Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

М.В. Романова
Е.В. Чернова

МЕТОДИКА ОРГАНИЗАЦИИ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ПО ИНФОРМАТИКЕ И ИКТ

*Утверждено Редакционно-издательским советом университета
в качестве учебного пособия*

Магнитогорск
2017

УДК 37:004

Рецензенты:
Заведующий кафедры экономики
ОУ ВО «Южно-Уральский институт управления и экономики»,
кандидат экономических наук, доцент
Л.В. Алферова

Директор МОУ «СОШ№ 33 с углубленным изучением
английского языка со 2-го класса» г.Магнитогорска,
кандидат педагогических наук
И.В. Шманева

Романова М.В.
Методика организации внеурочной деятельности по информатике и ИКТ [Электронный ресурс] : учебное пособие / Марина Викторовна Романова, Елена Владимировна Чернова ; ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». – Изд. 2-е, подгот. по печ. изд. 2017 г. –Электрон. текстовые дан. (2,49 Мб). – Магнитогорск : ФГБОУ ВО «МГТУ им. Г.И. Носова», 2017. – 1 электрон. опт. диск (CD-R). – Систем. требования : IBM PC, любой, более l GHz ; 512 Мб RAM ; 10 Мб HDD ; MS Windows XP и выше ; Adobe Reader 8.0 и выше ; CD/DVD-ROM дисковод ; мышь. – Загл. с титул. экрана.
ISBN 978-5-9967-1051-5

Учебное пособие представляет собой сборник проектов, разработанных студентами и магистрантами в процессе обучения и реализованных на практике с достаточно высоким уровнем результатов. Проекты содержат подробное описание этапов реализации, вероятные результаты проектной деятельности школьников и раскрывают современные аспекты проблем информационного сообщества.

Учебное пособие соответствует требованиям ФГОС к квалификационной характеристике выпускника направления 44.03.05 «Педагогическое образование», учитывает содержание компетенций и современные требования к результатам образовательной деятельности.

УДК 37:004 (075)

ISBN 978-5-9967-1051-5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Современный этап высшего профессионального образования характеризуется потребностью включения в образовательный процесс методик использования информационно-коммуникативных технологий, дистанционного обучения, формирования открытой образовательной среды для подготовки конкурентоспособного компетентного специалиста. Вопросы включения инновационных технологий в процесс обучения рассматриваются в работах Е. Полат, В.А. Сластенина, Г.К. Селевко, М.Е. Бершадского, В.В. Гузеева, А.В. Хуторского, И.П. Подласого, В.Д. Симоненко, В.В. Шапкина, В.И. Андреева и др. В современных образовательных стандартах высшего профессионального образования акцентируется необходимость выпустить не просто специалиста, а готового включаться в использование новых технологий в рамках своей профессии, быть адаптированным к меняющимся условиям рабочей среды, а так же способного к принятию решений и консалтинговой деятельности. Ученые-педагоги высшей школы отмечают ряд направлений, перспективных в развитии методики обучения в высшей школе. Особенно подчеркивается необходимость включения в учебную деятельность элементов проблемного обучения, научного поиска, различных форм самостоятельной исследовательской деятельности студента.

Таким образом, остро необходимо наряду с традиционными, хорошо зарекомендовавшими себя образовательными технологиями, включать в образовательный процесс современные, инновационные технологии образования.

Применение проектной деятельности на базе информационно-коммуникационных технологий дает дополнительные преимущества: использование многообразия информации, размещенной на открытых и бесплатных сетевых ресурсах, изучение информационных умений и навыков, включение их в свою деятельность, наблюдение за деятельностью участников сетевых сообществ. Преимущества проектной технологии заключается в совокупности творческих – исследовательских, поисковых, проблемных – методов, и направленности на результат решения той или иной проблемы.

Внеурочная деятельность – это деятельностная организация на основе вариативной составляющей базисного учебного (образовательного) плана, организуемая участниками образовательного процесса, отличная от урочной системы обучения: экскурсии, кружки, секции, «круглые столы», конференции, диспуты, КВНы, школьные научные общества, олимпиады, соревнования, поисковые и научные исследования и т. д.; занятия по направлениям внеучебной деятельности учащихся, позволяющие в

полной мере реализовать требования Федеральных государственных образовательных стандартов общего образования.

Основными целями внеурочной деятельности являются создание условий для достижения учащимися необходимого для жизни в обществе социального опыта и формирования принимаемой обществом системы ценностей; создание условий для многогранного развития и социализации каждого учащегося в свободное от учёбы время; создание воспитывающей среды, обеспечивающей активизацию социальных, интеллектуальных интересов учащихся в свободное время; развитие здоровой, творчески растущей личности с сформированной гражданской ответственностью и правовым самосознанием, подготовленной к жизнедеятельности в новых условиях, способной на социально значимую практическую деятельность, реализацию добровольческих инициатив.

Учебное пособие «Методика организации внеурочной деятельности по информатике и ИКТ» содержит в себе готовые проекты внеурочных мероприятий для школьников и студентов. Проекты содержат подробное описание этапов реализации, вероятные результаты проектной деятельности школьников и раскрывают современные аспекты проблем информационного сообщества.

1. ОБРАЗОВАТЕЛЬНЫЕ И ИССЛЕДОВАТЕЛЬСКИЕ ПРОЕКТЫ

Неосязаемые деньги

Автор Агафонов А. Д., руководитель: Чернова Е.В.

Описание проекта: Проект предназначен для ознакомления с электронными платежными системами, выбора удобной системы для себя, избегание угроз хищения денежных средств, а также для понимания, когда нужно использовать кошелёк, а когда нет. В ходе проекта проводится семинар, показывающий разницу между платежными системами. В заключение проекта предлагается тест, который подготовит учеников к опасностям и трудностям использования электронно-платежных систем.

Цель проекта – формирование начальных знаний в области электронных платежных систем.

Задачи проекта:

1. Проанализировать основные теоретические аспекты электронных платежных систем.

2. Ознакомить учащихся с видами электронных платежных систем.

3. Показать учащимся виды угроз.

План проведения проекта:

1 этап: Вводное занятие. Интеллектуальная игра. Лекция. (2 пары).

2 этап: семинар и презентация (1 пара).

3 этап: стресс-тест (1 пара).

Основополагающий вопрос

Как быть богатым без денег в кармане?

Проблемные вопросы

1. Зачем нужна электронно-платежная система?

2. Каковы негативные стороны электронно-платёжной системы?

Учебные вопросы

1. Что такое электронно-платёжная система?

2. Виды электронно-платёжной системы?

3. Покушение на кошелек – правда или вымысел?

4. Правда ли электронно-платежные системы делают нас ленивее?

Мероприятие № 1. Семинар по теме «Анализ платежных систем»

Цели: научиться различать платежные системы, найти индивидуальную систему для каждого, обезопасить себя от угроз.

Задачи:

1. Проверить умение учеников анализировать, работать в команде, логично и грамотно представлять информацию.

2. Доказать, что безопасное проведение электронных платежей является ключевым фактором успеха электронного бизнеса.

Ход работы:

Разделиться на группы по 3-4 человека, выбрать платежные системы для каждого, проанализировать систему, сравнить между собой, оформить в виде презентации.

Практические задания:

1. Провести анализ 3-4 платежных систем по следующим критериям:

- история создания;
- география применения;
- годовой оборот;
- схема работы и взаимодействия участников системы;
- требования к пользователям;
- гарантии пользователям;
- методы обеспечение безопасности.

2. Полученный статистический материал представить в форме презентации с обязательным указанием источников информации.

Список платежных систем:

1. WebMoney www.webmoney.ru
2. Яндекс. Деньги www.money.yandex.ru
3. Деньги@Mail.ru www.money.mail.ru
4. PayPal www.paypal.com
5. RUpay
6. EasyPay
7. e-Gold
8. StormPay
9. QuickPay
10. PayCash
11. Moneybookers
12. ChronoPay
13. CyberPlat: CyberPOS + CyberCheck
14. ASSIST
15. e-port
16. РАПИДА
17. Золотая Корона
18. EACCESS
19. RBS (Runet Business Systems)
20. КредитПилот
21. ЭлИТ
22. SimMP
23. DigiCash
24. CyberCash
25. CheckFree
26. NetCash

Мероприятие №2. Стресс-тест

Цель: обезопасить себя от возможных инцидентов в области электронных платежей

Задачи: показать ситуации, в которых возможна угроза. Научить учеников самостоятельно мыслить в области информационной безопасности.

Ход работы:

Перед началом теста ситуации распечатываются так, чтобы каждая была на отдельном листке, и раскладываются по столу в перевернутом виде.

Ученики по одному выходят и выбирают лист. Читают ситуацию, которая им попалась, и пытаются рассказать остальным, как избежать и обезопасить себя от такого инцидента.

После лист отдаётся преподавателю и выходит следующий участник.

После того как ситуации закончились, учитель вправе выложить их ещё раз и провести на оставшихся учениках, при условии что ответ ученика будет иным.

Ситуации

№	Проблема	Ситуация	Задание
1.	утечка конфиденциальной информации	Кто-то из близких людей рассказал ваш пароль	Как избежать и обезопасить себя от такого инцидента?
2.	неправомерный доступ к информации	Кто-то подсмотрел ваш пароль	Как избежать и обезопасить себя от такого инцидента?
3.	саботаж	Вам перевели на карту недостаточное количество денежных средств или вовсе не перевели ничего	Как избежать и обезопасить себя от такого инцидента?
4.	мошенничество с помощью ИТ	Проверяя свои денежные средства на карте вы заметили, что сумма пропала или её не хватает	Как избежать и обезопасить себя от такого инцидента?
5.	атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS)	Вы сделали запрос на получение денежных средств, но денег так и не дали, а сумма уменьшилась	Как избежать и обезопасить себя от такого инцидента?
6.	размещение конфиденциальной /провокационной информации в сети Интернет	Вам прислали сообщение, в котором говорится «Укажите ваш счёт в банке и туда перечислятся денежные средства»	Как избежать и обезопасить себя от такого инцидента?

№	Проблема	Ситуация	Задание
7.	взлом, попытка взлома	Кто-то нашёл или украл вашу карту	Как избежать и обезопасить себя от такого инцидента?
8.	анонимные письма (письма с угрозами)	Вам приходит сообщение с угрозами и требованием о перечислении денежных средств	Как избежать и обезопасить себя от такого инцидента?
9.	экономия времени	Вы решаете как вам лучше оплатить Интернет или заказ	Как понять когда следует пользоваться услугами электронного кошелька, а когда нет?

Результаты обучения

Подведением итогов можно считать результаты стресс-теста.

Дети и Интернет.
Интернет-угрозы для ребенка при работе в сети

Автор: Долженко И.С., руководитель: Лапшина В.Б.

Аннотация проекта. Учебный проект «Дети и Интернет. Интернет-угрозы для ребенка при работе в сети» включает в себя изучение следующих учебных тем: защита информации; информационная безопасность; правонарушения в информационной сфере, меры их предотвращения; введение в Интернет. Предмет: информатика и информационные технологии, 9 класс.

В ходе реализации проекта учащиеся знакомятся с понятием Интернет-угрозы, изучают существующие классификации Интернет-угроз, их влияние на детей; изучают методы проведения профилактики, защиты детей от Интернет-угроз. Самостоятельные исследования учащихся выполняемые с использованием базовых информационных технологий посвящены изучению существующих программных продуктов, предназначенные для обеспечения защиты информации; выработке правил профилактики и защиты от Интернет-угроз.

Проект рассчитан на 3 академических часа в классе (120 минут) и 6 часов (240 минут) самостоятельной работы.

Программное обеспечение:

- текстовый редактор Microsoft Word;
- программа для создания буклетов MS Publisher;
- программа для созданий презентаций MS Power Point.

Основные учебные темы проекта:

1. Защита информации, информационная безопасность.

2. Интернет и его влияние на человека.
3. Способы защиты от нежелательной информации в Интернет.
4. Интернет-зависимость.

Тип проекта:

- по предметно-содержательной области: межпредметный;
- по характеру координации: с явной координацией;
- по характеру контактов: внешний;
- по количеству участников: индивидуальный или групповой;
- по продолжительности выполнения: долгосрочный.

Тематический охват проекта: для реализации проекта учащимся необходимо изучить следующие разделы курса информатики:

1. «Аппаратные и программные средства ЭВМ»;
2. «Средства работы с текстовыми документами. Текстовый редактор Microsoft Word»;
3. «Основы компьютерных телекоммуникаций. Программа Internet Explorer»;
4. «Язык разметки гипертекста HTML. Автоматизация разработки веб-документов. Программа для создания веб-сайтов MS Publisher».
5. «Программа для создания презентаций MS Power Point»

Реализация учебного проекта преследует следующие цели:

- знакомство, профилактика и предотвращение негативного воздействия Интернет-угроз на психическое и физическое здоровье детей;
- развитие интереса к изучению информатики, навыков самостоятельной работы с учебной, научно-популярной литературой и материалами Интернет; способностей к формализации, элементов системного мышления;
- воспитание культуры информационной деятельности, в том числе умения работать в коллективе; чувства ответственности за результаты своего труда, используемые другими людьми; установки на позитивную социальную деятельность в информационном обществе, недопустимости действий, нарушающих правовые и этические нормы при работе с информацией;
- коллективная реализация информационных проектов, преодоления трудностей в процессе проектирования, разработки и реализации учебного проекта;
- овладение умениями представления результатов исследования с использованием современных информационных технологий (презентация, публикация, сайт).

Учащиеся должны

знать:

- существующие программные продукты, предназначенные для обеспечения защиты информации;

уметь:

- соблюдать требования информационной безопасности;
- искать и обрабатывать информацию из различных источников, приводить собственные примеры явлений и тенденций, связанных с безопасностью информационного общества;
- интерпретировать изучаемые явления и процессы, давать им сущностные характеристики, высказывать критическую точку зрения и свои собственные суждения по проблемным вопросам;
- сравнивать, анализировать и систематизировать имеющийся учебный материал;

иметь навыки:

- представлять результаты учебных исследовательских проектов с использованием ИКТ.
- самостоятельной работы с учебной, научно-популярной литературой и материалами Интернет;
- участия в групповой работе и дискуссиях, в решении задач в игровых ситуациях и проектной деятельности.

Основополагающий вопрос проекта:

«Угрожающий оскал Интернета, как от него уберечься?»

Вопросы учебной темы (проблемные):

1. Каковы угрозы для ребенка при работе в сети?
2. Как обеспечить безопасность детей при работе в Интернет?
3. Какие меры должны принимать родители для защиты детей от Интернет-угроз?

Творческое название учебного проекта:

«Чудовища в Интернете»

Самостоятельные исследования учащихся:

1. Составить классификацию наиболее распространенных в настоящее время Интернет-угроз.
2. Разработать меры защиты детей от Интернет-угроз, которые могут принимать родители.
3. Разработать правила профилактики от негативного воздействия Интернет-угроз для детей.

Оценивание деятельности учащихся

Деятельность учащихся будет оцениваться посредствам анализа итоговых творческих заданий. Предполагается проведение оценки, как самим учителем, так и другими учащимися.

Терпи, казак, толерантным будешь

Автор Пащенко К.Н., руководитель: Чернова Е.В.

Описание проекта: внеклассное мероприятие с целью профилактики защиты от террористических и экстремистских угроз в сети Интернет в условиях поликонфессионального, многонационального общества (доступ к материалам проекта http://wiki.iteach.ru/index.php/ Особенности_профилактики_кибертерроризма_и_киберэкстремизма_в_поликонфессиональном_и_многонациональном_обществе).

Цель проекта – формирование толерантного мировоззрения у учащихся и воспитание культуры толерантности, основанных на принципах уважения прав и свобод человека, стремления к межнациональному согласию, готовности к диалогу.

Задачи проекта:

1. Ввести и закрепить определение термина «толерантность», углубить понимание его значения;
2. Показать многоаспектность понятия «толерантность»;
3. Выявить пути формирования толерантного сознания;
4. Сформировать представление о толерантном поведении в условиях конфликта интересов.

Во время занятия школьники:

- попытаются дать свое определение толерантности;
- узнают об особенностях общения в виртуальном пространстве;
- разберутся что значит быть толерантным человеком;
- выяснят существуют ли границы толерантности;
- научатся быть толерантным в общении.

Ожидаемые результаты проекта:

- воспитание толерантного сознания в современном мире;
- формирование навыков независимого мышления, критического осмысления и выработки мировоззренческих суждений, основанных на моральных ценностях гражданского общества.

Методы, применяемые в проекте: тренинг, эвристическая беседа.

План проведения проекта: На реализацию проекта потребуется 4 аудиторных часа. На лекционном занятии (2 аудиторных часа), учащиеся познакомятся в презентации с явлениями терроризма и экстремизма в сети, узнают о причинах конфликтов, осознают актуальность этих явлений для России, а также получат вопросы для эвристической беседы на следующее занятие. Для проработки этих вопросов параллельно с работой в классе, планируется самостоятельная деятельность школьников по поиску, отбору, систематизации и представлению информации (2 аудиторных часа). На практическом занятии (2 аудиторных часа) ожидается проведение тренинга на воспитание толерантности, эвристическая бесе-

да, где каждый участник сможет высказать свое мнение, кроме того, в конце проекта планируется написание эссе на тему «Толерантность. Что вы вкладываете в это понятие?» и контрольного теста.

Основополагающий вопрос

Как нам быть разными и жить в мире?

Проблемные вопросы

1. Что является причиной социальных конфликтов?
2. Что можно противопоставить террору?

Учебные вопросы

1. Каковы причины межнациональных противоречий и конфликтов?
2. Почему люди разных конфессий испытывают неприязнь друг к другу?
3. Как разрешить социальные конфликты?
4. Толерантность. Что вы вкладываете в это понятие?
5. Как можно сформировать толерантность?
6. Существуют ли границы толерантности?

Практическое занятие на тему: «Терпи, казак, толерантным будешь»

Цель занятия: Формирование мировоззрения у учащихся и воспитание культуры толерантности, основанных на принципах уважения прав и свобод человека, стремления к межнациональному согласию, готовности к диалогу.

Задачи занятия:

1. ввести и закрепить определение термина «толерантность», углубить понимание его значения;
2. показать многоаспектность понятия «толерантность»;
3. выявить пути формирования толерантного сознания;
4. сформировать представление о толерантном поведении в условиях конфликта интересов.

Методы: тренинг, дискуссия, эвристическая беседа.

Ход занятия:

Сегодня мы поговорим о толерантности. Для начала давайте проделаем следующее упражнение.

Упражнение 1: *Чем мы похожи*

Участники сидят в кругу. Ведущий приглашает в круг одного из участников на основе одного реального или воображаемого сходства: Вася, выйди ко мне, потому что у нас тобой одинаковый цвет волос. Вася выходит и приглашает в круг еще кого-нибудь по другому признаку сходства. Все участники должны оказаться в кругу.

Понятие «толерантность» восходит к латинскому глаголу *tolerantia* – «нести», «держать», «терпеть». Этот термин первоначально применялся в тех случаях, когда было необходимо «нести», «держать» в руках какую-либо вещь. При этом подразумевалось, что для держания и переноса этой

вещи человек должен прилагать определенные усилия, страдать и терпеть.

В широкий научный оборот термин «толерантность» был введен в 1953 г. английским ученым П. Мевадаром для обозначения «терпимости» иммунной системы живого организма к пересаженным инородным тканям. Позднее это значение было дополнено в других науках иными толкованиями этого понятия.

В современном понимании толерантность есть способность человека, сообщества людей принимать и уважать мнение других. В международной практике сейчас широко используется определение, сформулированное в Декларации принципов толерантности, принятой Генеральной Конференции ЮНЕСКО в 1995 г.: «Толерантность – это то, что делает возможным достижение мира и ведет от культуры войны к культуре мира».

Вопросы для обсуждения:

1.Толерантность. Что вы вкладываете в это понятие?

2. Что есть толерантность – набор личностных черт, определяющих успешное или неуспешное коммуникативное поведение человека или что-то еще?

Упражнение 2: *Я с тобой не согласен*

В группах ведущий обращается к одному из участников со словами: Вася, я считаю, что в человеке главное это внешность. Человек, к которому он обратился, отвечает: Я с тобой не согласен, потому что ... Его ответ должен быть убедительным и неагрессивным, не переходящим на личности. Участники не должны устраивать диспуты. Участник формулирует свое спорное утверждение и обращается с ним к другому участнику.

Вывод: в общении, как и в споре, мы должны признавать:

- добровольность выбора,
- свободу совести,
- верить в искренность убеждений собеседника, оппонента.

Сегодня все более становится очевидным, что необходимым условием выживания народов в современном мире является только интеграция, признание суверенности и ценности каждого народа и его культуры. Это означает, что взаимодействие народов и культур должно развиваться на основе принципа толерантности, выражающегося в стремлении достичь взаимного понимания и согласованности, не прибегая к насилию, к отношениям господства и подчинения, к подавлению человеческого достоинства, а путем диалога и сотрудничества отдельных индивидов, социальных групп и этнических культур.

Должен быть разрушен психологический стереотип: принятие «другого» есть отказ от самого себя – и осознано отношение к «общечеловеческим» ценностям как к конкретному – разнонациональному – воплощению нравственных и духовных идеалов всего человечества. Нельзя

быть подлинно толерантным без любви «к отеческим гробам», будучи равнодушным к судьбам собственного народа. Но и нельзя быть настоящим патриотом, любя только собственный народ и ненавидя или презирая все остальное человечество.

Вопросы для обсуждения:

1. Как можно сформировать толерантность?

2. Толерантность – это только проявления внешних факторов, таких как уважение к ближнему, милосердие…или больше внутренняя убежденность в то, что у нас общие «корни», а, следовательно, общие прародители?

Упражнение 3: *Эмоционально-коррективное переживание интолерантного поведения*

Участникам нужно записать тревожащий эпизод проявления интолерантного поведения к ним в виде небольшого рассказа, написанного в настоящем времени от первого лица. При этом как можно более точно вспомнить все события, восстановить диалоги, описать свои чувства.

Затем историю нужно переписать так, как они бы хотели, чтобы она произошла (можно создать новые диалоги, отомстить обидчику и т.д.). Но в заключение – наметить пути консолидации сил с неприятным человеком.

В жизни человек общается с представителями различных национальностей, культур, миров, конфессий, социальных слоев, поэтому важно научиться уважать культурные ценности, как своего народа, так и представителей другой культуры, религии, научиться находить, что называется, точки соприкосновения. Кроме того, толерантность как качество личности считается необходимым для успешной адаптации к новым или неожиданно возникающим условиям. Люди, не обладающие толерантностью, проявляя категоричность, оказываются неспособными к изменениям, которых требует от нас жизнь.

Вопросы для обсуждения:

Можно ли воспитать толерантность в человеке?

Упражнение 4: *Как себя вести*

Участники делятся на группы; одна группа будет описывать основные черты, присущие толерантной личности, вторая – черты, присущие личности интолерантной.

Недавно в сети появилось новое ругательство – толераст. Так пренебрежительно называют людей, исповедующих «толерантность». На мой взгляд, это неправильно. Мы живем в многонациональном государстве, и капелька терпения должна быть в каждом. Другой вопрос, как много терпения должно быть в людях …?!

Вопросы для обсуждения:

Существуют ли границы толерантности?

Путь к толерантности – это серьезный эмоциональный, интеллектуальный труд и психическое напряжение, оно возможно только на основе изменения самого себя, своих стереотипов, своего сознания.

Данный проект наглядно показывает всю деятельность, которые проделывает студент, учащийся или педагог, разрабатывая свой проект. Это очень большая творческая, аналитическая работа, которая вместе с эффективно выстроенной внеурочной деятельности создает целый комплекс мер по формированию правильной личности информационного общества, которая способна противостоять как явлениям киберэкстремизма, так и другим угрозам в сети Интернет.

Угрозы кибертерроризма

Автор Путинихин П.С., руководитель: Чернова Е.В.

Описание проекта: Данный проект позволит участникам осознать угрозы, которые несет в себе кибертерроизм в условиях современности, также рассмотреть причины его возникновения и способы противодействия кибертерроризму (доступ к материалам проекта http://wiki.iteach.ru/index.php /Угрозы_кибертерроризма).

Цель проекта: изучить угрозы, которые несет в себе кибертерроризм. А также рассмотреть причины его возникновения и инструменты, которые используют кибертеррористы.

В соответствии с целью и предметом были определены следующие задачи:

1. Дать определение основным понятиям данной темы.
2. Изучить возможные нанесения ущерба кибертерроризмом.
3. Рассмотреть причины возникновения кибертерроризма.
4. Разработать структуру и содержание внеклассного мероприятия «Угрозы кибертеррозизма» при помощи семинарского занятия.

План проведения проекта

1. Вводное занятие. Анкетирование. (1 урок – 45 минут)
2. Лекция «Современные угрозы кибертерроризма», «Кибертерроризм в социальных сетях». (2 урока – 90 мин)
3. Практические занятие на усвоение материала. Выполнение контрольного теста на усвоение знаний. (1 урок – 45 минут)
4. Практическое занятие. Самостоятельная работа. Разработка презентации. (1 урок – 45 минут)
5. Отчетное занятие «Угрозы кибертерроризма» (семинар, учащиеся представляют результаты своей работы во время реализации проекта). (2 урока – 90 мин).

Основополагающий вопрос

Как противостоять кибертерроризму?

Проблемные вопросы

1. Какие угрозы проведения кибертеррористических атак существуют в современном мире?

2. Можно ли считать межконфессиональные и религиозные конфликты основой кибертерроризма?

3. Можно ли рассматривать социальную сеть в качестве пособника террора?

Учебные вопросы

1. Какие виды кибертеррористических атак существуют?

2. Как кибертеррористические атаки могут повлиять на жизнь людей?

3. В чем разница между понятиями «конфессиональный» и «религиозный»?

4. Имеет ли кибертерроризм религиозную принадлежность?

5. Какие инциденты на религиозной почве имели место быть?

6. Какова роль социальных сетей в содействии террору?

7. Как вести себя при встрече с кибертеррористами?

Семинар «Угрозы кибертерроризма»

Цель семинара: Осознать угрозы, исходящие от кибертерроризма и последствия проведения кибертеррористических атак. А также ответить на вопрос – «Что является основой для кибертерроризма?».

Задачи семинара:

1) раскрыть понятие «Кибертерроризм»;

2) закрепить умение работать в группе, слушать друг друга, оценивать себя и других участников;

3) представить результаты работы, проделанной во время реализации проекта, в виде презентации.

В подростковом возрасте учащиеся наиболее уязвимы к влиянию информации и не имеют полного представления об угрозах, исходящих от кибератак. Данное внеклассное мероприятие позволит учащимся осознать всю важность защиты информации и поможет избежать вовлечения в деятельность кибертеррористических групп.

Киберэкстремизм: история и современность

Автор Хоменко И.В., руководитель: Чернова Е.В.

Описание проекта: проект «Киберэкстремизм: история и современность» позволит учащимся больше узнать о данной теме, и чем больше они будут знать о способах защиты, тем более вероятно то, что в будущем они смогут использовать свои знания для защиты и борьбы с данным явлением (доступ к материалам проекта http://wiki.iteach.ru/index.php/Киберэкстремизм:_история_и_современность).

Цель проекта – познакомить учащихся старших классов с историей распространения киберэкстремизма с целью предупреждения вовлечения в киберэкстремистские сообщества и группировки.

План проведения проекта

1. Лекция «История возникновения киберэкстремизма». Обсуждение. (1 урок – 45 минут)

2. Лекция «Виртуальные экстремистские сообщества». Обсуждение. (1 урок – 45 мин)

3. Семинар «Киберэкстремизм: история и современность». (1 урок – 45 минут)

Основополагающий вопрос

Какова история появления и развития киберэкстремизма на данном этапе развития общества?

Проблемные вопросы

1. Как и когда зародилось такое явление, как киберэкстремизм?

2. Какими путями развивается киберэкстремизм в современное время?

3. Какие альтернативы киберэкстремизму зарождаются в современном мире?

Учебные вопросы

1. Что такое киберэкстремизм?

2. Когда зародился киберэкстремизм?

3. Кто является источником данной угрозы в современных условиях?

4. Как освещается в СМИ история появления киберэкстремизма?

Вопросы, предлагаемые ученикам для обсуждения и рассуждений:

1. Что мы пониманием под определениями: экстремизм, киберэкстремизм, киберпространство.

2. Почему информация в руках экстремистов превращается в опасное оружие преступления?

3. Почему преступления, совершаемые киберэкстремистами, стали источниками непосредственной угрозы национальной безопасности всему миру.

4. Что такое Интернет-сообщество?

5. Кем был введён термин «виртуальное сообщество»?

6. Почему люди объединяются в интернете?

7. Как классифицируются виртуальные экстремистские сетевые сообщества?

8. Какие качества характерны для виртуальных экстремистских сетевых сообществ?

Семинар по теме «Киберэкстремизм: история и современность»

Задачи проведения семинара (для учителя):

1. Углубить и закрепить знания обучаемых, полученные ими на лекции и в процессе самостоятельной работы.

2. Проверить качество знаний.

3. Помочь разобраться в наиболее сложных вопросах.

4. Выработать умение правильно применять теоретические положения к практике будущей профессиональной деятельности.

Задачи семинара (для учащихся):

1) углубленное изучение, прежде всего, теоретического материала;

2) формирование навыка переработки научных текстов, обобщения материала, развитие критичности мышления и др.;

3) развитие самостоятельности при освоении знаний, творческой инициативы и творческих способностей;

4) формирование навыка публичных выступлений, способности к рассуждениям перед аудиторией и защите своей точки зрения.

Цель семинара – развитие критического мышления и способность оценивать опасность вовлечения в киберэкстремистскую деятельность с помощью Интернет-ресурсов.

Ход семинара:

Обучаемые готовятся по вопросам семинарского занятия. Но каждый из них особенно тщательно изучает один из вопросов, можно распределить по 2 человека на один вопрос.

1. Как и когда зародилось такое явление, как киберэкстремизм?

2. Кто создал первый сайт экстремистского толка в 1995 году?

3. Стоит ли воспринимать экстремистские сайты как реальную угрозу обществу? Обоснуйте свою точку зрения.

4. Почему виртуальная среда дает личности гораздо большую свободу действий, чем реальная?

На занятии обучаемые рассаживаются за столами по - парно, в соответствии с изученными вопросами. По знаку преподавателя обучаемые в указанное время должны пересказать друг другу содержание, обсудить спорные моменты, прийти к общему мнению.

Затем один из рядов смещается на одно место. 1-й обучаемый объясняет 4-му содержание первого вопроса, уточненное и расширенное в беседе со 2-м обучаемым. 4-й объясняет 1-му содержание 2-го вопроса и т.д. За полный круг все слушатели могут обменяться мнениями по всем вопросам. Преподаватель дает короткие консультации тем, кто обращается к нему.

Достоинство этого приема – в повышении вербальной активности обучаемых и в неоднократном обсуждении одной и той же проблемы. Это способствует углублению знаний, их закреплению и выяснению новых аспектов, а также выработке единого подхода.

В заключительной части на общее обсуждение вынесен вопрос: Как освещается в СМИ деятельность виртуальных экстремистских сетевых сообществ?

После проведения семинара полезно провести анализ его эффективности, чтобы в дальнейшем не допустить тех же ошибок.

Кибертерроризм: история и современность

Автор Ахманаев Е.И., руководитель: Чернова Е.В.

Описание проекта: Данный проект позволит участникам познакомиться с историей возникновения кибертерроризма, а также с правовыми аспектами и практикой противодействия кибертерроризму (доступ к материалам проекта http://wiki.iteach.ru/index.php/Кибертерроризм:история_и_современность).

Цель – познакомить учащихся с историей возникновения кибертерроризма, а также с правовыми аспектами и практикой противодействия кибертерроризму.

В соответствии с целью и предметом были определены следующие задачи:

1. Дать определение основных понятий по данной теме.
2. Изучить историю возникновения кибертерроризма.
3. Рассмотреть правовые аспекты и практику противодействия кибертерроризму.
4. Разработать структуру и содержание внеклассного мероприятия «Кибертерроризм: история и современность» с использованием семинарского занятия.

Этапы проведения проекта

Подготовительный этап

Подготовка необходимых материалов: список информационных источников, презентация учителя для выявления представлений и интересов студентов, презентация проекта, брошюра, график оценивания и критерии для оценки работ. Определить время занятий в компьютерном классе. Определить в расписании время для консультаций и индивидуальных занятий. Обсудить необходимое оборудование (проектор, экран). Определить, как ученики собирают и где хранят результаты работы.

Основной этап

Оценка готовности учащихся с помощью анкетирования. Проведение презентации для выявления представлений и интересов. Изложение материала по теме «Кибертерроризм: история и современность». Познакомить учащихся с критериями оценивания работ. Распределение тем для создания проектной работы, консультация студентов. Проведение практической работы. Консультативная помощь учащимся, обсуждение и корректировка работ учащихся. Разработка плана проведения исследования. Подбор материала по темам исследования из различных источников

Заключительный этап.

Представление своих проектных работ. Оценивание работ учащихся. Представить презентацию проекта.

В рамках проекта, дети подготовятся к семинарскому занятию по данной теме, а по его окончании пройдут итоговый тест. В ходе работы над проектом, учащиеся изучат теоретические основы проблемы.

Основополагающий вопрос

Откуда есть пошёл кибертерроризм?

Проблемные вопросы

1. Каковы истоки и предпосылки возникновения кибертерроризма?

2. Что представляют из себя современные кибертеррористические группировки?

3. Какие правовые аспекты и практика противодействия кибертерроризму существуют?

Учебные вопросы

1. Что такое кибертерроризм?

2. Как возник кибертерроризм?

3. Что послужило толчком к началу кибертерроризма?

4. Что такое кибертеррористические группировки?

5. Какие кибертеррористические группировки существуют?

6. Чем занимаются кибертеррористические группировки?

7. Какова правовая сторона борьбы борьбы с кибертерроризмом?

8. Какие методы борьбы с кибертерроризмом существуют?

Вопросы к семинару:

1.На что направлены кибертеррористические действия

2.Кибертеррористические группировки (цели и деятельность)

3.Контрмеры государств против кибертерроризма (правовые аспекты и практика противодействия)

Терроризм с клавиатурой

Автор Белова Е.С., руководитель: Чернова Е.В.

Описание проекта: Данный проект позволит участникам разобраться, что такое экстремистская информация, пропаганда и компьютерный террор, что в общем можно назвать кибертерроризмом в сети Интернет. Участники узнают, какие меры борьбы с кибертерроризмом существуют и как можно себя обезопасить. Проблема данного исследования носит актуальный характер в современных условиях, так как пользователи Интернет, очень часто не понимают и не видят угрозу (доступ к материалам проекта http://wiki.iteach.ru/index.php/Терроризм_с_клавиатурой).

Цель проекта – обучить основам защиты от нападок и уловок киберпреступников в сети Интернет.

План проведения проекта: Участники разбиваются на 2 группы. Каждая группа готовит презентацию по одному из проблемных вопросов. В процессе обучения, участники проекта выполняют задания в блоге (http://terrorizmsklaviaturoi.blogspot.com/). В итоге, лучшая презентация и выполненные задания в блоге награждаются.

Основополагающий вопрос

Как обойти ловушки виртуального террора?

Проблемные вопросы

1.Как остановить распространение экстремисткой информации в сети?

2.Как избежать компьютерного террора?

Учебные вопросы

1.Что такое экстремистская информация?

2.Как распространяется экстремистская информация?

3.Какие бывают способы защиты от экстремизма?

4.Что такое кибертерроризм?

5.Какие методы противодействия кибертерроризму в Российской Федерации?

Результаты проекта:

Перед началом проекта учителем составляется список информационных источников, готовится вводная презентация проекта, шаблон вики-страницы, составляется расписание консультаций. На основном этапе учитель проводит консультации с учащимися, обеспечивает текущий формирующий контроль работы учащихся, обеспечивает учащихся доступ к ресурсам Интернет, поддерживает контакт с родителями, руководством и учителями. Перед защитой проект учащимися проводится самооценивание, генеральная репетиция выступления. Учитель подготавливает сертификаты для вручения участникам проекта. На защите проекта обеспечивается фото и видеосъемка для помещения материалов в Интернет и школьный архив и для школьной газеты. После защиты проекта проводится заключительное занятие, на котором происходит обсуждение выполненной работы, полученных результатов.

Межличностные, межконфессиональные противоречия – почва для террористической и экстремистской деятельности

Автор Евтюхина М.С., руководитель: Чернова Е.В.

Описание проекта: По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. По данным Национального антитеррористического комитета РФ, в настоящее время в мире действует около 5 тысяч Интернет-сайтов, активно используемых

террористами. Число порталов, обслуживающих террористов и их сторонников, постоянно растет. Всемирная сеть привлекает возможностью свободного доступа, невысокой стоимостью связи, отсутствием цензуры и других форм государственного контроля, анонимностью, быстрой передачей информации, огромной аудиторией, техническими возможностями. В ходе проекта участники изучают материалы по теме, знакомятся с новыми понятиями, самостоятельно находят интересные факты по теме, а также принимают участие в дискуссионном мероприятии (доступ к материалам проекта http://wiki.iteach.ru/index.php/Межличностные,_межконфессиональные_противоречия_-_почва_для_террористической_и_экстремистской_деятельности).

Цель проекта – профилактика защиты от террористических и экстремистских угроз в сети Интернет.

План проведения проекта: Данный проект реализуется в факультативной форме в рамках школьной программы и рассчитан на 6 уроков (45 мин):

1. Вводное занятие (учитель рассказывает о проекте, обозначает актуальность темы, дает задание) (1 урок - 45 мин).

2. Самостоятельная работа учащихся, консультации учителя (2 урока - 90 мин).

3. Дискуссионное занятие (учащиеся участвуют в дискуссии на тему, предложенную учителем) (1 урок - 45 мин).

4. Отчетное занятие (учащиеся представляют результаты своей работы во время реализации проекта) (1 урок - 45 мин).

Основополагающий вопрос

Как иметь свободу совести и не попасть в руки террористов?

Проблемные вопросы

1. Почему межэтнические и межконфессиональные конфликты являются почвой для терроризма и экстремизма?

2. Какими путями можно решить проблему межличностных и межконфессиональных противоречий?

Учебные вопросы

1. Какие существуют виды террористических и экстремистских угроз?

2. Почему террористическая и экстремистская деятельность осуществляется на основе межличностных и межконфессиональных конфликтов?

3. Какие существуют формы межличностных и межконфессиональных конфликтов?

4. Какие существуют способы по предотвращению межличностных и межконфессиональных конфликтов?

План-конспект урока по теме: «Кибертерроризм, основанный на межличностных и межконфессиональных противоречиях – реальная угроза или выдумка?»

Цель:

1) Обучить учащихся приемам дискуссии.

2) Развить критическое мышление у учащихся.

3) Воспитать способность принимать самостоятельные решения.

Тип занятия: урок-дискуссия.

Методы обучения: обсуждение с целью обобщения, систематизации, закрепления полученной учебной информации.

Ход урока:

1.Вступительное слово учителя.

Учитель: По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Всемирная сеть привлекает возможностью свободного доступа, невысокой стоимостью связи, отсутствием цензуры и других форм государственного контроля, анонимностью, быстрой передачей информации, огромной аудиторией, техническими возможностями. Так есть ли на самом деле угроза кибертерроризма или это чья-то выдумка?

2.Сообщения учащихся.

Брюс Шнайер (Bruce Schneier; род. 15 января 1963, Нью-Йорк) – американский криптограф, писатель и специалист по компьютерной безопасности. Автор нескольких книг по безопасности, криптографии и информационной безопасности. Основатель криптографической компании Counterpane Internet Security, Inc., член совета директоров Международной ассоциации криптографических исследований и член консультативного совета Информационного центра электронной приватности, также работал на Bell Labs и Министерство обороны США. Получил степень магистра в Американском университете в 1988 году. В ноябре 2011 года награждён степенью почетного доктора наук Университетом Встминстера за вклад в развитие информатки.

Евгений Валентинович Касперский (4 октября 1965, Новороссийск) – российский программист, специалист по антивирусной защите, один из основателей, ведущий разработчик и крупнейший акционер ЗАО «Лаборатория Касперского». Лауреат Государственной премии в области науки и технологий за 2008 год.

Учитель: а теперь давайте посмотрим, какие высказывания сделали эти известные люди по проблеме кибертерроризма.

Евгений Касперский: Кибертерроризм – это реальность.

Брюс Шнайнер: «Ущерб от действий киберпреступников несоизмеримо мал – по сравнению с тем, который наносят настоящие террористы. Кибертерроризм – это миф, и его значение переоценивают».

3. Дискуссия

Учитель: Чья позиция вам ближе? Аргументируйте свою точку зрения.

Учащиеся делятся на две группы, в зависимости от поддерживаемой точки зрения. После деления каждая группа аргументирует свой выбор. В процессе обсуждения учащиеся могут поменять свою точку зрения и присоединиться к оппонентам.

4. Выводы

В результате проведенной дискуссии у каждого учащего должно сформироваться свое мнение по поводу заданного вопроса.

Учитель: Итак, сегодня вы участвовали в дискуссии. У каждого из вас была возможность высказаться. Каждая группа привела доводы по своей позиции. Как вы думаете кто же все-таки был прав?

Учащиеся пытаются сами определить какая группа была права.

Учитель: Как мы видим на данный вопрос нельзя ответить однозначно, каждый из вас привел достаточные аргументы, каждый по-своему прав. Но каким бы ни было ваше мнение, вы всегда должны уважать мнение другого человека, даже если оно не совпадает с вашим.

5. Домашнее задание

Подготовить презентации, отражающие каждую из точек зрения (по группам).

Результаты обучения

В результате реализации проекта 2 группы учащихся представляют 2 презентации, в которых отражены 2 разные точки зрения ответа на дискуссионный вопрос. Лучшая презентация награждается.

Законодательные акты по противодействию киберэкстремизму

Автор Мордовина Е.В., руководитель: Чернова Е.В.

Описание проекта: в данном проекте будут рассмотрены законодательные акты по борьбе с киберэкстремизмом в России и за рубежом. Проект позволит участникам расширить свои знания в области информационной безопасности, а также использовать полученные знания для защиты от киберэкстремизма. (доступ к материалам проекта http://wiki.iteach.ru/index.php/Законодательные_акты_по_противодействию_киберэкстремизму).

Цель проекта – изучить законодательные акты противодействия киберэкстремистской деятельности.

План проведения проекта:

1. Вводное занятие (учитель рассказывает о проекте, обозначает актуальность темы, дает задание) (1 урок – 45 мин).

2. Лекция «Законодательные акты по противодействию киберэкстремизму» (1 урок – 45 мин).

3. Ролевая игра «Судебное заседание» (1 урок – 45 мин).

4. Отчетное занятие (учащиеся представляют результаты своей работы во время реализации проекта) (1 урок – 45 мин).

Ролевая игра «Судебное заседание»

Цель игры: в ходе ролевой игры изучить проблему экстремизма в сети, методы защиты информации и борьбы с киберэкстремизмом, познакомиться со статьями Уголовного Кодекса о несении уголовной ответственности за совершение компьютерного преступления.

Задачи игры:

1) развить творческое воображение;
2) закрепить знания в области киберпреступлений;
3) способствовать развитию умения в решении проблем, связанных с экстремизмом в сети.

Организация места проведения игры: Повесить перед уроком на дверь кабинета вывеску «Зал судебных заседаний». Организовать места для Судьи, Прокурора, Защиты, Подсудимого (оформить эти места при помощи табличек). На рабочие места слушателей положить планы-протоколы судебного заседания. Распределить роли между студентами.

Результаты обучения

Ученики разделились на 2 группы. В течение всего проекта ученики искали информацию по прослушанной теме. Группа 1 создавала буклеты или кроссворды, по выбору. Группа 2 готовила ролевую игру.

«Информационная война» с киберпреступлениями, киберэкстремизмом и кибертерроризмом

Автор Брылева А.С., руководитель: Чернова Е.В.

Описание проекта: в данном проекте рассказывается о таком важном явлении, затрагивающем сеть интернет, как информационные войны. Участники проекта узнают, какой ущерб наносит киберпреступление, киберэкстремизм и кибертерроризм. Во время работы ученики будут создавать буклеты, писать эссе и участвовать в «мозговом штурме». (доступ к материалам проекта http://wiki.iteach.ru/index.php/ «Информационная_война»_с_киберпреступлениями,_киберэкстремизмом_и_кибертерроризмом).

Цель проекта – изучить особенности ведения информационных войн и попытаться использовать их в борьбе с киберпреступностью.

План проведения проекта:

1. Анкетирование

2. Лекция на тему: ««Информационная война» с киберпреступлениями, киберэкстремизмом и кибертерроризмом»

3. Тест по пройденному материалу

4. Мозговой штурм на тему: «Как заставить «информационную войну» служить во благо общества?»

Основополагающий вопрос

Как заставить «информационную войну» служить во благо общества?

Проблемные вопросы

1. Где заканчивается территория «информационных войн»?
2. Как объявить войну киберпроблемам?

Учебные вопросы

1. Что такое «информационная война»?
2. Какой ущерб приносит киберпреступление?
3. Какой ущерб приносит киберэкстремизм?
4. Какой ущерб приносит кибертерроризм?
5. Как вести информационную войну с киберпреступлениями?
6. Как вести информационную войну с киберэкстремизмом?
7. Как вести информационную войну с кибертерроризмом?

Мозговой штурм на тему: «Как заставить «информационную войну» служить во благо общества?»

Метод мозгового штурма (мозговая атака, мозговой штурм, англ. brainstorming) – оперативный метод решения проблемы на основе стимулирования творческой активности.

Цель штурма: выявить как можно больше способов благотворного влияния «информационной войны» на общество. Найти нестандартные, креативные решения данной проблемы.

Задачи штурма:

- раскрыть понятие «Информационная война»;
- выявление нестандартных идей;
- помочь участникам «расковать» сознание и подсознание, стимулировать воображение, чтобы получить необычные идеи;
- закрепить умение работать в группе, слушать друг друга, оценивать себя и других участников мозгового штурма;

Правила мозгового штурма:

1. Критика исключается: на стадии генерации идей высказывание любой критики в адрес авторов идей (как своих, так и чужих) не допускается. Работающие в интерактивных группах должны быть свободны от опасений, что их будут оценивать по предлагаемым ими идеям.

2. Приветствуется свободный полет фантазии: участники должны попытаться максимально раскрепостить свое воображение. Разрешено высказывать любые, даже самые абсурдные или фантастические

идеи. Не существует идей настолько несуразных либо непрактичных, чтобы их нельзя было высказать вслух.

3. Идей должно быть много: каждого участника просят представить максимально возможное количество идей.

4. Комбинирование и совершенствование предложенных идей: на этом этапе, в отличие от второго, оценка не ограничивается, а наоборот, приветствуется. Участников просят развивать идеи, предложенные другими, например, комбинируя элементы двух или трех предложенных идей.

5. Результат: производится отбор лучшего решения общим голосованием.

Подготовка к мозговому штурму:

1. Формируется группа генераторов идей (5-10 человек).
2. Формируется группа экспертов (2 человека).
3. Зачитываются правила мозгового штурма.
4. Озвучивается проблемная тема: «Как заставить «информационную войну» служить во благо общества?».

Проведение мозгового штурма:

1 Этап. «Разогрев» генераторов:

*Упражнение 1.*Участники **говорят** первую возникшую ассоциацию к каждому слову? (информация, война, цель, безопасность, ущерб, сеть, закон, разрушение).

Упражнение 2. Описывается несколько гипотетических ситуаций, участникам предлагается перечислить всевозможные их последствия.

Информационные войны на нашей планете велись с тех пор, как люди научились говорить, понимать и соответственно этому пониманию запугивать и обманывать друг друга. Что бы было если люди не могли говорить, понимать информацию? (Тогда бы не было информационных войн? Но к чему бы это привело?)

Что если бы люди сами стали ощущать ту боль, которую они причиняют другим людям? (Были бы тогда войны? А каким способом тогда люди могли бы сбросить избыток агрессивности?)

2 Этап. Генерация идей: проблемная тема «Как заставить «информационную войну» служить во благо общества?» записывается на доске, чтобы участники постоянно видели ее перед собой, каждый выдвинет как можно больше идей, приветствуются озарения и необузданная фантазия. Можно высказывать безответственные, причудливые, нелепые идеи. Критиковать нельзя! Наложено табу на реплики: «Это глупо», «Детский лепет», «Ерунда», «Это невозможно» и т. п. Критика запрещается даже в форме жестов, ироничных взглядов и скептических усмешек. Иначе у генераторов может пропасть всякая охота генерировать.

Все идеи записываются в виде таблицы (первая колонка). Нет плохих идей! (для удобства можно записывать все идеи дополнительно на диктофон)

Для активизации процесса генерации во время мозгового штурма и для снятия напряжения участникам предлагаются методы:

1. Что подскажут фигуры? Выберите какую-нибудь фигуру, например, треугольник, и старайтесь определить связь между ним и вашей задачей. То же – с объёмными фигурами, цветами спектра (с каким цветом ассоциируется «информационная война», с каким – общество), с цифрами.

