**Чернова Е.В., Доколин А.С.**

# МЕТОД ПРОЕКТОВ В ПРЕВЕНЦИИ ВОВЛЕЧЕНИЯ МОЛОДЕЖИ В КИБЕРЭКСТРЕМИСТСКУЮ ДЕЯТЕЛЬНОСТЬ

*Магнитогорский государственный технический университет им. Г.И. Носова*

*Введение*

Информационные технологии в наше время развиваются огромными шагами. Практически, у каждого человека в нашей стране есть возможность получать, обрабатывать и сохранять информацию, пользоваться всеми социальными сервисами в сети Интернет. Сеть Интернет объединяет людей настолько, что сегодня мы не представляем себе жизнь без «Instagram», «Вконтакте», «Facebook», «Twitter» и других интернет сервисов. Стоит отметить, роль персонального компьютера сводится к минимуму. Теперь, достаточно иметь смартфон, и ты в полной мере можешь считать себя участником этого громадного информационного пространства. С одной стороны, данные сервисы и сеть Интернет делает нашу повседневную жизнь интереснее, помогает находить новых друзей, общаться с человеком, где бы он не находился, получать информацию, но с другой стороны, все эти сервисы могут использоваться в корыстных целях. Угроз в глобальной сети достаточно много и направлены они, в основном, на активных пользователей социальных и других сервисов сети, т.е. молодежь. Именно эта социальная группа подвержена наибольшей опасности, объясняется этой теми факторами, что не все молодые люди могут грамотно отличить достоверную и недостоверную информацию, правильно, с точки зрения информационной безопасности, использовать социальные сервисы, кроме того, большую роль играет не знание определенной исторической, юридической информации, чем пользуются различные группы лиц при вовлечении молодежи, в какую-либо противоправную деятельность. С этими угрозами нужно бороться как

техническими, так и социальными методами. Нужно воспитывать сильную, устойчивую и грамотную личность, которая могла бы противостоять различным информационным угрозам. В обязательном порядке необходимо «проводить разъяснительную работу среди подростков, привлекать их к выполнению различных проектов и решению задач, помогающих развить критическое мышление» [5].

*1. Развитие явления киберэкстремизма среди молодежи в ИКТ-среде*

В силу специфики инфраструктуры Интернета эта сеть наиболее подвержена рискам и уязвимостям в вопросах информационной безопасности и именно с Интернетом чаще всего ассоциируется у исследователей девиантное поведение пользователей. Девиантное поведение — это «поведение, отклоняющееся от общепринятых, наиболее распространённых и устоявшихся норм в определённых сообществах в определённый период их развития» [3]. Девиантное поведение в сфере ИКТ – «вид девиантного поведения индивида (группы индивидов), представляющий систему поступков (или отдельные поступки), опосредованных применением ИКТ (либо направленных в отношении ИКТ), причиняющую ущерб (моральный, физический, экономический и иной) обществу, организациям, частным лицам или самой личности» [6]. При этом уязвимость определяется как «недостаток, который человек может эксплуатировать для того, чтобы достигнуть чего-либо, к чему он не имеет полномочий доступа или что не предназначено для законного использования сети или системы в целом» [4]. Другими словами, в сети Интернет пользователи более уязвимы, чем в реальной среде. Причем по данным интернет-статистики, именно дети и подростки, выходя в Сеть, попадают в зону риска. На сегодняшний день исследователи говорят о том, что наибольшую угрозу для детей и подростков несет в себе, распространяемая в сети недостоверная информация, активная подмена жизненных ценностей, легкодоступные сообщества экстремистской направленности и многое другое. «В качестве основных поведенческих отклонений в ИКТ-насыщенной среде

