Государственное автономное профессиональное образовательное учреждение
Чувашской Республики
«Канашский транспортно-энергетический техникум»
Министерства образования и молодежной политики
Чувашской Республики

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

для организации и проведения кураторских часов по безопасности в сети Интернет

г. Канаш
Чувашская Республика

Методические указания предназначены для педагогических работников профессиональных образовательных организаций и могут быть использованы при организации и проведении тематического урока для студентов 1-го и 2-го курса, посвященного вопросам безопасности в сети Интернет.

Методические указания информируют о теоретических и практических аспектах организации защиты несовершеннолетних студентов от информации, причиняющей вред их здоровью и развитию.

Методические указания содержат: методическое обоснование урока, теоретический материал для преподавателя и студентов, план проведения урока, примерный план–конспект, приложения (анкета, задание для домашней работы, толковый словарь терминов, перечень информационных ресурсов, памятка), список литературы и информационных источников, оглавление.

Методические указания могут быть рекомендованы к использованию студентами и преподавателями ГАПОУ «КанТЭТ» Минобразования Чувашии

Авторы:

Заместитель директора по УВР ГАПОУ «КанТЭТ» Минобразования Чувашии Т.М. Данилова

Педагог-психолог ГАПОУ «КанТЭТ» Минобразования Чувашии

Д.Р. Мифтахутдинова

Рецензент:

Директор ГАПОУ «КанТЭТ» Минобразования Чуваши И.Р. Назмутдинов

Оглавление

1. Методическое обоснование урока

В соответствии с инициативой Валентины Ивановны Матвиенко, Председателя Совета Федерации Федерального Собрания Российской Федерации, во всех образовательных организациях Российской Федерации в октябре 2014 года проводится Единый урок по безопасности в сети Интернет (далее – Урок).

Организаторами проведения мероприятий в рамках Урока являются Совет Федерации Федерального Собрания Российской Федерации, Министерство образования и науки Российской Федерации, Министерство связи и массовых коммуникаций Российской Федерации при участии экспертного IT-сообщества.

Как отметила председатель Временной Комиссии СФ, заместитель председателя Комитета СФ по конституционному законодательству и государственному строительству Людмила Бокова, сегодня защита детей от угроз в Интернете стала одним приоритетных направлений.

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 и студентов 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 и подростков, так как может нанести вред их физическому и психическому здоровью, духовномуи 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 студентов, 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 образовательная организация и семья, причем образовательная организация инициирует и организует это сотрудничество, просвещая родителей и обучая своих студентов.

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

В рамках урока «Интернет-безопасность» на 1-2 курсах целесообразно познакомить студентов с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве: Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; № 252-ФЗ «О

внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки.)

Ознакомить студентов с адресами помощи в случае интернет угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Необходимо обратить внимание студентов на классификацию вредоносных информационных ресурсов:

- информация, причиняющая вред здоровью и (или) развитию детей;
- информация, запрещенная для распространения среди детей;
- информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:

- перечень рисков, подстерегающих ребенка в сети Интернет;
- рекомендации по грамотному использованию электронной почты;
- технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить студентов инструкциями по безопасному общению в чатах; советами по профилактике и преодолению Интернет–зависимости; общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете: нежелательные программы; защита личных данных; мошенничество; виртуальные “друзья”; пиратство; on-line-игры; этика; критический подход к информации.

Обеспечить студентов информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации.

Возможные формы проведения урока: лекция, деловая игра, урок–презентация проектов, мозговой штурм «Интернет-безопасность», дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

2. Теоретический материал

1) Безопасность в интернете.

1.1 Общая безопасность в интернете.

В наши дни интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их.

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы — например, вирусное программное обеспечение (далее — вирусы), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы.

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Рекомендации:

- Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.

- Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключать к своему компьютеру непроверенные съемные носители.
- Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Мошеннические письма.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Пример «нигерийского письма»:

«Дорогой друг!

