УДК 004.02

СОВРЕМЕННЫЕ АСПЕКТЫ РАСПРОСТРАНЕНИЯ КИБЕРЭКСТРЕМИСТСКОЙ ИДЕОЛОГИИ В МОЛОДЕЖНОЙ ИТ-СРЕДЕ

Макашова В.Н., Чернова Е.В., Боброва И.И.

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

Актуальность темы обусловлена популярностью использования современных информационных технологий в повседневной жизни молодежи. Именно молодежная среда становится благоприятной почвой для формирования радикальных взглядов, позволяющих эффективно прогнозировать развитие возможностей киберэкстремистских организаций, создавать новые формы и методы информационно-психологического воздействия; проводить их апробацию. В статье описаны тенденции возникновения и развития киберэкстремизма, описаны механизмы противодействия различным угрозам. Из-за существующих неточностей в законах; проблем доказательной базы; уязвимостей на программно-аппаратном уровне возникают сложности с приостановлением процесса распространения экстремистской информации. Авторы статьи предлагают пути обеспечения информационной безопасности образовательного учреждения (контент-фильтрация и мониторинг), которые позволяют обеспечить защиту инфраструктуры как образовательных учреждений, так и корпоративного сегмента. Затронуты вопросы просвещения родителей и учащихся. Выявлена проблема недостатка квалифицированных кадров, осуществляющих управление политикой информационной безопасности образовательных учреждений.

Ключевые слова: киберэкстремизм, ИТ-технологии, информационная безопасность, мониторинг контента

MODERN ASPECTS OF DISTRIBUTION CYBERACTIVISTS IDEOLOGY IN THE YOUTH ENVIRONMENT

Makashova V.N., Chernova E.V., Bobrova I.I.

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

The relevance of the topic due to the popular use of modern information technologies in the everyday life of young people. Youth environment to become fertile soil for the formation of radical views, allowing you to effectively predict the development of cyberactivists organizations, to create new forms and methods of information-psychological influence; to conduct their testing. This article describes trends in the occurrence and development of cyberactivism described mechanisms to counter a variety of threats. Because of inaccuracies in the laws; problems of evidence; vulnerabilities in software and hardware level, have difficulty suspending the process of distributing extremist information. The authors suggest ways of ensuring information security of an educational institution (content filtering and monitoring), which allow to protect the infrastructure of educational institutions and the corporate segment. The issues of education, parents and students. Has the problem of lack of qualified personnel, managing the information security policy of educational institutions.

Keywords: cyberactivism, information technologies, information security, monitoring content

Повсеместное использование информационных технологий в повседневной жизни пользователей, расширение сетевых сервисов, их доступность, массовая истерия СМИ по поводу «кровожадных приемов привлечения внимания зрителей и пользователей Интернет-ресурсов» оказывает влияние на растущий интерес молодежи к агрессивным экстремистским движениям.

Именно молодежная среда становится благоприятной почвой для формирования радикальных взглядов, позволяющих эффективно прогнозировать развитие возможностей киберэкстремистских организаций, создавать новые формы и методы информационно-психологического воздействия; проводить их апробацию. Все это позволяет им достаточно быстро и эффективно распространять киберэкстремистские послания. В силу низкого уровня раскрываемости подобных явлений в большинстве случаев просто невозможно вовремя выявить и пресечь киберэкстремистские атаки. Экстремизм является одной из наиболее сложных социально-политических проблем современного российского общества, что связано в первую очередь с многообразием экстремистских проявлений, неоднородным составом организаций экстремистской направленности, которые оказывают дестабилизирующее влияние на социально-политическую обстановку в стране [1].

Для успешной борьбы с киберэкстреизмом в современном мире необходимо понимать тенденции его возникновения и развития. Первое упоминание появления экстремизма в России встречается в середине 90-х годов. Это обусловлено в первую очередь длительной экономической нестабильностью страны, ярко выраженным социальным расслоением населения, низкой

эффективностью работы государственных институтов, отсутствием социальной защищенности граждан. Все это в итоге привело к стихийным недовольствам, к мелкому хулиганству и к преступлениям. Радикальные политические партии, которых в этот исторический период в России оказалось множество, стали проводниками экстремизма. В качестве основных лозунгов выбирались националистические или сепаратистские, в ряды партий вовлекалась молодежь, среди которой поощрялась активная борьба силовыми методами с противниками. 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» [2].

