ОГЛАВЛЕНИЕ

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-тес (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	Как избежать и обезопасить себя от такого инцидента?

№	Проблема	Ситуация	Задание
		средств или вовсе не перевели ничего	
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?
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_мн огонациональном_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 беседа, 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-корректиное 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 кибертерозизма» 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»7
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.