исследователи выделяют: асоциальное поведение (киберхулиганство, увлечение виртуальным сексом), делинквентное (компьютерные преступления, кибертерроризм, киберэкстремизм), аддиктивное (Интернет-зависимость, геймерство) и гиперспособности в области ИКТ (хакерство, программирование)» [6]. Остановимся на одном из наиболее разрушительных видов девиантного поведения в среде ИКТ – делинквентном, то есть преступном. Делинквентное (антисоциальное) поведение в сфере ИКТ – «отклоняющееся поведение, представляющее собой проступок либо уголовно наказуемое деяние, совершенное посредством либо в сфере ИКТ, влекущее за собой получение выгоды и/или нанесение материального, психологического, информационного вреда жертве» [6]. В рамках нашего исследования, одним из наиболее опасных видов делинквентного поведения среди молодежи, мы считаем киберэкстремизм. В последнее время мировое интернет-сообщество акцентировало свое внимание на многих проблемах, распространившихся со скоростью вируса: киберпреступность, киберэкстремизм, кибертерроризм. Особенность всех явлений с приставкой «кибер» заключается в том, что их очень сложно контролировать в огромной информационной Сети и при этом, они с молниеносной скоростью находят своих сторонников и получают активную поддержку. Несмотря на многочисленные попытки, предпринимаемые на различных уровнях – от владельцев сайтов до правительств различных государств – поставить распространение данных явлений в Интернет под контроль, на сегодняшний день нельзя говорить о безоговорочном успехе. Находятся всевозможные лазейки в законах или программно-аппаратном уровне, и процесс распространения продолжается. В настоящее время, наиболее остро в Рунете стоит проблема привлечения молодежи в сообщества экстремисткой направленности. «Киберэкстремизм – частое явление в социальных сетях, блогосфере, форумах и сетевых сообществах» [16]. Однако, прежде чем перейти к рассмотрению этого явления более подробно, сформулируем определение понятия «экстремизм».

В России экстремизм получил развитие в середине 90-х годов. По мнению специалистов, это обусловлено его особенностями: в первую очередь, это длительная экономическая нестабильность, сильное социальное расслоение, низкая эффективность работы государственных институтов, отсутствие социальной защищенности граждан. Все это и сопутствующие проблемы приводят к спонтанным, стихийным протестам, либо к мелкому вандализму, хулиганству и преступлениям. Чаще всего проводниками экстремизма выступают радикальные политические партии. В конце XX – начале XXI века подобных партий в России оказалось множество. В качестве основных лозунгов выбирались националистические или сепаратистские, в ряды партий вовлекалась молодежь, среди которой поощрялась активная борьба силовыми методами с «не нашими». Стоит заметить, что роль экстремизма в жизни молодежи России и в то время, и в наше, оказалась недооцененной, что приводит к трагическим событиям, калеча судьбы и отбирая жизни. По мнению Н.М. Сироты, экстремизм – «ориентация в политике на крайне радикальные идеи и цели, достижение которых осуществляется в основном силовыми, а также нелегитимными и противоправными методами и средствами» [14]. «Как отмечает Д.Е. Некрасов, «полисемичность термина «экстремизм» обусловливает многообразие подходов к его толкованию. Такое положение вызывает необходимость его определения, в первую очередь с позиций словообразования. С точки зрения этимологии термин «экстремизм» означает приверженность к крайним взглядам и мерам. Следует заметить, что термин помимо значения «крайний», используется еще и в смысле «последний», «чрезвычайный». Следует обратить внимание на смысловое толкование слова «крайний», под которым понимается очень сильный, исключительный, чрезвычайный, являющийся наиболее непримиримым, решительным, радикальным» [7]. «Учитывая происхождение термина «экстремизм», можно сказать, что данный феномен подразумевает приверженность к чрезвычайным, нетрадиционным, непринятым, непримиримым, решительным, исключительным взглядам и мерам. В этом плане имеется точка зрения, что

«экстремизм есть изначально отрицание всякого чувства меры» [9]. Таким образом, мы можем сказать, что экстремизм – это один из типов девиантного поведения, направленного против существующих в обществе норм, правил, принципов, обычаев, традиций. Исходя из этого определения, будем считать, что киберэкстремизм – это приверженность к чрезвычайным, решительным, исключительными взглядам и мерам, реализуемых в киберпространстве с использованием информационных технологий.

