УДК 004.41

ПЕДАГОГИЧЕСКИЕ, ПСИХОЛОГИЧЕСКИЕ И ЛИНГВИСТИЧЕСКИЕ АСПЕКТЫ ПРОБЛЕМЫ КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ В ВУЗЕ

Макашова В.Н., Трутнев А.Ю., Новикова И.Н., Ганиева Л.Ф.

ФГБОУ ВПО «Магнитогорский государственный технический университет имени Г.И. Носова», Магнитогорск, e-mail: lilit1708_@mail.ru

В статье поднимается проблема киберэкстремизма, его влияния на современную студенческую молодежь, указывается на её комплексный характер, описываются способы противодействия существующим угрозам. На данный момент тема является особо актуальной и обусловлена широким применением современных информационных технологий в вузе. Для эффективной защиты от киберугроз авторы предлагают учитывать как чисто технические, так и психолого-лингвистические аспекты. В связи с этим рассмотрены основные механизмы обеспечения информационной безопасности и даны рекомендации по использованию методов противодействия киберэкстремизму. Также затронуты проблемы неосведомленности родителей и обучающихся о таких видах угроз. Выявлена проблема развития киберэкстремистских наклонностей среди молодежи в вузе. Представлена статистика киберэкстремистских преступлений и мера наказания за содеянное. Предложены способы решения данной проблемы.

Ключевые слова: киберэкстремизм, киберпространство, психология, педагогика, лингвистика, информационная безопасность

PEDAGOGICAL, PSYCHOLOGICAL AND LINGUISTIC CYBER EXTREMISM ASPECTS OF YOUTH IN HIGH SCHOOL

Makashova V.N., Trutnev A.Y., Novikova I.N., Ganieva L.F.

Nosov Magnitogorsk State Technical University, Magnitogorsk, e-mail: lilit1708_@mail.ru

The article raises the problem of cyber extremist, its impact on today's college students, points to its complex nature, describes how to counter existing threats. At this time the theme is particularly relevant and due to the extensive use of modern information technology in higher education. For effective protection against cyber threats authors propose to consider as a purely technical and psycho-linguistic aspects. In this regard, the basic mechanisms of information security and recommendations on the use of methods of combating cyber extremism. Also affected by the problem of ignorance of parents and students about these kinds of threats. Has the problem of cyber extremist tendencies among young people in high school. Statistics presented cyber extremist crimes and punishment for their actions. The ways to solve this problem.

Keywords: cyber extremism, cyberspace, psychology, education, linguistics, information security

Современный мир экстремален по скорости развития событий и степени возникающих рисков. Культура и этика выдвигают повышенные требования к уровню ответственности человека, принуждая проявлять волевые качества, способность противостоять собственным негативным эмоциям (страху, гневу, агрессии) и оставаться человеком, а не уподобляться животным, несмотря ни на что. Контркультура в образе киберэкстремизма, напротив, снимает все культурные и этические ограничения с человека и группы, действуя по принципу «чем хуже, тем лучше». Безусловно, в этом смысле киберэкстремизм является одним из механизмов усиления негативных процессов в обществе и в культуре. Неумение жить в поликультурном, многоголосном мире, где трудно быть услышанным, замеченным. Это мир, где идет тотальная конкуренция за внимание. И ясно (еще с античности), что сжечь библиотеку легче, чем написать книгу, а шансы привлечь к себе внимание таким действием – более велики. Сегодня благодаря СМИ любое событие может стать мировой новостью. Экономические условия жизни не способствуют выбору в пользу культуры и этики. Экономика задает нам правила игры. Экономика работает, чтобы продавать. Для продажи нужно заполучить внимание и эмоции потенциального клиента. Наш мир превращен в огромную сцену, где нужно «продать себя». Но очевидно, что привлечь внимание выдающимся талантом дано немногим, зато скандал, агрессия – средство вседоступное.

На сегодняшний день сторонники экстремизма с легкостью могут использовать возможности, предлагаемые информационно-коммуникативными технологиями. Например, создание и регистрация информационных ресурсов, направленных на формирование и поддержку определенного мнения по ключевым вопросам, на обмен опытом, на вербовку последователей и др. В различных социальных сетях созданы многочисленные группы, целью которых является распространение информации экстремистской направленности.

