РАЗВИТИЕ СИСТЕМЫ

Есть уверенность в том, что технологические трудности, связанные, например, с методами стратегического планирования или аналитической обработкой больших объемов текстовых данных, если они и возникнут, не будут препятствием к дальнейшему ее освоению и развитию.

Сейчас становится все более актуальным решение вопросов совершенствования и развития методологического и нормативного правового обеспечения функционирования Системы. Важными аспектами развития Системы являются: обеспечение целостного охвата стратегических вопросов, быстрое достижение согласия руководителей, топ-менеджеров и экспертов относительно целей и путей действий, освоение ее пользователями нового для органов государственной власти экспертно-аналитического инструментария.

В части нормативного правового обеспечения функционирования Системы необходимо утверждение пакетов документов, касающихся работы как всей Системы, так и отдельных видов ее обеспечения. Так, в состав типовой документации Системы могут войти методики по созданию условий для улучшения реализации жизненно важных проектов в промышленности и социальной сфере, например, посвященных вопросам: диверсификации финансирования работ в перспективе; структуризации диверсифицированных источников; оценки сценариев инновационного развития; дифференциации государственных услуг; диверсификации инвестиционного обеспечения; залогового финансирования проектов; внебюджетного финансирования за счет государственных финансовых резервов, выпуска эмиссионных ценных бумаг, размещения акций за рубежом, механизма реальных опционов, отраслевой лотереи, рынка венчурного капитала.

Важными и полезными для пользователей Системы могут оказаться такие документы, как: положение о стратегическом маркетинге; руководство по сетевой экспертизе и стратегическим совещаниям; регламенты диверсификации холдингов; регламент сбора информации из органов государственной власти; кодекс профессиональной этики и др.

Для успешного внедрения Системы информационно-аналитической поддержки стратегического планирования, управления и контроля в практику потребуется утверждение соответствующего пакета документов на уровне Президента РФ и Правительства РФ.

Владимир ДАВЫДОВ

Актуальные проблемы противодействия информационному экстремизму в России

Экстремизм в его различных формах и проявлениях, сопровождаемый опасными насильственными преступлениями, в современных условиях становится для многонациональной и полирелигиозной России одним из опаснейших факторов, угрожающих целостности государства и стабильности общества.

Статистика свидетельствует о неуклонном росте преступлений данной категории: за последние 6 лет число зарегистрированных преступлений экстремистской направленности увеличилось в три раза – с 263 в 2006 г. до 622 в 2011 г. При этом приведенные данные нельзя считать абсолютно достоверными. В силу объективных и субъективных причин преступления экстремистской направленности зачастую регистрируются как совершенные по другим основаниям или входят в группу латентных преступлений. Так, например, в Республике Дагестан в 2008-2009 гг. по 130 преступлениям, совершенным членами религиозной секты ваххабитов, действия обвиняемых были квалифицированы в основном как «посягательство на жизнь сотрудника правоохранительного органа» [1, с. 3].

Явление экстремизма весьма динамично и с каждым днем приобретает все новые черты и характеристики. В информационном обществе экстремистские организации активно используют достижения коммуникационных технологий, внедряя в свою деятельность прежде всего те из них, которые достаточно эффективно воздействуют на массовое общественное сознание.

Глобальная сеть Интернет позиционируется идеологами экстремизма как своеобразная информационная площадка для популяризации своих идей, вербовки новых сторонников, организации их самообучения по вопросам идеологии, тактики действий при проведении противоправных акций, сбора финансовых средств для своей деятель-

Владимир ДАВЫДОВ – заместитель начальника полиции УМВД России по Тульской области, соискатель Тульского государственного университета

ности. И это далеко не полный перечень задач. Интернет-форумы, чаты, социальные сети, электронная почта и иные web-технологии дают возможность формировать структурные звенья экстремистских организаций и выстраивать их работу без непосредственного участия эмиссаров, позволяют значительно повысить уровень конспирации. Зачастую члены организаций нижнего звена могут не знать друг друга и своих непосредственных руководителей, узнавая о месте и времени проведения планируемой акции на форуме, посредством электронной почты или анонимной SMS-рассылки через Интернет.

Нередко путем использования возможностей социальных сетей, создания в них тематических групп и сообществ экстремисты пытаются втянуть молодых людей в дискуссию, заинтересовать их своей идеологией. И это им в определенной степени удается. По данным МВД России, 80% активных участников экстремистских организаций, состоящих на профилактических учетах, – это молодые люди в возрасте 16-20 лет [1, с. 7]. Так, в поле внимания сотрудников правоохранительных органов Уральского федерального округа попала группа учащихся школ и профессиональных колледжей г. Магнитогорска Челябинской области. Будучи активными пользователями Интернета, подростки вошли в контакт с одной из экстремистских организаций и по ее примеру создали свою экстремистскую группу под названием «Русское национальное движение». При этом ребята, имея лишь поверхностное представление об идеологии расизма, даже не подозревали об общественной опасности своих действий. Они распространяли в городе листовки ксенофобного содержания, размещали в Интернете видеоролики, унижающие честь и достоинство граждан других национальностей, наносили на стены зданий центральных улиц Магнитогорска расистские надписи и символику [2, с. 2].

Другим примером могут служить события, имевшие место в Москве. Члены националистической организации совершали преступления в вечернее время в различных районах столицы, предварительно договорившись о встречах через интернет-форум [2, с. 1]. Первое из таких преступлений было совершено в феврале 2008 г., а последнее – в апреле 2010 г. За полтора года группировка, состоящая из 10 человек, совершила серию покушений на убийство приезжих с Северного Кавказа, из Средней Азии и Китая, взрывы в кафе «Макдоналдс» и в церкви Николая Чудотворца.

Наличие в Интернете многочисленных информационно-развлекательных ресурсов обуславливает формирование значительной части сетевой аудитории из числа молодежи с еще недостаточно сформировавшимися социальными установками. Достаточно вспомнить ситуацию с сайтом «Большая Игра. Сломай систему» (http://rusigra. org), существовавшим в Интернете более года. Согласно правилам игры, созданной представителями экстремисткой группы «Северное братство», участники проекта должны были выполнять задания, заключавшиеся в совершении различных противоправных действий по мотивам национальной ненависти. На первом уровне игры было необходимо в людных местах, на автомобилях «пришельцев», зданиях «силовиков системы» нанести 50 экстремистских эмблем, придумать «пять смешных унижающих сценариев постановки пришельца на колени для последующей съемки видеороликов по лучшим сценариям», узнать адресные данные и телефоны участкового уполномоченного полиции или его руководства. На втором уровне требовалось прислать администрации сайта отчетный видеоролик, в котором «пришелец» поставлен на колени и извиняется перед «русскими», найти любого человека, позволившего себе негативные высказывания в отношении «Большой игры», и применить против него адекватные меры воздействия [3]. Дальнейшие уровни – по нарастающему сценарию.

Несмотря на существование Доктрины информационной безопасности Российской Федерации, Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации» (далее – эакон «Об информации»), ряда законов, регулирующих информационные отношения в отдельных сферах деятельности, до сих пор не создана логически завершенная структура регулирования информационных правоотношений даже в сфере информации ограниченного доступа. Не останавливаясь подробно на этой проблеме, отметим, что в ст. 5 закона «Об информации», давая классификацию информации в зависимости от порядка ее предоставления или распространения, законодатель выделяет четвертой категорией «информацию, распространение которой в Российской Федерации ограничивается или запрещается». В п. 6 ст. 10 закона содержится запрет на «распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность» [4]. Бланкетность данной нормы в специальном законе, посвященном защите информации, существенным образом осложняет квалификацию противоправных деяний в информационной сфере, снижая эффективность их пресечения.

В современных условиях противодействие проявлениям экстремизма в Интернете все в большей степени будет зависеть от объективности и глубины анализа данного социального явления, прогнозирования тенденций дальнейшего

развития содержания, стратегии и тактики деятельности деструктивных сил.

Угроза распространения идеологии экстремизма как способа управления социумом посредством информационно-психологического воздействия становится еще более опасной и предполагает применение адекватных мер противодействия со стороны государственных структур. Одним из инструментов, позволяющих своевременно выявлять и пресекать деятельность деструктивных сил, должен стать целевой мониторинг информационных ресурсов Интернета. Как правило, на web-страницах сайтов излагается достаточно подробная информация о действиях и внутренней политике экстремистских организаций, ее союзниках и конкурентах, запланированных и уже совершенных акциях, способах финансовой поддержки и т. п.

