Информационная безопасность и защита информации

О.В. Казарин, В.П. Охапкин,
Е.П. Охапкина, Р.А. Шаряпов

Социально-правовые и технологические аспекты проблемы выявления деструктивных информационных воздействий в сети Интернет

Рассматривается проблема выявления деструктивных информационных воздействий в сети Интернет, ее социально-правовые и технологические аспекты. Исследование их взаимосвязи может позволить создать эффективные социотехнические механизмы обнаружения и, в дальнейшем, предотвращения таких воздействий. Например, для автоматического обнаружения вредоносного, противоправного контента в социальных сетях необходимо знать, какая информация, в соответствии с законодательством Российской Федерации, подлежит запрету для распространения в стране, какие паттерны и шаблоны сообщений необходимо создавать для контент-анализа информационной среды социальных сервисов и как поддерживать их в актуальном состоянии и т. п.

Ключевые слова: глобальное информационное пространство, Интернет, социальные сети, угрозы информационной безопасности, деструктивные информационные воздействия.

Высокий уровень проникновения в повседневную жизнь информационно-коммуникационных технологий (ИКТ), развитие и доступность их мобильных вариантов, рост активности всех слоев населения в онлайн-среде наряду с позитивными явлениями создают серьезные новые риски и угрозы информационной безопасности для общества и его отдельных слоев, в первую очередь для детей, подростков и молодежи.

Общепризнано, что одним из ключевых элементов информационной сферы является сеть Интернет[1], где создаются, хранятся и передаются гигантские объемы информации, учесть и проконтролировать которые не представляется возможным. Потенциал сети Интернет,

его позитивное воздействие на развитие всех сфер человечества огромны. Особую роль здесь играют социальные сети, охватывающие на сегодня миллиарды пользователей[2]. Возникшие как один из способов объединения людей в социальные общности (группы) на основе различных интересов (профессиональных, гендерных, религиозных, образовательных, интересов, связанных с образом жизни, увлечениями, спортом и т. д.) и форм межличностного общения, сегодня социальные сети, и как глобальное социальное явление, и как информационный инструментарий, оказывают огромное воздействие практически на все сферы деятельности человека и общества.

Однако развитие ИКТ привело еще и к тому, что «возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности»[3]. Сеть Интернет и, в особенности, социальные сети сегодня превратились в мощнейший механизм, используемый региональными и международными экстремистскими и террористическими организациями для пропаганды идеологии насильственного экстремизма и терроризма, вербовки новых сторонников (и, в первую очередь, представителей молодого поколения) в свои ряды, а также для планирования, координации и проведения преступных акций, целевого отбора, обучения и другой необходимой подготовки к проведению противоправной деятельности. Активное использование террористическими группировками социальных сетей для деструктивного информационного воздействия (ДИВ) в достижении ими своих целей – факт, признанный ООН, другими международными организациями, главами государств, политиками, руководителями спецслужб, международным экспертным и бизнес-сообществом. Социальные сети и сеть Интернет в целом – это «удобная» среда для организации деструктивного информационно-психологического влияния, в том числе – в целях манипулирования личностью, социальными группами и обществом в целом.

Противодействие этому деструктивному влиянию должно вестись на разных направлениях: международном, правовом, социальном, политическом, технологическом, организационном. При этом исследования в этой области должны вестись в тесной методологической взаимоувязке всех аспектов проблемы выявления и противодействия ДИВ в сети Интернет. Особое место в этом случае занимает постоянный и систематический мониторинг (анализ) правового поля и состояния дел в области угроз информационной безопасности в сети Интернет и в информационной сфере в целом.

Социально-правовые аспекты проблемы

Признание того, что развитие и внедрение ИКТ несет человечеству не только прогресс и процветание, но и порождает новые риски и угрозы и может угрожать стабильности и безопасности глобального информационного пространства, впервые на международном уровне было зафиксировано в принятой 4 декабря 1998 г. на основе консенсуса в ходе 53-й сессии Генеральной Ассамблеи ООН резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/53/70)[4], представленной Российской Федерацией. В последней резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» A/RES/71/28, принятой 9 декабря 2016 г. в ходе 71-й сессии ГА ООН, вновь отмечался значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации[5]. При этом в резолюции (как и в предыдущих) выражалась озабоченность потенциальным использованием этих технологий и средств в целях, несовместимых с задачами обеспечения международной безопасности и стабильности, и возможного негативного воздействия на целостность инфраструктуры государств, нарушая их безопасность в гражданской и военной сферах, и содержался призыв к предотвращению использования информационных ресурсов или технологий в преступных или террористических целях.