2. Будьте как дети. Исследуйте проблему так, как бы это делал ребенок. Задайте очевидные вопросы. Найдите ответы, которые удовлетворили бы ребёнка.

3. Метод от противного. Великие озарения могут наступить, если вместо размышлений о том, как сделать что-то, попробовать решить вопрос, как этого не делать.

4. Нарисуйте идею. Участники оформляют следующее предложение в форме рисунка. И пусть все пытаются истолковать нарисованное.

3 Этап. Оценка идей: самая лучшая идея – та, которую рассматриваем сейчас. Анализируем её так, как будто других идей нет вообще. Это правило подразумевает предельное внимание к каждой записанной идее. В выборе подходящих идей участвуют как эксперты, так и генераторы идей.

В период обсуждений заполняется вторая колонка таблицы.

Оценка:

«+» - очень хорошая, оригинальная идея.

«*» - неплохая идея.

«-» - не удалось найти конструктива.

Выбираются 10-15 интересных, оригинальных решений поставленной в начале проблемы.

4 Этап. Обсуждение проделанной работы.

Участники отвечают на вопросы:

1. Как вы считаете, мы достигли поставленной цели?

2. Как, по вашему мнению, мозговой штурм эффективный метод в генерации идей?

3. Что вам понравилось, а что нет в мозговом штурме?

Результаты обучения

Подведение итогов проходит в форме защиты проектов и написания эссе.

Роль государства, бизнеса, институтов гражданского общества и СМИ в формировании системы противодействия идеологии киберэкстремизма

Автор Аскарова Н.А., руководитель: Романова М.В.

Описание проекта: В целях качественного изучения темы «Роль государства, бизнеса, институтов гражданского общества и СМИ в формировании системы противодействия идеологии киберэкстремизма», предлагается проведение комплекса мероприятий для старшеклассников. Проведение данных мероприятий необходимо начинать со второй половины сентября, когда учащиеся адаптируются к учебным нагрузкам. Сроки проведения мероприятий варьируются в течение учебной четверти. Мероприятия проводятся последовательно в предложенном ниже порядке.

Цель проекта – формирование общественного сознания и гражданской позиции подрастающего поколения, объяснение сущности кибертерроризма, осознание глубины явления кибертерроризма.

Задачи проекта:

1. Проанализировать основные теоретические аспекты кибертерроризма и систем противодействия идеологии киберэкстремизма.

2. Сформировать основные компоненты методики проведения комплекса мероприятий со старшими школьниками.

3. Разработать комплекс мероприятий по проведению темы «Роль государства, бизнеса, институтов гражданского общества и СМИ в формировании системы противодействия идеологии киберэкстремизма».

План занятия:

1. **Мероприятие №1 (45 минут):**

- Организационный момент, психологический настрой. (5 мин);
- Изучение нового материала. Теоретическая часть. (30 мин);
- Домашнее задание. (2 мин);
- Вопросы учеников. (5 мин);
- Итог занятия. (3 мин);

2. **Мероприятие №2 (от 30 до 40 минут):**

Мероприятие №1

Названия мероприятий: «Роль государства, бизнеса, институтов гражданского общества и СМИ в формировании системы противодействия идеологии киберэкстремизма».

Цель мероприятия: помочь учащимся усвоить понятия киберпреступность и кибертерроризм, выяснить влияния сфер деятельности человека на формирование идеологии противодействия киберэкстремизму.

Основные задачи проведения мероприятия:

1. Объяснить важность проблемы кибертерроризма;
2. Рассказать о существующих сферах деятельности человека;
3. Донести до учащихся, как данная деятельность влияет на формирование идеологии киберэкстремизма.

Методы и приемы проведения мероприятия: лекция.

Подготовка к мероприятию:

Оформление аудитории: на доске написана тема занятия «Роль государства, бизнеса, институтов гражданского общества и СМИ в формировании системы противодействия идеологии киберэкстремизма». На экране запущена презентация по теме.

Ход проведения мероприятий:

I. Организационный момент, психологический настрой:

Приветствие, проверка присутствующих.

На доске запущена презентация.

Сегодня мы познакомимся с одной из разновидностей терроризма, такой как кибертерроризм. Проанализируем масштабы угрозы данного терроризма.

Запишите тему нашего занятия в тетрадь: «Роль государства, бизнеса, институтов гражданского общества и СМИ в формировании системы противодействия идеологии киберэкстремизма» (Слайд №1).

II. Изучение нового материала.

Безусловно, Интернет – это очень удобный и эффективный источник информации. Именно широчайшая распространенность Интернета и его всеобщая доступность стали теми факторами, благодаря которым Интернетом пользуются не только в положительных целях, но и в целях корыстных. Интернет-преступность (киберпреступность) сегодня становится реальным источником общественной опасности, современным ответвлением преступности.

Киберэкстремизм – это экстремизм в сети Интернет. Экстремизм проще всего определить как склонность и приверженность личности или группы лиц к крайним взглядам или действиям. Чаще всего этим словом обозначают радикальные общественные движения – террористическая деятельность, возбуждение социальной, расовой, национальной или религиозной розни и т.д.

Экстремизм – это ориентация в политике на радикальные идеи и цели, достижение которых осуществляется в основном силовыми методами и средствами.

Кибертерроризм – это многогранный феномен, обусловленный во многом бесконтрольным использованием глобальных сетей, недостаточным вниманием со стороны государства, гражданского общества и спецслужб к данному сегменту политики. Проявляется он в атаках на компьютеры, компьютерные программы и сети или находящуюся в них информацию, с целью создания атмосферы страха и безысходности в обществе во имя достижения целей и интересов субъектов террористической деятельности, требующий объединения усилий мирового сообщества для эффективного противодействия ему.

Характерными средствами кибертерроризма являются:

– воздействие на программное обеспечение и информацию в целях их искажения или модификации в информационных системах и системах управления;

– раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, вооруженных сил, кодах шифрования и др.;

– уничтожение или активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммутаций.

Террористы активно эксплуатируют возможности Интернета: легкий доступ; незначительные масштабы госрегулирования и цензуры или их полное отсутствие; потенциально огромные масштабы аудитории; анонимность; быструю передачу информации; мультимедийность среды, позволяющую комбинировать различные типы информации: текстовую, графическую, аудиовизуальную. С помощью Интернета террористы могут «управлять восприятием» – то есть позиционировать себя точно такими, какими хотят казаться, без фильтров, налагаемых традиционными СМИ, а также создавать ажиотаж относительно нужных аспектов событий. Террористы получают возможность влиять на освещение своей деятельности в СМИ, которые часто обращаются к их сайтам за дополнительной информацией.

Основной контингент интернет-пользователей – это представители молодежной среды. Молодые люди – активные пользователи глобальной сети, получающие львиную долю информацию именно из интернет-пространства. Довольно-таки много свободного времени молодые люди проводят в популярных социальных сетях. Интернет окружает их повсюду: выйти в глобальную сеть можно при помощи различных устройств. Важным фактором в данном случае является тот факт, что мировоззрение молодых людей находится еще на стадии становления и развития. Поэтому Интернет, с его спектром мнений и взглядов, распространенностью идей разного смысла и содержания, может представлять реальную опасность. Особенно данное суждение верно в отношение тех порталов и интернет-источников, которые созданы для распространения идей экстремистского и террористического толка.

В настоящее время, с учетом развития процессов глобальной информатизации, экстремизм только усиливает свои позиции. Государства всего мира, затронутые опасным социальным и политическим явлением, противостоят экстремизму разными методами и способами. С учетом современных реалий, многие государства сегодня борются с экстремизмом и в реальной, и виртуальной действительности.

Существует противоположное мнение о том, что государство не должно вмешиваться в Интернет-пространство, так как Интернет был создан для свободной связи и обмена информацией. Контролируя гло-

бальную Сеть, государство ограничивает свободный доступ граждан к информации, а в некоторых случаях преследует свои цели, например, ограничивает доступ к сайтам, которые, по сути, являются оппозиционной направленности и не преследуют экстремистских целей. Однако такая точка зрения не является вполне обоснованной. Одной из первостепенных задач государства является защита интересов гражданина и всего общества в целом от преступности и негативных явлений. Свобода интернета не должна стоять на пути реализации данной задачи. Представляется, что государство должно найти необходимый баланс интересов между правом гражданина на доступ к информации и защитой общества от преступных посягательств.

Глобальная информатизация всех сфер жизнедеятельности общества, в большей степени, понижает безопасность общества. Современный кибертерроризм способен продуцировать системный кризис в любом государстве с высокоразвитой информационной инфраструктурой. В современных условиях уязвимость инфраструктур перестает быть проблемой каждого государства в отдельности. Это общая угроза, решить которую можно только сообща, выстроить систему коллективной информационной безопасности с учетом современных и потенциальных угроз в киберпространстве.

Для решения этой задачи необходимы не только принятие соответствующих законов на национальном уровне, но и выработка единых международных стандартов, таких как: унификация понятийного аппарата, определение круга деяний, подлежащих криминализации, имплементация международных норм в национальное уголовное законодательство. Кроме того, необходимо выработать технические средства защиты, которые способствовали бы быстрому реагированию на информацию, появляющейся в Интернете.

Анализ влияния государства, бизнеса, институтов гражданского общества и СМИ в сфере формирования системы противодействия идеологии киберэкстремизма приводит нас к выводу: каждая из вышеперечисленных сфер деятельности человека в равной степени влияют на формирование данной системы противодействия.

IV. Домашнее задание.

Повторить пройденный материал. Сделать выводы по ее работе.

V. Вопросы учеников.

Учащиеся задают учителю свои вопросы по изученному материалу занятия.

VI. Итог урока.

1.Что вы понимаете под словом «кибертерроризм»?

2.Перечислите характерные средства кибертерроризма.

3.Как террористы эксплуатируют возможности Интернета?

Мероприятие №2: «Умники и умницы».

Цель мероприятия: улучшение информированности подростков о факторах риска, создаваемые кибертеррористами.

Основные задачи проведения мероприятия:

1. Научить видеть ситуацию с точки зрения другого человека или другой группы.

2. Сформировать у учащихся старших классов активной гражданской позиции.

3. Способствовать осознаю учащимися масштабами проблемы киберпреступности и кибертерроризма.

4. Формирование устойчивого интереса к предмету.

Ожидаемые результаты:

1. Воспитание гражданских качеств у подростков через организацию социально значимой деятельности.

2. Воспитание у детей чувств ответственности и сознательности.

3. Сознательное отношение к людям, а не как к объекту преступления.

Подготовка к мероприятию:

Ученики сидят за партами. Учитель задает вопросы, выбираются три ученика. Этим трем ученикам предоставляются на выбор три дорожки, по которым можно передвигаться, правильно ответив на вопрос. На красной дорожке два шага и нет права на ошибку. На желтой – три шага и возможность ошибиться один раз. На зеленой – четыре шага и два неверных ответа. Тот, кто первым пройдет дорожку, станет победителем. Разумеется, у «зеленого» игрока шансов меньше, чем у других – но, с другой стороны, «красный» вообще не может ошибиться. В том случае, если никто из трех участников не сможет ответить на заданный ведущим вопрос, отвечают остальные участники игры, таким образом они получают медаль и зарабатывают баллы.

Оборудование мероприятия:

Костюмы действующих лиц, декорации, магнитофон, мультимедийный проектор и экран.

Ход проведения мероприятий:

Учитель информатики: Здравствуйте дорогие участники и гости сегодняшнего мероприятия «Умники и умницы». Это игра для всех, здесь нет зрителей, вы все ее участники. Давайте поприветствуем действующих героев нашего мероприятия (в центр аудитории выходят участники мероприятия, которых учитель по очереди представляет аудитории).

Учитель информатики: Давайте познакомимся с правилами игры**:**

1. Чтобы получить орден умника, вы должны отвечать на вопросы.

2. Получив орден, вы становитесь «теоретиками».

3. Те из участников, кто наберет большее количество орденов, станет на «дорожку практики».

4. Если «практик» справится с заданиями на своем пути, то он выходит в финал.

5. Финальный тур определит победителя – «Умника».

I тур.

Учитель информатики:

1.Что такое экстремизм? *(Это ориентация в политике на крайне радикальные идеи и цели, достижение которых осуществляется в основном силовыми, а также нелегитимными и противоправными методами и средствами)*

2.Дайте определение киберэкстремизма. *(Это экстремизм в киберпространстве)*

*3.*Что такое киберпреступление? *(Киберпреступление принято считать уголовно наказуемые действия, подразумевающие несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных.)*

4. Какие виды киберэкстремизма существуют в современном мире? *(- экономический, - политический, - националистический, - религиозный, - молодежный, - экологический, - духовный)*

5. Что такое экономический экстремизм? ***(****«стремление установить одну форму собственности и единые методы ведения хозяйства (коммунистический фундаментализм) либо полностью отказаться от государственного регулирования экономической сферы, резко сократить социальные расходы (либерализм)»****)***

6. Что такое политический экстремизм? (*Настолько сложное и неоднозначное явление, что на сегодняшний день существует несколько разных определений. Однозначно только то, что его последователи стремятся к разрушению существующей в обществе политической системы и установлению своей – например, анархия, монархия, марксизм и другие. Чаще всего данный вид экстремизма включает в себя все остальные разновидности*.)

7. Что такое национальный экстремизм? (*Чаще всего связан с сепаратизмом, акцентуируется на продвижении прав «наших» и ущемлении прав «не наших» национальностей и этнических групп.*)

8. Что такое религиозный экстремизм? *(Это экстремизм, основанный на религиозной почве, избирающий религиозные идеи своим источником)*

9. Что такое экологический экстремизм? *(«противоправные акции групп и движений, осуществляемые с целью защиты окружающей среды от научно-технического прогресса как такового и нередко создающие угрозу общественному порядку*»)

Учитель информатики: Итак, трое лучших «теоретиков» выходят на «дорожку практиков». Узнаем их имена.

В зависимости от количества набранных орденов, участники выбирают «Дорожку практики».

Примечание.

1. На красной дорожке нельзя ошибаться ни разу.
2. На желтой дорожке можно ошибаться один раз.
3. На зеленой дорожке можно ошибаться два раза.

II тур. (Вопросы на более углубленные знания)

Вопросы для «теоретика» на красной дорожке.

1. Что такое пропедевтика? *(«введение в какую-либо науку, предварительный вводный курс, систематически изложенный в сжатой и элементарной форме»)*

2. Что такое профилактика? *(Под профилактикой понимаются «научно обоснованные и своевременно предпринимаемые действия, направленные на: предотвращение возможных физических, психологических или социокультурных коллизий у отдельных индивидов группы риска; сохранение, поддержание и защиту нормального уровня жизни и здоровья людей; содействие им в достижении поставленных целей и раскрытие их внутренних потенциалов»)*

«Теоретик» должен безошибочно ответить на данные вопросы. В том случае, если он ошибается, то покидает игру, ответ спрашиваем у остальных игроков зала. Правильно ответивший ученик получает медаль и балл.

Вопросы для «теоретика» на желтой дорожке.

1. Что входит в сферу пропедевтики? *(– знания об экстремизме и киберэкстремизме: их виды, особенности, признаки и истоки; – знания об особенностях проявления киберэкстремизма в ИКТ-среде, особенно в молодежной: сведения о разнообразных социальных институтах, политических, религиозных и псевдорелигиозных организациях, неформальных молодежных группах; – знание нормативных, законодательных, этических, моральных, правовых норм работы в сфере ИКТ: механизмы регулирования деятельности в сфере ИКТ (государственные стандарты, законы, нормативные акты, морально-этические нормы), нормы информационной этики и права.)*

2. Что входит в сферу профилактики? *(– создание негативного общественного мнения по отношению к явлениям киберэкстремизма: способы формирования общественного мнения, методы работы с молодежной субкультурой, семьей, социальной группой, личностью; – информирование о негативных аспектах воздействия на личность: негативные аспекты использования ИКТ: особенности подачи информации, дифференциация по различным характеристикам; – формирование навыков безопасной деятельности с использованием ИКТ: методы формирования необходимых навыков, основы информационной безопасности, механизмы обеспечения безопасного использования сетевых ресурсов, механизмы*

защиты от манипулятивных технологий, обеспечение личной безопасности в ИКТ-сфере.)

3. Характерными средствами кибертерроризма являются. *(- воздействие на программное обеспечение и информацию в целях их искажения или модификации в информационных системах и системах управления; - раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, вооруженных сил, кодах шифрования и др.; - уничтожение или активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммутаций.)*

«Теоретик» имеет право на одну ошибку. В том случае, если он ошибается более одного раза, то покидает игру, ответ спрашиваем у остальных игроков зала. Правильно ответивший ученик получает медаль и балл.

Вопросы для «теоретика» на зеленой дорожке.

1. Что относится к экстремисткой деятельности? *(- распространение листовок или плакатов, на которых отображается информация, связанная с призывами к осуществлению насильственных действий; - доступ к экстремистским форумам или сайтам в интернет-кафе; - заседание экстремистской группы в помещениях, принадлежащих общине или в общинных центрах; - просмотр террористических или экстремистских рекламных роликов, призывающих к насильственной деятельности и т. д.)*

2. Что такое информационный терроризм? *(вид террористической деятельности, ориентированный на использование различных форм и методов временного или безвозвратного вывода из строя информационной инфраструктуры государства или ее элементов.)*

3. Главная роль СМИ заключается в… *(том, чтобы как можно раньше оповестить общество о возможных угрозах, проблемах вызванных теми или иными причинами, а не замалчивания одной стороны проблемы и раздувания другой.)*

4. Одной из первостепенных задач Государства является … *(защита интересов гражданина и всего общества в целом от преступности и негативных явлений)*

«Теоретик» имеет право на две ошибки. В том случае, если он ошибается более двух раз, то покидает игру, ответ спрашиваем у остальных игроков зала. Правильно ответивший ученик получает медаль и балл.

Учитель информатики: Финал! Выявляем победителя (победителем становится один из «теоретиков», ставим ему оценку, также подсчитываем медали у игроков из зала. Тот, кто набрал наибольшее количество медалей получает оценку «отлично»).

Молодцы ребята! Вы многому научились благодаря этой игре, проблема киберэкстремизма очень важная на сегодняшний день, каждый из Вас должен понимать проблему киберпреступности, знать о возможных угрозах и не попадаться в сети кибепреступников.

Кибертерроризм. Современные кибертеррористические группировки

Автор Калашникова Е.Ф., руководитель: Романова М.В.

Описание проекта: В целях качественного изучения темы «Кибертерроризм. Современные кибертеррористические группировки», предлагается проведение комплекса мероприятий для старшеклассников. Проведение данных мероприятий необходимо начинать со второй половины сентября, когда учащиеся адаптируются к учебным нагрузкам. Сроки проведения мероприятий варьируются в течение учебной четверти. Мероприятия проводятся последовательно в предложенном ниже порядке.

Цель проекта: формирование общественного сознания и гражданской позиции подрастающего поколения, объяснение сущности кибертерроризма, осознание глубины явления кибертерроризма.

План проведения проекта:

1. Мероприятие №1 (45 минут)
- организационный момент, психологический настрой. (5 мин);
- изучение нового материала. Теоретическая часть. (30 мин);
- домашнее задание. (2 мин) ;
- вопросы учеников. (5 мин);
- итог занятия. (3 мин);

2. Мероприятие №2 (от 30 до 40 минут)
3. Мероприятие №3 (от 50 до 60 минут)

Мероприятие №1: «Кибертерроризм. Современные кибертеррорестические группировки».

Цель мероприятия: помочь учащимся усвоить понятий киберпреступность и кибертерроризм, оценить уровень ущерба от деятельности кибертеррорестических группировок.

Основные задачи проведения мероприятия:

1.Объяснить важность проблемы кибертерроризма;

2.Рассказать о существующих кибертеррорестических группировках;

3.Донести до учащихся, что данная деятельность не есть хорошо и несет за собой неблагоприятные последствия.

Методы и приемы проведения мероприятия: лекция.

Ход проведения мероприятий:

I. Организационный момент, психологический настрой:

Приветствие, проверка присутствующих.

На доске запущена презентация со следующей картинкой рисунок 1 (Слайд №1):

Рисунок 1. Кибертерроризм

Учащиеся отвечают на вопросы:

1.Как вы думаете, что представлено на картинке?

2.Каков основной смысл данного изображения?

3.Назовите одним словом, что изображено на рисунке?

Сегодня мы познакомимся с одной из разновидностей терроризма, такой как кибертерроризм. Проанализируем масштабы угрозы данного терроризма. Рассмотрим деятельность нескольких кибертеррорестических группировок нашего времени.

Запишите тему нашего занятия в тетрадь: «Кибертерроризм. Современные кибертеррорестические группировки» (Слайд №2).

II. Изучение нового материала.

Развитие новых информационных технологий с их простотой доступа, относительно низкой стоимостью и широкомасштабностью открывает терроризму новые границы и обусловливает появление такой новой и опасной его разновидности как кибертерроризм. Данный процесс заметно ускорился в связи с существенным расширением сферы Интернета.

Кибертерроризм проявляется во вмешательстве в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированной модификации компьютерных данных, что вызывает дезорганизацию работы т.н. критически важных элементов инфраструктуры государства и создает опасность гибели людей, значительного имущественного ущерба или иных тяжких последствий.

Кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. Особую озабоченность среди специалистов вызывает уязвимость компьютерных систем управления критической инфраструктурой (транспорт, атомные электростанции, водоснабжение и энергетика), подключенных к Интернету.

Способы использования террористами сети Интернет весьма разнообразны. С помощью Интернета осуществляются:

1. Сбор подробной информации о предполагаемых целях, их местонахождении и характеристике.

2. Сбор денег для поддержки террористических движений. Так, например, сайт о Чеченской республике представляет номер счета банка в Калифорнии, на который можно перечислить средства для поддержки чеченских террористов.

3. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени и встрече людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., т. е. синергетическое воздействие на деятельность групп, поддерживающих террористов.

4. Вымогательство денег у финансовых институтов с тем, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.

5. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов.

6. Поскольку «электронам не надо предъявлять паспорт», терроризм не ограничен больше тем государством, где скрываются террористы, более того, базы подготовки террористических операций уже, как правило, не располагаются в тех странах, где находятся цели террористов.

7. Если раньше сеть террористов обычно представляла разветвленную структуру с сильным центром, то теперь это сети, где не просматривается четких командных пунктов, более того, могут быть ничего не подозревающие соучастники – например, хакеры, которым неизвестно, к какой конечной цели приведут их действия.

8. «Всемирная паутина» может инициировать психологический терроризм. С помощью Интернета можно посеять панику, ввести в заблуждение, привести к разрушению чего-либо. Всемирная сеть – благодатная почва для распространения различных слухов, в том числе и тревожных. Так, 5 ноября 2003 г. «Аль Каида» распространила через Интернет предупреждение всем мусульманам, проживающим в трех крупнейших городах США, о необходимости немедленно покинуть эти города в связи с предстоящим новым терактом.

9. Как уже было сказано выше, возможности электронной почты или электронных досок объявлений используются для отправки зашифрованных сообщений.

К вышеперечисленным способам можно добавить также размещение в Интернете сайтов террористической направленности, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также об их самостоятельном изготовлении. Только в русскоязычном Интернете десятки сайтов, на которых можно найти подобные сведения.

Терроризм в сети позволяет не только атаковать глобальные цели или готовиться к таким атакам, он также дает возможность проводить террористические акции без физического присутствия исполнителей.

Прежде чем перейти к анализу сложного феномена кибертерроризма, необходимо определиться с более общим понятием «киберпреступности». Термин «киберпреступность» российскими и международными нормативными правовыми актами официально не зафиксирован. Каждая организация, государство и авторы любого закона располагают собственным мнением о том, что является киберпреступлением и киберпреступностью, а что нет. Многочисленные попытки создания пригодной дефиниции киберпреступности и связанных с ней терминов иллюстрируют, что это такой широкий и обобщенный термин, что эти попытки практически бесполезны. В данном случае необходимо разработать типовое определение киберпреступности. Важность единой терминологии заключается в том, что если мы не будем использовать одинаковые – или, по крайней мере, существенно не отличающиеся – определения, единый подход к киберпреступлениям будет невозможен. Невозможен будет также сбор достоверных статистических данных, предназначенных для правового анализа способов совершения киберпреступлений и тенденций развития и трансформации киберпреступности.

Термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.

Преступление, совершенное в киберпространстве это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ. Подчеркну, что понятие киберпреступность не ограничивается рамками преступлений, совершенных в глобальной информационной сети Интернет, она распространяется на все виды преступлений совершенных в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, информационная техника могут выступать (являться) предметом (целью) преступных посягательств, средой, в которой совершаются правонарушения, и средством или орудием преступления.

Одна из наиболее опасных разновидностей киберпреступности – *кибертерроризм* также требует корректного определения. Переход в промышленности и иных сферах деятельности на методы электронного управления технологическими процессами послужил основанием для появления нового вида терроризма – кибертерроризма, который проявля-

ется во вмешательстве в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированной модификации компьютерных данных, что вызывает дезорганизацию работы критически важных элементов инфраструктуры государства и создает опасность гибели людей, значительного имущественного ущерба или иных общественно опасных последствий.

Кибертерроризм представляет собой серьезную социально опасную угрозу для человечества, причем степень этой угрозы в силу своей новизны, обществом не до конца еще осознана и изучена. Опыт, который уже имеется у мирового сообщества в этой области, со всей очевидностью свидетельствует о несомненной уязвимости любого государства, тем более что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара.

Итак, кибертерроризм можно отнести к так называемым технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии. Сам термин «кибертерроризм» появился в IT-лексиконе предположительно в 1997 году. Именно тогда специальный агент ФБР Марк Поллитт определил этот вид терроризма как «преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны суб-национальных групп или тайных агентов».

Известный эксперт в области обеспечения безопасности информационных технологий Д. Деннинг говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенную с целью принудить органы власти к содействию в достижении политических или социальных целей».

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением к традиционному виду терроризма.

В настоящее время к группировкам кибертерроризма можно отнести «КиберБеркут» и «Сирийская Электронная Армия». КиберБеркут – это современная организованная группа хактивистов. Приставка «Кибер», означает, что деятельность группа ведёт в так называемом киберпространстве (сети Интернет). Группа появилась после расформирования спецподразделений милиции «Беркут». Состав неизвестен. В силу понятных причин члены сообщества соблюдают анонимность. Провозгласили о своих целях, как борьба с неофашизмом, национализмом и произволом

власти в Украине. Так, например, объявили вне закона организацию «Правый сектор». Девиз напоминает таковой группы «Анонимус». Деятельность группировки:

- Создание помех в работе ЦИК Украины путём повреждения системы IFES накануне выборов. Блокировки сотовых телефонов организаторов выборов.
- Временно заблокирована работа сайтов МВД Украины и Генеральной прокуратуры Украины. Также временно заблокирована работа сайтов телеканалов «Интер» и «1+1».
- Атаки на сайты НАТО.
- Атака на сайты частных военных компаний США.
- Взлом почтового ящика и опубликование переписки И. В. Коломойского с прокурором Львовской области и взлом компьютера и электронной почты помощника олигарха. Также выложены архивы с содержимым 89 ящиков электронной почты сотрудников львовской областной прокуратуры.
- Опубликование переписки народных депутатов партий «Батькивщина» и «Удар». Опубликование переписки с посольством США и американскими фондами.
- Выкладывание в публичный доступ записи телефонных переговоров Ю. В. Тимошенко и Н. И. Шуфричем.
- Выкладывание в публичный доступ записи телефонных переговоров Верховной представительницы Европейского союза по иностранным делам и политике безопасности Кэтрин Эштон и Министра иностранных дел Эстонии Урмаса Паэта.
- Взлом и опубликование переписки исполняющего обязанности министра внутренних дел Украины А.Б. Авакова.
- Блокировки телефонов сотовой связи членов действующего правительства Украины и приближённым к ним лиц и т.п.

«Сирийская Электронная Армия» (англ. Syrian Electronic Army, SEA) или Сирийские Электронные Солдаты (англ. Syrian Electronic Soldiers) – группа сирийских хакеров, которая выступает в поддержку президента Сирии Башара аль-Асада. СЭА является первой виртуальной армией в арабском мире, которая начала проведение кибератак против своих противников. Впервые деятельность активистов была зафиксирована в мае 2011 года и была связана с началом в Сирии гражданской войны. Согласно анонимным заявлениям представителей Сирийской Электронной Армии, в ее состав входит патриотически настроенная молодежь, которая пытается защитить свою страну от иностранных медиакампаний, распространяющих дезинформацию о Сирии.

IV. Домашнее задание.

Найти информацию о деятельности современных кибертеррористических группировках. Выявить основные функции функционирования данной группировки. Сделать выводы по ее работе.

V. Вопросы учеников.

Учащиеся задают учителю свои вопросы по изученному материалу занятия.

VI. Итог урока.

Учащиеся отвечают на вопросы:

1.Что вы понимаете под словом «кибертерроризм»?

2.Какие группировки относятся к кибертеррорестическим?

3.Каковы основные функции деятельности таких группировок?

Мероприятие № 2: «На скамье подсудимых – КиберБеркут!».

Цель мероприятия: улучшение информированности подростков о факторах риска, создаваемые кибертеррористическими группировками, и в содействие не принимать участие в подобных группировках.

Основные задачи проведения мероприятия:

1.Научить видеть ситуацию с точки зрения другого человека или другой группы.

2.Сформировать у учащихся старших классов активной гражданской позиции.

3.Способствовать осознаю учащимися масштабами проблемы киберпреступности и кибертерроризма.

Ожидаемые результаты:

1. Воспитание гражданских качеств у подростков через организацию социально значимой деятельности.

2. Воспитание у детей чувств ответственности и сознательности.

3. Сознательное отношение к людям, а не как к объекту преступления.

Подготовка к мероприятию:

Задания для участников мероприятия: распределить действующих ролей судебного разбирательства (судьи, прокурора, адвоката, подсудимые (5 человек), потерпевших (4 человека), свидетели (1 человек), эксперт, секретарь суда, остальные зрители).

Оформление аудитории: на доске написана тема мероприятия «На скамье подсудимых – КиберБеркут!». Школьные столы расположены в примерном подражание судебному залу заседания: круглый стол - для заседания присяжных, отдельный стол для судьи и секретаря, стулья для остальных участников процесса, трибуна для свидетелей и потерпевших. В центре аудитории судейский стол, на столе таблички «Адвокат», «Судья» и «Прокурор». На стенах плакаты: «Скажи кибертерроризму нет!».

Оборудование мероприятия:

Костюмы действующих лиц, декорации, магнитофон, мультимедийный проектор и экран.

Ход проведения мероприятий:

Учитель информатики: Здравствуйте дорогие участники и гости сегодняшнего мероприятия «На скамье подсудимых – Кибер Беркут!». Давайте поприветствуем действующих героев нашего мероприятия (в центр аудитории выходят участники судебного заседания, которых учитель по очереди представляет аудитории

Учитель информатики (обращает внимание на пословицу): «От сумы да от тюрьмы не зарекайся». (Народная мудрость)

Учитель информатики: О чём нам напоминает эта народная мудрость?

Ученик: Неблагоприятные повороты судьбы.

Учитель информатики: О каких неблагоприятных поворотах судьбы мы посветили наше сегодняшнее мероприятие? (учащиеся отвечают)

Наше заседание прошу считать открытым! (в аудиторию входит секретарь)

Секретарь (громко): Всем встать! Суд идет! (Звучит музыкальная заставка из передачи «Осторожно Модерн» на сцене появляются Адвокат, Судья, Прокурор, проходят на свои места, музыка плавно убирается).

Судья: Сегодня (число, месяц) заслушивается дело против вредителей народа. Введите же в зал обвиняемых - это участники современной кибертеррористической группировки «Кибер Беркут». Звучит отрывок из песни и на сцене появляются участники группировки, которых на скамью подсудимых сопровожает милиционер.

Судья: Вы обвиняетесь по следующим нарушениям:

-конституционных прав человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых и иных сообщений, на защиту своей чести и своего доброго имени;

-сбора, хранения, использования и распространения информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

-взлома информационных систем федеральных органов государственной власти.

Судья: Слово предоставляется обвинителю.

Прокурор: Ваша Честь, Господа присяжные заседатели, надеюсь, вы внимательно слушали судью, который достаточно полно и беспристрастно охарактеризовал нарушения совершенные обвиняемыми. Следствием установлено, что обвиняемые в течение нескольких месяцев совершают противоправные действия с информацией, способствуют к сбоям работы органов правительства. За это они заслуживают самого сурового наказания. Прошу заслушать показания потерпевших и свидетелей обвинения.

Судья: Заслушаем показания потерпевших.

Прокурор: В качестве первого потерпевшего мы просим начальника ЦИК Украины. (Обращается к начальнику ЦИК Украины). Посмотрите внимательно на обвиняемых. Знакомы ли они вам? Что вы можете рассказать о их деятельности?

Первый потерпевший (начальник ЦИК Украины): Добрый день! Да, конечно знаком. Это участники кибертеррорестической группировки, которая создавала помехи в работе ЦИК Украины путем повреждения системы IFES накануне выборов. Блокировала сотовые телефоны организаторов выборов. Представленные мною обвинения могут быть подтверждены свидетелями следующей видеозаписью. (Передает секретарю видеозапись, которую демонстрируют на экране проектора, во время просмотра видеозаписи из зала заседания слышатся недовольные крики.)

Судья: Суд принял во внимание данную видеозапись.

Прокурор: Слово предоставляется второму потерпевшему администратору сайтов МВД Украины и Генеральной прокуратуры Украины.

Второй потерпевший (администратор сайтов МВД Украины и Генеральной прокуратуры Украины): Деятельность данной группировки способствовала временной блокировки сайтов МВД Украины и Генеральной прокуратуры Украины. Также временно была заблокирована работа сайтов телеканалов «Интер» и «1+1». В период с 24 по 26 апреля вы могли сами это наблюдать. Нашей разведывательной службой было выяснено, что именно деятельность этих людей послужила данному сбою. (Выкрики с зала заседания)

Секретарь: Для дачи показаний приглашается третий потерпевший - Коломойский Игорь Валерьевич.

Третий потерпевший (Коломойский Игорь Валерьевич, произносит речь громко с жестами и эмоционально): Здравствуйте! Я, Коломойский Игорь Валерьевич, унижен, оскорблен! Они, они взломали мой почтовый ящик и опубликовали переписки с прокурором Львовской области. Я имею право на личную жизнь! Они испортили мою репутацию! Прошу Вас господин судья накажите этих преступников.

Адвокат (вскакивая): Защита протестует. Свидетель называет моих подзащитных преступниками еще до вынесения приговора!

Судья: Протест принят. Прошу свидетелей быть корректными и не нарушать принцип презумпции невиновности. (Стучит молотком).

Секретарь: Приглашается четвертый потерпевший - Тимошенко Юлия Владимировна.

Четвертый потерпевший (Тимошенко Юлия Владимировна): Добрый день! Наказать! Наказать! Прошу этих людей. Они выложили в публичный доступ записи моих телефонных переговоров с Н. И. Шуфричем. Какое они имели право это делать без моего права? Вот доказательство!!! (Протягивает судье папку с подтверждениями).

Прокурор: Слово предоставляется пятому потерпевшему члену действующего правительства Украины.

Пятый потерпевший (Член действующего правительства Украины): Господин судья, прошу Вас обратить внимание на тот факт, что целенаправленная деятельность этих людей привела к блокировке телефонов и сотовой связи членов действующего правительства Украины и приближённым к ним лиц. Это немыслимо!!! Как они могут, против своего же правительства идти? Ужас! Ужас!

Судья: Есть ли свидетели со стороны обвинения?

Прокурор: Да, Ваша честь.

Судья: Суд приступает к показаниям свидетелей обвинения. Суд предупреждает: все свидетели обязаны говорить правду и ничего кроме правды.

Секретарь: Для дачи свидетельских показаний со стороны обвинения приглашается Член действующего правительства Украины - Арсений Яценюк.

Свидетель (Арсений Яценюк): Добрый день! Да, действительно я случайно стал свидетелем деятельности данной группировки. Ранее эти люди работали на правительство Украины, но по неопределенным причинам были исключены из его органов. И видимо в корыстных целях решили навредить его работе.

Судья: У стороны защиты есть дополнительные материалы для рассмотрения в данном судебном заседании?

Адвокат: Нет, ваша честь.

Судья: Суд предоставляет заключительное слово главному обвинителю.

Прокурор: Уважаемый господин судья. Я взываю к справедливости. Обвиняемые должны быть наказаны, так как они представляют опасность для человеческого общества в несанкционированном использовании информации с высоким уровнем секретности

Судья: Заключительное слово предоставляется главному защитнику.

Адвокат: Уважаемый судья. Вы, только, что прослушали речь господина прокурора. Но прежде чем моим подзащитным вынесут приговор, я хотел бы обратить Ваше внимание на следующие обстоятельства.

Да, мои подзащитные представлены серьезные обвинения, но нет конкретных причин для их обвинения. Все организации, органы и люди должны сами позаботиться о защите сетевой инфраструктуры. На смену одним кибертеррорестическим группировкам придут другие. Мои подзащитные, активно сотрудничают со следствием. Прошу учесть эти факты, как смягчающие вину обстоятельства и не выносить моим подзащитным слишком суровый приговор.

Судья: Последнее слово подсудимым.

Подсудимые: Уважаемый суд нам было горько и обидно выслушивать обвинения в наш адрес. Взгляните на нас внимательно, мы ведь люди. Мы просим суд проявить к нам снисхождение.

Судья: Суд удаляется для постановления приговора.

Секретарь: Всем встать. Судья возвращается.

Судья: *Суд постановляет:*

- признать данную группировку виновной в совершенных нарушениях;

- предложить специальным службам усилить контроль за их деятельностью;

- обратиться к каждому из владельцев секретной информации, научитесь защищать информацию от утечки и взлома.

Приговор окончательный и обжалованию не подлежит. Судебное заседание объявляю закрытым. Все свободны.

Учитель информатики: Мы закончили судебный процесс, но мы ещё будем возвращаться к этой теме. Борьба с кибертерроризмом – это дело не одного, и не нескольких человек, а всего человечества. Каждый должен внести в эту борьбу свою маленькую лепту. Спасибо за внимание!

***Мероприятие №3*: «Моё письмо спасёт человека».**

Цель мероприятия: закрепление полученных знаний по теме «Кибертерроризм. Современные кибертеррористические группировки».

Основные задачи проведения мероприятия:

1. Развитие навыков проектной деятельности, исследовательской деятельности.

2. Воспитание активности в деле предостережения людей от вступления в кибертеррористическую группировку.

Методы и приемы проведения мероприятия: конкурс.

Ожидаемые результаты:

▪ воспитание чувства ответственности, внимательности, аккуратности;

▪ развитие познавательных интересов, навыков осторожности, самоконтроля.

Подготовка к мероприятию:

Оформление аудитории: на доске написана тема занятия «Моё письмо спасёт человека», раздача карточек с баллами.

Учитель информатики: Завершением изучения темы «Кибертерроризм. Современные кибертеррористические группировки» будет следующая работа: участие в конкурсном проекте «Моё письмо спасёт человека». Вам предлагается написать письмо о предостережение от вступления в кибертеррористическую группировку. Ваше письмо должно выглядеть как послание, чтобы оградить людей от вступления в подобную

группировку. Это может быть письмо в будущее вашим детям и т.п. Можете приступать! Всем удачи!

Учитель информатики: Итак, письмо написано, пора и подвести итоги, каждый из вас по очереди у доски зачитывает свое письмо.

На вашем рабочем месте лежат карточки с одним баллом, который вы можете вручить автору понравившегося вам письма. В итоге, тот ученик, который наберет больше всего баллов и победил в нашем конкурсном проекте.

Объявление и награждение победителей.

Учитель информатики: Поздравляем победителя! Спасибо за внимание!

Опасности киберэкстремизма. Как уберечь своего ребенка

Автор Ерошин Н.В., руководитель: Новикова И.Н.

Описание проекта: внеклассное мероприятие с целью профилактики киберэкстремизма среди молодежи.

Цель проекта – ознакомление родителей с проблемой киберэкстремизма и способами защиты от него.

Задачи проекта:

1. Объяснить важность проблемы киберэкстремизма;
2. Рассказать о существующих видах, формах и специфических особенностях киберэкстремизма;
3. Рассказать о возможных методах решения проблемы вовлеченности детей в киберэкстремизм;
4. Мотивация родителей на проявление активной гражданской позиции посредством распространения материалов о проблеме и защите от киберэкстремизма;
5. Объяснить родителям, что они – последний и самый главный рубеж защиты своих детей от киберэкстремизма.

Во время занятия школьники:

- Рассказывают о видах, формах кибрэкстремизма:
- Выявляют возможные методы решения проблемы киберэкстремизма.

Ожидаемые результаты проекта:

- Родители должны в общих чертах понять проблему киберэкстремизма;
- Выявить основные пути решения данной проблемы.

Методы, применяемые в проекте: экспозиционный, управленческий.

План проведения проекта:

1. Организационный момент (1 мин);

2. Теоретическая часть (15 минут);

3. Обсуждение с родителями (20-30 минут).

Ход занятия:

При разработке методики проведения мероприятия «Опасности киберэкстремизма. Как уберечь своего ребенка» была использована андрагогическая модель обучения.

Мероприятие можно условно разделить на два этапа: в ходе первого классный руководитель рассказывает о киберэкстремизме и его особенностях, в ходе второго – идет обсуждение проблемы между родителями и учителем, родители задают вопросы, рассказывают о проблемах в общении со своими детьми, все вместе предлагают решение этих проблем и нахождение правильного подхода к ребенку. Разделение на этапы условно потому, что если у родителей возникают вопросы или необходимость обсудить что-то во время подачи материала, у них должна быть такая возможность.

Учитель в ходе мероприятия должен осуществлять контроль неявно (общаться с родителями на равных, но в качестве более опытного члена группы), т.к. один из основных принципов андрагогики – отсутствие жесткого контроля и недирективный характер обучения. Это означает, например, что если учитель обнаружил, что обсуждение начало сваливаться не в то русло или родители с ошибкой поняли какую-то часть информации, он должен незаметно и плавно воздействовать на группу, посредством пояснений, предложений и советов.

Теоретическая часть.

Ниже представлена примерная речь учителя. Она тезисно отражена в приложенной презентации.

(Слайд 2) Интернет значительно облегчил нашу жизнь. Мы используем его для развлечений, общения, работы, оплаты счетов и т.д. Но Интернет - всего лишь инструмент и люди определяют, будет он использован во благо или во зло.

(Слайд 3) В реальной жизни общество и государство обеспечивают нашу безопасность моралью, законами и правоохранительными органами. Но в Интернете защитить человека намного сложнее, потому что защита, обеспечиваемая государством от сетевых опасностей, не эффективна.

(Слайд 4) Почему государство и общество не могут защитить нас

1. Тот, кто ищет, тот всегда найдет. Сколько бы законов не выпускалось, как бы общество не осуждало те или иные действия, киберэкстремизм будет процветать до тех пор, пока кто-то в нем заинтересован.

2. Но самая главная причина, по которой законодательно невозможно эффективно защититься от киберэкстремизма заключается в том, что очень сложно дать однозначное определение киберэкстремистскому

контенту. Можно выделить категории, характерные признаки, но никогда нельзя сказать наверняка, что подтолкнет подростка к увлечению радикальными идеями.

Надеясь лишь на общественную защиту от киберэкстремизма, мы снимаем с себя ответственность за то, что происходит или может произойти с нами и нашими детьми. Нужно признать, что этот путь подвергает нас огромной опасности, обеспечивая мнимый психологический комфорт, заключающийся в идее о том, что кто-нибудь другой позаботиться о нашей безопасности.

(Слайд 5) Преступления в сети Интернет – очень опасное и коварное явление. Даже порядочный человек может стать участником преступных действий. Сам того, не подозревая, он способен нанести огромный моральный ущерб другим пользователям сети.

(Слайд 6) Самое главное – вы можете не знать, что ваш ребенок уже вовлечен. Даже если у вас установлены доверительные отношения, даже если вы на 100% убеждены в том, что ваш ребенок не способен кому-то навредить – он, сам того не понимая, так или иначе может быть вовлечен в киберэкстремизм.

(Слайд 7) Киберэкстремизм может быть направлен как против человека, так и на него. Например, если подросток становится объектом травли – киберэкстремизм направлен против него. Если же подросток после прочтения какой-то статьи или книги становится ярым приверженцем какой-либо радикальной идеи и группы, распространяющей радикальные взгляды – значит, контент был направлен на вовлечение его в преступную деятельность.

(Слайд 8) Подростки втягиваются проще. Подростков легко заинтересовать, задеть за живое, вызвать гнев или любую другую сильную эмоцию и, затем, на пике этой эмоции подкинуть нужную идею. Ослепленный сильными переживаниями неокрепший подростковый ум без колебаний примет эту идею как единственно правильную, а человека, который «открыл глаза на мир» возведет в ранг духовного учителя.

(Слайд 9) Как происходит вовлечение в киберэкстремизм. Анонимность при совершении преступлений в сети влияет на человека сразу с нескольких сторон. Во-первых, человек приобретает иллюзию защищенности: «никто не знает мою личность, следовательно, меня невозможно будет найти и наказать». Данное убеждение совершенно иллюзорно, т.к. если правоохранительные органы посчитают преступление достаточно серьёзным, им не составит совершенно никакого труда найти злоумышленника и привлечь его к ответственности. Во-вторых, при сочетании с групповым характером преступления, достигается ощущение мнимой невиновности: чаще всего невозможно понять, кто именно нанес наиболее тяжелые психические травмы жертве. Кроме того, групповая ответственность всегда легче, чем ответственность индивидуальная.

(Слайд 10) Групповой характер действий. Преступники в сети Интернет чаще всего действуют группой, организованной или не очень. Как правило, если речь идет о преступлениях финансового характера (кража средств с банковских счетов, электронных кошельков и т.д.) группа бывает строго организована и малочисленна: работают обычно профессионалы. Если же речь идет о травле какого-то человека в сети – группы зачастую не имеют строгой организации и довольно многочисленны: составом таких групп может быть кто угодно.

(Слайд 11) Обезличенность жертвы. Жертва в среде киберпреступлений зачастую предстает в обезличенном виде: преступникам психологически легче совершить злодеяние в силу того, что они не способы наблюдать страдания жертвы – она видится им не человеком, а просто профилем в социальной сети или банковским счетом с круглой суммой.

(Слайд 12) «Шуточный» характер действий. Данный фактор актуален именно для травли: участники зачастую думают, что просто шутят, не понимая, что жертва может вполне всерьёз воспринимать их слова.

(Слайд 13) Личностная недостаточность участников преступления. Этот фактор так же актуален для издевательских преступлений: основным мотиватором, подталкивающим преступников к действию является мнимая ненависть к людям и всему миру, возникающая на фоне психических травм различной степени тяжести и неудовлетворительной социализации.

(Слайд 14) Желание принадлежать к какой-либо социальной группе. Данный фактор проистекает из предыдущего: эмоционально неуравновешенные и неуверенные в себе люди зачастую чувствуют сильную потребность идентифицировать себя в качестве члена какой-либо социальной группы, причем для них совершенно неважно, будет эта группа заниматься чем-то, условно говоря «хорошим» или «плохим». Как правило, такие люди приобщаются к той социальной группе, к которой им приобщиться легче всего.

(Слайд 15) В случае с подростками можно выделить еще несколько факторов, которые делают их намного более уязвимыми перед вовлечением в киберпреступностную и киберэкстремистскую деятельность (перед перечислением и описанием спросить у родителей, какие, по их мнению, эти факторы).

(Слайд 16) Любопытство: эта черта присуща всем подросткам. Они активно познают мир, хотят попробовать как можно больше разных вещей, получить как можно больше ощущений от жизни.

(Слайд 17) Несформированная система жизненных ценностей: подростки находятся в активной стадии формирования моральных, этических и духовных ценностей, их взгляд на мир зачастую очень непостоянен, на него легко повлиять.

(Слайд 18) Юношеский максимализм: наряду с тем, что система взглядов еще не сформирована, как ни странно, присутствует предубеждение, что «мое» мнение или «наше» мнение (если подросток приобщает себя к какой-то группе), является единственно правильным. Взгляды зачастую носят однобокий и радикальный характер, любые явления делятся только на белые и черные.

(Слайд 19) К нежелательной информации экстремистского толка направленной на молодежь в сети Интернет можно отнести:

– пропагандирующие порнографию материалы;

– пропаганда насилия;

– пропаганда наркотических средств;

(Слайд 20)

– пропаганды социального, расового, национального и религиозного неравенства;

– пропаганда терроризма;

– рецепты по изготовлению оружия и взрывчатых веществ в кустарных условиях.

(Слайд 21) Способы защиты.

1.Общественное воздействие: в эту группу защиты от киберэкстремизма и киберпреступлений входят законы, общественная мораль, воздействие на человека различных СМИ антиэкстремистского толка.

2.Личное воздействие: защита, завязанная на близком круге общения человека – друзьях, родственниках. В эту группу так же входит воздействие человека на самого себя: самообразование, самоконтроль, честность с самим собой.

3.Программно-технические средства защиты.