Я миссис Сесе-секо, вдова бывшего президента Заира (ныне Демократической республики Конго) Мобуту Сесе-секо. Я вынуждена написать Вам это письмо. Это в связи с моими нынешними обстоятельствами и ситуацией. Я спаслась вместе со своим мужем и двумя сыновьями Альфредом и Башером в Абиджан, Кот-д'Ивуар, где мы и поселились - затем мы переехали в Марокко, где мой муж умер от рака. У меня есть банковский счет на сумму 18 000 000 (восемнадцать миллионов) долларов США. Мне нужно ваше желание помочь нам - чтобы вы получили эти деньги для нас, в таком случае я представлю Вас моему сыну Альфреду, который имеет право получить эти деньги. Я хочу инвестировать эти деньги, но не хочу, чтобы было известно, что это делаю я. Мне хочется приобрести недвижимость и акции транснациональных компаний, а также вложиться в надежные и неспекулятивные дела, которые Вы посоветуете.

Искренне Ваша,

Миссис Мариам М. Сесе-секо»

Рекомендации:

- Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.
- Игнорировать такие письма.

Получение доступа к аккаунтам в социальных сетях и других сервисах.

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи жертвы следующими способами:

- Заставить жертву ввести свои данные на поддельном сайте.
- Подобрать пароль жертвы, если он не вляется сложным.
- Восстановить пароль жертвы с использованием “секретного вопроса” или введенного ящика электронной почты.
- Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. Фишинг (англ. **phishing**, от **fishing** — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации:

- Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

- Никому не сообщать свой пароль.
- Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.
- Не передавать учетные данные – логины и пароли – по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).
- Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

2.2 Безопасность платежей в интернете.

В 2013 году ущерб от карточного мошенничества в России составил 4,6 млрд рублей (данные FICO), за год этот показатель вырос на треть. Это четвертое место по объему карточного мошенничества среди стран Европы (после Великобритании, Франции и Германии).

При этом большая часть мошеннических операций в интернете оказывается успешными по тем же причинам, что и в реальной жизни, – из-за таких людских качеств, как невнимательность, неосведомленность, наивность, беспечность.

В этом блоке мы постараемся выделить основные типы платежного мошенничества, с которыми сегодня сталкиваются пользователи Рунета, и постараемся дать основные рекомендации, как избежать обмана.

2.2.1 Распространенные примеры платежного мошенничества.

Фиктивные звонки от платежных сервисов

Мошенник может позвонить и представиться сотрудником банка или Яндекс.Денег и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька.

Рекомендации:

- Помнить, что банки и платежные сервисы никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из SMS.

- Никому не сообщать пароли, пин-коды и коды из SMS от своего кошелька или банковской карты.

Выманивание SMS-пароля незнакомцем

Пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа. Сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Рекомендации:

- Никому не сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, а также мобильных операторов.

Фальшивые письма от платежных сервисов

Пользователь может получить фальшивое письмо от имени Яндекс.Денег, своего банка или других платежных сервисов. Например, о том, что его счет заблокирован и для разблокировки необходимо перейти по ссылке и ввести свои данные.

Единственная цель таких писем — заставить пользователя перейти на поддельный (фишинговый) сайт и ввести там свои персональные данные, которые будут украдены. В дальнейшем эти данные могут быть использованы, например, для доступа к счету пользователя. Кроме того, на таком сайте компьютер может быть заражен вирусом.

Рекомендации:

- Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.
- Не переходить по ссылкам из таких писем и не вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка, Яндекс.Денег или другого платежного сервиса.

- Перед вводом своих платежных данных на каких-либо сайтах проверять название сайта в браузере. Например, вместо money.yandex.ru фальшивый сайт может называться money.yanex.ru

Фальшивые выигрыши в лотереи

Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет в Яндекс.Деньгах. При этом, конечно же, никакого обещанного приза пользователь не получит.

Признаки фальшивой лотереи:

- Пользователь никогда не принимал участие в этой лотерее и вообще ничего о ней не знает;
- Пользователь никогда не оставлял своих личных данных на этом ресурсе или в этой организации, от имени которой приходит письмо;
- Сообщение составлено безграмотно, с орфографическими ошибками;
- Почтовый адрес отправителя – общедоступный почтовый сервис. Например, gmail.com, mail.ru, yandex.ru.

Фальшивые сайты авиабилетов

В интернете появилось множество сайтов, продающих поддельные авиабилеты. Цены на таких сайтах выгодно отличаются от других официальных онлайн-площадок для покупки билетов. Дизайн сайта при этом может выглядеть вполне аккуратно, а процесс платежа казаться привычным. На электронную почту даже придет подтверждающая бронь. Тем не менее покупка билета будет фиктивной, о чем пользователь может узнать только уже в аэропорту или позвонив в авиакомпанию.