Во всех видах экстремизма присутствуют общие черты: угроза, фанатизм, одержимость в стремлении навязать свои принципы и взгляды оппонентам; опора на чувства, инстинкты, предрассудки, а не на разум; неспособность к толерантности, компромиссам либо игнорирование их.

Молодежь, особенно в возрасте 13–22 лет, является более подверженной экстремистским идеям, т.к. является активным и основным пользователем Интернета. Этому возрасту присуще обостренное чувство справедливости, попытка самовыражения, поиск ценностей и смысла жизни. Кроме того, в это время подросток озабочен желанием найти свою группу, поиском собственной идентичности, которая формируется по самой примитивной схеме «мы – они». Также у молодежи этого возраста неустойчивая психика, они легко подверженны внушению и манипулированию. Этим подсознательным запросам как нельзя лучше соответствуют экстремистские субкультуры с их четким разделением на «наших» и «не наших» и четко провозглашенными границами добра и зла (а также зримыми образами этого зла в лице «чужих» – темнокожих, евреев, кавказцев и т.д.).

В результате, в последние годы наблюдается обострение молодежного экстремизма, который в настоящее время может рассматриваться как проблема общегосударственного значения и угроза национальной безопасности России.

Киберэкстремистская деятельность молодежных групп осуществляется в отношении властных структур, отдельных политиков, объединений, социального строя или социальных групп, религиозных общин, религиозных деятелей, наций.

В современных условиях исследование форм проявления киберэкстремизма в молодежной среде имеет важное значение для деятельности государственных органов и спецслужб по предупреждению правонарушений со стороны молодежных неформальных объединений. Распространение экстремизма в молодежной среде в настоящее время приобрело очень большие масштабы и имеет опасные последствия для будущего нашей страны, так как подрастающее поколение – это ресурс национальной безопасности, гарант поступательного развития общества и социальных инноваций.

Экстремизм – (лат. extremus – крайний) – ориентация в политике на радикальные идеи и цели, достижение которых осуществляется в основном силовыми и нелегитимными и противоправными методами и средствами.

Киберэкстремизм – один из видов киберугроз, которые вызывают общую озабоченность. В число его целей могут входить политическая или экономическая дестабилизация, кража военных или гражданских активов и ресурсов в политических целях [1].

Думается, понятие киберэкстремизма следует рассматривать как комплексную проблему современности, включающую в себя не только чисто технические аспекты, но и психологические, педагогические, а также лингвистические. Такой подход призван обеспечить более объективный и всесторонний анализ существующих угроз и способствовать выявлению важнейших характеристик упомянутого социально опасного явления.

Очевидно, что понимание и использование психологических механизмов воздействия на человека существенно увеличивает негативный эффект от действий злоумышленников. Соответственно, необходимо разработать приёмы психологической защиты, позволяющие эффективно блокировать угрозу личности и волевое давление извне.

Лингвистический компонент киберугроз также требует пристального внимания. Он тесно связан с психологическими механизмами и способен усилить воздействие на целевую аудиторию. В условиях глобализации владение иностранными языками является очень важным, поскольку сетевое общение носит трансграничный характер и позволяет быстро устанавливать контакты по всему миру. Однако лингвистические навыки успешно используются не только добропорядочными гражданами для расширения возможностей личного и профессионального общения. В арсенале злоумышленников, действующих в виртуальном пространстве, умение оказывать влияние на аудиторию с использованием лингвистических средств занимает одно из существенных мест. В связи с этим особую актуальность приобретает понимание особенностей функционирования языковых механизмов в процессе коммуникации.

С сожалением приходится констатировать, что в условиях современного социально-экономического развития Российской Федерации масштабы компьютерной преступности настолько существенны, что представляют реальную угрозу общественной жизни.

Подтверждением роста таких преступлений являются статистические данные Совета безопасности РФ, согласно которым в начале века выявлено более 700 тыс. попыток осуществления компьютерных атак на официальные информационные ресурсы

органов государственной власти при этом более 50 тыс. О росте и масштабах компьютерных преступлений наглядно свидетельствуют приведённые ниже данные [8]. Средний показатель количества уголовных дел, по которым производство приостановлено, составляет 43 % и ярко отражает низкую степень профессионализма сотрудников правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению этих преступных посягательств [9]. Основная часть преступлений – это компьютерные преступления, связанные с незаконным доступом к информации и с использованием вредоносных программ. Анализ сложившейся ситуации показывает, что около 20 % преступников – люди в возрасте до 18 лет, 60 % – лица от 18 до 30 лет, около 65 % из них имеют высшее либо незаконченное высшее образование [11].

