**Областное бюджетное профессиональное образовательное учреждение**

**«Курский электромеханический техникум»**

**(ОБПОУ «КЭМТ»)**

**Информационная безопасность в сети Интернет**

**Методическая разработка открытого урока**

по учебному предмету ОВПб.01 Информатика

для специальности 13.02.11 Техническая эксплуатация и обслуживание

электрического и электромеханического оборудования (по отраслям)

Разработчик: *Калуга Юлия Вячеславовна*,

*преподаватель ОБПОУ «КЭМТ»*

2016 г.

|  |  |  |
| --- | --- | --- |
| РАССМОТРЕНА  на заседании предметной (цикловой) комиссии преподавателей физико-математических  дисциплин  Протокол №\_\_\_ от\_\_\_\_\_\_20\_\_\_\_г.  Председатель ПЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В.Николаенко  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г. |  | Заведующая отделением  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.А.Гнедышева  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г. |
| Данная методическая разработка рекомендована для практического применения (проведения открытого урока) в рамках календаря образовательных событий | | |
|  | |  |

**Информационная безопасность в сети Интернет**

**Методическая разработка открытого урока**

по учебному предмету ОВПб.01 Информатика

для специальности 13.02.11 Техническая эксплуатация и обслуживание

электрического и электромеханического оборудования (по отраслям)

в рамках календаря образовательных событий

Разработчик \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Калуга Юлия Вячеславовна,

преподаватель высшей квалификационной категории

ОБПОУ «КЭМТ»

Рецензенты:

1. Махова Лилия Анатольевна, преподаватель высшей категории ОБПОУ «Курский монтажный техникум»

2. Гренадер Н.Н., преподаватель ОБПОУ «Курский электромеханический техникум»

**деятельностная карта учебного занятия**

**план урока**

**Специальность:** 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)

**Учебная группа:** ЭМ-11

**Учебный предмет:** ОВПб.01 Информатика

**Тема учебного занятия:** Информационная безопасность в сети Интернет

**Тип урока:** урок «открытия» нового знания

**Вид урока:** проблемная лекция

**Место проведения:** учебный кабинет «Информатика»

**Средства обучения:**

* *технические:*
* мультимедийный проектор и интерактивная доска, персональный компьютер;
* *информационно-коммуникационные:*
* компьютерная мультимедийная презентация к уроку;
* видеофрагмент «Десять правил безопасности в сети Интернет» [Электронный ресурс] URL:http://единыйурок.рф.
* *дидактический материал:*
* шаблоны опорного конспекта – 25 шт.
* шаблон схемы «фишбоун» – 1 шт.
* памятки – 25 шт.
* листы А4 двух цветов для заполнения схемы «фишбоун».

**Цели урока:**

**деятельностная:** создание условий для усвоения и закрепления правил поведения в сети Интернет, развитие умений проводить наблюдения, планировать и выдвигать гипотезы, применять полученные знания для безопасной работы сети Интернет;

**содержательная:** углубление понимания значения категорий «Интернет», «угрозы сети Интернет», усвоение приемов безопасности при работе в сети Интернет;

**воспитательная:** воспитание устойчивого интереса к изучению информатики, культуры общения;

**методическая цель:** применение элементов технологии проблемного обучения и элементов технологии критического мышления при изучении правил информационной безопасности в сети Интернет.

**Задачи урока:**

*учебно-практические:*

* совершенствовать умения и навыки самостоятельной деятельности, работы в группах;
* совершенствовать умения ясно, логично и точно излагать свою точку зрения;
* развивать критическое мышление через проблемные ситуации, создание схемы «фишбоун»;
* совершенствовать речевые умения — комментировать, анализировать проблемные ситуации.

*учебно-познавательные:*

* расширить знания студентов об угрозах в сети Интернет и способах их распространения;
* формировать навыки поведения в информационном обществе с целью обеспечения информационной безопасности в сети Интернет;
* создавать условия для развития положительной мотивации к учению, стимулировать развитие творческих возможностей обучающихся;
* развивать способность к самостоятельной информационно-познавательной деятельности;
* создавать условия для применения полученных знаний;

*воспитательные:*

* содействовать воспитанию положительного отношения к знаниям и процессу обучения, уверенности в своих силах, аккуратности при выполнении записей;
* способствовать осознанию практической ценности правил безопасности в сети Интернет.

