

ТЕМА НОМЕРА

МЕТОДОЛОГИЯ В РОССИЙСКОЙ СОЦИОЛОГИИ

DOI: 10.19181/vis.2024.15.1.2

EDN: VWSNFH

**Практическая сетевая топология
в исследовании процесса
онлайн-радикализации молодежи:
возможности и ограничения**

Ссылка для цитирования: *Зубок Ю. А., Карпова А. Ю., Савельев А. О.* Практическая сетевая топология в исследовании процесса онлайн-радикализации молодежи: возможности и ограничения // Вестник Института социологии. 2024. Том 15. № 1. С. 13–42. DOI: 10.19181/vis.2024.15.1.2; EDN: VWSNFH.

For citation: Zubok Yu. A., Karpova A. Yu., Savelev A. O. Practical network topology in the study of online radicalisation of youth: opportunities and limitations. *Vestnik instituta sotziologii*. 2024. Vol. 15. No. 1. P. 13–42. DOI: 10.19181/vis.2024.15.1.2; EDN: VWSNFH.



AuthorID РИНЦ: 74721

**Зубок
Юлия Альбертовна^{1,2}**¹Институт социологии ФНИСЦ РАН, Москва, Россия;²Институт социально-политических исследований ФНИСЦ РАН, Москва, Россия

uzubok@mail.ru



AuthorID РИНЦ: 507861

**Карпова
Анна Юрьевна¹**¹Национальный исследовательский
Томский политехнический университет, Томск, Россия

belts@tpu.ru



AuthorID РИНЦ: 753578

**Савельев
Алексей Олегович¹**¹Национальный исследовательский
Томский политехнический университет, Томск, Россия

sava@tpu.ru

Аннотация. В настоящей статье представлены ключевые подходы к пониманию и исследованию радикализации, а также возможности и ограничения применения некоторых исследовательских методов для моделирования сетевой топологии и оценки контентного сходства онлайн-сообществ. Сегодня в исследованиях социальных сетей и участия в них молодежи часто применяются методы и технологии Web Mining и AI. Однако до сих пор остается открытым вопрос о том, как эти подходы могут быть эффективно использованы в целях изучения онлайн-радикализации. Ответ на него должен повысить объяснительную и прогностическую способность вычислительных моделей для обнаружения и прогнозирования радикализации в онлайн-пространстве. В значительной части российских исследований онлайн-радикализации распространен подход, при котором задача выявления взаимосвязей отдельных онлайн-сообществ или их кластеров сводится к оценке степени их сходства по подписчикам, либо по лингвистическим маркерам. Такой подход ограничен в прогнозировании новых связей между сообществами и обосновании путей радикализации, но в то же время актуален в моделировании информационной диффузии. В данной работе авторы стремятся продемонстрировать возможности и ограничения применения методов tf-idf, doc2vec для оценки контентного сходства онлайн-сообществ без признаков радикализации и онлайн-сообществ с признаками радикализации. Такой подход позволил выявить сообщества со значительной тенденцией к объединению (установлению прямых связей). В статье представлены результаты сравнительного исследования в виде социальных графов, сформированных по принципам общности подписчиков, сходства значимых слов, контекстного сходства на базе doc2vec модели. Социальный граф на основе doc2vec метода показал лучшие результаты с точки зрения кластеризации онлайн-сообществ, а также интерпретируемости результатов. Это является критически значимым для обнаружения и прогнозирования радикализации в Интернете, поскольку открывает перспективы для изучения природы ассортативности в наблюдаемой сети.

Ключевые слова: социальная сеть, сообщество, радикализация, сетевая топология, tf-idf, doc2vec

Введение

В течение последних десятилетий тема радикализации в молодежной среде не теряет актуальности. Молодые люди становятся активными участниками сообществ, демонстрирующих радикальные взгляды и настроения. Мобилизуясь на почве противостояния своих и чужих, неприязни и вражды, они время от времени совершают насильственные действия, жертвами которых, как правило, становятся их же сверстники.