Серьезной мерой наказания является уголовное преследование за пропаганду киберэкстремизма в Интернете. В прошлом году было вынесено 71 судебное решение за пропаганду, 50 были связаны с распространением запрещенных материалов в Интернете, социальных локальных сетях.

Материалы располагались:

- на сайтах – 18;
- в социальных сетях и форумах – 29;
- в виде фильмов в локальной сети – 2;
- в рассылках по электронной почте – 1.

Приговоры выносились по ст. 282 УК РФ (возбуждение национальной ненависти) и ст. 280 УК РФ (публичные призывы к осуществлению экстремистской деятельности).

В связи с этим часто обсуждается вопрос о правомерности применения ст. 280 и ст. 282 УК в Интернете. Состав ст. 280 и 282 УК относится к любым публичным высказываниям, и Интернет не может быть исключением. И тут важно верно оценить степень публичности. К сожалению, критерий публичности до сих пор никак не оценивается. В 2011 г. в наказания распределились следующим образом:

- лишение свободы – 5;
- условные сроки – 23;
- штрафы – 10;
- обязательные работы – 9;
- исправительные работы – 2;
- ограничение свободы – 1.

Таким образом, несмотря на значительный рост числа наказанных за пропаганду в Интернете, создается впечатление, что правоохранители по преимуществу занимаются имитацией борьбы с экстремизмом, и тем более с киберэкстремизмом, в мировой паутине.

Особенно актуальна данная проблема среди молодежи. Сложная социально-политическая среда, в которой приходится существовать современной российской молодежи, неопределенность ее социальных перспектив, приводит к тому, что конфессиональная либо этническая общность начинают рассматриваться в качестве референтных групп. Что способствует усилению и актуализации локальных солидарностей, которые предоставляют молодому человеку более доступные для понимания и практического воплощения ценности. Рост интолерантных установок, гиперидентичность, в том числе в сфере этнического самосознания, подкрепляются достаточно низким уровнем гражданской интеграции. Агенты социализации, способные транслировать идеи гражданской общности в молодежной среде, либо перестали существовать, либо в значительной степени утратили авторитет. Сама специфика молодежной среды способствует усилению объединяющих целей и ценностей.

Высшая школа, будучи одним из основных проводников гражданской интеграции, способна эффективно внедрять принцип толерантности в сознание и поведенческие модели современной молодежи.

Общество, по сути, пребывает в состоянии растерянности, под воздействием атмосферы неуверенности, опасений. И немалую лепту в формирование этой атмосферы вносят СМИ. Нет свидетельств готовности журналистского сообщества профессионально обсуждать эти вопросы с экспертами в области обеспечения безопасности.

Подытоживая сказанное, можно назвать некоторые направления комплексного исследования проблематики информационного противодействия угрозе:

- правовые аспекты функционирования СМК, включая Интернет;
- идейно-теоретические аспекты, в том числе создание системы социализации подрастающих поколений, формирования толерантности и культуры мира.

Информационная война протекает, если можно так выразиться, в различных пространственных координатах. Не только связанных с непосредственными боевыми действиями или операциями, но и в пространстве культурном, религиозном, научном, экономическом.

Если политика властей относительно СМИ выстроена грамотно, если налажено взаимодействие и доверие, СМИ могут служить серьезным орудием в борьбе с киберэкстремизмом. В противном случае они могут стать средством манипулирования

общественным мнением, невольным выразителем и пропагандистом идеологии терроризма. Самое нелепое, что может сделать власть, – ограничить свободу прессы и доступ к информации. В такой ситуации начинает работать альтернативная система пропаганды – слухи. А они в информационной пустоте имеют страшную разрушительную силу.

Выделяются следующие основные тенденции развития компьютерной преступности [12]:

- высокие темпы роста;
- корыстный умысел совершенных компьютерных преступлений;
- усложнение способов совершения компьютерных преступлений и появление новых видов противоправной деятельности в сфере компьютерной информации;
- рост уровня профессионализма компьютерных преступников;
- обновление компьютерных преступников и увеличение числа лиц, ранее не привлекавшихся к уголовной ответственности;
- рост материального ущерба от компьютерных преступлений в процентном соотношении потери от прочих видов преступлений;
- совершение преступлений с использованием компьютерных сетей.