В специальной отечественной и зарубежной литературе описывается множество способов организации процесса информационного мониторинга [5, 6, 7, 8, 9]. Назовем наиболее доступные для аналитиков разного уровня профессиональной подготовки и не требующие значительных затрат.

Мониторинг трафика ISPs. Действие данного метода основано на использовании алгоритма обнаружения экстремисткой информации в Интернете посредством анализа содержания ранее выявленных web-сайтов экстремистской направленности. Сканирование должно проводиться в режиме реального времени на основе лексических параметров отнесения информации к разряду экстремистской.

Выявление информационных угроз на основе IDS (Intrusion Detection Systems). IDS постоянно отслеживает активность в информационной среде и принимает решение о том, являются ли обнаруженные материалы частью информации экстремистского характера или нет. Здесь применяются методики определения коэффициента уровня опасности информации: от web-сайтов, непосредственно используемых экстремистами, до HTML-страниц, содержащих лишь одно или несколько слов, имеющих отношение к лексическим единицам экстремистской тематики.

Мета-поиск. Метод основан на поиске сочетаний фразеологических признаков, характерных для экстремистских высказываний.

Метод векторного анализа. Суть этого способа заключается в том, что каждая web-страница, имеющая экстремистское содержание, может быть представлена как часть общей матрицы экстремистской активности. Интересы экстремистов выражаются несколькими векторами, каждый из которых относится к различным направлениям деструктивной деятельности. Данный анализ также используется для определения авторства обнаруженных материалов.

Кластерный анализ. Кластерный анализ основан на разделении объектов (ситуаций) на непересекающиеся подмножества (кластеры) таким образом, чтобы каждый кластер состоял из схожих объектов, а объекты разных кластеров существенно отличались. Кластеризация экстремистской активности в Интернете используется для «интеллектуального» группирования при поиске файлов и HTML-страниц экстремистского содержания, предоставляя правоохранительным органам возможность применять более удобную классификацию информации экстремистского характера. Этот метод может также быть использован для обнаружения web-страниц, контролируемых или обновляемых одной и той же экстремистской организацией. Для каждого такого web-набора вычисляется главный объект, который отображается в модели векторного пространства.

Визуализация. Визуализация представляет собой наглядное отображение связей, структуры, направлений активности экстремистских организаций в Интернете. В рамках данного метода возможно составление матрицы большой размерности и вывода информации в двумерном виде для определенных признаков и характеристик интернет-экстремизма.

Прогресс в развитии и внедрении новейших информационно-коммуникационных технологий ставит на повестку дня задачу своевременной оценки угроз, возникающих в связи с возможностями использования таких технологий в целях, не совместимых с задачами обеспечения безопасности общества и государства.

Литература

1. Материалы Центра «Э» ОРБ ГУ МВД России по Уральскому федеральному округу к межведомственному совещанию по вопросам противодействия экстремистским проявлениям. Екатеринбург, 2011.
2. *Михайлова А.* Нацисты планировали нападения через Интернет. URL: http://www.gzt.ru/topnews/accidents/252237.html.2010.
3. Заместитель Генерального прокурора Российской Федерации В. Гринь направил в суд уголовное дело в отношении руководителя экстремистского сообщества «Северное братство». URL: http://www.genproc.gov.ru/news/news-72387/.
4. Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ.
5. *Батурин Ю.М.* Компьютерная преступность и компьютерная безопасность. М.: Юрид. лит., 1991. С. 160.
6. *Лопатина Т.М.* Противодействие преступлениям в сфере компьютерной информации // Законность. 2006. № 6. С. 50-51.
7. Sinrod E.J. Cyber-Crimes: A practical approach to the application of federal computer crime laws / E.J. Sinrod, W.P. Reilly // Santa Clara computer and high technology law journal. Vol. 16. № 2. P. 12-18.
8. «Polizei heute», Germany. 2010. № 4. P. 131.
9. «Kriminalistik», Germany. 2010. № 9. P. 17-22.