Крупнейшие IT-компании-гиганты, осознавая свою ответственность, принимают необходимые меры для противодействия деструктивному использованию ИКТ, в том числе за счет расширения сотрудничества с государственными структурами. Так, 8 января 2016 г. в Сан-Хосе (штат Калифорния, США) состоялась встреча действующих на тот момент высокопоставленных представителей администрации Белого дома, руководителей спецслужб и правоохранительных органов США с главами компаний, работающих в сфере высоких технологий (Microsoft, Apple, Facebook, Google, Twitter, Yahoo и LinkedIn), где обсуждались возможные меры по противодействию таким деструктивным информационным воздействиям, как пропаганда терроризма в сетях и вербовка террористами новых сторонников, а также создание условий, в которых виртуальное пространство перестало быть для них «безопасным убежищем».

Как сообщило информационное агентство РБК в мае 2016 г., компании Facebook, Twitter, Microsoft и Google согласились соблюдать новые правила Евросоюза, направленные на борьбу с разжиганием ненависти в Интернете. Компании обязались принимать

меры против нарушителей в течение 24 часов и при необходимости удалять соответствующие материалы из сети[6]. В августе 2016 г. представители компании Twitter сообщили, что за последние полгода сервис Twitter[7] приостановил действие 235 тысяч аккаунтов (учетных записей), владельцы которых использовали их для распространения пропаганды терроризма и иной экстремистской информации[8]. Также по данным РБК в декабре 2016 г. компании YouTube, Facebook, Twitter и Microsoft с целью объединения усилий для борьбы с терроризмом заявили о создании совместной базы данных идентификации террористического контента, что позволит другим платформам быстрее определять «запрещенные» видео- и фотоматериалы и удалять их со своих сайтов[9].

В январе 2016 г. Президент Российской Федерации В.В. Путин подписал перечень поручений по итогам встречи с участниками первого российского форума «Интернет-экономика», состоявшегося 22 декабря 2015 г. В п. 9 перечня содержалось поручение ФСБ России, Генеральной прокуратуре Российской Федерации, Минюсту России, Минкомсвязи России, Роскомнадзору, ФАДН России[10] совместно с заинтересованными федеральными органами исполнительной власти представить предложения по организации мониторинга информационных угроз в сети Интернет.

Так, ФАДН России с апреля 2015 года, в соответствии со Стратегией государственной национальной политики Российской Федерации на период до 2025 г.[11], ведет работу по созданию системы мониторинга состояния и прогнозирования развития межэтнических отношений. Объектами мониторинга являются СМИ, Интернет и социальные сети, органы государственной власти и местного самоуправления, некоммерческие и общественные организации, различные автономии и диаспоры. Система, ориентированная на выявление противоправной деятельности в сети Интернет, помогает выявлять опасные ресурсы для предотвращения массовых конфликтов и позволяет ФАДН России реализовывать механизм досудебной блокировки сайтов совместно с Генпрокуратурой России и Роскомнадзором. По информации ФАДН на март 2017 г., в базу данных системы внесены сведения почти о 100 тыс. средств массовой информации, а также блогах и аккаунтах в социальных сетях[12].

Для контроля над соблюдением операторами связи требований, установленных статьями 15.1–15.4 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»[13], была создана единая автоматизированная система мониторинга АС «Ревизор», осуществляющая мониторинг сети оператора связи на предмет отсутствия

доступности сайтов, включенных в Единый реестр запрещенной информации, хранящая полученную информацию и формирующая отчеты и протоколы результатов мониторинга[14].

