МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
для педагогических работников общеобразовательных организаций по Интернет безопасности детей

Проблема обеспечения информационной безопасности детей в сети Интернет становится актуальной в связи с постоянным ростом несовершеннолетних пользователей. Число пользователей Интернета в России стремительно растет и молодеет, доля детской аудитории среди них очень велика. Для многих российских школьников Интернет становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

Согласно российскому законодательству 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 (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет. Формирование навыков информационной безопасности должно осуществляться на уроках информатики, обществознания, права, ОБЖ и т.д. и во внеурочной деятельности. Этому вопросу должно быть уделено достаточное внимание в программе по воспитанию и социализации обучающихся, которая является частью основной образовательной программы. Знания об Интернет угрозах, умения предотвратить их, защититься от них способствуют социализации детей.

Достичь высоких результатов в обеспечении информационной безопасности детей невозможно без привлечения родителей. Часто родители не понимают и недооценивают угрозы, которым подвергается их ребенок в сети Интернет. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения. На родительских собраниях, лекториях, встречах со специалистами и др. нужно знакомить с видами существующих интернет угроз рекомендациями по обеспечению безопасности ребенка в сети Интернет дома (в зоне ответственности родителей).

Поэтому эффективное обеспечение безопасности детей при работе в сети Интернет является задачей, которую могут и должны решать вместе школа и семья, причем школа инициирует и организует это сотрудничество, просвещая родителей и обучая своих учеников.

Цель проведения занятий по интернет безопасности – обеспечение информационной безопасности обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в среде Интернет.

Занятие: **«Киберугрозы современности: главные правила их распознавания и предотвращения»**

Форма занятия: семинар

Цель: расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

Возраст обучающихся: 6-9 класс.

План занятия:

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Составление листовок «Правила защиты от киберугроз» (20 мин.)
2. Практикум «Опасность 419» (20 мин.)
3. Подведение итогов занятия. (5 мин.)

Ход занятия.

Занятие начинается показом социального видеоролика «Безопасный интернет - детям!»[1]. После просмотра ролика учитель объявляет тему занятия и предлагает ученикам самим сформулировать цель занятия.

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Продолжительность 20 минут.

У каждого ученика на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый ученик должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные ученики зачитывают свои листовки, остальные могут добавлять правила. Листовки собираются после урока для того, чтобы их раздать ученикам других классов.

Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит учеников перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников.

После короткого обсуждения учитель приводит данные За последний год 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждает, что количество кибератак за этот период увеличилось. Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и

[1] http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded

другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%)[2].

Таким образом, можно выделить 3 группы серьезных киберугроз:

1. Шпионское ПО и др. вредоносные программы,
2. Спамы,
3. Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.

При обсуждении внимание учеников обращается на то, откуда могут исходить опасность. На первом месте в этом списке стоят социальные сети. Хотя в последнее время стал распространенными атаки на компьютер через мобильные устройства памяти (флешки).

«Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные.
Если данные действительно важные и дорогостоящие, то для их похищения злоумышленники специально разрабатывают троян, который гарантированно будет работать на компьютерах в той организации, откуда нужно украсть данные. Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «троянов». Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их с большой долей вероятности наверняка найдёт именно сотрудник нужной организации. Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер – лучше сначала отдайте системному администратору, который просканирует её и при необходимости обезвредит.
Бывают и более банальные, но не менее эффективные способы заразить компьютер недостаточно осторожного пользователя. Например, от знакомого по Skype Вам может прийти сообщение в духе «Посмотри, на этой фотографии он так похож на нашего друга (одноклассника)!», ну и,

---

[2] Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf)

конечно, ссылка на саму эту фотографию. При переходе по ссылке фотография почему-то не открывается в браузере, а сохраняется на жесткий диск, но мало кто на это обращает внимание. Хотя они-то как раз и должны насторожить! В общем, когда «фото» не открывается, пользователь «входит» в папку с ним, и видит, что это не просто abcd.jpg, а abcd.jpg.scr, то есть, исполняемый файл, а его компьютер уже заражен вирусом».[3]

После обсуждения листовок на доске должен быть записаны основные правила защиты от киберугроз.

Практикум «Угроза 419».

Цель: формирование навыков распознавание спама в «нигерийских письмах».

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419». «Нигерийские письма» - вид мошенничества, получивший наибольшее развитие с появлением спама. Называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов. С появлением интернета «Нигерийские письма» стали нарицательным понятием.

Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится, у него выманиваются всё большие суммы денег на сборы, взятки и т. д. В худших вариантах жертве предлагается полулегально прибыть в Нигерию, где его либо арестовывали за незаконное прибытие в страну и у него вымогаются деньги за освобождение, либо похищали с целью получения выкупа.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде. Сделка подаётся как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям. Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.

Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности «Нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама.

Подавляющее большинство «нигерийского» спама идет на английском языке, но в 2004-2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни.

---

[3] Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

«Нигерийские письма» являются дидактическим инструментом для формирования навыков распознавания спама и фишинговых атак.

Учитель делит аудиторию на 4 группы. Каждой группе выдает конверт, в котором содержится образец «нигерийского письма» (Приложение) и задание:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.
3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными.

После того, как группы выполнят задание, начинается коллективное обсуждение. Вопросы для обсуждения:

1. Как можно распознать «нигерийское письмо»?
2. Как вы думаете кто авторы «нигерийских писем»?
3. Какую цель преследуют авторы «нигерийских писем»?
4. Можно ли считать безвредными «нигерийские письма»?

Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение. Учитель на доске записывает главные особенности «Нигерийских писем», которые нашли ученики, дополняет, систематизирует.

Подведение итогов занятия.

Приложение.

Карточка 1.

«Меня зовут Бакаре Тунде, я брат первого нигерийского астронавта, майора ВВС Нигерии Абака Тунде.

Мой брат стал первым африканским астронавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым.

Несмотря ни на что мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами.

Вечно ваш,
доктор Бакаре Тунде,
ведущий специалист по астронавтике».

Карточка 2.

«Дорогой друг,

Я послан к вам по поводу моего покойного клиента, фамилия которого совпадает с вашим. Хотя мы еще не встречались друг с другом и раньше, но я верю, что судьба свела нас на ссылка на purpose.It будет лучше, мы утверждаем, и использовать деньги, чем позволить Ecobank топ-чиновников делиться и отвлекать его в своих соответствующих частных счетов, как заброшенный месторождения. Если закон не мог по конституции банка предоставить их должностными лицами право на наследование месторождения умершего клиента, вы и у меня больше прав, потому что умерший может быть ваш дальний родственник, так как он является гражданином вашей страны.
Прежде всего, я работал на него в течение многих лет, поэтому я верю, что он будет счастлив с нашим расположением, чтобы претендовать на фонд особенно когда противоположное состояние деньги незнакомым выступает в подобных старший staffs.You *Ecobank, должны понимать, что в финансовых возможностей учреждения, подобные этой, общей, но не слышал. Люди вкладывают свои деньги в финансовые институты и некоторые из этих счетов являются либо закодированы или конфиденциально ссылка на operated.Normally, когда нечто подобное происходит в финансовом учреждении, сообщается в управлении. Он не опубликованы и соответствующие финансовые учреждения только информирует адвокат своего клиента в зависимости от обстоятельств может быть и ждет реальный наследник, чтобы показать. По истечении указанного периода определяется банком получателя, чтобы придумать, руководство отправляет деньги своим «долгом Re-преобразования Департамента и закрытия счета.*
Теперь вопрос в том, кто управляет «Долг Re-преобразования Департамента", а кто управления? Ответ прост: они председателей, управляющих директоров и членов Правления. Эти люди разделили деньги, и никто не задает вопросы. На самом деле, такой вопрос даже не обсуждается вне заседаний совета директоров. Если мое расположение обращаюсь к вам, и я получить ваше согласие работать в качестве партнеров в передаче фонда, я буду начинать с необходимой правовой процесс, как покойный адвокат. В сущности, мне нужно будет быть предоставлена информация ниже, так что я могу начать с правовой процесс создания ближайших родственников с умершим;
1. Ваше полное имя
2. Возраст
3. Адрес
4. Частная Телефон
5. Профессия
6. Национальность
7. Другой адрес электронной почты ссылка на yahoo.com, ссылка на hotmail.com.
После этого, я должен подготовить и отправить Вам образцы письмо-заявку, которая будет представлена в банке, положив претендовать на его балансе US $ 10,500,000.00. Фонд может быть оплачен на банковский счет, вы будете назначать в установленном порядке или по видам чек кассира обращается в ваше имя и пользу.
Хотя трудно точно оценить время, которое потребуется, чтобы заключить этот вопрос, но я уверен, что весь процесс не займет до 10 рабочих дней с момента вы официально обратиться с банком transfer.I фонда " м предлагается 40% от общего фонда как вознаграждение за вашу помощь, моя будет составлять 50%, и мы будем дарить 9% (US $ 945 000) для благотворительной организации нашего выбора в то время как 1% (US $ 105,000) будет установлена в сторону, с учетом всех прочих расходов, которые могут возникнуть в процессе transfer.I фонда надеемся, что вы оцените это предложение, как я взял многие вещи во внимание, прежде чем предлагать такое соотношение обмена.
Наконец, я хочу, чтобы вы знали, что я столкнулся с трудностями, пытаясь отправить это письмо к вам, как простой сообщении. Именно поэтому я прикрепил его. Поэтому мой скромный совет, который вы открываете новый адрес электронной почты либо в

ссылка на hotmail.com, ссылка на yahoo.com и ссылка на Gmail.com содействовать нашей электронной корреспонденции. Вы также можете связаться со мной через номер +22890945333.
С наилучшими пожеланиями,
Г-н Джонсон Slami Esq.»

Карточка 3.

«Уважаемый Добрый день!
Я юрист, г-н Карл Алекс Хендерсон
Юрист в семье покойного президента Мусу Yaradua, мне было поручено семья в поисках хорошей инвестицией в вашей стране, предпочтительно недвижимость, я должен был обеспечивать конфиденциальность и доверие в этой сделке, так что вы находитесь в лучшем положении, знать больше, чем меня на этом инвестиции.
Деньги наличными $ 25,2 млн., Муса Yaradua семей хотят инвестировать эти деньги в вашу страну с вашей поддержкой, и мы обнаружили, что этот план, чтобы переместить его с помощью дипломатических средств.
Пожалуйста, это очень конфиденциальная и совершенно секретной, я буду лететь вниз, чтобы посмотреть вам в лицо подписывать документы, необходимые для инвестиций, как только вы получите фонд.
Мы предлагаем 10% от общей суммы за вашу помощь в этом проекте, в то время как 5% будет использоваться для любых непредвиденных расходов, которые могут возникнуть при переводе средств.
Я с нетерпением ждем вашего ответа на это письмо.
Если вы примете мое предложение, я хотел бы иметь следующую информацию ниже, чтобы начать процесс.
1. Ваше полное имя:
2. Ваш номер телефона:
3. Ваш возраст:
4. Ваш пол:
5. Род занятий:
6. Вашей страны:
С уважением,
Адвокат г-н Карл Алекс Хендерсон
Сотовые +2348020574082
факс +23417641464»

Карточка 4.

