ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ДЛЯ ПРОВЕДЕНИЯ КЛАССНОГО ЧАСА «БЕЗОПАСНЫЙ ИНТЕРНЕТ»

Цель: познакомить учащихся с опасностями, которые подстерегают их в сети Интернете. Систематизировать и обобщить сведения о безопасной работе подростков в сети.

Задачи:

- информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, а также о негативных последствиях распространения такой информации;
- обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет, в том числе способам защиты от опасных посягательств в сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде);
- профилактика формирования у учащихся Интернет-зависимости;
- предупреждение совершения учащимися правонарушений с использованием информационных технологий.

Возраст участников:11-14 лет.

Время: 45 мин.

Подготовка к мероприятию. Выбираются 2 чтеца, обговаривается с ними сценарий, раздаются стихи (в сценарии использованы стихи с сайта «Дети России он-лайн» http://detionline.com/helpline/rules/604»).

Оборудование зависит от места проведения, это может быть как обычная классная доска, так и электронная доска или компьютер с проектором.

ХОД МЕРОПРИЯТИЯ

Учитель*: Наш классный час посвящен Интернету. Все мы знаем, что Интернет — интересный и многогранный мир, который позволяет узнавать много нового, общаться с людьми с разных концов света, играть в игры и делиться с другими своими увлечениями и мыслями.*

1 чтец:

«Где найти мне друга Колю?
Прочитать, что было в школе?
И узнать про все на свете?
Ну конечно, в ИНТЕРНЕТЕ!»

2 чтец:

«Там музеи, книги, игры,
Музыка, живые тигры!
Можно все, друзья, найти
В этой сказочной сети!»

1 чтец:

«В Интернете, в Интернете,
Пруд пруди всего на свете!
Здесь мы можем поучиться,
Быстро текст перевести,
А в онлайн библиотеке
Книжку нужную найти».

2 чтец:

«Расстоянья Интернету
Совершенно не страшны.
За секунду он доставит
Сообщенье хоть с Луны».

1 чтец:

«Не печалься, если вдруг
Далеко уехал друг.
Подключаешь Интернет —
Расстоянья больше нет!»

2 чтец:

«Электронное письмо

Вмиг домчится до него.

Ну а видео-звонок,

Сократит разлуки срок».

На доске записан следующий текст **«ВЖИПРБТОЬ КОУЖСОЖУ».**

Учащимся предлагается расшифровать запись и узнать тему классного часа.

Учитель: *Да, действительно, мы сегодня будем говорить о БЕЗОПАСНОМ ИНТЕРНЕТЕ. Наш девиз: «Предупрежден – значит, вооружен». Эта народная мудрость как ничто лучше характеризует важность знания безопасного поведения в сети Интернет.*

Учитель предлагает детям разбиться на 2 команды. Первая команда – «Активные юзеры (пользователи)», вторая – «Специалисты по информационной безопасности». Первая команда, при ответе на вопрос задания, называет опасности, которые могут встретиться в сети Интернет, вторая – как от них уберечься.

I. ЗАДАНИЕ ПЕРВОЙ КОМАНДЕ:

Какие существуют опасности при работе в сети Интернет?

Команда отвечает. Приводит примеры.

Учитель обобщает сказанное учащимися, приводит примеры и фиксирует на доске основные опасности (или открывает заранее подготовленные записи):

Вредоносные программы
Шпионские программы
Спам
Недостоверная информация
Интернет-мошенничества (фишинг)
Оскорбления и унижения (кибербуллинг)
Вредоносная информация
Кража личной информации, находящейся в открытом доступе
Нежелательное знакомство (контакты с незнакомцами)
Интернет-зависимость

1. Вредоносные программы

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред компьютеру и хранящимся на нем данным. Особенностью этих программ является способность к размножению.

Наибольшая опасность таких вирусов заключается в том, что прежде чем нанести вред компьютеру, они копируются в другие программные файлы и заражают их.

2. Шпионские программы

Задачей программ является сбор информации о пользователях: содержимое жесткого диска, список посещаемых Интернет-сайтов, контакты электронной почты, и другая информация личного характера. Полученную информацию используют в разных целях, например, это может быть сбор данных с целью воровства денег с кредитных карточек.

3. Спам

Спам — это письма, которые приходят по электронной почте от неизвестных людей, чаще всего это различные рекламные объявления, они забивают ящик, мешая загружать нормальные письма.

4. Недостоверная информация

Интернет предлагает большое количество возможностей для поиска информации на любую тематику, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной, поскольку абсолютно любой может опубликовать информацию в Интернете. Поэтому, прежде чем воспользоваться какой-либо информацией в сети Интернет (и не только), необходимо перепроверить ее по нескольким источникам (желательно таким, которые вызывают доверие).