Прежде всего, Интернет позволяет «легко, безопасно, дешево и без цензуры» распространять любую идеологию по всему миру (в том числе демонстрирование нацистской атрибутики или символики), что способствует формированию ранее не существовавшего единого неонацистского, расистского сообщества, которое вдохновляет своих членов на совершение актов насилия. Возможность размещения программных документов различных политических групп, содержащих информацию, побуждающую к насильственному изменению конституционного строя и нарушению целостности России, пропаганда превосходства, исключительности либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности и т.п. Кроме этого, активно используются участниками террористических и экстремистских организаций информационные ресурсы Интернета, позволяющие легко и без дополнительных затрат найти различные рецепты изготовления самодельных взрывных устройств, «проверенные» методы осуществления преступлений террористического характера. Наконец, экстремистские группы используют Интернет для финансирования своей деятельности (финансирование сайтов через рекламу, трафики захождения на сайт и т.п.) либо иного содействия в планировании, организации, подготовке и совершении указанных действий (координация действий).

Экстремизм – это дестабилизация существующего устойчивого состояния взаимоотношений в обществе, навязывание агрессивного подхода к разрешению появляющихся противоречий. Причем направление и степень той агрессии определяется лидерами или членами того или иного движения. Крайняя точка экстремизма – терроризм.

Понятия киберпреступность, киберэкстремизм, кибертерроризм давно перестали быть новостью для пользователей Интернета. Особенности киберпространства всемирной паутины не позволяют контролировать информационные ресурсы, скорость распространения которых просто фантастическая. Неудивительно, что подобная информация находит своих сторонников и получает активную поддержку.

Осознавая серьезность обозначенной проблемы, руководители правительственных структур различных государств, владельцы сайтов и хостингов предпринимают многочисленные попытки контролировать распространение подобной информации в Интернете. Тем не менее говорить о достигнутых результатах пока преждевременно. Существующие несостыковки, неточности в законах; проблемы доказательной базы подобных преступлений; уязвимости на программно-аппаратном уровне – не позволяют остановить процесс распространения экстремистской информации. Наиболее легко подвержена подобному влиянию молодежь. Она чаще всего и оказывается втянутой в сообщества экстремистской направленности. После повсеместного распространения Интернета экстремизм получил новую возможность для безконтрольного распространения, приобретя приставку «кибер». Киберэкстремизм распространяется через сетевые сообщества, социальные сети, форумы, блогосферу.

В целях обеспечения информационной безопасности и как, следствие, ограничения молодежи от киберэкстремистского явления широко применяются на практике технические средства защиты (программные, аппаратные и программно-аппаратные комплексы).

Существует ряд программных продуктов мониторинга и анализа действий пользователей, основными функциями которых являются: отслеживание общения пользователя в сети образовательного учреждения и того, какими приложениями, сетевыми сервисами, социальными сетями они пользовались; протоколирование и анализ содержимого общений или переписок; поддерживание отслеживания действий пользователей различными способами общения, в том числе общение голосом; формирование картины рабочего дня пользователя; предоставление отчетов об активности пользователей различной степени детализации.

Результат применения решения позволит достичь следующих преимуществ:

– снижение рисков утечки конфиденциальной информации;

– мониторинг и запись действий пользователей, их коммуникаций и, как

следствие, обнаружение и пресечение кибер-экстремистских посланий;

– поддержка и анализ различных форматов представления данных.

Наиболее распространенными в образовательных учреждениях являются контент-фильтры. Контент-фильтр, или программа ограничения Интернет-контента, – это программное или аппаратное решение для ограничения выхода в Интернет на нежелательные интернет-ресурсы.

Системы контроля безопасности контента в первую очередь призваны осуществлять контроль за содержанием потоков информации, передаваемых в Интернет и получаемых из сети в локальную вычислительную сеть. К задачам систем контент-фильтрации относятся также проверка информации, хранящейся в локальной сети, контроль за содержанием электронной почты, а также контроль за просматриваемой информацией с целью предотвращения использования Интернета в личных целях [6]. Необходимость систем контент-фильтрации диктуется тем, что Интернет – это источник информации, за который никто не несет ответственности, и вероятность получения из него недостоверной, оскорбительной, пиратской или запрещенной по другим причинам информации весьма велика. Наличие во внутренней сети учебного заведения подобной информации может вызвать не только претензии к ученикам, которые подобный контент скачивают на рабочую станцию сети, но и к уголовному преследованию администрации, которая допускает хранение подобных материалов.