Движущей силой радикальных, экстремистских сообществ молодежь выступает, прежде всего, в силу присущих ей групповых особенностей – лабильности и экстремальности сознания, и высокой установки на риск, свойственных становящемуся субъекту социальных отношений, а также субкультурных форм самоорганизации. И лабильность (подвижность, изменчивость смысловых структур), и экстремальность (склонность к крайностям в суждениях, оценкам, поведении), и риск (особенность состояния и действия в ситуации перехода от неопределенности к определенности) обусловлены возрастными психофизическими и эмоциональными особенностями, определяющими способы восприятия молодыми людьми

окружающей действительности, реагирования и выстраивания взаимодействий. С этой точки зрения они являются естественными атрибутами взросления, такими же, как и неформальная самоорганизация, выполняющая функции инструмента группового прорыва во взрослый мир. Однако сама групповая самоорганизация, призванная демпфировать травматичность взросления, часто становится питательной средой для эскалации спонтанной экстремальности.

Противоречия и проблемы, с которыми сталкиваются молодые люди в процессе взросления, требуют от них не только большого внутреннего напряжения, но и рискованных действий по их преодолению, что не всегда возможно в институционально одобряемых формах. Сопровождаемые глубокими, не имеющими выхода эмоциональными переживаниями, подпитываемые взаимодействием с радикально настроенным окружением, такие противоречия становятся глубинной предпосылкой не только радикальных настроений молодежи, но и соответствующих действий. Так, присущие молодежи экстремальность и неформальная самоорганизация приобретают экстремистские формы в пространстве ее социальных взаимодействий, прежде всего, младших молодежных группах – подростковых и юношеских [12]. При этом сами радикальные проявления могут быть как групповыми, так и индивидуальными, проявляться в форме настроения или действия. Все это делает молодежь одним из главных эмпирических объектов в исследованиях радикализации.

Распространение онлайн-коммуникаций существенно изменило способы вовлечения молодежи в процесс пропаганды и усвоения радикальных идей. Погружение в цифровую среду стало одновременно и триггером радикализации, и средством ее манифестации. Молниеносно распространяемые призывы, лозунги, взгляды, быстрый поиск единомышленников, неограниченная эмансипация и свобода самовыражения, возможность публичного заявления о себе и достижение быстрой «славы» сделали цифровое пространство основным элементом сложного механизма радикализации и, как следствие, предметом междисциплинарных исследований.

По типу решаемых задач современные российские и зарубежные исследования так называемой онлайн-радикализации можно разделить на три направления: (1) обнаружение целевых сообществ, противоправного и деструктивного контента, в том числе fake news, языка вражды и контента, распространяемого экстремистскими и террористическими организациями [50; 11; 32; 24; 44; 14; 48; 45; 51]; (2) анализ и интерпретация данных социальных медиа: статистический анализ распространения деструктивного контента; анализ сетевой топологии с целью поиска наиболее влиятельных узлов сети, моделирование процесса влияния информационных сообщений в социальных медиа [32; 42; 41; 71; 1; 52; 63; 55; 10; 30]; (3) формирование баз данных и знаний, описывающих ключевые маркеры деструктивного контента и сообществ; формализация механизмов радикализации, позволяющая перейти к этапу алгоритмизации решения отдельных задач противодействия распространению деструктивного контента и изучения радикализации в цифровой среде [8; 2; 24; 14; 63; 30; 20; 36; 46; 62; 17]. Прикладное значение исследования процесса онлайн-ради-

кализации связано с решением практических задач: разработки механизмов социального регулирования информационно-психологического воздействия на молодежь в интернете; пресечения деструктивного влияния внешних акторов на разные группы молодежи; недопущения вовлечения молодых в террористическую деятельность.