Наиболее уязвимы к влиянию киберэкстремизма являются такие слои населения как: учащиеся школ и студенты. Данная социальная группа не обучена правильно воспринимать и обрабатывать тот информационный поток, который находится в сети Интернет. В итоге члены экстремистских движений и групп получили возможность распространять свою идеологию, убеждения на интернет-ресурсах, где численность аудитории может колебаться от нескольких десятков до сотен тысяч человек. Такие ресурсы воздействия на молодежные сознания сравнимы с потенциалом традиционных СМИ, только не контролируемых государством. Приходится констатировать, что в современной ситуации российская молодежь оказывается уязвимой перед массированным воздействием экстремистского характера. Не всегда позитивную роль играет неформальная среда общения, где происходит активная социализация молодых людей. Все чаще неформальные объединения способствуют проникновению в сознание молодежи, особенно подростков, экстремистских взглядов, используя для этого интернет-ресурсы, провоцируя спонтанные экстремистские действия. Именно на это и направлена работа экстремистских организаций в сети Интернет. При помощи глобальной сети молодые люди получают огромное количество недостоверной информации экстремистской направленности. Однако, сам возраст молодых людей имеет склонность к экстремальным формам реакции на окружающею действительность. «Системным фактором роста практически всех видов экстремистских проявлений эксперты назвали специфические особенности молодежи» [8]. Возрастные особенности,

пропаганда насилия в СМИ, недостатки воспитания, ситуация в мире влияет на рост молодежного киберэкстремизма.

Исходя из этого, можно сделать вывод о том, что превенция киберэкстремизма, прежде всего, должна быть направленна на работу с молодежью, при этом задействовав все социальные институты. Основная работа должна проводиться как в школах с учащимися, так и в вузах с будущими учителями. На наш взгляд, наиболее эффективной работой по противодействию киберэкстремизму будут обладать учителя информатики и ИКТ. Но это не говорит, о том, что всю работу в образовательном учреждении по превенции киберэкстремизма и экстремизма вцелом будет проводить один педагог. «Универсальных методов борьбы с таким многоплановым и сложным явлением, как молодежный экстремизм, не существует. Профилактика каждого вида экстремистских проявлений требует особого подхода. Он складывается из комплекса мер, которые лишь в совокупности могут дать желаемый результат» [8]. Таким образом, мы можем сказать, что работа по превенции киберэкстремизма в молодежной среде требует комплексного подхода, включающего работу с детьми и с педагогами.

Я.И. Гилинский под превенцией различных форм девиаций предлагает понимать «такое воздействие общества, институтов социального контроля, отдельных граждан на причины девиантного поведения и факторы, ему способствующие, которое приводит к сокращению и/или желательному изменению структуры девиаций и к несовершению потенциальных девиантных поступков» [3].

Деятельность по превенции девиантного поведения выражается в раннем выявлении, изучении, оценке начальных признаков отклоняющегося поведения и их условий; прогнозировании негативных тенденций в формировании личности; воспитательно-профилактическом воздействии. Таким образом, превенция киберэкстремизма в молодежной среде включает в себя [16]:

- сферу пропедевтики;
- сферу профилактики.

Пропедевтика – «введение в какую-либо науку, предварительный вводный курс, систематически изложенный в сжатой и элементарной форме» [11]. Настало время говорить о необходимости подготовки молодежи к жизни, работе, саморазвитию в виртуальном мире без опасения быть вовлеченным в негативную или преступную деятельность. В контексте этой задачи, помимо обязательного минимума знаний по основам информатики и ИКТ, должны преподаваться базовые знания в области предупреждения возможного вовлечения в киберэкстремистскую деятельность.

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» [9].

Следует заметить, что механизмы превенции явлений киберэкстремизма необходимо включать в образовательную и воспитательную работу уже в школах, так как легче всего подобные явления распространяются именно среди старших школьников, накладываясь на подростковый максимализм и психологические особенности развивающейся личности. И в обязательном порядке необходимо проводить разъяснительную работу среди молодежи, привлекать их к выполнению различных проектов и решению задач, помогающих развить критическое мышление, просвещающих и в дальнейшем не позволяющих вовлечь молодежь в киберэкстремистскую деятельность

*2. Применение метода проектов и форм внеурочной деятельности учащихся по превенции киберэкстремизма среди молодежи*

В качестве одного из ведущих средств противодействия киберэкстремизму мы предлагаем использовать в учебном процессе такую технологию обучения, как «метод проектов». Метод проектов – один из основных современных активных инновационных методов обучения. Он широко внедряется в

образовательную практику в России благодаря благотворительной программе Intel® «Обучение для будущего». Проектность – определяющая черта современного мышления. Проектное мышление, проектная деятельность – процесс обобщенного и опосредованного познания действительности, в ходе которого человек использует технологические, технические, экономические и другие знания для выполнения проектов по созданию культурных ценностей [13]. Метод проектов особенно эффективен, если его использовать в рамках учебной дисциплины, в которой решаются большие практические задачи, например, в рамках дисциплины «Информационная безопасность» (для большинства специальностей) или «Информационная безопасность в образовании» (для педагогических специальностей). Особенно важно понимать его значимость в подготовке студентов педагогических специальностей и разработке материалов по использованию проектов в педагогической деятельности.

