Мероприятия проведенные в Согратлинской гимназии имени М. Махатилова по теме **«Безопасность в сети Интернет»**

1) Провели уроки в 9-11 классах на тему:

**«Безопасность в сети Интернет»**



**План урока по теме «Безопасность в сети Интернет»**

Задачи:

1. Ознакомить уч-ся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
2. Научить избегать этих угроз.
3. Рассказать о действиях, которые необходимо предпринять при столкновении с этими угрозами.
4. Освоить практические навыки работы в сети Интернет.

Литература и интернет-ресурсы:

1. Сайт [**http://content-filtering.ru/children/**](http://content-filtering.ru/children/)
2. Блинков И.А.: Безопасность детей и молодежи в сети Интернет
3. Брошюра «Безопасность детей в Интернете» изд. Microsoft

Программное обеспечение:

1. Microsoft Windows XP,
2. Microsoft Internet Explorer

**Ход занятия.**

**I. Орг. момент**

**II. Программы, позволяющие путешествовать по сети Интернет – браузеры (Internet Explorer, Opera, Firefox, и др.)**

Как пользоваться браузером (на примере Internet Explorer)

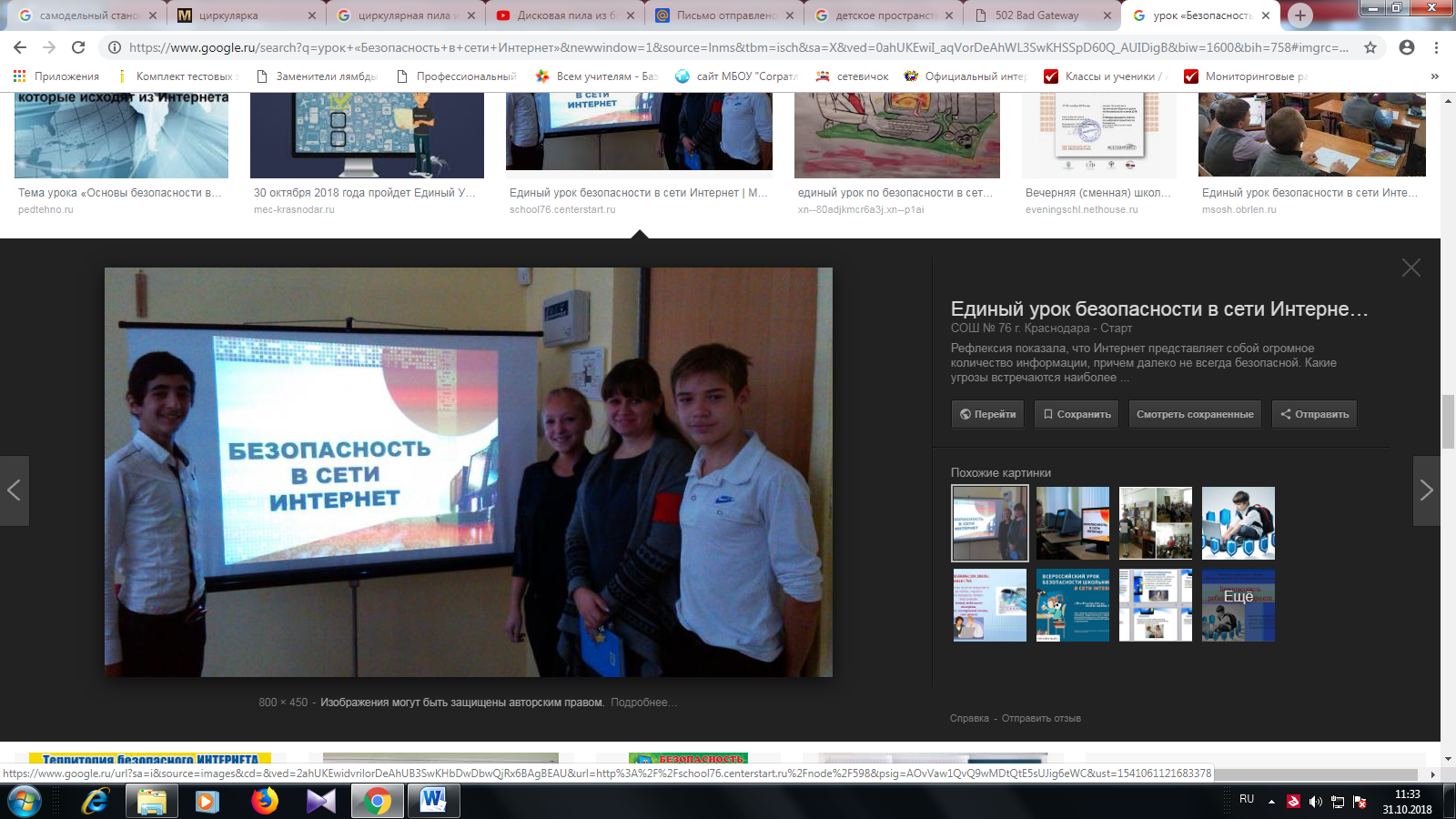
**Значение Интернет**

В Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями.