«From: Prince Joe Eboh
Date: Wednesday, April 21, 2004 12:53 PM
Subject: TRANSFER
Принц Джо Эбох
Уважаемый господин,/госпожа,
Надеюсь, что это послание найдет Вас в хорошем здравии. Я - Принц Джо Эбох, Председатель "Комитета заключения контрактов", "Нигерийской Комиссии Развития Дельты (NDDC)", являющейся филиалом нигерийской Национальной Нефтяной Корпорации (NNPC).
Нигерийская Комиссия Развития Дельты (NDDC) была создана покойным Главой государства, генералом Сани Абача, который умер 18-ого июня 1998 года, для управления прибылью, образующейся от продаж нефти и ее субпродуктов.
Предполагаемый ежегодный доход на 1999 год составил свыше 45 миллиардов долларов США, сведения об этом содержаться в отчете Генерального аудитора Федеративной республики Нигерия (FMF A26 ONE 3B Параграф "D") за ноябрь 1999 года.

Я - Председатель Комитета заключения контрактов, и мой комитет исключительно ответственен за то, как и куда должны распределяться денежные средства. Во всех случаях мы действуем от имени Федерального правительства Нигерии. Мой Комитет заключает контракты с иностранными подрядчиками для разработки нефтяных месторождений в районе дельты Нигера.
Так случилось, что в одном из контрактов нам удалось сэкономить US$25,000,000. Но, из-за существования некоторых внутренних законов, запрещающих государственным служащим в Нигерии открытие иностранных счетов, мы не имеем возможности перевести эти деньги за границу.
Однако, эти деньги US$25,000, 000 могут быть оформлены в форме оплаты иностранному подрядчику, поэтому мы хотели бы использовать ваш счет в банке как держателя бенефициария фонда. Мы также достигли соглашения, о том, что Вам будет предоставлена награда за содействие в этой операции в размере 20 % полной суммы, переданной как нашему иностранному партнеру, в то время как 5 % будут сохранены на непредвиденные расходы, которые обе стороны понесут в ходе реализации этой сделки, а остаток в 75 % будет сохранен для членов комитета.
Если Вы решите принять наши условия, Вы должны послать мне немедленно детали вашего счета или открыть новый счет в банке, куда мы сможем осуществить перевод денег в сумме US$25,000, 000 , держателем которой вы будете, до тех пор, пока мы не прибудем в вашу страну за нашей долей. Для нас не важно, каким бизнесом вы занимаетесь.
Все, что нам необходимо, это название вашей компании, ваш личный номер телефона / факса, полное имя, адрес и детали вашего счета в банке, на который будет осуществлен перевод через Apex Bank .
Отметьте, что эта сделка, как ожидается, должна будет реализована в пределах 21 рабочего дня со дня, когда мы предоставим все необходимые сведения Федеральному Министерству финансов, которое одобрит необходимое валютное распределение для перемещения этих средств на ваш счет. Пожалуйста, рассматривайте вышесказанное как конфиденциальные сведения.
Прошу Вас ответить мне как можно скорее.
Спасибо за ваше сотрудничество. Искренне ваш, Принц Джо Эбох»

Подведение итогов занятия.

Занятие завершается ответом на вопрос «Как и для чего нужно знать основные правила безопасной работы в Интернете?».

Для подготовки и проведения занятий по безопасной работе детей в Интернете рекомендуем использовать материалы журнала для педагогов, психологов и родителей «Дети в информационном обществе», который издается Фондом Развития Интернет (http://detionline.com).

Материал для проведений родительского собрания, родительского лектория, заседания родительского клуба «Основные правила защиты наших детей от Интернет опасностей»

Интернет постепенно проникает в каждую организацию, общественное и учебное учреждение, в наши дома. Число пользователей Интернета в России стремительно растет и молодеет, доля молодежи и совсем юной аудитории среди пользователей Всемирной сети очень велика. Для многих из них, он становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

Согласно ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация: 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; 2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом; 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи; 5) оправдывающая противоправное поведение; 6) содержащая нецензурную брань; 7) содержащая информацию порнографического характера.

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. И, это не удивительно: ведь в Интернете можно найти информацию для реферата или доклада, послушать любимую мелодию, проверить свои знания в интернет конкурсах или on-line тестированиях, 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 – как и реальный мир – Сеть тоже может быть опасна: в ней появилась своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Правило 1. Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и

заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2. Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Правило 3. Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Правило 4. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. 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 преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга: Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу; Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. Предупреждение кибербуллинга: Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите

детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга: 1) Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии. 2) Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире. 3) Нервозность при получении новых сообщений. Негативная реакция ребенка на звук электронного письма должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Правило 5. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Правило 6. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Правило 7. Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости. Предвестниками «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство») являются: навязчивое стремление постоянно проверять электронную почту; предвкушение следующего сеанса онлайн; увеличение времени, проводимого онлайн; увеличение количества денег, расходуемых онлайн. Если Вы считаете, что ваши дети, страдают от чрезмерной увлеченности компьютером, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь.