9 марта 2017 г. президент РФ В.В. Путин, выступая на расширенном заседании коллегии МВД России, особо отметил, что в информационной сфере появилась еще одна угроза,– это распространение сайтов, пропагандирующих суицид. По мнению президента, преступники «прежде всего нацелены на подростковую и молодежную аудитории, на детей с неокрепшей психикой или находящихся в трудной жизненной ситуации»[15]. В.В. Путин поддержал инициативу депутатов Госдумы РФ о дополнении законодательства нормой, расширяющей перечень действий, при которых наступает уголовная ответственность за доведение до самоубийства. По мнению президента, «это позволит привлекать к ответственности хозяев, создателей и администраторов подобных сайтов, пресекать их деструктивную, еще раз хочу подчеркнуть, преступную деятельность»[16].

В тот же день 9 марта 2017 г. в Государственную думу РФ был внесен согласованный с Правительством РФ и Верховным судом РФ законопроект о внесении в УК и УПК Российской Федерации изменений, направленных на борьбу с призывами к подросткам в социальных сетях к суициду, по которым будет суммарно предусматриваться наказание сроком до 12 лет лишения свободы. В пояснительной записке к законопроекту было указано, что «устанавливается самостоятельная уголовная ответственность за организацию деятельности, сопряженной с побуждением граждан к совершению самоубийства путем распространения информации о способах совершения самоубийства, а также призывов к совершению самоубийства». В частности, речь идет об ответственности для администраторов так называемых «групп смерти» и организаторов любых неформальных сообществ, деятельность которых сопряжена с побуждением, прежде всего детей, к совершению самоубийства[17].

О необходимости установления дополнительной уголовной ответственности также свидетельствует официальная статистика, касающаяся выявления запрещенного суицидального контента в сети Интернет: с 2012 г. по настоящее время специалистами Роспотребнадзора была проведена экспертиза более 13 тысяч ссылок на страницы сайтов в сети Интернет с суицидальной тематикой, а в 2016 году было выявлено 4864 ссылки, из которых 4751 ссылка содержала запрещенную информацию о способах совершения самоубийства и/или призывов к их совершению[18]. По сообщению Роскомнадзора, с начала 2017 г. ведомство выявило более 4 тысяч

групп и личных страниц в социальных сетях, содержащих информацию о способах самоубийства и призывов к суициду[19]. Роскомнадзор ведет круглосуточное совместное сотрудничество с администрациями ведущих социальных сетей с целью осуществления мониторинга групп и личных страниц пользователей на предмет выявления суицидального контента. Это дает возможность ежедневно блокировать более 150 сообществ, посвященных самоубийствам, и удалять суицидальный контент с личных страниц.

Представители компании Facebook, управляющей социальной сетью Instagram, подтвердили Роскомнадзору готовность в оперативном режиме противодействовать распространению противоправной информации. Администрация Instagram в результате сотрудничества с Роскомнадзором удалила 321 ссылку с информацией, имеющей отношение к деятельности «групп смерти»[20].

В целях профилактики самоубийств и с учетом роста распространения в информационном пространстве среди подростков и молодежи призывов к суициду в 2016 г. Роспотребнадзор при участии экспертов в области суицидологии и информационной безопасности разработал «Рекомендации по распространению в СМИ информации о случаях самоубийства»[21], целью которых явилась необходимость снабдить представителей СМИ рекомендациями по подготовке и распространению информации (новостей, статей, выпусков телевизионных передач и других) на тему самоубийства, а также предупредить об ошибках, которые необходимо избегать в сообщениях о суициде.

14 марта 2017 г. в Москве состоялось расширенное заседание Коллегии Генеральной прокуратуры России, на котором генпрокурор Ю.Я. Чайка в своем докладе, рассматривая вопросы противодействия терроризму и экстремизму, отметил активизацию межведомственного взаимодействия в целях противодействия пропаганде запрещенной информации. Ю.Я. Чайка сообщил, что в 2016 г. по материалам прокуроров суды признали девять организаций экстремистскими и одну – террористической; был прекращен доступ к 1200 интернет-ресурсам; с 18,5 тысячи сайтов удалена запрещенная информация[22]. В выступлении генпрокурор отметил важность использования высоких технологий на всех направлениях прокурорского надзора и сообщил о создании Экспертного совета при Генеральной прокуратуре России по вопросам информационных технологий, который предоставит дополнительные возможности осуществления надзора, определит принципиально новое его направление в сфере ИКТ[23].