Но сеть Интернет скрывает и угрозы.

**Наиболее часто встречающиеся угрозы при работе в Интернет:**

1. Угроза заражения вредоносным программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы. Эти методы довольно часто используется хакерами для распространения троянских вирусов;
2. Доступ к нежелательному содержимому. Это насилие, наркотики, страницы подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию;
3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи;
4. Поиск развлечений (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег.
5. Неконтролируемые покупки.



Посещение сайта [**http://content-filtering.ru/children/**](http://content-filtering.ru/children/)

Чтение вступительной статьи на сайте

Переход по ссылке «Средние классы»

Чтение раздела «Вы должны это знать», и обсуждение правил безопасности.

Деление уч-ся на группы.

**Задание для каждой группы:**

Зайти на страницы сайта, посвященные различным видам деятельности в сети Интернет. Прочитать правила работы, и объяснить, чем может обернуться невыполнение этих правил.

**Обобщение полученной информации:**

Рекомендации, с помощью которых посещение Интернет может стать менее опасным:

1. Посещайте Интернет вместе с родителями, или делитесь с ними успехами и неудачами в деле освоения Интернет;
2. Если в Интернет вас что-либо беспокоит, то вам следует не скрывать этого, а поделиться своим беспокойством со взрослыми;
3. При общении в чатах, использовании программ типа ICQ, использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Выберите регистрационное имя (псевдоним), не содержащее никакой личной информации;
4. 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.;
5. Уважайте собеседников в Интернет. Правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
6. Никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
7. Далеко не все, что можно прочесть или увидеть в Интернет – правда. Спрашивайте у взрослых о том, в чем вы не уверены;

**Составление сводной таблицы правил поведения в сети Интернет**

|  |  |
| --- | --- |
| Никогда | Всегда |
| Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы без разрешения родителей | Всегда будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть |
| Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями | Всегда спрашивай у родителей разрешения посидеть в чате |
| Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах | Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями |
| Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера | Всегда держи информацию о пароле при себе, никому его не говори |
| Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые | Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман |
|  | Всегда держись подальше от сайтов "только для тех, кому уже есть 18". Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой счет за Интернет |

Если ты услышишь или увидишь, что твои друзья заходят в «небезопасные зоны», напомни им о возможных опасностях и посоветуй, как им правильно поступить.

Будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в «небезопасную зону» или загрузить на свой компьютер вирус или программу-шпион.

Если вы получили оскорбляющие сообщения, расскажите об этом родителям.

Всегда принимайте помощь от взрослых или друзей, разбирающихся в вопросах безопасного Интернета. Мама и папа могут не знать ответов на все интересующие вас вопросы.