Широкие возможности изучения цифрового пространства открылись перед учеными в связи с использованием методологического аппарата Data Science как набора технологий и методов получения разнообразных данных для решения, как научных, так и практических задач. Так называемая вычислительная социальная наука (Computational social science), представляющая собой соединение методологий социальных и вычислительных наук с применением всего многообразия доступных информационных технологий и изобретательностью ученых в области Data Science [57], способна служить решению многих социологических задач. Ее преимущество определяется тем, что в короткие сроки и на большом объеме данных применение методов интеллектуального анализа данных социальных медиа позволяет проводить аналитические операции с объектами сетевой природы и моделировать процессы. Это соединение матаппарата, методов и технологий Data Science в предметной области для превращения извлекаемых данных в знания [3].

Анализ современного состояния исследований позволил сформулировать проблему, решение которой является ключом к повышению точности полученных результатов изучения предметной области. Методическая проблема заключается в том, что с одной стороны, имеется действительно экстраординарное количество информации и соответствующие инструменты ее извлечения, но, с другой стороны, данных может быть все еще недостаточно для целей каждого отдельно взятого исследования. Соответственно, во-первых, в каждом конкретном случае, необходимо знать и учитывать возможности и ограничения применения технологий и методов Data Science, во-вторых, результаты, полученные на основе открытых данных социальных медиа, могут быть использованы только как дополнительный источник данных для понимания исследуемых процессов в цифровом пространстве социальных медиа.

Целью этой статьи является представление ключевых подходов к пониманию и исследованию радикализации, а также возможностей и ограничений применения методов *tf-idf*, *doc2vec* для моделирования сетевой топологии и оценки контентного сходства онлайн-сообществ без признаков радикализации и онлайн-сообществ с признаками радикализации.

Радикализация как социальный феномен и объект исследования

Радикализация – социальный феномен, изучаемый в контексте исследования терроризма и насильственного экстремизма. С того момента, когда накопленный, начиная с 1970 года, «специализированный набор данных по конкретным подгруппам дел о терроризме» позволил представить

достаточные доказательства принципиальной невозможности создания универсального профиля террориста, экстремиста, исследовательские усилия были направлены на поиск предикторов совершенных преступлений [23; 19; 42]. Исследователи акцентировали внимание на том, что предиктором участия в насильственной деятельности является радикализация, и ее изучение имеет критически важное значение для понимания источников экстремистских и террористических действий [47; 61, с. 39–98; 17; 18; 52].

С течением времени в научно-исследовательском поле сложилось два противоположных подхода: релятивистский (отрицающий идею о том, что радикализация вызывает терроризм)¹ и контекстуальный или мета-подход (радикализацию необходимо изучать в широком контексте, не ограничиваясь только изучением насильственного экстремизма и терроризма) [46; 49; 27, с. 1–36], но поиск консенсуса в определении самого термина радикализация еще не завершен. Как следствие, на сегодняшний день, этот термин не имеет согласованного определения и не укладывается в рамках какой-либо одной академической дисциплины. Созданию общепринятой теории радикализации препятствует многогранность и сложность этого процесса и обилие монокаузальных объяснений. При этом консенсус сложился в отношении важности междисциплинарного подхода к изучению этого сложного феномена, что открывает возможность создания более обстоятельной объяснительной концепции.

Все многообразие толкований привело к тому, что радикализация определяется и как «процесс вовлечения или участия в экстремистских действиях» [17], и как процесс формирования экстремальных убеждений [37], и как процесс эскалации, ведущий по пути от первоначально ненасильственных установок к насильственным действиям, когда происходит «трансформация в убеждениях, установках, поведении и поворот в сторону экстремизма, жаждущего насилия и самопожертвования» [46], и как постепенное принятие экстремальных убеждений, ведущее к сути того, что именуется радикализацией – «террористического поведения как конечной точки» на этом «пути» [66] или объединение двух составляющих, при котором радикализация трактуется как «процесс, в ходе которого отдельные люди или группы становятся идеологически приверженными насилию, т. е. начинают исповедовать систему убеждений, которая узаконивает или даже требует насильственных действий против оппонента» [60].