По данным Роспотребнадзора, с ноября 2012 г. по март 2017 г. специалистами ведомства проведена оценка материалов, размещен-

ных на почти 13 тысячах страницах сайтов, поступивших на экспертизу, из которых в 98% случаев были приняты решения о наличии на страницах сайтов информации, запрещенной к распространению в Российской Федерации[24].

Подробное исследование, постоянный и систематический анализ социально-правовых аспектов, связанных с ДИВ в сети Интернет, позволит составить их типологию, которая, в свою очередь, позволит разработать совокупность технологических методов, инструментов и приемов выявления (обнаружения), идентификации ДИВ и в дальнейшем их нейтрализации и противодействия (предупреждения) ДИВ в будущем. Мониторинг деятельности федеральных органов исполнительной власти и решений, принимаемых ими на направлении противодействия ДИВ в сети Интернет, является необходимой технологической составляющей деятельности в этой области.

Технологические аспекты проблемы

Типология деструктивных информационных воздействий

Можно выделить следующую типологию (как классификацию по существенным признакам), связанную с ДИВ[25]. Последние могут осуществляться путем информационно-технического и/или информационно-гуманитарного воздействия (информационно-психологического воздействия) на объекты воздействия. Информационно-техническое воздействие предполагает использование ИКТ для осуществления враждебных действий и актов агрессии, при этом ИКТ превращаются в информационное оружие, которое может быть использовано в военно-политических, террористических, преступных и иных целях[26]. Информационно-гуманитарное воздействие предполагает использование специально подготовленного контента, распространяемого, как правило, с помощью сети Интернет, в том числе для вмешательства во внутренние дела суверенных стран, других деструктивных действий в отношении личности, общества, государства.

Информационно-гуманитарное деструктивное воздействие, в отличие от информационно-технического деструктивного воздействия, менее зависимо от проблемы выявления и атрибуции, так как в ряде случаев предполагает использование ИКТ и специально подготовленной информации для воздействия на личность, общество и государство в явном виде и определенным

автором. Объектом информационно-гуманитарного воздействия является сознание общества (его части) и отдельных индивидов. Среди инструментов, используемых для оказания информационно-гуманитарного воздействия, можно выделить современные СМИ и социальные сервисы, функционирующие в глобальном информационном пространстве. При этом непосредственно воздействие осуществляется с использованием методов психологии, социологии и социальной инженерии посредством содержания (контента) информационных сообщений.

В типологию ДИВ предлагается также включать их источники и виды информации, запрещенной к распространению в Российской Федерации.

В новой Доктрине информационной безопасности Российской Федерации (декабрь 2016 г.)[27] источники ДИВ можно рассматривать как военно-политические, информационно-психологические, террористические и экстремистские, источники, связанные с компьютерной преступностью.

К последним, в свою очередь, следует отнести источники информации, которая в соответствии с законодательством Российской Федерации[28] подлежит запрету для распространения в стране, в том числе информации:

– о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, а также о способах и местах культивирования наркосодержащих растений (компетенция МВД России и Роскомнадзора);
– о способах совершения самоубийства, а также призывов к совершению самоубийства (компетенция Роспотребнадзора);
– с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера (компетенция Роскомнадзора);
– о проведении азартных игр и лотерей с использованием сети Интернет и иных средств связи (компетенция ФНС России и Роскомнадзора).

Еще одним классификационным признаком предлагаемой типологии следует рассматривать типы информации, составляющие ДИВ. А именно видео-, фото-, графическая электронная информация (где для обнаружения ДИВ должны применяться методы распознавания образов) и текстовая электронная информация (где единственным методом выявления ДИВ, скорее всего, является контент-анализ и его различные модификации).

Следует считать, что ДИВ с использованием специально подготовленного вредоносного (противоправного) контента (информационно-гуманитарные воздействия) в социальных сетях будут постоянно эволюционировать и «разрастаться». Поэтому необходимо систематически обновлять существующие перечни потенциальных ДИВ и, более того, необходимо проводить прогнозные исследования в этой области, чтобы по возможности им противостоять, хотя бы в ближайшей и среднесрочной перспективе. И здесь не обойтись без совершенствования технологического инструментария для контент-анализа текстовых и распознавания графических структур социальных сетей на предмет выявления ДИВ в них.