**Задание:**

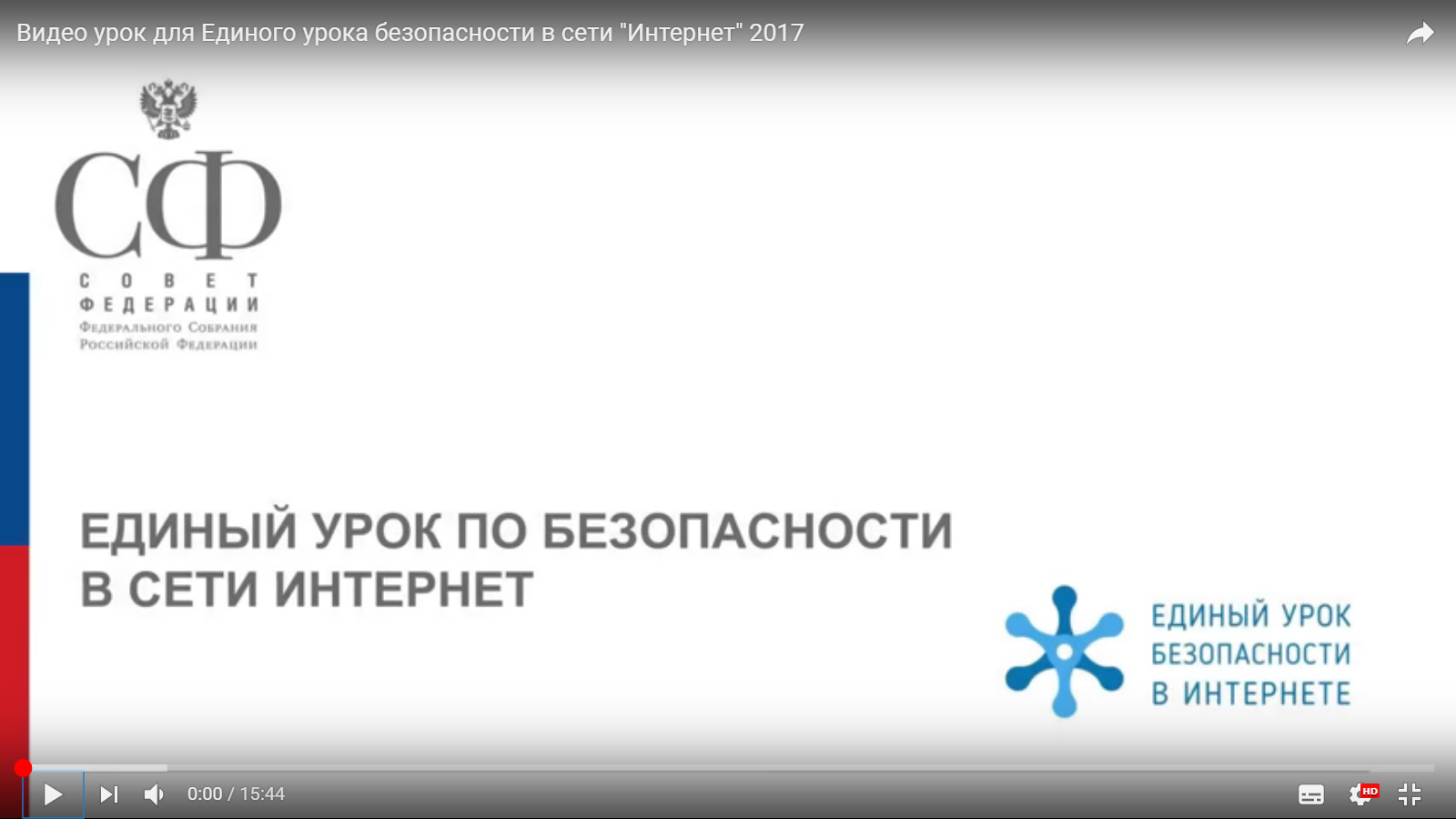
Обсудите предложенные идеи по сохранению безопасности в сети Интернет со своими друзьями. Возможно, вы придумаете новые и дополните список правил.

**III. Подведение итогов занятия**

**IV. Домашнее задание.**

Составьте список правил сетевого этикета и оформите его в электронном виде (Word, презентация). Можно с иллюстрациями.

2)Просмотр с учащимся видео урок для Единого урока безопасности в сети "Интернет" (<https://www.youtube.com/watch?v=yTCcfc3i5NQ>)





3) На родительском собрании провели беседу на тему **«Безопасность в сети Интернет»**

****

**ПАМЯТКА**

**ПО БЕЗОПАСНОСТИ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ**

**Классификация интернет-угроз**

Во Всемирной паутине существует следующие виды опасности юных пользователей:

* суицид-сайты;
* сайты-форумы потенцинальных самоубийц;
* наркосайты (интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья»);
* сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
* сайты порнографической направленности;
* сайты знакомств (виртуальное общение разрушает способность к реальному общению, у подростков теряются коммуникативные навыки);
* сайты, пропагандирующих экстремизм, насилие и девиантные формы поведения, прямые угрозы жизни и здоровью школьников от незнакомцев, предлагающих личные встречи, а также различные виды мошенничества;
* секты (виртуальный собеседник может повлиять на мировоззрение подростка).

**Правила работы в сети Интернет**

1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник)
7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9. Не всей  информации, которая размещена в Интернете, можно верить.
10. Не оставляйте без присмотра компьютер с важными сведениям на экране
11. Не сохраняйте важные сведения на общедоступном компьютере.

**Возраст от 7 до 8 лет**

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интеренета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Wmdows\Temporary Internet Files в операционной системе Windows Vista). В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернет, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

**Советы по безопасности в сети Интернет для детей 7-8 лет**

* Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
* Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
* Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
* Используйте специальные детские поисковые машины, типа MSN Kids Search.
* Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
* Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
* Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
* Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
* Научите детей не загружать файлы, программы или музыку без вашего согласия.
* Не разрешайте детям использовать службы мгновенного обмена сообщениями.
* В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
* Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

**Советы по безопасности для детей от 9 до 12 лет**

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

* Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
* Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
* Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
* Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
* Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
* Не забывайте беседовать с детьми об их друзьях в Интернет.
* Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.
* Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
* Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
* Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
* Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
* Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
* Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

**Советы по безопасности в этом возрасте от 13 до 17 лет**

* Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).
* Компьютер с подключением к сети Интернет должен находиться в общей комнате.
* Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
* Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
* Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
* Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
* Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
* Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
* Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
* Приучите себя знакомиться с сайтами, которые посещают подростки.
* Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
* Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.