Некоторые исследователи полагают, что пути к экстремизму и следующему за ним насилию настолько индивидуальны, что поиск причинных факторов радикализации если не контрпродуктивен, то, по крайней мере, является пустой тратой времени. Другие утверждают, что индивидуального в радикализации мало, а вовлечение в процесс происходит благодаря различного рода социальным связям. Они определяют социокультурные

¹ Horgan, J. (2013) Everything You've Been Told About Radicalization Is Wrong. Rolling Stone. URL: <https://www.rollingstone.com/politics/politics-news/everything-youve-been-told-about-radicalization-is-wrong-80445/>; Sageman, M. (2013) Woolwich Attack: Overreacting To Extremism 'Could Bring Back Al Qaeda' Ex CIA Officer Warns. Huffington Post. URL: https://www.huffingtonpost.co.uk/2013/05/27/sageman-interview_n_3342206.html (дата обращения: 20.09.2023).

особенности среды общения, выступающей значимым фактором формирования экстремального типа сознания. Для молодежи таковыми являются связи, устанавливающиеся в рамках различных молодежных сообществ. Как показывали исследования, практически во всех типах таких сообществ обнаруживается определенная доля радикальности во взглядах, воззрениях и декларируемых установках. Само включение в групповые взаимодействия и эффект эмоционального заражения, присущий молодежным сообществам, повышает вероятность радикализации настроений и проявлений, реализация которых может быть, как групповой, так и индивидуальной. Неоднозначность определений, лежащих в основе понятия «радикализация», породило другую проблему. С одной стороны, исследования позволили выйти на новый уровень в изучении радикализации как предиктора терроризма, с другой – наряду с достижениями исследования изобилуют двусмысленностью определений и отсутствием понимания причинно-следственных связей. Ощущается дефицит объяснения условий и механизмов формирования и протекания этого процесса.

Разнообразие определений на этом фоне представляется менее проблематичным, чем тот факт, что совершенно разные толкования смешиваются в научных исследованиях и перетекают в публичный дискурс и политические дискуссии. А разногласия, по существу, заключаются в том, на что именно сделан акцент.

Понятие «онлайн-радикализация» еще более расплывчато, чем понятие «радикализация», и общепринятого, согласованного определения также не существует. Между тем, есть консенсус в отношении того, что сам этот процесс приобретает массовый, вирусный, масштабируемый характер в результате применения новых коммуникативных технологий. И хотя утверждение о том, что Интернет никого ни к чему не принуждает и не заставляет принимать крайние взгляды и убеждения используется как основной аргумент против его демонизации, некоторые технологические возможности могут способствовать определенному сдвигу в сторону радикальных убеждений. То есть, интернет является не причиной, а инструментом, позволяющим радикализировать в короткие сроки пользователей социальных медиа на индивидуальном, групповом, массовом уровне.

Из имеющегося многообразия определений акцентируем внимание на консенсусе в интерпретации онлайн-радикализации, которая рассматривается «как процесс, в ходе которого люди подвергаются влиянию экстремистских убеждений и взглядов, имитируют и усваивают их посредством Интернета, в частности социальных сетей, и других форм онлайн-коммуникации» [16]. Такие аспекты социальных медиа как способность адаптировать контент к конкретным ценностям и интересам пользователей, а также включение их в сети единомышленников – являются ключевым активом групп выраженной экстремистской направленности. Как в физическом, так и в виртуальном мире, такие группы в значительной степени полагаются на изоляцию потенциальных новобранцев от альтернативных взглядов и мнений. Использование Интернета ультрарадикальными сообществами быстро развивается и эффективно адаптируется к постоянно меняющейся онлайн среде. Продолжительность процесса радикализации

сокращается в результате использования технологических возможностей Интернета¹, а потому радикализация в пространстве интернет-коммуникаций квалифицируется как осязаемая угроза [62]. Учитывая общий рост онлайн-влияния как основную движущую силу распространения и принятия экстремистских идеологий, основанных на базовых элементах радикализации (формирование индивидуального/коллективного недовольства, формирование идеологической «дорожной карты», мобилизация ресурсов) актуализируется направление исследований, фокус которых сосредоточен на изучении механизмов онлайн-радикализации и последующего совершения актов насилия в оффлайн пространстве.