Формализованное изложение некоторых задач выявления ДИВ

С момента запуска первых социальных сетей в масштабах стран и континентов прошло более 20 лет. За это время социальные сети ни на минуту не останавливались в своем программно-техническом развитии, в их структуре было организовано значительное количество тематических сообществ, персональных страниц пользователей, образованы миллиарды коммуникационных связей различного типа и порядка. Процесс выявления ДИВ, очевидно, сопряжен не только со сложностями социально-правового характера, но и с необходимостью решать задачи прикладного порядка с привлечением средств вычислительной математики.

Так, на предварительном этапе выявления и анализа ДИВ пространство сообществ социальной сети должно быть кластеризовано[29], дабы обеспечить высокую (по заранее установленным критериям) эффективность контент-анализа в рамках однородных, но не разнородных с точки зрения ДИВ сообществ. Формально задача кластеризации сообществ социальной сети может быть поставлена в следующем виде: пусть дано некоторое множество разнородных сообществ социальной сети $I = \{i_1, i_2, \ldots, i_n\}$, каждый элемент которого можно охарактеризовать вектором $\mathbf{x}_j$, $j = 1, \ldots, m$. Кратко указанный вектор параметров в соотношении с рассматриваемым множеством I можно представить как:

$$\mathbf{X}_j = \begin{pmatrix} x_{11} & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{1m} & \cdots & x_{nm} \end{pmatrix}.$$

Необходимо построить множество кластеров C и отображение F-множества I на множество C, а именно $F : I \to C$. Таким образом, задача кластеризации сводится к построению следующего множества:

$$C = \{c_1, c_2, \dots, c_k, \dots, c_g\},$$

где c_k – это k-й кластер, которому принадлежат близкие по критерию объекты из множества I, $k = 1, \dots, g$.

Кроме того, масштаб обозначенной проблематики и ее поле деятельности естественным образом подразумевают работу с большими данными (англ. *Big Data*), что неизбежно потребует снижения затрат по времени для процесса выявления и анализа ДИВ.

На сегодняшний день авторами настоящей работы проведены вычислительные экспериментальные исследования в части кластеризации сообществ, содержащих суицидальный контент, социальной сети «ВКонтакте»[30] с использованием метода *k-means++*. Этот алгоритм в отличие от классического алгоритма *k-means* предусматривает использование предварительного алгоритма, в котором последующий центроид обладает максимальным в геометрическом смысле расстоянием по отношению к текущему кластеру. Достоинством такого способа кластеризации перед *k-means* является приближение к выявлению естественной кластерной структуры анализируемого множества – пространства социальных сетей. Таким образом, *k-means++* позволяет частично разрешить одну из главных проблем классического метода *k-means*: отсутствие гарантий того, что в ходе работы алгоритма будет достигнут глобальный минимум суммарного СКО[31]. Заметим также, что в терминах векторного пространства всякое анализируемое сообщество социальной сети представляется в виде n-мерного вектора, каждый компонент которого отражает некоторый параметр сообщества (например, название сообщества, средняя длина диалога, численность подписчиков, наличие специфической лексики и т. д.)[32]. Отсюда наибольшее в геометрическом смысле удаление, обеспечиваемое выполнением указанного предварительного алгоритма, позволяет выявить и наибольшее отличие сообществ в смысле характеризуемых параметров. Вместе с этим необходимо отметить, что, несмотря на решение проблемы идентификации «выгодных» центроидов методом *k-means++*, остается актуальной проблема выявления сложноорганизованной кластерной структуры: кластеров, которые имеют пересечения[33] с иными кластерами или же специфическую геометрическую форму[34] в векторном пространстве (например, спиралевидную).

Решение задачи о выявлении сложноорганизованной кластерной структуры возможно с использованием так называемой машины опорных векторов (англ. *supported vectors machine*, сокр. *SVM*). Подход к разделению множества сообществ социальной сети на однородные подмножества заключен в построении простого классификатора с максимальным зазором, который представляет собой оптимальную разделяющую гиперплоскость. В терминах *n*-мерного пространства гиперплоскость есть плоское аффинное подпространство с размерностью $n-1$[35]. Для двумерного пространства такой гиперплоскостью будет являться линия (плоское одномерное подпространство), в случае трехмерного пространства классификатор – плоскость. С математической точки зрения гиперплоскость является обычным уравнением прямой и для случая *n*-мерного пространства будет иметь вид:

$$\alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0 .$$

Уравнение (1) задает *n*-мерную плоскость, для которой одно подмножество множества *I* находится по одну сторону гиперплоскости, а второе подмножество – по другую сторону (1). Таким образом, гиперплоскость есть классификатор, разделяющий *n*-мерное пространство на два подмножества, принадлежность объекта к которым определяется знаком выражения (1).