5. Интернет-мошенничества (фишинг)

Фишинг – это одна из разновидностей шпионских программ - вид Интернет-мошенничества, основанный на получение доступа к конфиденциальным данным - логинам и паролям. Злоумышленник в комментарии вставляет ссылку на изображение (видеоролик, программу и т.д.), загружающееся с его сайта. Пользователь, нажимая на ссылку, получает сообщение о том, что ему необходимо авторизоваться, и, будучи уверенным, что авторизацию запросила социальная сеть, вводит все свои данные. В результате пользователь смотрит на картинку, а злоумышленник – на логин и пароль пользователя. И теперь с Вашими друзьями будет общаться другой человек, который похитил Ваш пароль и все Ваши контакты.

6. Оскорбления и унижения (кибербуллинг)

Притеснения со стороны других пользователей Сети (чаще всего злоумышленниками оказываются другие дети), которые грубо ведут себя в Интернете,

оскорбляют и угрожают, выкладываются факты из чужой личной жизни человека, фото, вымышленные события и видеоролики.

☝ Шестиклассника Сашу К. одноклассники неоднократно терроризировали в сети, оскорбляя, обзывая его, посылая непристойные картинки. Сашин папа обратился по этому поводу к директору школы и написал заявление в полицию. Хулиганов поставили на учет в отделе по делам несовершеннолетних, а их родители были оштрафованы.

7. Вредоносная информация (нецензурная лексика и др.)

Это информация о нездоровом образе жизни, принесении вреда здоровью и жизни, нецензурная брань, оскорбления, реклама алкоголя, табака и пр.

8. Кража личной информации

Кража личной информации, выложенной в открытом доступе с целью нанесения вреда. По данным статистиков 42 процента пользователей социальных сетей публикуют дату рождения. 7 процентов вывешивают свой домашний адрес, при этом 3 процента заботливо всех предупреждают, когда они бывают в отъезде.

☝ В 2011 г. в Москве был похищен сын известного бизнесмена, специалиста по компьютерной безопасности. Преступники связались с отцом и потребовали выкуп в 3 млн. евро.

Оказалось, что преступники собрали информацию о похищенном, используя ресурс «Вконтакте», где был указан адрес проживания с улицей и номером дома.

☝ Пятиклассница Маша Н. выложила в сети сообщение о том, что уезжает с родителями на неделю в Турцию. Пока семья отдыхала, квартира была ограблена. На личной страничке был выложен номер домашнего телефона, по которому преступники смогли узнать адрес Маши.

9. Нежелательное знакомство (контакты с незнакомцами)

В Интернете многие люди рассказывают о себе неправду и выдают себя за других людей. Встреча с Интернет-знакомыми в реальной жизни, бывает опасной: за псевдонимом может скрываться преступник.

10. Интернет-зависимость

Интернет-зависимость – это болезнь современного поколения: дети и многие взрослые сутками проводят за компьютером, в частности, во всемирной паутине. Ученые полагают, что в скором времени Интернет-зависимость встанет в один ряд с такими пагубными пристрастиями, как наркотическая зависимость, алкоголизм, курение.

II. ЗАДАНИЕ ВТОРОЙ КОМАНДЕ

Какие существуют средства профилактики и борьбы с опасностями при работе в сети?

Дети отвечают, а учитель обобщает и дополняет, если это необходимо.

1. Вредоносные программы

- *Не устанавливайте на своём компьютере программного обеспечения из неизвестных источников, с пиратских DVD и сайтов. Пиратские копии программ, особенно компьютерных игр, довольно часто бывают заражены вирусами.*
- *Проверяйте файл, скачанный из сети, с помощью антивирусной программы перед тем, как открыть его.*
- *Вставив в компьютер флешку (даже свою), прежде чем открывать, проверьте ее на наличие вирусов.*

2. Шпионские программы

- *Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы.*
- *Письма от неизвестных людей, в которых вложены файлы, как правило, содержат вирусы или другие вредоносные программы, их надо сразу удалять, не читая.*

3. Спам

- *Не открывайте вложенные файлы электронной почты, когда не знаете отправителя.*

4. Недостоверная информация

- *Всегда проверяйте собранную в Интернет информацию не менее, чем по трем другим источникам. Это могут быть сайты, журналы, книги.*

5. Интернет-мошенничества (фишинг)

- *Для фишинговой атаки чаще используют социальные сети, рекламу, поэтому открывайте только те ссылки, в которых уверены.*

6. Оскорбления и унижения (кибербуллинг)

- *Если Вы получили сообщение с неприятным и оскорбляющим Вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом родителям.*

- *Не общайтесь с агрессором и не пытайтесь ответить ему тем же. Поместите его в «черный» список».*

7. Вредоносная информация (нецензурная лексика и др.)

