, предварительно собрав весь материал и сделав его резервные копии. По возможности, временно ограничьте Ваших детей от использования потенциально опасных информационных систем

*Знакомство с памяткой* «Интернет безопасность вашего ребенка», подготовленной учителем *(Приложение 3).*

 **5. Рефлексия (2 мин)**

 ***Учитель:***

***-*** Мы с вамисовместно обсудили, какие риски встречаются нашим детям в сети Интернет, ответили на вопрос: «Как сделать Интернет безопасным для детей?»

 - Закончите, пожалуйста, предложения:

Теперь я знаю, что…

Теперь я могу ….
 Я обязательно ….

**Список использованных Интернет – источников**

1. <https://youtu.be/MSvVHqxnLFU-> до 1:15 мин.
2. http://www.oszone.net/6213/
3. <https://childrenssecurity-school9tihvin.eduface.ru/folders/post/405021>
4. https://infourok.ru/roditelskoe-sobranie-bezopasnost-detey-v-seti-internet-roditeli-i-deti-vmeste-v-internete-267333.html
5. <https://fcprc.ru/tvoy-bezopasniy-kibermarshrut/vidy-i-harakteristika-internet-riskov-i-ugroz-zhizni/>
6. <https://www.sites.google.com/site/kyrsbez/15>
7. <http://rkn.gov.ru/>
8. интернет – цензор - [http://icensor.ru/soft/](http://infourok.ru/go.html?href=http%3A%2F%2Ficensor.ru%2Fsoft%2F) - бесплатная программа).
9. [cyberpsy.ru](http://cyberpsy.ru/2011/01/internet-izdevatelstva/)

**3. Материально-технические условия**

1. Компьютер

 2. Проектор

 3. Колонки

 4. Экран

 5. Канцелярские принадлежности для каждой группы: маркеры, фломастеры, листы бумаги А3, А4.

 6. Распечатанные на каждую группу по одному экземпляру приложения № 1 «Основные риски сети Интернет», приложения № 2 «Основные правила безопасности детей в сети Интернет», 25 экземпляров приложения № 3 «Памятки для родителей»,

**4. Приложения**

*Приложение № 1*

*Основные риски сети Интернет*

 **Потребительские риски** - злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибермошенничества, и др.;

 **Электронные риски** - это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн- мошенничеству, спам-атаке, шпионским программам и т.д.

 **Контентные риски** - это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.-;

 **Коммуникационные риски** связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры, социальные сети, сайты знакомств, форумы, блоги и т.д.

 **Интернет-зависимость -** навязчивое желание войти в интернет и невозможность выйти из интернета, патологическая, непреодолима тяга к интернету, «оказывающая пагубное воздействие на бытовую, учебную деятельность.

*Приложение № 2*

 *Основные правила безопасности детей в сети Интернет*

1. Советуйтесь со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
2. Не пользуйтесь банковскими картами и платежными данными для совершения покупок без одобрения взрослых,
3. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
4. Убедитесь в безопасности сайта, на котором Вы планируете совершить покупку:
	* ознакомьтесь с отзывами покупателей,
	* избегайте предоплаты.
5. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
6. Используйте лицензионное программное обеспечение (оперативная система, антивирусная программа)
7. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой.
8. Создайте на компьютере несколько учетных записей, когда каждый пользователь сможет входить в систему независимо и иметь собственный уникальный профиль. Создавайте для работы надежные и защищенные пароли.
9. Помните, что далеко не все, что можно прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете.
10. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
11. Используйте только лицензионные программы и данные, полученные из надежных источников.
12. Регулярно делайте резервную копию важных данных.
13. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п)
14. Не рассказывайте никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
15. Если вы пользуетесь интернетом с помощью чужого устройства, то должны не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы.
16. Создайте загрузочный диск на случай повреждения данных на Вашем компьютере.
17. Никогда не разглашайте в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также не пересылайте интернет-знакомым свои фотографии;
18. Не встречайтесь с онлайн-знакомыми без разрешения или в отсутствии взрослого человека.
19. Нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
20. Научитесь правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем;
21. Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию.
22. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
23. Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.
24. Ограничьте возможность доступа к интернету только своим компьютером или компьютером, находящимся в общей комнате – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.
25. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в интернете.
26. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь.
27. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время «выпадет» из жизни интернет-сообщества.
28. В случае серьезных проблем обратитесь за помощью к специалисту.