Проект – это некий замысел, мысль или идея, которые описаны каким-либо образом, который раскрывает всю их сущность и дает возможность практической реализации данного замысла. Естественно, что при решении какой-либо практической или теоретической проблемы получается тот или иной результат. И именно идея о направленности учебного процесса на этот результат и лежит в основе метода проектов.

Метод проектов предполагает самостоятельное решение учащимися какой-то теоретической или практической проблемы, за счет совокупности учебно-познавательных действий и приемов, и обязательную презентацию полученных учащимися результатов. Метод проектов предполагает совместные действия преподавателя и учащегося и, таким образом, позволяет отойти от жесткой авторитарности в обучении, которая присутствует при применении традиционных форм. Этот метод ориентирован на самостоятельную работу учащихся и, как следствие, позволяет учащимся не только получить те или иные знания, но и научиться приобретать знания самостоятельно, а также формирует навыки использования полученных знаний при решении

теоретических и практических задач, что очень важно при противодействии вовлечения в киберэкстремистские деяния.

На основании вышеизложенного можно выделить ряд основных требований при использовании метода проектов:

1. Наличие проблемы, значимой в исследовательском плане;
2. Практическая или теоретическая значимость результатов;
3. Самостоятельная деятельность ученика;
4. Структурирование проекта и использование исследовательских методов [18].

Главная цель проекта с точки зрения педагогики – сформировать взаимосвязанные знания, умения, навыки, ценностные отношения и способы деятельности, а также умение использовать все вышеперечисленное.

Главная задача педагога – научить учащихся мыслить самостоятельно. При таком подходе преподаватель выступает лишь организатором и координатором деятельности учащихся, которые, в свою очередь, приобретают возможность проявить свою индивидуальность и творческое мышление.

Можно выделить следующие виды проектов, которые эффективно использовать при организации превенции явлений киберэкстремизма в молодежной среде:

**Информационные проекты** направлены на сбор информации о каком-то объекте, явлении. Участники проекта должны проанализировать эту информацию и представить широкой аудитории только обобщенные факты. Такие проекты становятся частью исследовательских проектов.

**Исследовательские проекты** по структуре напоминают научные работы. Они состоят из пояснения актуальности темы проекта, формулировки проблемы, обозначения задач исследования, выдвижения и проверки гипотез решения проблемы, обсуждение полученных результатов и, конечно, выводы.

**Прикладные проекты**, в которых результат обозначен в начале и ориентирован на социальные интересы самих участников. Результат может быть представлен в любой форме: от словаря терминов до проекта закона.

**Ролевые проекты**, в которых учащиеся примеряют на себя те или иные роли, которые определяются характером и содержанием проекта. Герои, которых изображают ученики, имитируют политические, общественные или другие отношения, которые могут быть осложнены придуманными участниками ситуациями.

**Творческие проекты**, ориентированные на самовыражение участников проекта. Они имеют свободную форму, как в проведении проекта, так и в типе получаемого результата, которым может быть все, что угодно: совместная газета, видеофильм, праздник и т.д.

Преимущества использования проектного метода в обучении достаточно очевидны. Так как при таком подходе к обучению, знания добываются самостоятельно и, что самое главное, с хорошей мотивацией, то учащиеся усваивают эти знания очень прочно и, как следствие, могут эффективно их применять. Это основное преимущество, однако, не единственное. Использование проектного метода позволяет:

- работать с личным сознанием учащихся;
- развить их индивидуальные навыки;
- сформировать навыки общения и работы в команде.

Использование метода проектов дает все вышеперечисленные преимущества, только если проект успешен. Однако не каждый проект может считаться успешным. Успешный проект имеет следующие характеристики:

**Учащиеся находятся в центре образовательного процесса**. Проекты дают возможность учащимся строить свою учебную деятельность в соответствии с их интересами и увлечениями. Учащиеся активно участвуют в работе над проектом, т.к. они учатся через поиск, рассматривают различные варианты решения задач проекта.