Однако в настоящее время исследователи все чаще ставят под сомнение автономность понятия онлайн-радикализация, поскольку онлайн и оффлайн пространства онтологически неразделимы. Такая «дихотомия представляется неоправданной, поскольку приводит к сужению понимания роли коммуникационных технологий в процессе радикализации» [68; 26; 64]. Появилось направление исследований, согласно которому радикализация понимается как процесс, который разворачивается в онлайн и оффлайн одновременно, т. е. в гибридном онлайн-пространстве [64]. Приверженцы этого подхода используют меткое выражение “Onlife” [29], придуманное философом Лучано Флориди и его производную “Onlife Spaces” [64].

Разделяя эту точку зрения, сформулируем свою интерпретацию понятия «онлайн-радикализация», как (1) стохастического процесса, который влечет за собой (2) вовлечение в экстремистскую систему убеждений, которая готовит почву для (3) совершения актов насилия в оффлайне. Стохастичность процесса обусловлена характеристиками нелинейности случайных социальных процессов, которые увеличивают неопределенность и вариативность аттрактивных состояний субъектов при прохождении «пути» радикализации. Кроме того, «путь радикализации» вариативен. Вовлечение в воронку экстремистских убеждений мы рассматриваем как процесс формирования смыслов (устойчивых фреймов, радикальных нарративов, эмоциональных паттернов), в которых созревает, вырабатывается, развивается идея применения насилия как единственно возможного способа достижения любых целей (идеологических, политических, религиозных, террористических, личных и др.). Ключевая часть этого процесса – технологические возможности Интернета (рекомендательные алгоритмы, замыкающие пользователей в эхо-камеры, образующие «filter bubble», сетевые эффекты, и др.). Переход к совершению насилия в оффлайне мы склонны рассматривать как процесс «морального отстранения» («нормализации»), при котором «моральный компас» перестает функционировать. Моральный компас действует как механизм саморегуляции на двух уровнях: (1) ориентирует индивидов и группы на гуманное отношение к дру-

¹ Jensen, M., James, P., LaFree, G., Safer-Lichtenstein, A., and Yates, E. (2018). Research Brief. The use of social media by United States extremists. National Consortium for the Study of Terrorism and Responses to Terrorism (START). URL: https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf (дата обращения: 15.12.2023).

гим, и (2) предписывает воздерживаться от проявлений бесчеловечного поведения. В результате нарушения внутренних моральных норм в действие вступает механизм морального размежевания для самооправдания насильственных действий. Фактически «моральное отстранение» – это постепенное принятие бесчеловечного, преступного, нецивилизованного поведения, приводящего в конечном счете, к совершению насильственных действий для достижения цели. При этом мы исходим из того, что эта цель не обязательно должна иметь какое-то политическое или религиозное основание, она может быть и вполне частной, корыстной. Допустимость насилия – это основной критерий радикализации. Изучение процесса радикализации в таком контексте требует постановки множества исследовательских задач, для решения которых необходимо расширение методов и инструментов поиска, обработки и анализа данных социальных сетей.

Но, как уже отмечалось, проблема смыслового наполнения категорий, которыми оперируют исследователи, нагружается острой общественной потребностью в ранней диагностике предикторов и предрасположенностей к радикальным действиям, а также высоким алармистским напряжением в общественном дискурсе. Стремление обрести универсальный инструмент – своего рода «серебряную пулю» – с помощью которого общество предотвратит радикальные проявления, с особой надеждой разворачивает исследовательскую оптику в сторону Data Science.

