

## СОЦИОЛОГИЯ ИНТЕРНЕТА

---

DOI: 10.14515/monitoring.2020.3.1585



**А. Ю. Карпова, А. О. Савельев, А. Д. Вильнин, Д. В. Чайковский**

### **ИЗУЧЕНИЕ ПРОЦЕССА ОНЛАЙН-РАДИКАЛИЗАЦИИ МОЛОДЕЖИ В СОЦИАЛЬНЫХ МЕДИА (МЕЖДИСЦИПЛИНАРНЫЙ ПОДХОД)**

**Правильная ссылка на статью:**

Карпова А. Ю., Савельев А. О., Вильнин А. Д., Чайковский Д. В. Изучение процесса онлайн-радикализации молодежи в социальных медиа (междисциплинарный подход) // Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 3. С. 159—181. <https://doi.org/10.14515/monitoring.2020.3.1585>.

**For citation:**

Karpova A. Y., Savelev A. O., Vilnin A. D., Chaykovskiy D. V. (2020) Studying Online Radicalization of Youth through Social Media (Interdisciplinary Approach) . *Monitoring of Public Opinion: Economic and Social Changes*. No. 3. P. 159—181. <https://doi.org/10.14515/monitoring.2020.3.1585>.

**ИЗУЧЕНИЕ ПРОЦЕССА ОНЛАЙН-РАДИКАЛИЗАЦИИ МОЛОДЕЖИ В СОЦИАЛЬНЫХ МЕДИА (МЕЖДИСЦИПЛИНАРНЫЙ ПОДХОД)**

*КАРПОВА Анна Юрьевна — доктор социологических наук, доцент Школы базовой инженерной подготовки, Национальный исследовательский Томский политехнический университет, Томск, Россия*

*E-MAIL: belts@tpu.ru*

*<https://orcid.org/0000-0002-4211-5856>*

*САВЕЛЬЕВ Алексей Олегович — кандидат технических наук, доцент Инженерной школы информационных технологий и робототехники, Национальный исследовательский Томский политехнический университет, Томск, Россия*

*E-MAIL: sava@tpu.ru*

*<https://orcid.org/0000-0002-7466-6142>*

*ВИЛЬНИН Александр Даниилович — кандидат технических наук, заведующий лабораторией Инженерной школы информационных технологий и робототехники, Национальный исследовательский Томский политехнический университет, Томск, Россия*

*E-MAIL: vilninad@tpu.ru*

*<https://orcid.org/0000-0003-4838-3760>*

*ЧАЙКОВСКИЙ Денис Витольдович — кандидат философских наук, директор Школы базовой инженерной подготовки, Национальный исследовательский Томский политехнический университет, Томск, Россия*

*E-MAIL: dnvit@tpu.ru*

*<https://orcid.org/0000-0001-5146-6853>*

**STUDYING ONLINE RADICALIZATION OF YOUTH THROUGH SOCIAL MEDIA (INTERDISCIPLINARY APPROACH)**

*Anna Yu. KARPOVA<sup>1</sup> — Dr. Sci. (Soc.), Assistant Professor at the School of Core Engineering Education*

*E-MAIL: belts@tpu.ru*

*<https://orcid.org/0000-0002-4211-5856>*

*Alexei O. SAVELEV<sup>1</sup> — Cand. Sci. (Tech.), Assistant Professor at the School of Computer Science & Robotics*

*E-MAIL: sava@tpu.ru*

*<https://orcid.org/0000-0002-7466-6142>*

*Alexander D. VILNIN<sup>1</sup> — Cand. Sci. (Tech.), Head of the School of Computer Science & Robotics*

*E-MAIL: vilninad@tpu.ru*

*<https://orcid.org/0000-0003-4838-3760>*

*Denis V. CHAYKOVSKIY<sup>1</sup> — Cand. Sci. (Philos.), director, School of Core Engineering Education*

*E-MAIL: dnvit@tpu.ru*

*<https://orcid.org/0000-0001-5146-6853>*

<sup>1</sup> National Research Tomsk Polytechnic University, Tomsk, Russia

**Аннотация.** В статье доказывается, что междисциплинарный подход на основе интеграции уже показавших свою эффективность исследовательских инструментов перспективен для изучения процесса онлайн-радикализации молодежи в социальных сетях. Мы опираемся на международный опыт междисциплинарных исследований в области изучения радикализации, накопленный в таких научных центрах, как START, ICSR, CSEC, ISGA, и др.

В статье представлен опыт междисциплинарной проектной группы Томского политехнического университета по созданию прототипа программной системы для выявления ультраправых сообществ в социальной сети «ВКонтакте». Новый гибридный метод календарно-корреляционного анализа сочетает в себе скорость компьютерного анализа больших данных (чувствительный для обнаружения ультраправых сообществ), математическую модель для выявления целевой группы по характерному изменению активности группы в «окрестности» ключевых событий и базу знаний. Методика работы алгоритма позволит выявлять предикторы радикализации для разработки критериев отбора и маркирования триггерных объектов, значимых для ультрарадикальных сообществ в российской социальной сети; создать социальный граф из кластеров и перекрестных связей; прогнозировать угрозы и риски распространения радикальных идеологий. В перспективе прототип может применяться для анализа других социальных сетей и ультра-радикальных сообществ при условии пополнения базы знаний, адаптации правил анализа информации и соответствующих социологических шабло-

**Abstract.** The article attempts to prove that interdisciplinary approach based on a combination of research tools can be helpful in studying online radicalization of youth in social media. The authors rely on international interdisciplinary studies carried out by research centers such as START, ICSR, CSEC, ISGA, etc.

The article presents an experience of a multidisciplinary team from the Tomsk Polytechnic University in creating a prototype software system to identify far-right extremist communities on Vkontakte. A new hybrid method of calendar correlation analysis (CCA) combines the speed of Big Data computing (sensitive in detecting far-right extremist communities), a mathematical model helping to identify the target group based on the group activity in the “neighborhood” of key events, and a knowledge base. This methodology helps to identify predictors of radicalization to develop criteria for the selection and labeling of trigger objects being significant for ultra-radical communities on the Russian social networking website; to create a social graph of clusters and cross-links; to predict what threats and risks the spread of radical ideologies may pose. The prototype might be used for further analysis of other social networking platforms and ultra-radical communities provided that the knowledge base is replenished and the guidelines for analyzing the information and the corresponding sociological models are adapted. The authors also propose research strategies to test their method.

нов и моделей. Мы также излагаем исследовательские стратегии для проверки нашей методики.

**Ключевые слова:** молодежь, радикализация, ультраправые, экстремизм, терроризм, аналитика социальных сетей, Big data, web mining

**Keywords:** youth, radicalization, far-right, extremism, terrorism, social media analytics, Big data, web mining

**Благодарность.** Исследование выполнено при финансовой поддержке ГЗ «Наука», в рамках проекта FSWW-2020-0014.

**Acknowledgments.** The study is funded by the Science State Program as part of the project No. FSWW-2020-0014.

## Введение

Молодежь находится в группе риска, являясь наиболее уязвимой категорией населения для деструктивного информационно-психологического воздействия со стороны ультрарадикальных сообществ. Мерилом правовой оценки действий ультрарадикальных акторов и сообществ выступает правовая оценка уровня опасности для общества и государства применяемых ими методов. Приставка «ультра» означает, что радикалы принимают идею о том, что насилие необходимо для продвижения к цели. Они оправдывают, пропагандируют эту идею, выражают готовность перейти к насильственным действиям, а также берут на себя моральное обязательство по защите групп, продвигающих эту идею для достижения определенных политических, идеологических, религиозных, социальных и/или экономических целей [Borum, 2011].

Экстремистские и террористические группировки эффективно используют искусственно управляемые инструменты вовлечения молодежи через социальные медиа по всему миру. «Информационные интервенции» приобретают такие черты, как стремительность, всеохватность, вездесущность. Предиктором совершения насильственных инцидентов террористической и экстремистской направленности является радикализация. В самом общем виде под радикализацией понимается процесс перехода от ненасильственных форм выражения мнения к насильственным действиям. Интернет сам по себе — не причина радикализации, а фактор, способствующий переходу человека к совершению насильственных действий.

Радикализация как социальная проблема представляет собой комплекс сложных причинно-следственных связей и процессов, в которых множество факторов работают вместе. За последние два десятилетия все больше ученых, занимающихся изучением радикализации, сосредоточили усилия на том, чтобы классифицировать разнообразие радикальных идеологий, а также изучить технологии продвижения деструктивного контента для понимания механизмов вовлечения потенциальных новобранцев в ультрарадикальные сообщества.

Проблему вовлечения молодежи в экстремистские и террористические сообщества пытаются решить и на уровне силовых ведомств, Роскомнадзора, в сфере

государственной молодежной политики. Зачастую в качестве ограничительных мер принимаются решения, несоразмерные величине угрозы: либо завышающие предел допустимых ограничений, либо занижающие его. Кроме того, за неимением открытых постоянно обновляющихся источников официальных статистических данных и мониторинговых исследований в зарубежной научной периодике нередко публикуются исследования по России, искажающие реальную картину радикализации. Пример такого исследования — статья «Правый терроризм и насилие в путинской России» [Enstad, 2018]. Автор работы представляет Россию как «выдающийся случай правого терроризма по сравнению с западными странами», опираясь только на статистические данные Информационно-аналитического центра «Сова» и собственный анализ новостных сюжетов из датасета RTV-RUSSIA. Скучная статистика, тенденциозный подбор новостных сюжетов и некорректный сравнительный анализ превращают исследование в политическую «торговлю угрозами».

Федеральный список экстремистских материалов как источник данных для создания системы параметризованного поиска ключевых слов исключает возможность работы с ним по следующим причинам: отсутствует классификация по категориям идеологических платформ; отсутствуют систематизированные данные по решениям судов (дублирование, хаотичное размещение); не приведена классификация по типу загруженных в базу материалов (аудио, видео, письменный текст и т. п.); данные не систематизированы по составу преступления.

Публикуется значительное количество научных исследований об онлайн-радикализации, практически в каждом из которых подчеркивается «эффект массмедиа» — широкое освещение в средствах массовой информации деятельности экстремистских и террористических группировок. Фактически СМИ дают бесплатную рекламу экстремистам и террористам, стимулируют рост интереса молодежи к персонам и лидерам деструктивных организаций, увеличивают вероятность подражания им. Детальная отчетность, интенсивное медиафокусирование, многократное повторение месседжа — все это задает эмоциональную окраску отдельным фактам, идеям, персонам или группам и вдохновляет подражателей<sup>1</sup>.

В регионах России местные активисты создают добровольческие организации и иницируют разработку интернет-платформ для поиска противоправного контента, вовлекая в эту деятельность молодежь. Проекты такого рода, как «Киберпатруль» и «Кибердружина»<sup>2</sup>, сами по себе крайне опасны — по двум причинам. Во-первых, потому что к поиску деструктивного контента привлекается молодежь, не обладающая сформированной системой психологической защиты, развитыми навыками критического мышления. Обработывая такого рода контент, молодежь получает «дорожную карту» в виде стройной системы убеждений, интерпретирующей повод для недовольства (существование какой-то неспра-

<sup>1</sup> Hennigan W. J. (2018) How Big a Role Does Social Media Play in Homegrown Terrorism? *Time*. URL: <http://time.com/5438481/terrorism-social-media> (дата обращения: 10.06.2020).

<sup>2</sup> Киберпатруль и Кибердружина — это интернет-платформы, созданные общественными организациями, на которых волонтеров призывают собирать сведения об интернет-ресурсах, где предположительно содержится запрещенная информация. К данной категории причислена информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иная информация, за распространение которой предусмотрена уголовная или административная ответственность. Пример: <https://moi-portal.ru/proekty/bezopasnii-internet/>; <http://xn--8sbbqnlm4ahdvn2j.xn-p1ai/>.

ведливости). Демиурги радикальных организаций различного толка через такого рода «дорожную карту» навязывают молодежи видение того, каким должен быть справедливый мир и кто виноват в том, что существует некая несправедливость. И самое главное, показывают человеку то, что он может делать или что нужно сделать для построения справедливого мира, оправдывая достижение любых целей насильственными способами.

Во-вторых, кураторы такого рода общественных движений, руководствуясь благой идеей, недооценивают опасность практики подстрекательства к доносительству, стигматизации сообществ и конкретных пользователей социальных сетей. При этом она также способна принимать экстремистскую форму.

Такая практика закрепляется в сознании вовлеченных в нее молодых людей в виде габитуса и впоследствии распространяется на другие социальные группы. Мишенью при этом могут стать любые сообщества или отдельные индивиды, отличающиеся иными взглядами. В случае легитимации снятия барьеров экстремальность может проявляться, как в одну, так и в другую сторону, придавая конфронтационный характер социальным взаимодействиям. Все вышеописанные проблемы в практике противодействия вовлечению молодежи в экстремистские и террористические организации связаны либо с отсутствием, либо с искаженным пониманием самого процесса радикализации. Основатель ICSR (Международного центра по изучению радикализации) Питер Ньюманн указывает на тот факт, что радикализация как процесс принятия и поддержки убеждений не означает, что человек обязательно перейдет к мобилизации и совершению насильственных действий от имени группы или движения [Neumann, Smith, 2008]. Его позицию поддерживают и такие известные исследователи радикализации, как Кларк МакКоли и София Москаленко. Они разработали двухпирамидную модель политической радикализации, в которой наглядно отразили различие между радикализацией мнений и радикализацией действий [McCauley, Moskalenko, 2008]. Радикальные мнения и убеждения не являются преступными и отличаются от радикального поведения тем, что при последнем человек продвигает радикальные идеи посредством насилия и убежден в том, что насилие необходимо для продвижения к цели. Переход от ненасильственных способов выражения радикальных мнений и убеждений к радикальным действиям (насильственный экстремизм, терроризм) не является линейным процессом. Такой переход обусловлен целым рядом причин и сопутствующих факторов. Это и условия, среда, и ситуационные факторы, и идеологические, личностные, мотивационные факторы и многое другое. Именно поэтому модель радикализации мнений и модель радикализации действий исследователи представляют как два параллельных процесса, поскольку радикальных мнений недостаточно для запуска производства радикальных действий. «Плохие идеи не похожи на „нюхательную соль“, вдохнув которую, человек обязательно произведет радикальные действия» [McCauley, Moskalenko, 2017].

Радикализация представляет собой социальное явление, поскольку чаще формируется в сплоченной, замкнутой группе, а не среди одиночек. Понимание причин возникновения, катализатора процесса и механизмов перехода субъектов от радикальных мнений к радикальным действиям одинаково значимо для социологов, психологов, антропологов, криминологов. Научной проблемой является

отсутствие в российском исследовательском поле концепции радикализации (в том числе онлайн-радикализации). Также практически не представлены работы междисциплинарного характера, ориентированные на автоматизированный контент-анализ социальных медиа. Научная проблема может быть решена при помощи оперативного сопровождения исследований социальных медиа, которое напрямую зависит от скорости, надежности и эффективности компьютерных аналитических методов, а также использования соответствующих IT-инструментов.

Однако в российском научном поле накоплен теоретический и эмпирический материал в области изучения молодежного экстремизма. Наиболее полно в социологическом плане этот феномен был исследован учеными Института социально-политических исследований РАН, раскрывшими его сущность, отличительные черты, формы проявления и основные социальные детерминанты, условия конвертации типичной для молодости экстремальности в экстремизм, а также источники его эскалации и локализации [Зубок, Чупров, 2009; Зубок, 2015]. Данный опыт исследований остается актуальным в силу его фундаментальности, однако необходимы и новые исследования, раскрывающие с помощью создаваемых программных инструментов постоянно меняющийся механизм радикализации молодежи.

Выявление механизмов индивидуальной и групповой онлайн-радикализации в российских социальных сетях позволит ученым, занимающимся исследованиями в данной области, решать фундаментальные и прикладные задачи, в том числе:

- сформировать матрицы научных знаний для создания концепции радикализации применительно к российской специфике;
- создать методологию исследования процесса радикализации;
- получить целостную социально-топологическую картину структурной, реляционной и социальной динамики радикализации;
- проследить изменения масштаба и характера социальных и вспомогательных связей радикалов, проводить сравнительный анализ сходств и различий в идеологических платформах насильственной/ненасильственной радикальной среды;
- выявить когнитивные и личностные процессы, побудительные мотивы, опосредующие прямое и косвенное влияние различных факторов, запускающих в действие процесс радикализации.

Процесс изучения онлайн-радикализации в социальных медиа имеет специфические черты:

- таргетинговые технологии онлайн-радикализации в социальных сетях, которые изучаются зарубежными учеными (например, Facebook, Twitter, Gab и др.), значительно отличаются от технологий в российском поле (таких как «ВКонтакте» или «Одноклассники»);
- технологии продвижения ультрарадикальных сообществ в большой степени зависят от идеологической платформы (ультраправые, ультралевые, исламисты);
- API (программные интерфейсы приложений) для сбора данных в социальных сетях имеют существенные различия (например, у «ВКонтакте» и у Facebook), поэтому для исследований в российских популярных социальных сетях не-

возможно адаптировать имеющиеся зарубежные аналоги: необходимы специальные ПО, разработанные под возможности API и под конкретные исследовательские задачи;

- объем контента не позволяет исследователям отбирать его вручную, затрудняет поиск общих закономерностей и тенденций в данных, что ведет к неточностям/ошибкам в идентификации.

В связи со всем вышеперечисленным большое значение приобретает такой инструмент диагностики, как «аналитика социальных сетей». Это междисциплинарная исследовательская область, направленная на объединение, расширение и адаптацию методов анализа социальных медиа на основе применения методов web mining и создания инструментов для исследований в сфере общественно-политических наук [Sureka, Agarwal, 2014; Xie, Xu, Lu, 2016; Conway, 2017; Gilani, Kochmar, Crowcroft, 2017; Stieglitz et al., 2018]. Web mining, в свою очередь, сочетает методы информационного поиска, машинного обучения и интеллектуального анализа данных.

Количество зарубежных научных работ по аналитике в социальных сетях для изучения процесса радикализации за последнее десятилетие значительно выросло, но все еще имеются исследовательские лакуны. Широкие дискуссии о радикализации недостаточно хорошо проясняют, что представляет собой онлайн-радикализация и как, если они применяются, работают технологии деструктивного информационно-психологического воздействия на пользователей социальных сетей. Поэтому влияние онлайн-взаимодействия и пропаганды на процессы радикализации на уровне групп (мезоуровень) и индивидуальных акторов (микроуровень) остается предметом научных дискуссий. Опубликованные исследования содержат информацию об изучении факторов макроуровня радикализации. Например, террогенных<sup>3</sup> как внешних, так и внутренних факторов, в зависимости от страны, в которой проводились исследования. Ключевые направления исследований макроуровня: влияние бедности на развитие процесса радикализации [Jensen, Seate, James, 2018]; культурные, межконфессиональные и межнациональные противоречия, этнополитические конфликты [Disha, Cavendish, King, 2011]; причины социальной поляризации населения [Bejan, Parkin, 2015]; социальная мобильность и социальные лифты для молодежи [Kruglanski et al., 2016]; влияние политических возможностей и организационных ресурсов социальных движений [McCauley, 2011; Neumann, 2013; Morris, 2016; Conway, 2017; della Porta, 2018;]; оценка и влияние радикализации в тюрьмах на рост экстремистских и террористических инцидентов [Freilich, Gruenewald, Mandala, 2019; Valasik, 2017].

Сложность изучения онлайн-радикализации заключается в том, что технологии использования социальных сетей ультрарадикальными сообществами быстро развиваются и эффективно адаптируются к постоянно меняющимся возможностям онлайн-среды. Эта проблема привела к появлению широкого спектра исследований с использованием разнообразных методологий из различных дисциплин.

<sup>3</sup> Террогенные факторы — обуславливающие, определяющие причинные, функциональные, статистические, стохастические и другие формы детерминации (установления причин появления или проявления явления/феномена) терроризма.



## Междисциплинарный подход в области изучения процесса онлайн-радикализации

Междисциплинарный подход, основанный на интеграции знаний и методов социологов, специалистов в области computer science, психологов и лингвистов, позволяет создавать многоуровневую архитектуру для анализа социальных сетей, многофункциональные инструменты автоматического параметрического сбора и обработки данных для изучения онлайн-радикализации [Savelev, 2019].

Междисциплинарные подходы с применением и совершенствованием инструментов для исследований социальных медиа классифицированы А. Ю. Карповой по следующим категориям:

- *автономный* — применение методов вычислительной лингвистики на основе выявления речевых клише, лингвистических маркеров для анализа контента;
- *аддитивный* — применение методов вычислительной лингвистики, sentiment analysis и других методов для анализа и определения ролевых моделей и поведенческих траекторий;
- *гибридный* — применение методов, относящихся к группе технологий Data Science, метода NER (распознавание именованных сущностей), для выявления типологии социальных связей, операциональных механизмов, внешних факторов влияния;
- *многоуровневый* — применение всех вышеперечисленных методов в комплексе для создания инструментов прогнозирования и оценки рисков онлайн-радикализации, корреляции переменных микро-, макро- и мезоуровня для построения структуры сетевых кластеров и решения других задач.

Каждый из подходов имеет ограничения. Наиболее перспективным на сегодняшний день представляется многоуровневый подход, поскольку позволяет создать социально-топологическую картину структурной, реляционной, социальной индивидуальной и групповой динамики в онлайн-среде с учетом геопространственных и временных компонент, фиксируя масштаб и характер изменений сетевых контактов [Карпова, 2019].

Основные направления исследований в области изучения процесса онлайн-радикализации в мировой науке с применением междисциплинарного подхода можно классифицировать по следующим направлениям.

1. Общетематические исследования процесса онлайн-радикализации и созданные на их основе концепции и модели радикализации:

- концепция и модель индивидуальной радикализации [Moghaddam, 2005];
- концепция и модель политической радикализации [Borum, 2011; Neumann, 2009; McCauley, Moskalenko, 2008, 2017];
- концепция и модель террористической радикализации [Spaaij, Hamm, 2015].

2. Узкотематические исследования идеологических платформ радикалов (ультраправых, ультралевых, одиночек) [Kruglanski et al., 2018; Fahey, Pete, 2018], индивидуальной и групповой динамики мобилизации ультрарадикальных сообществ [Lewis, 2018; Vergani et al., 2018], ролевых моделей поведения [Langman, 2018; Faragó, Kende, Krekó, 2019].

Угрозы радикализации на ультраправой идеологической платформе отмечают в своем докладе за 2018 г. исследователи ICSR «ISIS [Исламское государство Ирака и Сирии] поглотил львиную долю правоприменительных и разведывательных ресурсов, в результате чего сильно ослаблено внимание к ультраправым экстремистским группам, которые развиваются и мобилизуются по всей Европе» [van der Heide, Winter, Maher, 2019: 10].

Исследователи отмечают, что сократилось количество физических инцидентов со стороны ультраправых групп, что возможно связано с их перемещением в онлайн среду. Такая гипотеза выдвигается на основании того, что использование компьютерных взломов и кибератак, чтобы вызвать экономический и социальный вред совершенных ультраправыми радикалами увеличились за период с 2010 по 2015 г. [Holt et al., 2019].

Одиночки, как отмечают исследователи из ICSR и START, мотивированы не какой-либо конкретной идеологией, а одной проблемой. Они создают многочисленные сетевые контакты, они не одиноки в сети, но одиноки в реальной жизни. Интернет — движущая сила для такого типа радикалов, и именно они оставляют многочисленные «цифровые следы» в интернете. Инструменты, созданные на основе web mining, позволяют выявлять таких радикалов по психологическим, эмоциональным, поведенческим «цифровым следам». Данный подход имеет свои ограничения: вероятностный характер выявленных причинно-следственных механизмов; пробелы в исходных данных; необходимость многократного эмпирического тестирования [Карпова и др., 2019].

3. Узкотематические исследования религиозно-политических исламских радикалов (мотивация, поведение, сетевые связи, влияние социальных медиа, методы вербовки и пропаганды). Стоит отметить, что компьютерный sentiment analysis текста, который еще в начале 2000-х годов стали применять к исламистским текстам, характеризуется большей воспроизводимостью и надежностью. LIWC (Linguistic Inquiry and Word Count) — самое популярное программное обеспечение для анализа текста с начала 2000-х, которое повышает надежность извлечения идеологических элементов из текста в области изучения исламистских материалов. Все больше внимания при создании такого программного обеспечения уделяется функциональным словам: количественный подсчет местоимений, экспрессивных прилагательных, артиклей по сравнению с содержанием слов. Данный инструмент имеет значительные ограничения, связанные со сложностью однозначной интерпретации триггерных слов, вероятностным набором языковых маркеров для определения речевых шаблонов, «информационный шум». Кроме того, в данном подходе подсчитываются все слова (лингвистический «эталон»), несмотря на их возможное потенциально неправильное значение. Существуют и другие трудности по созданию программного обеспечения, поскольку методы компьютерной лингвистики, основанные на взаимосвязи между использованием естественного языка и социальным поведением, имеют базовые словари на фарси, арабском, английском. Соответственно, для того чтобы адаптировать имеющиеся прототипы к исследованию российских социальных сетей необходима многоплановая, масштабная работа лингвистов [Neumann, Rogers, 2011; Pennebaker et al., 2015; Shuki et al., 2018; van der Heide, Winter, Maher, 2019; Kearns, Betus, Lemieux, 2019; Pieslak, Pieslak, Lemieux, 2019].

4. Создание баз данных инцидентов и профилей радикалов по многомерным переменным с использованием строгих методов классификации и кластеризации; маркеров условий, среды, событий жизненного цикла, социальных связей радикалов и других переменных для автоматической обработки данных:

- базы данных радикалов (например, PIRUS, CIDB);
- репозиторий из объединенных баз данных для изучения поведенческих, географических и временных характеристик насильственных инцидентов, матрицы научных знаний о влиятельных экстремистских организациях (например, TEVUS, BAAD, IVEO);
- базы данных террористических инцидентов (например, GTD, WITS);
- база данных скулшутеров (SchoolShooters.info).

Программное обеспечение в данной области позволяет формализовать множество многомерных переменных с информацией по широкому спектру от социометрических характеристик, событий жизненного цикла до мобилизационных факторов совершения инцидентов, выявлять различные типы подражания и вдохновения, определять подтипы радикалов. В целом такие базы данных дают возможность проводить по заданным критериям комплексную оценку рисков; коррелировать переменные макро-, мезо- и микроуровня. Основные ограничения такого программного обеспечения: проводить исследования возможно только при наличии постоянно обновляемых баз данных; существуют значительные ограничения доступа к полным данным для широкого круга исследователей.

Анализ показывает, что все имеющееся в зарубежном исследовательском поле ПО направлено на исследования популярных в международном поле социальных сетей, мессенджеров, имиджбордов, таких как Facebook, Twitter, YouTube, Tumblr, Gab, 8chan и др. Однако в российском поле социальных медиа самой востребованной площадкой для взаимодействия молодежи является социальная сеть «ВКонтакте».

Теоретический и эмпирический материал зарубежных исследований радикализации (индивидуальной, групповой) возможно использовать применительно к российским социальным сетям только с учетом адаптации.

### **Методология проектирования прототипа (опыт Томского политехнического университета)**

Предлагаемая нами методология включает три этапа. Первый этап — проектирование функции поиска по ключевым словам. Второй этап — проектирование функции поиска смежных сообществ (сообществ-сателлитов), построение социального графа пользователей для отображения связи между ультраправыми сообществами. Третий этап — программная реализация функции автоматизированной оценки календарной активности сообщества. Работа осуществлялась на примере открытых данных социальной сети «ВКонтакте» при соблюдении условий и ограничений лицензионного соглашения. При этом анализировались сообщества, а не отдельные учетные записи пользователей. Сбор, обработка и хранение персональных данных не осуществлялись.

*Первый этап.* Для решения задачи идентификации ультраправых экстремистских онлайн-групп (устойчивых, известных, многочисленных) и их «сателлитов»

(меньших по численности и малоизвестных) были созданы лингвистические маркеры — инструментальные специализированные словники ультраправых экстремистских групп.

Источники данных: Федеральный список экстремистских материалов Минюста РФ; Перечень общественных и религиозных объединений, иных некоммерческих организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом «О противодействии экстремистской деятельности»; Словарь экстремистских лозунгов ультраправой идеологической платформы, разработанный экспертом Ю. А. Сафоновой (Лаборатория экспертных исследований и ситуационного анализа, Москва); набор материалов по символике, предоставленный сотрудником Томского Центра «Э»; иные открытые источники.

Выделение ключевых слов на основе характеристики тематической значимости позволило автоматически получить из текстов слова и словосочетания, характеризующие тематику и содержание текста или множества текстов, для описания обобщенного лексикона сетевого сообщества (с выделением значимых объектов обсуждения) и для оценки близости и глубины пересечения индивидуальных лексиконов с обобщенным лексиконом сообщества.

Отобранный специфический контент был формализован и применен для автоматического поиска из набора данных «ВКонтакте» на май 2019 года — более 185 млн сообществ. В результате были отобраны экспериментальные группы — 94 наиболее репрезентативных сообщества, соответствующих критериям ультраправых и имеющих высокую онлайн-активность; всем им были присвоены идентификационные номера. По количеству участников эти онлайн-сообщества варьируются от сотни до нескольких тысяч человек. Все 94 сообщества были классифицированы по типу идеологической платформы (например, alt-right, нацисты, националисты, женоненавистники, неоязычники и др.). На данном этапе были выявлены следующие проблемы:

- Поиск по ключевым словам содержит большое количество «мусорного контента». Это связано с тем, что пользовательские данные содержат «шум» — флуктуацию значений признаков, описывающих процесс, неправильную грамматику, слова с ошибками, интернет-сленг, аббревиатуры, многоязычный текст, неформальные языковые выражения и т. п. Наличие некачественных метаданных увеличивает сложности и технические проблемы для сбора и анализа данных. Соответственно, сбор данных для подбора экспериментальных групп был дополнен вручную.
- Формализация словников под решаемые задачи не способствует точности установления корреляционной зависимости между значениями различных параметров.
- Объем контента затрудняет поиск общих закономерностей и тенденций в данных, что ведет к неточностям, ошибкам, ложным срабатываниям в идентификации деструктивного контента.

Таким образом, функция поиска по ключевым словам может быть эффективно применима только при наличии дополнительных, уточняющих поисковый результат инструментов.

*Второй этап.* Для изучения взаимосвязей ультраправых сообществ была реализована программная функция поиска сообществ-сателлитов на основе анализа пересечений участников. Проектирование данной программной функции основывается на использовании списка уже выявленных ультраправых сообществ. Социальная сеть «ВКонтакте» позволяет сообществам публиковать в открытом доступе ссылки на прочие источники (сообщества социальной сети «ВКонтакте», посты, страницы, а также на другие социальные сети или внешние веб-ресурсы). Группы, относящиеся к различным классам, и не ссылающиеся друг на друга, могут иметь общие ссылки на прочие сообщества, как относящиеся к ультраправым, так и не относящиеся к ним. В случае, если количество таких сообществ существенно, возможно выявить «недостающие звенья» в виде других ультраправых сообществ, а также обнаружить связи между сообществами различных классов (при наличии между ними тесной взаимосвязи: связи «сообщество—сообщество» или «сообщество — ссылка — сообщество»). В результате второго этапа были выделены компоненты связности для кластеризации, проведен анализ взаимосвязи между экспериментальными сообществами.

*Третий этап.* Специфический фактор, выявленный в процессе исследования ультраправых сообществ, — это «скрепы» в виде дат, событий. С помощью таких «скреп» активизируются вялотекущие обсуждения в сообществе, происходит разогрев участников, провоцирование на агрессивные высказывания, разжигание ненависти, использование «языка вражды». Была сформулирована гипотеза о том, что сообщества данной направленности не оставляют без внимания важные для них даты (даты инцидентов, дни рождения идеологических лидеров и вдохновителей и т. п.). Таким образом, значение активности в сообществе социальной сети в окрестностях значимых для идеологической платформы дат может быть использовано в качестве уточняющего поискового критерия. Программно были реализованы функции автоматизированной оценки календарной активности сообщества. Метод получил название «календарно-корреляционный анализ» (ККА). Схема работы ККА представлена на рисунке 1. Суть ККА заключается в автоматизации процесса выявления целевой группы по характерному изменению активности группы и контента в «окрестности» ключевых событий. При реализации были учтены следующие факторы:

а) отсутствие возможности извлечь ретроспективные данные об активности сообществ; возможность оценить только общее количество просмотров, «лайков», репостов и комментариев (с даты публикации сообщения);

б) сообщество может демонстрировать аномальную активность по сравнению с обычной за некоторое время до наступления значимой даты и некоторое время спустя;

в) активность сообщества в значимые даты может быть случайной или общей не только для сообществ радикальной направленности;

г) сильным признаком радикального сообщества являются совпадения знаковых дат и определенных лексических маркеров в материалах, связанных с этой датой.

Элементом базы знаний, служащим основой для работы ККА, является dataset ключевых слов и дат (см. табл. 1).

Таблица 1. *Пример dataset (база знаний ключевых слов и событий)*

date*	category*	tags*	keywords*	stars*	comment*
18.05.2006	Ультраправые	Неонацисты; Неоязычники	дмитр, александр, боровиков, нацист, язычник, экстремист, террорист	3	погиб Дмитрий Александрович Боровиков — русский неонацист и неоязычник, организатор двух экстремистских группировок «Mad Crowd» и «Боевой террористической организации». Погиб от смертельного ранения при задержании оперативниками 18-го отдела УБОП

*Примечание:* *date* — дата события, заполняется в формате ДД.ММ.ГГГГ, если известна точно и в формате ДД.ММ, если известен только календарный день;

*category* — идеологическая платформа, характерная для данного события или ключевого слова;

*tags* — теги, лексические маркеры, обозначающие принадлежность к идеологической платформе;

*keywords* — ключевое слово;

*stars* — рейтинг, ключевого слова или события, характеризующий его значимость при идентификации группы;

*comment* — комментарий.

Для расчета абсолютной и относительной активности сообщества была разработана математическая модель. Абсолютной активностью будем называть средневзвешенный показатель количества элементарных действий членов сообщества, а именно: просмотры, маркер «лайк», цитирование, просмотры. За относительную активность принято значение абсолютной активности дня, отнесенное к средней активности сообщества в окрестности данного дня. Примеры абсолютной и относительной активности кодированного сообщества FB 1.19 представлены на рисунке 2.

Для надежной идентификации группы фиксируется подъем, высокий уровень и спад активности в группе, причем в разные даты (представляющие календарь ключевых событий, базу знаний). Например, активность значительно увеличивается в окрестности даты «29.04» — знакового для ультраправых дня, когда неонацистом был совершен инцидент. Другой пример: повышение активности в окрестности «16.10» — дата создания российской ультраправой националистической организации «Русское Национальное Единство» (ООПД РНЕ). Показателен также пример с датами рождений «09.06» и «17.10». Стоит отметить, что «скрепы» в виде дат в ультраправых сообществах показывают, как интенсифицируется активность и задается идеологическая повестка дня группы, что дает возможность пользователю четко продемонстрировать свою связь с движением. Фактически «демиурги» ультраправых сообществ находятся в постоянном поиске значимых «скреп», чтобы фундировать активность.

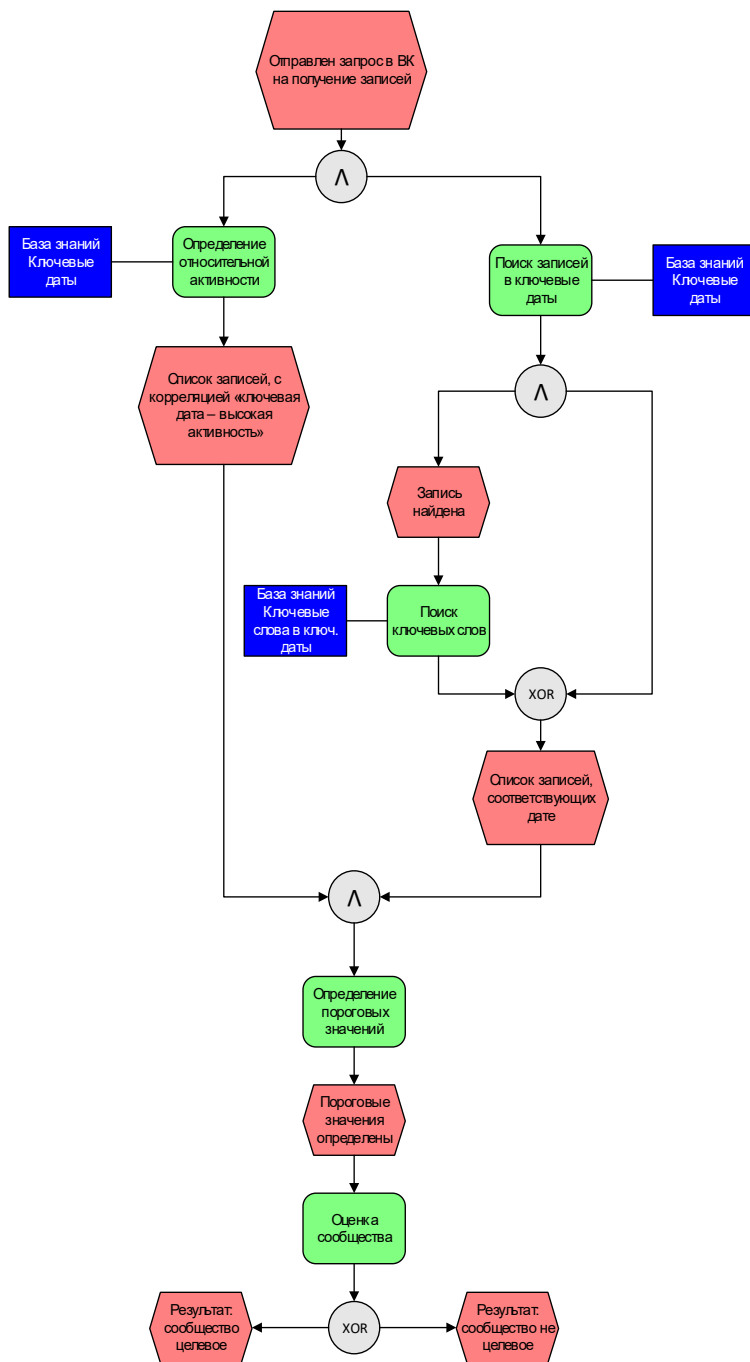


Рис. 1. Обобщенная eEPC-схема оценки принадлежности сообщества социальной сети к целевой группе (ультраправые) на основе ККА

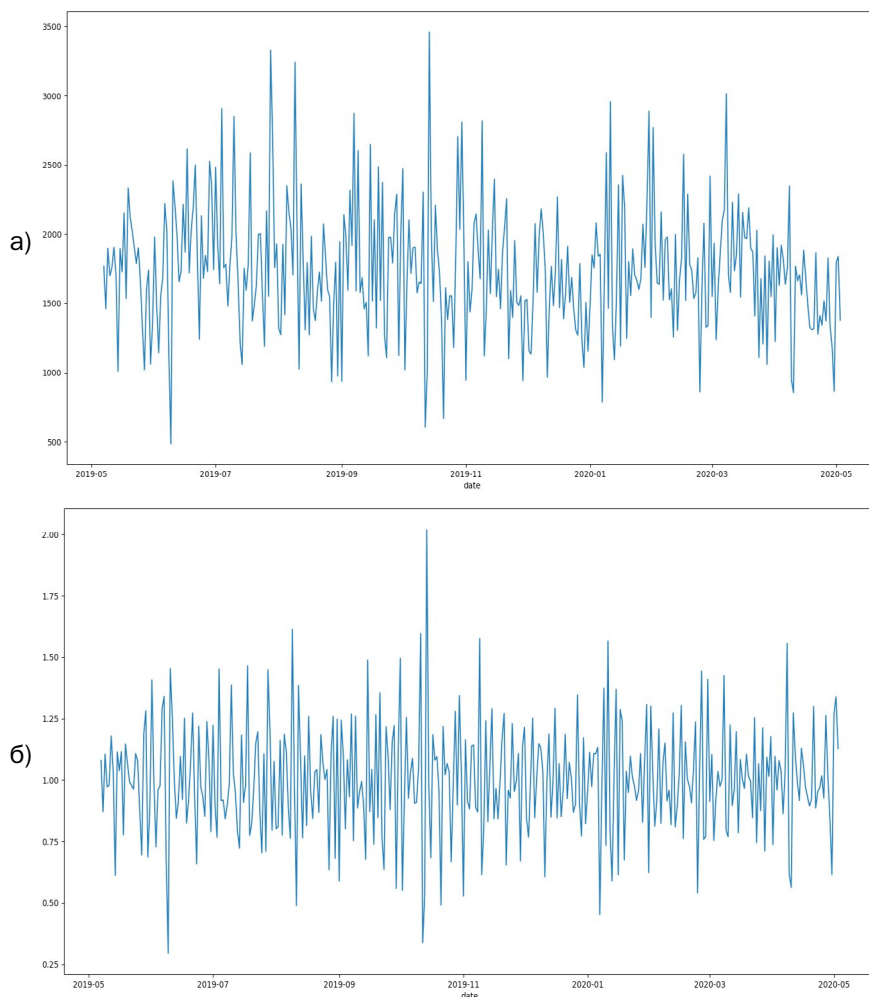


Рис. 2. Примеры графиков (а) абсолютной и (б) относительной активности группы FB 1.19

Разработанный метод позволяет не только извлечь абсолютные значения активности сообщества, но и нормировать их, а также дополнительно уточнять характер активности (каждой значимой дате соответствует набор ключевых слов и выражений, связанных с ней). Таким образом обеспечивается бóльшая точность выявления ультраправых радикальных сообществ и минимизация ложных срабатываний.

### Апробация

Для оценки эффективности работы алгоритма были выполнены тестовые испытания. В рамках первого из них был осуществлен поиск сообществ по подготовленным формализованным ключевым словам (49 слов). Найдено 6151 сообщество.



Сообщества проверены методом ККА, который указал только на три сообщества. Все они — с ультраправой идеологической платформой, что и требовалось проверить (учитывались только сообщества, проявляющие активность в течение календарного года до даты анализа).

При втором испытании был проверен ранее упоминавшийся список из 94 сообществ. При тестировании данного списка сообществ обнаружено, что из них активных — 68, заблокировано — 3, закрыто — 1, не найдено — 2. При определении активности принято: если сообщество публикует одну запись в неделю, оно считается активным. Из указанного списка ККА «сработал» на 14 сообществах.

В рамках третьей проверки алгоритма был выполнен тестовый вариант «обратного ККА». Выбраны 39 наиболее популярных сообщества по версии «ВКонтакте». Эксперты проверили их вручную. Ни одно из сообществ экспертом не было отнесено к ультрарадикальным. Апробация показала, что на данных сообществах «чувствительность» алгоритма не сработала. Следовательно, эффективность работы алгоритма подтверждена.

Эффективность работы алгоритма также может быть проиллюстрирована через значения ошибок первого и второго рода. Последние могут быть вычислены для второй и третьей проверок, поскольку априорная информация о степени принадлежности к ультраправой идеологической платформе каждой из 6151 групп, найденных по ключевым словам, отсутствует. В качестве нулевой гипотезы  $H_0$  примем, что анализируемое сообщество не содержит признаков принадлежности к ультраправой идеологической платформе. Соответственно, альтернативная гипотеза —  $H_1$  — сообщество содержит признаки принадлежности.

В рамках второй проверки гипотеза  $H_0$  была ошибочно принята в 54 случаях, гипотеза  $H_1$ , соответственно, верно принята в 14. Таким образом, вероятность ошибки второго рода равна  $\beta = 0,79$  и мощность критерия  $(1 - \beta) = 0,21$ .

В рамках третьей проверки гипотеза  $H_0$  ни разу не была ошибочно отвергнута и гипотеза  $H_1$  не была ошибочно принята, то есть ошибок применения критерия не обнаружено.

Сравнительно низкая эффективность алгоритма при второй проверке может быть объяснена неполнотой информации в базе знаний, описывающей значимые для ультраправых «скрепы». Поскольку представленные в экспертном списке сообщества относятся к различным подклассам ультраправых, то и специфическую активность они могут проявлять в различные даты. Также отметим, что алгоритм в рамках проверок не показал ошибок первого рода, что позволяет говорить о его применимости в качестве дополнительного «фильтра» при анализе поисковых результатов по ключевым словам.

В общем виде функции алгоритмов были собраны в единую поисково-аналитическую систему (ПАС) и представлены в такой последовательности:

- 1) пользователь-эксперт формирует базу знаний (перечень ключевых слов, выражений и дат, определяя их взаимосвязь);
- 2) пользователь запускает функцию первичного поиска по ключевым словам;
- 3) предварительная обработка полученных результатов (удаление закрытых, неактивных, «пустых» сообществ);
- 4) методом ККА уточняется список выявленных ультраправых сообществ;

5) результаты анализируются пользователем и при необходимости заносятся в базу знаний;

6) пользователь формирует множество групп для последующего поиска смежных сообществ (сателлитов);

7) анализируются результаты поиска сообществ-сателлитов, при необходимости уточняется информация в базе знаний.

Обобщенная схема работы алгоритма представлена на рисунке 3.

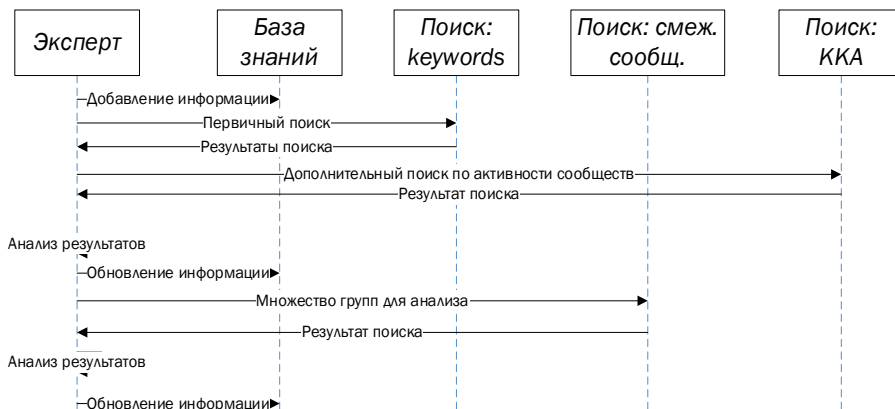


Рис. 3. Последовательность обобщенного алгоритма выявления активных ультраправых идеологических платформ в социальной сети

Стек использованных при программной реализации технологий: язык программирования Python 3, база данных MongoDB, среда разработки Anaconda 3, система контроля версий git и облачный репозиторий github.com.

## Заключение

Скорость и надежность ПАС для сопровождения научных исследований радикализации молодежи в социальных медиа напрямую зависит от качества:

- формализации переменных экспертом, охватывающим субъективное значение и содержание, которое компьютерное программное обеспечение может обнаружить;
- представления неструктурированных данных в форме, пригодной для последующей алгоритмизации задач исследования.

Направление дальнейшей работы по созданию ПАС:

- подготовка и разметка датасетов для обучения модели автоматизированной классификации сообществ;
- формализация неструктурированных данных для базы знаний в виде распознавания символики; мемов (синтезирующих поп-культуру, идеологические и политические убеждения); музыки, видео; уникального языка (сленга), с помощью которого сообщества демонстрируют взаимосвязь, идентификацию, веру и убеждения;

— предикторы и целевые признаки dataset необходимо создать на основе текста, аудио- и видеоконтента.

При соответствующих изменениях в базе знаний возможен поиск не только ультраправых сообществ. Наполнение базы знаний информацией по иным идеологическим платформам позволит изучить характер и силу их взаимосвязей и взаимного влияния.

Применение ККА (при условии наполнения базы знаний по датам) может позволить эффективно выявлять одиночек (скулшутеры, массовые убийцы, террористы-одиночки), которые имеют высокую степень радикализации и, соответственно, опасность совершения инцидентов. Одиночки мотивированы на совершение противоправных насильственных действий одной идеей или одной проблемой, которая может быть идентифицирована по идеологической платформе, может быть смешанной. Но именно для этой категории радикалов особенно важны такие «скрепы», как честование дат и событий. Соответственно, алгоритм к выявлению данной категории будет «чувствителен».

Практическое применение междисциплинарного подхода для изучения процесса радикализации молодежи в социальных медиа является перспективным направлением, поскольку позволяет создавать высокоточные программные алгоритмы, преодолевая исследовательские лакуны. Ключевые задачи, которые необходимо решить при конструировании такого рода инструментов: создание или адаптация методов классификации и кластеризации; подбор критериев взаимосвязанности между теоретическими исследованиями и эмпирическими данными; выявление статистических типологий; наполнение базы знаний.

## Список литературы (References)

Зубок Ю. А., Чупров В. И. Молодежные движения как форма социальной самоорганизации // Россия в условиях глобального кризиса: социальная и социально-политическая ситуация в России в 2008 году. М.: Институт социально-политических исследований РАН, 2009. С. 167—182.

Zubok Yu.A., Chuprov V.I. (2009) Youth movements as a form of social self-organization. In: Russia in the context of the global crisis: the social and socio-political situation in Russia in 2008. Moscow: Institute for Social and Political Studies, RAS. P. 167—182. (In Russ.)

Зубок, Ю. А. Доверие в саморегуляции молодежного экстремизма // Знание. Понимание. Умение. 2015. № 4. С. 63—77. <https://doi.org/10.17805/zpu.2015.4.6>.  
Zubok Yu.A. (2015) Confidence in the self-regulation of youth extremism. *Knowledge. Understanding. Skill*. No. 4. P. 63—77. <https://doi.org/10.17805/zpu.2015.4.6>. (In Russ.)

Карпова А. Ю., Савельев А. О., Вильнин А. Д., Чайковский Д. В. Новые технологии выявления ультраправых экстремистских сообществ в социальных медиа // Вестник Томского государственного университета. Философия. Социология. Политология. 2019. № 52. С. 138—147.

Karpova A. Yu., Savelyev A. O., Vilnin A. D., Tchaikovsky D. V. (2019) New technologies for identifying ultra-right extremist communities in social media. *Tomsk State University Bulletin. Philosophy. Sociology. Political science*. No. 52. P. 138—147. (In Russ.)

Карпова А. Ю. Модели построения профилей радикалов для прогнозирования инцидентов террористической и экстремистской направленности. Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации // XI Всероссийская межведомственная научная конференция: материалы и доклады (Орёл, 5—6 февраля 2019 года). В 10 ч. Ч. 10 / под общ. ред. П. Л. Малышева. Орёл : Академия ФСО России, 2019. С. 84—87.

Karpova A. Yu. (2019) Models for constructing radical profiles for forecasting incidents of a terrorist and extremist nature. Actual directions of the development of security systems, special communications and information for the needs of state authorities of the Russian Federation. In: P. L. Malysheva (ed.). *XI All-Russian Interdepartmental Scientific Conference: materials and reports*. At 10 hours, part 10. Orel: Academy of the Federal Security Service of Russia. P. 84—87. (In Russ.)

Bejan V., Parkin W. S. (2015) Examining the effect of repressive and conciliatory government actions on terrorism activity in Israel. *Economics Letters*. Vol. 133. P. 55—58. <https://doi.org/10.1016/j.econlet.2015.05.016>.

Borum R. (2011) Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*. Vol. 4. No. 4. P. 7—36. <https://doi.org/10.5038/1944-0472.4.4.1>.

Braniff W. (2017) Recasting and Repositioning CVE as a Grand Strategic Response to Terrorism. *START*. Vol. 11. URL: <https://www.start.umd.edu/news/recasting-and-repositioning-cve-grand-strategic-response-terrorism> (accessed: 10.03.2020).

Conway M. (2017) Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism*. Vol. 40. No. 1. P. 77—98. <https://doi.org/10.1080/1057610X.2016.1157408>.

Disha I., Cavendish J. C., King R. D. (2011) Historical events and spaces of hate: Hate crimes against Arabs and Muslims Post-9/11 America. *Social Problems*. Vol. 58. No. 1. P. 21—46. <https://doi.org/10.1525/sp.2011.58.1.21>.

della Porta D. (2018) Radicalization: A Relational Perspective. *Annual Review of Political Science*. Vol. 21. P. 461—474. <https://doi.org/10.1146/annurev-polisci-042716-102314>.

Enstad J. (2018) Right-Wing Terrorism and Violence in Putin's Russia. *Perspectives on Terrorism*. Vol. 12. No. 6. P. 89—103.

Kearns E. M., Betus A. E., Lemieux A. F. (2019) When Data Do Not Matter: Exploring Public Perceptions of Terrorism. *Studies in Conflict & Terrorism*. P. 1—22. <https://doi.org/10.1080/1057610X.2018.1543145>.

Fahey S., Pete S. (2018) Pathways to violent extremism: a qualitative comparative analysis of the US far-right. *Dynamics of Asymmetric Conflict*. Vol. 12. No. 1. P. 42—66. <https://doi.org/10.1080/17467586.2018.1551558>.

Faragó L., Kende A., Krekó P. (2019) Justification of intergroup violence — the role of right-wing authoritarianism and propensity for radical action. *Dynamics of Asymmetric Conflict*. Vol. 12. No. 2. P. 113—128. <https://doi.org/10.1080/17467586.2019.1576916>.

Freilich J. D., Gruenewald J., Mandala M. (2019) Situational crime prevention and terrorism: An assessment of 10 years of research. *Criminal Justice Policy Review*. Vol. 30. No. 9. P. 1283—1311. <https://doi.org/10.1177/0011128717718488>.

Gilani Z., Kochmar E., Crowcroft J. (2017) Classification of Twitter Accounts into Automated Agents and Human Users. In: *International Conference on Advances in Social Networks Analysis and Mining*. P. 489—496. <https://doi.org/10.1145/3110025.3110091>.

Holt T. J., Stonhouse M., Freilich J., Chermak S. M. (2019) Examining Ideologically Motivated Cyber attacks Performed by Far-Left Groups. *Terrorism and Political Violence*. <https://doi.org/10.1080/09546553.2018.1551213>.

Jensen M. A., Seate A. A., James P. A. (2018) Radicalization to Violence: A Pathway Approach to Studying Extremism. *Terrorism and Political Violence*. P. 1—24. <https://doi.org/10.1080/09546553.2018.1442330>.

Kruglanski A. W., Gelfand M. J., Sheveland A., Babush M., Hetiarachchi M., Bonto M. Ng, Gunaratna R. (2016) What a difference two years make: patterns of radicalization in a Philippine jail. *Dynamics of Asymmetric Conflict*. Vol. 9. No. 1—3. P. 13—36. <https://doi.org/10.1080/17467586.2016.1198042>.

Kruglanski A. W., Woolley K., Chernikova M., Fishbach A., Bélanger J., Molinario E., Pierro A. A. (2018) Structural Model of Intrinsic Motivation: On the Psychology of Means-Ends Fusion. *Psychological Review*. Vol. 125. No. 2. P. 165—182. <https://doi.org/10.1037/rev0000095>.

Langman P. (2018) Different Types of Role Model Influence and Fame Seeking Among Mass Killers and Copycat Offenders. *American Behavioral Scientist*. Vol. 62. No. 2. P. 210—228. <https://doi.org/10.1177/0002764217739663>.

Lewis R. (2018) Alternative ENDNOTES Influence: Broadcasting the Reactionary Right on YouTube. Report. Data & Society's Media Manipulation research initiative. URL: [https://datasociety.net/wp-content/uploads/2018/09/DS\\_Alternative\\_Influence.pdf](https://datasociety.net/wp-content/uploads/2018/09/DS_Alternative_Influence.pdf) (accessed: 10.06.2020).

McCauley C. (2017) Toward a Psychology of Humiliation in Asymmetric Conflict. *American Psychologist*. Vol. 72. No. 3. P. 255—265. <https://doi.org/10.1037/amp0000063>.

McCauley C., Moskalkenko S. (2008) Mechanisms of Political Radicalization: Pathways Toward Terrorism. *Terrorism and Political Violence*. Vol. 20. No. 3. P. 415—433. <https://doi.org/10.1080/09546550802073367>.

- McCauley C., Moskalenko S. (2011) Friction: How Radicalisation Happens to Them and Us. *Journal of Strategic Security*. Vol. 4. No. 4. P. 195—196. <https://doi.org/10.1080/09546553.2012.728938>.
- McCauley C., Moskalenko S. (2017) Understanding political radicalization: The two-pyramids model. *American Psychologist*. Vol. 72. No. 3. P. 22—23. <https://doi.org/10.1080/09546553.2020.1763964>.
- Moghaddam F. M. (2005) The staircase to terrorism: a psychological exploration. *American Psychologist*. Vol. 60. No. 2. P. 161—169. <https://doi.org/10.1037/0003-066X.60.2.161>.
- Morris T. (2016) *Dark ideas: How Neo-Nazi and violent Jihadi ideologues shaped modern terrorism*. Lanham: Lexington Books.
- Neumann P. R. (2009) *Old and New Terrorism*. Cambridge: Polity Press.
- Neumann P. R. (2013) The trouble with radicalization. *International Affairs*. Vol. 89. No. 4. P. 873—893. <https://doi.org/10.1111/1468-2346.12049>.
- Neumann P., Rogers B. (2011) *Recruitment and Mobilisation for the Islamist Militant Movement in Europe*. London: King's College London,
- Neumann P., Smith M. L. R. (2008) *The Strategy of Terrorism: How it Works, and why it Fails*. New York and London: Routledge.
- Pennebaker J. W., Booth R. J., Boyd R. L., Francis M. E. (2015) *Linguistic Inquiry and Word Count (LIWC)*. Austin, TX: Pennebaker Conglomerates.
- Pieslak J., Pieslak B., Lemieux A. F. (2019) Trends of Anashid Usage in Da'esh Video Messaging and Implications for Identifying Terrorist Audio and Video. *Studies in Conflict & Terrorism*. <https://doi.org/10.1080/1057610X.2018.1545828>.
- Savelev A., Karpova A., Chaykovskiy D., Vilnin A., Kaida A., Kuznetsov S., Igumnov L., Maksimova N. (2019) The High-Level Overview of Social Media Content Search Engine. Proceedings of the 14th International Forum on Strategic Technology (IFOST). Tomsk: TPU Publishing House. P. 306—309. URL: [http://earchive.tpu.ru/bitstream/11683/57450/1/conference\\_tpu-2019-C127.pdf](http://earchive.tpu.ru/bitstream/11683/57450/1/conference_tpu-2019-C127.pdf) (accessed: 10.06.2020).
- Shuki J. Cohen, Kruglanski A., Gelfand M. J., Webber D., Gunaratna R. (2018) Al-Qaeda's Propaganda Decoded. *A Psycholinguistic System for Detecting Variations in Terrorism Ideology, Terrorism and Political Violence*. Vol. 30. No. 1. P. 142—171. <https://doi.org/10.1080/09546553.2016.1165214>.
- Spaaij R., Hamm M. (2015) Lone wolf terrorism in America: Using knowledge of radicalization pathways to forge prevention strategies. *National Criminal Justice Reference Service*. Vol. 38. No. 2. <https://doi.org/10.1080/1057610X.2014.986979>.
- Stieglitz S., Mirbabaie M., Ross B., Neuberger C. (2018) Social media analytics — Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*. Vol. 39. P. 156—168. <https://doi.org/10.1016/j.ijinfomgt.2017.12.002>.

Sureka A., Agarwal S. (2014) Learning to classify hate and extremism promoting tweets. In: Intelligence and Security Informatics Conference (JISIC). P. 320. <https://doi.org/10.1109/JISIC.2014.65>.

Valasik M., Phillips M. (2017) Understanding modern terror and insurgency through the lens of street gangs: ISIS as a case study. *Journal of Criminological Research, Policy and Practice*. Vol. 3. No. 3. P. 192—207. <https://doi.org/10.1080/1057610X.2018.1450613>.

van der Heide L., Winter Ch., Maher Sh. (2019) The Cost of Crying Victory: Policy Implications of the Islamic State's Territorial Collapse. International Centre for Counter-Terrorism — The Hague (ICCT). URL: <https://icsr.info/2019/01/09/the-cost-of-crying-victory-policy-implications-of-the-islamic-states-territorial-collapse/> (accessed: 10.06.2020).

Vergani M., Iqbal M., Ilbahar E., Barton G. (2018) The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence about Radicalization into Violent Extremism. *Studies in Conflict & Terrorism*. <https://doi.org/10.1080/1057610X.2018.1505686>.

Xie D., Xu J., Lu T.-C. (2016) Automated Classification of Extremist Twitter Accounts Using Content-Based and Network-Based Features. In: International Conference on Big Data, Washington. P. 2545—2549.