Акция «Безопасный Интернет»

Автор: Иванец Надежда Ивановна, учитель информатики.
Место проведения: МБОУ «СОШ № 10» г. Майкопа

Родительское собрание «Безопасный Интернет для детей»

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

- профилактика преступлений совершаемых в сети Интернет в отношении несовершеннолетних;
- привлечение внимания родителей и педагогов к необходимости защиты ребенка при использовании Интернета – знакомство с видами онлайн-угроз;
- повышение интернет-грамотности родителей и педагогов;
- распространение практических навыков по обеспечению безопасности детей в сети Интернет при помощи технических средств.

Программно-дидактическое обеспечение: презентация «Безопасный Интернет глазами родителей и детей» (статистика результатов анкетирования), памятки для родителей и учителей.

Использованные web-ресурсы:

https://www.youtube.com
https://ru.wikipedia.org/
http://www.kaspersky.ru/
http://минобрнауки.рф
http://nsportal.ru/
http://деткивсетке.рф
http://methodological_terms.academic.ru/
http://www.wildwebwoods.org/popup.php?lang=ru – онлайн-игра «Прогулка по лесу»
http://www.единыйурок.рф

Подготовительная работа: анкетирование родителей и обучающихся, подготовка статистики, разработка памяток для родителей, учителей.

Ход собрания.

1. Постановка целей и задач собрания, мотивация к деятельности.

Всероссийский центр изучения общественного мнения представил результаты опроса 26 - 27 марта 2016 г. в 130 населенных пунктах в 46 областях, краях и республиках и 9 ФО России. **В России 70% граждан в возрасте от 18 лет и старше пользуются Интернетом** (год назад - 69%). В последние три года эта доля остается практически неизменной. При этом число ежедневных пользователей неуклонно растет, достигнув на настоящий момент 53% (в 2015 г. - 52%). С 2006 г. этот показатель увеличился в 10 раз.

В России 85 миллионов интернет - пользователей в возрасте 12+ или 69% населения. Выходят в Сеть каждый день 66,5 миллиона россиян.

Сегодня мы с вами остановимся на особенно важной проблеме современных школьников – о безопасности в сети Интернет.

Очень часто родители не понимают и недооценивают угрозы, которым подвергается ребёнок, находящийся в сети Интернет. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети. Понимание данной проблемы учителями, родителями и самими детьми – цель акции «Безопасный Интернет».

2. Результаты анкетирования родителей и учащихся по безопасности в Интернете (статистика и анализ).
3. Беседа по проблеме доступа ребенка к сети Интернет *(в форме дискуссии или лекции)*.

Дискуссия. Список вопросов, которые планируется обсудить на родительском собрании:
– В каком возрасте следует разрешить детям посещение интернета?
– Следует ли разрешать детям иметь собственные учетные записи электронной почты?
– Какими внутрисемейными правилами следует руководствоваться при использовании интернета?
– Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?
– Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, MailAgent)?
– Могут ли дети стать интернет-зависимыми?
– Что должны знать дети о компьютерных вирусах?
– Как проследить какие сайты посещают дети в интернете?
– Что следует предпринять, если моего ребенка преследуют в Интернете?
– Помогает ли фильтрующее программное обеспечение?
– На какие положения политики конфиденциальности детского сайта нужно обращать внимание?
– Какие угрозы встречаются наиболее часто?
– Как научить детей отличать правду ото лжи в Интернет?

Лекция «Основные угрозы для детей в сети Интернет»
1. Системы мгновенного обмена сообщениями

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messsenger, Google Talk, ICQ…) стали широко используемым каналом общения для молодых людей. Это не могло остаться незамеченным со стороны кибер-преступников, которые быстро сделали его основным каналом для своей деятельности.

Одна из самых опасных угроз заключается в том, что преступники, используя данные программы, обманывают детей и подростков и представляются им другим человеком, чем они есть на самом деле.

В этих программах пользователи авторизуются с использованием адреса электронной почты и пароля. Например, если кто-то узнает данные другого пользователя и подключится к программе от его лица, то остальные люди, с которыми этот пользователь общается, будут думать, что они общаются именно с данным пользователем, хотя это не так. Если Вы

обмениваетесь информацией или файлами с этим псевдо-пользователем, то преступник сможет легко ими завладеть. Именно по этой причине очень важно не распространять любую конфиденциальную информацию (персональные данные, фактический адрес проживания, банковские реквизиты и пр.) через подобные небезопасные каналы связи, как системы обмена мгновенными сообщениями.

Другая опасность состоит еще в том, что к подобным преступлениям часто прибегают педофилы. Их задача – собрать сведения о детях и подростках, а затем договориться с ними о реальной встрече или заставить их пойти на встречу. Педофилы зачастую представляются другими молодыми людьми, профессиональными фотографами или т.п.

Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайне, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.

Другой **потенциальный риск** в обмене мгновенными сообщениями – это инфицирование вирусами и вредоносными кодами. Почти 60% червей (вредоносные коды, которые распространяют сами себя), обнаруженных антивирусной лабораторией PandaLabs на протяжении первого полугодия, были созданы для распространения через системы обмена мгновенными сообщениями. Некоторые из них созданы для кражи паролей к онлайн-банкам. В

этом случае в большей степени рискуют сами родители, потому что будут украдены их банковские данные, и, следовательно, могут пропасть их деньги.

Существуют простые способы, которые могут быть полезны для предотвращения случаев проникновения вредоносных кодов на компьютеры через системы обмена мгновенными сообщениями: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через эти системы. По крайней мере, не делайте этого, пока точно не убедитесь, что человек, который их Вам прислал, является именно тем, кем он себя называет.

2. Электронная почта

Электронная почта – это другой источник опасности для молодых ребят. В этом случае также существует несколько угроз:

- Во-первых, это спам. Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств. Дети более подвержены доверять сообщениям, которые представлены в данных письмах, со всеми вытекающими отсюда последствиями. Они могут получить доступ к онлайн-казино и проиграть большую сумму денег, или они могут купить лекарства или даже наркотики с большим риском для своего здоровья.
- Далее, существуют ложные предложения работы. Это не представляет серьезную опасность для детей, но может являться таковой для подростков. Обычно эти сообщения содержат фантастические условия работы. Они обещают большие зарплаты без каких-либо усилий. Все, что в таких случаях необходимо, - это номер банковского счета, куда будут перечисляться деньги, а затем, в обмен на комиссию, получателя попросят перевести эти средства на другой банковский счет. Это выглядит слишком хорошо, чтобы быть правдой, и любой здравомыслящий взрослый человек насторожиться от такого предложения. Однако молодые люди ищут легких денег. В результате этого они непроизвольно становятся соучастником преступления, т.к. целью подобных финансовых переводов является «отмывание» преступных денег.
- Другой риск связан с вирусами и вредоносными программами, которые могут попасть на компьютер. Как правило, они распространяются через сообщения в электронной почте, которые имеют определенную тематику (реклама новых фильмов, эротические фотографии, скачивание игр и т.д.) и предлагают пользователям нажать на ссылку или скачать файл, являющиеся причиной инфекции. Данная техника известна как «социальная инженерия». Многие взрослые люди становятся жертвами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.

Лучший способ защитить детей и подростков от этих угроз – это **научить их быть бдительными по отношению к письмам из неизвестных источников**. Они должны знать, что большинство из написанного в этих письмах является ложью, и что они никогда не должны открывать файлы или нажимать на ссылки в письмах подобного рода.

3. Программы обмена файлами

Обмен файлами в P2P-сетях является еще одним из основных источников распространения инфекций. Большинство вредоносных кодов (преимущественно, черви) копируются в папки с этими программами под заманчивыми именами (названия фильмов, программ и т.д.) для того, чтобы привлечь внимание других пользователей, которые захотят скачать эти файлы и запустить их на своих компьютерах.

По сути дела, это еще один вариант социальной инженерии: названия файлов могут быть умышленно созданы таким образом, чтобы привлечь именно детей и подростков, которые по незнанию скачают вредоносные программы на свои компьютеры.

Именно по этой причине детям следует знать, какие файлы они могут скачивать, а какие скачивать нельзя. Более того, очень хорошая идея – это **проверять каждый скаченный файл с помощью решения безопасности** до момента их первого открытия / запуска.

Если при запуске файла возникает ошибка или открывается диалоговое окно с вопросом о лицензии или предложением скачать дополнительный кодек, то подобные действия должны сразу же Вас заставить быть бдительным, потому что, скорее всего, данный файл содержит в себе вирусы или другое вредоносное программное обеспечение.

4. Социальные сети и блоги

Сайты социальных сетей (например, Facebook, MySpace, одноклассники, Вконтакте) широко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д.