Часто на практике гарантировать линейную разделимость множества сообществ социальной сети не представляется возможным в силу уже упомянутой выше сложноорганизованной кластерной структуры множества *I*. Для устранения проблемы нелинейной разделимости существует подход, связанный с переходом от исходного пространства **X**, характеризующего признаки сообществ, к новому пространству **H** при помощи некоторого преобразования $\psi : \mathbf{X} \to \mathbf{H}$. Такое пространство **H** называют спрямляющим.

Несмотря на значительное количество методов кластеризации, не все из них могут эффективно обрабатывать большие наборы данных. Одним из методов, позволяющих эффективно кластеризовать большие данные, является *EM*-алгоритм (расш. англ. *expectation-maximization*, в переводе – ожидание-максимизация). При некоторых недостатках этого алгоритма: возможность получения квазиоптимального решения; отсутствие гарантий наличия гауссова распределения для всех наблюдений, его использование позволяет получить выгодное решение в случае пересечения кластеров, а также их сигнатуры. Использование *EM*-алгоритма в задаче кластеризации подразумевает, что каждый кластер подчиняется нор-

мальному закону распределения, а множество всех анализируемых комбинаций может быть описано линейной комбинацией гауссовых распределений. Критерием качества кластеризации выступает логарифмическая функция правдоподобия. Отсюда необходимо таким образом оценить параметры распределений, чтобы доставить максимум функции правдоподобия.

Важным следствием *EM*-алгоритма является его аналитическая составляющая, связанная с оценкой параметров распределений. Эти оценки в количественном виде указывают на характерные уникальные особенности, выделенные в подмножества сообществ социальной сети. В этом смысле, при решении частной задачи кластеризации, можно обнаружить дополнительную информацию о средних, вариациях, асимметрии, эксцессе, сильной связности действующих пользователей в выделенных кластерах с различными типами ДИВ. К методам, позволяющим получить такого рода информацию, можно отнести методы теории графов и решающих деревьев. В частности, построение дерева классификации по данным параметров сообществ социальной сети дает возможность оценить мощность и характеристики реализуемых ДИВ: величину аудитории, подвергающейся воздействию, среднюю длину диалогов, среднее количество просмотров зарегистрированных (незарегистрированных) пользователей и др. В свою очередь, выделение компонент сильной связности в графе, построенном по сообществам социальной сети, вероятно, позволит определить активно действующие группы пользователей: анализ подграфа (бикомпоненты) на предмет реализации ДИВ может указать на локальную организованную ячейку пользователей, организующую распространение запрещенной на территории РФ информации.

Очевидно, что анализ текстов, содержащих ДИВ, подразумевает применение методов информационного поиска и обработки текстов. Часто используемым подходом к идентификации ДИВ является использование паттернов как некоторого словаря, содержащего термины, свойственные определенному типу воздействия. Фактически чем в большей степени сообщение в сообществе социальной сети ближе к паттерну ДИВ, тем с большей долей вероятности можно утверждать, что в анализируемом сообществе осуществляется целенаправленное воздействие. Однако с точки зрения авторов настоящей работы применение паттерна ДИВ как словаря терминов не является эффективным подходом, в силу того что идентификация терминов, характеризующих ДИВ, может происходить как в сообщениях, содержащих ДИВ, так и в информационных текстах нейтрального характера. С целью выявления сообщений, действительно направленных на деструктивное

воздействие, разумным было бы использование мультиуровнего паттерна, в котором каждый последующий уровень терминов был бы уточняющим дополнением предшествующих уровней.

Эти и другие технологические методы выявления (а в перспективе и нейтрализации) ДИВ является областью научных интересов авторов настоящей работы.