Рекомендации:

- Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в интернете. Если не удается найти положительные отзывы или нет вообще никаких пользовательских сообщений об этом ресурсе, это должно насторожить. Сайт может быть создан за один день, а закрыться уже

на следующий или даже сразу после того, как на нем будет совершено несколько покупок.

Слишком выгодные покупки

Выгодную, но фальшивую покупку могут предложить пользователю где угодно – в интернет-магазине, в группе в соцсети, по электронной почте. На первый взгляд, объяснение может быть правдоподобное: подарили – не понравилось, это — распродажа конфискованного на границе товара и т.д. Оплатить такой товар предлагается онлайн — переведя деньги на банковскую карту, электронный кошелек или мобильный номер.

Рекомендации:

- Не доверять объявлениям о подозрительно дешевых товарах;
- Перед покупкой искать отзывы в интернете об интернет-магазине или частном продавце, который предлагает товар. Если информации нет или ее недостаточно, отказаться от покупки.

Фальшивые квитанции

Подделать могут не только сайт, но и бумажную квитанцию – например, за ЖКУ. (Также по поддельным квитанциям могут предлагать оплатить доставку книг, журналов и т.д. Для этих случаев действуют рекомендации из пункта «Слишком выгодные покупки».)

Рекомендации:

- Проверять реквизиты, указанные в платежке. Если они не совпадают с прежними, не оплачивать по счету. Информацию о смене реквизитов можно проверить по официальным телефонам (на квитанции они могут быть неверные).
- Проверять номер своего лицевого счета, указанный на платежке за ЖКУ. Он всегда один.
- Обратить внимание на дату получения платежки. Как правило, мошенники приносят поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи.

- Настроить онлайн-платежи на заранее проверенные реквизиты и платить только по ним через проверенные сайты (сервис «Городские платежи», интернет-банк «Сбербанк.Онлайн», Альфа-Банк и др.).

Выпрашивание денег со взломанных аккаунтов в соцсетях или мессенджерах

Мошенник может попросить денег в долг под видом знакомого – например, через взломанный аккаунт в соцсетях или Skype. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

Рекомендации:

- Всегда лучше перезвонить знакомому и уточнить, правда ли он сейчас нуждается в деньгах.
- Если возможности позвонить нет, можно задать какой-нибудь проверочный вопрос, ответ на который может знать только знакомый.

Фальшивые SMS якобы от знакомого

Мошенник может прислать SMS родителям пользователя с неизвестного номера, но якобы от имени пользователя. Например: «Мама, я попал в аварию, срочно нужны деньги, переведи их, пожалуйста, на этот номер телефона». «Папа, у меня проблемы, я в больнице, срочно нужны деньги, кинь их, пожалуйста, на этот кошелек. Маме не говори». Цель мошенника – выманить деньги у близких пользователя: они сами переведут их на указанный мобильный номер, электронный кошелёк или банковскую карту (в зависимости от того, какой способ будет указан в SMS).

Рекомендации:

- Связаться лично с пользователем, от имени которого прислано SMS, чтобы проверить информацию. Например, позвонить ему.

Бесплатное скачивание файлов с подпиской

Часто, чтобы скачать бесплатный файл или посмотреть видео в хорошем качестве без рекламы, сайты предлагают ввести мобильный номер. Если сделать это, включится подписка и с указанного номера могут начать списываться деньги.

Рекомендации:

- Не указывать свой мобильный номер на незнакомых сайтах.
- Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.

2.2.2. Платежные данные, которые нельзя раскрывать.

Что делать? — если...

…вы потеряли карту.

Срочно позвоните в банк, попросите ее заблокировать и перевыпустить. Желательно, с новым номером. Пока вы не заблокируете карту, любой, у кого она окажется в руках, сможет воспользоваться ей — например, оплатить дорогую покупку в интернет-магазине.

…вам пришло уведомление о платеже, который вы не совершали.

Подайте в банк заявление о чарджбеке (отмене операции). В нём максимально подробно опишите произошедшее. Банк рассмотрит ваше обращение и вернет вам деньги. Не затягивайте с подачей заявления, чтобы обработка вашего чарджбека успела произойти в срок от 30 до 60 дней с момента совершения операции.

…вы забыли пароль от электронного кошелька.

Зайдите на сайт платежного сервиса и нажмите на ссылку "Восстановить пароль", система запросит мобильный номер, к которому привязан кошелёк. Укажите его, и на него придёт SMS с кодом для восстановления пароля.

2.2.3. Безопасность при оплате картами

Не сообщайте номер карты другим людям

Избежать проблем несложно, если придерживаться следующих рекомендаций:

- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.
- Заведите отдельную карту для покупок в интернете.
- Используйте для покупок в интернете только личный компьютер.
- Регулярно обновляйте антивирусную защиту компьютера.
- Старайтесь делать покупки в известных и проверенных интернет-магазинах.

- Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах.
- Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

3. План проведения урока «Интернет-безопасность»

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

Задачи:

1) информирование студентов о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование студентов о способах незаконного распространения такой информации в информационно–телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление студентов с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение студентов правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5) предупреждение совершения студентами правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет - безопасности студенты должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной или иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

По итогам проведения уроков проводится итоговое анкетирование по теме «Безопасный интернет» (Приложение 1).

Для подготовки к уроку предлагается использовать «Толковый словарь» (Приложение 3) и информационные Интернет-ресурсы образовательного назначения (Приложение 4).

В конце урока студентам предлагается выдать памятки (Приложение 5)


Я ИМЕЮ ПРАВО
НА БЕЗОПАСНЫЙ
ИНТЕРНЕТ

План - конспект урока на тему: «Безопасный Интернет»

(1–2 курс)

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

Задачи:

- изучение информированность пользователей о безопасной работе в сети Интернет;
- знакомство с правилами безопасной работы в сети Интернет;
- ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;
- формирование информационной культуры студентов, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами;
- воспитание дисциплинированности при работе в сети.

Студентыдолжны знать:

- перечень информационных услуг сети Интернет;
- правила безопасной работы в сети Интернет;
- опасности глобальной компьютерной сети.

Студенты должны уметь:

- ответственно относиться к использованию on-line-технологий;
- работать с Web-браузером;
- пользоваться информационными ресурсами;
- искать информацию в сети Интернет.

Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Ссылки на web-ресурсы:

1) http://www.kaspersky.ru– антивирус «Лаборатория Касперского»;
2) http://www.onlandia.org.ua/rus/- безопасная web-зона;
3) http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета;
4) http://www.saferinternet.ru– портал Российского Оргкомитета по безопасному использованию Интернета;
5) http://content-filtering.ru– Интернет СМИ «Ваш личный Интернет»;
6) http://www.rgdb.ru– Российская государственная детская библиотека.

Этапы урока:

1. Организация начала урока. Постановка цели урока.
   Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html.Постановка темы и главного вопроса урока.
2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения студентов, обсуждение с разъяснением преподавателем).
3. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.
4. Закрепление изученного материала. Рекомендации по правилам безопасной работы. Тестирование.
5. Подведение итогов урока. Оценка работы группы. Домашнее задание. **Ход урока**

1. Организация начала урока. Постановка цели урока.

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всѐм мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. Возможно, что прямо сейчас.

Просмотр видеороликов(по выбору):

- Как оставаться в безопасности на YouTube

http://www.youtube.com/watch?v=HbVgg6-3EWo&feature=autoplay&list=PLD70B32DF5C50A1D7&playnext=1;

- Развлечения и безопасность в Интернете

http://www.youtube.com/watch?v=3Ap1rKr0RCE&feature=relmfu;

- Остерегайся мошенничества в Интернете

http://www.youtube.com/watch?v=AMCsvZXCd9w&feature=BFa&list=PLD70B32DF5C50A1D7&lf=autoplay;

- Мир глазами Gmail - ЗАЩИТА ОТ СПАМА

http://www.youtube.com/watch?v=xRSnLKveMpY&feature=relmfu

Итак, как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет».

Главный вопрос урока: Как сделать работу в сети безопасной?

2. Изучение нового материала.

Игра «За или против».

Учитель предлагает игру «За или против». На слайде - несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

- Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
- Интернет – это глобальный рекламный ресурс. И это хорошо!
- Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.
- Интернет является мощным антидепрессантом.
- В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли

Учитель предлагает студентам ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». (Целесообразно заранее нескольким студентам подготовить короткие сообщения по темам: «Интернет-зависимость», «Вредоносные и нежелательные программы», «Психологическое воздействие на человека через Интернет», «Материалы нежелательного содержания», «Интернет мошенники»).

Анализ ситуации. Для разъяснения студентам незнакомых определений и терминов прилагается «Толковый словарь» (Приложение 3).

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако, очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту

Преподаватель предлагает ответить на главный вопрос урока – «Как сделать работу в сети безопасной?»

3. Практическая работа.

Что можно? Что нельзя? К чему надо относиться осторожно? Студентам предлагается посмотреть ресурсы

http://content-filtering.ru/aboutus,

http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.html,http://www.youtube.com/watch?v=y37Ax5TPc3s&feature=related.

Преподаватель спрашивает, что об этом можно прочитать на web-страницах и просит студентов сформулировать правила безопасной работы.

Резюме (обсуждение найденной информации). Какие правила безопасной работы выбрали студенты, посещая web-сайты?

4. Закрепление изученного материала.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет-общение будет приносить пользу.

Рефлексия. На данном этапе предлагается подвести итоги урока Интернет–безопасности: на столе лежат три смайлика, студентам необходимо выбрать и положите перед собой тот, который соответствует настроению.

	Урок понравился. Узнал что-то новое
	Урок понравился. Ничего нового не узнал.
	Урок не понравился. Зря время потерял.

И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Анкетирование студентов/ Тестирование студентов

Анкетирование/тестирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде. Примерная форма анкеты представлена в Приложении 1, тесты «Безопасность в сети Интернет» представлены на ресурсе: www.ege.yandex.ru

Оценивание студентов.

Информация о домашнем задании, инструкция о его выполнении: домашнее задание студентам предлагается выполнить в форме рефератов – исследовательских проектов по предложенной тематике (Приложение 2).

ПРИЛОЖЕНИЯ

Приложение 1

Примерные материалы итогового анкетирования студентов по теме "Безопасный Интернет"

1. Укажите свой возраст_____

2. Какие опасности существуют в Интернете?

_____

3. Использование Интернета является безопасным, если:

(выберите один или несколько вариантов из списка ответов)

1) защитить свой компьютер, защитить себя в Интернете, соблюдать правила;
2) разглашать личную информацию, заботиться об остальных, регулярно обновлять операционную систему;
3) защитить компьютер, создавать резервные копии документов, закону надо подчиняться даже в Интернете;

4.Как защитить себя в Интернете?

(выберите один или несколько вариантов из списка ответов)

1) расширять круг знакомств с неизвестными людьми;
2) стараться давать как можно меньше информации о себе;
3) размещать фотографии свои, друзей и родственников.

5.Как обезопасить свой компьютер?

(выберите один вариант из списка ответов)

1) не производить никаких действий;
2) установить антивирусную программу;

6.Что надо делать, чтобы антивирусная программа была эффективной.

(выберите один или несколько вариантов из списка ответов)

1) лучше не иметь антивирусную программу;
2) обновлять антивирусную базу;
3) не посещать сайты, где нет достоверности, что сайт находится под защитой

7.Кто создаѐт опасные программы?

(выберите один или несколько вариантов из списка ответов)

1) вирусы 2) хакеры 3) шпионы 4) геймеры

8.Перечислите правила поведения в Интернете

(если вы не знаете ответа на этот вопрос, то напишите "Без ответа")

_____

Приложение 2

Темы рефератов и требования к оформлению

Темы:

1. «Интернет среди нас»;
2. «Я и мои виртуальные друзья»;
3. «Интернет в моей семье»;
4. «Мой Интернет»;
5. «Интернет и природа»;
6. «Мой социум в Интернете»;
7. «Интернет и моя будущая профессия»;
8. «Интернет в современной школе»;
9. «Интернет и мое здоровье» ;
10. «Этические нормы поведения в информационной сети».

Требования к оформлению:

Объем реферата 10 – 15 страниц текста, оформленного в соответствии с требованиями:

- ✓ Титульный лист;
- ✓ Содержание, с указанием страниц;
- ✓ Нумерация страниц;
- ✓ Шрифт Times new roman, 14;
- ✓ Междустрочный интервал – 1,5;
- ✓ Отступ первой строки 1,25;
- ✓ Выравнивание по ширине;
- ✓ Заголовки строчными буквами;
- ✓ Список литературы по алфавиту (указать ссылки на Интернет-ресурсы):
  Образец оформления ссылки на интернет–ресурс:
  Официальный сайт графического редактора GIMP, форма доступа: http://gimp.ru/ (дата обращения: 10.10.2014)

После написания реферата проверить его уникальность на сайте: http://text.ru/

Приложение 3

Толковый словарь терминов «Интернет в образовании»

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.

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 студентам, 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, физиологогигиенических, 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, программноаппаратных 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 какойлибо 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 информационныхресурсовобразовательного 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.

Приложение 4

Информационные Интернет-ресурсы образовательного назначения

Коллекции цифровых образовательных ресурсов

- Единая коллекция цифровых образовательных ресурсов http://schoolcollection.edu.ru
- Единое окно доступа к образовательным ресурсам http://window.edu.ru
- Каталог электронных образовательных ресурсов http://fcior.edu.ru

Системы тестирования

- Единый портал Интернет-тестирования в сфере образования http://www.iexam.ru
- Онлайн–сервис для проведения тестирований Let's test http://letstest.ru
- Онлайн-тестирование по информационным технологиям (проект учебного центра «Сетевая академия»)http://tests.academy.ru Сервер тестированияhttp://www.rostest.runnet.ru
- Система StartExam (прежнее название – OpenTest) http://www.opentest.ru
- Система оценки знаний «Инфотест» http://infotest.by
- Система тестирования INDIGO http://indigotech.ru
- Тесты по информатике и информационным технологиям (Центр образования «Юниор») – http://www.junior.ru/wwwexam
- Федеральный центр тестирования – http://www.rustest.ru
- Яндекс. Единый государственный экзамен –http://ege.yandex.ru

Ресурсы образовательного назначения

- ВСЕВЕД: все об образовании http://www.ed.vseved.ru/
- Методические материалы и программное обеспечение для школьников и учителей: сайт К.Ю. Полякова, http://kpolyakov.narod.ru
- Обучающие сетевые олимпиады http://oso.rcsz.ru
- Игра «Изучи интернет-управляй им», позволяет изучить устройство Интернета через игровую форму http://игра-интернет.рф/

Приложение 5

ПАМЯТКА

Как уберечь компьютер от заражения вирусом

- Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.
- Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключайте к своему компьютеру непроверенные съемные носители.
- Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные

- Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).
- Никому не сообщайте свой пароль.
- Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.
- Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).
- Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

Как не попасться на удочку смс-мошенников

- Не отправляйте смс на незнакомые телефонные номера, за оправку таких смс могут взимать плату.
- Переводите деньги только на известные телефонные номера.
- Не вводите телефонный номер на незнакомых сайтах.

Как избежать мошенничества при платежах

- Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.
- Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.
- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.
- Заведите отдельную карту для покупок в интернете.
- Используйте для покупок в интернете только личный компьютер.
- Регулярно обновляйте антивирусную защиту компьютера.
- Старайтесь делать покупки в известных и проверенных интернет-магазинах.
- Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.
- Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Список литературы и информационных источников

1. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет. http://vladbez.spaces.live.com
2. Концепция информационной безопасности детей [электронный ресурс]. URL: http://rkn.gov.ru/mass-communications/p700/p701. (Дата обращения: 29.09.2014).
3. Методические рекомендации ФГНУ «Институт информатизации образования» Российской академии образованияhttp://depobr.gov35.ru/index.php/documents/viewdownload/1/5614
4. Мухаметзянов И.Ш. Образование и здоровье. Здоровьесберегающая информационно-коммуникационная образовательная среда: монография / И.Ш. Мухаметзянов. – Германия, Саарбрюккен: LAP LAMBERT Academic Publishing, 2011. – 140 с.
5. Мухаметзянов И.Ш. Предотвращение возможных негативных психолого-педагогических последствий использования информационных и коммуникационных технологий в образовательном процессе // Казанский педагогический журнал. – 2012. - № 1. – 16 с.
6. Роберт И.В. Теория и методика информатизации образования (психолого-педагогический и технологический аспекты). – М.: БИНОМ. Лаборатория знаний, 2014. – 398 с.: ил. – (Информатизация образования).
7. Сайт «Безопасность детей» Онлайн Энциклопедия http://bezopasnost-detej.ru/
8. Толковый словарь терминов понятийного аппарата информатизации образования / составители *И.В. Роберт, Т.А. Лавина*. – М.: БИНОМ. Лаборатория знаний, 2012. - 69 с.