Детям следует постоянно напоминать, что необязательно предоставлять эту информацию, а достаточно только указать адрес электронной почты и имя, которое может быть псевдонимом. Нельзя распространять такую информацию, как возраст, адрес проживания, а также свои фотографии и видео.

Многие подростки используют блоги в качестве своих персональных дневников. Как правило, такие онлайн-журналы содержат значительно более широкую информацию, чем следовало бы публиковать. Крайне важно предотвратить публикацию любых данных, которые могли бы идентифицировать пользователя как ребенка или подростка, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию.

Аналогично, в некоторых социальных сетях, например в MySpace, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание ребенка на то, какими файлами он может обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье.

Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей. Родители также должны быть способны проинструктировать своих детей о том, как использовать эти сервисы правильно и безопасно.

5. Мобильные телефоны с выходом в Интернет

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак.

В настоящее время сотовые телефоны широко используются детьми и подростками. Соответственно, они сталкиваются с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.

Во-первых, сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Дети могут войти в чаты в любой момент, при этом не важно, где они находятся физически, и столкнуться с теми рисками, о которых мы подробно говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.

Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии. Это означает, что дети могут столкнуться с подобной информацией не только при выходе в Интернет со своего компьютера, но и при использовании собственного мобильного телефона.

В результате, родители также должны контролировать то, как дети пользуются своими сотовыми телефонами. Поэтому мы рекомендуем родителям покупать своим детям сотовые телефоны без встроенных функций, которые могли бы подвергать их такому риску (подключение к Интернету, SMS, наличие Bluetooth и т.д.), а подросткам необходимо объяснять, как следует безопасно использовать свой сотовый телефон. Постоянно напоминайте им, чтобы они не отвечали на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

4. Рекомендации родителям.

Нормы времени работы за компьютером для школьников

- до 6 лет не более — 10-15 минут — и то не каждый день.

- 7-8 лет — 30-40 минут в день
- 9-11 лет — не более часа-полутора в день
- 12 – 15 лет – не более 2 часов в день

Распространение памятки для родителей. (Приложение 3)

5. Вывод: Главное, вы сами должны быть образцом и примером для ребенка. Вы не достигнете никакого результата, если ваше дитя будет видеть родителя, часами сидящего за компьютером.

Приложение 1

Анкета для родителей «Безопасный Интернет для детей»
(подчеркните ответы, с которыми Вы согласны или считаете верными, или напишите своё мнение)

1. **Укажите возраст Вашего ребёнка:**

– 7-10 лет;
– 11-13 лет;
– 14-16 лет;
– 17-19 лет;
– 20 лет и старше.

2. **Есть ли у Вашего ребёнка доступ к Интернету?**

– да;
– нет.

3. **В каком возрасте Ваш ребёнок стал пользователем сети Интернет:**

– 7-10 лет;
– 11-13 лет;
– 14-16 лет;
– 17-19 лет;
– 20 лет и старше.

4. **Как часто Ваш ребёнок выходит в Интернет:**

– почти каждый день;
– 1-2 раза в неделю;
– 1-2 раза в месяц;
– реже, чем раз в месяц;
– не пользуюсь Интернетом.

5. **Где расположен компьютер, с которого Ваш ребёнок чаще всего выходит в сеть Интернет:**

– дома в своей комнате;
– дома в общей комнате;
– дома у друзей;
– в школе;
– в интернет-клубе или интернет-кафе;
– в библиотеке;
– в других общественных местах.

6. **Для чего Ваш ребёнок обычно использует сеть Интернет:**

– выполнение домашнего задания (поиск необходимой информации);
– поиск информацию для саморазвития;
– скачивание музыки, видео;

- играю в онлайн игры;
- общение в социальных сетях (Вконтакте, Одноклассники и т.п.), чатах, форумах;
- разрабатка собственных проектов (видео, сайт, презентации, фотоальбом, рисует и т.п.);
- другое _____ .

7. С какими проблемами и опасностями Ваш ребёнок сталкивается в сети Интернет:

- кибер-буллинг (неоднократное умышленное агрессивное поведение, направленное против кого-то с целью унижения его достоинства);
- блокировка компьютера, взлом профиля, вирусы, спам, вымогательство денег за разблокировку;
- неподобающая или незаконная информация различного рода;
- онлайн-мошенничество;
- попытка посторонних узнать Вашу личную информацию;
- приглашение к общению в сомнительные (подозрительные) сообщества, связанные с экстремизмом, национализмом, употреблением алкоголя, наркотиков;
- не подвергались никаким опасностям.