**Образовательные технологии:**

* технология проблемного обучения;
* здоровьесберегающие технологии;
* информационно-коммуникационные технологии.

**Организационные формы образовательной деятельности:** фронтальная, групповая.

**Методы обучения:**

* *словесные*: проблемная лекция; проблемное изложение, диалогический метод;
* *наглядные*: компьютерная мультимедийная презентация;
* *практические*: проблемный, частично-поисковый.

**Планируемые результаты:**

**а) предметные:**

* усвоение навыков поведения в информационном обществе с целью обеспечения информационной безопасности;

**б) метапредметные:**

* **регулятивные:**
* умение ставить перед собой цель, видеть ожидаемый результат работы;
* умение планировать свою деятельность;
* умение рационально распределять рабочее время;
* **познавательные:**
* формулирование познавательной цели;
* поиск и отбор необходимой информации;
* структурирование полученной информации;
* самостоятельное и групповое изучение материала, анализ, обобщение;
* **коммуникативные:**
* умение слышать, слушать и понимать собеседника;
* умение планировать и согласованно выполнять совместную деятельность;
* умение выражать свои мысли с достаточной полнотой и точностью;
* умение взаимно контролировать действия друг друга, оказывать поддержку друг другу.

**в) личностные:**

* формирование ответственного отношения к учению, готовности и способности обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;
* осознание социальной, практической и личностной значимости учебного материала.

***Нормативный документ***

Федеральный государственный образовательного стандарт среднего общего образования (утв. приказом Министерства образования и науки Российской Федерации (Минобрнауки России) от 17 мая 2012 г. №413.). – М.: Министерство образования и науки РФ. – 2012.

**СПИСОК ЛИТЕРАТУРЫ**

*Основная литература*

1. Гафнер В.В. Информационная безопасность: учеб. пособие. – Ростов н/Дону: Феникс, 2010. - 324 с.

2. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студентов высших учебных заведений.- М.: Издательский центр «Академия», 2008. – 336 с.

3. Рогозин В.В. Основы информационной безопасности: учеб. пособие. – М.: Юнита-Дана, 2016. – 287 с.

*Интернет-источники, электронные образовательные ресурсы*

1. Вопросы обеспечения информационной безопасности от компании Microsoft - [Электронный ресурс] URL: http://www.microsoft.com/rus/protect/default.mspx#.

2. Вопросы безопасности - сайт от компании Semantec [Электронный ресурс] URL: http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs\_teach\_kids

3. Интернет СМИ «Ваш личный Интернет» [Электронный ресурс] URL: http://content-filtering.ru

4. Квест Сетевичок. Единый урок по безопасности в сети [Электронный ресурс] URL: [http://kvestsetevichok.ru](http://kvestsetevichok.ru/).

[5. Методические рекомендации к Единому уроку безопасности в сети Интернет](file:///E:\Урок%20безопасности\6.%20Методические%20рекомендации%20к%20Единому%20уроку%20безопасности%20в%20сети%20Интернет) [Электронный ресурс] URL: <http://единыйурок.рф>.

6. [Методические рекомендации по организации и проведению в общеобразовательных организациях Российской Федерации тематического урока, посвященного Интернет безопасности детей](http://goo.gl/5tNYbg) [Электронный ресурс] URL: <http://единыйурок.рф>.

7. Специальный портал, созданный по вопросам безопасного использования сети Интернет. Безопасный Интернет [Электронный ресурс] <http://www.saferinternet.ru/>.

Портал Сети творческих учителей [Электронный ресурс] URL: http://www.it-n.ru/communities.aspx?cat\_no=71586&tmpl=com.

*Дополнительная литература*

Солдатова Г.В., Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования Ч1: лекции, Ч2: практикум. М., 2013 – 302 с.

*Видеоресурсы*

Десять правил безопасности в сети Интернет [Электронный ресурс] URL: <http://единыйурок.рф>.