Контент-фильтр помогает защитить компьютеры от вирусов, проникающих на ПК пользователей через сомнительные сайты, спам-рассылок на почту. Такие фильтры работают по принципу списков сайтов, объединяемых в специальные группы в зависимости от контента. Контент-фильтр помогает устранить проблемы, связанные с хищением персональных данных, ограничивает доступ к содержанию вычислительной сети благодаря созданию особых списков, разрешенных в данной группе. Компьютер с базой персональных данных осуществляет подключение к Интернету через контент-фильтр путём использования защищенного SSL подключения, которое обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP подключение, для шифрования используется асимметричный алгоритм с открытым ключом. Таким образом, данные системы контент-фильтрации позволяют обеспечить защиту инфраструктуры как образовательных учреждений, так и корпоративного сегмента.

Каждый день в Интернете появляются тысячи новых сайтов, поэтому даже используя обновления баз данных с нежелательными ресурсами, добиться 100%-ной фильтрации не представляется возможным. Особая проблема – некачественная фильтрация русскоязычного контента западными продуктами. Возможны ошибки, при которых фильтр отсеивает сайты полезного содержания. Чем более интеллектуален фильтр и чем больше база, на которую он опирается, тем дороже решение и тем оно менее доступно для государственных образовательных учреждений.

Администраторы в школах имеют различный опыт работы с компьютерами, но даже непрофессионал должен иметь возможность создавать и поддерживать политику фильтрации. Образовательный процесс включает множество различных областей науки, и фильтрация должна быть легко настраиваемой, корректируемой, а также обеспечивать защиту от новейших угроз.

Не менее популярным для использования механизмом обеспечения информационной безопасности образовательных учреждений является мониторинг Интернет-ресурсов, дающий быструю и точную картину Web-пространства. Данные об интернет-активности защищены криптографически и хранятся в недоступном для несанкционированного просмотра виде. Любой посещенный ресурс может быть просмотрен и впоследствии добавлен в список разрешенных или запрещенных листов. Используя специальные механизмы ограничения работы по времени, можно задать в период учебного дня «список» порталов исключительно для образования, а во внеурочное время открыть доступ к порталам, попадающим в белый список, не нарушая «Единый реестр» доменных имен, указателей страниц сайтов в сети Интернет [7].

Известные программы для организации серверной контент-фильтрации для Windows-систем: МКФ, UserGate, Kerio, ISA Server, SafeSquid, а также прокси-серверы, на которых можно организовать фильтрацию. Для Linux-систем наиболее популярны DansGuardian и 27Mindwebfilter и др. При клиентской фильтрации на каждом компьютере устанавливается и настраивается программа-фильтр, что позволяет задать индивидуальные настройки для каждой машины. Примеры программных продуктов для Windows-систем: Интернет Цензор, ПКФ, NetPolice, KinderGate и др. Для Linux-систем: NetPolice ALT Linux, СКФ и др.

Таким образом, считаем, что профилактика распространения идей киберэкстремизма – комплексная проблема, для решения которой необходимо задействовать

юридические, психолого-педагогические и технологические инструменты.

Решение обозначенных выше проблем мы видим в разработке содержательного аспекта пропедевтики явлений киберэкстремизма в молодежной среде.

Пропедевтика – «введение в какую-либо науку, предварительный вводный курс, систематически изложенный в сжатой и элементарной форме» [8]. Наблюдается острая необходимость 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:

– виды экстремизма и киберэкстремизма, их особенности, признаки и истоки;

– особенности проявления киберэкстремизма в ИКТ-среде, особенно в молодежной;

– законодательные, нормативные, правовые, этические, моральные нормы работы в сфере ИКТ, нормы информационной этики и права;

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

Важно помнить о необходимости включения пропедевтического аспекта профилактики киберэкстремизма в молодежной ИТ-среде в образовательную и воспитательную работу образовательных учреждений на ранних этапах развития школьников, так как легче всего подобные явления распространяются именно в этом возрасте, 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 бездумно пополнять ряды киберэкстремистов.

Статья публикуется при поддержке Российского гуманитарного научного фонда в рамках гранта № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Список литературы

1. Методические рекомендации по профилактике и противодействию экстремизму в молодежной // Наша молодежь. – 2011. – № 6. – С. 40–41.

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

3. Номоконов В.А., Тропина Т.Л. Терроризм с помощью Интернета // Терроризм в России и проблемы системного реагирования. – М.: Российская криминологическая ассоциация, 2008. – 192 с.