**Работа над проектом соответствует образовательным стандартам и программе обучения.** При разработке проекта за основу принимают центральные понятия учебной дисциплины, соответствующей местным или

национальным образовательным стандартам. Проект имеет четкие цели, определяющие планируемые результаты обучения.

**Проекты управляются основополагающими вопросами.** Проекты помогают учащимся осмысленно исследовать проблемы, обозначенные в основополагающем вопросе, вопросах учебной темы, частных вопросах. Эта триада помогает учащимся погрузиться в сложные проблемы реального мира и исследовать их.

**Проекты включают в себя разнообразные виды оценки.** Задачи, стоящие перед учащимся на каждом этапе проекта, четко сформулированы, и их выполнение контролируется с помощью умения отвечать на вопрос: чему нужно научиться для решения поставленной задачи?

**Проекты имеют связь с реальным миром.** Темы проектов связаны с жизнью учащихся и миром за пределами класса. Это означает, что учащиеся исследуют реальные проблемы и могут представить свои результаты реальной аудитории, пользоваться ресурсами сообщества, консультироваться с экспертами в рамках своей темы исследования и общаться с использованием ИТ.

**Учащиеся представляют свои достижения через конечный продукт исследования.** Проекты обычно заканчиваются тем, что учащиеся демонстрируют свои знания через конечные продукты исследования или презентации. Конечные продукты исследования дают учащимся возможность самовыражения и осознания самостоятельности учебной деятельности.

**Информационные технологии обеспечивают и повышают эффективность обучения.** Информационные технологии используются для развития мыслительных умений и знаний по предмету. Деятельность учащихся не ограничивается работой в классе. Они взаимодействуют с удаленными классами, делятся информацией на web-сайтах или проводят презентации за пределами класса, решая реальные проблемы.

**Для работы над проектом необходимы мыслительные умения высокого уровня.** Работа над проектом способствует развитию

метапознавательных и познавательных мыслительных умений, таких, как самооценка, решение проблем, принятие решений.

**Образовательные стратегии разнообразны и обеспечивают многообразные стили учения.** Применение целого спектра образовательных стратегий гарантирует возможность вовлечения каждого ученика в деятельность по реализации проекта. Обучение может включать различные виды групповой работы, деятельность, обеспечивающую обратную связь с учителем и одноклассниками.

В ходе выполнения проектов достигаются следующие результаты:

1. Формируются и отрабатываются:

- Навыки сбора, систематизации, классификации, анализа информации.
- Навыки публичного выступления (ораторское искусство).
- Умения представить информацию в доступном, эстетичном виде.
- Умение выражать свои мысли, доказывать свои идеи.
- Умение работать в группе, в команде.
- Умение работать самостоятельно, делать выбор, принимать решение.

2. Расширяются и углубляются знания в различных предметных областях.

3. Повышается уровень информационной культуры, включающий в себя работу с различной техникой (принтер, сканер, микрофон и т.д.)

4. Обучающийся довольно основательно изучает ту компьютерную программу, в которой создает проект и даже больше - программы, которые помогают лучше представить свою работу.

5. Учащийся имеет возможность воплотить свои творческие замыслы.

6. Отношения с педагогом переходят на уровень сотрудничества.

7. Повышается самооценка тех учащихся, которые по той или иной причине считали себя неуспешными [18].

Все вышеперечисленное дает обучающемуся возможность стать успешной, саморазвивающейся, самодостаточной личностью, имеющей знания, умения и навыки по противодействию киберэкстремизма и других угроз в ИКТ-среде. Стоит отметить, что немаловажным фактором развития личности способствует выбор эффективных форм внеурочной деятельности учащихся. Формы внеурочной деятельности должны соответствовать тематике проектов и дополнять их.

Внеурочные мероприятия – это занятия, ситуации в коллективе, организуемые преподавателями с целью непосредственного воспитательного воздействия на учащихся. Также сюда можно отнести игры, дискуссии, круглый стол, встречи с психологами и специалистами в области информационной безопасности.

Внеурочные мероприятия по сравнению с обычными занятиями, строятся на другом материале, проводятся в других формах и их основой в большей степени является самостоятельность обучающихся.

Целью внеурочных мероприятий – является обеспечение гармонического всестороннего развития учащихся, сочетающего в себе духовное обогащение и моральную чистоту.