Так какова же причина компьютерных преступлений? Ответить однозначно нельзя. Это и сложность в поисках следов преступников, и скрытность. Так, шансов быть найденным у компьютерного преступника гораздо меньше, чем у грабителя банка, даже при поимке у него меньше шансов попасть за решетку. Обнаруживается около 1% компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, составляет меньше 10% [8].

К причинам или мотивам, по которым совершаются преступления в области компьютерной информации, можно отнести:

- получение злоумышленником материальных ценностей (61%);
- хулиганство (17%);
- месть (5%);
- компьютерный шпионаж и слежка (7%);
- самовыражение (5%);
- случайные факторы (5%).

Причем наиболее типичными преступными целями являются:

- подделывание счетов;
- фальсификация платежных документов;
- хищение денежных средств;
- перечисление денежных средств на фиктивные счета;
- совершение покупок;
- незаконные валютные операции;
- незаконное получение кредитов;
- манипуляции с недвижимостью;
- продажа конфиденциальной информации;
- хищение материальных ценностей или товаров.

При этом, как правило, с хищением денежных средств связано 52% преступлений, с разрушением и уничтожением средств компьютерной техники – 16%, с подменой исходных данных – 12%, с хищением информации и программ, а также с хищением услуг – 10% [8].

Оценка вероятных источников угроз безопасности глобальных сетей

(по степени потенциальной опасности)

Категория нарушителей:

1. Внутренние пользователи системы – 58%.
2. Независимые хакеры – 51%.
3. Бывшие служащие – 45%.
4. Конкуренты – 44%.
5. Компьютерные террористы – 43%.
6. Консультанты и временные сотрудники – 32%.
7. Персонал вычислительных систем – 29%.
8. Сотрудники иностранных разведок – 14%.
9. Поставщики оборудования и программного обеспечения – 13%.
10. Клиенты – 7%.

Борьбу с киберэкстремизмом необходимо усилить. Речь не идёт о голословной пропаганде, в цветах показывающей негативные качества мелких экстремистов. Необходимо донести до людей идеи и мысли об истинной опасности киберэкстремизма. Важно, чтобы люди знали, с чем они могут столкнуться, на что они идут, выражая симпатии идеям экстремистского толка. Информационная борьба должна идти в первую очередь не против самого явления киберэкстремизма, а за умы людей, их осознание современных общественно-политических реалий. Ведь проблема киберэкстремизма в целом и в СМИ в частности исключительно актуальна и важна в условиях социальных изменений современного российского общества. Она имеет правовые, социологические, социально-психологические и духовно-нравственные аспекты.

Список литературы

1. О противодействии терроризму: федеральный закон от 6 марта 2006 г. № 35-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 11. – Ст. 1146.

2. Закон РФ «О средствах массовой информации» // Официальный сайт Роскомнадзора. 2011. URL: http://www.rsoc.ru/docs/preduprezhdenija._st.4_._2012_g._obshhaja.rtf.

3. Ожегов С.И. Словарь русского языка. – 17-е изд. – М., 1995.

4. Сабитов Р.А. Расследование преступлений экстремистской направленности: методикаи квалификация: учеб. пособие / Р.А. Сабитов, П.В. Худяков. – Челябинск: Челяб. Юрид. Ин-т. МВД России, 2010.

5. Сазанова Е. Молодежный экстремизм как социальный феномен // Экстремизм и другие криминальные явления. – М., 2008.

6. Хуторской А.В., Король А.Д. Диалогичность как проблема современного образования (философско-методологический аспект) // Вопросы философии. – 2008. – № 4.

7. Альперович В., Верховский А., Юдина Н. Между Манежной и Болотной: Ксенофобия и радикальный национализм и противодействие им в 2011 году в России // Центр «СОВА». 2012. 24 февраля. URL: http://www.sova-center.ru/racismxenophobia/publications/2012/02/d23739.

8. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: «Диа-Софт», 2011. – 38 с.

9. Бирюков А.А., Информационная безопасность: защита и нападение. – 2012. – URL: http://e.lanbook.com/books/element.php?pl1_id=39990.

10. Бехтерев В.М., Внушение и его роль в общественной жизни. – М.: Изд-во «Лань» 2013. – URL: http://e.lanbook.com/books/element.php?pl1_id=30536.