(Слайд 22) Программно-технические средства защиты. Существует большое количество программно-технических средств для ограничения доступа подростков к нежелательной информации: различные сетевые экраны, программы для контроля деятельности детей в сети, различные услуги типа «детский интернет» от провайдеров. Этот способ защиты легко обойти при определенных навыках владения компьютером, кроме того, подросток может просто выйти в Интернет не из дома или школы, а из неконтролируемого места.

(Слайд 23) Личная защита от киберэкстремизма, требует значительных умственных усилий и воли, развитого умения сомневаться во всем, что происходит в нашем уме, а так же умения воспитывать самого себя. Многие родители бессознательно не хотят вкладывать подобные вещи в своих детей, т.к. есть и обратная сторона медали: их дети станут независимыми в своих взглядах, могут усомниться в авторитете самих родителей.

(Слайд 24) Киберэкстремизм совершенно бессилен в отношении людей, способных контролировать свои эмоции, критически мыслить,

подвергать здравому сомнению все, что они слышат и видят. Этот путь требует большого усердия, взаимопонимания, любви и доверия своим детям. Фактически, это именно то, что нужно, чтобы защитить своих детей от экстремизма в любых его проявлениях, онлайн или в реальности: любить своих детей, заботиться о них и доверять им, ведь мы – взрослые – самый последний рубеж защиты наших детей от негативного психического воздействия.

(Слайд 26) Как понять, что подростк вовлечен. О том, что подросток вовлечен в киберэкстремизм, можно понять по косвенным признакам:

1. Агрессивность.
2. Замкнутость.
3. Подавленное настроение, депрессия.
4. Навязчивые разговоры о политике, национализме и т.д. с ярким негативным окрасом.

Для того чтобы разобраться в ситуации нужно найти с подростком общий язык и поговорить.

Обсуждение проблемных вопросов и ситуаций с родителями:

Информация для учителя: следует во всех ситуациях сделать акцент на то, что при взаимодействии с подростком родителям всегда следует действовать спокойно, без лишних эмоций и резких движений. Ни в коем случае нельзя осуждать или ругать подростка, т.к. это может только усилить психологический барьер.

1. Подросток стал объектом травли. Как можно уменьшить психический стресс, связанный с этим и по возможности прекратить травлю? Во-первых, следует провести с ребенком разъяснительную беседу. Нужно донести до него, что мнение окружающих не имеет жизненной важности, как ему может казаться. Во-вторых, следует объяснить ему, что чем менее близко он принимает к сердцу оскорбления в свой адрес, тем спокойнее он будет и тем меньший интерес это будет вызывать у травящих. Опционально можно заблокировать профили своего ребенка в социальных сетях и форумах, которые он посещает. В-третьих, необходимо установить, кто травит ребенка и насколько серьёзные оскорбления или угрозы он получает. Если угрозы и оскорбления явно носят серьезный характер, то необходимо обратиться в правоохранительные органы. Выясните, можете ли вы каким-то образом повлиять на травящих: если, например, этим занимаются его одноклассники, можно подключить к решению этого вопроса их родителей.

2. Подросток травит одноклассников. Какие действия следует предпринять родителям? Ни в коем случае не наказывайте его, не ругайте и не осуждайте. Важно понять, что если подросток начал травить других людей, издеваться над ними – у него самого присутствуют серьёзные психические проблемы. Если вы можете найти общий язык со своим ребенком, попробуйте выяснить, что именно заставляет его вести себя та-

ким образом. Если он отказывается говорить об этом, попробуйте успокоить его и сходить с ним к психологу, который поможет установить истинную причину заинтересованности вашего ребенка в страдании других людей.

3. Ребенок оказался вовлечен в киберэкстремистскую деятельность. Что можно посоветовать его родителям? Превентивная защита всегда лучше. Чем разбираться с проблемой, лучше сделать так, чтобы ее не было в принципе. Если у вашего ребенка здоровая и счастливая жизнь, если он чувствует себя полноценным человеком, не сомневается в том, что родители всегда поддержат и позаботятся о нем, если он не замкнут, не потерян – его шансы увлечься преступностью в реальности или Интернете намного ниже. Самое главное, что необходимо понять: когда-нибудь ваш ребенок вырастет. В нем разовьется все то, что вы в него сейчас вкладываете, ни одно ваше взаимодействие с ним не пройдет бесследно. Никто не знает, с какими трудностями ему придется столкнуться, в каких ситуациях побывать, с какими людьми он будет общаться. Спросите себя, какими качествами должен, по-вашему, обладать взрослый, сильный, ответственный и счастливый человек со здоровой психикой. Таким ли вы воспитываете своего ребенка?

Социально-психологические факторы развития киберэкстремизма

Автор Долматова Д.Е., руководитель: Чернова Е.В.

Описание проекта: внеклассное мероприятие с целью профилактики киберэкстремизма среди молодежи.

Цель проекта – ознакомление студентов с проблемой киберэкстремизма и способами защиты от него.

Ход занятия:

Разработанное мероприятие делится на 2 этапа.

1 этап. Ознакомительный.

Воспитательное мероприятие проводит: куратор/преподаватель

Состав группы учащихся: студенты.

Форма проведения мероприятия: вводное занятие.

Вид деятельности: познавательная.

Цель мероприятия: ознакомить участников с правилами игры.

Методы и приемы проведения мероприятия: беседа.

Задачи проведения мероприятия:

1. Выбор тезиса
2. Разделение на команды
3. Объяснение правил игры «Дебаты»

4. Постановка задачи о съемке ролика.

Тезисы на выбор:

1. «Киберэкстремизм в защиту свободы – не преступление»;
2. Закон о едином реестре сайтов: за или против.

Далее происходит разделение группы на команды:

Команда утверждающих – 4 человека, команда отрицающих – 4 человека, остальные зрители (данную игру можно провести несколько раз, чтобы все студенты группы смогли поучаствовать в команде утверждающих/отрицающих, и обыграть разные тезисы).

Правила игры «Дебаты»:

- в дебатах участвуют все (часть студентов принимает на себя роли спикеров и действует в соответствии с ними, остальные – «зрители» – подбирают аргументы «за» и «против», формулируют вопросы);
- в процессе выступлений все соблюдают регламент, в противном случае председатель имеет право прервать выступающего;
- каждый участник команды имеет право выступить только один раз;
- в случае затруднений при ответах на вопросы каждый спикер, кроме подводящего итоги, имеет право взять один таймаут длительностью до 2 мин;
- спикер имеет право не отвечать на вопрос без объяснения причин;
- к концу игры каждый определяет свою позицию и аргументирует ее;
- эксперты оценивают аргументы, но не участников;
- оратор (спикер, зритель) должен начинать свое выступление обращением к ведущему дискуссию «Уважаемый председатель...».

Участники дебатов обращаются один к другому, употребляя форму «Уважаемый (Уважаемая)…» или любую другую подобную форму.

В качестве представления команды и её позиции по выбранному вопросу участникам команд утверждающих и отрицающих необходимо снять видеоролик. Ролик должен содержать представление команды, а так же отдельно каждого из участников команды, формулировку тезиса, основные понятия.

2 этап. Дебаты.

Воспитательное мероприятие проводит: куратор/преподаватель.

Состав группы учащихся: студенты.

Форма проведения мероприятия: дебаты.

Подготовка к мероприятию: описана в этапе 1.

Оборудование урока: компьютер, мультимедийный проектор и экран, видеоролики, раздаточный материал.

Ход проведения мероприятия

Перед дебатами участники занимают места в следующем порядке:

- в начале аудитории по центру – председатель и эксперты;

- справа от председателя – 4 человека команды «Утверждения»;
- слева от председателя – 4 человека команды «Отрицания»;
- напротив председателя и экспертов, посередине – зрители.

Зрителям раздаются чистые листы бумаги.

Председатель: Добрый день, уважаемые гости и участники нашего мероприятия. Сегодня у вас всех есть возможность поучаствовать в таком увлекательном деле, как дебаты. Справа и слева от меня располагаются две команды, которые уже провели большую работу. Сейчас нас ожидают результаты их работы. Дебаты состоят из 4 туров. Первые два тура – выступление спикеров. Третий тур – тур вопросов, которые будут задавать зрители. Заключительный тур – подведение итогов. У первого спикера есть пять минут на выступление, у второго – семь. На подведение итогов выделяется 3 минуты. Главной темой наших сегодняшних дебатов является - киберэкстремизм. Всё остальное вам расскажут наши участники. Приступим.

Слово берет первый спикер команды утверждения. Он приветствует присутствующих, представляет свою команду и показывает видеоролик. После этого выступает первый спикер команды отрицания. Он так же всех приветствует, представляет свою команду и показывает видеоролик.

Председатель: Теперь мы узнали главный тезис наших дебатов и отношение команд к нему. Позволим им раскрыть свое мнение подробнее.

Слово берет второй спикер утверждающий команды. Он дает развернутую аргументацию названных ранее тезисов. Далее аналогично выступает второй спикер команды отрицания.

Председатель: Итак, мы выслушали выступление двух спикеров обеих команд. Настало время тура вопросов. Каждый спикер работает с вопросами индивидуально, т. е. не имеет возможности обратиться за помощью к другим участникам команды. Отвечая на вопросы зрителей, спикер должен помнить, что это тоже оценивается экспертами в общем протоколе игры. Ответ на вопрос должен быть точным, конкретным, достаточно обоснованным. Спикер имеет право обратиться к задавшему вопрос с просьбой повторить его, если вопрос прозвучал невнятно или слишком витиевато, или взять тайм-аут, если не знает точного ответа на вопрос. Каждая команда имеет право получить не более 6 минут для консультаций друг с другом. Один тайм-аут не может превышать 2 минуты. Ваши вопросы.

Зрители задают вопросы участникам команд. Каждый спикер может ответить не более чем на два вопроса.

Председатель: Уважаемые зрители, надеюсь, вы узнали ответы на все интересующие вас вопросы. Я же предоставлю слово третьим спикерам, если у них остались аргументы.

Выступают по очереди третьи спикеры обеих команд с оставшимися аргументами.

Председатель: Теперь мы точно услышали все аргументы команд. Настало время четвертым спикерам подвести итоги.

Четвертый спикер делает резюме выступления своей команды и называет те аргументы своих спикеров, которые наиболее ярко подчеркивают преимущество позиции своей команды.

Председатель: Обе наши команды высказались в полном составе. Уважаемые зрители, пришло время определиться и вам, какую сторону вы выберете.

Среди зрителей проводится голосование, в котором все высказываются в пользу выбранной позиции. При голосовании должен оцениваться не тезис, а аргументы, представленные сторонами. За это время команда экспертов выбирает победителя.

Команда экспертов подводит итоги. Выделяет ключевые проблемы обсуждения, сравнивает аргументацию команд, отмечает сильные и слабые места выступлений обеих команд, объективность приведенных аргументов и поддержек. Награждает как отдельных спикеров, так и команду-победительницу.

После выступлений экспертов проводится заключительный этап дебатов – их обсуждение, на котором подводятся итоги, анализируется, насколько успешно осуществили свою деятельность председатель, секретарь, эксперты и зрители. Кроме того, спикеры могут поделиться впечатлениями относительно того, как они сами справились с порученной им ролью.

В качестве домашнего задания студентам предлагается написать эссе с целью закрепить полученную информацию.

Окно в виртуальный мир

Автор: Горбунова Е.А., руководитель: Чернова Е.В.

Аннотация проекта: проект предназначен для учащихся -10х, -11х классов, для ознакомления с наиболее популярными браузерами и их мобильными версиями, и обеспечение безопасности в сети с помощью средств браузера. В ходе работы над проектом, учащиеся научатся выявлять наиболее оптимальный для своих целей браузер, грамотно настраивать браузеры с целью обеспечения максимальной безопасности при работе в сети, устанавливать, удалять и настраивать мобильные браузеры.

Направляющие вопросы

Основополагающий вопрос

Где тут выход?

Проблемные вопросы

1. Какой браузер выбрать?
2. Зачем защищаться от угроз сети?

3. Как правильно настраивать браузеры на смартфонах и телефонах?

Учебные вопросы

1. Какие Вы знаете браузеры?

2. Чем браузеры отличаются друг от друга?

3. Какие типы угроз существуют?

4. Что такое сертификат безопасности?

5. На что нужно ориентироваться при настройке браузера?

6. Можно ли обеспечить полную защиту от угроз сети одними только средствами браузера?

7. Что такое мобильный браузер и где его взять?

8. Чем отличаются настройка браузеров на ПК от настройки браузеров на смартфонах?

План проведения проекта

1 этап. Вводное занятие. Групповая деятельность. Оценка начальных знаний, опыта использования учащимися браузеров на ПК и мобильных устройствах, выявление предпочтений.

2 этап. Игра «Опасность – защита».

3 этап. Распределение учащихся по группам. Распределение проектных заданий. Консультация по проектам. Озвучивание критериев оценивания. Преступление к самостоятельному выполнению проектов.

4 этап. Выполнение учащимися проектных работ. Консультация по проектам.

5 этап. Защита проектных работ. Подведение итогов по проектам.

6 этап. Итоговое занятие. Краткая презентация учителя о том, что не вошло в проекты. Подведение общих итогов. Выдача грамот.

Приблизительная продолжительность проекта 6 академических часов.

Планируемые результаты обучения

После завершения проекта учащиеся приобретут следующие умения:

личностные

- распознание возможных угроз безопасности;
- предупреждать возможные угрозы безопасности;

метапредметные

- сохранять конфиденциальную информацию;
- использовать возможности браузеров для защиты от угроз безопасности;

предметные

- использование специализированного ПО;
- правильно выбирать и настраивать браузеры.

Игра «Опасность-защита»:

Учащиеся делятся на две группы.

1-я группа составляет список опасностей в сети Интернет.

2-я группа называет способы защиты от этих угроз.

План проведения:

1. 1-й группе дается 5 минут, на составление списка опасностей (сколько успеют)

2. 1-я группа озвучивает первую опасность. 2-й группе дается 5 мин на то, чтобы ответить на вопрос: «Какие способы защиты существуют от данной угрозы?».

3. 2-я группа отвечает на вопрос. 1-я группа говорит правилен ли ответ, если нужно дополняет или выдвигает свою версию ответа.

Пункты 1-4 повторяются пока не будут названы все угрозы в сети Интернет или пока не закончится время. Обязательно оставляется время на подведение итогов и озвучивание угроз, которые не назвали учащиеся.

Учитель во время игры направляет игру и говорит правильно или неправильно учащиеся говорят. Помогает правильно сформулировать угрозу и методы защиты от нее.

Интернет – новая категория опасности

Автор Колесников И. В., руководитель: Чернова Е.В.

Описание проекта: Данный проект позволит участникам мероприятия рассмотреть общие вопросы, связанные с безопасностью компьютера и правил поведения в Интернете (доступ к материалам проекта http://wiki.iteach.ru/index.php/ Учебный_проект:_Интернет_–_новая_категория_опасности).

Цель проекта: научится распознавать основные угрозы в Интернете, предупреждать их, с осторожность разглашать личную информацию, определять какая информация является надежной и соблюдать нормы поведения.

План проведения проекта:

1 этап. Вводное занятие. Оценка начальных знаний учащихся. Дискуссия. Распределение заданий. Консультация по практическим работам.(1 урок)

2 этап. Практические работы:(1 урок)

3 этап. Защита практических работ. (1 урок)

4 этап. Распределение заданий. Консультация по итоговой практической работе. Знакомство с программой MS Publisher. (1 урок)

5 этап. Проведение итоговой практической работы. (1 урок)

6 этап. Подведение итогов проекта. Конкурс на самую лучшую листовку. (1 урок)

Основополагающий вопрос

Какие опасности таят в себе просторы Интернета?

Проблемные вопросы

1. Как защитить свой компьютер?

2. Как защитить себя в Интернете?

3. Какие правила поведения существуют в Интернете?

Учебные вопросы

1. Как защитить операционную систему от угроз, исходящих из сети Интернета?

2. Что такое антивирусная программа?

3. Что такое брандмауэр?

4. Что такое резервное копирование файлов?

5. Что понимается под термином надежная информация?

6. Стоит ли разглашать личную информацию в сети Интернет?

7. Надо думать, с кем разговаривать в сети Интернет?

8. Что такое сетевой этикет?

9. Каким образом сетевой этикет может обезопасить нас в Интернете?

Практическая работа № 1: «Фишинг-сайты, Мошенничество в контекстной рекламе»

Цель практической работы: Научится выявлять фишинг-сайты и мошенническую рекламу.

Задачи:

1. Определить вид фишинг-сайтов и мошеннической рекламы;

2. Понять, где можно встретить данный вид угроз;

3. Выработка алгоритма профилактики.

Фишинг – это особый вид компьютерного мошенничества. Фишинг-атаки организуются следующим образом: киберпреступники создают подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через интернет. Затем мошенники пытаются обманным путем добиться, чтобы пользователь посетил фальшивый сайт и ввел на нем свои конфиденциальные данные – например, регистрационное имя, пароль или PIN-код. Используя их, злоумышленники крадут деньги со счетов попавшихся на удочку пользователей.

Мошенническая реклама

К сожалению, не все рекламные объявления создаются с добрыми намерениями. По мере развития Интернета число мошенников тоже растет, а их методы становятся все изощреннее. Вот несколько советов, которые помогут вам обезопасить себя от мошенничества в Интернете.

1. **Если что-то выглядит слишком заманчиво, скорее всего, это обман.**

Игнорируйте интернет-рекламу, которая предлагает неправдоподобно выгодные условия. Объявления, в которых дорогие продукты или услуги (например, новые автомобили или отдых за рубежом) предлагаются очень дешево или вообще бесплатно, скорее всего, созданы не из добрых побуждений.

2. **Не попадайтесь на уловки.**

Объявления, в которых вас поздравляют с тем, что вы стали миллионным посетителем веб-сайта, предлагают призы (например, новый ноутбук или планшетный ПК) за участие в опросе или рекламируют быстрый и несложный способ заработка («как разбогатеть, работая из дома всего два часа в день!»), не принесут вам ничего хорошего.

3. **Опасайтесь мошенников, которые выдают себя за представителей интернет-компаний, банков, социальных сетей и т. п.**

В некоторых объявлениях в Интернете (например слово «Google») и другие товарные знаки незаконно используются для рекламы мошеннических систем «работы на дому» или «быстрых способов разбогатеть». Помните: официальные интернет-компании, банки не предлагает подобных программ.

4. **Если у вас возникли сомнения, лучше перестрахуйтесь.**

Реклама вызывает у вас смутные подозрения? Доверьтесь своей интуиции! Переходите только по объявлениям, которые считаете надежными и которые ведут на легитимные веб-сайты.

Задания:

1. Найти любой сайт, где содержится мошенническая реклама или фишинг. Сделать скриншот.
2. Заполнить таблицу.

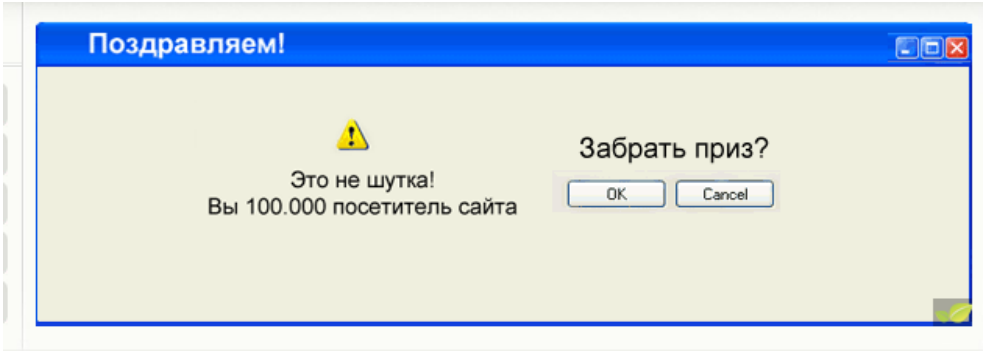
	Название сайта или тип сайта (например, рекламный, файлобменный, игровой)	Ссылка	Скриншот (номер приложения)
1	Игровой (торрент-трэккер)	http://torrent-games.net/	приложение № 1, № 2, №3
2			

Требования к выполнению практической работы №1:

1. Сделать практическую работу на отдельном документе, включающий в себя имя и фамилию участника, номер и название практической работы, таблицу, и раздел со скриншотами.
2. Указать не менее 10 сайтов, где находится мошенническая реклама или фишинг.
3. Результаты практической работы заносить в таблицу.
4. Скриншоты указывать в конце практической работы в разделе Приложения.

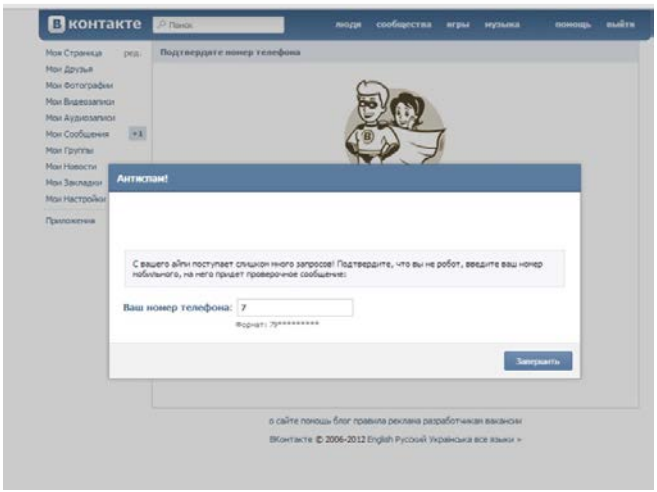
Приложения

Приложение № 1



Приложение № 2

Приложение № 3



Практическая работа № 2: «Социальные сети»

Цель: Выработать комплекс мер по обеспечению безопасности себя в социальных сетях.

Задачи:

1. Научится контролировать доступ к своей личной информации в социальных сетях;

2. Понять, что за любое свое действие в социальных сервисах несем ответственность.

Ход работы:

I. Анализ ситуаций, за которые можно понести реальную ответственность.

Ситуация №1. За «неадекватный комментарий» увольнение

«…9 мая после сообщений об авиакатастрофе SSJ-100 пользователь Твиттера 4katrin (Kate Solovyeva) написала: "*А че суперджет рухнул?! Хахаха! Говномашина! Жаль не в Аэрофлоте, на один бы стало меньше, а может и вовсе продали их обратно кому-нибудь*". Твит вызвал возмущение других пользователей сервиса микроблогов. По страницам в социальных сетях Facebook и "Вконтакте", которые были привязаны к аккаунту 4katrin, удалось установить, что автор сообщения является стюардессой "Аэрофлота" Екатериной Соловьевой.

Возмущенные пользователи Твиттера сделали скриншот сообщения Соловьевой и обратились с жалобами в "Аэрофлот". Девушка сначала удалила комментарий, а потом все свои аккаунты в социальных сетях. 10 мая "Аэрофлот" в своем твиттер-аккаунте опубликовал приказ о расторжении трудового договора с Соловьевой по соглашению сторон. Приказ вступает в силу 11 мая… »

Источник: http://lenta.ru/news/2012/05/10/flightattendant/

Ваше мнение:

1) В чем ошибка пользователя?
2) Как избежать подобной ситуации?
3) Оставляете ли вы подобные комментарии?
4) Есть ли среди ваших «друзей», кто пользуется Твиттером, подобными блогами? Замечали комментарии подобного характера?

Ситуация №2. За размещенный видеоролик статья

«…в январе 2012 г. молодой человек, используя персональный компьютер, разместил в социальной сети «В Контакте» *видеоролики*, содержащие информацию, направленную *на разжигание национальной и религиозной ненависти и вражды*.

В данных видеозаписях, имеющих ярко выраженный агитационный характер, пропагандировалась необходимость применения насилия в отношении лиц, не исповедующих его религию… »

Источник: http://prokhmao.ru/news/36685/

Ваше мнение:

1) В чем ошибка пользователя?
2) Как избежать подобной ситуации?
3) Наблюдали ли вы подобные видеоролики, материалы подобного характера среди ваших «друзей» «В Контакте»?

Ситуация №3. Оскорбление в социальной сети

«… в феврале 2009 года Казанцева не самым лестным образом отозвалась о внешности обладателя аккаунта и ее семейном положении. Пострадавшая обратилась в местное отделение милиции с просьбой привлечь обидчицу к уголовной ответственности, что и было сделано.

«..Суд классифицировал Социальную сеть “Одноклассники” как *Средство массовой информации*, поэтому речь шла уже о нанесении оскорбления через СМИ…»

Источник: http://www.kommersant.ru/doc/1204655

Ваше мнение:

1) В чем ошибка пользователя?
2) Как избежать подобной ситуации?
3) Используете ли вы подобные комментарии в социальных сетях?
4) Бывали ли вы жертвами подобных комментариев? Как часто?

Ситуация №4. Скандал из-за откровенного фото и видео учительницы

Ученики одной из школ Екатеринбурга обнаружили откровенные фотографии учительницы английского языка, которые та выложила на свою страничку в социальной сети. Страничка не была закрыта от посторонних глаз, поэтому снимки педагога быстро расходились среди школьников, пока их не увидел кто-то из родителей.

Родителей не устроило такое положение вещей, что вызвало скандал.

Источник: http://www.nr2.ru/ekb/373701.html

Ваше мнение:

1) В чем ошибка пользователя?
2) Как избежать подобной ситуации?
3) Размещаете ли вы подобные материалы или материалы, которые надо скрывать, в социальных сетях?
4) Вы используете возможности социальной сети, чтобы скрыть подобные материалы?
5) Является ли ваш способ безопасным?

II. Анализ информации на странице выбранных друзей в социальной сети «В Контакте».

Задания:

1. Взять любых 2-3 друзей или знакомых в социальной сети «В Контакте» и проанализировать их страницу и заполнить таблицу.

Основные разделы личной информации	Друг № 1	Друг № 2
Имя Фамилия, дата рождения, место рождения		
Контактная информация (номер телефона, эл. почта, скайп и т.п.)		
Родственники, лучшие друзья		
Место учебы, работы		
Любимый жанр музыки, любимая группа		
Проанализировать видеозаписи (чем интересуется пользователь, ролики имеют развлекательный характер, имеются провокационные ролики, призывающие к агрессии, ненависти, демонстрирующие непотребные вещи и т.п.)		
Имеются ли личные фотографии, которые не стоит размещать?(да/нет)		
Имеются ли ссылки на другие социальные ресурсы (instagram, вопросники spring.me (formspring), ask.fm и т.п.)		
Места посещения, постоянного пребывания (анализ данного раздела сделать на основе фотографий, стены ответов в вопроснике и других источников)		
Анализ оперируемых терминов (наличие нецензурной брани, агрессии в словах, использование научных терминов, речь имеет нейтральный характер и т. п.)		

2. Удалиться из выбранных друзей (заранее предупредите, что удаляетесь, чтоб не возникло недопонимание). Проанализируйте их страницы аналогично и заполните таблицу.

Основные разделы личной информации	Друг № 1 (после удаления)	Друг № 2 (после удаления)
Имя Фамилия, дата рождения, место рождения		
Контактная информация(номер телефона, эл. почта, скайп и т.п.)		
Родственники, лучшие друзья		
Место учебы, работы		
Любимый жанр музыки, любимая группа		
Проанализировать видеозаписи (чем интересуется пользователь, ролики имеют развлекательный характер, имеются провокационные ролики, призывающие к агрессии, ненависти, демонстрирующие непотребные вещи и т.п.)		
Имеются ли личные фотографии, которые не стоит размещать?(да/нет)		
Имеются ли ссылки на другие социальные ресурсы (instagram, вопросники spring.me(formspring), ask.fm и т.п.)		
Места посещения, постоянного пребывания (анализ данного раздела сделать на основе фотографий, стены, ответов в вопроснике и других источников)		
Анализ оперируемых терминов (наличие нецензурной брани, агрессии в словах, использование научных терминов, речь имеет нейтральный характер и т. п.)		

3. Сделать выводы (имеется ли информация, которая относится к личной или которую не стоит выкладывать в общий доступ, имеются ли угрозы связанные с разглашением личной информации). Подумайте как злоумышленник может использовать информацию, которая размещена у выбранных Вами друзей на странице «ВК».

Требования к выполнению практической работы №2:

1. Заполнять все столбцы таблицы обязательно.
2. Вывод о проделанной работе предоставить в печатной форме после заполнения таблицы.

Итоговая практическая работа: «Безопасность в Интернете в наших руках»

Цель: Закрепить знания по основам безопасности в Интернете.

Задачи:

1. Познакомится с программным средством MS Publisher.
2. Вспомнить, отыскать информацию по данной теме.

Задание.

Средствами MS Publisher сделать листовку на одну из 2 тем:

1. Как защитить себя в Интернете?
2. Какие правила поведения существуют в Интернете?

Требования к выполнению:

1. Содержание листовок должно соответствовать теме.
2. Листовка должна содержать заголовок.
3. Листовка должна содержать лаконичные рекомендации или инструкции.
4. Используемые фотографии и рисунки должны соответствовать теме.
5. Орфография.

Критерии оценивания

Работа в проекте

оценка	критерии
5	Участник активно принимал участие, ответы обоснованы, аргументированы и логически выстроены.
4	Участник менее активно принимал участие, ответы местами обоснованы, приведенные аргументы не дают полноты ясности картины на поставленный вопрос
3	Участник вяло принимал участие, ответы носят случайный характер, без доказательной базы.
2	Участник вообще не принимал участия или отвечал очень редко.

Практические работы.

оценка	критерии
5	Выполненные практические работы соответствуют всем требованиям или хотя бы почти всем.
4	В выполненных практических работах есть ряд недочетов в нескольких требованиях.
3	Выполненные практические работы посредственны, т.е. не выполнены меньше половины требований.
2	Выполненные практические работы сделаны на половину и меньше.

Итоговая практическая работа

оценка	критерии
5	Выполненная практическая работа соответствует всем 5 требованиям
4	Выполненная практическая работа соответствует 4 требованиям
3	Выполненная практическая работа соответствует 3 требованиям
2	Практическая работа не выполнена или соответствует 2 и меньше требованиям.

Защита от нежелательной информации в Интернет

Автор: Исрафилов Р.Р., руководитель: Лапшина В.Б.

Цели проекта:

1. Развитие навыков работы с компьютерной техникой;
2. Закрепление умений и навыков работы в текстовом редакторе Microsoft Word;
3. Обучение работе в программе для создания буклетов Publisher;
4. Обучение работе с информацией: целенаправленному поиску, методам поиска и отбора информации; знакомство с систематизацией, различными способами обработки информации;
5. Развитие познавательного интереса, творческой активности, умения излагать мысли;
6. Повторение и закрепление основного программного материала;
7. Развитие умения работать с дополнительной литературой, правильно выбирать источники информации;
8. Развитие логического мышления, памяти, внимания;
9. Совершенствование мыслительных приемов анализа и синтеза;
10. Воспитание негативного отношения к нежелательному контенту;
11. Воспитание самостоятельности и ответственности, упорства в достижении цели.

Для проведения проекта предполагается внедрение метода проектов в процесс обучения информатике на примере преподавания темы «Способы защиты от нежелательной информации в Интернет».

Данный проект реализуется в факультативной форме в рамках школьной программы.

Изучение материала рекомендуется изучать в течении 8 уроков:

1. Введение в тему (45 мин).
2. Организация групповой работы, распределение тем исследований (45 мин).
3. Самостоятельная работа.
4. Консультации и доработка материала учащимися (5 уроков – 225 мин).
5. Представление результатов (45 мин).

Контроль усвоения материала проводится на последнем уроке в виде открытого урока: ученики представляют творческие проекты (презентации, публикации, кроссворды, видеоролики, альбомы с фотографиями, буклеты), а также проводится обсуждение.

Целевая аудитория: учителя и учащиеся 10 – 11 классов, родители учащихся.

Программное обеспечение:

- текстовый редактор Microsoft Word;
- программа для создания буклетов MS Publisher;
- программа для созданий презентаций MS Power Point.

Тип проекта:

1. По предметно-содержательной области – межпредметный;
2. По характеру координации – с явной координацией;
3. По характеру контактов – внешний;
4. По количеству участников – индивидуальный или групповой;
5. По продолжительности выполнения – долгосрочный.

Тематический охват проекта: для реализации проекта учащимся необходимо изучить следующие разделы курса информатики:

6. «Аппаратные и программные средства ЭВМ»;
7. «Средства работы с текстовыми документами. Текстовый редактор Microsoft Word»;
8. «Основы компьютерных телекоммуникаций. Программа Internet Explorer»;
9. «Язык разметки гипертекста HTML. Автоматизация разработки веб-документов. Программа для создания публикаций MS Publisher».
10. «Программа для создания презентаций MS Power Point»

Предметы, с которыми связан данный проект:

1. Информатика;
2. Информационные технологии.

Техническое обеспечение, необходимое для успешного осуществления работы: компьютеры, подключенные к Интернету.

Рекомендации для учителя

В данном разделе представлены рекомендации для учителя информатики, который решит применять метод проектов в своей работе:

1. Возраст учащихся – некорректно предлагать учащимся задания, которые они не могут выполнить или которые им неинтересны в силу его возраста.

2. Время – чтобы у ученика не пропал интерес к выполняемой работе, нельзя затягивать время выполнения проекта. Максимальное время от получения задания до представления результата не должно составлять более двух недель.

3. Актуальность тем проектов – темы проектов должны быть актуальны для современных школьников.

4. Самостоятельность – нельзя устанавливать строгий контроль над работой детей. Проект – это возможность ребенка самоутвердиться, выразить себя и свои идеи и мировоззрение, поэтому важно не мешать ему в этом.

5. Увлеченность заданием – необходимо включить в процесс обучения различные игры, занимательные задания, шутки и т.д., так как школьники усваивают больше материала и выдают лучшие результаты тогда, когда они получают удовольствие от обучения.

6. Вариативность – метод проектов предполагает групповую, парную и индивидуальную формы работы. Желательно использовать различные типы упражнений и различные темы.

Список проблемных вопросов, согласно которым учащиеся проводят свои исследования:

1. Анализ существующих методов защиты от нежелательной информации?

2. Технология защиты от нежелательной информации (спам).

3. «Спам – не спам?»

План работы над проектом:

- Информационный этап: рассказ ученикам о создании проектов, опыте других учащихся в этой области, описание эмоций и ощущений при работе над проектом, пробуждение у школьников желания сделать что-нибудь подобное;

- Определение темы проекта: учитель и ученики обсуждают название проекта, его содержание и форму представления результатов. На этом этапе педагог не мешает детям выбирать тематику проекта, а только помогает разрешить возникшие трудности при обсуждении, и дает советы;

- Формулировка задач, функций каждого ученика, распределение этапов работы: учитывается желание каждого ученика при работе над проектом;

• Подготовка проекта: проект дети готовят самостоятельно. Учителю нужно знать, как продвигается работа по созданию проекта, но без строго контроля над деятельностью детей, так как проект – один из лучших способов выработать у детей самостоятельность и умение работать в коллективе;

• Коррекция: учитель советует детям, что нужно сделать, какие дополнения внести, чтобы проект стал интересным, исправляет ошибки;

• Презентация проектов: представление проектов проходит в праздничной атмосфере. Класс украшается в соответствии с тематикой проектов, возможно использование костюмов или элементов костюмов;

• Анализ представленных проектов: спрашивается мнение каждого ребенка о проекте, что понравилось, какие изменения необходимо внести, чтобы следующий проект стал более удачным. Заключительное слово предоставляется учителю. Важно найти теплые слова благодарности всем детям за выполненную работу.

Вкусивши яд компьютерных игр…

Автор Пензина Н., руководитель: Чернова Е.В.

Описание проекта: В современном информационном обществе подрастающее поколение развивается очень быстро. Ребенок начинает осваивать окружающий мир, предметы, новые технологии, в том числе и компьютер, а с ним и компьютерные игры. Поэтому очень актуальным является вопрос о влиянии компьютерных игр на детей. Исходя из актуальности вопроса, была выбрана тема проекта: «Вкусивши яд компьютерных игр…», сформулирован основополагающий вопрос: «Как зажечь луч света в темном царстве компьютерных игр?». Проект рассчитан на 4 академических часа в классе (180 минут) и 6 часов (240 минут) самостоятельной работы. Проводиться он может как среди учащихся среднего, так и старшего звена. Деятельность учащихся будет оцениваться посредствам тестов, анализа итоговых творческих заданий. Предполагается проведение оценивания, как самим учителем, так и другими учащимися и самим учеником.

Дидактические цели проекта:

• Развитие детей с помощью специальных компьютерных игр.

• Формирование осведомленности учащихся о пользе и вреде компьютерных игр.

• Овладение умениями представления результатов исследования с использованием современных информационных технологий (презентация, публикация, сайт).

Методические задачи проекта:

Учащиеся должны

Знать:

• Негативные последствия воздействия компьютерных игр на психическое и физическое здоровье;

• развивающие возможности компьютерных игр;

• классификацию компьютерных игр.

Уметь:

• Определить какие компьютерные игры являются «полезными» и «вредными»;

• соблюдать требования информационной безопасности, информационной этики и права;

• осознавать последствия зависимости от компьютерных игр;

• сравнивать, анализировать и систематизировать имеющийся учебный материал.

Иметь навыки:

• Представлять результаты учебных исследовательских проектов с использованием ИКТ.

Определены проблемные вопросы учебной темы:

• Сколько времени и во что мы играем?

• Чем полезны компьютерные игры?

• Какой вред могут нанести компьютерные игры?

• Как оградить ребенка от компьютерно-игровой зависимости?

• По каким признакам можно классифицировать компьютерные игры на вредные и полезные?

Далее проводится соответствие выбранной темы и тематического учебного плана школьного предмета Информатика и ИКТ:

• Информация и информационные процессы. Защита информации.

• Информационная деятельность человека.

• Информационные ресурсы и сервисы компьютерных сетей.

• Компьютеризация и информатизация.

• Информационный потенциал общества.

Для более детального рассмотрения темы и вопросов проекта учащимся предлагаются примерные **темы самостоятельных исследований:**

• Разновидности компьютерных игр.

• Развитие ребенка с помощью компьютерных игр.

• Выявить признаки отрицательного и положительного воздействия компьютерных игр на детей.

• Проанализировать время, проводимое учащимися за компьютерными играми, выявить их предпочтения в жанрах компьютерных игр.

Блоги и форумы: Веб-дворцы интернет-ораторов

Автор Черевичный В.В., руководитель: Чернова Е.В.

Аннотация: проект предоставлен для ознакомления с такими Веб-инструментами, как блоги и форумы. В ходе работы над проектом, дети обучаются основам ведения блога, его продвижения, способности отличать «фейк»-блог от настоящего, а также учатся нормам поведения при общении с модераторами блогосфер и форумов, авторами других блогов, читателями и подписчиками блогов, и основам использования инструментов для упрощения коммуникации с ними.

Цель проекта: показать учащимся перспективы, открываемые за счет блогов, обучить их правилам ведения блога, нормам общения с читателями блога и форума, а также научить отличать фейк-блоги.

Задачи проекта:

1. Расширить знания учащихся о блогах и форумах.
2. Научить создавать и пользоваться собственными блогами.

План проведения проекта

1 Этап: Проведение вводного занятия. Проверка и выявления знаний у учащихся о блогах и форумах при помощи опроса. Опрос

2 Этап: Ознакомительный семинар по блогам.

3 Этап: Семинар по вопросам и первое практическое задание.Знакомство с блог-платформой LiveJournal. Регистрация собственного блога, публикация первого сообщения-поста и сообщения-комментария (можно в своем же блоге).

4 Этап: Углубленное знакомство с инструментарием LiveJournal. Практическое задание по оформлению и поддержке своего блога.

5 Этап: Лекция по этике в блогосфере.

6 Этап: Результирующее занятие. Оценка полученных знаний о блогах, проверка способностей через итоговое практическое задание.

Вопросы, направляющие проект:

Основополагающий вопрос

Как поделиться интересной историей в современном мире?

Проблемные вопросы

Что такое блог и форум?

Что следует знать о блогах и форумах, а также о правилах их ведения?

Учебные вопросы

Как вести блог?

Какая польза от ведения блога?

Как следует себя вести при общении с читателями блога?

Что такое фэйк-блог?

Общение на форуме - в чем различие от социальных сетей?

Проведение мероприятий.

1 Этап. Вводное занятие. Опрос.

Данный опрос позволит определить имеются ли у учащихся знания о блогах и форумах, желание завести свой блог, или уже наличие собственного блога, а также позволит определить каким вещам и деталям следует отдать больше времени на изучение.

Вопрос:	Ответ:	Вы бы хотели узнать об этом больше?
1) Вы бы хотели рассказать миру о своих впечатлениях?		
2) Вы знаете что такое блог?		
3) Являетесь ли вы читателем какого-либо блога?		
4) А у вас есть собственный блог?		
5) Вы решились завести свой блог. Сможете постоянно пополнять его?		
6) Как вы считаете, можно ли получить прибыль за ведение блога?		
7) Вы знакомы с какими-либо опасностями, имея дела с блогами?		
8) Вы знакомы с таким веб-приложением как форум?		
9) Для чего нужны форумы и их отличие от соц. сетей?		

2 Этап. Теоретический урок

«Знакомство с блогами»

Ребята, на данном уроке мы познакомимся с блогами.

Рассказываем теорию, по желанию ученики могут записывать основные моменты.

Слово «Блог» многим людям в современном мире может оказаться неизвестным. Для простоты в понимании, блоги – это интернет-дневники.

Блоги бывают 5 различных типов:

1) Личные блоги;

2) Профессиональные блоги;

3) Бренд блоги;

4) Новостные блоги;

5) Нетрадиционные блоги;

Личный блог – это все тот же старый добрый дневник, где мы можем изливать душу, писать о своих мыслях, делиться впечатлениями, и рассказывать о чем-либо интересном. Единственное различие с бумажным дневником разумеется то, что блог – дневник электронный. Профессиональный блог представляет собой дневник человека, занимающегося

какой-либо профессиональной деятельностью. Со временем при наборе блогом оборотов, владелец дневника может получать прибыль с него.

Бренд блог создается с целью продвижения бренда какого-либо человека или компании.

Новостные блоги часто ведутся несколькими авторами. Они выбирают какую-то одну тему, например, «все про Apple», и пишут в день по несколько заметок в блог. В основном, различные новости, касающиеся Apple.

Остальные виды блогов. Некоторые блоги создаются на бесплатных блогохостингах типа ЖЖ. Но все-таки абсолютное большинство блогов создается на бесплатном движке WordPress.

3 Этап. Примерные темы для ознакомления с блогами и форумами, а также особенности работы с ними.

1. Правила и особенности ведения блога.
2. Какую блог-платформу выбрать?
3. Как оформить свой блог.
4. Как продвигать свой блог.
5. Как комментировать записи чужих людей?
6. Фальсификация, или что такое фэйк-блог.
7. Форумы, что это?
8. Если на форуме общаются, то это социальная сеть?

4 Этап. Практическое задание по оформлению и поддержке своего блога.

5 Этап. Лекция по этике в блогосфере.

6 этап. Итоговое занятие

Ребята, вашим заданием будет размещение на своем блоге мини-сочинения о каком-либо интересном случае в вашей жизни или о воспоминании, о котором вы бы хотели рассказать друзьям. Оформление текста приветствуется. По окончанию работы я оценю ваше сочинение, оставив соответствующий комментарий исходя из того, насколько успешно вы справились с заданием. В конце не забудьте ответить на комментарий небольшим предложением о вашем впечатлении о блогах.

За данную работу вы получите оценки.

По результатам работы можно будет определить то, насколько хорошо ученик приспособился к ведению блога, к особенностям ведения, оформления своего «журнала», смог ли он разобраться в том, как находить интересующие его записи других людей, как их комментировать, и как отслеживать комментарии в своем блоге.

Результатом занятия должна быть запись в вашем блоге на LiveJournal, содержанием которого должно являться мини сочинение. Дополнительные баллы ставятся за оформление текста и ответ на комментарий учителя.

Антивирусная защита: Если вирус не один,

всё равно он победим

Автор Федотов В.В., руководитель: Чернова Е.В.

Аннотация: Проект предназначен для учащихся 10-11 классов. На старте проекта рассматриваем общее вредоносное ПО, виды вирусов, уровни опасности. Рассматриваем антивирусное ПО на ПК, смартфонах и телефонах.

Цель проекта: научить учащихся работать с антивирусным ПО на ПК, смартфонах и мобильных телефонов.

Задачи проекта:

1. Научить использовать антивирусную защиту на компьютерах, телефонах и смартфонах.

2. Расширить знания учащихся об информационной защите, о видах вирусов, о существующих законах, о защите информации.

Направляющие вопросы

Основополагающий вопрос

Как броня влияет на защиту?

Проблемные вопросы

1. Каким образом использовать антивирусную защиту на смартфонах и телефонах?

2. Почему мы защищаем свое ПО?

3. На какие виды делятся антивирусы

4. Какой антивирус поставить: платный или бесплатный?

Учебные вопросы

1. Что такое вредоносное ПО?

2. Что такое сигнатура?

3. Какие типы угроз существуют?

4. Как часто обновлять сигнатуры?

5. Для чего нужно обновлять ПО?

6. Какие признаки заражения вирусом на ПК?

7. Какие признаки заражения, смартфонов и телефонов, вредоносным ПО?

8. Чем отличаются вирусы на ПК от вирусов на смартфоны?

9. Какие существуют антивирусы?

10. Что такое «Фаги»?

План проведения проекта.

План проведения проекта

1 этап. Вводное занятие. Оценка начальных знаний учащихся (тест). Выдача домашнего задания – сделать презентацию по теме: "Как броня влияет на защиту".

2 этап. Практическая работа.

3 этап. Подведение итогов домашней работы и практической работы.

4 этап. Творческое занятие: представить свое видение процесса заражения вредоносными программами (в классе). Подведение итогов творческого занятия.

5 этап. Проведение итоговой практической работы.

6 этап. Заключительное занятие. Обсуждение результатов итоговой практической работы на основе схемы (пример схемы). Подведение итогов.

Проведение мероприятия.

1 этап.

Тест: «Вирусы и антивирусные программы»

1. Что такое компьютерный вирус?

1) Прикладная программа.

2) Системная программа.

3) Программа, выполняющая на компьютере несанкционированные действия.

4) База данных.

2. Основные типы компьютерных вирусов:

1) Аппаратные, программные, загрузочные .

2) Программные, загрузочные, макровирусы.

3) Файловые, программные, макровирусы.

3. Этапы действия программного вируса:

1) Размножение, вирусная атака.

2) Запись в файл, размножение.

3) Запись в файл, размножение, уничтожение программы.

4. В чем заключается размножение программного вируса?

1) Программа-вирус один раз копируется в теле другой программы.

2) Вирусный код неоднократно копируется в теле другой программы.

5. Что называется вирусной атакой?

1) Неоднократное копирование кода вируса в код программы.

2) Отключение компьютера в результате попадания вируса.

3) Нарушение работы программы, уничтожение данных, форматирование жесткого диска.

6. Какие существуют методы реализации антивирусной защиты?

1) Аппаратные и программные.

2) Программные, аппаратные и организационные.

3) Только программные.

7. Какие существуют основные средства защиты?

1) Резервное копирование наиболее ценных данных.

2) Аппаратные средства.

3) Программные средства.

8. Какие существуют вспомогательные средства защиты?

1) Аппаратные средства.

2) Программные средства.

3) Аппаратные средства и антивирусные программы.

9. На чем основано действие антивирусной программы?

1) На ожидании начала вирусной атаки.

2) На сравнении программных кодов с известными вирусами.

3) На удалении зараженных файлов.

10. Какие программы относятся к антивирусным

1) AVP, DrWeb, Norton AntiVirus.

2) MS-DOS, MS Word, AVP.

3) MS Word, MS Excel, Norton Commander.

Критерии оценки теста:

9-10 правильных ответов – “5”

7-8 правильных ответов – “4”

5-6 правильных ответов – “3”

меньше 5 – “2”

2 этап. Практическая работа.

Практическая работа№1

Антивирусная программа AntiViral Toolkit Pro

Цель практического занятия: «Научиться использовать антивирусные программы для проверки носителей на наличие вирусов и лечения, изучить состав компонентов защиты на ПК, смартфонах и телефонах».

Задачи:

1. Обновить антивирусные базы

2. Познакомиться с возможностями программы

3. Проверить ПК, смартфоны и телефоны на наличие вирусов.

Ход работы:

1. Организационный момент:

1.1 проверка явки учащихся и их готовности к занятию;

1.2 определения направленности практической работы:

Сегодня мы проводим практическую работу по антивирусной программе AntiViral Toolkit Pro, которая установлена на вашем рабочем компьютере. Прошу занять свои «боевые корабли».

2. Основная часть:

2.1 определение последовательности в запуске и обнаружении вредоносного ПО на проверяемых объектах:

- Запустить программу (ярлык на Рабочем столе);
- Дождаться загрузки базы, отменить обновление базы;
- Ознакомиться с вкладками окна программы: Область, Объекты, Действия, Настройки;
- Установить Область сканирования – диск D:, Объекты – программы по расширению, Действия – запрос на лечение, Настройки - файл отчета;
- Запустить сканирование;
- После окончания сканирования проанализировать результаты (вкладка Статистика).

2.2 законспектировать этапы по обнаружению вредоносного ПО.