8. Осуществляется ли дома Интернет-фильтрация?

- да, встроенными средствами браузеров;
- да, приобретённым контент-фильтром (контент – информационное наполнение сайта);
- да, бесплатным контент-фильтром;
- используем «Родительский контроль» Microsoft;
- другое _____ ;
- нет.

9. Ваше отношение к публикации своей персональной информации и Вашего ребёнка в сети Интернет:

- это опасно;
- иногда это ведет к неприятностям;
- это абсолютно безопасно.

10. Какую степень приватности Ваш ребёнок выбирает для личной страницы в социальных сетях?

- всем пользователям;
- только друзьям;
- друзьям и друзьям друзей;
- некоторым друзьям;
- никому;
- не пользуюсь социальными сетями;

11. Наиболее часто посещаемые сайты Вашего ребёнка (укажите не менее 3-х)

_____

12. Используете ли Вы какие-либо ограничения в пользовании электронными средствами коммуникации?

- да, телевизором;
- да, мобильным телефоном, планшетом и т.п.;
- да, игровыми приставки;
- да, Интернетом;
- да, компьютером, ноутбуком и т.п. (без выхода в Интернет);
- нет, никаких правил нет.

13. Какие из перечисленных правил Вы устанавливаете при использовании Интернета?

- не разрешается размещать личную информацию в Интернете;
- есть набор сайтов, на которые ребенку запрещается заходить;
- я должен рассказывать о том, что заставило меня почувствовать себя в Интернете неловко;
- не разрешается использовать грубые (нецензурные) выражения в электронных письмах или чатах;
- не должен встречаться с теми, с кем познакомился в Интернете без Вашего ведома;
- не должен копировать документы, картинки, защищённые авторскими правами;
- не должен общаться в чатах/социальных сетях с незнакомыми людьми;
- не разрешается скачивать музыку, фильмы;
- не разрешается бесконтрольно скачивать и устанавливать программы;
- устанавливается временной режим нахождения в Интернете;
- другие правила _____;
- нет никаких правил.

14. Знаете ли Вы и Ваш ребёнок, где и кому можно сообщить о замеченном незаконном или негативном контенте в Интернете?

- да, мне известен телефон «горячей линии»;
- да, я сообщу в правоохранительные органы;
- да, на специальные сервисы Интернет-провайдеров;
- да, в школу;
- да, в родительский комитет (управляющий совет и т.п.) школы;
- я не знаю, кому я могу сообщить о незаконном и негативном Интернет-контенте;
- я не буду никуда сообщать, это бесполезно;
- затрудняюсь ответить .

15. Откуда и как Вы и Ваш ребёнок получаете информацию о безопасном использовании Интернет?

- уроки, беседы в школе, сайт школы, другие информационные возможности для обучающихся;
- информация от провайдеров или телефонных компаний;
- информация на сайтах производителей программного обеспечения для фильтрации контента;
- из разъяснений поставщиков (розничных продавцов) компьютеров;
- из телевизионных передач, по радио, в периодических изданиях;
- читаю специализированную справочную литературу;
- информируют правоохранительные органы;
- имею другие источники _____;
- я не владею такой информацией;
- затрудняюсь ответить.

Приложение 2

Анкета для обучающегося «Безопасный Интернет»
(подчеркните ответы, с которыми Вы согласны или считаете верными, или напишите своё мнение)

16. Укажите Ваш возраст:

- 7-10 лет;
- 11-13 лет;
- 14-16 лет;
- 17-19 лет;
- 20 лет и старше.

17. Есть ли у Вас доступ к Интернету?

- да;
- нет.

18. В каком возрасте Вы стали пользователем сети Интернет:

- 7-10 лет;
- 11-13 лет;
- 14-16 лет;
- 17-19 лет;
- 20 лет и старше.

19. Как часто Вы выходите в Интернет:

- почти каждый день;
- 1-2 раза в неделю;
- 1-2 раза в месяц;
- реже, чем раз в месяц;
- не пользуюсь Интернетом.

20. Где расположен компьютер, с которого Вы чаще всего выходите в сеть Интернет:

- дома в своей комнате;
- дома в общей комнате;
- дома у друзей;
- в школе;
- в интернет-клубе или интернет-кафе;
- в библиотеке;
- в других общественных местах.