11. Семечкин Н.И., Психология социальных групп. – М.: Изд-во «Лань», 2011. – URL: http://e.lanbook.com/view/book/2999/page20.

12. Хайдарова В.Ф., Краткий словарь интернет – языка. – М.: Изд-во «Лань», 2013. – URL: http://e.lanbook.com/view/book/44286/page118.

13. Сабитов Р.А. Расследование преступлений экстремистской направленности: методика и квалификация: учеб. пособие / Р.А. Сабитов, П.В. Худяков. – Челябинск: Челяб. Юрид. Ин-т. МВД России, 2010.

14. Зеркина. Е.В., Чусавитина. Г.Н. Подготовка будущих учителей к превенции девиантного поведения в сфере информационно-коммуникационных технологий: монография. – Магнитогорск: МаГУ, 2008. – 185 с.

15. Чусавитина Г.Н., Чернова Е.В. Толерантность как средство борьбы с экстремизмом и терроризмом // Современные проблемы науки и образования: тезисы докл. XLIII внутривуз. науч. конф.преп. МаГУ. – Магнитогорск. 2011. – С. 100–102.

References

1. On Combating Terrorism: the federal law of March 6, 2006 no. 35-FZ // Meeting of the legislation of the Russian Federation. 2006. no. 11. Art. 1146.

2. Federal Law «On mass media» // Official WebsiteРоскомнадзора.2011.URL:http://www.rsoc.ru/docs/preduprezhdenija._st.4_._2012_g._obshhaja.rtf.

3. Ozhegov S.I. Russian dictionary. 17 th ed. M., 1995.

4. Sabitov R.A. Investigation of extremist crimes: qualification testing procedures / R.A. Sabitov, P.V. Khudiakov: Proc. allowance. Chelyabinsk Chelyaba. Jurid. Inst. Russian Ministry of Internal Affairs, 2010.

5. Sazanova E. Youth extremism as a social phenomenon // Extremism and other criminal phenomena. Moscow, 2008.

6. The farm A.V., King A.D. Dialogic as a problem of modern education (philosophical and methodological aspect) // Problems of Philosophy. 2008. no. 4.

7. Al'perovich V., Verkhovsky A., Yudina N. Between the Manege and the Swamp: xenophobia and radical nationalism and opposition to them in 2011 in Russia // Center «owl». 2012 February 24th. URL: http://www.sova-center.ru/racismxenophobia/publications/2012/02/d23739.

8. Domarev V.V. Data protection and security of computer systems. K.: «Dia-Soft», 2011. 38 p.

9. Biryukov A.A. Information security: defense and attack. 2012. URL: http://e.lanbook.com/books/element.php?pl1_id=39990.

10. Bekhterev V.M.., Suggestion and its role in public life // Publisher «Lan» 2013. URL: http://e.lanbook.com/books/element.php?pl1_id=30536.

11. Semechkin N.I., Psychology of social groups // Publisher «Lan» 2011. URL: http://e.lanbook.com/view/book/2999/page20.

12. Khaidarova V.F., Concise Dictionary of the Internet Publishing Language // «Lan» 2013. URL: http://e.lanbook.com/view/book/44286/page118.

13. Sabitov R.A. Investigation of extremist crimes: technique and skills / R.A. Sabitov, P.V. Khudiakov: Proc. allowance. Chelyabinsk Chelyaba. Jurid. Inst. Russian Ministry of Internal Affairs, 2010.

14. Zerkina E.V., Chusavitina G.N. Preparing future teachers for the prevention of deviant behavior in the field of information and communication technologies: a monograph. Magnitogorsk Magnitogorsk State University, 2008. 185 p.

15. Chusavitina G.N., Chernova E.V. Tolerance as a means of combating extremism and terrorism // Modern problems of science and education: Abstracts. XLIII vnutrivuz. scientific. konf.prep. MaSU. Magnitogorsk. 2011. pp. 100–102.

Рецензенты:

Сайгушев Н.Я., д.п.н., профессор кафедры профессионального образования, МГТУ им. Г.И. Носова, г. Магнитогорск;

Севостьянова В.С., д.фил.н., доцент кафедры иностранных языков для профессиональной коммуникации, МГТУ им. Г.И. Носова, г. Магнитогорск.

Работа поступила в редакцию 19.12.2014.