3. Заключительная часть:

3.1 по данным вкладки Статистика в дискуссионной форме учащиеся делают выводы о проделанной работе, аргументируя свои доводы;

3.2 по результатам пункта 3.1 преподаватель оценивает проделанную работу;

3.3 выдача вопросов на самоподготовку:

Что такое компьютерный вирус?

Основные типы компьютерных вирусов.

Действие программного вируса (этапы).

Методы защиты.

Средства антивирусной защиты.

Примеры антивирусных программ.

Практическая работа№2

Антивирусная программа **Dr. Web/Kaspersky Mobile Security Lite**

Цель практического занятия: «Научиться использовать антивирусные программы для проверки носителей на наличие вирусов и лечения, изучить состав компонентов защиты на смартфонах и телефонах».

Задачи:

1. Обновить антивирусные базы
2. Познакомиться с возможностями программы
3. Проверить смартфоны и телефоны на наличие вирусов.

Ход работы:

1. Организационный момент:

1.1 проверка явки учащихся и их готовности к занятию;

1.2 определения направленности практической работы:

Сегодня мы проводим практическую работу по антивирусной программе Dr. Web/Kaspersky Mobile Security Lite, которая установлена на вашем «мобильном» устройстве.

2. Основная часть:

2.1 определение последовательности в запуске и обнаружении вредоносного ПО на проверяемых объектах:

- Запустить программу на Andoid.
- Дождаться загрузки базы, отменить обновление базы.
- Ознакомиться с вкладками окна программы: Область, Объекты, Действия, Настройки.
- Установить Область сканирования – диск D:, Объекты – программы по расширению, Действия – запрос на лечение, Настройки - файл отчета.
- Запустить сканирование.
- После окончания сканирования проанализировать результаты (вкладка Статистика).

2.2 законспектировать этапы по обнаружению вредоносного ПО.

3. Заключительная часть:

3.1 по данным вкладки Статистика в дискуссионной форме учащиеся делают выводы о проделанной работе, аргументируя свои доводы;

3.2 по результатам пункта 3.1 преподаватель оценивает проделанную работу;

3.3 выдача вопросов на самоподготовку:

Что такое вирус?

Действие программного вируса (этапы).

Методы защиты на смартфонах и телефонах.

Средства антивирусной защиты.

Примеры антивирусных программ для телефонов.

Практическая работа№3

Антивирусная утилита Dr. Web Curelt.

Цель практического занятия: «Научиться использовать антивирусную утилиту для выявления вредоносного ПО и уничтожения вируса на ПК».

Задачи:

1. Обновить антивирусные базы
2. Познакомиться с возможностями программы
3. Проверить ПК на наличие вирусов.

Ход работы:

1. Организационный момент:

1.1 проверка явки учащихся и их готовности к занятию;

1.2 определения направленности практической работы:

Сегодня мы проводим практическую работу по антивирусной утилите Dr. Web Curelt, которая установлена на вашем рабочем компьютере.

2. Основная часть:

2.1 определение последовательности в запуске и обнаружении вредоносного ПО на проверяемых объектах:

- Запустить утилиту на Windows XP-7.
- Дождаться загрузки базы, отменить обновление базы.
- Ознакомиться с вкладками окна программы: Область, Объекты, Действия, Настройки.
- Установить Область сканирования – диск D:, Объекты – программы по расширению, Действия – запрос на лечение, Настройки - файл отчета.
- Запустить сканирование.
- После окончания сканирования проанализировать результаты (вкладка Статистика).

2.2 законспектировать этапы по обнаружению вредоносного ПО.

3. Заключительная часть:

3.1 по данным вкладки Статистика в дискуссионной форме учащиеся делают выводы о проделанной работе, аргументируя свои доводы;

3.2 по результатам пункта 3.1 преподаватель оценивает проделанную работу;

3.3 выдача вопросов на самоподготовку:

Что такое антивирусная утилита?

Как запустить Dr. Web Curelt в безопасном режиме?

Средства антивирусной защиты.

Примеры антивирусных программ ПК.

Практическая работа№4

Антивирусная защита Avira(Free Antivirus).

Цель практического занятия: «Научиться использовать антивирусные программы для проверки носителей на наличие вирусов и лечения, изучить состав компонентов защиты на ПК».

Задачи:

1. Обновить антивирусные базы
2. Познакомиться с возможностями программы
3. Проверить ПК на наличие вирусов.

Ход работы:

1. Организационный момент:

1.1 проверка явки учащихся и их готовности к занятию;

1.2 определения направленности практической работы:

Сегодня мы проводим практическую работу по антивирусной защите Avira(Free Antivirus), которая установлена на вашем рабочем компьютере.

2. Основная часть:

2.1 определение последовательности в запуске и обнаружении вредоносного ПО на проверяемых объектах:

- Запустить утилиту на Windows XP-7.
- Дождаться загрузки базы, отменить обновление базы.
- Ознакомиться с вкладками окна программы: Область, Объекты, Действия, Настройки.
- Установить Область сканирования – диск D:, Объекты – программы по расширению, Действия – запрос на лечение, Настройки - файл отчета.
- Запустить сканирование.
- После окончания сканирования проанализировать результаты (вкладка Статистика).

2.2 законспектировать этапы по обнаружению вредоносного ПО.

3. Заключительная часть:

3.1 по данным вкладки Статистика в дискуссионной форме учащиеся делают выводы о проделанной работе, аргументируя свои доводы;

3.2 по результатам пункта 3.1 преподаватель оценивает проделанную работу;

3.3 выдача вопросов на самоподготовку:

– Что такое антивирусная защита?
– Методы защиты.
– Средства антивирусной защиты.
– Примеры антивирусных программ.

3 этап. Подведение итогов домашней работы и практической работы.

4 этап. Творческое занятие: представить свое видение процесса заражения вредоносными программами (в классе). Подведение итогов творческого занятия.

5 этап. Проведение итоговой практической работы.

6 этап. Заключительное занятие. Обсуждение результатов итоговой практической работы на основе схемы (пример схемы 1).

Век живи – век учись!

Автор Литвин Е.В., руководитель: Чернова Е.В.

Краткое содержание проекта: данный проект «Обучение в Интернет» проводится в рамках дисциплины «Информатика и ИКТ» для школьников 10-11 класса, а также для студентов 1-ого курса по предметам, связанных с информационными технологиями. Основными направлениями этого проекта являются самообразование и повышение квалификации.

Цель проекта заключается в раскрытии возможности Интернета как образовательной среды.

Задачи проекта:

1. Формировать ответственного отношения к учению, готовности и способности, обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;

2. Уметь самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;

3. Уметь использовать термины «информация», «сообщение», «данные», «кодирование», «алгоритм», «программа»; понимание различий между употреблением этих терминов в обыденной речи и в информатике;

Планируемые результаты обучения:

После завершения проекта учащиеся приобретут следующие умения:

– личностные: способность к саморазвитию и самообучению;

– метапредметные: умение самостоятельно подбирать для себя необходимую информацию,

– предметные: владение данными об образовательных стандартах, сайтах и порталах, возможности получить дополнительное образование, и повысить квалификацию.

План проведения проекта:

1 этап (1 урок): Вводное занятие. Видеоролик Мир Интернета. Групповая работа.

2 этап (продолжение вводного занятия): Теоретическое занятие. Презентация Интернет-ресурсы

3 этап (1 урок): Результирующий урок. Итоговая работа «Доклад + фотоконкурс».

Вопросы, направляющие проект

Основополагающий вопрос

К чему стремиться?

Проблемные вопросы

1. Что такое самообразование?
2. Что такое повышение квалификации?

Учебные вопросы

1. Какие существуют образовательные сайты и порталы?
2. Что такое электронные библиотеки?
3. Что такое видеоуроки?
4. Как можно получить дополнительное образование?
5. Какие существуют сайты для повышения квалификации?

Практическое занятие на тему «Век живи - век учись». 1 урок.

Вводное занятие: групповая работа.

Групповая работа проводится на вводном занятии, с целью определения уровня знаний учеников в данной теме, а так же для того чтобы ученики поняли о чем мы будем говорить в данном проекте.

Ученикам предлагается разделиться на небольшие группы по 3 человека. В течение 10 минут каждая группа обдумывает и составляет список Интернет-ресурсов, которыми они реально пользуются при подготовке домашнего задания, самостоятельного изучения материала, в общем, для обучения. В результате группы выступают со своими ответами, и решают вместе с остальными, какой Интернет-ресурс лучше всего помогает в обучении.

После небольшой дискуссии учитель собирает эти списки и ставит на них пометки, кто и как отвечал.

Задание предлагается в небольших группах, для того чтобы создать спокойную рабочую атмосферу, чтобы не запугать учеников на первом же занятии проведением каких-то самостоятельных работ**.**

Видеоролик:

https://www.youtube.com/watch?v=9dSzVjZJJ0U&feature=youtu.be

2 урок. Теоретическое занятие. Презентация

3 урок. Результирующий урок. Результирующий урок. Итоговая работа «Доклад + Фотоконкурс».

Цель проведения: Закрепить усвоение материала по данной теме.

Формат работы: Ученики разбиваются на 3 группы. Каждой группе дается две темы, по которым они готовят доклад и фотографию для фотоконкурса. Работа выполняется в течение 2 дней. В результате, на итоговом занятии каждая группа представляет свой доклад в виде презентации (5-8 мин) и одну фотографию. Если у слушателей возникают какие-либо вопросы или комментарии, выступающие отвечают на них (3-4 мин).

Задание к докладу: Подготовить информацию по своей теме, а именно какие есть информационные, обучающие сайты; какие курсы в Интернете можно пройти, какие платно какие бесплатно.

Темы для докладов:

1. Графика и дизайн.
2. Искусство, музыка и танцы.
3. Компьютер и интернет.
4. История. Бизнес.
5. Иностранные языки.
6. Спорт.

Задание к фотоконкурсу: Подготовить фотографию на определенную тему. Фотография должна быть занимательной и содержательной.

Предполагаемый результат: При подготовке докладов ученики узнают много новых Интернет-ресурсов для обучения, а так же обсудят между собой, насколько хорош тот или иной ресурс. При создании фотографии ученики поймут, насколько интересна данная тема.

План оценивания

График оценивания

До работы над проектом: Групповая работа

Ученики работают над проектом и выполняют задания : Подготовка доклада

После завершения работы над проектом: Выступление с докладом +творческое задание

Описание методов оценивания

Групповая работа. Проводится с целью определения уровня знаний учеников в данной теме, а так же для того чтобы ученики поняли о чем мы будем говорить в данном проекте.

Подготовка доклада. Ученики делятся на 3 группы, выбирают темы по интересам и сами добывают необходимую информацию, подготавливают презентацию.

Выступление с докладом + творческое задание. Каждая группа выступает с презентациями перед остальными учениками, так же отвечают на вопросы, и обсуждают их. Выступление с докладом завершается фотоконкурсом, на заранее выбранную тему.

Сведения о проекте

Необходимые начальные знания, умения, навыки:

Владение ПК, азами Интернета; наличие электронной почты.

Процедуры обучения

1 этап. Вводный урок (представление презентации для выявления интересов, цель которой: заинтересовать учащихся, зародить в них мотивацию для изучения данной темы; групповая работа).

2 этап. Теоретический урок – продолжение вводного (презентация, содержащая информацию о конкретных местах в Интернете, в которых можно получить дополнительное образование; о существовании образовательных сайтов и порталов; о повышении квалификации).

3 этап. Результирующий урок (доклад + творческая работа).

Огненные стражи у порога ваших данных

Автор Гараев И.М., руководитель: Чернова Е.В.

Описание проекта: проект рассматривает общие вопросы, связанные с безопасностью пользователя в сети Интернет. В ходе проекта учащиеся научатся распознавать основные угрозы Интернет. Будут перечислены средства и методы обеспечения информационной безопасности. Отдельно будут рассмотрены: все особенности, связанные с понятием – межсетевые экраны, их типах и алгоритмах работы.

Изучение обучающимися, данного материала поможет:

- пополнить знания в области ИТ и информационной безопасности;
- ознакомится с аппаратным обеспечением, обеспечивающим защиту сети от внешних угроз;
- узнать что такое межсетевые экраны и как их используют;
- понять,механизм работы межсетевого экрана;
- уяснить, какие типы межсетевых экранов бывают, и чем они отличаются между собой;
- осознать, насколько необходима защита компьютеров, подключенных к сети.

Цель проекта - заинтересовать и активизировать студентов в направлении защиты данных в компьютерных сетях.

План проведения проекта:

1. Актуализация знаний студентов по данной теме, постановка проблемы, рассмотрение целей и вопросов проекта, формирование групп в соответствии с личным желанием, ознакомление с общей темой и критериями оценок, указание источников. Стартовая презентация преподавателя по теме «Средства защиты информации» – основана на первом проблемном вопросе: «Как оградить себя от кражи конфиденциальных данных в сети Интернет?» Это должно заинтересовать студентов. В процессе презентации ученики находят ответы на учебные вопросы, общая картина, сложившихся ответов, есть решение проблемного вопроса.

Стартовая презентация содержит: «Мозговой штурм» для коллективной работы при решении проблем, результатом их работы, являются знания передаваемые друг другу и оценка учителя. Также студенты участвуют в нулевом срезе, отвечая на вопросы подготовленные учителем по общей теме: «Средства защиты информации» это необходимо для выявления и обобщения имеющихся знаний по теме, а так же постановки новых проблемных вопросов, ответы на которые заинтересовали учащихся.

Домашнее задание. Доклад с сопровождением презентации по одной из тем:

«Технические средства защиты информации»

«Программные средства защиты информации»

«Встроенные средства защиты информации»

«Специализированные средства защиты информации»

«Аппаратные средства защиты информации»

«Технические средства защиты информации»

«Процесс проникновения вирусов в компьютер»

«Защита информации»

2. Состоит в групповой работе над докладами и презентациями. Преподаватель проводит консультации,отвечает на вопросы корректирует содержания. Студенты изучают материал по заданной теме, которую выбрали по собственному интересу.

3. Защита докладов с сопровождением презентаций.

4. Заключительная презентация учителя по теме: «Межсетевые экраны»

Практическое задание: установка и правильная настройка Firewall Comodo

5. Подведение итогов: Закрепление изученного материала вопросы по теме «Межсетевые экраны».

Далее преподаватель проводит тестирование по теме «Средства защиты информации».В течение небольшого промежутка времени (30 минут) обучающиеся должны выполнить и сдать решенные тесты.

В итоге преподаватель делает выводы по работе и активности в ходе проекта,для каждого студента. Ставит оценку каждому студенту.

На заключительном этапе подводятся итоги проделанной работы: вносятся коррективы в план и дидактические материалы проекта с целью повышения их эффективности.

Основополагающий вопрос

▪ Эффективная защита информационной безопасности это сказка или быль?

Проблемные вопросы

▪ Как оградить себя от кражи конфиденциальных данных в сети Интернет?

▪ С какими задачами межсетевые экраны справиться не в силах?

Учебные вопросы

1. Средства защиты данных?
2. Межсетевой экран это?
3. Виды межсетевых экранов?
4. Какие задачи выполняют межсетевые экраны?
5. Как осуществляется передача данных через межсетевые экраны?
6. Какими возможностями обладают межсетевые экраны и как они осуществляются при работе с сетью?

Ход проекта:

1. Актуализация знаний студентов по данной теме, постановка проблемы, рассмотрение целей и вопросов проекта, формирование групп

в соответствии с личным желанием, ознакомление с общей темой и критериями оценок, указание источников. Стартовая презентация преподавателя по теме «Средства защиты информации» – основана на первом проблемном вопросе: «Как оградить себя от кражи конфиденциальных данных в сети Интернет?» Это должно заинтересовать студентов. В процессе презентации ученики находят ответы на учебные вопросы, общая картина, сложившихся ответов, есть решение проблемного вопроса.

Стартовая презентация содержит: «Мозговой штурм» для коллективной работы при решении проблем, результатом их работы, являются знания передаваемые друг другу и оценка учителя. Также студенты участвуют в нулевом срезе, отвечая на вопросы подготовленные учителем по общей теме: «Средства защиты информации» это необходимо для выявления и обобщения имеющихся знаний по теме, а так же постановки новых проблемных вопросов, ответы на которые заинтересовали учащихся.

Домашнее задание. Доклад с сопровождением презентации по одной из тем:

«Технические средства защиты информации»

«Программные средства защиты информации»

«Встроенные средства защиты информации»

«Специализированные средства защиты информации»

«Аппаратные средства защиты информации»

«Технические средства защиты информации»

«Процесс проникновения вирусов в компьютер»

«Защита информации»

2. Состоит в групповой работе над докладами и презентациями. Преподаватель проводит консультации, отвечает на вопросы корректирует содержания. Студенты изучают материал по заданной теме, которую выбрали по собственному интересу.

3. Защита докладов с сопровождением презентаций.

4. Заключительная презентация учителя по теме: «Межсетевые экраны»

Практическое задание: установка и правильная настройка Firewall Comodo

5. Подведение итогов: Закрепление изученного материала вопросы по теме «Межсетевые экраны».

Далее преподаватель проводит тестирование по теме «Средства защиты информации».В течение небольшого промежутка времени (30 минут) обучающиеся должны выполнить и сдать решенные тесты.

В итоге преподаватель делает выводы по работе и активности в ходе проекта, для каждого студента. Ставит оценку каждому студенту.

На заключительном этапе подводятся итоги проделанной работы: вносятся коррективы в план и дидактические материалы проекта с целью повышения их эффективности.

Воронка продаж

Автор Григорьева Н., руководитель: Чернова Е.В.

Описание проекта: данный проект «Интернет-маркетинг» предназначен для школьников 10-11 классов в рамках дисциплины Информатика. В учебном проекте будут рассмотрены такие вопросы как что такое интернет-маркетинг, какие способы привлечения клиентов существуют, как изучить потенциальную аудиторию, как продвигать товары, что такое сетевые пирамиды.

Цель проекта – ознакомить учащихся с Интернет-маркетингом и вопросами, касающимися этой темы.

План проведения проекта:

1. Вводное занятие. Знакомство учеников с проектом, проверка начальных знаний в ходе фронтальной беседы.
2. Презентация учителя «сетевые пирамиды», практическое занятие «Я никогда не занимался маркетингом. Я просто любил своих клиентов».
3. Выбор тем для итоговой работы – создание буклетов по выбранным темам.
4. Итоговая работа, обобщение полученных знаний в ходе обсуждения, подведение итогов.

Основополагающий вопрос

Как изведать неизведанное?

Проблемные вопросы

1. Как понять клиента?
2. Как выбрать эффективные инструменты продвижения?

Учебные вопросы

1. Что делать, если интернет-реклама не дает результата?
2. Что такое интернет-маркетинг?
3. Какие способы привлечения клиентов существуют?
4. Что такое сетевые пирамиды?
5. Как поймать внимание клиента в тексте?

Ход проекта:

Вводное занятие.

Знакомство учеников с проектом, проверка начальных знаний в ходе фронтальной беседы.

Практическое занятие

Задание1. Заполните таблицу, распределив наиболее покупаемые товары по возрастным группам потребителей. Необходимо на указанных сайтах найти товары и распределить их по возрастным группам.

Возраст	Группа	Товары (по 2 примера на каждый сайт)		
		ozon.ru	slando.ru	sotmarket.ru
0–5	Маленькие дети			
6–19	Школьники и подростки			
20–34	Молодые люди			
35–49	Люди среднего возраста			
50–64	Люди зрелого возраста			
65 и более	Пожилые люди			

Задание 2

Одним из наиболее популярных видов рекламы в Сети является баннерная. Выберите на любых веб-ресурсах три баннера, которые вам запомнились и понравились, и три баннера, которые вызвали у вас негативную реакцию, или, по вашему мнению, не привлекают потребителей. Распечатайте баннеры, дайте ссылку на них. Проанализируйте их, с точки зрения исполнения, вида графического формата, привлекательности и т.д.

Один из непонравившихся баннеров переработать так, чтобы он стал привлекательным для потребителей.

Задание 3

Придумайте по 4-5 вопросов, касающихся темы «сетевые пирамиды» (отношение людей к ним, знают ли они, что это такое и т.д.). Опросите по 3-4 человека, результаты занесите в таблицу:

вопросы	1 вопрос	2 вопрос	… вопрос	n- вопрос
Опрошенные Ф.И.				

Итоговое занятие:

Создание памятки

Все ученики поделены на группы по 2-3 человека.

Выбрать самостоятельно тему памятки по пройденному материалу, по выбранной теме создать памятку и презентовать ее.

Примерный перечень тем:

1. Что делать, если интернет-реклама не дает результата?
2. Что такое интернет-маркетинг?
3. Какие способы привлечения клиентов существуют?
4. Что такое сетевые пирамиды?
5. Как поймать внимание клиента в тексте?

Интерактивное окно в мир новостей

Автор Шаляев А., руководитель: Чернова Е.В.

Описание проекта: данный проект «Электронные СМИ» проводится в рамках дисциплины «Информатика и ИКТ» для школьников 10-11 класса. Основными содержательными линиями этого проекта являются познакомиться с электронными СМИ, оценить удобство и доступность «новостей под рукой».

Цель проекта: научиться находить достоверные СМИ и уметь в них ориентироваться.

Задачи:

1. Ввести и закрепить определение понятие «Электронные СМИ», углубить понимание его значения;
2. Проверить умение учеников логично и грамотно представлять информацию;
3. Развить навыки исследовательской деятельности;

План проведения проекта

1. Проведение вводного занятия. Выявления знаний о электронных СМИ, опрос.
2. Практическое занятие. Использование поисковых сервисов для нахождения электронных СМИ. Отчет
3. Теоретическое занятие. Разновидности электронных СМИ. Отличие от блогов. Теория
4. Результирующий урок. Нахождение пары новостных электронных СМИ, при поддержке основных каналов телевидения. Задание. Подведение итогов

Основополагающий вопрос

Электронные СМИ полезное новшество или способ попасться «на крючок»?

Проблемные вопросы

Что же такое электронные СМИ?

Что нужно знать об электронных СМИ?

Учебные вопросы

Какие электронные СМИ бывают?

Каким электронным СМИ верить?

Какие отличия электронных СМИ от блога или ЖЖ?

Как проверить новость на достоверность?

Этапы проведения проекта

Вводное занятия

Оценка знаний учащихся в данной области с помощью опроса. Таблица, представленная в опросе, активирует предварительные знания учащихся, выясняя, что они уже знают о теме проекта. Также таблица

используется как оценочное портфолио каждого ученика, чтобы увидеть то, что ученик узнал в ходе проекта.

ОПРОС

Ребята, пожалуйста, заполните представленную таблицу.

За данную таблицу никаких оценок не ставиться.

Будьте предельно честны в своих ответах и не обращайтесь к помощи Интернет.

Внимательно посмотрите на перечень вопросов. В столбце №2 ответьте на вопросы, так как Вы думаете, своими словами. Время на выполнение ~ 4-5 минут.

Ф.И., класс _____

Вопрос	Ответ
Новости о чем вам интересны?	
Где чаще всего вы знакомитесь с последними новостями?	
Какие электронные СМИ вам знакомы?	

Практическое занятие

В начале занятия, учитель для каждого ученика определяет тему, на которую ученик будет искать СМИ. В ходе данного занятия ученики заполнят отчет-таблицу, которая покажет нам, насколько ученики умеют ориентироваться в поисковых сервисах для нахождения электронных средств массовой информации на определенную тематику (спорт, искусство, техника, политика, экономика). Использование поисковых сервисов для нахождения электронных СМИ. Время на выполнение работы 20-30 мин.

Отчет по практике

За данную работу вы получите зачет\незачет.

(Если ученик работал во время работы и предоставил 3 ссылки, получает зачет)

Желаю успехов!

Ф.И.,класс_____

Тематика	Адрес

Теоретическое занятие

«Разновидности электронных СМИ. Отличие от блогов»

На данном уроке учитель рассказывает основные теоретические моменты по данной теме. По желанию ученики могут записывать основные моменты

Ребята, данный урок мы посвятим теории, я расскажу вам всю необходимую информацию по данной теме

Теория:

С появлением и распространением Интернета он стал сам по себе во многом использоваться как средство массовой коммуникации, и в его рамках стали действовать традиционные средства массовой коммуникации, появились интернет-СМИ. Они быстро завоевали популярность, хотя их аудитория пока гораздо меньше, чем «традиционных» (как их стали называть) СМИ. Почти все СМИ имеют сайты в Интернете, на многих из них публикуются регулярно обновляемая информация: как правило, это интернет-версии тех же материалов, иногда они выходят с задержкой. Благодаря развитию интернет-СМИ, количество людей, предпочитающих читать бумажную прессу, с каждым годом сокращается.

Но люди зачастую путают иные интернет-публикации со СМИ, например, такими публикациями являются блоги.

Блог – веб-сайт, основное содержимое которого — регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа. Для блогов характерны недлинные записи вре́менной значимости , отсортированные в обратном хронологическом порядке (последняя запись сверху). Отличия блога от традиционного дневника обусловливаются средой: блоги обычно публичны и предполагают сторонних читателей, которые могут вступить в публичную полемику с автором (в комментарии к блог записи или своих блогах).

Исходя из данного понятия мы видим, что блог есть ни что иное, как просто мысли конкретного человека, а не достоверным фактом, освещающим некоторое событие.

Проверить информацию на достоверность можно только «качеством» источника, если это сайт закрепленный за каким-то центральным каналом или же печатным изданием, то такие новости можно воспринимать в серьез.

Результирующий урок

Учитель:

Ребята, пожалуйста, разделитесь на группы по ~5 человек.

Вам будет мною предоставлена тема, на которую вы должны найти 3 электронных СМИ, аналоги которых существуют на тв или в печатном виде. За данную работу вы получите оценки.

Результатом занятия должна быть презентация с адресами на СМИ и комментариями, которые вы должны озвучить в группах у доски.

Презентация покажет нам, насколько ученики научились находить электронные СМИ на заданную тему. Темы на выбор: спорт, политика, экономика, искусство, технологии. Работа похожа на «отчет по практике» за исключением того, что ученики к моменту итогового занятия должны ориентироваться в новостных лентах и находить достоверные новости. Достоверность электронного СМИ будет доказываться аналогом на телевидении (то есть сайт при телевизионном канале) или же аналогичном печатном издании (не обязательно на всероссийском уровне, городские издания также допускаются).

Желаю успехов!

Оценка будет ставиться по количеству найденных СМИ.

1 адрес – оценка три

2 адреса – оценка четыре

3 адреса – оценка пять

Поисковые сервисы: истина где-то рядом

Автор Ласточкин Д., руководитель: Чернова Е.В.

Описание проекта: Данный проект предназначен для учащихся старших классов. Проект даст ученикам возможность научиться правильно составлять поисковые запросы, а так же пользоваться средствами поисковых сервисов по фильтрации контента.

Цель проекта – ознакомить школьников со способами решения основных проблем, с которыми мы сталкиваемся в процессе работы с поисковыми сервисами: обеспечение личной защиты от нежелательного контента и поиск той информации, которая необходима пользователю.

План проведения проекта:

1. Вводная презентация
2. Лабораторная работа поиску информации в Интернет
3. Конкурс «В поисках истины»
4. Итоговая работа (Кубок Яндекса)

Основополагающий вопрос

Как найти иголку в стоге сена и не уколоться?

Проблемные вопросы

1. Как найти то, что искал?
2. Как защитить себя от опасности?

Учебные вопросы

1. Что такое поисковые сервисы?
2. Как правильно организовать поиск в сети Интернет?
3. Как сформулировать запрос так, чтобы найти то, что нужно?
4. Зачем нужно фильтровать контент при поиске?
5. Какие способы фильтрации контента при поиске существуют?

Лабораторная работа по теме «Поисковые сервисы»

Оборудование: компьютер с выходом в Интернет.

Цель работы – познакомиться с понятием и принципом работы поисковых сервисов, а так же с возможностями для поиска и фильтрации информации, которыми обладают поисковые сервисы.

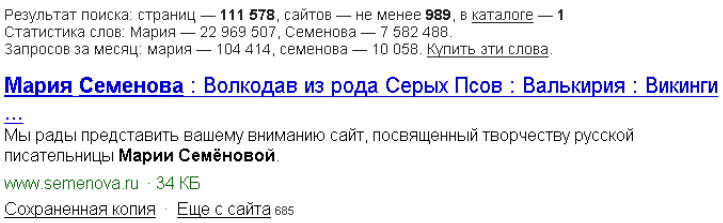
Ход работы:

1.С чего начать простой поиск?

1.1. Откройте страницу поисковой системы: в поле Адрес браузера введите http://yandex.ru

1.2. В поле запроса введите *Мария Семенова*, нажмите Искать.

1.3. На экране файл отчета, содержащий ссылки на web-страницы, соответствующие словосочетанию Мария Семенова. Формат ссылок в таком отчете следующий:


Результат поиска: страниц — **111 578**, сайтов — не менее **989**, в каталоге — **1**
Статистика слов: Мария — 22 969 507, Семенова — 7 582 488.
Запросов за месяц: мария — 104 414, семенова — 10 058. Купить эти слова.

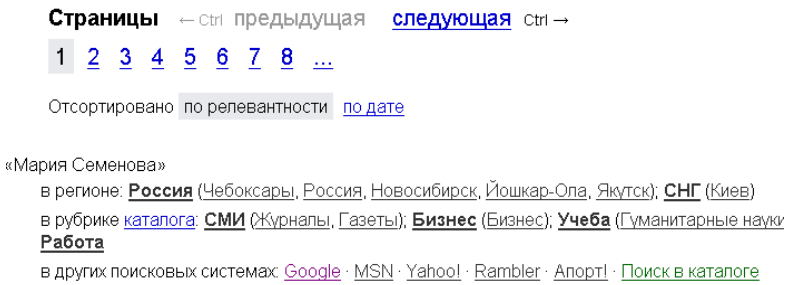
1. **Мария Семенова** : Волкодав из рода Серых Псов : Валькирия : Викинги ...
Мы рады представить вашему вниманию сайт, посвященный творчеству русской писательницы **Марии Семёновой**.
www.semenova.ru · 34 КБ
Сохраненная копия · Еще с сайта 685

- 1 - номер ссылки по порядку
- Мария Семенова : Волкодав из рода Серых Псов … - ссылка на web-страницу
- Мы рады представить вашему вниманию сайт, посвященный Марии Семёновой – описание сайта.
- www.semenova.ru · 34 КБ – адрес web-страницы
- Рубрика: Фантастика и фэнтези – рубрика в каталоге Яндекса
- Еще с сайта 685 – ссылка на другие страницы с этого сайта.
- В верхней части отчета Яндекс показывает общее количество найденных страниц - 111578.

1.4. Откройте найденную страницу: выберите Мария Семенова: Волкодав из рода Серых Псов: Валькирия: Викинги , МП, выберите Открыть в новой вкладке.

1.5. Теперь по другому: выберите Сохраненная копия , МП, выберите Открыть в новой вкладке, откроется тот же документ, но с выделенными словами запроса.

1.6. Выберите рубрика: Фантастика и фэнтези , нажмите МП, выберите Открыть в новой вкладке, откроется тематический каталог. Каталоги удобны тем, что содержат уже упорядоченную систему.



Внизу страницы браузера отображаются количество страниц в файле отчета, перемещаться по которому можно нажимая цифры 1,2 и т.д. Еще ниже располагаются сведения о методе сортировки. По умолчанию результаты поиска сортируются по релевантности, то есть на первом месте стоит документ наиболее соответствующий запросу. Можно выбрать другой метод сортировки. В самом низу окна располагаются ссылки для повторения запроса в региональной базе данных, город можно выбрать из списка. Также имеется поиск в каталоге Яндекса.

2. С чего начать сложный поиск?

Сложный поиск нужно начинать с определения ключевых слов. Нас интересует адрес фирмы, которая продала бы и смонтировала отопительный котел средней мощности, например фирмы Mora. Поскольку мы находимся в Магнитогорске, то нас интересует именно фирмы в Магнитогорске. Получаем следующие ключевые слова: Отопительный котел Mora, Магнитогорск. Заметьте, средней мощности мы не пишем, если точно не знаем. Если мы это укажем, то при строго заданном запросе поисковая система скорей всего не найдет ни одного сайта с таким содержанием, потому, что редко в прайс-листах используют такие заголовки. Ведь обычно прайс-листы содержат в .ZIP файлах, которые недоступны для поиска.

2.1. Введите *Отопительный котел Mora Магнитогорск*, нажмите Искать.

Результат будет не самым эффективным. Почему? Потому что по умолчанию поисковик настроен на максимальные возможности поиска и без использования синтаксиса поисковая система выдаст все сайты, где находится хотя бы одно из указанных слов. Необходимо использовать возможности синтаксиса.

3. Поиск по словам и словоформам

Независимо от того, в какой форме вы употребили слово в запросе, поиск учитывает все его формы по правилам русского языка. Например, если задан запрос *идти* то в результате поиска будут найдены ссылки на документы, содержащие слова *идти, идет, шел, шла* и т.д.

3.1. В поле запроса Яндекса введите *Медведев*, нажмите Искать, найдены документы содержащие *МедведевУ, МедведевА, Медведев* и т.п.

Если вы набрали в запросе слово с большой буквы, будут найдены только слова с большой буквы (если это слово не первое в предложении). В противном случае будут найдены как слова с большой, так и с маленькой буквы.

По умолчанию поиск учитывает все формы заданного слова согласно правилам русского языка. Однако существует возможность поиска по точной словоформе, для этого перед словоформой надо поставить восклицательный знак '!'.

3.2. В поле запроса Яндекса введите *!Медведева*, нажмите Искать, по такому запросу будут найдены все документы, содержащие словоформу *Медведева*.

4.иЛогические операторы

Если вы хотите, чтобы слова из запроса обязательно были найдены, поставьте перед каждым из них +.

4.1. В поисковой форме введите *частные объявления продажа гараж* нажмите Искать. Запрос выдаст много ссылок на сайты с разнообразными частными объявлениями.

4.2. В поисковой форме введите *частные объявления продажа +гараж* нажмите Искать. Такой запрос покажет объявления о продаже именно гаража.

Если вы хотите исключить какие-либо слова из результата поиска, поставьте перед каждым из них -. Знак минус надо писать через пробел от предыдущего и слитно с последующим словом.

4.3. В поисковой форме *введите частные объявления продажа -гараж* нажмите Искать. Результат: ссылки на документы о продаже, в которых нет слова гараж.

Несколько набранных в запросе слов, разделенных пробелами, означают, что все они должны входить в одно предложение искомого документа. Тот же самый эффект произведет употребление символа &. Оператор «логическое И», обозначающийся знаком &, позволяет перечислять слова, которые должны встречаться в пределах одного предложения искомого документа.

Например, при запросах *лечебная физкультура* и *лечебная & физкультура*, результатом поиска будет список документов, в которых в одном предложении содержатся и слово лечебная, и слово физкультура. Эквивалентно запросу *+лечебная +физкультура.*

4.4. В поисковой форме введите лечебная & физкультура нажмите Искать

Оператор логическое ИЛИ, обозначающийся символом |, позволяет искать документы, в тексте которых содержится только одно из перечисленных слов. Удобно при поиске синонимов.

4.5. В поисковой форме введите *фото | фотография | фотоснимок | снимок | фотоизображение* нажмите Искать. Результат: документы, содержащие хотя бы одно из перечисленных слов.

Символ ~, как правило, описывает действие, аналогичное действию знака минус, то есть исключает из искомого документа отмеченные подобным образом слова.

4.6. В поисковой форме введите *банки ~ закон* нажмите Искать. Будут найдены все документы, содержащие слово банки, рядом с которым (в пределах предложения) нет слова закон.

Удвоение какой-либо команды означает, что данное условие необходимо применять не к одному предложению, а ко всему документу в целом. Одинарный оператор (&, ~) ищет в пределах абзаца, двойной (&&, ~~) в пределах документа.

4.7. В поисковой форме введите рецепты && (плавленый сыр) нажмите Искать. В результате будут найдены документы, в которых есть и слово рецепты и словосочетание «плавленый сыр», причем «плавленый сыр» должен быть в одном предложении.

4.8. В поисковой форме введите Компьютеры ~~ цена нажмите Искать. Результат: документы со словом компьютеры, но без слова цена.

Логические операторы языка запросов можно комбинировать. Для этих целей служат символы открывающей и закрывающей скобки. Например, запрос *музыка & (beatles | Rolling Stones)* означает, что, пользователь ищет документы, содержащие либо слова *музыка* и *beatles*, либо слова *музыка* и *Rolling Stones*.

4.9. В поисковой форме введите легковые & автомобили &&Mercedes ~~запчасти. То есть пользователю нужны документы, в которых встречаются слова легковые и автомобили в пределах одного предложения, слово Mercedes в пределах всего текста и ни разу не встречается слово запчасти.

5. Операторы контекстной близости

Часто в запросах ищут устойчивые словосочетания. Если поставить их в кавычки, то будут найдены те документы, в которых эти слова идут строго подряд.

5.1. В поисковой форме введите "красная шапочка" нажмите Искать. Будут найдены документы с это фразой. При этом словосочетание «а шапочка у нее была красная» найдено не будет.

Если между двумя словами поставлен знак /, за которым сразу напечатано число, значит, требуется, чтобы расстояние между ними не превышало этого числа слов.

Например, задав запрос *поставщики /2 кофе*, вы требуете найти документы, в которых содержатся и слово поставщики и слово кофе, причем расстояние между ними должно быть не более двух слов и они

должны находиться в одном предложении. Найдутся страницы, которые содержат, например словосочетания «поставщики колумбийского кофе», «поставщики кофе из Колумбии» и т.д.

5.2. В поисковой форме введите поставщики /2 кофе нажмите Искать.

Если порядок слов и расстояние точно известны, можно воспользоваться пунктуацией /+n. Так, например, задается поиск слов, стоящих подряд. Запрос *синяя /+1 борода* означает, что слово борода должно следовать непосредственно за словом синяя.

5.3. В поисковой форме введите синяя /+1 борода нажмите Искать.

В общем виде ограничение по расстоянию задается при помощи пунктуации вида /(n m), где n минимальное, а m максимально допустимое расстояние. Отсюда следует, что запись /n эквивалентна /(-n +n), а запись /+n эквивалентна /(+n +n).

Запрос *музыкальное /(-2 4) образование* означает, что музыкальное должна находиться от образование в интервале расстояний от 2 слов слева до 4 слов справа.

5.4. В поисковой форме введите музыкальное /(-2 4) образование нажмите Искать.

Практически все знаки можно комбинировать с ограничением расстояния. Например, результатом поиска по запросу *вакансии ~ /+1 студентов* будут документы, содержащие слово вакансии, причем в этих документах слово студентов не следует непосредственно за словом вакансии.

5.5. В поисковой форме введите вакансии ~ /+1 студентов нажмите Искать.

Когда знаки ограничения по расстоянию стоят после двойных операторов, то употребленные там числа - это расстояние не в словах, а в предложениях. Расстояние в абзацах определяется аналогично расстоянию в словах.

5.6. В поисковой форме введите банк && /1 налоги нажмите Искать. Это означает, что слово налоги должно находиться в том же самом, либо в соседнем со словом банк предложении.

Вместо одного слова в запросе можно подставить целое выражение. Для этого его надо взять в скобки.

5.7. В поисковой форме введите (история, технология, изготовление) /+1 (сыра, творога) нажмите Искать. Результат - документы, которые содержат любую из фраз история сыра, технология творога, изготовление сыра, история творога и т.д.

6. Поиск по параметрам

Можно искать информацию в заголовках (Title), ссылках (Anchor) и адрес (Address). Синтаксис: **$имя_зоны (поисковое выражение).**

6.1. Ищет в заголовках документов слово Сегодняшняя газета: в поисковой форме введите $title (Сегодняшняя газета) нажмите Искать.

6.2. В поисковой форме введите $anchor (Сегодняшняя газета) нажмите Искать. Запрос находит документы, в ссылках внутри которых есть Сегодняшняя газета.

Можно ограничить поиск информации списком серверов или наоборот исключить сервера из поиска (url). Можно также искать документы, содержащие ссылки на определенные URL (link), и файлы картинок (image). Если вы хотите работать не с конкретным URL (image), а со всеми, начинающимися с данной последовательности символов, используйте *. Синтаксис: #имя_элемента="имя_файла (URL)".

6.3. В поисковой форме введите (Сегодняшняя газета) ~~ #url="www.sgzt.com*" нажмите Искать. По запросу будут искаться упоминания Сегодняшняя газета везде, кроме ее собственного сервера www.sgzt.com.

6.4. В поисковой форме введите #link="www.sgzt.com" нажмите Искать. Покажет все документы, которые сослались на сервер компании.

6.5. В поисковой форме введите #image="tort*" нажмите Искать. Система выдаст ссылки на документы с изображениями тортов (хотя, возможно, найдется и портрет черепахи Тортиллы).

Можно также искать по ключевым словам (keywords), аннотациям (abstract) и подписям под изображениями (hint). Синтаксис: #имя_элемента=(поисковое выражение).

Регламент проведения конкурса «В поисках истины»

Цель проведения конкурса – проверить и закрепить навыки безопасного поиска информации в сети Интернет, полученные ими в ходе работы над проектом «Истина где-то рядом».

Участниками конкурса могут быть все ученики, которые участвуют в проекте.

Условия проведения конкурса**:** компьютерный класс с выходом в Интернет, принтер (для печати раздаточного материала).

Этапы проведения:

№	Этап	Время проведения
1	Подготовительный	До начала урока
2	Вступительное слово, раздача заданий	3-5 минут
3	Выполнение учениками заданий	20 минут
4	Оценивание учителем результатов	15 минут
5	Определение победителей, подведение итогов	5 минут

На подготовительном этапе учителем готовится раздаточный материал, сертификаты для участников конкурса, а так же призы для победителей.

Итоги конкурса подводятся в конце урока.

Примечание: в случае, если количество участников превышает количество заданий, допускается возможность выдачи одинаковых заданий нескольким ученикам, при условии, что они не сидят рядом друг с другом.

Итоговая работа по теме «Поисковые сервисы»

Цель работы – закрепление навыков безопасного поиска информации в сети Интернет, полученных в результате работы над проектом.

Участники: все ученики, принимавшие участие в проекте.

Условия проведения: компьютерный класс с выходом в Интернет.

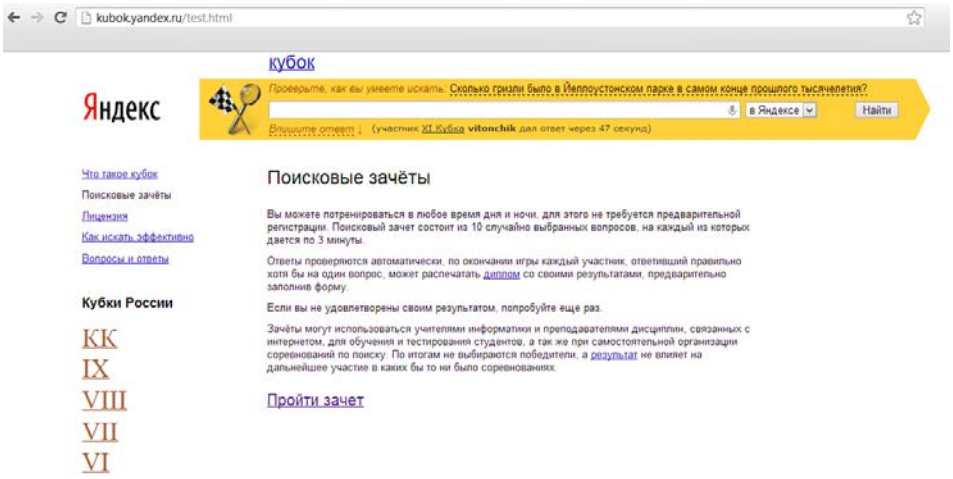
Этапы проведения:

№	Этап	Время проведения
1	Вступительное слово	2 минуты
2	Выполнение учениками заданий	30 минут
3	Оценивание учителем результатов	3 минут
4	Определение победителей, подведение итогов	5 минут
5	Подведение итогов проекта, вручение сертификатов и призов	5 минут

Подведение итогов учитель производит на основе результатов, выданных системой

Ход работы

В качестве итоговой работы используется Кубок Яндекса. Для этого все ученики переходят по ссылке http://kubok.yandex.ru/test.html и нажимают Пройти зачет.



Далее они в течении 3 минут отвечают на поставленный вопрос и переходят к следующему. По завершении всеми учениками зачета, учитель оценивает результаты, выданные системой и распределяет места по количеству баллов. Максимальное количество баллов: 10.

IP-Коммуникации: Здравствуйте! Вам звонит Интернет

Автор Варакин М., руководитель: Чернова Е.В.

Описание проекта: Проект предназначен для учеников 10-11 классов. Будут рассмотрены угрозы безопасности, связанные с IP-коммуникациями, способы выявления угроз и их устранения.

Цель проекта – познакомить с IP-телефонией, IP-видеосвязью и видеонаблюдением, научить выбирать необходимые программы для работы с данными технологиями.

План проведения проекта:

1 этап. Вводное занятие. Оценка начальных знаний учащихся с помощью опроса. Разделение на группы. Выбор учениками темы исследования в группах.

2 этап. Семинар.

3 этап. Проведение итоговой работы (Игра: «X-Files»). Обсуждение результатов итогового занятия. Выдача грамот.

Основополагающий вопрос

У меня зазвонил телефон.Кто говорит?

Проблемные вопросы

1) Темные и светлые стороны IP-коммуникаций. На чьей ты стороне?

2) Коммуникационное ассорти. Что в составе?

Учебные вопросы

1) Что такое IP-телефония и видеосвязь?

2) Какие программы существуют для поддержки IP–коммуникации?

3) Что такое IP-видеонаблюдение?

4) Как работает IP-видеонаблюдение и где оно используется?

5) Какие меры предосторожности следует соблюдать при работе с IP-коммуникациями?

6) IP-видеонаблюдение – залог защиты?

Опрос по теме «IP-Коммуникации»

Данный опрос определяет начальные знания учеников на тему IP-коммуникаций, знаний об IP-телефонии и видеосвязи, выясняет, что они уже знают о данных технологиях, а о чем необходимо будет рассказать подробнее.

Вопрос:	Ответ:	Хотели бы узнать об этом подробнее?
Что такое IP-коммуникации?		
Что такое IP-телефония?		
Что такое IP-видеосвязь?		
Что такое IP-видеокамеры?		
Где используется IP-видеонаблюдение?		
Как помогают нам IP-коммуникации?		
Какие Вы знаете программы для IP-связи?		

Семинар по теме «IP-Коммуникации»

Цель семинара – узнать о видах, местах применения и безопасности использования IP-коммуникаций**.**

Задачи:

1. Проверить умение учеников анализировать
2. Самостоятельно искать информацию
3. Работать в команде
4. Логично и грамотно представлять информацию.

Ход работы:

Разделиться на 2 группы, выбрать тему для каждой группы, подготовить материал по своей теме, оформить в виде небольшой презентации.

Ролевая игра «X-Files» по теме «IP-Коммуникации»

Цели:

- **образовательные**
- повторить и закрепить знания об IP - коммуникациях;
- научить правильно и безопасно использовать IP - коммуникации;
- **развивающие**
- развитие познавательного интереса и творческой активности учеников;
- развитие умения правильно излагать свои мысли;
- **воспитательные**
- воспитание уважения к оппонентам;
- воспитание умений вести спор

Действующие лица:

1) Злоумышленник
2) Команда ЦРУ
3) Команда ФСБ

Роли распределяются заранее по жеребьевке. Участники игры, исполняющие роли, подбирают необходимый материал, и на консультации руководитель проекта помогает отобрать нужную информацию каждому ученику в зависимости от его роли.

Роли и задачи

Роль	Задача
Злоумышленник (руководитель)	Задача злоумышленника: выкрасть секретные данные с базы команд ЦРУ и ФСБ
Команда ЦРУ, ФСБ	Получить секретные данные у руководителя проекта, спрятать их, организовать IP – видео наблюдение, предотвратить кражу секретных данных, в случае кражи – доказать виновность злоумышленника.

Ход игры

Перед началом игры, группа детей делится на 2 команды: ЦРУ и ФСБ.

Руководитель проекта выдает командам папку с секретными данными, которую в свою очередь команды должны сохранить.

Командам раздаются необходимые технические средства для реализации технической стороны игры. С данного момента руководитель становится злоумышленником, задача которого – выкрасть секретные данные из лагерей команд.

Команды, в свою очередь, должны предотвратить кражу секретных данных, а в случае кражи – доказать виновность злоумышленника (фото-видео – материал, сделанный непосредственно с помощью технических средств).

Выигрывает команда, сумевшая предотвратить кражу секретных данных, а в случае ничьей, побеждает тот, кто смог реализовать IP – видео наблюдение более эффективно.

Необходимые технические средства:

1) Ноутбук + браузер
2) Смартфон на ОС ANDROID
3) Программа IP Webcam (бесплатна в магазине android)

Пример использования (подготавливается руководителем) :

На смартфон устанавливается бесплатная программа IP Webcam.

Между смартфоном и ноутбуком создается локальная сеть.

Через браузер открывается панель управления камерой телефона.

Основы защиты информации: Обезопась себя как можешь

Автор Филимошин В.Ю., руководитель: Чернова Е.В.