Внеурочные мероприятия сочетают в себе не только задачу сформировать целостную личность, но и развить у учащихся следующие черты:

- взаимопомощь;
- дружбу;
- умение работать в коллективе;
- умение слушать оппонента;
- умение защищать свою точку зрения.

Данная форма организации занятий помогает обогатить молодых людей новыми интересными для них фактами и понятиями, отражающими различные стороны жизни человека и общества, усилить их интерес к изучению науки.

Развить интерес у учащихся к какой-то проблеме довольно сложная задача, однако с помощью внеурочных мероприятий это становится намного проще, за

счёт привлечения средств занимательности, проведения круглых столов, конкурсов, встреч со специалистами в области информационной безопасности.

Функции внеурочного мероприятия определяются его целью и задачами, можно выделить 3 функции:

- обучающая;
- воспитательная;
- развивающая.

В рамках проведения внеурочного занятия по теме превенции киберэкстремизма, обучающая функция имеет скорее вспомогательную роль и заключается в формировании у учащихся определенных навыков поведения, общения в ИКТ-среде.

Воспитательная функция реализуется за счет формирования личностных качеств учащегося, которые, непосредственно, влияют на поведения человека в сети, а также его отношения к мнению других пользователей. Формируется толерантная составляющая.

Развивающая функция отражена в развитии индивидуальных способностей и интересов учащихся, вовлечение в деятельность по противодействию различным информационным угрозам, в том числе киберэкстремизму.

Выделяются некоторые особенности организации внеклассных мероприятий, отличающие их от обычных занятий:

1. Добровольная организация и участие. Учащиеся в зависимости от интересов и склонностей самостоятельно принимают участие в массовой и индивидуальной работе во внеурочное время.

2. Многообразие форм и методов. Очень трудно перечислить все формы и методы внеурочной деятельности.

3. Массовость. Она охватывает интересы большого количества учащихся, позволяет затронуть множество проблем. Массовые ее формы дополняются групповыми и индивидуальными занятиями.

Для успешной работы по превенции явлений киберэкстремизма среди молодежи необходимо комбинировать проектный метод и различные формы

внеурочной работы. Например, можно использовать следующие формы вместе с методом проектов:

- Круглый стол (обсуждение темы проектов, анализ выполнения проектов).
- Стенды и газеты (демонстрация проекта).
- Игровые формы (ролевые игры, «КВН», «Что? Где? Когда?» по теме проекта).
- Встреча со специалистом (беседа с экспертом по теме проекта).

На основе использования этих форм вместе с проектным методом достигается комплексный подход к формированию знаний, умений и навыков по выявлению и противодействию киберэкстремизму и другим угрозам современного информационного общества.

*3. Примеры проектов по превенции вовлечения в киберэкстремистскую деятельность*

В данном разделе представлены примеры проектов внеклассных мероприятий для старшеклассников по противодействию вовлечения молодежи в киберэкстремистскую деятельность, разработанных будущими учителями информатики и реализованных в рамках программы Intel® «Обучение для будущего» и педагогической практики.

***Проект внеклассного мероприятия***

***«Терпи, казак, толерантным будешь»*** [10]

***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 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-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:**

1. 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:**

1. 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.

***Проект внеклассного мероприятия для старших классов***

***«Угрозы кибертерроризма»*** [12]

***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.

***Проект «Киберэкстремизм: история и современность»*** [15]

***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.

### *Проект внеклассного мероприятия для старшеклассников «Кибертерроризм: история и современность»* [1]

***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)

***Проект внеклассного мероприятия для старшеклассников***

***«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.

***Проект внеклассного мероприятия для старшеклассников «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.

***Учебный проект для старшеклассников***

***«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.

***Учебный проект для старшеклассников***

***««Информационная война» с киберпреступлениями, киберэкстремизмом и кибертерроризмом»*** [2]

***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.

Все представленные проекты были проведены с учениками школ и показали свою высокую практическую и теоретическую значимость. Обучаемые в ходе подведения итогов проектов отметили востребованность полученных знаний и навыков, активно и с удовольствием выполняли поставленные перед ними задачи.