Например, на сайте «Дети онлайн» www.detionline.com открыта линия телефонного и онлайн-консультирования, которая оказывает психологическую и информационную поддержку детям и подросткам, столкнувшимся с различными проблемами в Интернете. На линии помощи «Дети Онлайн», созданной в 2009 г., работают психологи Фонда Развития Интернет и выпускники факультета психологии МГУ имени М.В.

Ломоносова, которые оказывают психологическую и информационную помощь по проблемам безопасного использования Интернета. Целевая аудитория — дети, подростки, родители и работники образовательных и воспитательных учреждений.

Служба Линия помощи «Дети Онлайн» включена в базу единого федерального номера телефона доверия для детей, подростков и их родителей. Обратиться на Линию помощи можно по телефону 8-800-25-000-15, бесплатно позвонив из любой точки страны, либо по электронной почте: helpline@detionline.com. Звонки принимаются в рабочие дни с 9.00 до 18.00 по московскому времени.

Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.

Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет дневник, регулярно посещайте его. Будьте внимательны к вашим детям! Помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

Обеспечение безопасности детей при работе в Интернет.

Безмалый В.Ф.

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. При этом все большее распространение получает подключение по высокоскоростным каналам, как на работе, так и дома. Все большее количество детей получает возможность работать в Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в Интернет. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и взрослые? Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз,

о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Какие угрозы встречаются наиболее часто? Прежде всего:

• Угроза заражения вредоносным ПО. Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

• Доступ к нежелательному содержимому. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера;

• 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. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи;

• Неконтролируемые покупки. Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Именно обеспечению безопасности наших детей при пребывании в сети Интернет и будет посвящена наша статья. Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна. Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

2. Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

3. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.),

использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;
4. Объясните ребенку, что 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. Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;
6. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
7. Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
8. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет– правда. Приучите их спрашивать о том, в чем они не уверены;
9. Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает. Как научить детей отличать правду ото лжи в Интернет?
Следует объяснить детям, что нужно критически относиться к полученным из Интернет материалам, ведь опубликовать информацию в Интернет может абсолютно любой человек. Объясните ребенку, что сегодня практически каждый человек может создать свой сайт и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в Интернет. Как это объяснить ребенку?
• Начните, когда ваш ребенок еще достаточно мал. Ведь сегодня даже дошкольники уже успешно используют сеть Интернет, а значит нужно как можно раньше научить их отделять правду от лжи;
• Не забывайте спрашивать ребенка об увиденном в Интернет. Например, начните с расспросов, для чего служит тот или иной сайт.
• Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в Интернет информацию по другим источникам (по другим сайтам, газетам или журналам). Приучите вашего ребенка советоваться с вами. Не отмахивайтесь от их детских проблем.
• Поощряйте ваших детей использовать различные источники, такие как библиотеки или подарите им энциклопедию на диске, например, «Энциклопедию Кирилла и Мефодия» или Microsoft Encarta. Это поможет научить вашего ребенка использовать сторонние источники информации;
• Научите ребенка пользоваться поиском в Интернет. Покажите, как использовать различные поисковые машины для осуществления поиска;
• Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда. Несмотря на то, что некоторые подобные материалы можно

заблокировать с помощью специальных программных фильтров, не стоит надеяться
на то, что вам удастся отфильтровать все подобные сайты.

Семейное соглашение о работе в Интернет

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними
соглашение по использованию Интернет. Учтите, что в нем вы должны однозначно описать
права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы
на следующие вопросы:

• Какие сайты могут посещать ваши дети и что они могут там делать;
• Сколько времени дети могут проводить в Интернет;
• Что делать, если ваших детей что-то беспокоит при посещении Интернет;
• Как защитить личные данные;
• Как следить за безопасностью;
• Как вести себя вежливо;
• Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по
мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы
должны проверять выполнение соглашения вашими детьми.

Научите вашего ребенка использовать службу мгновенных сообщений

При использовании службы мгновенных сообщений напомните вашему ребенку некоторые
несложные правила безопасности:

• Никогда не заполняйте графы, относящиеся к личным данным, ведь просмотреть их
может каждый;
• Никогда не разговаривайте в Интернет с незнакомыми людьми;
• Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают
всех, с кем они общаются;
• Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает;
• Не следует использовать систему мгновенных сообщений для распространения слухов или сплетен. Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения свашими детьми.

Может ли ваш ребенок стать интернет-зависимым?

Не забывайте, что Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать? Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. В конце-концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.

Советы по безопасности для детей разного возраста

Как показали исследования, проводимые в сети Интернет, наиболее растущим сегментом пользователей Интернет являются дошкольники.

В этом возрасте взрослые будут играть определяющую роль в обучении детей безопасному использованию Интернет.

Что могут делать дети в возрасте 5-6 лет?

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

• В таком возрасте желательно работать в Интернет только в присутствии родителей;

• Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира;

• Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;

• Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

• Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Ваши дети растут, а, следовательно, меняются их интересы.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому в данном возрасте

особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок. Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Что можно посоветовать в плане безопасности в таком возрасте?

• 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;

• Приучите детей, что они должны посещать только те сайты, которые вы разрешили,

т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее;

• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

• Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);

• 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;

• Используйте фильтры электронной почты для блокирования сообщений от

конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах http://www.microsoft.com/rus/athome/security/email/fightspam.mspx;
• 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;
• Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;
• 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.
9-12 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. Советы по безопасности в этом возрасте
• 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;
• Расскажите детям о порнографии в Интернет;
• 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.

13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

• Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет1, руководство по общению в Интернет (в том числе в чатах);
• Компьютер с подключением к Интернет должен находиться в общей комнате. Часы работы в Интернет могут быть легко настроены при помощи средств
• 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 моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
• Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из 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.
• Расскажите детям о порнографии в Интернет.
• 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 по закону дети не могут играть в эти игры. Обеспечивать родительский контроль в Интернет можно с помощью различного программного обеспечения.

Список литературы

1. Методические рекомендации: Методика организации недели «Безопасность
2. Интернет»./Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А.,
3. Кривопалова И. В. - Тамбов, ИПКРО 2012.
4. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет. http://vladbez.spaces.live.com
5. Безмалый В.Ф. Современные угрозы в цифровом мире. http:/BEZMALY.WORDPRESS.COM
6. Сайт «Безопасность детей» ОнлайнЭнциклопедия http://bezopasnost-detej.ru/
7. Сайт «Фонд развития Интернет» http://www.fid.su/
8. Журнал «Дети в информационном обществе» http://detionline.com

ПРИЛОЖЕНИЕ 1

Толковый словарь терминов «Интернет в образовании» [2]

Автоматизированное рабочее место (АРМ) – комплекс технических, программных и методических средств, обслуживающих рабочее место специалиста, обеспечивающий осуществление информационной деятельности, информационного взаимодействия и доступ к информационным ресурсам.

Администратор информационной сети – лицо или группа лиц, занимающихся текущим управлением сети и перспективой ее развития. Основные функции: обеспечение надежности функционирования, определение и выдача адресов и паролей доступа, обеспечение взаимодействия с другими сетями, взаимодействие с администраторами базы данных и пр. Инструмент управления – система сетевого управления.

Асинхронная передача данных – способ передачи и метод извлечения данных из непрерывного потока сообщений с задержкой по времени.

Гипермедиа (Hyper-Media)– гипертекст, в состав которого входит структурированная информация разных типов (текст, иллюстрации, звук, видео и пр.).

Гиперссылка – ссылка от одного электронного информационного объекта к другому (например, из текста к примечанию или элементу списка литературы, из одной энциклопедической статьи к другой). Гиперссылки расставляет разработчик текста в соответствии с требованиями браузера.

Гипертекст (Hyper-Text) – технология обработки информации, обладающая методом организации данных, который характерен следующим: в ***иерархическую базу данных*** помещены участки обычного текста (объекты) с возможными иллюстрациями; между объектами установлены именованные связи, которые являются указателями; на экране помещается участок текста, в котором объекту соответствует визуальная пометка, которой могут служить специально выделенные в тексте слова и окна, содержащие всю или часть информации о данном объекте; эта информация, в свою очередь, может содержать текст, в котором имеются слова, относящиеся к тем или иным объектам, и указатели на другие объекты и (или) соответствующие окна.

Дидактические возможности информационных и коммуникационных технологий:

- незамедлительная обратная связь между пользователем и средствами ИКТ, определяющая реализацию ***интерактивного диалога,*** который характерен тем, что каждый запрос пользователя вызывает ответное действие системы и, наоборот, реплика последней требует реакции пользователя;

- ***компьютерная визуализация учебной информации*** об изучаемом объекте, процессе (наглядное представление на экране: объекта, его составных частей или их моделей; процесса или его модели, в том числе скрытого в реальном мире; графической интерпретации исследуемой закономерности изучаемого процесса);
- ***компьютерное моделирование*** изучаемых или исследуемых объектов, их отношений, явлений, процессов, протекающих как реально, так и «виртуально» (представление на экране математической, информационно-описательной, наглядной модели адекватно оригиналу);
- ***архивирование***, хранение любых объемов информации с возможностью легкого доступа к ней, ее передачи, тиражирования;
- ***автоматизация процессов вычислительной, информационно-поисковой деятельности***, и ***операций*** по сбору, обработке, передаче, отображению, тиражированию информации, архивного хранения достаточно больших объемов информации с возможностью легкого доступа и обращения пользователя к ней, а также процессов обработки результатов учебного эксперимента (как реально протекающего, так виртуального), его экранного представления с возможностью многократного повторения фрагмента или самого эксперимента;
- ***автоматизация процессов информационно-методического обеспечения, организационного управления*** учебной деятельностью и контроля результатов усвоения.

Диалоговый режим – режим прямого взаимодействия между человеком и компьютером, компьютерами в сети или между компьютером и периферийным устройством, при котором связь между взаимодействующими системами не прерывается. Часто называется интерактивным режимом, или (при работе в сети) режимом «on-line».

Дистанционное обучение (дистантное обучение, распределенное обучение) – процесс передачи знаний, формирования умений и навыков при интерактивном взаимодействии как между обучающим и обучающимся, так и между ними и интерактивным источником информационного ресурса (например, Web-сайта или Web-страницы), отражающий все присущие учебному процессу компоненты (цели, содержание, методы, организационные формы, средства обучения), осуществляемый в условиях реализации средств ИКТ (незамедлительная обратная связь между обучаемым и средством обучения; компьютерная визуализация учебной информации; архивное хранение больших объемов информации, их передача и обработка; автоматизация процессов вычислительной, информационно-поисковой деятельности, обработки результатов учебного эксперимента; автоматизация процессов информационно-методического обеспечения, организационного управления учебной деятельностью и контроля результатов усвоения учебного материала).

Здоровьесберегающие технологии в условиях информатизации образования – система мер по охране и укреплению здоровья учащихся, учитывающая важнейшие характеристики образовательной среды, реализованной на базе средств ИКТ, и условия жизни учащегося, воздействующие на здоровье.

Интерактивный диалог – взаимодействие пользователя с программной (программно-аппаратной) системой, характеризующееся (в отличие от диалогового, предполагающего обмен текстовыми командами, запросами и ответами, приглашениями) реализацией более развитых средств ведения диалога (например, возможность задавать вопросы в произвольной форме, с использованием «ключевого» слова, в форме с ограниченным набором символов и пр.); при этом обеспечивается возможность выбора вариантов содержания учебного материала, режима работы с ним. ***Интерактивный режим взаимодействия пользователя с ЭВМ*** характерен тем, что каждый его запрос вызывает ответное действие программы и, наоборот, реплика последней требует реакции пользователя.

Интернет-провайдер – организация, обеспечивающая доступ в Интернет для других пользователей. Деятельность провайдера ориентирована на поддержку и оплату высокоскоростного канала доступа в Интернет, провайдер обеспечивает подключение к нему за соответствующую плату множества внешних пользователей, одновременно предоставляя ряд дополнительных услуг: размещение личных сайтов, адреса электронной почты и пр.

Интерфейс – средство сопряжения устройств вычислительной техники (аппаратный интерфейс); организация взаимодействия человека и компьютерной программы (программный интерфейс).

Информатизация образования – процесс обеспечения сферы образования методологией и практикой разработки и оптимального использования средств ИКТ, ориентированных на реализацию психолого-педагогических целей обучения, воспитания. Вместе с тем, ***информатизация образования*** рассматривается как область педагогического знания, интегрирующая научные направления психолого-педагогических, социальных, физиолого-гигиенических, технико-технологических исследований, находящихся в определенных взаимосвязях, отношениях между собой и образующих определенную целостность, которая ориентирована на обеспечение сферы образования теорией, технологией и практикой решения образовательных проблем и задач.

Информатизация общества – глобальный социальный процесс, особенность которого состоит в том, что доминирующим видом деятельности в сфере общественного производства является сбор, накопление, обработка, хранение, передача, использование, продуцирование информации, осуществляемые на основе современных средств микропроцессорной и

вычислительной техники, а также разнообразных средств информационного взаимодействия и обмена. ***Информатизация общества обеспечивает*** активное использование постоянно расширяющегося интеллектуального потенциала общества, сконцентрированного в печатном фонде, в научной, производственной и других видах деятельности его членов; интеграцию информационных технологий с научными, производственными, инициирующую развитие всех сфер общественного производства, интеллектуализацию трудовой деятельности; высокий уровень информационного обслуживания, доступ любого члена общества к источникам достоверной информации, визуализацию представляемой информации, существенность используемых данных.

Информационная деятельность – деятельность по регистрации, сбору, обработке, хранению, передаче, отображению, транслированию, тиражированию, продуцированию информации об объектах, явлениях, процессах, в том числе реально протекающих, и скоростная передача любых объемов информации, представленной в различной форме, при реализации дидактических возможностей ИКТ.

Информационные технологии (ИТ) – практическая часть научной области информатики, представляющая собой совокупность средств, способов, методов автоматизированного сбора, обработки, хранения, передачи, использования, продуцирования информации для получения определенных, заведомо ожидаемых, результатов. Ее характерные особенности:

- реализация возможностей современных программных, программно-аппаратных и технических средств и устройств, функционирующих на базе микропроцессорной и вычислительной техники, средств и систем передачи, транслирования информационных ресурсов, информационного обмена;
- использование специальных формализмов (логико-лингвистических моделей) для представления декларативных и процедурных знаний в электронной форме; при этом логико-лингвистическое моделирование резко расширяет возможности решения задач для трудно или совсем неформализуемых областей знаний и сфер деятельности;
- обеспечение прямого (без посредников) доступа к диалоговому режиму при использовании профессиональных языков программирования и средств искусственного интеллекта;
- обеспечение простоты процесса взаимодействия пользователя с компьютером, исключение необходимости регулятивного сопровождения.

Информационное взаимодействие образовательного назначения, реализованное на базе средств ИКТ – деятельность, направленная на сбор, обработку, применение и передачу информации, осуществляемую

субъектами образовательного процесса (обучающийся, обучаемый, средство обучения, функционирующее на базе средств ИКТ) и обеспечивающую психолого-педагогическое воздействие, ориентированное: на развитие творческого потенциала индивида; на формирование системы знаний определенной предметной области; на формирование комплекса умений и навыков осуществления учебной деятельности по изучению закономерностей предметной области. ***Структура информационного взаимодействия*** – это внутренняя форма организации информационного взаимодействия, выступающая как единство устойчивых взаимосвязей между субъектами взаимодействия.

Образовательная среда – совокупность условий, обеспечивающих осуществление деятельности пользователя с информационным ресурсом (в том числе распределенным информационным ресурсом), с помощью интерактивных средств ИКТ и взаимодействующих с ним как с субъектом информационного общения и личностью. ***Образовательная среда включает:*** множество информационных объектов и связей между ними; средства и технологии сбора, накопления, передачи (транслирования), обработки, продуцирования и распространения информации, собственно знания, средства воспроизведения аудиовизуальной информации; организационные и юридические структуры, поддерживающие информационные процессы.

Информационный объект – обобщающее понятие, описывающее различные виды объектов: простых (звук, изображение, текст, число) и комплексных структурированных (элемент, база данных, таблица, гипертекст, гипермедиа).

Информационный ресурс – совокупность всей получаемой и накапливаемой информации в процессе развития науки, культуры, образования, практической деятельности людей и функционирования специальных устройств, используемых в общественном производстве и управлении.

Компьютерная зависимость (патологический гемблинг) – психологическая зависимость от виртуальной среды, реализованной на базе средств ИКТ.

Организационное управление учебным заведением на основе систем баз данных и средств телекоммуникаций – упорядочение, приведение к определенной структуре и на единой методологической основе системы информационно-методического обеспечения и ведения делопроизводства, сохранение ее структуры, поддержание режима ее деятельности, состояния, ведущие к достижению определенных целей. К целям относятся следующие: поддержание заданной степени комфорта деятельности работника сферы образования при решении задач реализации возможностей современных средств ИКТ в процессе

информационно-методического обеспечения и организационного управления, в том числе и при ведении делопроизводства; формирование и развитие его информационной культуры, соответствующей этапу информатизации и коммуникации современного общества.

Открытая тестовая система – информационная (программная) система, предоставляющая преподавателю, методисту, автору учебника возможность создавать новые тесты или изменять существующие.

Пользователь – человек, организация, система, использующие в своей работе в той или иной степени информационную систему, функционирующую на базе ИКТ, в том числе вычислительную систему, базу данных, сеть и пр. ***Конечный пользователь*** – это пользователь, как правило, не работающий непосредственно с системой, но использующий результат ее функционирования.

Предметная (учебная) среда – условия информационного взаимодействия в процессе обучения определенному учебному предмету (предметам) между учителем, учеником и средствами обучения, функционирующими на базе средств ИКТ.

Представление знаний – способ формального выражения всех видов знаний (представимых для машинной обработки), который используется для обработки знаний в системах искусственного интеллекта; способ преобразования человеческих знаний в совокупности символов и связей между ними, пригодных для хранения в памяти компьютера и использования их для решения задач на ЭВМ.

Продуцирование информации – деятельность по созданию информационного продукта, отличающегося определенными существенными признаками, характеризующими его качество или принадлежность к определенной сфере использования.

Распределенный информационный ресурс образовательного назначения – совокупность научно-педагогической, учебно-методической, хрестоматийной, нормативно-инструктивной, технической, организационной информации, программных средств и систем образовательного назначения, представленных в формате, обеспечивающем их технико-технологическую поддержку в локальных и глобальной сетях и хранящихся на различных серверах.

Сайт – набор Web-страниц, составляющих единое целое (посвященных какой-либо одной тематике, либо принадлежащих одному и тому же автору), как правило, размещенных на одном и том же сервере, имеющих одно и то же доменное имя и связанных между собой перекрестными ссылками.

Санитарные правила и нормы – свод нормативной документации по обеспечению безопасного применения элементов компьютерной

техники и прочих компонентов информационного обеспечения человека.

Синхронная передача данных – способ осуществления информационного обмена в реальном времени.

Содержание информационных ресурсов образовательного назначения (контент) – содержание различных видов научно-педагогических, учебно-методических, информационных, инструктивно-организационных, нормативных, технических и других материалов, представленных в электронном виде.

Средства информационных и коммуникационных технологий (средства ИКТ) – программные, программно-аппаратные и технические средства и устройства, функционирующие на базе микропроцессорной, вычислительной техники, а также современных средств и систем транслирования информации, информационного обмена, обеспечивающие операции по сбору, накоплению, хранению, обработке, передаче, формализации, продуцированию информации и возможность доступа к информационным ресурсам, в том числе сетевым. ***К средствам ИКТ относятся:*** ЭВМ, ПЭВМ; комплекты терминального оборудования для ЭВМ всех классов, локальные вычислительные сети, устройства ввода-вывода информации, средства ввода и манипулирования текстовой и графической информацией, средства архивного хранения любых объемов информации и другое периферийное оборудование, сопрягаемое с компьютером; устройства для преобразования данных из текстовой, графической, звуковой форм представления данных, видео информации в цифровую и обратно; средства и устройства манипулирования аудиовизуальной информацией (на базе технологий мультимедиа и «Виртуальная реальность»); системы искусственного интеллекта; системы машинной графики, программные комплексы (языки программирования, трансляторы, компиляторы, операционные системы, пакеты прикладных программ и пр.) и др.; все современные средства связи, обеспечивающие информационное взаимодействие пользователей как на локальном уровне (например, в рамках одной организации или нескольких организаций), так и глобальном (в рамках Всемирной информационной сети Интернет).

Телекоммуникационная сеть реализует синтез компьютерных сетей и средств телефонной, телевизионной, спутниковой связи. Эти комплексы объединяются в системы передачи-приема для информационного обеспечения региональных территорий. При этом возможен обмен текстовой, графической, звуковой, видеоинформацией в виде запросов пользователя и получения им ответов из центрального информационного банка данных. Осуществление информационного обмена производится в реальном времени (синхронная телекоммуникация), с задержкой по времени (асинхронная телекоммуникация, в том числе электронная почта). Использование

телекоммуникационных сетей в образовательных целях позволяет: формировать умения составлять информационно емкие сообщения, сортировать информацию по определенному(ым) признаку(ам); обеспечивать непрерывность общения пользователя с центральным информационным банком данных; тиражировать передовые педагогические технологии как при одновременном обучении нескольких групп в различных регионах страны, так и при обучении территориально удаленных групп, «распределенных» по интересам и объединенных в творческие коллективы.

Телеконференции – сервис, предназначенный для коллективных текстовых коммуникаций (массового информирования, совместного обсуждения, информационного взаимодействия и пр.). Виды телеконференций*:*

- ***закрытые*** – доступ ко всей информации и возможность отправки сообщений разрешается ограниченному кругу зарегистрированных пользователей;
- ***модерируемые*** – управляемые ***администратором*** (***модератором***), который определяет права остальных участников по доступу к имеющейся информации и отправке новых сообщений; как правило, чтение сообщений при этом разрешено всем желающим, отправка же сообщений отслеживается модератором (в том числе заранее до размещения сообщений в конференции – ***премодерация***), который может удалять сообщения, не соответствующие тематике конференции или содержащие недопустимую (нецензурную, секретную и т.п. информацию), либо запрещать отправку сообщений отдельным пользователям в качестве штрафа;
- ***свободные*** – конференции, полный доступ к которым разрешен всем желающим (соответствие сообщений тематике и правилам хорошего тона лежит при этом на совести их авторов).

Тест – измерительная процедура, включающая инструкцию и набор заданий, прошедшая апробацию и стандартизацию.

Тестирование – измерение или формализованное оценивание на основе тестов, завершающееся количественной оценкой, опирающейся на статистически обоснованные шкалы и нормы.

Тестовое задание – минимальная составляющая единица теста, которая состоит из условия (вопроса) и, в зависимости от типа задания, может содержать, или не содержать набор ответов для выбора.

Технология информационного взаимодействия образовательного назначения в условиях использования средств ИКТ – совокупность детерминированных средств и методов, реализованных на базе ИКТ, обеспечивающих информационное взаимодействие, реализация которого определяет заранее заданный результат (педагогическое воздействие, направленное на достижение определенных образовательных целей).

Технология телекоммуникации – совокупность приемов, методов, способов и средств обработки, информационного обмена, транспортировки, транслирования информации, представленной в любом виде (символьная, текстовая, графическая, аудио-, видеоинформация) с использованием современных средств связи, обеспечивающих информационное взаимодействие пользователей как на локальном уровне (например, в рамках одной организации или нескольких организаций), так и глобальном, в том числе и в рамках Всемирной информационной сети Интернет.

Формализация знаний – представление знаний в формализованной структуре средствами математической логики. Построение логических исчислений в математической логике позволяет применить ее средства к формализации целых областей науки. При этом области знания, формализованные средствами математической логики, приобретают вид формальных систем.

Формализация информации – формальное представление информации в виде символической записи и определенной формализованной структуры, адекватно отражающих свойства данной информации и обладающей ее существенными признаками.

Фрейм – хранимая в компьютерной программе структура данных, описывающая объект или понятие через атрибуты и числовые значения.

Электромагнитная безопасность – предотвращение вредного для организма пользователя влияния переменного электромагнитного и электростатического полей при использовании компьютера.

Электронная библиотека – программный комплекс, обеспечивающий возможность накопления и предоставления пользователю на основе ИКТ полнотекстовых информационных ресурсов, представленных в электронной форме, снабженный собственной системой документирования и безопасности.

Электронная почта (e-mail) – сервис Интернет, осуществляющий возможность разделенного во времени обмена текстовыми сообщениями, в том числе дополненными любыми файлами (***вложения, attachment***), между двумя и более пользователями. Работа пользователя с письмами (написание, редактирование, чтение, добавление/извлечение вложений и пр.) осуществляется в режиме off-line с помощью специальной программы – ***почтового клиента***; соединение с Интернетом требуется только для отправки писем, а также для приема писем, накопленных для данного пользователя (адресата).

Электронное тестирование – компонент образовательного электронного издания, функционирующего на базе ИКТ, являющийся аналогом традиционного тестирования. В случае электронного тестирования осуществляется предъявление теста, фиксация результата, реализуются

те или иные связанные с этим алгоритмы (например, возможность или невозможность возврата к уже выполненному или пропущенному заданию, ограничение времени, отведенного на один тест и т.п.).

Электронные конференции («электронные доски объявлений») позволяют принять участие в обсуждении интересующих проблем самому широкому кругу желающих, обеспечивая при этом участникам возможность одновременного «присутствия» сразу на нескольких конференциях, не отходя от своих компьютеров.

Электронный учебник (ЭУ) – это информационная система (программная реализация) комплексного назначения, обеспечивающая посредством единой прикладной программы, без обращения к бумажным носителям информации, реализацию дидактических возможностей ИКТ во всех звеньях процесса обучения: постановку познавательной задачи; предъявление содержания учебного материала; организацию применения первично полученных знаний (организацию деятельности по выполнению отдельных заданий, в результате которой происходит формирование научных знаний); организацию обращения к сетевым информационным ресурсам; организацию подготовки к дальнейшей учебной деятельности (задание ориентиров для самообразования, для чтения дополнительной литературы); обратную связь, контроль деятельности учащихся. При этом ЭУ, обеспечивая непрерывность и полноту дидактического цикла процесса обучения, предоставляет теоретический материал, организует тренировочную учебную деятельность и контроль уровня знаний, информационно-поисковую деятельность, математическое и имитационное моделирование с компьютерной визуализацией и сервисные функции.

Библиография:

1. *Платонов К.К.* Краткий словарь системы психологических понятий. – 2-е изд., перераб., доп. – М.: Высшая школа, 1984. – 86 с.

2. Толковый словарь терминов понятийного аппарата информатизации образования / составители *И.В. Роберт, Т.А. Лавина*. – М.: БИНОМ. Лаборатория знаний, 2012. - 69 с.

3. Dictionary of Computer and Internet Term / *Duglas A. Downing, Micael A.* Covington, Melody Mauldin Covington. – 8th ed.