Описание проекта: рассмотрены основные определения а также подготовлены практические задания для выполнения участниками проекта для достижения цели.

Цель проекта – подготовить участников проекта к различным ситуациям связанные с угрозой информационной безопасности.

План проведения проекта

Основополагающий вопрос

Информационная безопасность - нужна ли?

Проблемные направления

Все ли владеют компьютерной грамотностью?

Так ли важная защита информации для «простых» людей?

Как не попасться на уловку мошенников?

Учебные вопросы

Что такое информационное общество?

Что такое информационная культура?

Что такое информационная безопасность?

Что такое защита информации?

Компьютерный вариант практических работ

Для выполнения данных практических работ, студенты должны уметь работать с компьютерами, а именно с семейством операционных систем Windows.

Практическая работа №1 «Отключение автозапуска»

Для выполнения практической работы №1 понадобится компьютер с ОС Windows Seven.

После выполнения практической работы №1, студент должен:

- **знать**:
  - зачем отключать автозапуск у внешних носителей;
  - методы отключения автозапуска в ОС Windows Seven.
- **уметь**: отключать автозапуск в ОС Windows Seven.

Теория

Внешние носители используют обычно для переноса информации и зачастую эти носители подключаются к потенциально опасным компьютерам (заражённые вирусами), после чего внешний носитель заражается от этого компьютера. Если дома, на работе или ещё где-то не установлен антивирус, то «зараза» распространяется дальше через автозапуск, то есть при автозапуске вирус сразу же пытается проникнуть в операционную систему и если ему ничего не мешает, то он свободно туда внедряется. Для решения данной проблемы можно отключать автозапуск, тогда вирус не будет сразу активирован. Перед открытием внешнего носителя его можно будет просканировать антивирусом, либо специальной утилитой.

Какой бы антивирус не стоял – это не гарантия того, что антивирус не пропустит вирусы или потенциально опасное программное обеспеченье с внешних носителей, поэтому рекомендуется всем отключить автозапуск с флеш и других носителей.

Выполнение

Для того чтобы отключить автозапуск со всех устройств (так будет безопаснее) следует выполнить несколько простых действий.

Для операционных систем Windows Seven

1. Зайдите в панель управления (пуск→панель управления);
2. Найдите и зайдите в «Автозапуск»;
3. Уберите галочку «Использовать автозапуск для всех носителей и устройств» и сохраните результат, нажав на кнопку «Сохранить».

Другие советы по работе с внешними носителями

Открывайте флеш и другие носители с помощью команды «открыть» из контекстного меню (правая кнопка мыши), либо через проводник или сторонние файловые менеджеры (Far Manager, Total Commander и т.д.).

Если боитесь заражения своих программ на съёмных носителях, то архивируйте их, ибо вирусы заражают только исполняемые файлы.

Есть вирусы, которые из папок делают исполняемые файлы (exe), чтобы предотвратить это – архивируйте целые папки. Чтобы архивирование проходило быстро – в свойствах архиватора выбирайте «без сжатия».

Контрольные вопросы

1. Зачем нужно отключать автозапуск?
2. Что делает команда «gpedit.msc»?
3. Может ли антивирус «спасти» от всех вирусов?
4. Каким способом лучше открывать внешние носители?

Практическая работа №2 «Защита данных»

Для выполнения практической работы №2 понадобится архиватор 7zip.

После выполнения практической работы №2, студент должен:

- **знать**:
  - зачем нужны сложные пароли;
  - как можно обеспечить безопасность данных;
  - зачем шифровать данные.
- **уметь**:
  - составлять сложные пароли;
  - с помощью архиватора 7zip шифровать данные;
  - классифицировать пароли.

Теория

В последнее время важную информацию стали хранить в электронном виде, но не все её защищают. При краже этой информации последствия могут быть очень плачевными (кража электронных денег, «угон» сайта и т.д.). Поэтому стоит принимать меры по защите важной и конфиденциальной информации.

Один из способов защиты информации – это архивирование файлов с шифрованием. Для шифрования нужно будет придумать свой пароль.

Пароли можно классифицировать следующим образом:

- лёгкие: только буквы (русские или английские) или цифры.
- обычные: буквы (русские или английские) + цифры или специальные знаки.
- сложные: буквы (русские и английские) + цифры + специальные знаки.
- супер сложные: буквы (русские и английские с разным регистром) + цифры + специальные знаки.

Так же важна и длина пароля, если к примеру составить пароль по правилам сложного и длина его будет минимальна (4 символа), то такой пароль будет не таким уж и сложным по сравнению с обычным паролем, где использовано 15 символов.

Выполнение

Задание №1

Заархивировать файлы с помощью архиватора 7zip, для этого выполните следующие пункты:

1. Выберите нужные Вам файлы;
2. Если файлов несколько, то выделите их или создайте для них папку и переместите туда;
3. Откройте контекстное меню для всех файлов или папки (правая кнопка мыши);
4. Нажмите на 7zip и «добавить к архиву...»;

5. В появившемся окошке (рис. №1) нужно выбрать «формат архива» – 7z, остальные параметры можно и не менять, так же можете изменить название архива;

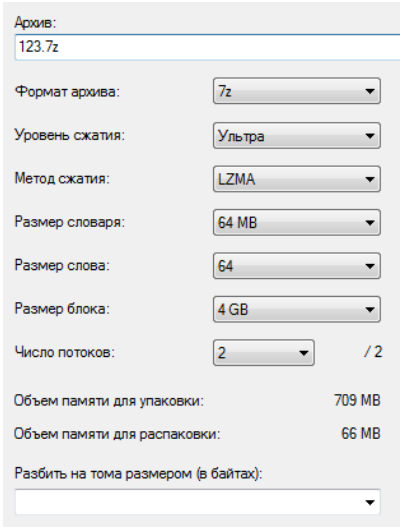


Рис. 1. Фрагмент окна с параметрами архиватора 7zip

6. Теперь введите пароль в соответствующих полях (рис. №2), так же можете поставить галочку на «шифровать имена файлов», чтобы архив не открывался без ввода пароля;

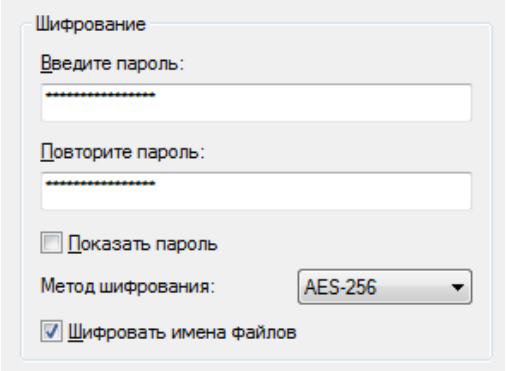


Рис. 2. Фрагмент окна с полями «Шифрование» архиватора 7zip

7. Нажмите «Ок» и подождите пока закончится процесс шифрования, потом проверьте архив.

Задание №2

Используя классификацию из теории, данной практической работы, классифицируйте следующие пароли: Ivanov96Vova, 05031981, asKeqw4$@kdU8, qwerty, 5nN*ф, ФыNIas78Md#$g.

Задание №3

Проверьте свои пароли на устойчивость ко взлому на ресурсе http://szkti.ru/polezno/psw

1. Пароль от учетной записи пользователя.
2. Пароль от ICQ (или другого мессенджера).

3. Пароль от доступа в социальную сеть (если вы зарегистрированы в нескольких – от каждой).

4. Пароль от электронной почты.

Измените свои пароли, чтобы они соответствовали рейтингу «Достаточный», «Сильный» или «Очень сильный».

Предоставьте преподавателю анализ, почему ваш пароль уязвим, опираясь на данные таблицы ресурса.

Контрольные вопросы

1. Что можно сделать с помощью архиватора 7zip?
2. Зачем шифровать данные?
3. Какие виды паролей бывают?
4. Как правильно составить пароль?

Практическая работа №3 «Обнаружение угрозы»

Для выполнения практической работы №3 понадобятся утилиты Kaspersky Virus Removal Tool, Dr.Web CureIt!.

После выполнения практической работы №3, студент должен:

– **знать**:

- какие существуют утилиты для «лечения» компьютера от вирусов и вредоносных программ;
- способы «лечения» компьютера от вирусов и вредоносных программ.

– **уметь**:

- «лечить» компьютер от вирусов и вредоносных программ;
- осуществлять разблокировку входа в ОС.

Теория

Практически каждый человек сталкивался с заражёнными компьютерами, на которых находились вирусы и другие вредоносные программы. Признаки заражённости бывают разные: от незаметных (нельзя просмотреть скрытые файлы и др.) до баннеров на весь экран (рекламные баннеры, баннеры вымогающие деньги и т.д.).

Обычно проблема в том, что на заражённых компьютерах нет антивирусов, либо базы антивирусов давно не обновлялись или же распространение вирусов было вызвано человеческим факторов (антивирус предупреждал, а человек проигнорировал).

Вирусы бывают резидентными и нерезидентными. Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными лишь ограниченное время.

Для того чтобы понять, какие последствия могут быть после заражения компьютера вирусами, классифицируем их по двум признакам: по деструктивным возможностям и по особенностям алгоритма вируса.

По деструктивным возможностям вирусы можно разделить на:

- *безвредные* вирусы, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- *неопасные* вирусы, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- *опасные* вирусы, которые могут привести к серьезным сбоям в работе;
- *очень опасные* вирусы, которые могут привести к сбоям программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти и т.д.

Классификацию вирусов по особенностям алгоритма можно разделить на:

- компаньон-вирусы (companion) – алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением *.com. При запуске такого файла DOS первым обнаружит и выполнит com-файл, т.е. вирус, который затем запустит и exe-файл;
- вирусы-«черви» (worm) – вариант компаньон-вирусов. «Черви» не связывают свои копии с какими-то файлами. Они создают свои копии на дисках и в подкаталогах дисков, никаким образом не изменяя других файлов и не используя com-exe прием, описанный выше;
- «паразитические» – все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются «червями» или «компаньон-вирусами»;
- «стелс»-вирусы (вирусы-невидимки, stealth), представляют собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме того, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы;
- «полиморфик»-вирусы (самошифрующиеся или вирусы-призраки, polymorphic) – достаточно труднообнаруживаемые вирусы, не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика;
- макро-вирусы - вирусы этого семейства используют возможности макроязыков (таких как Word Basic), встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время широко распространены макро-вирусы, заражающие доку-

менты текстового редактора Microsoft Word и электронные таблицы Microsoft Excel;

- сетевые вирусы (сетевые черви) – вирусы, которые распространяются в компьютерной сети и, так же, как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Для лечения компьютера от вирусов и других вредоносных программ лучше всего использовать утилиты по удалению вирусов и других вредоносных программ, такие как Kaspersky Virus Removal Tool, Dr.Web CureIt!

Скачать утилиты по удалению вирусов и вредоносных программ можно по следующим адресам: http://www.kaspersky.ru/, http://www.drweb.com/

Так же существует сервис для разблокировки входа в Windows по адресу http://www.drweb.com/unlocker/index/?lng=ru

После разблокировки Windows рекомендуется просканировать персональный компьютер на вирусы с помощью утилиты Kaspersky Virus Removal Tool или Dr.Web CureIt!

Лучше всего сканировать жёсткие диски, на других компьютерах, либо через безопасный режим.

Выполнение

Утилита «Kaspersky Virus Removal Tool»

1.Запустить программу с помощью ярлыка «Kaspersky Virus Removal Tool» на вашем рабочем столе, должно появится окно с программой (рис. №1);

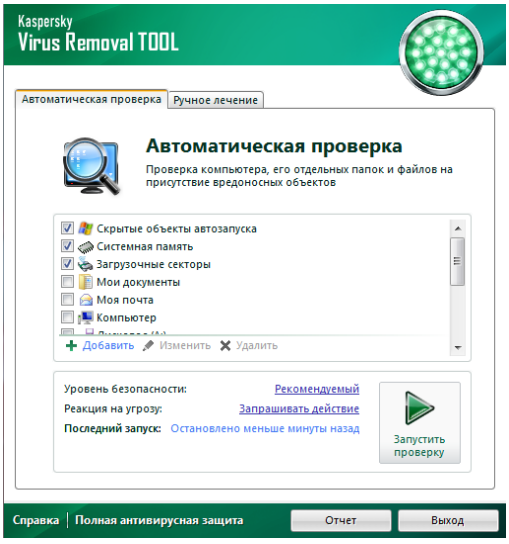


Рис. 1. Окно утилиты «Kaspersky Virus Removal Tool»

2. Выбрать области для сканирования. По умолчанию уже выбраны: «Скрытые объекты автозапуска», «Системная память», «Загрузочные секторы», к этим областям добавить «Локальный диск (C:)»;

3. По умолчанию «Уровень безопасности» – рекомендуемый, нажмите на ссылку «Рекомендуемый» и из списка выберите «настройка» и самостоятельно задайте следующие параметры: типы файлов – все файлы, проверять файлы почтовых форматов, установить глубокий эвристический анализ, установить сигнатурный поиск уязвимостей и углублённый анализ;

4. Запустить проверку с помощью кнопки (рис. №2);

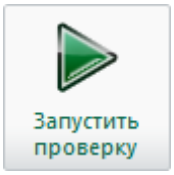


Рис. 2. Кнопка «Запустить проверку»

5. Если программа найдёт вирус или другой вредоносный объект, то появится окошко, с возможными действиями (рис. №3), если вылечить не возможно, то нажмите на «Удалить».

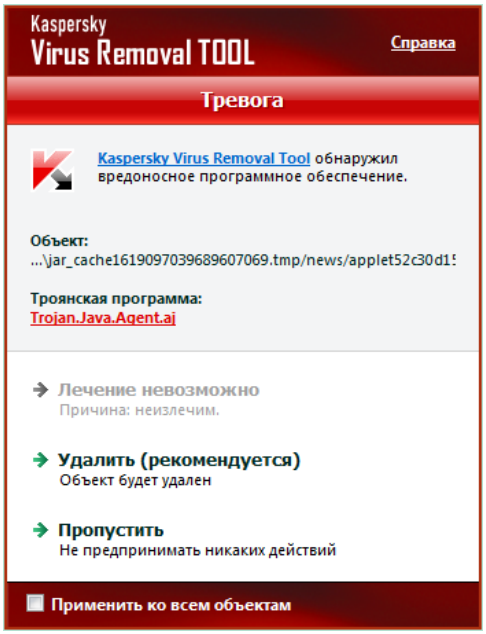


Рис. 3. Окно с выбором действий

Утилита «Dr.Web® CureIt!»

1. Запустить программу с помощью ярлыка «Dr.Web® CureIt» на вашем рабочем столе;

2. Принять «режим усиленной защиты», при появлении запроса, появится окно программы (рис. №4);

Рис. 4. Окно утилиты «Dr.Web® CureIt»

3. Нажать на «Пуск», появится запрос на быструю проверку, нажмите на кнопку «Да»;

4. Остановите быструю проверку нажав на кнопку «Остановить проверку» (рис. №5);

5. В настройках программы самостоятельно задайте следующие параметры: для инфицированных – переместить, для неизлечимых – удалить, для подозрительных – информировать. Настроить эвристический анализ, проверять выбранные файлы (базовые), запрос подтверждения действий, использовать звуки, вести вседетальный отчет, приоритет проверки средний, автосохранение настроек;

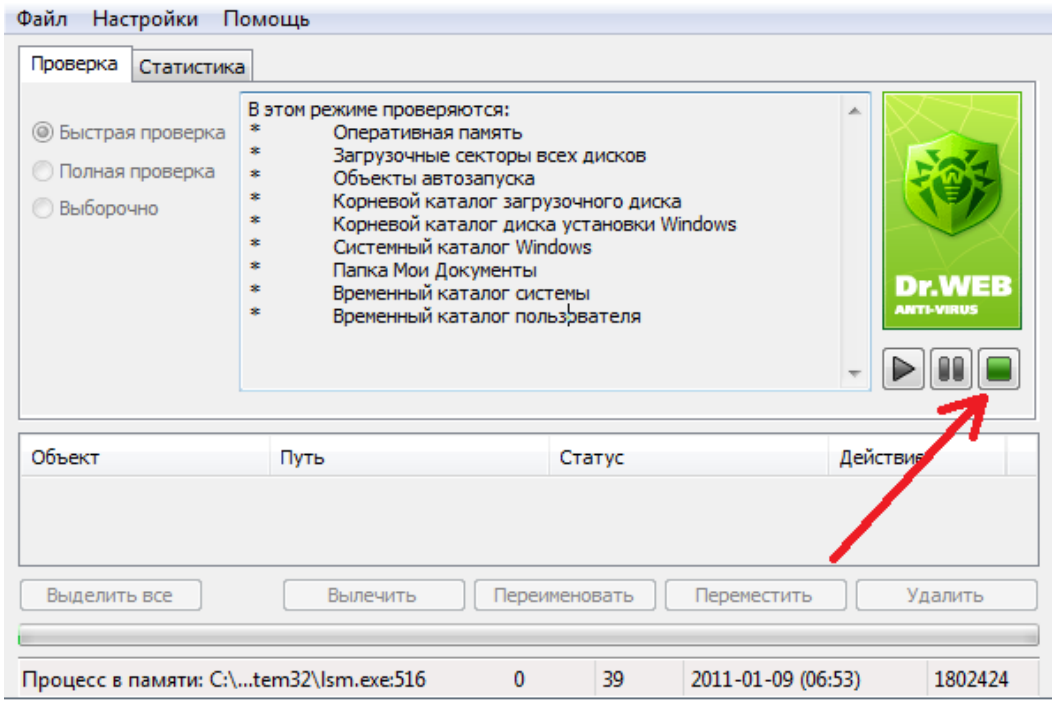


Рис. 5. Окно утилиты «Dr.Web® CureIt»

6. Запустите полную проверку или проверку любого диска и продемонстрируйте преподавателю статистику сканирования.

Контрольные вопросы

1. В чём отличие резидентных от нерезидентных вирусов?
2. Что может сделать вирус?
3. Для чего нужны лечащие утилиты?

Игра №1 «Вспомнить всё!»

Для проведения игры необходимо будет подготовить рисунки в электронном виде из практических работ «отключение автозапуска», «защита данных», «обнаружение угрозы», в электронном виде, а также распечатать карточки с различными ситуациями.

После проведения данной игры, учащийся должен:

– **знать**: основы по обеспечению информационной безопасности.

– **уметь**: находить выход из стандартных ситуаций, связанных с информационной безопасностью.

Проведение

Каждому студенту выдаются все рисунки в электронном виде из практических работ «Отключение автозапуска», «Защита данных», «Обнаружение угрозы». Студенты должны сначала отнести рисунки к определённым темам, а потом уже отсортировать в последовательности выполнения данного задания.

С помощью данных рисунков они должны восстановить все действия, которые они выполняли на практических работах, а также описать, что находится на рисунках с подробным объяснением.

После выполнения, студентам выдаются карточки с двумя разными ситуациями, они должны будут написать те действия, которые необходимо выполнить для определенной ситуации.

Ситуации

1. К вам пришёл друг с флешкой, для того чтобы распечатать реферат.
2. Включив компьютер, вы обнаруживаете, что вход в Windows заблокирован рекламным баннером.
3. Другой пользователь вашего персонального компьютера, проигнорировал предупреждение антивируса и установил потенциально опасное программное обеспеченье.
4. Для переноса важной информации вы используете внешний жёсткий диск, который понадобилось передать в другой город, через знакомого.
5. К вашему почтовому ящику, злоумышленники подобрали пароль.
6. К вам на персональный компьютер проник вирус с внешнего носителя.
7. У вас на флешке очень важная информация, и вам нужно сбросить её на другой потенциально опасный персональный компьютер.

Подведение итогов

Проверить у студентов порядок расположения рисунков и их описания. Озвучить все ситуации и рассмотреть выход из каждой ситуации, выбрать наиболее лучший «алгоритм» выхода из ситуации между студентами.

Безмашинный вариант практических работ.

Игра №1 «Мошенники везде!»

После проведения данной игры, студент должен:

– **знать**:

- признаки, по которым можно выявить мошенников;
- почему нельзя выдавать конфиденциальную информацию незнакомцам.

– **уметь**: отличать Интернет-мошенников от обычных людей.

Теория

Сколько бы не было типов мошенничества в Интернете, у мошенника все сводится к простой схеме:

1. Найти жертву;
2. Завоевать его доверие;
3. Кинуть его;
4. Исчезнуть.

Основной целью мошенника является завоевать доверие своей жертвы. Если доверие завоевано, жертва будет делать то, что требуется.

Есть множество различных обманов в интернете, есть достаточно правдоподобные, есть и абсолютно бредовые, тем не менее находятся люди, которые на них ведутся, ибо народ любит халяву. Особенно часто жертвами мошенников становятся новички, которые ищут работу или заработок в интернете. Когда им говорят, что можно просто и быстро разбогатеть они теряют голову, не задумываясь о том, что это может быть обман.

Волшебные кошельки

Суть данного интернет обмана в следующем: жертву заверяют, что обнаружен так называемый «волшебный кошелек» и если на него послать денег, они возвращаются обратно в увеличенном размере. Чаще встречаются волшебные электронные кошельки Яндекс.Деньги и волшебные кошельки WebMoney. Волшебства не бывает, но этот классический обман все еще работает и тысячи людей теряют свои деньги.

Еще есть такой обман, когда жертве предлагают «наказать» владельцев волшебных кошельков. Жертва посылает совсем небольшую сумму для теста и жертве обещают обязательно вернуть ее обратно – развод.

6 кошельков

Суть обмана в следующем: жертву просят посылать на 6 различных кошельков немного денег (часто по 1$) и вписать свой номер кошелка в конец списка. Далее жертве нужно привлекать такой же народ и

ждать когда же на жертву обрушится богатство. Получается своего рода пирамида, а как известно почти все пирамиды – сплошной обман, в котором очень и очень сложно что-то заработать.

Продажа программ для заработка

Стандартный вид интернет мошенничества. Жертве пытаются продать то, что, по словам продавца должно приносить деньги, но когда жертва покупает товар, оказывается, что его обманули и продали какую-то ерунду. Вот несколько распространенных программ: генератор WebMoney, автосборщик бонусов, Программа для взлома WebMoney.

Обмен валют в обменниках

Мошенник уверяет, что есть обменник, где можно обменять валюту с выгодой. Вот, один из примеров подобного обмана (орфография сохранена):

«Теперь возможность зарабатывать большие деньги есть у каждого!!!

Недавно нашла методику по заработку в Интернете, обещали $1000 в день.

Попробовала, все реально работает!!!

Вот данная методика:

1. Вы обмениваете через русский обменник https://www.roboxchange.com WMZ на E-Gold по курсу 20WMZ=20E-Gold.

2. Потом обмениваете обратно через иностранный обменник http://pots-exchanger.com по курсу 20E-Gold=22.4WMZ.

3. Чистая прибыль с одного обмена с учетом комиссии составила $2.

4. Повторяете данную операцию 30 раз (примерно 40 минут) чистый доход $60

Внимание: минимальная сумма обмена в иностранном обменнике $20.

Я сама целый день обмениваю деньги и зарабатываю более $500 в день.»

Письмо от администратора

Мошенник присылает жертве письмо от имени администратора сайта или от имени платежной системы. В письме сообщают, что жертва должна либо выслать денег, чтобы аккаунт жертвы не заблокировали, либо просят ввести свой логин и пароль.

Ложная информация

Жертве приходит письмо якобы от имени его знакомого, в котором он делиться информацией, которая должна принести выгоду. Например (орфография сохранена):

«Недавно узнал, что если отправить смс с любого оператора с текстом smt100 на номер 1171 то на счет приходит 100рублей! Попробывал… Деньги пришли!!!!!!!!Правда не сразу, где то через час. За смс сняли 1 рубль(билайн). Не знаю как это действует, но мне уже 1700рублей пришло! Жаль что деньги не снять….зато могу разговари-

вать сколько хочу…Если интересно, торопись, пока операторы не просекли это!».

Это написал не знакомый, его компьютер просто заражен трояном, который рассылает данные сообщения, без ведома хозяина.

Проведение

Группе объясняются правила игры.

Вызываются по очереди пары студентов и они демонстрируют свою игровую ситуацию, потом идёт обсуждение этой игровой ситуации. В конце игры собираются все признаки с помощью которых можно выявить мошенника.

Если участников игры слишком много и не хватает времени, то игровые ситуации проигрываются между парами без озвучивания, даётся около 10-15 минут. Далее выбираются пары, где было меньше всего замечено признаков мошенничества и эта ситуация проигрывается заново, после чего все участники анализируют эту игровую ситуацию.

Правила игры

Группа студентов разбивается на пары: мошенник и пользователь.

Мошенник должен, за короткое время, как можно больше выманить информации у простого пользователя, но так, чтобы простой пользователь не догадался, что у него выманивают какую либо информацию. Мошенник может принимать любое обличие, к примеру: администратор сайта, директор фирмы, модератор форума, дальнего родственника и т.д. Мошенник должен быть убедительным, иначе ничего не получится с самого начала.

Пользователь, при общении с мошенником, должен будет по каким либо признакам догадаться, что с ним общается мошенник и пытается выманить из него информацию.

Примерные действия мошенника

1. Представится пользователю под чужим именем;
2. Убедиться в том, что это действительно тот пользователь, который вам нужен (узнать имя, фамилию);
3. Убедить пользователя в том, что вы действительно являетесь представленным человеком (рассказать о себе что ни будь);
4. Сказать каким образом вы нашли этого пользователя (не обязательно);
5. Любыми способами выманить нужную вам информацию (если 3 этап был выполнен хорошо, то проблем возникнуть не должно).

Какую информацию можно узнать:

- пароли от сайтов.
- адрес проживания и когда дома ни кого нет.
- сколько зарабатывает человек и где работает, во сколько заканчивает работу и когда получает зарплату.

- какое программное обеспеченье использует для защиты своего персонального компьютера.
- на чём ездит человек и где оставляет свою машину, какую использует защиту от угона.
- и т.д., то есть ту информацию, которую мошенник может использовать для своей выгоды.

Подведение итогов

В итоге простой пользователь должен рассказать по каким признакам он понял, что с ним общается мошенник и пытается выманить у него какую либо информацию. Мошенник должен рассказать, какие «слабые места» есть у простых пользователей, с помощью которых можно выманить информацию.

Игра №2 «Назад в прошлое»

Игра направлена на то, чтобы студенты могли предвидеть возможную причину порчи или утечки информации и заранее защититься от данных воздействий.

После проведения данной игры, студент должен:

– **знать**: потенциально опасные факторы, из-за которых может произойти утечка или порча информации.

– **уметь**:

- анализировать обстановку и выявлять факторы, из-за которых может произойти утечка или порча информации;
- принимать меры по предотвращению утечки или порчи информации.

Проведение

Игра проводится в стиле: «А чтобы вы сделали, если смогли вернуться в прошлое?». Игра коллективная, то есть ситуации сообщаются сразу всем и отвечать могут все.

Студентам сообщаются ситуации, из-за которых была испорчена или похищена информация, проанализировав данный случай, студенты должны определить в чём были допущены ошибки и каким образом предотвратить данные ошибки.

Ситуации

1. Выход из строя жёсткого диска на сервере, который невозможно восстановить. На жёстком диске находилась вся электронная информация предприятия.
2. Утечка конфиденциальной информации по вине сотрудника.
3. Непреднамеренное удаление ценной информации сотрудником фирмы.
4. Перехват данных хакером через беспроводную связь.
5. Кража оборудования с конфиденциальной информацией.

Примерные виды ошибок

1. Сервер плохо охлаждался; не создавались копии на других носителях информации; жёсткий диск не проходил своевременную диагностику (проверка на ошибки); выход из строя жёсткого диска из-за срока годности.

2. Сотрудник попался на уловку мошенника (ICQ, e-mail); у сотрудников не установлен пароль на их учётные записи; у сотрудника открыт общий доступ к папке с важной информацией.

3. «А что будет, если нажать вот на эту кнопочку» - подумал сотрудник и нажал на кнопку delete, а потом не глядя на сообщение нажал Enter; сотрудник сделал копию файла и удалил оригинал, потом оказалось что он создал ярлык; от нечего делать сотрудник нажимал все кнопки подряд на клавиатуре.

4. Незащищённая беспроводная связь, то есть, нет пароля на подключение; перехват данных и подбор пароля для беспроводной сети (нет привязки к определённым компьютерам); «выход» беспроводной связи за стены предприятия (очень мощный сигнал).

5. Мошенник, подделав документ и представившись электриком или кем-то ещё, вынес внешний накопитель с конфиденциальной информацией; недобросовестный сотрудник вынес жёсткий диск или какой либо другой носитель информации.

Подведение итогов

Если были названы не все допустимые ошибки, то преподаватель сообщает их. Студенты могут придумать и свои ситуации и озвучить их.

Игра №3 «Обеспечение информационной безопасности предприятия»

Перед проведением игры желательно, чтобы студенты выполнили компьютерные практические задания №1, №2 и №3.

После проведения данной игры, студент должен:

– **знать**:

- какие способы атак и махинаций существует для получения или уничтожения конфиденциальной информации;
- методы защиты конфиденциальной информации.

– **уметь**: обеспечивать защиту конфиденциальной информации.

Проведение

Студенты должны разделиться на несколько групп по 5 человек. Студентам объясняются правила игры, после чего даётся время на подготовку.

По истечении времени на подготовку, группы студентов озвучивают свои данные о фирме. Когда все группы студентов выступят, обсуждаются способы атак и махинаций, с помощью которых можно выманить нужную информацию или же её уничтожить и проанализировать, к каким фирмам применимы данные атаки.

Правила игры

Для подготовки студентам даётся около 20-25 минут.

За время подготовки студенты должны:

1. Придумать название фирмы.

2. Придумать, что производит или какие услуги предоставляет данная фирма.

3. Выявить, какая информация является конфиденциальной в придуманной фирме (доходы, информация о сотрудниках, алгоритм производства и т.д.).

4. Продумать меры по защите конфиденциальной информации (физические, аппаратные, программные).

5. Придумать способы атак или махинаций, с помощью которых можно выманить нужную информацию у других фирм.

Изначально у каждой фирмы есть компьютерная техника, где имеется:

- сервер с различной информацией предприятия (обращаться к нему могут все сотрудники фирмы);
- оборудование для выхода в сеть Интернет, с помощью которого производится блокировка потенциально опасных сайтов, идёт слежка за сотрудниками фирмы (кто куда заходил, на какие сайты), так же можно закрыть доступ к сервисам ICQ и других месенджеров для быстрого обмена сообщениями;
- пользовательские компьютеры с выходом в сеть Интернет и доступом к серверу с информацией;
- мобильные компьютеры (ноутбуки) – для начальства, с выходом в сеть Интернет, подключенные через беспроводную связь и доступом к серверу с информацией;
- точки доступа беспроводной связи, для подключения мобильных компьютеров к сети Интернет. У беспроводной связи очень мощный сигнал и доступен он соседним жилым домам, который находятся по соседству с предприятием;
- начинающий системный администратор, но не знающий что ему делать, пока ему не скажут.

Фирма дополнительно может нанять ещё 2 человек, для каких либо целей.

Если есть возможность, то студенты, на время подготовки, могут пользоваться Интернетом.

Примерные виды атак, махинаций и решения данных проблем

- сетевые вирусные атаки. Решение проблемы: установить антивирус, закрыть не нужные порты, запретить вход на потенциально опасные сайты;
- подделка удостоверения сотрудника. Решение проблемы: более тщательная проверка на входе, установка видеонаблюдения, установка

паролей на учётные записи сотрудников, отдельная закрытая комната под сервер;

- переписка по внутренней почте с сотрудником и мошенником. Решение проблемы: подтверждение начальства о необходимости конфиденциальной информации;
- внедрение вирусов через внешние носители. Решение проблемы: установка антивируса, отключение автозапуска с внешних носителей, сканирование на наличие вирусов специальной утилитой.

Подведение итогов

Выбирается самая «защищенная организация» и студентами озвучивается каким образом была построена данная информационная защита организации.

Ожидаемые результаты проекта

- Приобретение новых умений и навыков, необходимых для защиты информации;
- Применять свои знания на практике по обеспечению информационной безопасности.

Ощущение полной безопасности наиболее опасно

Автор Валяева Н., руководитель: Чернова Е.В.

Описание проекта: Данный проект посвящен теме «Основы психологической защиты в Интернет». Целью проекта является обучить таким правилам поведения в сети, которые помогут оградить от негативных последствий психологических угроз. Важно, чтобы учащиеся поняли, что Интернет-пространство небезопасно, и помимо вирусов их ожидают различные опасности для психологического состояния, а также как нужно действовать, подвергаясь такого вида опасности.

Цель проекта – обучить учащихся таким правилам поведения в сети, которые помогут оградить от негативных последствий психологических угроз.

План проведения проекта:

1 этап. Вводное занятие. Знакомство учеников с проектом, проверка начальных знаний при помощи дискуссии.

2 этап. Практическое занятие

3 этап. Защита презентаций. Знакомство с условиями конкурса памяток.

4 этап. Конкурс памяток, обобщение полученных знаний в ходе обсуждения, подведение итогов.

Основополагающий вопрос

Как не дать себя в обиду?

Проблемные вопросы:

1. Как может оказываться психологическое давление на человека в Интернет?
2. Как защитить себя от влияния в Интернет?

Учебные вопросы

1. Как не попасться на уловки мошенников?
2. Какие существуют виды психологических угроз в Интернет?
3. Как работать в Интернете безопасно?
4. Что нужно помнить при общении с новыми людьми в Интернет?

Дискуссия «Насколько опасен Интернет»

Цель проведения: Оценка начальных знаний учеников по теме.

Формат проведения: Практическая работа рассчитана на половину урока. Все ученики поделены на 3 группы. На протяжении 10 минут ученики ищут ответ на первый вопрос учителя: «Какие угрозы существуют в Интернет?». К доске вызываются по одному человеку от группы. Каждая группа по очереди называет одну угрозу из списка, который они подготовили. Представитель этой группы записывает ее на доске. Учитель и ученики следят за тем, чтобы угрозы не повторялись. Следующий этап – из большого списка угроз выбрать те, которые можно отнести к психологическим.

Вопросы для обсуждения:

1. Какие угрозы поджидают в Интернет?
2. Какие из угроз можно отнести к психологическим?

Предполагаемый результат: Преподаватель сможет определить, какое представление о теме имеется у учеников.

Практическая работа «На чужих ошибках учатся»

Цель проведения: Изучение проблемы психологических угроз в Интернет учениками и осознание ее актуальности**.**

Формат проведения: Практическая работа рассчитана на один 1 час классной работы и 2 часа самостоятельной работы. Все ученики поделены на 3 группы, у каждой группы своя тема. На протяжении урока ученики занимаются изучением темы и поиском примеров психологических угроз в Интернет по своей теме. Задание на дом: оформить найденную информацию в форме презентации, проанализировать поведение людей, сделать вывод.

Участники: Ученики проводят исследование выбранной темы и представляют информацию в виде презентации.

Темы для исследования:

1. Опасные знакомства;
2. Нежелательная информация;
3. Кибер-буллинг;

Предполагаемый результат: Ученики научатся обнаруживать психологические угрозы в Интернет, различать их виды, а также получат представление о том, какие ошибки совершает неопытный пользователь, попадая под «психологическую атаку».

Ход работы (действия учителя):

1. Ученики разбираются, что представляет собой данная угроза. Для этого осуществляется поиск в Интернет, при необходимости задаются вопросы преподавателю.
2. Поиск примеров психологических угроз в сети на различных форумах, в социальных сетях и других сайтах на просторах Интернет. Каждый найденный пример фиксируется в виде скриншотов.
3. Ученики, исходя из своего жизненного опыта и полученных знаний, оценивают, насколько правильным было поведение людей, на которых была направлена «психологическая атака».
4. Представление найденной и проанализированной информации в виде презентации.
5. Выступление перед одноклассниками. Ученики перед всем классом рассказывают о своей теме, показывают презентацию, делают вывод о том, как нужно себя вести находясь под психологическим воздействием в сети, при необходимости отвечают на вопросы одноклассников и учителя.

Действия учеников.

1. Зайдите в поисковую систему, найдите информацию о виде угрозы, которая разбирает ваша группа. Выделите наиболее важный материал, который вы представите в презентации.
2. Проконсультируйтесь с преподавателем по поводу примеров психологической угрозы вашей группы.
3. Осуществите поиск примеров угрозы в Интернет при помощи поисковой системы, просмотра страниц различных форумов и социальных сетей. Найденные результаты фиксируйте в виде скриншотов.
4. Представьте найденную информацию в виде презентации.
5. Подготовьте выступление перед классом, которое ваша группа будет показывать на следующем уроке.

Конкурс памяток

Цель проведения: проверка и закрепление полученных знаний учеников по теме проекта**.**

Формат проведения: Конкурс проводится в течение одного урока.

Этапы проведения:

1. Ознакомление с условиями конкурса.
2. Выбор темы и подготовка памятки участниками конкурса
3. Представление созданной памятки, оценивание работ другими участниками (оценивают работу по различным критерия, представленные в файле «Критерии оценивания творческой работы»).
4. Победителем становится тот, чья работа набрала наибольшее количество баллов.

Участники: Ученики разрабатывают памятки для неопытных пользователей, в которых описывают правила безопасной работы в Интернет в конкретной области. Участниками конкурса являются ученики, участвовавшие в проекте.

Ход проведения конкурса:

1. Для участия в конкурсе ученику необходимо подготовить памятку по выбранной им теме. Памятка разрабатывается в графическом редакторе и предоставляется в электронном и распечатанном виде. *Требования к работе***:**

1) Работа должна быть красочно оформлена.

2) Текст сформулирован грамотно, по существу.

3) Работа должна содержать изображения, соответствующие заданной теме.

2. **Темы для обсуждения:**

1) Как не попасться на уловки мошенников?

2) Какие существуют виды психологических угроз в Интернет?

3) Как работать в Интернете безопасно?

4) Что нужно помнить при общении с новыми людьми в Интернет?

3. Представление работы происходит следующим образом:

Ученик демонстрирует работу перед всем классом, кратко описывает ее, аргументирует выбор оформления, кратко описывает составленные им правила, которые необходимы для безопасной работы в Интернет.

4. Оценка работ осуществляется другими учениками по 5-бальной шкале по следующим критериям:

- Грамотность – насколько грамотно, лаконично, без ошибок излагается материал.
- Содержание – в работе содержится только необходимая информация.
- Графическое оформление – насколько выбранные изображения для работы соответствуют теме.
- Читабельность информации – насколько легко можно прочитать представленный текст, контрастные ли цвета выбраны для фона и текста, комфортно ли читать такой текст.

Оценки заносятся в следующую таблицу:

ФИО ученика	Грамотность	Содержание	Графическое оформление	Читабельность информации	Итого баллов

Предполагаемый результат: Ученики систематизируют свои знания, разработают правила для безопасной работы в Интернет, наглядно оформят результат.

Задание для профильных классов «Один день из жизни»

Цель проведения: Оценка полученных знаний учеников по теме.

Формат проведения: Написание эссе на тему «Один день из жизни». В этом эссе ученики описывают день человека, который думает, что Интернет безопасен, и человека, который заботиться о своей безопасности в сети. Описываются примеры психологических угроз в Интернет, поведение человека в таких ситуациях. В заключении делается вывод о том, какие ошибки чаще всего совершает человек и каким образом можно избежать негативных последствий психологических угроз.

Предполагаемый результат: Преподаватель сможет определить, какое представление по теме имеется у учеников.

Виртуальное общение

Автор Яриз А.В., руководитель: Чернова Е.В.

Описание проекта: Проект предназначен для исследования сервисов и программ для общения в сети Интернет, рассмотрения и анализа психологических аспектов в ходе данного общения, для изучения основных норм этикета виртуального общения. В ходе реализации проекта учащиеся знакомятся с понятием виртуальное общение, электронная почта, программы быстрого обмена сообщениями, аспекты психологического воздействия. Самостоятельные исследования учащихся выполняемые с использованием базовых информационных технологий посвящены изучению существующих программных продуктов, предназначенные для общения в виртуальном мире.

Цель проекта – в ходе исследования выявить плюсы и минусы общения в сети Интернет.

Задачи проекта:

1. Анализ понятия виртуального общения.
2. Рассмотрение психологических аспектов виртуального общения.
3. Рассмотрение видов виртуального общения.
4. Развитие навыков работы с компьютерной техникой;
5. Закрепление умений и навыков работы в текстовом редакторе Microsoft Word;
6. Обучение работе в программе для создания буклетов Publisher;
7. Обучение работе с информацией: целенаправленному поиску, методам поиска и отбора информации; знакомство с систематизацией, различными способами обработки информации;

8. Развитие познавательного интереса, творческой активности, умения излагать мысли;

9. Повторение и закрепление основного программного материала;

10. Развитие умения работать с дополнительной литературой, правильно выбирать источники информации;

11. Развитие логического мышления, памяти, внимания;

12. Совершенствование мыслительных приемов анализа и синтеза;

13. Воспитание самостоятельности и ответственности, упорства в достижении цели.

Учащиеся должны:

знать:

- методы обмена информацией в сети Интернет;
- существующие программные продукты, предназначенные для общения в сети Интернет;

уметь:

- применять методы обмена информацией в сети Интернет;
- соблюдать требования информационной этики и права;
- искать и обрабатывать информацию из различных источников, приводить собственные примеры явлений и тенденций, связанных с виртуальным общением;
- интерпретировать изучаемые явления и процессы, давать им сущностные характеристики, высказывать критическую точку зрения и свои собственные суждения по проблемным вопросам;
- сравнивать, анализировать и систематизировать имеющийся учебный материал;

иметь навыки:

- представлять результаты учебных исследовательских проектов с использованием ИКТ.
- самостоятельной работы с учебной, научно-популярной литературой и материалами Интернет;
- участия в групповой работе и дискуссиях, в решении задач в игровых ситуациях и проектной деятельности.

Данный проект реализуется в факультативной форме в рамках школьной программы.

План проекта:

1. Введение в тему (45 мин).
2. Организация групповой работы, распределение тем исследований (45 мин).
3. Самостоятельная работа.
4. Консультации и доработка материала учащимися (6 уроков – 225 мин).
5. Представление результатов (45 мин).

Программное обеспечение:

- текстовый редактор Microsoft Word;
- программа для создания буклетов MS Publisher;
- программа для созданий презентаций MS Power Point.

Тип проекта:

1. По предметно-содержательной области – межпредметный.
2. По характеру координации – с явной координацией.
3. По характеру контактов – внешний.
4. По количеству участников – индивидуальный или групповой.
5. По продолжительности выполнения – долгосрочный.

Тематический охват проекта: для реализации проекта учащимся необходимо изучить следующие разделы курса информатики:

1. «Аппаратные и программные средства ЭВМ»;

2. «Средства работы с текстовыми документами. Текстовый редактор Microsoft Word»;

3. «Основы компьютерных телекоммуникаций. Программа Internet Explorer»;

4. «Программа для создания презентаций MS Power Point»

Проблемные вопросы проекта:

1. Виртуальное общение – самое «экологически чистое»?

2. Какие угрозы подстерегают при общении детей и подростков в сети Интернет?

3. Каким образом компенсируется «эмоциональный дефицит» в виртуальном общении?

4. Виртуальна ли виртуальная дружба?

5. «Я» или «Виртуальное Я»?

План работы над проектом:

1. Информационный этап: рассказ ученикам о создании проектов, опыте других учащихся в этой области, описание эмоций и ощущений при работе над проектом, пробуждение у школьников желания сделать что-нибудь подобное;

2. Определение темы проекта: учитель и ученики обсуждают название проекта, его содержание и форму представления результатов. На этом этапе педагог не мешает детям выбирать тематику проекта, а только помогает разрешить возникшие трудности при обсуждении, и дает советы;

3. Формулировка задач, функций каждого ученика, распределение этапов работы: учитывается желание каждого ученика при работе над проектом;

4. Подготовка проекта: проект дети готовят самостоятельно. Учителю нужно знать, как продвигается работа по созданию проекта, но без строго контроля над деятельностью детей, так как проект – один из лучших способов выработать у детей самостоятельность и умение работать в коллективе;

5. Коррекция: учитель советует детям, что нужно сделать, какие дополнения внести, чтобы проект стал интересным, исправляет ошибки;

6. Презентация проектов: представление проектов проходит в праздничной атмосфере. Класс украшается в соответствии с тематикой проектов, возможно использование костюмов или элементов костюмов;

7. Анализ представленных проектов: спрашивается мнение каждого ребенка о проекте, что понравилось, какие изменения необходимо внести, чтобы следующий проект стал более удачным. Заключительное слово предоставляется учителю. Важно найти теплые слова благодарности всем детям за выполненную работу.

Выполнение проекта.

Этап 1.

На уроке информатики учитель предлагает задание учащимся: создать статью на социальном сервисе Летописи, посвященную исследованию виртуального общения. В разработке этого проекта могут участвовать один или несколько человек.

1. Первым шагом работы является определение концепции статьи, мысленное его конструирование, формулирование замысла. На этом этапе определяются такие вопросы, как тематическое направление статьи, цели его создания, применяемые технологии и программные средства.

2. Поисково-исследовательская деятельность. В данной части разбивается каждый раздел на подтемы и выполняется сбор информации. При этом используются материалы, собранные из разнообразных источников (Интернет, специализированная литература и т.д.).

Этап 2.

Подготовка статей по каждой теме раздела из собранных материалов.

Этап 3.

На данном этапе осуществления проекта выполняется сканирование фотографий, рисунков, ввода имеющихся статей в компьютер, создание шаблонов буклетов.

Этап 4.

Завершающей стадией этого этапа является проверка работоспособности страницы на социальном сервисе Летописит и подготовка ее к презентации и защите проекта.

Результаты проекта:

В результате выполнения проектной работы учащиеся овладеют знаниями и умениями работы в таких программных средствах, как:

1. Программа для создания буклетов MS Publisher (создание буклетов, размещение объектов на них, использование тем для оформления и т.д.);

2. Программа для создания презентаций MS Power Point (создание слайдов, размещение на них различных объектов, применение тем для оформления слайдов, и т.д.).

Электронная книга – твой друг, без неё как без рук

Автор Беляшова А.А., руководитель Романова М.В.

Описание проекта. Основная тема проекта: «Электронные книги и библиотеки». Проект по предметно – содержательной области является межпредметным так, как охватывает такие школьные предметы как информатика и обществознание; по характеру координации - с открытой координацией; по характеру контактов – внутриклассный; по количеству участников – групповой; по продолжительности – краткосрочный (4 урока).

Дидактические цели проекта:

- Формирование у учащихся представлений об электронных книгах и электронных библиотеках, и правилах работы с ними.
- Развитие умений представления результатов исследования с использованием современных информационных технологий (презентация, эссе).
- Воспитание у детей ответственности в учебных делах, и адаптивности, коммуникативных умения, толерантности и самостоятельности.

Изучение материала рекомендуется изучать в течение 4 уроков:

1. Оценка начальных знаний учащихся по теме проекта. Введение в тему и её осуждение. Разделение учеников на группы, и выбор темы для информационного проекта (45 мин).
2. Выполнение практической работы (45 мин).
3. Помощь ученикам в подготовке информационных проектов(45 мин).
4. Защита информационных проектов (45 мин).

Программное обеспечение:

- текстовый редактор Microsoft Word;
- программа для созданий презентаций MS Power Point.

Методические задачи проекта:

Учащиеся должны

Знать:

1. Понятие электронных книг как документа, и как устройства;
2. Форматы электронных книг;
3. Достоинства и недостатки электронных книг;
4. Виды электронных устройств и программ для чтения.
5. Понятие электронной библиотеки.
6. Задачи, функции и классификации электронных библиотек.
7. Положительные и отрицательные стороны электронных библиотек.
8. Информацию, которую нельзя размещать в электронных библиотеках

Уметь:

1. Работать с электронными библиотеками;

2. Сравнивать, анализировать и систематизировать найденную информацию.

Иметь навыки:

3. Представлять результаты учебных информационных проектов с использованием ИКТ.

В начале проектной деятельности проводится оценка начальных знаний учащихся с использованием метода опроса и обсуждения. Тема, связанная с электронными библиотеками, довольно обширная, поэтому для лучшего понимания она был разделена на составные темы, по которым ученики должны разработать и защитить, в дальнейшем, свои информационные проекты. Для дальнейшей работы учащиеся делятся на группы, выбирают темы информационных проектов, и в дальнейшем продолжают работать в таком составе до последнего занятия.

В ходе самостоятельных исследований, направленных на выявление роли электронных книг и библиотек в современном обществе; положительных и негативных сторон электронных книг и библиотек; проблем функционирования электронных книг и библиотек учащиеся ответят на проблемные вопросы проекта:

1. Какую пользу оказывают электронные библиотеки?
2. Правомерно или нет функционирование электронных библиотек?
3. Что лучше: бумажная или электронная книга?

В соответствии с проблемными вопросами определим учебные, которые будем решать со старшеклассниками:

1. Что такое электронная книга и электронная библиотека?
2. Какие существуют цели, задачи, функции и классификации электронных библиотек?
3. Нарушают ли электронные библиотеки авторские права?
4. Какие правила существуют при скачивании электронных книг?
5. В каких форматах существуют электронные книги?
6. Какими программами и устройствами можно открыть электронную книгу?