*Научно-методические ресурсы*

1. Инновационные педагогические технологии: Учеб. пособ. / В.Н. Михилькевич, В.М. Нестеренко, П.Г. Кравцов; Самар. гос. ун-т. - Самара, 2001. – 89 с.
2. Коменский Я.А. Избранные педагогические сочинения: В 2-х т. Т. 2. – М.: Педагогика, 1982. – 576 с.
3. Кукушин B.C. Теория и методика обучения / B.C. Кукушин. – Ростов н/Д.: Феникс, 2005. – 474 с.
4. Кульневич С.В., Лакоценина Т.П. Современный урок. Часть III: Проблемные уроки. Научно-практич. пособие для учителей, методистов, руководителей учебных заведений, студентов и аспирантов пед. учеб. заведений, слушателей ИПК. – Ростов н/Д: Учитель, 2006. – 288 с.
5. Махмутов М.И. Проблемное обучение: Основныевопросы теории. – М.: Педагогика, 1975. – 368 с.
6. Михилькевич В.Н., Полушкина Л.И., Мегедь В.М. Справочник по педагогическим инновациям. – Самара, 1998. – 172 с. – С. 166-188
7. Оконь В.В. Основы проблемного обучения. – М, 1988. – 184 с.

**ПРИЛОЖЕНИЯ**

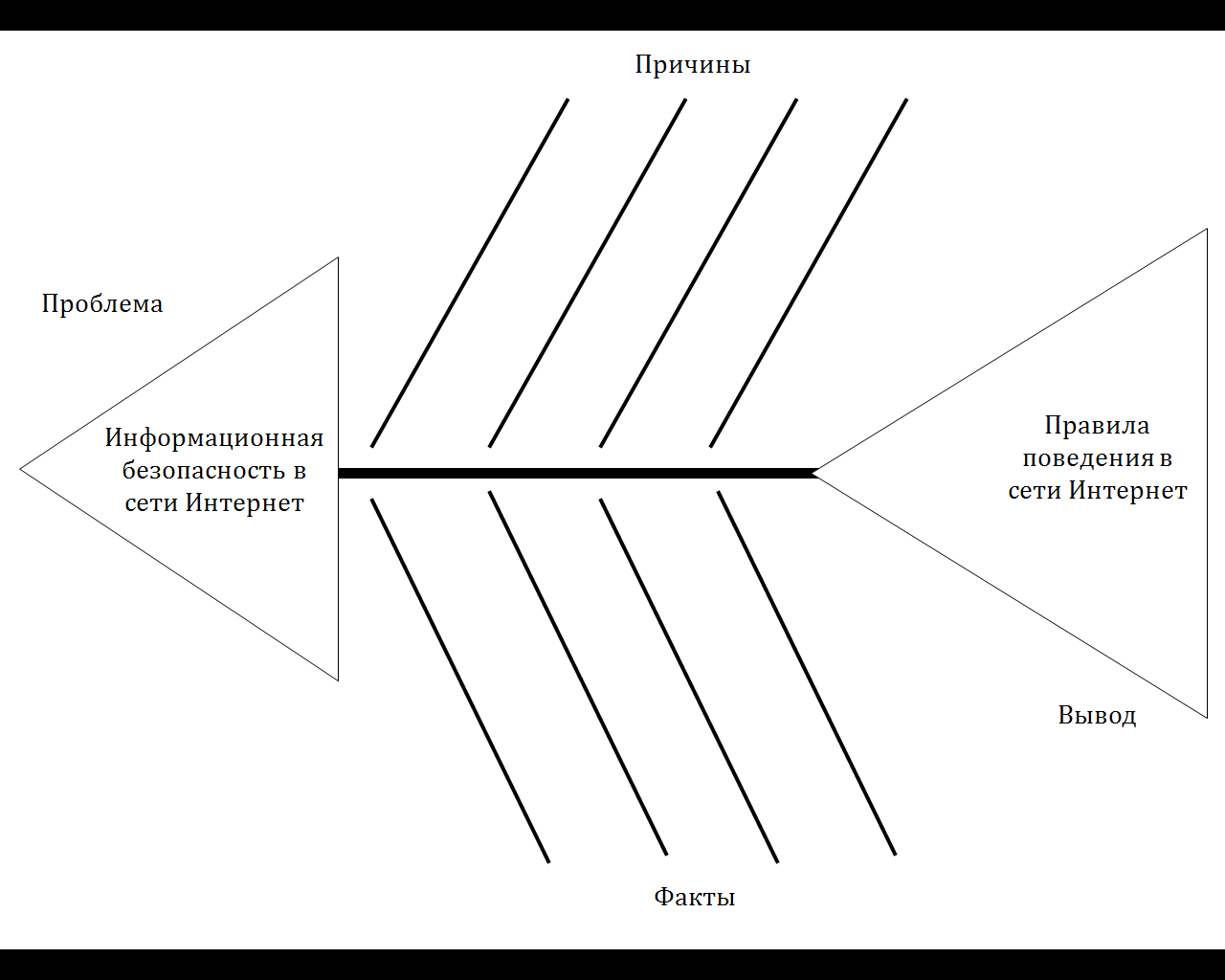
Приложение 1

Схема «фишбоун»

Приложение 2

Карточки с заданиями

Ситуация 1. Вы получаете сообщение «Примите участие в конкурсе и выиграй планшет». Для этого Вас просят перейти по указанной ссылке и ввести личную информацию: фамилию, имя, номер телефона, адрес электронной почты, пароль, номер банковского карты. Ваши действия?

Ситуация 2. Вы просматриваете сайты. Вдруг на экране появляется сообщение о том, что Ваш компьютер заражен 123 троянскими программами, вирусами, червями. На Вашем компьютере установлена защитная программа, и она никак не отреагировала на угрозы. Вам сообщают, что Вы можете загрузить новое бесплатное антивирусное ПО, которое поможет решить Вашу проблему. Что делать в такой ситуации?

Ситуация 3. Ваш близкий друг просит Вас о помощи в социальной сети. Вы спрашиваете, как ему позвонить, но, естественно, его телефон украли. И он просит чтобы «положили деньги» на другой номер. Ваши действия?

Приложение 3

**Памятка**

**Правила поведения в сети Интернет**

***Правило № 1.  Защитите ваш компьютер с помощью антивирусных программ и программ безопасной работы в интернете.***

* Установите Антивирус.
* Регулярно [обновляйте сигнатуры угроз](mk:@MSITStore:C:\Program%20Files\Kaspersky%20Lab\Kaspersky%20Anti-Virus%206.0\Doc\context.chm::/Help42.html#wp5000980), входящие в состав программы.
* Задайте рекомендуемые экспертами параметры защиты вашего компьютера. Постоянная защита начинает действовать сразу после включения компьютера и затрудняет вирусам проникновение на компьютер.
* задайте рекомендуемые экспертами параметры для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю. Если вы не установили компонент Фаервол, рекомендуется сделать это, чтобы защитить компьютер при работе в интернете.

***Правило № 2. Будьте осторожны при записи новых данных на компьютер:***

* [проверяйте на присутствие вирусов все съемные диски](mk:@MSITStore:C:\Program%20Files\Kaspersky%20Lab\Kaspersky%20Anti-Virus%206.0\Doc\context.chm::/Help40.html#wp5000954) (дискеты, CD-диски, флеш-карты и пр.) перед их использованием.
* осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми.
* внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
* если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью Антивируса.
* внимательно относитесь к выбору посещаемых вами Интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или Интернет-червями.

***Правило № 3. С недоверием относитесь к вирусным мистификациям - программам-шуткам,*** письмам об угрозах заражения.

***Правило № 4  Регулярно устанавливайте обновления операционной системы Microsoft Windows.***

***Правило №5 Покупайте дистрибутивные копии программного обеспечения у официальных продавцов.***

***Правило 6. Будьте осторожны с электронной почтой***

* не стоит передавать какую-либо важную информацию через электронную почту.
* Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

***Правило 7 . Используйте сложные пароли.***

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

***Правило 8. Не отправляйте SMS-сообщения.***

* сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.
* при отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.
* поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

***Правило 9. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.***

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

***Правило 10. Используйте брандмауэр.***

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

***Правило 11. Делайте резервные копии.***

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.