21. Для чего Вы обычно используете сеть Интернет:

- выполнение домашнего задания (поиск необходимой информации);
- поиск информацию для саморазвития;
- скачивание музыки, видео;
- играю в онлайн игры;
- общение в социальных сетях (Вконтакте, Одноклассники и т.п.), чатах, форумах;
- разрабатка собственных проектов (видео, сайт, презентации, фотоальбом, рисует и т.п.);
- другое _____ .

22. С какими проблемами и опасностями Вы сталкивались в сети Интернет:

- кибер-буллинг (неоднократное умышленное агрессивное поведение, направленное против кого-то с целью унижения его достоинства);
- блокировка компьютера, взлом профиля, вирусы, спам, вымогательство денег за разблокировку;
- неподобающая или незаконная информация различного рода;
- онлайн-мошенничество;
- попытка посторонних узнать Вашу личную информацию;

- приглашение к общению в сомнительные (подозрительные) сообщества, связанные с экстремизмом, национализмом, употреблением алкоголя, наркотиков;
- не подвергались никаким опасностям.

23. Осуществляется ли дома Интернет-фильтрация?

- да, встроенными средствами браузеров;
- да, приобретённым контент-фильтром (контент – информационное наполнение сайта);
- да, бесплатным контент-фильтром;
- используем «Родительский контроль» Microsoft;
- другое _____ ;
- нет.

24. Ваше отношение к публикации своей персональной информации в сети Интернет:

- это опасно;
- иногда это ведет к неприятностям;
- это абсолютно безопасно.

25. Какую степень приватности Вы выбираете для личной страницы в социальных сетях?

- всем пользователям;
- только друзьям;
- друзьям и друзьям друзей;
- некоторым друзьям;
- никому;
- не пользуюсь социальными сетями;

26. Наиболее часто посещаемые сайты (укажите не менее 3-х)

_____

27. Используете ли Ваши родители какие-либо ограничения в пользовании электронными средствами коммуникации?

- да, телевизором;
- да, мобильным телефоном, планшетом и т.п.;
- да, игровыми приставки;
- да, Интернетом;
- да, компьютером, ноутбуком и т.п. (без выхода в Интернет);
- нет, никаких правил нет.

28. Какие из перечисленных правил Ваши родители устанавливают при использовании Интернета?

- не разрешается размещать личную информацию в Интернете;
- есть набор сайтов, на которые ребенку запрещается заходить;
- я должен рассказывать о том, что заставило меня почувствовать себя в Интернете неловко;
- не разрешается использовать грубые (нецензурные) выражения в электронных письмах или чатах;
- не должен встречаться с теми, с кем познакомился в Интернете без Вашего ведома;
- не должен копировать документы, картинки, защищённые авторскими правами;
- не должен общаться в чатах/социальных сетях с незнакомыми людьми;
- не разрешается скачивать музыку, фильмы;
- не разрешается бесконтрольно скачивать и устанавливать программы;

- устанавливается временной режим нахождения в Интернете;
- другие правила _____;
- нет никаких правил.

29. Знаете ли Вы где и кому можно сообщить о замеченном Вами незаконном или негативном контенте в Интернете?

- да, мне известен телефон «горячей линии»;
- да, я сообщу в правоохранительные органы;
- да, на специальные сервисы Интернет-провайдеров;
- да, в школу;
- да, в родительский комитет (управляющий совет и т.п.) школы;
- я не знаю, кому я могу сообщить о незаконном и негативном Интернет-контенте;
- я не буду никуда сообщать, это бесполезно;
- затрудняюсь ответить .

30. Откуда и как Вы получаете информацию о безопасном использовании Интернет?

- уроки, беседы в школе, сайт школы, другие информационные возможности для обучающихся;
- информация от провайдеров или телефонных компаний;
- информация на сайтах производителей программного обеспечения для фильтрации контента;
- из разъяснений поставщиков (розничных продавцов) компьютеров;
- из телевизионных передач, по радио, в периодических изданиях;
- читаю специализированную справочную литературу;
- информируют правоохранительные органы;
- имею другие источники _____;
- я не владею такой информацией;
- затрудняюсь ответить.

Приложение 3

Уважаемые родители! Чтобы помочь своим детям, Вы должны это знать:

- Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильно телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
- Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.
- Объясните детям, что нельзя открывайте файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.
- Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.

- Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
- Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратится.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.