Информационные проекты оформляются в виде презентации и эссе.

На последнем занятии проводится защита информационных проектов, где заслушиваются выступления учащихся с итогами своей работы, и рефлексия.

Практическая работа

«Кто ищет, тот всегда найдет, что почитать»

Цели:

– закрепление знаний об электронных библиотеках и поисковых систем;

– формирование алгоритма действий при поиске информации.

Задачи:

– показать возможности библиотеки в удовлетворении тематических запросов;

– определить преимущества и недостатки поиска в электронных и поисковых системах;

– активизировать на практике полученные знания;

– выполнить поиск нужной информации в разных электронных библиотеках и поисковых системах.

Ход работы

1 этап.

Выполните задания при помощи сайтов, специализирующихся на поиске электронных книг. Ответы пришлите по электронной почте, оформив по образцу (сами книги скачивать и пересылать не надо!).

Задания. Найдите книги, выбрав любой подходящий сайт, из ниже перечисленных, а также попробуйте найти свои другие аналогичные сайты (желательно без рекламы, баннеров и т.п.):

1. Айзек Азимов «Три закона робототехники»
2. Владимир Орлов «Альтист Данилов»
3. Чарльз Диккенс «Приключения Оливера Твиста»
4. Марк Твен «Том Сойер – сыщик»
5. Пушкин А.С. «Медный всадник»
6. Билл Гейтс «Бизнес со скоростью мысли»
7. Инструкцию по эксплуатации цифрового фотоаппарата «Nikon Coolpix D70»
8. Учебник по FTP с популярным изложением
9. Руководство по безопасной работе в Интернете
10. Толковый словарь терминов Интернета
11. Описание задач олимпиад по информатике с решениями.

Полезные ссылки

1. Каталог электронных библиотек Library.Ru http://www.library.ru/2/catalogs/elibs ·
2. «Чернильница» http://www.kulichki.com/inkwell/
3. Библиотека Максима Мошкова: lib.ru
4. Google книги http://books.google.com/
5. Вся компьютерная и техническая документация: www.emanual.ru
6. Студенческая библиотека ABC (электронные версии учебников): abc.vvsu.ru
7. Каталог инструкций по эксплуатации (поставка инструкций платная):www.rusmanual.ru

Образец письма

Иванов Иван, 11 класс

Результаты практической работы «Кто ищет, тот всегда найдет, что почитать».

1. Найдите книгу Аркадия и Бориса Стругацких "Улитка на склоне".

Ответ:
Книга найдена на сайте "Вся русская фантастика" (www.sf.amc.ru)
на странице: http://www.sf.amc.ru/abs/books.htm

Поиск выполнялся сначала по разделам каталога:
Писатели/Стругацкие/Творчество/Книги/
Затем на странице с помощью поисковых средств браузера по слову "улитка".
На странице предложен вход в раздел для чтения книги в режиме онлайн, а также предложено копирование ZIP-архива размером 176 килобайт.

2 этап.

Обсуждаем результаты поиска.

– С помощью какой системы Вы быстрее нашли нужную информацию?

– А чья информация обширнее, может быть, подробнее?

– Какому поиску или электронной библиотеке отдадите предпочтение?

– Есть ли недостатки в проведении такого поиска?

Предполагаемый итог работы:

– Ученики делают выводы и отмечают, что:

– Информация в электронных библиотеках ищется быстро и в большом количестве;

– Попадались сайты с нежелательной информацией;

– Чтобы найти интересующее издание не нужно открывать каждый сайт, а можно использовать для этого поисковик.

Вопросы для учеников:

1. Что Вы узнали в ходе данного проекта об электронных книгах, об электронных библиотеках?
2. Понравилось ли Вам работать в группах?
3. Что Вам особенно запомнилось или понравилось?
4. Что Вам не удалось или было трудно выполнять?
5. В ходе проекта Вы научились…
6. Пригодятся ли Вам знания и умения, приобретенные в рамках этого проекта?
7. Ваши пожелания или замечания…

Материалы к проекту

Опрос

Ребята, пожалуйста, заполните представленную таблицу.

За данную таблицу никаких оценок не ставиться.

Будьте предельно честны в своих ответах и не обращайтесь к помощи Интернет.

Таблица активирует предварительные знания учащихся, выясняя, что они уже знают о теме проекта.

Знания до начала проекта.

Внимательно посмотрите на перечень вопросов. В столбце №2 ответьте на вопросы, так как Вы думаете, своими словами. Время на выполнение ~ 4-5 минут.

Желаю успехов!

Вопрос	Ответ
1. Что Вы знаете об электронной книге? (понятие, область применения, виды и т.д.)	
2. Что Вы знаете об электронных библиотеках? (понятие, виды и т.д.)	
3. Законно или нет существование электронных библиотек? (да / нет.) Почему? Ответ обосновать.	

Обсуждение в группах

Класс: 11

Тема урока: «Электронные книги»

Цель урока:

- формирование общего представления об электронных книгах;
- побудить желание заниматься проектной деятельностью;
- развитие творческого мышления;
- развитие умений логического рассуждения;
- воспитание активной позиции и культуры отношений в коллективе и группе;

Метод обучения: обсуждение с целью ознакомления с новым материалом.

Основной структурный элемент урока: диалог.

Дополнительные структурные элементы: обмен информацией и её коллективный анализ, обмен репликами, формулирование выводов.

Ожидаемые результаты:

1. учащиеся получат представление об электронных книгах;
2. узнают о преимуществах электронной книги над бумажной;

Время на выполнение: 15- 20 минут.

Ход обсуждения

1 этап.

1. Учащиеся делятся на группы по личному предпочтению.

2. Перечисляют 4-5 мнений по вопросу: *«Что лучше бумажная книга или электронная?»*.

3. Обсуждают в группе вопрос и заполняют таблицу.

электронная	бумажная

4. Каждая группа представляет свои ответы другим, аргументируя свою точку зрения.

2 этап.

1. Учащиеся обсуждают вопрос: *«Вытеснит ли электронная книга бумажную?»*.

2. Приводят свои мнения, и опровергают или присоединяются к мнению других участников дискуссии в процессе непосредственного общения.

Темы информационных проектов

Данные темы предлагаются учащимся, по которым проводятся исследовательские работы в группах. Перечень тем рекомендован для рассмотрения, но при возникновении у учеников новых тем и идей для проведения исследования, может меняться при согласовании с руководителем проекта. Данные задачи исследований предлагаются ученикам в помощь, о том, что им нужно отразить в исследовательских работах.

Каждая группа учеников должна выбрать тему для исследования и записаться в таблицу.

Тема	Задачи исследования
Электронная книга и её перспективы	Понятие электронной книги. Форматы электронных книг. Положительные и отрицательные стороны электронных книг. Роль электронных книги в современном обществе (эссе). Получить знания об электронной книге как о документе; Обобщить и систематизировать накопленную информацию; Определить и обосновать место электронной книги в современном обществе (эссе).
E-Book как устройство для чтения	Понятие электронной книги как устройство. Программы для чтения электронных книг. Виды устройств для чтения электронных книг. Популярность устройств, которые используются для чтения электронных книг (эссе.) Получить знания об электронной книге как об устройстве; Обобщить и систематизировать накопленную информацию; Обосновать популярность устройств для чтения электронных книг (эссе).

Библиотек будущего	Понятие электронной библиотеки. Задачи, функции и классификации электронных библиотек. Положительные и отрицательные стороны электронных библиотек. Роль электронных библиотек в современном обществе (эссе). Получить знания об электронной библиотеке; Обобщить и систематизировать накопленную информацию; Выяснить какую роль играют электронные библиотеки в современном обществе (эссе).
Закон и электронные библиотеки	Выяснить правомерность существования электронных библиотек. Определить какую информацию нельзя размещать в электронных библиотеках. А также выяснить есть ли законы, регулирующие деятельность электронных библиотек.

Руководство для создания презентации:

Наличие картинок обязательно!

Слайд 1. (Титульный)

- единый стиль оформления;
- единый стиль шрифта;
- наличие слов Информационный проект по теме «…»;
- в правом нижнем углу Выполнили: фамилии и имена участников, класс.

Слайд 2. Цель, гипотеза проекта.

Слайд 3. Задачи проекта.

Слайд 4. Заголовок слайда: Главные понятия.

Слайд 5. Немного истории. (когда, как, где и т.п.).

Слайд 6. и далее согласно плану раскрытия тем.

Последний слайд. Вывод!

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ПО ИНФОРМАТИКЕ И ИКТ

Конспект урока «Технические характеристики и особенности современных роботов»

Автор Е.А. Чернева, руководитель М.В. Романова

Время урока: 45 минут.

Тип учебного занятия: комбинированный.

Цели урока:

Образовательная – ознакомить обучаемых со современными моделями робототехники, их техническими характеристиками.

Воспитательная – Развитие у детей памяти, логического мышления, формирование умения правильно излагать свою мысль

Развивающая – Воспитание информационной культуры, самостоятельно находить материал для изучения, поддержание интереса к информатики и формирование у обучаемых умения работать в коллективной группе и грамотное оформление докладов и презентаций

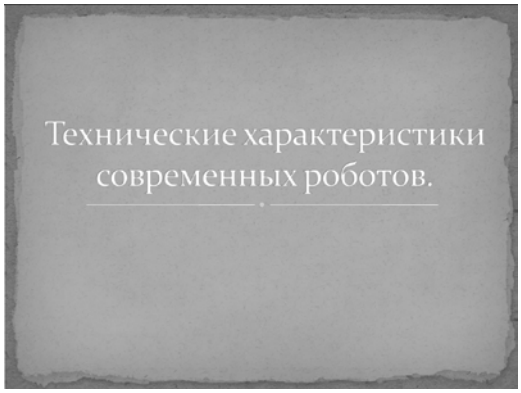
Оборудование урока: Доска мел, компьютер, пазл, презентация.

Технологическая карта урока

1.	Название темы.	«Технические характеристики и особенности современных роботов».
2.	Дидактическая цель темы	Ознакомить с современными моделями роботов.
3.	Тип.	Рассказ, беседа, игра.
4.	Знания, необходимые для изучения темы	Знать этапы развития роботов и робототехники.
5.	Умения, необходимые для изучения темы	Умение работать в программе MS Word.
6.	Методы проверки необходимых ЗУН	Игра «Собери паззл»
7.	Формируемые знания (что должны знать по окончании изучения темы)	Знания современных роботов и их характеристики.
8.	Формируемые умения (что должны уметь по окончании изучения темы)	Уметь работать более углубленно в MS Word.
9.	Планируемый уровень обученности	средний
10.	Методы (формы) проверки достижимости цели темы.	Беседа.

Ход урока:

1. Приветствие обучаемых формулировка целей урока (3 минуты)



(слайд 1) Здравствуйте, сегодня на уроке мы с вами познакомимся с техническими характеристиками современных роботов, такие как: Робот i-SOBOT, Plen, Robosapien V2, Дегустатор, AR-100 «Добрыня». Итак, запишем тему сегодняшнего урока «Технические характеристики и особенности современных роботов»

2. Лекция по теме урока (30 минут)

(слайд 2) Первый робот, с которого мы начнем – это робот i-SOBOT самый маленький гуманоидный робот, который запущен в массовое производство.

Технические характеристики:

- встроенный набор выражений и действий (порядка 200),
- встроенные голосовые команды (знает порядка 180 слов),
- может быть перепрограммирован под ваши предпочтения,
- высота составляет 165 мм,
- вес 350 граммов.

(слайд 3) Второй робот это робот Plen способен самостоятельно вставать на свой скейтборд и двигаться без посторонней помощи.

- высота 23 см
- вес около 700 граммов

Робот имеет 18 степеней свободы и способен воспринимать некоторые команды с телефона при помощи интерфейса Bluetooth

(слайд 4) Третий робот это Robosapien V2 Один из самых интеллектуальных роботов полностью функциональный робот с дистанционным управлением, воспринимающий голосовые команды!

Основные возможности робота:

- многоуровневая реакция на внешние воздействия: людей и другие объекты, свет, звук и прикосновения;
- естественные движения тела отличаются гибкостью;
- Robosapien V2 комментирует подаваемые с пульта команды, реагирует голосом и движением на прикосновения и перемещения объектов, попадающих в его поле зрения;
- робот распознает цвета: синий, красный, зеленый, телесный;
- Robosapien V2 умеет говорить на 7 языках (нет русского в этом числе);
- робот может жестикулировать кистью;
- реалистичные повороты головы в двух плоскостях с «живым» взглядом голубых глаз;
- 100 функций программирования;
- 4 демо-режима (в том числе «танцы»);
- 4 основных режима программирования.

(слайд 5) Четвертый робот это Дегустатор В 2006 г. специалисты лаборатории NEC System Technologies создали робота-дегустатора. Спектрометр, встроенный в руку робота, определяет содержание воды, «узнаёт» белки и другие вещества. Благодаря этому, он может распознавать сыры, фрукты, сорта вина (причем определять его подлинность прямо через стекло бутылки), подбирать к вину подходящую закуску и наоборот. Весь процесс занимает около 30 секунд.

(слайд 6) Пятый робот AR-100 «Добрыня». Именно с этой моделью мы будем работать. Поэтому остановимся на нем более подробно. Андроид серии AR-100 «Добрыня» − первый серийный отечественный, универсальный андроидный робот. Выпущен в июне 2007 года. Создан на основе двухлетнего опыта поставок и изучения ведущих зарубежных аналогов. Разработан специально с учетом специфики эксплуатации, задач и потребностей учебных и исследовательских заведений.

При разработке конструкции особое внимание уделялось таким факторам, как:

- общая технологичность;
- доступная элементная база;
- высокая надежность и ремонтопригодность;
- расширенная функциональность;
- оперативная техническая поддержка;
- дешевизна и доступность отечественному пользователю.

При этом учтены различные недостатки зарубежных моделей. В частности, улучшено размещение датчиков исполнительных механизмов, усилены сервоприводы, увеличены прочностные характеристики конструкции.

Быстрый, 32х-битный процессор и обилие (512Кб, с возможностью расширения до 1Гб) встроенной памяти позволяют легко реализовать голосовые и прочие сервисные функции. Все конфигурации, включая базовую, снабжены беспроводным интерфейсом Bluetooth.

Усиленный алюминиевый каркас с высокопрочным полимерным покрытием гарантирует длительную эксплуатацию моделей без потери товарного вида.

Конструкция андроидных роботов серии AR-100 непрерывно совершенствуется.

В результате возможности AR-100 даже в базовой конфигурации значительно превышают параметры моделей ведущих мировых производителей.

Роботы серии AR-100 также могут реализовываться в составе программно-аппаратного комплекса «Андромеда», который разработан в июне 2005 года − уникальное средство обработки систем искусственного интеллекта, технического зрения, сенсорики, взаимодействия робогрупп. Данный программно-аппаратный комплекс дает возможность управлять шестерыми роботами с одного персонального компьютера. Он выполняет синхронизацию движений, что позволяет всем роботам выполнять различные поставленные задачи одновременно. В качестве управляющей системы могут использоваться персональный компьютер, ноутбук, или КПК. Передача данных осуществляется посредством беспроводного интерфейса Bluetooth. «Андромеда» совместима с моделями AP-100, AP-101, ROBONOVA-1. Создание такого комплекса стало одним из главных шагов в установлении отраслевых стандартов отечественной робототехники.

Технические характеристики:

Микроконтроллер МК-65

- Количество управляемых сервоприводов − 24
- Память − 512 Кб
- Количество портов I/O − 40
- Максимальное количество базовых операций − 128

Сервопривод

- Поворот − 176 º
- Крутящий момент − 14 кг/см
- Скорость − 60º/ 0,2 сек.
- Напряжение питания − 6-7,4 V
- Время автономной работы − 60 мин.
- Передача данных − Bluetooth V1.2

Габариты (мм):

- Высота: 350 мм
- Ширина: 185 мм
- Длина: 105 мм
- Вес − 1,5 кг [8]

Что уже умеют человекоподобные механизмы:

- ходить, бегать, подниматься по лестницам, перепрыгивать препятствия высотой до полуметра;
- танцевать, ходить на лыжах, играть в футбол, кидать дротики;
- играть в шахматы, на музыкальных инструментах, дирижировать оркестром;

- делать уколы и хирургические операции;
- распознавать и синтезировать человеческую речь, вести беседу, пожимать руки, улыбаться;
- убираться по дому, выполнять функции секретаря, следить за детьми и животными, смешивать коктейли, подавать на стол;
- охранять дом, драться с другими механизмами.

3. Закрепление пройденного материала (Игра «Собери пазл») (10 минут)

(слайд 7) А теперь для закрепления материала сыграем в игру «Собери пазл». У вас на каждом компьютере есть файл «Пазлы», который находиться в «Рабочая папка». Вам необходимо составить фрагменты рисунка, путем их перетаскивания, ответить на вопрос.

4. Подведение итогов, выставление оценок (2 минуты)

Итак, сегодня на уроке мы познакомились с современными моделями роботов с их техническими характеристиками. Познакомились более углубленно с моделью робота AR-100 «Добрыня», именно этих роботов мы будем программировать и создавать групповые танцы.

За работу на уроке получают оценки:

1._____

2_____

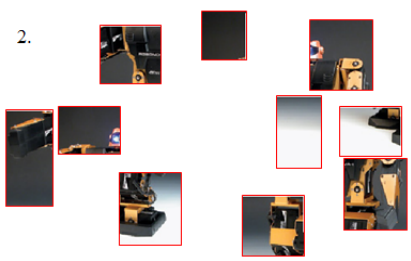
3._____ и т.д.

Материалы для проведения урока:

Паззлы

Составь фрагменты, получишь картинку робота.

Как он называется?



3.

Какую интересную функцию выполняет этот андроидный робот?_____

Викторина по информатике «Умники и Умницы»
для учащихся 8-9 классов
Автор Котельникова Е.Н., руководитель: Чернова Е.В.

Цель – в игровой соревновательной форме проверить знания и основы владения терминологией по темам: «Аппаратное обеспечение компьютера» и «Действия с информацией».

Задачи:

1. Воспитательная: воспитание умения работать в команде, уважения к сопернику, воспитание чувства ответственности;

2. Учебная: теоретическое повторение ранее изученного материала по темам: «Аппаратное обеспечение компьютера» и «Действия с информацией»;

3. Развивающая: развитие познавательного интереса, логического мышления, творческой активности, умения грамотно излагать свои мысли.

Оборудование:

- Доска;
- Компьютер;
- Мультимедийный проектор;
- Презентация, демонстрирующая тексты вопросов и заданий;
- Карточки с заданиями;
- Рабочие столы для игроков;
- Стол для жюри;
- Секундомер;
- Бумага для вычислений для игроков и для жюри;
- Листы ответов для жюри;
- Ручки;
- Призы, грамоты.

План проведения викторины:

1. Организационный момент;
2. Интеллектуальная разминка (конкурс «Веришь, не веришь»);
3. Блиц-опрос (конкурс «Торопись, да не ошибись»);
4. Замена буквы (конкурс «Заменишь букву, получишь новое слово»);
5. Брейн-ринг (конкурс «Вопрос – ответ»);
6. «Забавная пауза»;
7. Поиск слов в предложении (конкурс «Ответ ищи в тексте»);
8. Конкурс «Крылатые слова» и информатика;
9. Терминологический конкурс (конкурс «Третий лишний»);
10. Подведение итогов

Предварительная подготовка:

Разделение учащихся на 2 команды, выбор капитанов и названия команд. На доске чертится таблица для оценивания команд:

№ конкурса	**1 команда «_____»**	**2 команда «_____»**
1		
2		
3		
…		
Итого баллов:		

Правила игры:

Игра проходит в форме соревнования между двумя командами, задача которых – набрать максимальное количество баллов, которые

начисляются за правильное выполнение задания и тактичное поведение во время игры. Ведущий – учитель может влиять на ход игры, участвовать в дискуссии, подавая реплики и задавая вопросы. По окончании игры подсчитываются общие баллы, набранные командами за всю игру. Победителем становится команда, набравшая максимальное количество баллов.

1. «Веришь, не веришь»

Произносится поочередно для каждой команды утверждения, а участники команд должны согласиться с ним или не согласиться. За каждый правильный ответ команда получает 1 балл.

1) Верите ли вы, что элементной базой ЭВМ второго поколения являются электронные лампы? (*Нет – транзисторы*)

2) Верите ли вы, что были первые модели персональных компьютеров, у которых отсутствовал жесткий диск? (*Да)*

3) Верите ли вы, что создателем языка программирования Паскаль является Блез Паскаль? (*Нет, его создателем был Никлаус Вирт*)

4) Верите ли вы, что компьютерные вирусы появились в 2000 году? (*Нет, первый в мире компьютерный вирус «родился» в 1981 году*.)

5) Верите ли вы, что в Великобритании есть город Винчестер? (*Да*)

6) Верите ли вы, что для доступа к свойствам объектов используется контекстное меню? (*Да*)

7) Верите ли вы, что основным элементом управлением рабочего стола является кнопка Пуск? (*Да*)

8) Верите ли вы, что одной из главной функций компьютера является передача информации? (*Нет – обработка*)

2. «Торопись, да не ошибись»

Каждой команде поочередно задаются вопросы, на которые нужно ответить не раздумывая. каждый правильный ответ команда получает 1 балл.

1) Устройство ввода в ЭВМ информации непосредственно с листа (*Сканер*)

2) Базовым элементом растровой графики является? (*Точка)*

3) Перечень файлов. (*Каталог*)

4) Пересылка данных с носителя данных в основную память *(Загрузка)*

5) Строго определенная последовательность действий при решении задачи *(Алгоритм*)

6) Базовым элементом векторной графики является? (*Линия*)

7) Минимальная единица измерения кол-ва информации (*Бит*)

8) Начинающий пользователь (*Чайник*)

9) Специальная программа, выполняющая нежелательные для пользователя действия на компьютере (*Вирус*)

10) Назовите клавиши удаления символов (*Delete, Backspace*)

3. «Заменишь букву, получишь новое слово»

(Замени одну букву и получи новое слово.)

На слайде расположены слова, в которых нужно заменить одну букву и получится новое слово, связанное с информатикой или компьютерами. За каждый правильный ответ команда получает 1 балл.

Слова для I команды:

1) Бант – *байт*

2) Болонка – *колонка (звуковая или в таблице)*

3) Кит– *бит*

4) Злак – *знак (символ, стоящий между операндами в арифметическом или логическом выражении)*

5) Ком – *код (число в системе условных обозначений символов)*

Слова для II команды:

1) Блик – *блок (системный)*

2) Нависание – *зависание (особое состояние компьютера)*

3) Пробег – *«пробел» (название клавиши)*

4) Профессор – *процессор*

5) Риск – *диск*

4. «Вопрос – ответ»

На слайде располагаются клетки с числами 1, 2, 3 (стоимость вопроса в баллах). Участники команд по очереди делают щелчок мышью по соответствующей клетке (на слайде появляется вопрос). В случае правильного ответа команда получает соответствующее количество баллов. При любом ответе ход переходит к команде-сопернице.

На размышление команде дается до 10 секунд (для вопросов сложностью 1 бал), 20 секунд (для вопросов сложностью 2 балла) или 30 секунд (для вопросов сложностью 3 балла). По мере выбора клеток командами они удаляются из рядов.

Вопросы:

1 балл

1) Какая система обеспечивает работоспособность компьютера? (*Операционная*)

2) Взломщик компьютерных программ (*Хакер*)

3) Как называется человек - фанат компьютерных игр (*Геймер*)

4) Что больше: 1024 Кб или 1 Мб? (*Величины равны*)

2 балла

1) В какой стране впервые появилось слово «компьютер» (*Англия. В Англии компьютером раньше называли человека, чья деятельность была связана с расчетами)*

2) Назовите клавиши, которые работают всегда в прижатом состоянии, в комбинации с другими клавишами. (*Shift, Ctrl, Alt*)

3) Необычайно богатая цветовая палитра современных компьютеров (более 16 миллионов оттенков) получается смешением, каких трех основных цветов? (*Красного, зеленого и синего*)

4) Как еще называют внешние устройства компьютера? (Периферийные)

3 балла

1) Изображаемый на экране список объектов, из которых пользователь выбирает необходимый вариант (*Меню*)

2) На экране изображены символы, которые нельзя включать в имя файла, двух символов недостает, каких? \ : ? “ < > | (/ *)

3) Нужно переставить буквы так, чтобы получилось слово, причём все буквы должны быть использованы. Нртиеетн (Интернет)

4) Нужно переставить буквы так, чтобы получилось слово, причём все буквы должны быть использованы. Счертивен (Винчестер)

5. «Забавная пауза»

Чтобы участники викторины немного отдохнули, сделаем маленькую паузу и послушаем забавные стишки о том, как не нужно себя вести на уроках информатики.

Если ты случайно вспомнишь,
Что вас где-то ждёт учитель,
И уже минут пятнадцать продолжается урок,
То не нужно идти шагом,
Так теряешь только время,
Лучше будет пробежаться - так полезней и быстрей.

Если на клавиатуре
Западает пара клавиш,
Это значит вы - ударник
И вообще герой труда.
Незаметно поменяйтесь
Ей с бездельником - соседом
У таких клавиатуры
Не стареют никогда!

Если вдруг твоя машина
Не работает, как надо,
Ты по материнской плате
Сильно стукни кулаком.
Не поможет – бей кувалдой,
Дай ногой по монитору...
И скажи лишь педагогу:
«Она первой начала!»

Если грязь с твоих ботинок
Осыпается кусками,
То тебе совсем не нужно
Обувь чистую нести.
Чем грязней будут ботинки,
Тем рассерженней учитель,
Тем быстрее тебя выгонят домой.

Если ты на перемене
Не успеешь пообедать,
То закончить можно в классе,
Молча слушая урок.
Если ты раскрошишь булку
Или стол измажешь маслом,
То залей всё это чаем – легче будет отмывать.

6. «Ответ ищи в тексте»

В приведенных текстах некоторые идущие подряд буквы нескольких слов образуют термины, связанные с информатикой и компьютерами. Найдите эти термины. За каждый найденный термин команда получает 1 балл. Пример: «Этот процесс орнитологии называют миграцией» - *процесс ор*нитологии – процессор.

Предложения для I команды:

1) Потом они торжествовали и радовались, как дети.

Ответ: Монитор. (потоМ ОНИ ТОРжествовали).

2) Река Днепр интересна тем, что на ней имеются несколько гидроэлектростанций.

Ответ: Принтер. (ДнеПР ИНТЕРесна).

3) По просьбе хозяина квартиры мы шкаф сдвинули в угол.

Ответ: Мышка. (МЫ ШКАф).

4) Этот старинный комод ему достался в наследство от бабушки.

Ответ: Модем (коМОД ЕМу).

Предложения для II команды:

1) Его политический курс ориентировался на либеральные идеи.

Ответ: курсор (КУРС Ориентировался).

2) Порядок у Менташина в квартире был не ахти какой.

Ответ: документ (ПоряДОК У МЕНТашина).

3) И только уже будучи на пароме, Нюра вспомнила об этом.

Ответ: меню (пароМЕ, НЮра).

4) Только после этого Митя понял, где находится на диске так называемая «таблица размещения файлов».

Ответ: дискета (ДИСКЕ ТАк).

7. «Крылатые слова» и информатика

Будут названы пословицы, поговорки, цитаты из известных литературных произведений и т. п. Для каждого из этих «крылатых слов» будут также предложены три понятия, связанные с компьютером и информатикой. Необходимо выбрать понятие, которое больше всего соответствует названным «крылатым словам». За каждый найденный термин команда получает 1 балл.

1. «Лебедь рвется в облака, Рак пятится назад, а Щука тянет в воду».

a) Использование элементов компьютера с различным быстродействием.

b) Использование компьютера с процессором Intel Pentium II с винчестером вместимостью 40 мегабайт.

c) Несколько программистов разрабатывают одну большую программу, не согласовывают программы между собой.

2. «Возмутитель спокойствия».

a) Звуковой сигнал на компьютере.

b) Антивирусная программа.

c) Компьютерный вирус.

3. «А все-таки она вертится!»

a) Дискета.

b) «Мышь».

c) Системная шина.

4. «Видит око, да зуб неймет».

a) Ошибка в программе.

b) Скрытый файл.

c) Антивирусной программой обнаружен новый вид вируса.

5. «Меньше не бывает».

a) Ноль

b) «Пустой» цикл.

c) Бит.

6. «Что имеем - не храним, потерявши - плачем».

a) Локальная переменная.

b) Скрытый файл.

c) Удаленный файл, у которого отсутствует резервная копия.

8. «Третий лишний»

Для каждого из выделенных терминов приведены три определения, одно из которых не соответствует термину. Необходимо это указать

1. Винт – это…

a) Крепежная деталь;

b) Один из инструментов в графическом редакторе;

c) Жаргонное название жесткого магнитного диска

2. Дорожка – это…

a) специально устроенная дистанция для бега, плавания и т.п.;

b) участок магнитного диска;

c) часть экрана компьютера в текстовом редакторе

3. Иголка – это…

a) элемент матричного принтера;

b) элемент дисковода гибких дисков;

c) элемент швейной машины

4. Порт – это…

a) устройство для подключения внешних устройств к компьютеру;

b) точка в программе для вызова другой программы;

c) место для стоянки и разгрузки судов

5. Путь – это

a) направление, маршрут движения;

b) перечисление всех папок, в которые вложен файл;

c) указание способа перехода от одного оператора программы к другому

6. Ярлык – это…

a) отметка в некотором месте программы, с помощью которой можно перейти в это место;

b) значок на экране, щелкнув мышью на котором можно открыть некоторую программу, документ или папку;

c) листок с наименованием товара и другими сведениями

Подведение итогов:

Жюри подсчитывает баллы.

Пока жюри ведет подсчет баллов, можно обсудить проведенное мероприятие. Ученикам для выявления результативности внеклассного дела предлагается завершить ряд фраз. Желательно, чтобы каждый ученик завершил хотя бы одну фразу, так как их ответы позволят учителю сделать выводы насколько и как ученик был вовлечен в викторину, над какими вопросами предстоит еще поработать.

Например, при проведении рефлексии можно предложить ученикам завершить следующие фразы:

- Среди пройденных конкурсов мне особенно понравился…;
- Во время занятия я приобрел…;
- Мне хотелось бы еще спросить…;
- Я испытывал(а) трудности…;
- Меня удивило…;
- Я приобрел/ я научился…;
- Я почувствовал(а), что…
- У меня получилось…

После обсуждения дать слово жюри для объявления результатов и награждения команд грамотами (1 и 2 место).

Интерактивный урок «Насилие в Интернет. Киберпреступность и киберэкстремизм»

Автор А.О. Виниченко., руководитель: Е.В.Чернова

Аннотация: Проведение интерактивного урока представляет собой комплекс связанных между собой мероприятий, а также предлагает разнообразные формы деятельности, способствует личностному развитию обучающихся. Нами был разработан интерактивный урок на тему «Насилие в Интернет. Киберпреступность и киберэкстремизм», для студентов первого и второго курсов, направления Бизнес информатика и Прикладная информатика института энергетики и автоматизированных систем, с целью привлечения внимания студентов, развития их креативного и логического мышления, а также с целью сплочения коллектива.

Цель: Освоение студентами темы «Насилие в Интернет. Киберпреступность и киберэкстремизм».

План проведения проекта:

1. Дискуссия в стиле телевизионного ток-шоу (Panel Debate);
2. Интеллектуальная игра «Что? Где? Когда?» на тему «Разновидности насилия в Интернет»;
3. Фотоэкстрим на тему «Насилие в Интернет».

Инструкция для организатора урока «Насилие в Интернет. Киберпреступность и киберэкстремизм»

Перед началом урока необходимо ознакомить участников с правилами проведения урока.

1. Группа разбивается на команды. Количество участников в команде должно равняться 5 или 6 (равнее количество мальчиков и девочек).

2. Ведущему необходимо выдать участникам шаблон заявки на участие в игре, заявку заполняет капитан от всей.

3. Победителя необходимо выбирать по количеству набранных баллов. На втором и третьем этапе урока будет своя команда – победитель.

Подробное описание проведения урока

1. Дискуссия в стиле телевизионного ток-шоу (Panel Debate)

Эта форма дискуссии совмещает в себе преимущества лекции и дискуссии в группе.

Группа из 3-5 человек (экспертов) ведет дискуссию на выбранную тему в присутствии остальных участников (по одному участнику из каждой команды).

Зрители (остальные участники команд) вступают в обсуждение позже: они высказывают свое мнение или задают участникам вопросы.

Не следует забывать, что основные участники обсуждения должны быть достаточно компетентны в данной области и хорошо подготовлены к конкретной беседе. Важно также, чтобы личные качества основных действующих лиц не отвлекали внимания от темы дискуссии и чтобы все участники имели равную возможность высказать свою точку зрения (выступление не должно продолжаться более 3-5 минут).

Ведущий следит за тем, чтобы участники дискуссии не отклонялись от заданной темы. Продолжительность дискуссии не должна превышать 1,5 часа.

Предварительно:

1. Отберите экспертов за день до проведения дискуссии (по одному эксперту от каждой команды). Попросите экспертов подготовиться к краткому выступлению по теме (2-3 минуты), подготовить справочную информацию.

2. За день до проведения дискуссии попросите всех зрителей подготовить вопросы к экспертам и продумать собственную позицию по теме дискуссии.

3. Организуйте аудиторию по типу студии: зрители размещаются полукругом по отношению к экспертам.

Ход дискуссии

1. Представьте тему дискуссии (Насилие в Интернет.) Представьте экспертов.

2. Сообщите правила проведения ток-шоу:

Правила проведения:

- Сначала эксперты высказываются по проблеме (2–3 минуты каждый);
- Чтобы получить слово надо поднять руку;
- Слово зрителям предоставляет ведущий;
- Зрители могут выступать со своим мнением или задавать вопросы отдельным или всем экспертам (не дольше 1 минуты);
- Ведущий имеет право задавать вопросы;
- Ведущий имеет право прервать выступающего, превысившего лимит времени;
- Эксперты отвечают на вопросы как можно конкретнее и короче;

3. Предоставьте слово экспертам.

4. Попросите зрителей выступать и задавать вопросы. Следите за временем.

5. Попросите записать вопросы, на которые не хватило времени, и передайте их экспертам.

6. Поблагодарите экспертов и зрителей.

7. Проведите подведение итогов по содержанию дискуссии. В конце дискуссии каждый из присутствующих должен знать ответы на вопро-

сы: Что такое насилие в Интернет? Какие существуют разновидности насилия в Интернет? Как защититься от него? Что предпринимать, если вы подверглись его воздействию?

2. Интеллектуальная игра «Что? Где? Когда?» на тему «Разновидности насилия Интернет».

Подготовка к игре

Заранее формируются команды учащихся из 5 - 6 человек каждая (в команде равное количество девочек и мальчиков).

Необходимо подготовить секундомер,

Бланки для ответов находятся в приложении Б (распечатываются на каждую команду)

Звуковое сопровождение.

Условия игры:

На игре 15 вопросов.

За каждое правильно отгаданное слово команде дается 1 балл, за неправильный ответ снимается 0,5 балла.

На размышление дается 1 минута.

Ход игры

Музыкальная заставка.

Ведущий:

Добрый день, уважаемые зрители! Сегодня у нас интеллектуальная игра «Что? Где? Когда?». Против команд знатоков играю я (ФИО ведущего). За первым столом команда знатоков в составе …….. За вторым столом команда следующих игроков……. За n-м столом команда следующих игроков…… Попросим под аплодисменты зрителей команды знатоков занять свои места.

Для вас, знатоки, подготовлено 15 вопросов и всего 30 минут на саму игру. Сегодня вам потребуются знания по теме «Разновидности насилия в Интернете» Пожелаем Вам успеха!

1 вопрос. Нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: кибербуллинг.

2 вопрос. Повторяющиеся оскорбительные сообщения, направленные на жертву (например, сотни sms на мобильный телефон, постоянные звонки), с перегрузкой персональных каналов коммуникации.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: нападки.

3 вопрос. Скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: киберпреследование.

4 вопрос. Вредоносная программа, распространяемая людьми (в отличие от вирусов и червей, которые распространяются самопроизвольно).

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: троян.

5 вопрос. Обмен короткими эмоциональными репликами между двумя и более людьми, разворачивается обычно в публичных местах Сети.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: флейминг.

6 вопрос. Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: фишинг.

7 вопрос. Любые видеоролики с записями реальных сцен насилия.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: хеппислепинг.

8 вопрос. Исключение из группы людей.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: остракизм.

9 вопрос. Доведение до самоубийства путем психологического насилия.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: буллицид.

10 вопрос. Незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: киберпреступность.

11 вопрос. Одна из многих видов киберугроз, которые вызывают всеобщую озабоченность.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: киберэкстремизм.

12 вопрос. Получение персональной информации и публикация ее в Интернете или передача тем, кому она не предназначалась.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: надувательство.

13 вопрос. Распространение оскорбительной и неправдивой информации.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: клевета.

14 вопрос. Массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений (информации) лицам, не выражавшим желания их получать.

Гонг.

По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: спам.

15 вопрос. Размещение в Интернете (на форумах, в дискуссионных группах, блогах и др.) провокационных сообщений с целью вызвать флейм, конфликты между участниками, взаимные оскорбления и т. п.

Гонг.

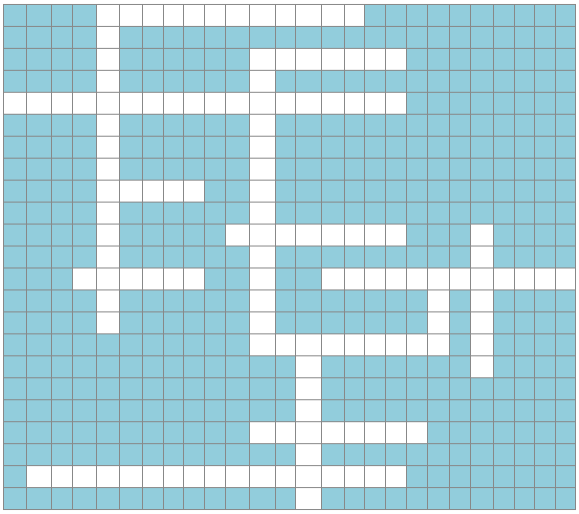
По истечении минуты звук гонга. По истечении минуты команда сдает бланк с ответами.

Ведущим озвучивается правильный ответ.

Ответ: троллинг.

Далее из всех отгаданных слов командам предлагается составить кроссворд. На составление кроссворда отводится 30 минут. За составленный кроссворд команда получает максимум 15 баллов (за каждое слово в кроссворде).

Пример кроссворда:



Подведение итогов по игре:

Подсчитываются баллы команд. Награждается лучший участник каждой команды и команда – победитель.

3. Фотоэкстрим на тему «Насилие в Интрнет»

Фотоэкстрим — безбашенная и весёлая игра для больших и шумных команд. Команды получают задания. В них подробно описано, что именно необходимо сфотографировать. Как правило, это какая-то необычная ситуация.

Что потребуется для игры:

- Фотоаппарат (не ниже 3 Мегапикселей);
- Маркеры, краски;
- Желание весело провести время;
- Отсутствие комплексов в себе и в людях, которых вы будите снимать;
- Море энергии и позитива;

- Подручные материалы;
- Фантазия.

Оценивание:

Побеждает команда, которая наберет максимальное количество баллов.

Максимальное количество баллов за все задания с бонусами - 55.

Та команда, которая выполнит все задания быстрее других команд, получает дополнительные 10 баллов.

Самым главным критерием считается соответствие снимка предъявляемым требованиям.

Время проведения игры: игра проводится в субботу, длительность от 4 до 6 часов.

Вначале игры каждая команда разрабатывает/выбирает свой логотип, который должен присутствовать на каждой фотографии (на это не дается дополнительного времени, все происходит в процессе игры). Логотип может быть нарисован на бумаге или же им может стать одинаковая вещь, которая будет присутствовать у всех членов команды (это может быть все, что угодно, за исключение одинаковых элементов одежды).

Далее команды начинают выполнение предложенных заданий. Как только команда выполнила все задания, она должна вернуться на точку начала игры и сдать распечатанные фотографии.

Задание №1 «Свобода»

Сделайте фотографию, на которой видно всю команду, одновременно находящуюся в воздухе (никакие части тела не касаются никаких жёстких опор). Всю команду видно на фото в полный рост (+5 баллов).

Бонусы:

- привлечение 3х человек, не входящих в состав команды (+3 балла);
- Все люди на фотографии улыбаются (+1 балл).

Штрафы:

- не хватает хотя бы одного человека из команды на фотографии (-3 балла);
- отсутствие логотипа команды (-1 балл).

Задание №2 «Агрессия везде достанет»

Трое человек в туристическом походе на привале на берегу реки. У одного из них открыт ноутбук и он выглядит раздраженно (+5 баллов).

Бонусы:

- присутствие больших рюкзаков (+2 балла);
- присутствие лодки на берегу реки (+2 балла);
- присутствие костра (+3 балла).

Штрафы:

- отсутствие палатки (–1 балл);
- отсутствие логотипа команды (–1 балл).

Задание №3 «Хеппислепин»

На фото должны присутствовать подростки/студенты избивающие прохожих, тогда как другие записывают это на камеру мобильного телефона (+5 баллов).

Бонусы:

- массовость (привлечение более 8 человек (трое из которых участники команды)) (+3 балла);
- использование различные орудий избиения (+2 балла);
- в роли прохожих взрослые люди (+3 балла);
- создание реалистичности картины (использование красок для создания «побоев») (+3 балла).

Штрафы:

- привлечение детей (до 14 лет) (–5 баллов);
- отсутствие логотипа команды (–1 балл).

Здадание №4 «Кибербуллинг»

Проиллюстрируйте последствия кибербуллинга. На фото должен присутствовать расстроенный ребенок, его испуганные родители/бабушки/дедушки (+5 баллов).

Бонусы:

- ребенок одет в школьную форму (+2 балла);
- присутствует минимум 3 члена семьи (не включая ребенка) (+2 балла).

Штрафы:

- на фото отсутствует компьютер/ноутбук/телефон (–1 балл);
- отсутствие логотипа команды (–1 балл).

Задание №5 «Троллинг»

Проиллюстрируйте троллинг в интернете (+5 баллов).

Бонусы:

- изображение тролля: картинка (+1 балл) или костюм тролля (+ 3 балла).

Штрафы:

- отсутствие компьютера/ноутбука/телефона (–1 балл);
- отсутствие логотипа команды (–1 балл).

Подведение итогов по игре:

Подсчитываются баллы команд. Награждается команда – победитель.

Результаты проекта: Подводя итоги урока можно сказать, что студенты полностью освоят тему «Насилие в Интернет. Киберпреступность и киберэкстремизм», помимо того они необычно проведут свое учебное время, и коллектив станет более сплоченным.

Игра «Что важно знать, чтобы в сети не попасть»

Автор: Арапова В.В.

Цель: повторение и контроль знаний по теме «Защита информации», развитие всесторонней личности ребят, повышение их интеллектуального уровня развития

Задачи:

1. Расширить знания учащихся об информационной защите, о видах вирусов, о существующих законах о защите информации;

2. Продолжить воспитывать у учащихся чувство дружбы, формировать умение работать в коллективе.

3. Сформировать умение работать с дополнительной литературой, использовать средства ИКТ (при подготовке к игре);

Оборудование:

Компьютер, экран, проектор, компьютерная презентация, компьютерный класс.

Правила игры:

В игре принимают участие 2 команды, в каждой команде по 7 человек. Команды должны придумать название команды, девиз. Предварительно был пройден раздел «Защита информации», состоящий из уроков по темам:

«Вредоносные программы и антивирусные программы»

1. «Компьютерные вирусы и защита от них»
2. «Сетевые вирусы и защита от них»
3. «Троянские программы и защита от них»
4. «Рекламные и шпионские программы и защита от них»
5. «Спам и защита от него»
6. «Хакерские утилиты и защита от них»
7. «Защита информации от несанкционированного доступа».
8. Также были проведены практические работы по защите информации от различных видов компьютерных вирусов, настройка антивирусной программы. Данная игра проводится как урок-обобщение.

Назначаются два помощника для подготовки и проведения игры, выбирается жюри.

Продолжительность игры: 45 минут.

1. Организационный момент.

Учитель представляет участников игры. Участники объявляют свое название и девиз команды. Учитель желает им удачи игра начинается.

2. Проведение игры.

1 раунд. Разминка "Дальше, дальше!" За 30 секунд команды должны ответить на 5 вопросов. Каждый правильный ответ оценивается в 1 балл. Если команда ответа не знает, она говорит: «Дальше». Команды приглашаются по очереди.

Вопросы 1 команде.

1. Как называются вирусы, использующие для своего распространения протоколы или команды компьютерных сетей и электронной почты? (сетевые вирусы)

2. Как называются вирусы, написанные на макроязыках, заражают файлы данных? (макровирусы)

3. Как называются вирусы, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии? (вирусы-репликаторы или черви)

4. Как называются вирусы, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того вируса не имеют ни одной повторяющейся цепочки байтов? (вирусы-мутанты)

5. Как называются программы-вирусы, различными методами удаляющие и модифицирующие информацию в определённое время, либо по какому-то условию? (логические (временные) бомбы)

Вопросы 2 команде.

1. Как называются вирусы, внедряющиеся в исполняемые модули, т.е. файлы, имеющие расширения COM и EXE? (файловые вирусы)

2. Как называются вирусы, внедряющиеся в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска? (загрузочные вирусы)

3. Как называются вирусы, которые очень опасны, так как маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков? (квазивирусные или троянские программы)

4. Как называются вирусы, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска? (вирусы-невидимки или стелс-вирусы)

5. Как называются программы-вирусы, собирающие информацию и складирующие её определённым образом, а не редко и отправляющие собранные данные по электронной почте или другим методом? (шпионы)

Жюри подводят итоги 1 раунда.

2 Раунд начнем с улыбки, так как называется он «*Заморочки из бочки»*

«Заморочки из бочки» (по 5 б. за задачу + по 1 б. за быстр.) (10 мин). Сейчас вы по очереди будете доставать бочонки с номерами вопросов**.**

Заморочки.

1. Волк, коза и капуста

2. Переливашка

3. Где золотой ключик?

4. Встреча подруг

1.Волк, коза и капуста.

Один человек должен был перевести через реку волка, козу и капусту.

Но его лодка была такая маленькая , что он при каждом переезде мог взять с собой или одно животное или капусту.

Между тем волка нельзя было оставлять на берегу одного с козой, т.к. он мог ее съесть. Нельзя было так же допустить, чтобы коза оставалась одна с капустой, т.к. она могла ее съесть , как при этих условиях перевести все на другой берег?

Составьте алгоритм переправы на другой берег.

2. Переливашка

Имеются 2 кувшина ёмкостью 3 л и 8 л. Составьте алгоритм, выполняя который, можно набрать из речки 7 л . воды. (Разрешается пользоваться только этими кувшинами)

3. Золотой ключик.

Рассказывают, что черепаха Тортилла отдала золотой ключик Буратино не так просто, а вынесла 3 коробочки: красную, жёлтую и зелёную. На красной коробочке было написан: «Здесь золотой ключик»; на жёлтой – «Зелёная коробочка пуста»; а на зелёной – «Здесь сидит змея». Все надписи неверны. Где золотой ключик? *(ответ - в зелёном)*

4. Встреча подруг.

Встретились 3 подруги: Белова, Краснова, Чернова. Девочка в белом платье говорит Черновой: «Нам надо всем поменяться, а то цвет наших платьев не соответствует фамилиям». Кто в какое платье одет? *(ответ Чернова – в красном, Краснова – в белом, Белова – в черном)*

А сейчас, пока жюри проводит итоги этого гейма у нас игра со зрителями.

Жюри объявляет счет.

3 раунд «Конкурс капитанов»

За 3 минуты капитаны попытаются расшифровать тексты и объяснить способы кодирования.

Расшифровать закодированный текст и объяснить способ кодирования:

1.Поса шила ф фасе.

2. Коляманлядаля.

3. Акитамрофни.

Ответы:

1. Роза жила в вазе (способ кодирования: глухие согласные заменяются на звонкие, звонкие - на глухие)

2. Команда (способ кодирования: после каждого слога вставляется слог ля)

3. Информатика (способ кодирования: слово пишется наоборот)

4 раунд «Опознай пословицу».

Этот конкурс можно провести, используя заранее подготовленную презентацию.

За каждую отгаданную пословицу команде начисляется 1 балл. Если участник команды затрудняется дать ответ, то команде-сопернице дается шанс угадать пословицу, за что она получает дополнительное очко.

Скажи мне, какой у тебя компьютер, и я скажу, кто ты (Скажи мне, кто твой друг, и я скажу, кто ты)

Компьютер памятью не испортишь (Кашу маслом не испортишь).

Дареному компьютеру в системный блок не заглядывают (Дареному коню в зубы не смотрят)

В Силиконовую долину со своим компьютером не ездят (В Тулу со своим самоваром не ездят).

Утопающий за F1 хватается (Утопающий за соломинку хватается).

Бит байт бережет (Копейка рубль бережет)

Что из Корзины удалено, то пропало (Что с возу упало, то пропало).