*Выводы*

Подводя итог проблемы противодействия распространения идей киберэкстремизма среди молодежи, требуется обратить внимание на особенности подросткового возраста, воспитанию и образованию детей. Работа по превенции киберэкстремизма должна быть комплексной и грамотно выстроенной, проводиться с использованием новейших методов, которые были бы интересны не только педагогам, но и учащимся школ и студентам вузов. Метод проектов – это лишь один из множества методов по противодействию киберэкстремизму, но разработанность и технологическая поддержка этой технологии делает его очень эффективным и востребованным в наше время. Кроме того, в совокупности с методом проектов стоит применять эффективные формы внеурочной деятельности учащихся такие, как: круглый стол, стенды, газеты, игровые формы и т.д. Метод проектов позволяет сформировать у учащегося основы самостоятельной работы с информацией, способами ее получения, хранения и обработки. Эти навыки позволяют грамотно сепарировать достоверную и недостоверную информацию. С применением этих методов у учащегося формируется толерантное отношение к собеседнику, сдержанное восприятие другого мнения, понимание правил поведения и этикета в сети Интернет. Стоит помнить, что превенция киберэкстремизма состоит из комплекса взаимосвязанных мер, например, таких, как метод проектов и внеурочная деятельность. Нельзя оставить без внимания и административную помощь государства по борьбе с информационными угрозами, а также внедрение и усовершенствование технических мер. Однако,

работа с молодежью стоит на первом месте. Нужно с самого раннего возраста, воспитывать и развивать ребенка «в ногу со временем», используя все новейшие методы педагогики. Основной проблемой организации противодействия киберэкстремистской деятельности является недостаточное методическое оснащение, состоящее из методов и форм работы с учащимися. Организация их учебной и внеурочной работы. Правильно выстроенная учебная и внеурочная деятельность учащегося является залогом успешного формирования личности, способной противостоять современным угрозам информационного общества, в том числе, киберэкстремизму.

Публикация выполнена в рамках работы над проектом РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Литература:

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. – 322с. – с. 186-199.

2. 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. – 322с. – с. 280-293.

3. Гилинский Я.И. Социология девиантного поведения / Я.И. Гилинский, В.С. Афанасьев. – СПб. : ИСИ РАН, 1993. – 167 с.

4. Громов И. А., Мацкевич И. А., Семёнов В. А. Западная социология. — СПб.: ООО «Издательство ДНК», 2003. — С. 532.

5. Доколин А.С., Чернова Е.В. Превенция вовлечения молодежи в киберэкстремистскую деятельность посредством компьютерных игр // Фундаментальные исследования. - 2014. – №12 (часть 5). – С. 1074-1077.

6. 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.

7. Кубякин Е.О. Молодежный экстремизм в условиях глобализации информационно-коммуникационной среды общественной жизни: дис. канд. социол. наук: 22.00.04. - Краснодар, 2012. - 351 с.

8. Некрасов Д.Е. Расово-этнический экстремизм (криминологический аспект): дис. канд. юрид. наук. – Рязань, 2006. – С. 12-14.

9. Ожегов С.И. Словарь русского языка: Около 57000 слов / [Под ред. Н.Ю.Шведовой]. –15-е изд. – М.: Русский язык, 1984. – 816 с.

10. 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. – 322с. – с. 143-160.

11. Большой энциклопедический словарь [Гл. ред. А.М. Прохоров]. 2-е изд., перераб. и доп. – СПб. : Норинт, 2004. – 1456 с.

12. 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. – 322с. – с. 260-270.

13. Социализация студентов в профессиональном образовании: монография / Л.И. Савва, А.Л. Солдатченко, Е.Б. Плотникова, Е.И. Рабина, Л.С. Рязанова; под общей ред. Л.И. Савва. – М.: Издательский дом Академии Естествознания, 2012. – 300 с.

14. Сирота Н.М. Политология: Учебное пособие. – СПб. : Национальный открытый институт России, 2009. – 113 с.

15. 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. – 322с. – с. 218-224.

16. Чернова Е.В. Компетенции педагогических кадров в области превенции идеологии киберэкстремизма среди молодежи // Фундаментальные исследования. – 2013. – № 10. - часть 9. – с. 2075-2079.

17. Чупров В.И., Зубок Ю.А. Молодежный экстремизм: сущность, формы проявления, тенденции. – М.: Academia, 2009. – 320 с.

18. Факультативный курс «Основы безопасности жизнедеятельности в Интернет»: метод. пособие / М.И. Шубинский – СПб.: МПСС, 2010. – 68 с.