Решение, казалось бы, рутинной технической задачи выявления ДИВ в сети Интернет на самом деле ставит фундаментальные проблемы поиска новых технологий и математических методов ее решения. И в данной работе авторы попытались показать эту методологическую взаимосвязь.

Воздействия с использованием специально подготовленного контента (информационно-гуманитарные воздействия) будут постоянно эволюционировать и разрастаться. Появляются различного рода новые акторы в сети Интернет, сделавшие своим орудием насилие и беззаконие в нем. Поэтому необходимо систематически обновлять существующие перечни потенциальных ДИВ, разрабатывать новые механизмы выявления и противодействия им. И более того, необходимо проводить прогнозные исследования в этой области, чтобы по возможности им противостоять, хотя бы в ближайшей и среднесрочной перспективе.

Наши зарубежные партнеры преуспели и активно совершенствуют ИКТ, которые нередко в явном и неявном виде являются средством агрессивного продвижения своих политических интересов, демонстрацией силы. Компьютерные атаки на государственные и негосударственные учреждения по всему миру в середине мая 2017 г. еще раз продемонстрировали возможность реализации деструктивных воздействий на информационную и коммуникационную инфраструктуру целых государств и конкретных организаций.

Необходимость систематического обновления существующих перечней потенциальных ДИВ, разработка новых механизмов выявления и противодействия им есть важная составляющая информационной безопасности государства. Для этого необходим непрерывный и всеобъемлющий мониторинг отечественного информационно-правового поля, того, что делается в этой области за рубежом.

Исследования подобного характера являются в явном виде междисциплинарными и в технических науках (информационные технологии, информационная безопасность, телекоммуникации и т. д.), и в гуманитарных (социальных науках, психологии,

правоведении, криминалистике, религиоведении, международных отношениях и т. д.). И учет, и исследование именно этой взаимосвязи позволит более эффективно решать проблему, вынесенную в заглавие настоящей работы.

Примечания

[1] По данным ресурса InternetWorldStats, на 31 декабря 2016 г. количество пользователей сети Интернет составило 3 696 238 430 пользователей. [Электронный ресурс] URL: http://www.internetworldstats.com/stats.htm (дата обращения: 10.05.2017).

[2] По данным ресурса Internet World Stats, на 30 июня 2016 г. количество пользователей одной из крупнейших социальных сетей Facebook составило 1 679 433 530 пользователей. [Электронный ресурс] URL: http://www.internetworldstats.com/facebook.htm (дата обращения: 10.05.2017).

[3] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // Совет Безопасности Российской Федерации [официальный сайт]. URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения: 05.05.2017).

[4] Резолюция Генеральной Ассамблеи ООН от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/53/70) [Электронный ресурс] URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 05.05. 2017).

[5] Резолюция Генеральной Ассамблеи ООН от 05.12.2016 г. № 71/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс] URL: http://undocs.org/ru/A/RES/71/28 (дата обращения: 05.05.2017).

[6] Google и Facebook приняли правила ЕС о борьбе с разжиганием ненависти [Электронный ресурс] URL: http://www.rbc.ru/technology_and_media/31/05/2016/574d83129a7947f4737b4fd7 (дата обращения: 05.05. 2017).

[7] По данным РБК, в феврале 2017 г. количество активных пользователей микроблогов Twitter упало на 4% и достигло 319 млн.

[8] Twitter приостановил действие более 230 тысяч аккаунтов, содержавших пропаганду терроризма. [Электронный ресурс] URL: http://tass.ru/mezhdunarodnaya-panorama/3549527 (дата обращения: 05.03.2017).

[9] YouTube, Facebook и Twitter объединились для борьбы с терроризмом [Электронный ресурс] URL:http://www.rbc.ru/rbcfreenews/584603c89a7947d15795875f?from=newsfeed(дата обращения: 05.03.2017) См.: http://www.rbc.ru/rbcfreenews/584603c89a7947d15795875f?from=newsfeed

[10] Федеральное агентство по делам национальностей (ФАДН России) образовано согласно Указу Президента России от 31 марта 2015 г. №168. [Электронный ресурс] URL: http://base.garant.ru/70928316/ (дата обращения: 05.05.2017).