- *Пользуйтесь ресурсами, созданными специально для подростков, которые помогут вам общаться с ровесниками, находить информацию для учебы и развлечений.*
- *Не открывайте неизвестные ссылки.*
- *Сообщайте родителям обо всех случаях в Интернете, которые вызвали у Вас смущение или тревогу.*

8. Кража личной информации

- *Никогда не публикуйте в сети Интернет какую-либо личную информацию, в том числе фамилию, домашний адрес, номера телефонов, название школы, адрес электронной почты, дату рождения.*
- *Перед публикацией любой информации или своих фотографий (а также фотографий других людей) следует помнить, что любой сможет получить доступ к этой информации, скопировать её и в дальнейшем использовать против Вас.*
- *Периодически меняйте пароли (например, от профилей в социальных сетях), и не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов, имена, названия и т.п.).*
- *Не сообщайте пароли своим друзьям и знакомым.*
- *Перед завершением работы в социальной сети, в почте и на других сайтах выберите «Выход», чтобы покинуть свой аккаунт (даже на личном компьютере).*
- *Используйте программы, которые очищают кэш (то, что сохраняется на компьютере в процессе посещения сайтов и других действий), например ccleaner.*

9. Нежелательное знакомство (контакты с незнакомцами)

- *При общении на ресурсах, требующих регистрации (в чатах, на форумах, в онлайн-играх), лучше использовать не реальное имя, а «ник» (выдуманное имя).*
- *Используйте веб-камеру только при общении с друзьями.*
- *Не добавляйте в друзья в социальных сетях всех подряд.*

- *Не соглашайтесь на личную встречу с людьми, с которыми Вы познакомились в Интернете, без согласования с взрослыми.*
- *Всегда рассказывайте взрослым обо всех случаях в Интернете, которые вызвали у Вас смущение или тревогу.*
- *Прекращайте любые контакты по электронной почте или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера.*

10. Интернет-зависимость

- *Установите, желательно с участием родителей, для себя правила использования компьютера и постарайтесь найти разумный баланс между виртуальной и реальной жизнью. Ведь реальная жизнь намного ярче и интереснее (спорт, хобби, походы и пр.).*
- *Виртуальное общение не может заменить живой связи между людьми.*

III. ОБЩЕЕ ЗАДАНИЕ КОМАНДАМ:

При общении в Интернет существуют правила сетевого этикета (нетикет), назовите эти правила.

Команды по очереди отвечают, учитель при необходимости дополняет и комментирует.

Эталоны ответов

- При общении в Интернете вы должны быть дружелюбными с другими пользователями. Ни в коем случае не надо писать резкие и оскорбительные слова, распространять сплетни и угрозы.
- Нельзя опубликовывать в сети чужие фотографии и сведения без разрешения хозяина.
- Нельзя рассылать спам и другой «информационный мусор».
- Никогда не пересылайте никому «письма счастья», удаляйте их сразу после получения.
- Отправляемое электронное письмо всегда должно быть подписано и указана тема сообщения.
- Если у Вас нет возможности сразу ответить на полученное письмо, сообщите, что Вы его получили и ответите позже.
- Незаконное копирование файлов в Интернете (музыкальных, видеофайлов) = воровство. Не будьте «пиратами»!
- Пользуетесь Интернет-источником – делайте на него ссылку.

IV. ПОДВЕДЕНИЕ ИТОГОВ

1. *О чем мы сегодня говорили на классном часе?*
2. *Каким образом вы можете использовать знания, полученные сегодня, в вашей жизни?*
3. *Помните, Интернет может быть полезным средством для обучения, отдыха или общения с друзьями, но в сети вас могут поджидать и опасности, поэтому вы должны знать определенные правила защиты.*

1 чтец:

«Мы хотим, чтоб Интернет

Был вам другом много лет!

Будешь знать СЕМЬ правил этих –

Смело плавай в Интернете».

2 чтец:

« Иногда тебе в сети

Вдруг встречаются вруны.

Ты мошенникам не верь,

Информацию проверь».

1 чтец*:*

« Не хочу попасть в беду –

Антивирус заведу!

Всем, кто ходит в Интернет,

Пригодится наш совет».

2 чтец:

« Если кто-то НЕЗНАКОМЫЙ

Вас попросит рассказать

Информацию о школе,

О друзьях и телефоне,

Иль к страничке доступ дать –

Мы на это НЕТ ответим,

Будем все держать в секрете!»

1 чтец*:*

« С грубиянами в сети

Разговор не заводи.

Ну и сам не оплошай,

Никого не обижай».

2 чтец:

«Злые люди в Интернете

Расставляют свои сети.

С незнакомыми людьми

Ты на встречу не иди!»

1 чтец*:*

«Как и всюду на планете

Есть опасность в Интернете.

Мы опасность исключаем,

Если фильтры подключаем».

2 чтец:

«Если что-то непонятно,

Страшно или неприятно,

Быстро к взрослым поспеши,

Расскажи и покажи».

8 800 25 000 15 — бесплатная всероссийская служба консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи.