Методические рекомендации по проведению Единого урока по безопасности в информационно-телекоммуникационной сети «Интернет»

Аннотация

Методические рекомендации подготовлены в помощь педагогам для проведения и организации Единого урока по безопасности в информационно-телекоммуникационной сети «Интернет». В данных методических рекомендациях освещаются вопросы безопасной работы учащихся с ресурсами сети Интернет для подготовки домашних заданий, поиска и обмена информацией, общения и размещения личной информации в социальных сетях, а также риски при работе с мобильными устройствами.

В основе рекомендаций лежит опыт работы по проведению вебинаров и семинаров, посвященных Интернет-безопасности, рекомендации мобильных операторов и банков, специализированных сайтов, правовые нормы по вопросам информационной безопасности.

Данные методические рекомендации могут быть использованы учителями информатики, классными руководителями при работе со школьниками разного возраста в рамках проведения тематических уроков, уроков-дискуссий, бесед, классных часов.

Содержание методических рекомендаций

Содержание Единого урока по безопасности в информационно-телекоммуникационной сети «Интернет» решает две педагогические задачи. Во-первых, в ходе урока предполагается освещение технических, правовых, и социально-культурных аспектов обеспечения информационной безопасности детей. Во-вторых, предусматривается более детальное знакомство школьников с новыми опасностями информационного общества и способами их предотвращения.

Для того, чтобы предотвратить негативные последствия использования школьниками сети Интернет необходимо придерживаться нескольких основных правил:

1. Рассказать школьникам о возможных рисках при работе в сети Интернет.
2. Мотивировать школьников использовать проверенные ресурсы сети Интернет для определенных целей.
3. Выстроить беседы с ребенком в максимально доверительном тоне. Доверие между ребенком и взрослым – залог успеха в таком важном деле.

4. Настроить аппаратную защиту – иметь постоянно обновляемый антивирус, поставить контент-фильтр для сортировки и отсеивания негативной информации.

Содержание урока

Урока рекомендуется проводить в форме круглого стола. В ходе урока педагог управляет дискуссией, выступает в качестве ведущего, задает вопросы школьникам по заранее подготовленному сценарию, предлагает высказаться на поставленные проблемные вопросы.

Итогом такого урока может стать разработка рекомендаций или информационного материала (буклет, плакат, листовка о безопасности в сети Интернет) для последующего использования школьниками на занятиях по данной проблематике на уроках информатики, внеклассных мероприятиях, на мероприятиях для родителей.

Во вступительной части урока учитель вводит ключевые понятия, связанные с информационной безопасностью.

Разберемся в понятиях: «информационная безопасность», «информационная грамотность», «медиаграмотность».

Информационная безопасность детей — 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. Такую защищенность ребенку могут и должны обеспечить, прежде всего, значимые взрослые.

Информационная грамотность - поиск, интерпретация, оценка различных источников информации, работа с видами учебных, деловых и научно-популярных текстов.

Информационная культура- совокупность материальных и духовных ценностей в области информации.

Медиаграмотность - это 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.

Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить киберпространство. Теперь преступнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Конвенцией Совета Европы виды киберпреступлений объединены в пять групп.

Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

Вторую группу составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами) – мошенничество в Интернете.

Правонарушения третьей группы связаны с содержанием данных или контентом – негативный интернет.

Нарушение авторских и смежных прав (пиратство) относится к четвертой группе, выделение определенных видов преступлений в которой отнесено к законодательству конкретных государств.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в пятую группу киберпреступлений.

Количество киберпреступлений, совершаемых в мире, неуклонно растет. Например, в нашей стране количество преступлений, совершенных с помощью IT-технологий, выросло в 2019 году на 68,5%. Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно. Законодательство большинства стран мира предполагает уголовную ответственность за совершение преступлений данного вида, наша страна не исключение. Ответственность за киберпреступления в России предусматривается главой 28 УК РФ и касается только компьютерных преступлений.

Все эти виды угроз рассматриваются далее учащимися в форме домашних заготовок по данным им темам (каждому ученику по виду рисков).

Тема 1. Риски, которыми подвергаются школьники в сети Интернет.

В сети Интернет существует немало серьезных рисков, с которыми сталкиваются дети.

Все опасности интернет-среды можно объединить в четыре крупные группы рисков:

Контентные риски.

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. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения. Негативные контентые материалы можно условно разделить на:

- Незаконные, к которым могут относиться: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным), азартные игры и т.д. Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.
- Неэтичные, противоречащие принятым в обществе нормам морали и социальным нормам. Подобные материалы не попадают под действие уголовного кодекса, однако могут оказывать негативное влияние на психику столкнувшимися с ними человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, в том числе и порнография, агрессивные

онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др. Информация, относящаяся к категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

Контентные риски связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

Коммуникационные риски.

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 (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д. Даже если большинство пользователей существующих чат-систем (вебчатов или IRC) обладают добрыми намерениями, существует, к сожалению, растущее число людей, использующих эти беседы со злым умыслом. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в интернете и др. В других случаях они могут оказаться педофилами в поисках жертвы. Выдавая себя за сверстника и устанавливая дружеские отношения с ребенком, они выведывают о нем много информации и понуждают к личной встрече. Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блоговом сообществе и чате появляются такие участники, которые хамят и оскорбляют других участников.

Коммуникационные риски включают в себя «незаконный контакт» и «киберпреследование» (или кибер-буллинг).

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Это понятие включает в себя такие интернет-преступления как домогательство и груминг.

Домогательство — причиняющее неудобство или вред поведение, нарушающее неприкосновенность частной жизни лица. Такое поведение может заключаться в прямых или косвенных словесных оскорблениях или угрозах, недоброжелательных замечаниях, грубых шутках или инсинуациях, нежелательных письмах или звонках, показе оскорбительных или унизительных фотографий, запугивании, похотливых жестах, ненужных прикосновениях, похлопываниях, щипках, ударах, физическом нападении или в других подобных действиях.

Груминг — установление дружеских отношений с ребенком с целью изнасилования. Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично («в привате»), он входит в доверие к ребенку, пытается узнать номер мобильного и договориться о встрече.

Киберпреследование (или кибер-буллинг) — это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; хулиганство (интернеттроллинг); социальное бойкотирование.

По форме буллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными. Подобный унизительный контент может исходить от одного человека или группы людей по одному или нескольким электронным контактам жертвы, на электронный ящик или в сообщениях онлайн-мессенджеров. Распространены также случаи преследования в социальных сетях или на подобных им ресурсах. При этом помимо рассылки оскорбительных сообщений и вывешивания унизительных материалов, изображений или видеозаписей, буллер может также взломать

профиль или страницу жертвы и организовать спам-рассылку по всем контактам жертвы.

К сожалению, кибербуллинг — очень распространенное явление среди российских подростков. Каждый пятый ребенок может признать, что подвергался буллингу онлайн или в реальной жизни. И это беда не только России, она распространена во всем мире. Но в России дети становятся жертвами буллинга в интернете так же часто, как и в реальной жизни. Нередко кибербуллинг берет начало в отношениях с реальными людьми, и в этом случае, жертва знает своих оскорбителей. Когда же буллинг берет свое в интернете, всегда важно удостовериться, чтобы он не перерос в реальное насилие над ребенком.

Электронные риски.

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

Вредоносное ПО (Программное Обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры, не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов. К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Защита в социальных сетях — это задача, которая не так давно стала актуальна для их пользователей. Буквально несколько месяцев назад, взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете. В частности, теперь вирусное ПО (программное обеспечение), которое рассылает спам в социальной сети может быть установлено на ваш компьютер с любого сайта. И от вашего лица могут регулярно рассылаться абсолютно любые сообщения, избавиться от которых не поможет ни одна защита самого сайта. Хотя бы просто по той причине, что в этом случае потребуется не защита вашей страницы, а современное антивирусное программное обеспечение. Поэтому не забывайте обновлять свою антивирусную программу и следить за защитой своего компьютера. К

сожалению, вероятность наткнуться на подобные вредоносные программы очень велика.

Помимо негативного воздействия на компьютер и мобильное устройство, можно стать жертвой еще одного вида киберпреступления — кибер-мошенничества. В самом широком смысле мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды.

Мошенничество в сети Интернет (кибермошенничество) — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

Потребительские риски.

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 кибер-мошенничества, и др. Также дети, зачастую совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ.

Одним из самых распространенных видов данного типа рисков является мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды. Мошенничество, как правило, является преступлением. Поскольку мошенничество в сети интернет совершается с помощью различных технических средств и разнообразного количества программ, то некоторые его виды могут быть отнесены и к группе электронных рисков, а часть к группе коммуникационных, поскольку включает в свою схему установления более близкого контакта с жертвой в течение какого-либо времени (например, с помощью электронных писем и смс, которые могут привести и к реальным встречам с мошенниками).

Вопросы для дискуссии.

1. Для чего нужен Интернет?
2. Какие существуют риски при пользовании Интернетом, и как их
3. можно снизить?

4. Какие виды мошенничества существуют в сети Интернет?
5. Как защититься от мошенничества в сети Интернет?
6. Что такое безопасный чат?
7. Виртуальный собеседник предлагает встретиться, как следует поступить?

По итогам обсуждения необходимо зафиксировать с детьми возможные пути, приводящие к опасности или рискам при работе в сети Интернет.

Существует несколько типов рисков, с которыми дети могут встретиться, пользуясь Интернетом:

1. Дети могут получить доступ к неподходящей их возрасту информации. К ней относятся: порнография, дезинформация, обман, пропаганда ненависти, нетерпимости, насилия, жестокости.

2. Дети могут получить доступ к информации, совершить действия и купить товары, потенциально опасные для них. Существуют сайты, предлагающие инструкции по изготовлению взрывчатых веществ, продающие оружие, алкоголь, отравляющие и ядовитые вещества, наркотики, табачные изделия, а также сайты, предлагающие принять участие в азартных онлайн играх.

3. Дети могут быть подвержены притеснениям со стороны других пользователей Сети (чаще всего злоумышленниками оказываются другие дети), которые грубо ведут себя в Интернете, пишут оскорбления и угрожают. Дети также могут загрузить себе на компьютеры вирусы или подвергнуться нападению хакеров.

4. Дети могут выдать важную и личную информацию, заполняя анкеты и принимая участие в онлайн конкурсах и, в результате, стать жертвой безответственных торговцев, использующих нечестные, запрещенные маркетинговые методы.

5. Дети могут стать жертвами обмана при покупке товаров через Интернет, а также выдать важную финансовую информацию другим пользователям (например, номер кредитной карточки, пин-коды и пароли).

6. Дети могут стать жертвой киберманьяков, ищущих личной встречи с ребенком.

Выводы по Теме 1.

Рекомендации для разработки памятки:

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 указывать свои личные данные, а использовать псевдоним (ник).

7. Без контроля взрослых ни в коем случае не встречаться 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. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.
10. Не всей той информации, которая размещена в Интернете, можно верить.
11. Не оставляйте без присмотра компьютер с важными сведениям на экране.
12. Опасайтесь подглядывания через плечо.
13. Не сохраняйте важные сведения на общедоступном компьютере.

Тема 2. Технологии безопасной работы в сети Интернет.

Для учеников рекомендуется дать понятие компьютерного вируса и программы антивирус, рассказать о средствах защиты для безопасной работы в интернете.

Технологии безопасной работы в сети Интернет включают в себя антивирусную защиту компьютера, настройки параметров безопасности для программы браузера.

Залогом безопасной работы в сети Интернет является соблюдение основных правил и рекомендаций, таких как грамотное посещение сайтов и проверка электронной почты. Особенно это становится актуальным при работе на общедоступном компьютере. Обсудите с учащимися правила, мотивируйте из самостоятельно сформулировать каждый из пунктов.

Выводы по Теме 2.

Рекомендуется добавить в памятку следующие пункты для обеспечения безопасности. Безопасность при навигации по сайтам и по приему почты будет достигнута при соблюдении следующих рекомендаций.

1. Установить на своем компьютере антивирусную программу, следить за ее обновлением, реагировать на ее сообщения.
2. Если на вашу электронную почту пришло письмо с прикрепленным к нему незнакомым вложением, ни в коем случае нельзя открывать это вложение, а лучше сразу удалить и очистить корзину в программе чтения почты.
3. Никогда не говорите никому свой пароль.
4. При регистрации на сайте необходимо использовать сложный пароль, состоящий из набора цифр, букв и знаков (не менее 8 символов).
5. Не сохранять свои учетные данные (логин и пароль) для входа в систему на компьютере.
6. Не оставлять без присмотра компьютер с важными сведениями на экране. Закончив работу на общедоступном компьютере, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться конфиденциальные данные.

Тема 3. Социальные и мобильные сети.

Обсудите с учащимися возможные опасности при работе с соцсетями.

Выводы по Теме 3.

Рекомендации, как не стать жертвой мошенников в социальных и мобильных сетях:

1. Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.
2. Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученным посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию. Поспешные действия могут привести к финансовому ущербу.
3. Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.

4. Не торопитесь давать телефон на «один звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.

5. Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения – то и от известных. По возможности, установите на мобильное устройство одну из многих антивирусных программ.

6. Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.

7. Для разблокировки компьютера от вирусов используйте антивирусные программы известных разработчиков, в том числе бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от вируса или исчезновение Интернет-баннера при отправке SMS на короткий номер.