Вирусов бояться – в Интернет не ходить (Волков бояться – в лес не ходить).

За одного хакера семь кандидатов наук дают (За одного битого семь небитых дают)

Всяк Web-дизайнер свой сайт хвалит (Всяк кулик свое болото хвалит).

Слово жюри

Подведение итогов

Жюри (учитель) (озвучивает результаты общего счета)

Команда-победительница награждается дипломами победителей и все участники команды получают оценку «5». Участники проигравшей команды получают оценку «4».

Мероприятие «Киберпреступления»

Автор Ращупкин А.А., руководитель: Чернова Е.В.

Описание: Кто такие киберпреступники? И что они из себя представляют? Какие виды киберпреступлений наиболее распространены в сети Интернет? И как защитить свою информацию от киберпреступников? На все эти вопросы ответит данный проект.

Цель – научить учащихся определять основные виды компьютерных преступлений, применять меры, основной составляющей которых является защита компьютеров от несанкционированного копирования и выведениях данных, а также развить коммуникативные и презентационные умения и навыки.

План проведения

1 этап: Вводное занятие. Лекция. (2 урока по 45 минут)

2 этап: Практические занятие на усвоение материала. Выполнение контрольного теста на усвоение знаний. (1 урок - 45 минут)

3 этап: Практическое занятие. Самостоятельная работа. Выполнение небольшой лабораторной работы на компьютере. Разработка презентации. (1 урок - 45 минут)

Основополагающий вопрос

Почему киберпреступник никого и ничего не боится?

Проблемные вопросы

1. Какие виды компьютерных преступлений существуют в сети Интернет?
2. Хакерство - профессиональная или преступная деятельность?
3. В чем заключается специфика борьбы с киберпреступностью?
4. Какие самые громкие киберпреступления были зафиксированы в мире?

Учебные вопросы

1. Что понимается под компьютерными преступлениями?
2. Какие виды компьютерных преступлений существуют в сети Интернет?
3. Кто такие хакеры?
4. Хакерство - профессиональная или преступная деятельность?
5. Как защитить себя от виртуальных мошенников?
6. Какую ответственность несут киберпреступники за неправомерный доступ к компьютерной информации?
7. Какие самые громкие киберпреступления были зафиксированы в мире?
8. Расследования киберпреступлений: кому это нужно?

Практическая работа по теме «Киберпреступления»

Цель работы: получение практических навыков по выявлению вредоносных программ с помощью браузера Internet Explorer.

Задание: Изучить настройки браузера Internet Explorer и установить в настройках браузера свою стартовую страницу.

Вирусные проявления бывают явными, косвенными и скрытыми. Если первые обычно видны невооруженным глазом, то косвенные и тем более скрытые требуют от пользователя проявления изрядной доли интуиции. Они часто не мешают работе, и для их обнаружения требуется знать, где и что нужно искать.

Явные проявления обычно выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие про-

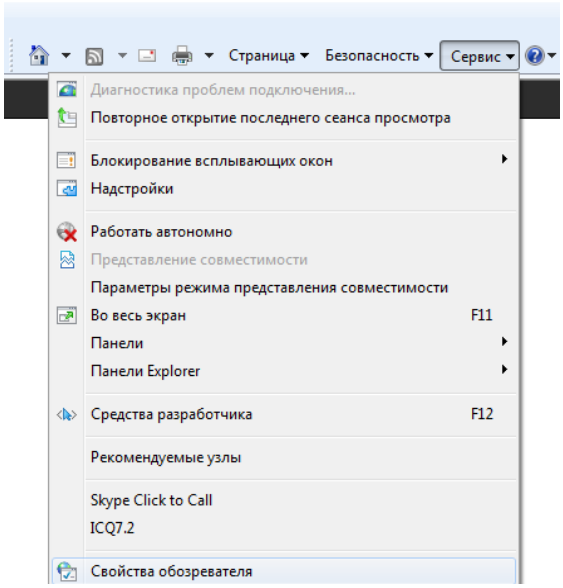
никновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также, явные проявления могут вызывать ряд троянских программ, например утилиты несанкционированного дозвона к платным сервисам.

В этом задании предлагается исследовать явные проявления вирусной активности на примере несанкционированного изменения настроек браузера. Этот механизм иногда используется для того, чтобы вынудить пользователей зайти на определенный сайт, часто порнографического содержания. Для этого меняется адрес домашней страницы, то есть адрес сайта, который автоматически загружается при каждом открытии браузера.

Порядок выполнения задания:

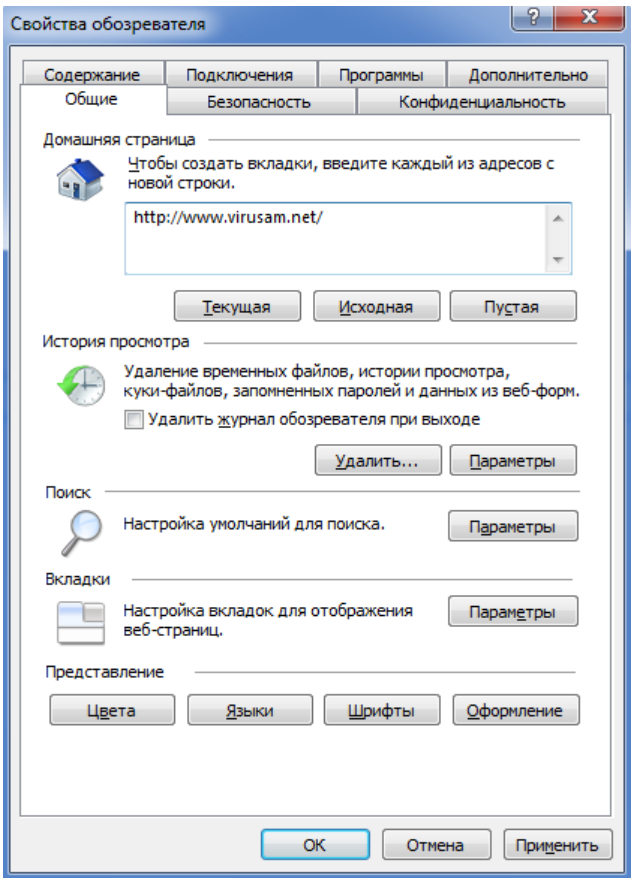
1. Необходимо открыть браузер Internet Explorer, воспользовавшись либо одноименным ярлыком на рабочем столе, либо открыв браузер в меню **Пуск - Все программы - Internet Explorer**

2. Дальше будет необходимо проверить значение параметра, который отвечает за стартовую страницу. Для этого нужно воспользоваться меню **Сервис**. Откройте его и выберите пункт **Свойства обозревателя**.



3. Адрес стартовой страницы указан сразу же в первом поле открывшегося окна **Свойства обозревателя** на закладке **Общие**. Значение этого поля совпадает с тем адресом, который был автоматически задан при открытии браузера.

Измените данное поле, введя новый адрес www.virusam.net



4. Чтобы изменения вступили в силу необходимо нажать **ОК.**

5. Завершите работу браузера, закрыв окно с Internet Explorer, а после заново откройте.

6. Убедитесь, что теперь первым делом была загружена страница, которую мы указали ранее www.virusam.net

Таким образом, если Ваш браузер начал самостоятельно загружать посторонний сайт, в первую очередь нужно изучить настройки браузера: какой адрес выставлен в поле домашней страницы.

Ряд вредоносных программ ограничиваются изменением этого параметра и для устранения последствий заражения нужно лишь исправить адрес домашней страницы. Однако это может быть только частью вредоносной нагрузки. Поэтому если Вы обнаружили несанкционированное изменение адреса домашней страницы, следует немедленно установить антивирусное программное обеспечение и проверить весь жесткий диск на наличие вирусов.

Отчет о выполнение практической работы предоставить в печатном виде.

Итоговый контрольный тест по теме «Киберпреступления»

1. Что такое киберпреступление?

1) уголовно наказуемое действие, подразумевающее несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных

2) хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием

3) рассылка электронных сообщений и спама

2. В каком году были сформулированы основные признаки компьютерных преступлений?

1) 1991

2) 1985

3) 1974

3. Укажите основные виды компьютерных преступлений

* Вариант ответа в письменном виде

4. Люди, крадущие личную информацию, в частности, номера кредитных карт

1) Хакеры

2) Кардеры

3) Фишеры

5. Ломают программную защиту от серийных номеров до аппаратных ключей…

1) Фрикеры

2) Сетевые хакеры

3) Кракеры

6. Кто такой хакер?

1) человек, систематически совершающий воровство

2) чрезвычайно квалифицированный ИТ-специалист, человек, который понимает самые глубины работы компьютерных систем

3) человек, рассылающий коммерческую, политическую и иную рекламу в сеть

7. Самый известный хакер в мире, в 1983 году проникший в глобальную сеть ARPANet?

1) Кевин Митник

2) Нешон Ивен-Чейм

3) Адриан Ламо

8. Первый российский хакер, о котором заговорили в 90-х годах прошлого века?

1) Дмитрий Голубов

2) Игорь Клопов

3) Владимир Левин

9. Самая громкая хакерская атака 2002 года?

1) Проникновение в компьютеры НАСА

2) Незаконное вторжение в серверы компании Dassault Systemes

3) Незаконный доступ во внутреннюю сеть редакции газеты New York Times

10. Чего нельзя делать, чтобы не подвергнуть себя взлому?

1) регистрировать электронную почту и посещать web-сайты

2) работать в сети без установленной на компьютере антивирусной программы

3) создавать только сложные пароли

Разработка классного часа с использованием метода проектов

Автор: Захаркин, руководитель: Лапшина В.Б.

Цели проекта:

1. Развитие навыков работы с компьютерной техникой;
2. Обучение работе с информацией: целенаправленному поиску, методам поиска и отбора информации; знакомство с систематизацией, различными способами обработки информации;
3. Развитие познавательного интереса, творческой активности, умения излагать мысли;
4. Развитие умения работать с дополнительной литературой, правильно выбирать источники информации;
5. Развитие логического мышления, памяти, внимания;
6. Совершенствование мыслительных приемов анализа и синтеза;
7. Воспитание самостоятельности и ответственности, упорства в достижении цели;
8. Умение представь исследование с помощью мультимедийных средств;
9. Формирование бережного отношения к русскому языку.

Техническое обеспечение, необходимое для успешного осуществления работы: компьютеры подключенные к Интернет.

Этапы выполнение проекта:

1. Электронные ресурсы для учебного проекта

На данном этапе стоит выдавать раннее подобранную литературу учащимся и ссылки на информацию в Интернет ребята «посещают» их и «скачивают» необходимую информацию.

Для того чтоб учащиеся с легкостью выполняли поиск проводиться ознакомительный урок по способам поиска, сохранения информации с Интернета, о авторском праве и т.д в виде презентаций.

На данном этапе учащиеся заполняют список использованных ресурсов. На этом этап заканчивается.

2. Создание презентации учащегося

В начале данного этапа происходит объяснение учащимся как необходимо создавать, какова структура и требования к презентациям в теме планирование презентации.

Структура презентации должна быть следующей:

1 слайд: Вопрос для исследования ученика, тема исследования ученика, автор(ы);

2-й слайд: Вопрос учебной темы (как объект исследования), гипотеза исследования;

3-й слайд: Цель исследования, задачи и гипотеза исследования (что нужно поэтапно и конкретно сделать, чтобы достичь цели);

4-й слайд - 5-й слайд: Краткое, тезисное представление решенных задач (или, иными словами, представление хода исследования).

Здесь важно обратить внимание учеников на то, что презентация является визуальным представлением и сопровождением результатов проведенного исследования, поэтому для лучшего понимания целесообразно иллюстрировать тезисы графическими изображениями, схемами, диаграммами, таблицами;

n +1 слайд: Выводы, которые могут быть представлены в форме *обобщении,* перечня результатов, предложений, рекомендаций, алгоритмов деятельности и др. Здесь важно обратить внимание учеников на соотнесение выводов с целью и гипотезой исследования.

n +2 слайд: Список используемой литературы.

Важно: Оформление, начертание шрифтов всех слайдов должны быть одинаковы.

После того как ученикам дана структура презентации, им предлагается начать разрабатывать собственные презентации полагая, что они уже знакомы с программой Microsoft Office PowerPoint. Разработанная презентация учащегося оценивается по разработанному учителем критерию оценивания презентации.

3. Создание публикации учащегося

На данном этапе нужно рассказывать учащимся о том, что существуют различные виды печатных изданий:

Афиша - реклама, одностороннее листовое издание, крупноформатное.

Брошюра – непериодическое издание, в мягкой обложке, в виде скрепленных или склеенных листов.

Буклет (Booklet) - как правило, многокрасочное издание, отпечатанное на одном листе, сфальцованное любым способом в два и более сгибов (гармошкой, дельтообразно, с поперечным фальцем и т.д.). Обычно применяются дна метода фальцовки: гармошкой, когда каждый последующий сгиб направлен в сторону, противоположную предыдущему, и салфеткой - сгибы направлены в одну сторону (для рекламных листков, проспектов, путеводителей). Вот он и будет нас интересовать.

Дайджест - издание, и котором сжато передается содержание самых интересных публикаций за какой-то период.

Журнал - периодическое сброшюрованное печатное издание, имеющее постоянную рубрикацию и содержащее статьи по различным вопросам жизни, природы, науки, литературные произведения, иллюстративный и другие материалы.

Книга один из вида полиграфической продукции, непериодическое издание в виде сброшюрованных бумажных листов или тетрадей с отпечатанной на них текстовой, графической, иллюстрационной информацией, объемом более 48 страниц, как правило, в твердом переплете. Может быть и рукописным периодическим изданием.

Обложка - бумажное иллюстрированное или текстовое покрытие издания, предохраняющее его страницы (блоки) от разрушения и загрязнения, содержит ряд выходных сведений, является также элементом внешнею оформления.

Плакат - чистовое издание большого формата и др.

После знакомства с различными видами публикаций учащиеся выбирают понравившейся им виды публикаций, но чаще всего учитель рекомендует буклет т.к. он несет максимум текстовой и графической информации в своем компактном размере. Для правильного создания публикации, приводиться ее структура с точки зрения представления результатов исследования:

- Краткое описание проблемы исследования;
- Какие существуют точки зрения на проблему исследования;
- Кто занимался исследованием проблемы;
- Каковы были этапы исследования;
- Какие получены результаты, на что стоит обратить внимание;
- Какие можно сделать выводы по результатам исследования [15].

Предполагая, что учащиеся знакомы с созданием публикаций, все же следует обратить внимание на логическое расположение информации в буклете. Как известно, буклет имеет две стороны: внешнюю (на которой находиться название буклета) и внутреннюю.

Разработанная публикация учащегося оценивается по разработанному учителем критерию оценивания публикации.

4. Разработка плана проведения проекта в школе.

С одной стороны, работа по планированию образовательной деятельности учащихся является знакомой учителю, но с другой стороны, планирование проектной деятельности достаточно ново и не освоено. Поэтому чтобы любой проект состоялся, требуется тщательное планирование, потому что именно на основе хорошо продуманного плана возможно эффективное управление проектом и получение нужного результата.

Наш проект создается для разработки серии классных часов, поэтому проведение проекта будет осуществляться непосредственно в классные часы.

На данном этапе проводится:

- организация проведения проекта в школе;
- обзор и корректировка материалов УМП к проекту;
- поиск дополнительных ресурсов;
- подготовка к защите проекта.

5. Защита учебных проектов

Коллективное обсуждение, экспертиза, результаты внешней оценки, выводы.

На этом этапе производится защита курсовой работы участниками проекта на классных часах, готовятся рецензии и отзывы на представляемую программу и ее описание, дается оценка проекту членами аттестационной комиссии.

Несмотря на наблюдаемое разнообразие проектов, все они в своем завершенном виде, в виде конечного продукта, должны отвечать определенным общим требованиям. Требования эти продиктованы необходимостью обеспечения максимального удобства пользователя. Рассмотрим наиболее общие из них.

Во-первых, предъявляемый материал должен быть структурирован в соответствии с логикой авторского изложения, подан, представлен пользователю в соответствии с этой структуризацией. Пользователь должен свободно ориентироваться в программе, для чего его следует ознакомить со стратегией освоения предлагаемой информации [24].

Требования к дизайну презентаций и публикаций: умелый подбор цветовой гаммы, подбор шрифтов в сочетании с их начертанием и размерами, обеспечивающий «читабельность» текста, тщательность исполнения картинок, заполняющих экранное пространство, высокое качество вставляемых аудио- и видеофрагментов.

Таким образом, приступая к реализации проекта, научный руководитель должен продумать в деталях конечный вид создаваемого продукта. Прогностическую оценку следует производить как с точки зрения воплощения дидактической авторской идеи, так и с точки зрения пользова-

теля, для которого создается программа. И то, и другое концентрируется в форме бланка технического задания [25].

Создайте тему, определите ее графическое решение – своеобразный лейтмотив создаваемого ресурса. Проверьте, соответствует ли найденное решение смысловому содержанию, отражает ли его суть. Определите, соответствуют ли элементы оформления выбранной визуальной теме, гармонично ли «вписываются» в общий дизайн, не выглядят ли чужеродными элементами.

В ходе проектирования образовательных Web-ресурсов не следует забывать о ряде требований, соблюдение которых может быть приравнено к следованию авторами правилам хорошего тона. Прежде всего для сетевого проекта важны:

- простота и согласованность, особая привлекательность титула (по статистическим данным, если пользователь Web-ресурсов, заглянувший на ваш сайт, не задержался там долее 30 секунд, можете не рассчитывать на то, что завладеете его вниманием в дальнейшем);
- правило двух щелчков в маршрутизации;
- красочность и увлекательность: избегайте «скучных» формулировок, непонятных аббревиатур;
- правильность, грамотность речи;
- уважение авторских прав, культура цитирования;
- «бесшовность»: последовательность в визуальном представлении.

Общие требования к дизайну: грамотный подбор цветовой гаммы, подбор шрифтов (начертание и размер), обеспечивающий «читабельность» текста, выбор оптимального формата и размера графических объектов, заполняющих экранное пространство, высокое качество вставляемых аудио- и видеофрагментов.

Из вышесказанного можно кратко выделить **внешнюю оценку проекта:**

- значимость и актуальность выдвинутых проблем, адекватность их изучаемой тематике;
- корректность используемых методов исследования и методов обработки получаемых результатов;
- активность каждого участника проекта в соответствии с его индивидуальными возможностями;
- коллективный характер принимаемых решений (при групповом проекте);
- характер общения и взаимопомощи, взаимодополняемости участников проекта;
- необходимая и достаточная глубина проникновения в проблему; привлечение знаний из других областей;
- доказательность принимаемых решений, умение аргументировать свои заключения, выводы;

• эстетика оформления результатов проведенного проекта;

• умение отвечать на вопросы оппонентов, лаконичность и аргументированность ответов каждого члена группы.

Методика проведения родительского собрания «Родительский контроль: не навреди» для младшего звена СОШ

Автор Пиший С.А., руководитель Чернова Е.В.

Часть 1 (Вступительная)

В первой части классный руководитель говорит небольшую вступительную речь (5-7 мин.), в которую входит:

1. Приветствие собравшихся родителей.

Краткое описание проблемы родительского контроля среди младшего звена школьников. Стоит кратко объяснить родителям, что использование информационных технологий их детьми таит в себе не мало опасностей и угроз (более подробно это сделает приглашенный специалист). В данную часть могут входить слова о том, что несомненно правильное использование компьютерных технологий и сети Интернет может помочь ребенку в обучении, самореализации, личностном росте, а также развить коммуникабельность, социальные навыки, самостоятельность и новые интересы. Однако, ребенок при взаимодействии с новыми технологиями и особенно с сетью Интернет подвергается огромному количеству информационных угроз таких, как «взрослый контент», запрещенная или нежелательная информация (наркотики, алкоголь, экстремизм), нежелательные игры, социальные сети, мошенничество.

2. Описание собственных наблюдений по поводу использования школьниками информационных технологий и особенно Интернета, что подчеркнет актуальность обсуждаемой проблемы. В данном пункте можно особо уделить внимание тому, что дети как на уроках, так и на переменах не выпускают из рук свои смартфоны, планшеты и другие мобильные гаджеты. Кроме того стоит подчеркнуть, что дети и на уроках (например, информатики), и дома очень часто пользуются Интернетом для выполнения домашней работы – составления докладов и рефератов, просмотра дополнительных сведений по изучаемым в школе темам. Также большинство школьников имеют хобби, и Интернет часто является самым удобным способом получить информацию об их увлечениях.

3. Представление приглашенного специалиста (специалистов) по информационной безопасности.

4. Передача слова приглашенному специалисту.

Часть 2 (Выступление специалиста по ИБ по теме собрания)

Во второй части специалист ярко, лаконично и доступно раскрывает суть обсуждаемой проблемы и рассказывает (в нашем случае еще и демонстрирует) средства, позволяющие сократить риск воздействия на

школьников нежелательной информации при работе с информационными технологиями и особенно с Интернетом.

В своем выступлении специалист по ИБ придерживается следующего плана:

1. Поприветствовать собравшихся родителей, классного руководителя и других педагогов (в случае, если они присутствуют).
2. Произнести вступительную речь о повсеместном использовании детьми информационных технологий, поддерживая слова сказанные классным руководителем (часть 1, п. 3).
3. Объяснить родителям, что, кроме компьютеров, ноутбуков и мобильных гаджетов, дети могут получить доступ в Интернет еще и через электронные книги, игровые приставки и телевизоры с функцией Smart TV (многие родители не знают всех каналов доступа к Интернету).
4. Объяснить родителям, что существуют серьезнейшие проблемы, которые являются причиной недостаточной бдительности родителей за информационной безопасностью своих детей. В качестве одного примера можно привести то, что часто родители считают себя продвинутыми пользователями информационных технологий, но их дети разбираются в этом гораздо лучше и легко обходят все ограничения, установленные родителями. Другой пример – родители часто просто не догадываются обо всех угрозах, которые возникают при работе детей с их гаджетами и в Интернете.
5. Привести родителям данные статистики о том, что современные дети проводят куда больше времени с их мобильными гаджетами, чем с домашними компьютерами и поэтому именно смартфоны и планшеты являются основным источником воздействия на детей нежелательной информации.
6. Подробно, но лаконично описать самые распространенные типы угроз информационной безопасности, возникающие при взаимодействии школьников с информационными технологиями и особенно с Интернетом. Здесь следует упомянуть о наличии в интернете большого количества порнографической информации, а так же информации пропагандирующей расовую нетерпимость, фашизм, сектантство, терроризм, жестокое отношение к людям или животным, наркотики, алкоголь, курение и прочее. Еще стоит напомнить родителям, что видеоигры часто содержат откровенные сцены и сцены жестокости, которые могут повлиять на психику ребенка. Обязательно нужно затронуть проблему использования детьми социальных сетей и зависимости от них. Кроме того напомнить родителям о наличии огромного числа мошенников и виртуальных казино в Интернете. Так же нельзя не затронуть тему преступлений по отношению к детям, связанных с общением и доверием детей «друзьям» из Интернета, особенно если они противоположного пола.
7. После освещения всех угроз безопасности необходимо задать краткие вопросы аудитории. Такими вопросами могут быть: обо всех ли

угрозах знали родители; все ли средства доступа в интернет были им известны. Так же можно попросить поднять руки тех родителей, кто уже активно участвует в организации информационной безопасности собственного ребенка, спросить, как они это делают. Спросить у родителей, повлияла ли новая полученная информация на их отношение к обеспечению информационной безопасности их детей.

8. Далее следует сказать, что воспитательные и организационные меры являются одним из самых действенных способов ограждения ребенка от нежелательной информации. Объяснить родителям, что нельзя давать детям в Интернете полную свободу: необходимо беседовать с детьми об их знакомстве с Интернетом; научить ребенка правильно искать информацию; рассказать ребенку о полезных и нужных сайтах; объяснить ребенку что нужно уважать других людей в Интернете и их собственность; рассказать о мошенничестве в Интернете, о том что не все люди являются теми, за кого они себя выдают, что нужно рассказывать родителям о подозрительных знакомых в Интернете и не указывать свой адрес, телефон и другую личную информацию. Кроме того нужно постараться убедить родителей улучшать свои навыки владения информационными технологиями для обеспечения безопасности их собственных детей. Необходимо донести, что кроме Интернета и видеоигр, у ребенка должны быть и другие (невиртуальные) хобби.

9. Далее следует анализ и наглядная демонстрация программных средств родительского контроля. Нужно рассмотреть самые основные типы родительского контроля: встроенные в поисковые системы; встроенные в браузеры; встроенные в антивирусы; специализированные браузеры для выхода в интернет; специализированные программы родительского контроля; встроенные в операционную систему; ПО на мобильных устройствах. Нельзя ограничиваться только теоретическим лекционным материалом. Нужно наглядно на компьютере и мобильном устройстве продемонстрировать по одному самому популярному программному продукту из каждого типа. Наглядно показать какие возможности дает такое ПО, как его настроить и как им пользоваться. Особое внимание нужно уделить мобильному программному обеспечению, подчеркнув, что данное направление использования Интернета и игр сейчас самое популярное.

Особенно следует уделить внимание обеспечению информационной безопасности детей посредством мобильных устройств. Обзор мобильных решений родительского контроля содержит в себе следующую информацию.

Нужно рассмотреть средства, предоставляемые на каждой из самых распространенных на сегодняшний день мобильных платформ – Windows Phone, iOS, Android, Blackberry.

Речь может быть построена следующим образом.

На сегодняшний день самой распространенной является мобильная платформа Android, однако встроенные средства для осуществления роди-

тельского контроля здесь практически отсутствуют. Согласно политике официального онлайнн-магазина Google Play, разработчики обязаны присваивать всем загружаемым приложениям соответствующую возрастную категорию: «для всех», «для детей», «для подростков» и «для взрослых». Родители могут настроить доступ к приложениям на своем мобильном устройстве, ограничив его одной или несколькими из указанных категорий, и защитить выбранные возрастные настройки PIN-кодом, что не позволит детям качать «взрослое» программное обеспечение из Google Play. Если пользователи находят приложения, которым присвоена неверная категория, они могут сообщить об этом в Google, пометив приложение «флажком». Каждое отмеченное приложение будет проанализировано командой Google на соответствие правилам. Однако такой подход абсолютно не гарантирует, что ребенок не наткнется на взрослый контент. Во-первых, до тех пор, пока приложение с неправильной категорией будет обнаружено и проанализировано, его смогут успеть скачать миллионы детей. Во-вторых, Android позволяет устанавливать приложения из любых источников, а не только из официального магазина приложений. В-третьих, никакой фильтрации запросов в Интернет это не предусматривает.

Но не стоит думать, что Android не позволяет защитить ребенка от нежелательной информации. В Play Market есть огромное количество как платных, так и бесплатных приложений, помогающих родителям оградить их детей от негативной информации. Больше всего распространены приложения, работающие по типу «песочницы» (sandbox). Одним из самых популярных приложений в России является «Родительский контроль» от компании PlayPad. Это приложение по сути является детским лаунчером с родительским контролем, который блокирует приложения, запрещенные ребенку, ограничивает время пользования приложениями и мобильным гаджетом в целом, блокирует звонки и смс, отслеживает местоположение ребенка и многое другое.

Нужно понимать, что в Google Play огромное множество альтернатив данной программе, поэтому подходящее приложении сможет найти даже самый привередливый родитель. Стоит пояснить, что приложения такого типа чаще всего не позволяют фильтровать запросы в Интернет, а лишь могут открыть/закрыть в него доступ. Поэтому, если ребенок уже начал знакомство с интернетом, необходимо воспользоваться соответствующими приложениями-фильтрами. Сегодня самыми популярными фильтрами на Android являются средства, созданные производителями антивирусов, например: Norton Safety Minder компании Symantec, Parental Control «Лаборатории Касперского», Parental Control компании Bitdefender и «Mobile Security & Antivirus» от TrendMicro со встроенным Parental Control. Такие приложения имеют те же возможности, что и фильтры, устанавливаемые на компьютер: создание черных и белых списков ресурсов, использование стандартных черных и белых списков, отслеживание действий ребенка в сети и т.д. Продукт Лаборатории Кас-

перского, ко всему прочему, имеет возможность задания возраста ребенка, для автоматического подбора безопасных ресурсов.

Следующая по популярности мобильная ОС – это iOS от компании Apple. В операционной системе iOS встроенный «Родительский контроль» есть. В его возможности входит ограничение использования некоторых приложений, запуск/удаление приложений, отключение браузера Safari, клиента для просмотра видеороликов YouTube, камеры и приложения для покупок в интернет-магазинах iTunes.

Родительские настройки надежно защищены от ребенка: во-первых, для изменения настроек необходимо ввести четырехзначный пароль. Во-вторых, после нескольких неудачных попыток телефон начинает считать их количество, а так же увеличивает время ожидания перед следующим вводом пароля. Поэтому ребенок просто не сможет скрыть факт попытки взломать родительский iPhone.

К сожалению, способ заблокировать нежелательный интернет-контент в браузере Safari нет. Вариантов решения проблемы два: либо отключить Safari вовсе, либо использовать стороннее приложение родительского контроля, аналогичное рассмотренным выше для платформы Android. Рекомендуемым приложением в данном случае является Parental Control от Лаборатории Касперского.

Мобильная платформа Blackberry хоть и не является популярной в России и вообще позиционируется как операционная система для деловых людей, тоже имеет средства, предназначенные для осуществления родительского контроля. Сама компания разработала приложение Parental Control, доступное на BlackBerry App World. Функционально «Родительский контроль» Blackberry похож на iOs: можно запретить установку/удаление программ, разрешить звонки на определенные телефоны, установить запрет на использование камеры и Bluetooth. Так же, как у iOs, отсутствует фильтрация контента в Интернете. Нужно отметить, что гаджет на данной мобильной платформе не лучший способ обезопасить ребенка, поскольку изначально был рассчитан на использование взрослым человеком. Кроме того возможность выбора приложения родительского контроля в официальном магазине BlackBerry App World практически отсутствует.

Компания Microsoft в своей ОС Windows Phone не может похвастаться достаточно серьезным встроенным функционалом родительского контроля. Приложение «Родительского контроля» в устройстве Microsoft Windows Phone 8 носит название Kid's Corner и работает по принципу «песочницы» – то есть полного запрета части функционала, например выхода в Интернет, то есть ни о какой фильтрации запросов ребенка в Интернет и речи быть не может. Основной упор разработчики делают на ограждении родительской информации от случайного удаления с устройства. Поэтому, для ограничения доступа к вредоносным сайтам родителю придется использовать сторонний антивирус или дополнительное прило-

жение. К слову, таких приложений сейчас совсем не много, и их качество и функционал оставляет желать лучшего. Найти средства, хотя бы отдаленно приближенные к Kaspersky Parental Control или PlayPad Родительский контроль просто не получится. Поэтому данная операционная система является не лучшим кандидатом для знакомства ребенка с мобильными технологиями.

10. В заключение нужно обязательно сказать, что каждое из рассмотренных средств не является абсолютным гарантом информационной безопасности детей, и использовать эти средства нужно комплексно.

11. Далее следует поблагодарить родителей за внимание, попросить раздать рекомендации с основными воспитательными и организационными мерами родительского контроля, а также список рекомендуемых специалистами программных средств родительского контроля и попросить родителей задать вопросы.

Часть 3 (Вопросы от родителей и обсуждение)

В третьей части родители задают вопросы специалисту по ИБ, а так же возможна небольшая дискуссия как между родителями, так и между родителями и приглашенным специалистом.

Часть 4 (Заключительная)

В заключительной части классный руководитель благодарит специалиста по информационной безопасности за лекцию, родителей за внимание и просит в течение некоторого периода времени после собрания (месяц-четверть) написать, что было сделано в их семье для обеспечения родительского контроля при взаимодействии ребенка с компьютером, мобильными устройствами и Интернетом.

Методика преподавания языка программирования AR Basic

Автор Самсонова А.А., руководитель Чернова Е.В.

Обучение основано на принципах интеграции теоретического обучения с процессами практической, исследовательской, самостоятельной научной деятельности учащихся и технико-технологического конструирования.

Задачи:

- формирование творческой личности установкой на активное самообразование;
- ранняя ориентация на инновационные технологии и методы организация практической деятельности в сферах общей кибернетики и роботостроения;
- развитие коммуникативных способностей, умения работать в команде;
- организация разработок технико-технологических проектов;
- развитие критического, логического и алгоритмического мышления;

- формирование, развитие и закрепление знаний, умений и навыков алгоритмизации и программирования учащихся в игровой форме;
- развитие познавательного интереса к изучению информатики и программирования, а также привлечение внимания школьников к новым информационным технологиям
- освоение принципов работы андроидного робота AR-100 и формирование у учащихся знаний об основных понятиях теории программирования на языке AR Basic Studio ;
- выявление и объединение наиболее одаренных в области информатики и программирования школьников и дальнейшее развитие их способностей;
- создание возможности общения ребят и обмена опытом программирования;
- развить у учащихся культуру труда при выполнении творческих работ.

В основу программы положено моделирование андроидных (человекообразных) роботов, как прогрессивного, наглядного и одновременно практически полезного раздела робототехники, вобравшего в себя ее передовые достижения.

В процессе теоретического обучения учащиеся знакомятся с назначением, структурой и устройством роботов различных классов, с технологическими основами сборки и монтажа, основами электроники и вычислительной техники, средствами отображения информации, историей и перспективами развития робототехники.

Программа включает проведение практикума начинающего робототехника, включающего проведение лабораторно-практических, исследовательских работ и прикладного программирования. В ходе специальных заданий учащиеся приобретают общетрудовые, специальные и профессиональные умения и навыки по монтажу отдельных элементов и сборке готовых роботов, их программированию, закрепляемые в процессе разработки проекта.

На учебных занятиях уделяется особое внимание соблюдению учащимися правил безопасности труда, противопожарных мероприятий, личной гигиены и санитарии, выполнению экологических требований при работе с робототехникой, монтаже и пайке ее электронных элементов.

Программа содержит сведения по истории современной электроники, информатики и робототехники, о ведущих ученых и инженерах в этой области и их открытиях с целью воспитания интереса учащихся к профессиональной деятельности, направлениям развития и перспективам робототехники.

Содержание программы реализуется во взаимосвязи с предметами школьного цикла. Теоретические и практические знания по робототехнике значительно углубят знания учащихся по ряду разделов физики (статика и

динамика, электрика и электроника, оптика), черчению (включая основы технического дизайна), математике и информатике.

Программа курса «Программирование андроидных роботов на языке программирования AR Basic» 1-го года обучения

Тема 1. Введение. Предмет и содержание курса. Значение теоретического и практического материала программы

Цель занятий по данной теме: ввести в курс дела, что предстоит изучить для овладения навыками работы в среде **AR Basic Studio**.

- ознакомить учащихся со значимостью изучения курса и основными понятиями робототехники, с правилами безопасности при выполнении практических работ (образовательная);
- развитие у школьников памяти, логического стиля мышления, формирование умения правильно излагать свою мысль (развивающая);
- воспитание информационной культуры, поддержание интереса к информатике и формирование у учащихся умения работать в коллективной дисциплине, а также формирование аккуратности в оформлении конспекта (воспитательная).

План проведения занятий по теме 1

Время, мин	Деятельность учителя	Деятельность ученика
10	Обсуждение тематики занятий, порядок работы.	Ознакомление с тематикой занятий и их значениями.
20	Вводный инструктаж по технике безопасности при работе с электроинструментами и приводами, питающимися от сети переменного тока.	Внимательно слушают и преподавателя и конспектируют в тетради. Расписываются в журнале техники безопасности за то, что инструктаж прослушали и обязуются выполнять.
30	Первичная проверка знаний о понятиях, связанных с робототехникой. Обсуждение значения робототехники для современного общества.	Ведут диалог с учителем (беседу), показывая свои первичные знания.
20	Знакомство с основными понятиями курса: робот, андроидный робот, как он двигается и «чувствует»	Внимательно слушают преподавателя и фиксируют в тетрадях основные моменты.
10	Предоставление информации об учебных пособиях и литературе, рекомендованные для освоения курса и самостоятельного изучения.	Ознакомление со списком учебной литературы.
40	Творческое задание после проведения вводного занятия Фантазийный рисунок на тему, «Какие бывают роботы», «Робот моей мечты», «Роботы в нашем будущем».	Выполняют в любом графическом редакторе.

Тема 2. Обзор моделей современной робототехники. История создания и развития.

Цель занятий по данной теме: ознакомить учащихся с темой «Модели современной робототехники, ее история и развитие.

- ознакомить учащихся со современными моделями робототехники, их техническими характеристиками курса и основными понятиями робототехники, с правилами безопасности при выполнении практических работ (образовательная);
- развитие у детей памяти, логического стиля мышления, формирование умения правильно излагать свою мысль (развивающая);
- воспитание информационной культуры самостоятельно находить материал для изучения, поддержание интереса к информатике, формирование у учащихся умения работать в коллективной дисциплине и оформлять грамотно доклады и презентации (воспитательная).

План проведения занятий по теме 2

Время, мин	Деятельность учителя	Деятельность ученика
20	Обзор моделей и их особенности.	Обсуждение вместе с учителем в разновидностях моделей робототехники и их особенностях. Проводят сравнительный анализ.
25	Технические характеристики и особенности.	Изучение технических характеристик, в чем суть каждой.
45	История зарождения робототехники. Ученые и разработчики.	Учащиеся слушают и вступают в диалог с учителем.
30	Первые андроидные роботы.	Ознакомление с понятием «андроидный робот» и историей развития.
60	*Практическая работа* Выбор и подробное описание какой-либо модели андроидного робота. Создание отчетной работы – презентации и буклета.	Выполняют практическое задание.

Тема 3. Понятие о языке программирования AR Basic.

Цель занятий по данной теме: познакомить учащихся с новым языком программирования AR Basic.

- ознакомить учащихся с понятиями о языке программирования AR Basic, каким образом можно использовать базовые структуры для написания алгоритма программы (образовательная);
- развитие у детей памяти, логического и алгоритмического стиля мышления (развивающая);
- поддержание интереса к информатике, формирование у учащихся умения работать в коллективной дисциплине (воспитательная).

План проведения занятий по теме 3

Время, мин	Деятельность учителя	Деятельность ученика
80	Структурное алгоритмизация и программирование. Базовый набор структур. Повторение изученного материала: основы языка программирования Basic.	Обсуждение и повторение изученного ранее материала по разделу в информатики «Алгоритмизация и программирование».
90	Введение в язык программирования AR Basic.	Осваивают новый понятийный аппарат, использованный в среде AR Basic Studio, знакомятся с самой средой и ее особенностями.
60	Рассмотрение структур, операторов, команд.	Изучение использования базовых структур, которые вспоминали во время повторения материала.
60	Примеры готовых программ и их разбор.	Знакомятся с примерами готовых программ на языке программирования AR Basic и разбираются с учителем как были использованы базовые структуры, операторы и команды.
120	*Практическая работа* Решение задач на основе базовых структур алгоритмов.	Выполнение практической работы

Тема 4. Среда разработок AR Basic Studio: интерфейс, меню, подключение модулей.

Цель занятий по данной теме: познакомить учащихся со специфическими характеристиками среды программирования AR Basic.

- ознакомить учащихся с интерфейсом среды AR Basic Studio, возможностью подключения модулей программы, а также основными специфическими командами языка AR Basic (образовательная);
- развитие у детей памяти, логического стиля мышления (развивающая);
- поддержание интереса к информатике, формирование у учащихся умения работать в коллективной дисциплине и оформлять грамотно свои работы (воспитательная).

План проведения занятий по теме 4

Время, мин	Деятельность учителя	Деятельность ученика
40	Изучение интерфейса среды программирования.	Знакомство с интерфейсом среды AR Basic Studio. Задают возникающие вопросы.
40	Подключение модулей программ.	Вместе с учителем разбираются в работе по подключению модулей программы.

Время, мин	Деятельность учителя	Деятельность ученика
60	Специфические команды для программирования роботов.	Изучение специфических команд и применение их на практике.
120	Практическая работа Решение задач в среде программирования с подключением дополнительных модульных структур.	Выполнение практической работы.

Тема 5. Общая структура роботов. Способы соединения деталей и узлов робота.

Цель занятий по данной теме: доступно рассказать об структуре робота.

- ознакомить учащихся с общей структурой и основными составляющими андроидных роботов, а также со способами соединения деталей робота (образовательная);
- развитие познавательного интереса у детей, памяти, логического и алгоритмического стилей мышления (развивающая);
- формирование у учащихся умения работать в коллективной дисциплине и индивидуально (воспитательная).

План проведения занятий по теме 5

Время, мин	Деятельность учителя	Деятельность ученика
40	Общая структура и основные узлы андроидного робота.	Внимательно разбираются вместе с учителем в структуре андроидного робота.
40	Разъемные и неразъемные, подвижные и неподвижные соединения.	Знакомятся с видами соединений деталей андроидного робота.
180	Практическая работа **1.** Программирование основных команд манипуляторов. **2.** Знакомство с отладкой программ. Модификация параметров готовых программ робота из учебного набора и анализ результатов.	Выполняют практические работы.

Тема 6. Технические расчеты.

Цель занятий по данной теме: интересно и понятно объяснить тему занятий.

- ознакомить учащихся с правилами расчета и скорости движений робота (образовательная);
- развитие логического и математико-физического стилей мышления (развивающая);

- формирование у учащихся умения работать в коллективной дисциплине и индивидуально, внимательно следить за ходом занятий, принимая участие (воспитательная).

План проведения занятий по теме 6

Время, мин	Деятельность учителя	Деятельность ученика
45	Правила расчета общей кинематики и скорости движения робота и его узлов, скорости вращения деталей.	Ознакомление с правилами расчетов. Повторение разделов из курсов математики и физики.
45	Практическая работа Выполнение простейших расчетов по кинематике андроидного робота. Анализ и программирование простейших комплексов движений (имитация деятельности человека). Примеры: «Семафорная азбука». «Регулировщик» и т. д.	Выполнение практической работы.

Тема 7. Андроидные роботы АР-100 и АР-101 М: основные характеристики, понятие библиотеки движений, стандартные позы.

Цель занятий по данной теме: интересно и понятно объяснить тему занятий.

- ознакомить учащихся с андроидными роботами, которых им и предстоит программировать на языке программирования AR Basic, учащиеся должны знать основные характеристики роботов, иметь представление о библиотеке движений и стандартных позах роботов (образовательная);
- развитие познавательного и творческого интереса у школьников (развивающая);
- формирование у учащихся умения работать в коллективной дисциплине и индивидуально, внимательно следить за ходом занятий, принимая участие (воспитательная).

План проведения занятий по теме 7

Время, мин	Деятельность учителя	Деятельность ученика
40	Характеристики роботов, строение, принципы работы.	Разбираются вместе с учителем в характеристиках роботов, их строении и принципах работы.
40	Библиотека движений.	Знакомятся с понятием, из чего состоит и как пополняется данная библиотека.
180	Стандартные позы и их программная реализация.	На основе приобретенных знаний по изучению данного курса осваивают навыки по реализации алгоритмов программ на основе стандартных поз робота, тем самым разбираются в данном понятии.

Время, мин	Деятельность учителя	Деятельность ученика
180	Практическая работа Создание простейшей библиотеки движений. Расчет координат движений робота.	Выполняют практическую работу.

Тема 8. Электронная схема. Микроконтроллер. Датчики.

Цель занятий по данной теме: интересно и понятно объяснить тему занятий.

- ознакомить учащихся с темой занятий, учащиеся должны знать и разбираться в основных понятиях электронной схемы, микроконтроллера и датчика (образовательная);
- развитие познавательного и творческого интереса у школьников, памяти и умению применять свои знания на практике и в других сферах деятельности (развивающая);
- формирование у учащихся умения работать в коллективной дисциплине и индивидуально, внимательно следить за ходом занятий, принимая участие (воспитательная).

План проведения занятий по теме 8

Время, мин	Деятельность учителя	Деятельность ученика
30	Принципиальная электрическая схема робота.	Знакомство с принципиальной электрическая схема робота.
30	Общее устройство и основы программирования микроконтроллера.	Знакомство с понятием микроконтроллера и основ его программирования.
60	Принципы устройства и описание основных видов датчиков.	Знакомство с понятием датчика и изучение основных видов датчиков.
90	Практическая работа Модификация модели готовыми дополнительными датчиками. Продолжение программирования модели.	Выполняют практическую работу вместе с преподавателем.

Тема 9. Испытания робототехники.

Цель занятий по данной теме: объяснить значимость испытаний робототехники.

- ознакомить учащихся с видами испытаний и способами передачи движений роботу, учащиеся должны уметь проводить испытания конструкций и программ и проводить отладку программного кода (образовательная);
- развитие познавательного и творческого интереса у школьников, памяти, логического и алгоритмического стилей мышления (развивающая);

- формирование у учащихся умения работать в коллективной дисциплине и индивидуально, внимательно следить за ходом занятий, принимая участие (воспитательная).

План проведения занятий по теме 9

Время, мин	Деятельность учителя	Деятельность ученика
30	Виды испытаний.	Знакомство с видами испытаний. Обсуждение с учителем.
40	Способы передачи движений роботу из среды программирования в виде алгоритма программы.	Формирование умений передачи движений роботу.
90	Организациями проведение испытаний изготовленных конструкций и их программ.	Принятие участие в организации проведений испытаний. Представление о форме проведения испытаний.
120	Практическая работа Кинематические (ходовые) испытания. Оценка логики и замер скорости исполнения операций. Отладка программного кода.	Выполняют практическую работу вместе с преподавателем.

Тема 10. Практикум юного робототехника

Цель занятий по данной теме: учащиеся самостоятельно должен научиться устранять неисправности и недоработки, выявленных в ходе испытаний робота.

- предоставить возможность применить полученные знания об испытаниях робота и закрепить умения проводить отладку программного кода (образовательная);
- развитие познавательного и творческого интереса у школьников, памяти, логического и алгоритмического стилей мышления (развивающая);
- формирование у учащихся умения работать в коллективной дисциплине и индивидуально (воспитательная).

План проведения занятий по 10

Время, мин	Деятельность учителя	Деятельность ученика
180	Практическая работа **1.** Устранение неисправностей и недоработок, выявленных в ходе испытаний робота. **2.** Совершенствование конструкции. **3.** Предоставить результат, оформленный в виде доклада, где должен быть описан ход работы.	Выполняют практическую работу вместе самостоятельно, но возникающих вопросах, консультируясь с преподавателем.

Тема 11. Техническая документация.

Цель занятий по данной теме: объяснить значимость испытаний робототехники.

- ознакомить учащихся с видами испытаний и способами передачи движений роботу, учащиеся должны уметь проводить испытания конструкций и программ и проводить отладку программного кода (образовательная);
- развитие познавательного и творческого интереса у школьников, памяти, логического и алгоритмического стилей мышления (развивающая);
- формирование у учащихся умения работать в коллективной дисциплине и индивидуально, внимательно следить за ходом занятий, принимая участие (воспитательная).

План проведения занятий по теме 11

Время, мин	Деятельность учителя	Деятельность ученика
30	Понятие о технической документации.	Знакомство с особенностями документации, ее необходимостью создавать и понятием технической документации.
40	Оформление документации.	Приобретение навыков создавать документацию.
120	Практическая работа Оформление технической документации: технический рисунок, фотография общего вида, краткая техническая характеристика. Написание пояснительной записки о назначении, принципе действия и правилах эксплуатации, описание пользовательского интерфейса. Подготовка к итоговой выставке технического творчества. Определение роботов и программ для демонстрации. Подготовка к транспортировке, инструкции по упаковке/распаковке и т. д.	Создают и оформляют техническую документацию к разработанной модели во время изучения курса. Создание инструкций по транспортировке и упаковке/распаковке.

Тема 12. Заключительное занятие.

Цель занятий по данной теме: обсудит перспективы дальнейшего изучения и подвести итог, полученный знаний, умений и навыков.

- предоставить возможность поделиться своим полученным опытом с одноклассниками, выставив свою разработку на всеобщее обозрение, при этом школьник должен уметь правильно излагать свои идеи по дальнейшей перспективе изучения данного курса (образовательная);
- развитие познавательного и творческого интереса у школьников (развивающая);
- формирование у учащихся умения работать в коллективной дисциплине и индивидуально, внимательно следить за ходом занятий,

принимая участие, а также излагать грамотно излагать свою точку зрения (воспитательная).

План проведения занятий по теме 12

Время, мин	Деятельность учителя	Деятельность ученика
30	Подведение итогов работы за истекший год.	Ведут диалог с учителем. Представляют свои разработки (результат работы за год).
40	Обсуждение дальнейшие перспективы изучения на следующий год.	Планирование и обсуждение работы на следующий год, чтобы учитель смог отразить пожелания учеников в своем тематическом плане.

Учащиеся после первого года обучения должны знать:

- роль и место робототехники в жизни современного общества;
- назначение, особенности проектирования и программирования роботов различных классов, включая андроидных;
- основы программирования на языке AR Basic;
- характеристики, стандартные позы, библиотеку движений моделей андроидных роботов АР-100 и АР-101 М;
- порядок и правила оформления начальной технической документации.

Уметь:

- программировать в среде разработок AR Basic Studio под задачами начального уровня сложности;
- программировать простейшие комплексы движений робота.
- проводить отладку и настройку работы робота;
- выполнять расчеты по кинематике движения робота;
- оформлять начальную техническую документацию на готовые изделия.

Тематический план 1-го года обучения

Первый год обучения рассчитан на 66 часов				
№	Тема	Количество часов		
		теор.	практ.	всего
1.	Введение. Предмет и содержание курса. Значение теоретического и практического материала программы	2	1	3
2.	Обзор моделей современной робототехники. История создания и развития.	7	2	9
3.	Понятие о языке программирования AR Basic.	3	3	6
4.	Среда разработок AR Basic Studio: интерфейс, меню, подключение модулей.	3	3	6
5.	Общая структура роботов. Способы соединения деталей и узлов робота.	2	4	6
6.	Технические расчеты.	1	1	2

7.	Андроидные роботы АР-100 и АР-101 М: основные характеристики, понятие библиотеки движений, стандартные позы.	7	3	10
8.	Электронная схема. Микроконтроллер. Датчики.	5	2	7
9.	Испытания робототехники.	3	3	6
10.	Практикум юного робототехника.	-	4	4
11.	Техническая документация.	2	3	5
12.	Заключительное занятие.	-	2	2
	Всего:	35	31	66

Описание и примерный тематический план спецкурса «Групповое взаимодействие андроидных роботов на языке AR-Basic»

Автор Е.А. Чернева, руководитель: М.В. Романова

Примерная программа спецкурса «Групповое взаимодействие андроидных роботов на языке AR-Basic» рассчитан на внеклассную работу в количестве 70 академических часов. Предусматривает основы знаний языка AR-Basic. Рассчитан на обучаемых старших классов (10-11 класс).

Целью данного спецкурса является обучение старшеклассников основам робототехники, программирования.

Обучение по данному спецкурсу основано на принципах интеграции теоретического обучения с процесса и практической, исследовательской, самостоятельной научной деятельности воспитанников.

Задачи курса:

1. Овладение знаниями в области робототехники и программирования;

2. Формирование умений программирования на языке AR Basic, развитие креативного мышления;

3. Приобретение навыков коллективного труда и организация информационной деятельности;

Особенности спецкурса.

Спецкурс базируется на основе системного анализа технических средств робототехники и принципа типичности. Сущность принципа сводится к рассмотрению типичных схем, раскрывающих наиболее устойчивые, характерные признаки всего класса вместо изучения всех разновидностей.

В основу спецкурса положено моделирование андроидных (человекообразных) роботов, как прогрессивного, наглядного и одновременно практически полезного раздела робототехники, вобравшего в себя ее передовые достижения.

Содержание программы доработано в ходе экспериментальной проверки с целью освещения тем, интересных старшеклассникам как

теоретически, так и для самостоятельного программирования андроидных роботов.

Учебные занятия предусматривают особое внимание соблюдению старшеклассниками правил безопасности труда, противопожарных мероприятий, личной гигиены и санитарии, выполнению экологических требований при работе с робототехникой.

Спецкурс содержит сведения по истории современной электроники, информатики и робототехники, о ведущих ученых и инженерах в этой области и их открытиях с целью воспитания интереса учащихся к профессиональной деятельности, направлениям развития и перспективам робототехники.

Содержание спецкурса реализуется во взаимосвязи с предметами школьного цикла. Теоретические и практические знания по робототехнике значительно углубят знания учащихся по ряду разделов физики (статика и динамика, электрика и электроника, оптика), математике и информатике.

Примерный тематический план спецкурса
«Групповое взаимодействие андроидных роботов на языке AR Basic»

Тематический план спец курса рассчитан на 70 часов				
№	Тема	Количество часов		
		теории	практ.	всего
1.	Введение. Предмет и содержание курса, значение теоретического и практического материала программы.	2	1	3
2.	Обзор моделей современной робототехники. История создания и развития.	5	2	7
3.	Понятие о языке программирования AR Basic. Программа «Андромеда»	4	5	9
4.	Среда разработок AR Basic Studio: интерфейс, меню подключение модулей.	3	3	6
5.	Общая структура роботов. Способы соединения деталей и узлов робота.	2	4	6
6.	Технические расчеты.	1	1	2
7.	Андроидные роботы AP-100 и AP-101M: основные характеристики, понятие библиотеки движений, стандартные позы.	7	3	10
8.	Методика группового взаимодействия.	2	1	3
9.	Разработка сценария для проведения праздника «Первое сентября».	2		2
10.	Начало танца (переменная robot_id).	1		1
11.	«Шапка» программы. Файлы завода.	1		1
12.	Написание программы.		15	15
13.	Отладка программного кода.		3	3
14.	Защита проекта.		2	2
	Всего:	30	40	70

Тема 1. Введение. Предмет и содержание курса, значение теоретического и практического материала программы.

Цель занятия по данной теме: ввести в курс, что предстоит изучить для овладения навыками работы в среде AR Basic Studio.

- Ознакомить учащихся со значимостью изучения курса и основными понятиями робототехники, с правилами безопасности при выполнении практических работ (**образовательная**);
- Развитее у обучаемых памяти, логического стиля мышления, формирование умения правильно излагать свою мысль (**развивающая**);
- Воспитание информационной культуры, поддержание интереса к информатики и формирование у обучаемых умения работать в коллективной группе, а также формирование аккуратности в оформлении конспекта (**воспитательная**).

План проведения занятия по теме 1

Время, мин	Деятельность учителя	Деятельность обучаемых
10	Обсуждение тематики занятия, порядок работы.	Ознакомление с тематикой занятий и их значениями.
20	Вводный инструктаж по технике безопасности при работе с электроинструментами и приводами, питающимися от сети переменного тока.	Внимательно слушают преподавателя и конспектируют в тетради. Расписываются в журнале техники безопасности, за прослушанный инструктаж.
20	Первичная проверка знаний о понятиях, связанный с робототехникой. Обсуждение значения робототехники для современного общества.	Внимательно слушают преподавателя и фиксируют в тетрадях основные моменты.
20	Знакомство с основными понятиями курса: робот, андроидный робот, как он двигается, как он «чувствует».	Внимательно слушают преподавателя и фиксируют в тетрадях основные моменты.
10	Представление информации об учебных пособиях и литературе, рекомендованные для освоения курса и самостоятельного изучения.	Ознакомление со списком учебной литературы.
40	Творческое задание после проведения вводного занятия Фантазийный урок на тему: «Робот – кто это?», «Я и робот в будущем», «Робот в современности».	Выполняют в любом графическом редакторе.

Тема 2. Обзор моделей современной робототехники. История создания и развития

Цель занятия по данной теме: ознакомить обучаемых с темой «Модели современной робототехники, ее история и развитие».

- Ознакомить обучаемых со современными моделями робототехники, их техническими характеристиками курса и основными понятиями робототехники, с правилами безопасности при выполнении практических работ (**образовательная**);
- Развитие у детей памяти, логического мышления, формирование умения правильно излагать свою мысль (**развивающая**);
- Воспитание информационной культуры, самостоятельно находить материал для изучения, поддержание интереса к информатики и формирование у обучаемых умения работать в коллективной группе и грамотное оформление докладов и презентаций (**воспитательная**).

План проведения занятия по теме 2

Время, мин	Деятельность учителя	Деятельность обучаемых
20	Обзор моделей и их особенности.	Обсуждение вместе с учителем в разновидностях моделей робототехники и их особенностей. Проводят сравнительный анализ.
25	Технические характеристики и особенности.	Изучение технических характеристик, в чем суть каждой.
45	История зарождения робототехники. Ученые и разработчики.	Обучаемые слушают и ступают в диалог с преподавателем.
30	Первые андроидные роботы.	Ознакомление с понятием «андроидный робот» и историей развития.
60	***Практическая работа*** Выбор и подробное описание какой-либо модели андроидного робота. Создание отчетной работы – презентации и буклета.	Ознакомление со списком учебной литературы.

Тема 3. Понятие о языке программирования AR Basic. Программа «Андромеда»

Цель занятия по данной теме: познакомить обучаемых с новым языком программирования AR Basic и программой «Андромеда».

- Ознакомить обучаемых с понятием о языке программирования AR Basic, каким образом можно использовать базовые структуры для написания алгоритма программы, взаимодействие робота и компьютера (**образовательная**);
- Развитие у обучаемых памяти, логического и алгоритмического мышления (**развивающая**);
- Поддержание интереса к информатике, формирование у учащихся умения работать в коллективной группе (**воспитательная**).

План проведения занятий по теме 3

Время, мин	Деятельность учителя	Деятельность обучаемых
50	Структурное алгоритмизация и программирование. Базовый набор структур. Повторение изученного материала: основы языка программирования Basic.	Обсуждение и повторение ранее изученного материала по разделу информатики «Алгоритмизация и программирование»
60	Введение в язык программирования.	Осваивают новый понятийный аппарат, использованный в среде AR Basic Studio, знакомятся с самой средой и ее особенностями.
50	Рассмотрение структур, операторов, команд.	Изучение использования базовых структур, которые вспоминали во время повторения материала.
50	Программа «Андромеда»	Изучение как робот связывается с компьютером.
50	Примеры готовых программ и их разбор.	Знакомятся с примерами готовых программ на языке программирования AR Basic и разбираются с учителем как были использованы базовые структуры, операторы и команды.
100	***Практическая работа*** 1. Составление простейших алгоритмов на основе базовых структур. 2. Связь робота и компьютера с помощью программы «Андромеда»	Выполнение практической работы.

Тема 4. Среда разработок AR Basic Studio: интерфейс, меню, подключение модулей

Цель занятий по данной теме: познакомить обучаемых со специфическими характеристиками среды программирования **AR Basic .**

- Ознакомить обучаемых с интерфейсом среды **AR Basic Studio,** возможностью подключения модулей программы, а также основными специфическими командами языка **AR Basic (образовательная);**
- Развитие у детей памяти, логического стиля мышления (**развивающая)**;
- Поддержание интереса к информатике, формирование у учащихся умения работать в коллективной дисциплине и оформлять грамотно свои работы (**воспитательная).**

План проведения занятий по теме 4

Время, мин	Деятельность учителя	Деятельность ученика
40	Изучение интерфейса среды программирования.	Знакомство с интерфейсом среды AR Basic Studio. Задают возникающие вопросы .
40	Подключение модулей программ.	Вместе с учителем разбираются в работе по подключению модулей программы.
60	Специфические команды для программирования роботов.	Изучение специфических команд и применение их на практике.
120	***Практическая работа*** Решение задач в среде программирования с подключением дополнительных модульных структур.	Выполнение практической работы.

Тема 5. Общая структура роботов. Способы соединения деталей и узлов робота.

Цель занятий по данной теме: доступно рассказать об структуре робота.

- Ознакомить учащихся с общей структурой и основными составляющими андроидных роботов, а также со способами соединения деталей робота (**образовательная);**
- Развитие познавательного интереса у детей, памяти, логического и алгоритмического стилей мышления (**развивающая);**
- Формирование у учащихся умения работать в коллективной дисциплине и индивидуально (**воспитательная).**

План проведения занятий по теме 5

Время, мин	Деятельность учителя	Деятельность ученика
40	Общая структура и основные узлы андроидного робота.	Внимательно разбираются вместо с учителем в структуре андроидного робота.
40	Разъемные и неразъемные, подвижные и неподвижные соединения.	Знакомиться с видами соединений деталей андроидного робота.
180	***Практическая работа*** 1. Программирование основных команд манипуляторов. 2. Знакомство с отладкой программ. 3. Модификация параметров готовых программ робота из учебного набора и анализ результатов.	Выполняют практические работы.

Тема 6. Технические расчеты

Цель занятия по данной теме: интересно и понятно объяснить тему занятий.

- ознакомить учащихся с правилами расчета и скорости движений робота (**образовательная**);
- развитие логического и математико-физического мышления (**развивающая**);
- формирование у учащихся умения работать в коллективной группе и индивидуально, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятий по теме 6

Время, мин	Деятельность учителя	Деятельность ученика
45	Правила расчета общей кинематики и скорости движения робота и его узлов, скорости вращения деталей.	Ознакомление с правилами расчетов. Повторение разделов из курсов математики и физики.
45	***Практическая работа*** Выполнение простейших расчетов по кинематике андроидного робота. Анализ и программирование простейших комплексов движений (имитация деятельности человека). Основные движения: верх, вниз руки, присесть встать и т.д.	Выполняют практические работы.

Тема 7. Андроидные роботы АР-100 и Ар-101М: основные характеристики, понятие библиотеки движений, стандартные позы

Цель занятия по данной теме: интересно и понятно объяснить тему занятий.

- еще раз ознакомить обучаемых с андроидными роботами, которых им предстоит программировать на языке программирования AR Basic, обучаемые должны знать основные характеристики роботов, иметь представление о библиотеке движений и стандартных позах роботов (**образовательная**);
- развитие познавательного и творческого интереса у школьников (**развивающая**);
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятия по теме 7

Время, мин	Деятельность учителя	Деятельность ученика
40	Характеристики роботов, строение, принципы работы.	Разбираются в месте с преподавателем характеристиках роботов, их строении и принципах работы.
45	Библиотека движений.	Знакомятся с понятием, из чего состоит и как пополняется данная библиотека.
180	Стандартные позы и их программирование.	На основе приобретенных знаний по изучению данного курса осваивают навыки по реализации алгоритмов программ на основе стандартных поз робота, тем самым разбираются в данном понятии.
180	***Практическая работа*** Создание простейших библиотеки движений. Расчет координат движений робота.	Выполняют практическую работу.

Тема 8. Методика группового взаимодействия

Цель занятия по данной теме: интересно и понятно объяснить тему занятий.

- ознакомить с различными групповыми взаимодействиями в природе и обществе (**обучающая**)
- развитие познавательного и творческого интереса у школьников (**развивающая**)
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**)

План проведения занятия по теме 8

Время, мин	Деятельность учителя	Деятельность ученика
80	Ознакомить обучаемых с различными групповыми группировками в природе и обществе.	Внимательно слушают конспектируют в тетради.
45	***Практическая работа*** Фантазийный урок на тему «Какие работы будут выполнять андроидные роботы в бедующем»	Выполняют практическую работу в любом графическом редакторе.

Тема 9 Разработка сценария для проведения праздника «Первое сентября»

Цель занятия по данной теме: разработать сценарий.

- научить планировать свою работу, составить примерно план программирования робота к проведению праздника «Первое сентября» (**обучающая**);

- развитие познавательного и творческого интереса у школьников (**развивающая**);
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятия по теме 9

Время, мин	Деятельность учителя	Деятельность ученика
130	Помочь составить примерный план программирования андроидного робота для проведения праздника «первое сентября»	Составляют примерный план программирования андроидного робота.

Тема 10. Начало танца (переменная robot_id)

Цель занятия по данной теме: интересно и понятно объяснить тему занятий.

- познакомить с переменной robot_id (**обучающая**);
- развитие познавательного и творческого интереса у школьников (**развивающая**);
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятия по теме 10

Время, мин	Деятельность учителя	Деятельность ученика
45	Игра «» robot_id	Играют в игру «»

Тема 11. «Шапка» программы. Файлы завода

Цель занятия по данной теме: интересно и понятно объяснить тему занятий.

- ознакомить с понятием «шапка программы», значение и функции файлов завода (**обучающая**);
- развитие познавательного и творческого интереса у школьников (**развивающая**);
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятия по теме 11

Время, мин	Деятельность учителя	Деятельность ученика
45	Рассказать значение и функции «шапки» программы, файлов завода.	Внимательно слушают, конспектируют себе в тетради.

Тема 12. Написание программы

Цель занятия по данной теме: научить самостоятельно составлять программы для роботов АР-100 «Добрыня».

- самостоятельно составлять программы (**обучающая**);
- развитие познавательного и творческого интереса у школьников (**развивающая**);
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятия по теме 12

Время, мин	Деятельность учителя	Деятельность ученика
65	Помогать группам в написании программного кода.	Пишут программный код.

Тема 13. Отладка программного кода.

Цель занятия по данной теме: обучаемые должны самостоятельно научиться устранять неисправности и недоработки, выявленные в ходе испытаний робота.

- предоставить возможность применить полученные знания об испытаниях робота и закрепить умения проводить отладку программного кода (**образовательная**);
- развитие познавательного и творческого интереса у школьников (**развивающая**);
- формирование у обучаемых умения работать в коллективной группе и самостоятельно, внимательно следить за ходом занятий, принимая участие (**воспитательная**).

План проведения занятия по теме 13

Время, мин	Деятельность учителя	Деятельность ученика
675	Практическая работа 1. Устранение неисправностей и недоработок, выявленных в ходе испытаний конструкций. 2. Совершенствование конструкции.	Выполняют самостоятельно практическую работу, но в возникающих вопросах обращаются к преподавателю.

Тема 14. Защита проекта

Цель занятия по данной теме: посмотреть достигнутые результаты.

- научить выступать перед аудиторией, и защищать свои проекты (**образовательная**);
- развитие познавательного и творческого интереса у школьников (**развивающая**);
- умение выслушивать оппонента (**воспитательная**).

План проведения занятия по теме 14

Время, мин	Деятельность учителя	Деятельность ученика
130	Оценивать достигнутые результаты.	Защищают своего робота.

Технологическая карта спецкурса «Групповое взаимодействие андроидных роботов на языке AR-Basic»

№	Название темы	Номер темы	
		1 (3 урока)	2 (7 уроков)
1.	Название темы.	Введение. Предмет и содержание курса, значение теоретического и практического материала программы.	Обзор моделей современной робототехники. История создания и развития.
2.	Дидактическая цель темы	Ознакомить учащихся со значимостью изучения курса и основными понятиями робототехники, с правилами безопасности при выполнении практических работ	Ознакомить обучаемых со современными моделями робототехники, их техническими характеристиками курса и основными понятиями робототехники
3.	Тип.	Рассказ, беседа.	Репродуктивный (демонстрация картинок, фильмов с современными моделями роботов).
4.	Знания, необходимые для изучения темы	Знание понятие алгоритма, алгоритмические структуры.	Знание понятий робот, робототехника.
5.	Умения, необходимые для изучения темы	Умение составлять алгоритмические структуры, простейшие алгоритмы. Умение работать в любом графическом редакторе.	Умение работать в программе MS Word, MS PowerPoint, MS Publisher.
6.	Методы проверки необходимых ЗУН	Беседа	Фронтальный опрос
7.	Формируемые знания (что должны знать по окончании изучения темы)	Знания понятия робот, робототехника, правила безопасности при выполнении практических работ.	Знания истории и развития робототехники, знать технические характеристики роботов, знать основные тенденции в современном мире в области робототехники.
8.	Формируемые умения (что должны знать по окончании изучения темы)	Умение выполнять практические задания самостоятельно, не нарушая технику безопасности.	Умение работать более углубленно в MS PowerPoint, MS Publisher.
9.	Планируемый уровень обученности	средний	средний

№	Название темы	Номер темы	
10.	Методы (формы) проверки достижимости цели темы.	Практический. «Робот – кто это?», «Я и робот в будущем», «Робот в современности».	Игровой (составление пазлов)
		3 (9 уроков)	**4 (6 уроков)**
1.	Название темы.	Понятие о языке программирования AR Basic. Программа «Андромеда».	Среда разработок AR Basic Studio: интерфейс, меню, подключение модулей.
2.	Дидактическая цель темы	Ознакомить обучаемых с понятием о языке программирования AR Basic, каким образом можно использовать базовые структуры для написания алгоритма программы, взаимодействие робота и компьютера	Ознакомить обучаемых с интерфейсом среды **AR Basic Studio,** возможностью подключения модулей программы, а также основными специфическими командами языка **AR Basic**
3.	Тип.	Моделирование.	Объяснительно-иллюстративный.
4.	Знания, необходимые для изучения темы	Знание понятие алгоритма, алгоритмические структуры.	Знание понятие алгоритма, алгоритмические структуры. Понятие о языке программирования AR Basic.
5.	Умения, необходимые для изучения темы	Умение составлять алгоритмические структуры, простейшие алгоритмы.	Уметь использовать базовые структуры для написания алгоритма программы, уметь организовывать взаимодействие робота и компьютера.
6.	Методы проверки необходимых ЗУН	Игровой (делятся на команды и составляют простейшие алгоритмы для андроидных роботов)	Фронтальный опрос.
7.	Формируемые знания (что должны знать по окончании изучения темы)	Понятие о языке программирования AR Basic, Знать теоретический аспект принципа работы программы «Андромеда»	Изучение интерфейса среды программирования. Специфические команды для программирования роботов.
8.	Формируемые умения (что должны знать по окончании изучения темы)	Уметь использовать базовые структуры для написания алгоритма программы, уметь организовывать взаимодействие робота и компьютера.	Уметь подключать модули программ, подключать дополнительные модульные структуры.

№	Название темы	Номер темы	
9.	Планируемый уровень обученности	Средний	Средний
10.	Методы (формы) проверки достижимости цели темы.	Практический	Практический, моделирование.
		5 (6 уроков)	**6 (2 урока)**
1.	Название темы.	Общая структура роботов. Способы соединения деталей и узлов робота.	Технические расчеты.
2.	Дидактическая цель темы	Ознакомить учащихся с общей структурой и основными составляющими андроидных роботов, а также со способами соединения деталей робота.	Ознакомить учащихся с правилами расчета и скорости движений робота, развитие логического и математико-физического мышления
3.	Тип.	Объяснительно-иллюстративный, моделирование.	Повторение разделов из курсов математики и физики, моделирование.
4.	Знания, необходимые для изучения темы	Знать современные модели робототехники, их технические характеристики и основные понятия робототехники.	Правила расчета общей кинематики и скорости движения робота и его узлов, скорости вращения деталей.
5.	Умения, необходимые для изучения темы	Уметь подключать модули программ, подключать дополнительные модульные структуры, организовывать взаимодействие робота и компьютера.	Уметь подключать модули программ, подключать дополнительные модульные структуры, организовывать взаимодействие робота и компьютера.
6.	Методы проверки необходимых ЗУН	Игровой «Научи робота ходить ☺» (кто лучше и быстрее справиться с заданием)	Игровой «Заставь робота сесть, встать и поднять руки»
7.	Формируемые знания (что должны знать по окончании изучения темы)	Знать общую структуру и основные узлы андроидного робота, разъемные и неразъемные, подвижные и неподвижные соединения.	Знать формулы расчета общей кинематики и скорости движения робота и его узлов, скорости вращения деталей.
8.	Формируемые умения (что должны знать по окончании изучения темы)	Уметь программировать робота на ходьбу.	Уметь программировать робота, чтобы он мог ходить поднимать руки, садиться и вставать.

№	Название темы	Номер темы	
9.	Планируемый уровень обученности	Средний.	Средний.
10.	Методы (формы) проверки достижимости цели темы.	Практический.	Практический, игровой «Чей робот пройдет быстрее 1 метр»
		7 (10 уроков)	**8 (3 урока)**
1.	Название темы.	Андроидные роботы АР-100 и Ар-101М: основные характеристики, понятие библиотеки движений, стандартные позы.	Методика группового взаимодействия.
2.	Дидактическая цель темы	Ознакомить и дать представление о библиотеке движений и стандартных позах роботов.	Ознакомить с различными групповыми взаимодействиями в природе и обществе
3.	Тип.	Репродуктивно-игровой (показ клипов со стандартными позами)	Рассказ, беседа.
4.	Знания, необходимые для изучения темы	Обучаемые должны знать основные характеристики роботов, знать формулы расчета общей кинематики и скорости движения робота и его узлов, скорости вращения деталей.	Знать современные модели робототехники, их технические характеристики и основные понятия робототехники.
5.	Умения, необходимые для изучения темы	Уметь организовывать взаимодействие робота и компьютера.	Уметь организовывать взаимодействие робота и компьютера.
6.	Методы проверки необходимых ЗУН	Игровой (организовать взаимодействие робота и компьютера командно, но с друг другом не общаться, только при помощи жестов)	Беседа.
7.	Формируемые знания (что должны знать по окончании изучения темы)	Знать какие движения входят в библиотеку движений.	Знать различные групповые группировки в природе и обществе.
8.	Формируемые умения (что должны знать по окончании изучения темы)	Уметь программировать робота через библиотеку движений.	Уметь определять различные группировки в природе и обществе по виду и типу.

№	Название темы	Номер темы	
9.	Планируемый уровень обученности	Средний	Средний
10.	Методы (формы) проверки достижимости цели темы.	Практическо-игровой (составить алгоритм движения робота «Знакомство двух людей») две команды работают раздельно, затем одновременно запускаются два и робота.	Практический ««Какие работы будут выполнять андроидные роботы в бедующем»»
		9 (3 урока)	**10 (1 урок)**
1.	Название темы.	Разработка сценария для проведения праздника «Первое сентября».	Начало танца (переменная robot_id).
2.	Дидактическая цель темы	Научить планировать свою работу, составить примерно план программирования робота к проведению праздника «Первое сентября».	Познакомить с переменной robot_id.
3.	Тип.	Объяснительно-иллюстративный.	Игровой.
4.	Знания, необходимые для изучения темы	Знать понятие алгоритма, алгоритмические структуры, знать современные модели робототехники, их технические характеристики и основные понятия робототехники, знать основные движения робота, которые находятся в библиотеки движений.	Знать понятие алгоритма, алгоритмические структуры, знать современные модели робототехники, их технические характеристики и основные понятия робототехники, знать основные движения робота, которые находятся в библиотеки движений.
5.	Умения, необходимые для изучения темы	Умение составлять алгоритмические структуры, простейшие алгоритмы, уметь применять движения робота, которые находятся в библиотеки движений.	Умение составлять алгоритмические структуры, простейшие алгоритмы, уметь применять движения робота, которые находятся в библиотеки движений.
6.	Методы проверки необходимых ЗУН	Индивидуальный контроль.	

№	Название темы	Номер темы	
7.	Формируемые знания (что должны знать по окончании изучения темы)	Представление танца в целом.	Знать назначение переменной robot_id.
8.	Формируемые умения (что должны знать по окончании изучения темы)	Умение заранее определить примерный код программы робота.	Уметь применять переменную robot_id.
9.	Планируемый уровень обученности	Средний	Средний
10.	Методы (формы) проверки достижимости цели темы.	Практический (написании сценария проведения праздника «Первое сентября»)	Игровой.
		11 (1 урок)	**12 (15 уроков)**
1.	Название темы.	«Шапка» программы. Файлы завода.	Написание программы.
2.	Дидактическая цель темы	Ознакомить с понятием «шапка программы», значение и функции файлов завода	Научить самостоятельно составлять программы для роботов АР-100 «Добрыня».
3.	Тип.	Игровой	Практический
4.	Знания, необходимые для изучения темы	Знать понятие алгоритма, алгоритмические структуры, знать современные модели робототехники, их технические характеристики и основные понятия робототехники, знать основные движения робота, которые находятся в библиотеки движений.	Знать понятие алгоритма, алгоритмические структуры, знать современные модели робототехники, их технические характеристики и основные понятия робототехники, знать основные движения робота, которые находятся в библиотеки движений.
5.	Умения, необходимые для изучения темы	Уметь организовывать взаимодействие робота и компьютера.	Уметь организовывать взаимодействие робота и компьютера.
6.	Методы проверки необходимых ЗУН	практическая	практическая
7.	Формируемые знания (что должны знать по окончании изучения темы)	Знать понятие «Шапка программы», значение и функции файлов заводов.	Знать основные команды робота.

№	Название темы	Номер темы	
8.	Формируемые умения (что должны знать по окончании изучения темы)	Уметь применять на практике файлы завода и уметь составлять «шапку программы».	Уметь оформлять алгоритм программы в среде AR Basic Studio.
9.	Планируемый уровень обученности	Средний	Средний
10.	Методы (формы) проверки достижимости цели темы.	Практический	практический
		13 (3 урока)	**14 (2 урока)**
1.	Название темы.	Отладка программного кода.	Защита проекта.
2.	Дидактическая цель темы	Обучаемые должны самостоятельно научиться устранять неисправности и недоработки, выявленные в ходе испытаний робота.	Научить выступать перед аудиторией, и защищать свои проекты
3.	Тип.	Практический	Дебаты
4.	Знания, необходимые для изучения темы	Знать понятие алгоритма, алгоритмические структуры, знать современные модели робототехники, их технические характеристики и основные понятия робототехники, знать основные движения робота, которые находятся в библиотеки движений.	Знать понятие алгоритма, алгоритмические структуры, знать современные модели робототехники, их технические характеристики и основные понятия робототехники, знать основные движения робота, которые находятся в библиотеки движений.
5.	Умения, необходимые для изучения темы	Уметь организовывать взаимодействие робота и компьютера.	Уметь организовывать взаимодействие робота и компьютера.
6.	Методы проверки необходимых ЗУН	практическая	Дебаты
7.	Формируемые знания (что должны знать по окончании изучения темы)	Знать как исправить недоработки выявленные в ходе испытаний робота.	Знать, как представлять свою работу на публике.

№	Название темы	Номер темы	
8.	Формируемые умения (что должны знать по окончании изучения темы)	Уметь редактировать программный ход.	Уметь грамотно держаться перед аудиторией, защищать свой проект.
9.	Планируемый уровень обученности	Средний	средний
10.	Методы (формы) проверки достижимости цели темы.	практический	практический

Поурочная разработка спецкурса «Групповое взаимодействие андроидных роботов на языке AR-Basic»

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
Тема 1. Введение. Предмет и содержание курса, значение теоретического и практического материала программы. (2 теории, 1 практика)					
1	Введение в предмет.	Ознакомить учащихся со значимостью изучения курса, техника безопасности.	Беседа, рассказ		Опрос.
2	Андроидный робот это кто?	Ознакомить с основными понятиями робототехники.	Комбинированный	Составление характеристик андроидного робота и человека	Игровой «Сходство и различие адроидного робота и человека»
3	Фантазийный урок «Робот – кто это?», «Я и робот в будущем», «Робот в современности».	Развить творческие способности, навыки работы в графическом редакторе.	Практический, игровой	Работа в графическом редакторе	Проверка рисунков.
Тема 2. Обзор моделей современной робототехники. История создания и развития. (5 теории, 3 практика)					
4	История зарождения робототехники.	Познакомить с историей создания и развития.	Игровой «С чего все началось?»		
5	Ученые и разработчики.	Познакомить с родоначальниками науки робототехники.	Игровой «Кто папа и мама роботов?»		

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
6 (как форма)	Этапы развития роботов.	Выделить основные этапы развития робототехники.	Игровой «Расскажи про робота по картинке»	Каждой группе предлагается набор картинок, необходимо найти характеристику в интернет и конспектах. Определить к какому этапу развития относятся их роботы.	В конце урока проверка результатов, сопоставление общей таблицы по этапам развития роботов.
7 (как метод)	Технические характеристики и особенности.	Охарактеризовать наиболее современные модели роботов.	Беседа, рассказ	Составление пазлов	Игровой «Составление пазлов»
8-10	Обобщение пройденного.	Обобщить сведения полученные по теме «Обзор моделей современной робототехники. История создания и развития».	Практический	1. Составление презентации (2 часа) 2. Составление буклета (1 час)	Проверка презентаций и буклетов.
Тема 3. Понятие о языке программирования AR Basic. Программа «Андромеда». (4 теории, 5 практики)					
11	Структурное алгоритмизация и программирование. Базовый набор структур. Повторение изученного материала: основы языка программирования Basic.	Познакомить обучаемых с новым языком программирования AR Basic.	Лекция		
12	Введение в язык программирования.	Ознакомить обучаемых с понятием о языке программирования AR Basic.	Лекция		

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
13	Рассмотрение структур, операторов, команд.	Познакомить с основными операторами команд.	Лекция		
14	Программа «Андромеда»	Познакомить каким образом взаимодействуют робот и компьютер.	Объяснительно-иллюстративный		
15	Примеры готовых программ и их разбор.	Познакомить каким образом можно использовать базовые структуры для написания алгоритма программы,	Практический	Разобраться в принципе работы простейших алгоритмов	Просмотр результатов, выставление оценок
16-17	Составление простейших алгоритмов на основе базовых структур.	Познакомить каким образом можно использовать базовые структуры для написания алгоритма программы,	Практический, игровой «Составь алгоритм»	Составить простейшую комбинацию из базовых структур	Просмотр результатов, выставление оценок
18	Связь робота и компьютера с помощью программы «Андромеда»	Научить настраивать связь между роботом и компьютером.	Практический, игровой «Соедини «друзей»»	Установить связь между роботом и компьютером	Просмотр результатов, выставление оценок
19	Соединение нескольких роботов с одним компьютером	Научить настраивать связь между несколькими роботами и одним компьютером.	Практический, игровой «Создай танцевальную команду»	Установить связь между несколькими роботами и компьютером	Просмотр результатов, выставление оценок
Тема 4. Среда разработок AR Basic Studio: интерфейс, меню подключение модулей. (3 теории, 3 практики)					
20	Изучение интерфейса среды программирования.	Ознакомить с интерфейсом среды AR Basic Studio**.**	Объяснительно-иллюстративный		
21	Подключение модулей программ.	Ознакомить с возможностью подключения модулей .	Объяснительно-иллюстративный		

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
22	Специфические команды для программирования роботов.	Ознакомить с основными специфическими командами языка AR Basic.	Объяснительно-иллюстративный		
23-25	Решение задач в среде программирования с подключением дополнительных модульных структур.	Научить решать задачи с дополнительными модулями.	Практический	Составляют алгоритмы с дополнительными модулями.	Просмотр результатов
Тема 5. Общая структура роботов. Способы соединения деталей и узлов робота. (2 теории, 4 практики)					
26	Общая структура и основные узлы андроидного робота.	Ознакомить с общей структурой и основными составляющими андроидных роботов.	Игровой «Сердце робота – какое оно?»		
27	Разъемные и неразъемные, подвижные и неподвижные соединения.	Ознакомить со способами соединения деталей робота	Рассказ, беседа		Игровой «Разбери и собери робота»
28	Программирование основных команд манипуляторов.	Научить программировать манипуляторы робота.	Практический	Программируют манипуляторы робота	
29	Знакомство с отладкой программ.	Научить отлаживать программы.	Практический, Игровой «Что значит отладить робота»	Отлаживают робота в процессе игры.	
30-31	Модификация параметров готовых программ робота из учебного набора.	Научить модифицировать параметры готовых программ.	Практический Игровой «Научи робота ходить»	Программируют робота на ходьбу.	

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
Тема 6. Технические расчеты. (1 теория, 1 практика)					
32	Правила расчета общей кинематики и скорости движения робота и его узлов, скорости вращения деталей.	ознакомить обучаемых с правилами расчета и скорости движений робота	Повторение		Игровой «Утренняя зарядка робота»
33	Повторение и обобщение пройденного материала.	Повторение темы 5 и 6.	Практический, игровой «Кто сильнее всех на свете?»		
Тема 7. Андроидные роботы АР-100 и АР-101М: основные характеристики, понятие библиотеки движений, стандартные позы. (7 теории, 3 практики)					
34	Характеристики роботов, строение, принципы работы.	Познакомить с характеристиками роботов, их строением и принципах работы.	Лекция		
35-37	Библиотека движений.	Знакомятся с понятием, из чего состоит и как пополняется данная библиотека.	Лекция		
38-40	Стандартные позы и их программирование.	Знакомятся с программированием стандартных поз.	Объяснительно-иллюстративный		
41	Программирование стандартных поз.	Практически реализуют программирование поз.	Практический	По командно программирую стандартные позы.	Просмотр результатов
42-43	«История знакомства двух роботов»	Спрограммировать робота на комплекс движений.	Практический, игровой «История знакомства двух роботов»	Составить алгоритм движения робота, две команды работают раздельно, затем	Проверка результата. В случае необходимости доработка.

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
				одновременно запускаются два и робота.	
Тема 8. Методика группового взаимодействия. (2 теории, 1 практика)					
44-45	Ознакомить обучаемых с различными групповыми группировками в природе и обществе.	ознакомить с различными групповыми взаимодействиями в природе и обществе			
46	Фантазийный урок	Закрепить навыки работы в графическом редакторе.	«Какие работы будут выполнять андроидные роботы в бедующем»	Создают рисунок в любом графическом редакторе.	Просмотр результатов, выставление оценок.
Тема 9. Разработка сценария для проведения праздника «Первое сентября». (2 теории)					
47-48	Разработка сценария	Научить планировать свою работу, составить примерный план программирования робота к проведению праздника «Первое сентября»	Объяснительно-иллюстративный.	Составляют план своей работы, сценарий.	
Тема 10. Начало танца (переменная robot_id). (1 теория)					
49	Переменная robot_id	познакомить с переменной robot_id	Игровой «Страна программного кода - 1»		
Тема 11. «Шапка» программы. Файлы завода. (1 теория)					
50	«Шапка» программы. Файлы завода	Ознакомить с понятием «шапка программы», значение и функции файлов завода	Игровой «Страна программного кода - 2»		

№	Наименование темы	Цель урока	Тип урока	Самостоятельная работа	Методы контроля
Тема 12. Написание программы. (15 практика)					
51	Определение переменных	Определить переменные, которые будут использоваться в программе, контрольные точки.	Объяснительно-иллюстративный	Пишут программный код.	Индивидуальный контроль
52-65	Программирование робота.	Научить самостоятельно составлять программы для роботов АР-100 «Добрыня».	Практический	Пишут программный код.	Индивидуальный контроль
Тема 13. Отладка программного кода. (3 практика)					
66-68	Предварительная проверка	обучаемые должны самостоятельно научиться устранять неисправности и недоработки, выявленные в ходе испытаний робота.	Практический	Редактирую программу	Индивидуальный контроль
Тема 14. Защита проекта. (2 практика)					
69-70	Зачетное занятие	научить выступать перед аудиторией, и защищать свои проекты	Практический	Защищают своих роботов	Подведение итогов, вставление оценок.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ахманаев Е.И., Чернова Е.В. Проект внеклассного мероприятия для старшеклассников «Кибертерроризм: история и современность» // Материалы Всероссийской научно-практической конференции «Современные проблемы информационных систем и информационных технологий». – Кизляр, 2013. – 322 с. – с. 186-199.

2. Боброва И.И., Трофимов Е.Г. Практический курс. Информационные технологии в образовании. – 2-е изд., стереотип. – М.: Флинта, 2014. – 202 с.

3. Боброва И.И. Технологии создания и внедрения интерактивных методических средств обучения в образовательный процесс // Вестник компьютерных и информационных технологий. – 2010. – № 6. – С. 48-52.

4. Брылева А.С., Чернова Е.В. Проект внеклассного мероприятия ««Информационная война» с киберпреступлениями, киберэкстремизмом и кибертерроризмом» для старшеклассников // Материалы Всероссийской научно-практической конференции «Современные проблемы информационных систем и информационных технологий». – Кизляр, 2013. – 322 с. – с. 280-293.

5. Виниченко А.О., Севостьянова Д.Н., Чернова Е.В. Киберэкстремистские влияния на молодежь в современном мире // Труды VIII международной научно-практической интернет-конференции / под ред. Г.К. Сафаралиева, А.Н. Андреева, В.А. Казакова – Пенза: Издательство Пензенского филиала ФГБОУ ВПО «РГУИТП», 2013-2014. – 486 с. – с. 398-404.

6. Виниченко А.О., Чернова Е.В. Методика проведения цикла мероприятий «Насилие в Интернет. Киберпреступность и киберэкстремизм» // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи (сборник статей) / под ред. Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова; Магнитогорский Дом Печати, 2015. – 480 с. – с. 131-138.

7. Ганиева Л.Ф. Методика проведения цикла воспитательных мероприятий по антипропаганде киберэкстремизма среди молодежи в вузе // Информационная безопасность и вопросы профилактики киберэкстремиз-

ма среди молодежи (сборник статей) / под ред. Г.Н. Чусавитиной, Е.В. Черновой. – Магнитогорск: МГТУ, 2014. – с. 57-63.

8. Ганиева Л.Ф. Ефимова И.Ю. Чернова Е.В. Метод проектов в подготовке молодёжи к противодействию вовлечения в киберэкстремистскую деятельность // Всеросс. студ. Форум: Актуальные проблемы теории и методики информатики, математики и экономики (21-22 марта). – Шадринск: ШГПИ, 2014. – с. 128-135.

9. Ганиева Л.Ф. Информационная безопасность в системе открытого образования на примере организации и проведения игры «Международный день Интернета» // Гуманитарные научные исследования. – № 6 (46). – Ч. 1. – 2015. – С. 30-36.

10. Ганиева Л.Ф., Савельева Л.А., Трейбач Е.Л. Методика проведения конкурса «Я – будущий учитель информатики» // VI Международная конференция «Информатика: проблемы, методология, технологии». Воронеж, 2016. – С. 196-204.

11. Гараев И.М., Чернова Е.В. Возможности информационных технологий в противодействии киберэкстремизму и кибертерроризму // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов II Международной конференции «Информационные технологии в науке, управлении, социальной сфере и медицине» / под ред. О.Г. Берестневой, О.М. Гергет. − Томск: Изд-во Томского политехнического университета, 2015. – С. 126-127.

12. Доколин А.С. Метод проектов в превенции киберэкстремистских идей в молодежной среде // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: сборник статей под ред. Г.Н. Чусавитиной, Е.В. Черновой. – Магнитогорск: Магнитогорский Дом печати, 2014. – С. 91-95.

13. Доколин А.С., Чернова Е.В. Превенция вовлечения молодежи в киберэкстремистскую деятельность посредством компьютерных игр // Фундаментальные исследования. – 2014. – № 12. – Ч. 5. – С. 1074-1077.

14. Златопольский Д.М. Интеллектуальные игры в информатике – СПб.: БХВ-Петербург, 2004. – 400 с.: ил.

15. Ерошин Н.В., Ошурков В.А., Чернова Е.В. Методика проведения мероприятия для родителей по проблемам киберэкстремизма в молодеж-

ной среде / Мир науки и инноваций. – Выпуск 1(1). Том 6. – Иваново: Научный мир, 2015. – С. 61-65.

16. Зеркина Е.В., Чусавитина Г.Н. Подготовка будущих учителей к превенции девиантного поведения школьников в сфере информационно-коммуникативных технологий: Монография. – Магнитогорск: МаГУ, 2008. – 184 с.

17. Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи (сборник статей) / под ред. Г.Н. Чусавитиной, Е.В. Черновой. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова; Магнитогорский Дом Печати, 2014. – 204 с.

18. Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи (сборник статей) / под ред. Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова; Магнитогорский Дом Печати, 2015. – 480 с.

19. Литвин А.В., Чернова Е.В. Создание собственных проектов в анимационной среде Скретч (Методические материалы в поддержку курса «Анимационная среда программирования Скретч» для системы дополнительного образования) / А.В. Литвин, Е.В. Чернова. – Магнитогорск : МаГУ, 2009. – 44 с.: ил.

20. Методические рекомендации по изучению дисциплины «Информационная безопасность в системе открытого образования» для обучающихся педагогических специальностей всех форм обучения / Е.В. Чернова. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2015. – 27 с.

21. Мовчан И.Н. Учебный проект «Этические аспекты поведения в сети интернет» как одна из форм противодействия киберэкстремизму в молодежной среде // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: сборник статей / под ред. Г.Н.Чусавитиной, Е.В.Черновой. – Магнитогорск : Изд-во Магнитогорск. гос. техн. ун-та им. Г.И.Носова; Магнитогорский Дом печати, 2014. – С. 128-133.

22. Мовчан И.Н., Чернова Е.В., Чусавитина Г.Н.Учебный проект как одна из форм противодействия киберэкстремизму среди школьников // Фундаментальные исследования. – 2015. – № 9-3. – С. 486-490.

23. Недосекина А.Г., Чусавитина Г.Н. Формирование эстетического идеала как средство профилактики киберэкстремизма // Фундаментальные исследования. – 2014. – № 12. – Ч. 5. – с. 1083-1088.

24. Организация самообразовательной деятельности студентов вуза в система дистанционного обучения: учеб-метод. пособие/ кол. Авт.: Т.Е. Климова, Д.А. Хабибулин, М.В. Романова, С.Н. Юревич, Е.В. Карманова. – Магнитогорск: МаГУ, 2013. – 217 с.

25. Пащенко К.Н., Чернова Е.В. Проект внеклассного мероприятия: «Терпи, казак, толерантным будешь» // Материалы Всероссийской научно-практической конференции «Современные проблемы информационных систем и информационных технологий». – Кизляр, 2013. – С. 143-160.

26. Подготовка учителя к использованию новых информационных технологий в профессиональной деятельности: учебно-методическое пособие/ Климова Т.Е., Федченко Е.В., Романов Е.П. – Магнитогорск: МаГУ, 2006 –174с.

27. Путинихин П.С., Чернова Е.В. Проект внеклассного мероприятия для старших классов «Угрозы кибертерроризма» // Материалы Всероссийской научно-практической конференции «Современные проблемы информационных систем и информационных технологий». – Кизляр, 2013. – С. 260-270.

28. Романов Е.П. Использование информационных технологий как инструмента познания и построения знания// Южно-уральский педагогический журнал: научный журнал. – 2015. – № 2(3). – С. 9-12.

29. Романова М.В. Метод проектов как основа курса Intel «Обучение для будущего»: методические указания к практическим занятиям. – Магнитогорск: МаГУ, 2011. – 27с.

30. Романова М.В., Романов Е.П. Технология проектного обучения в образовательном учреждении // Южно-уральский педагогический журнал: научный журнал. – 2010. – № 1. – С. 172-180.

31. Романов П.Ю. Моделирование процесса формирования исследовательских умений обучающихся в системе непрерывного педагогического образования / Вестник Оренбургского государственного университета. – Оренбург, 2003. – № 3. – С. 35-39.

32. Романов П.Ю. Управление формированием исследовательских умений обучающихся в системе непрерывного педагогического образования Государственная служба. – М., 2002. – № 6 (20). – С. 99-105.

33. Романов П.Ю., Усанова О.А. Теоретические аспекты развития творческих способностей студентов высших учебных заведений // Южно-Уральский педагогический журнал. – Магнитогорск, 2015. – № 1(2). – С. 77-82.

34. Романова Т.Е. Моделирование как основа реализации преемственности при обучении учащихся решению текстовых задач // Южно-Уральский педагогический журнал. – Магнитогорск. – № 2(3) – 2015. – С. 90-95.

35. Савельева Л.А. Вопросы подготовки будущих учителей информатики к использованию инновационных технологий // Современная педагогика. – Май 2014. – № 5 (18).

36. Савельева Л.А. Компетентностный подход в обучении будущих учителей информатики /Л.А.Савельева // Перспективные инновации в науке, образовании, производстве и транспорте 2013: Сборник научных трудов Sworld. – 2013. – Т. 21. – № 4. – С. 86-89.

37. Хоменко И.В., Чернова Е.В. Проект «Киберэкстремизм: история и современность» для учащихся старших классов // Материалы Всероссийской научно-практической конференции «Современные проблемы информационных систем и информационных технологий». – Кизляр, 2013. – С. 218-224.

38. Чернова Е.В., Доколин А.С. Метод проектов в превенции вовлечения молодежи в киберэкстремистскую деятельность // Психология и педагогика: на рубеже веков: монография. В 2 к. К. 1 / [авт.кол.: Карпова Н.К., Васильева С.А., Головань М.С. и др.]. – Одесса: КУПРИЕНКО СВ, 2015. – С. 6-38.

39. Чернова Е.В., Доколин А.С. Применение интерактивных методов обучения для противодействия киберэкстремистской деятельности среди молодежи / Informative and communicative space and a person : materials of the V international scientific conference on April 15-16, 2015. - Prague :

Vědeecko vydavatelské centrum «Sociosféra-CZ». – 177 p. – ISBN 978-80-7526-017-8. – p. 167-172.

40. Чернова Е.В. Образовательный проект по защите личной информации в Интернет // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов II Международной конференции «Информационные технологии в науке, управлении, социальной сфере и медицине» / под ред. О.Г.Берестневой, О.М.Гергет; Национальный исследовательский Томский политехнический университет. − Томск: Изд-во Томского политехнического университета, 2015. – С. 784-786.

41. Chernova E.V, Dokolin A.S. PROJECT METHOD IN THE PREVENTION OF YOUTH INVOLVEMENT IN CYBER EXTREMISM ACTIVITY in SWorld Journal, Vol.J11508 (Scientific world, Ivanovo, 2015) – URL: http://www.sworldjournal.com/e-journal/j11508.pdf (date:...) - page - 25-31. – J11508-002.

Учебное текстовое электронное издание

Романова Марина Викторовна
Чернова Елена Владимировна

МЕТОДИКА ОРГАНИЗАЦИИ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ПО ИНФОРМАТИКЕ И ИКТ

Учебное пособие

2,49 Мб
1 электрон. опт. диск

г. Магнитогорск, 2017 год
ФГБОУ ВО «МГТУ им. Г.И. Носова»
Адрес: 455000, Россия, Челябинская область, г. Магнитогорск,
пр. Ленина 38

ФГБОУ ВО «Магнитогорский государственный
технический университет им. Г.И. Носова»
Кафедра информатики и информационной безопасности
Центр электронных образовательных ресурсов и
дистанционных образовательных технологий
e-mail: ceor_dot@mail.ru