4. Фридинский С.Н. Борьба с экстремизмом (уголовно-правовой и криминологический аспекты): автореф. дис. ... канд. юрид. наук. – Ростов-на-Дону, 2003 – С. 8.

5. Чернова Е.В. Пропедевтика явлений киберэкстремизма в молодежной среде Сборник научных трудов SWorld. – Вып. 2. Т. 16. – Одесса: КУПРИЕНКО, 2013 – 94 с. – С. 44–47.

6. Программы контроля, родительский контроль [интернет портал], URL: http://nicekit.ru/parental-control/time-boss.php.

7. Абулин, К.А. Безопасность в интернете [интернет портал], URL: http://www.comprice.ru.

8. Прохоров А.М. Большой энциклопедический словарь. – 2-е изд., перераб. и доп. – М.: Норинт, 2004. – 1456 с.

9. Зеркина Е.В., Чусавитина Г.Н., ИКТ: инновация небезопасная // Народное образование. – 2008. – № 8, – С. 273–276.

10. Зеркина Е.В., Чусавитина Г.Н. Проблемы организации учебно-воспитательной работы со школьниками в целях нейтрализации негативного воздействия ИКТ // Вестник МГОУ, МГОУ. – М., 2006, – С. 100–105.

11. Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи (сборник статей) / под ред. Г.Н. Чусавитиной, Л.З. Давлеткириевой, Е.В. Черновой. – Магнитогорск: МаГУ,2013. – 162 с.

12. Чусавитина Г.Н., Чусавитин М.О. Модель подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде // Новые информационные технологии в образовании: материалы Международной научно-практической конференции, ФГАОУ ВПО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2012. – С. 519–521.

References

1. Metodicheskie rekomendacii po profilaktike i protivodejstviyu e'kstremizmu v molodezhnoj // Nasha molodezh'. 2011. no. 6. pp. 40–41.

2. Sirota N.M. Politologiya: Uchebnoe posobie. SPb.: Nacionalnyj otkrytyj institut Rossii, 2009. 113 p.

3. Nomokonov V.A., Tropina T.L. Terrorizm s pomoshhyu Interneta // Terrorizm v Rossii i problemy sistemnogo reagirovaniya. M.: Rossijskaya kriminologicheskaya associaciya, 2008. 192 p.

4. Fridinskij S.N. Borba s ekstremizmom (ugolovno-pravovoj i kriminologicheskij aspekty): Avtoref. dis. kand. yurid. nauk. Rostov-na-Donu, 2003 pp. 8.

5. Chernova E.V. Propedevtika yavlenij kiberekstremizma v molodezhnoj srede Sbornik nauchnyx trudov SWorld. Vypusk 2. T. 16. Odessa: KUPRIENKO, 2013 94 p. pp. 44–47.

6. Programmy kontrolya, roditelskij kontrol [internet portal], URL: http://nicekit.ru/parental-control/time-boss.php.

7. Abulin K.A., Bezopasnost v internete [internet portal], URL: http://www.comprice.ru.

8. Proxorov A.M. Bolshoj enciklopedicheskij slovar. 2-e izd., pererab. i dop. M.: Norint, 2004. 1456 p.

9. Zerkina E.V., Chusavitina G.N., IKT: innovaciya nebezopasnaya, Narodnoe obrazovanie, Narodnoe obrazovanie, 2008, no. 8, pp. 273–276.

10. Zerkina E.V., Chusavitina G.N. Problemy organizacii uchebno-vospitatel'noj raboty so shkolnikami v celyax nejtralizacii negativnogo vozdejstviya IKT. Vestnik MGOU, MGOU, Moskva, 2006, pp. 100–105.

11. Informacionnaya bezopasnost i voprosy profilaktiki kiberekstremizma sredi molodezhi (sbornik statej) / pod red. G.N. Chusavitinoj, L.Z. Davletkirievoj, E.V. Chernovoj. Magnitogorsk: MaGU,2013. 162 p.

12. Chusavitina G.N., Chusavitin M.O. Model podgotovki nauchno-pedagogicheskix kadrov k obespecheniyu informacionnoj bezopasnosti v IKT-nasyshennoj srede // Materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii «Novye informacionnye texnologii v obrazovanii», FGAOU VPO «Ros. gos. prof.-ped. un-t». Ekaterinburg, 2012, pp. 519–521.

Рецензенты:

Мусийчук М.В., д.ф.н., профессор кафедры психологии, ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск;

Савва Л.И., д.п.н., профессор кафедры педагогики профессионального образования, ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск.

Работа поступила в редакцию 19.12.2014.