[11] Утверждена Указом Президента Российской Федерации от 19 декабря 2012 г. № 1666. [Электронный ресурс] URL: http://kremlin.ru/acts/bank/36512 (дата обращения: 05.05.2017).

[12] ФАДН заявило о нехватке 1 млрд руб. для полного запуска системы мониторинга этнических конфликтов [Электронный ресурс] URL: https://rns.online/regions/FaDN-zayavilo-o-nehvatke-1-mlrd-rub-dlya-polnogo-zapuska-sistemi-monitoringa-etnicheskih-konfliktov-2017-03-10/ (дата обращения: 05.05.2017).

[13] Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] URL: http://eais.rkn.gov.ru/docs/149.pdf (дата обращения: 05.05.2017).

[14] Полное название системы — «Автоматизированная система контроля за соблюдением операторами связи требований, установленных статьями 15.1–15.4 Федерального закона от 27 июля 2006 г. № 149-ФЗ “Об информации, информационных технологиях и о защите информации” (АС “Ревизор”)».

[15] Расширенное заседание коллегии МВД России. [Электронный ресурс] URL: http://www.kremlin.ru/events/president/news/54014 (дата обращения: 05.05.2017).

[16] Там же.

[17] Официальный сайт Государственной Думы РФ: http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/5BB9B36A1C42865E432580DE00429B33/$File/118634-7_09032017_118634-7.PDF?OpenElement

[18] Там же.

[19] Роскомнадзор выявил более четырех тысяч групп о суицидах в соцсетях. [Электронный ресурс] URL: http://rkn.gov.ru/press/publications/news43517.htm (дата обращения: 05.05.2017).

[20] Instagram удалил более 300 ссылок с суицидальным контентом. [Электронный ресурс] URL: http://rkn.gov.ru/news/rsoc/news43367.htm (дата обращения: 05.05.2017).

[21] Рекомендации по распространению в СМИ информации о случаях самоубийств. [Электронный ресурс] URL: http://rospotrebnadzor.ru/upload/iblock/2a1/rekomendatsii-smi-_4_.pdf (дата обращения: 05.05.2017).

[22] Заседание коллегии Генеральной прокуратуры России [Электронный ресурс] URL: http://www.kremlin.ru/events/president/news/54035(дата обращения: 05.05.2017).

[23] Там же.

[24] Официальный сайт Роспотребнадзора: http://11.rospotrebnadzor.ru/news/-/asset_publisher/m3yU/content/

[25] *Казарин О.В., Скиба В.Ю., Шаряпов Р.А.* Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия «Документоведение и архивоведение. Защита информации и информационная безопасность». 2016. № 1(3). С. 54–72.

[26] *Казарин О.В., Шаряпов Р.А.* Вредоносные программы нового поколения – одна из существенных угроз международной информационной безопасности // Там же. 2015. № 12 (155). С. 9–23.

[27] Доктрина информационной безопасности Российской Федерации...

[28] Постановление Правительства РФ от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе “Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено».

[29] *Okhapkina E., Tarasov A., Okhapkin V.* Problem of identifying destructive informational influence in social networks // Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC): Third International Conference. Moscow, 6–8 July 2016. IEEE.

[30] *Okhapkina E., Okhapkin V., Kazarin O.* Adaptation of information retrieval methods for identifying of destructive informational influence in social networks // 31st IEEE International Conference on Advanced Information Networking and Applications. Tamkang University, Taipei, Taiwan. March 27–29, 2017.

[31] Среднеквадратическое отклонение.

[32] *Охапкина Е.П., Охапкин В.П., Казарин О.В.* Идентификация деструктивного информационного воздействия в социальных сетях на основе модели векторного пространства // Интеллектуальные системы в информационном противоборстве: Сб. науч. тр. Российской науч. конф. М.: РЭУ им. Г.В. Плеханова, 2016.

[33] Пересечение кластеров может означать, что в сообществах социальной сети реализуется два и более деструктивных информационных воздействия.

[34] Специфическая геометрическая форма может соответствовать группе сообществ под управлением единого центра и реализующих деструктивное информационное воздействие на различных нишах социальной сети.

[35] *Джеймс Г. и др.* Введение в статистическое обучение с примерами на языке R / Пер. с англ. С.Э. Мастицкого. М.: ДМК Пресс, 2016.