Реагируя на актуальный запрос, исследователи активно применяют эти методы, накапливая соответствующий опыт. В представленной работе мы сосредоточились на постановке исследовательской задачи, которая представляется главной: как по тематическому контенту выявить среди не радикальных онлайн-сообществ те из них, в которых существует риск радикализации и есть признаки, по которым с течением времени можно ожидать тенденции, если не к объединению, то к установлению связей с радикальными сообществами. Решение поставленной задачи расширяет возможности обнаружения и прогнозирования разных путей радикализации в Интернете, условно говоря «тропы радикализации» в контексте взаимодействия и прогнозирования новых связей онлайн-сообществ на основе тематической повестки. Однако увлечение этими методами требует осмысленности и осторожности в силу особой чувствительности самого предмета.

Технологии и методы Data Science в изучении онлайн-радикализации

Автоматизация исследований онлайн-радикализации относится к числу актуальных задач современной социологии, социальной психологии [28; 33; 31; 58]. Интерес исследователей к интеллектуальному анализу деструктивного контента социальных медиа, включая задачи сбора, обработки и интерпретации содержания интернет-ресурсов с целью прогнозирования процесса радикализации, предупреждения инцидентов экстремистской и террористической направленности устойчиво растет

[62; 65; 44; 67; 64; 13; 54; 56]. Вместе с тем, ученые находятся на этапе осознания и новых возможностей, и ограничений названных методов. С одной стороны, доступность Интернет-данных, в том числе данных социальных сетей, предоставляет уникальные возможности с точки зрения полноты охвата исследуемых явлений и процессов. Невозможно не принимать во внимание колоссальный объем доступной для анализа информации, которую предоставляют социальные сети. С другой стороны, нельзя полагаться только на них, как на источник первичных данных. Несмотря на возросшую доступность инструментов Data Science, эффективность их использования зависит в равной степени как от соответствующих навыков, так и от компетентности в прикладной предметной области. Критическую значимость в оценке надежности данных подчеркивают и сами исследователи: «качество данных есть и всегда будет в центре внимания исследователей в индустрии аналитики. Как в сегодняшних постоянно меняющихся условиях можно быть уверенным в надежности ваших данных?»¹.

Существенные ограничения интеллектуального анализа данных, которые необходимо учитывать при планировании и организации исследований, базирующихся на данных социальных сетей, мы выделяем по следующим критериям: (1) парадокс больших данных (Big Data Paradox), несмотря на значительный объем доступных для анализа данных, для конкретной прикладной задачи данных может все еще быть недостаточно; (2) проблема доступа к данным (Obtaining Sufficient Samples), доступ к данным социальных медиа через программные интерфейсы приложений (API) имеет ограничения по объему и доступности значений отдельных полей, что усугубляет проблемы, связанные с репрезентативностью; (3) удаление шума (Noise Removal Fallacy) актуализирует задачу его автоматического выявления для повышения эффективности процесса анализа и интерпретации результатов; (4) дилемма оценки (Evaluation Dilemma), при наличии в качестве исходных данных только общедоступной информации социальных медиа проверка достоверности невозможно; (5) гетерогенность (Heterogeneity), наличие разнородных анализируемых объектов и процессов в рамках сети, которые при этом на уровне доступных данных проявляются схожим образом или полностью идентичны; (6) эволюция сети (Evolution), состояние анализируемой сети меняется в режиме реального времени – требуются ресурсоемкие механизмы фиксации состояния сети и оценки разницы состояний; (7) коллективные взаимодействия (Collective Intelligence), наличие общедоступных наблюдаемых реакций на размещенный контент (комментарии, рейтинги, теги, лайки и т. д.) может в том числе оказывать влияние на пользователей, не оставляя фактических следов этого процесса [70; 59; 56; 65; 22].

Еще совсем недавно исследователи начали применять методы интеллектуального анализа данных в предметной области исследований онлайн-радикализации, цифровые следы в социальных сетях в качестве признаков

¹ Lisa Wilding-Brown. Chief Executive Officer // InnovateMR. Business & Innovation GRIT Report. 2022. URL: <https://www.greenbook.org/mr/grit/business-innovation-edition/> (дата обращения: 20.09.2023).

для обнаружения и прогнозирования радикально настроенных пользователей. Настоящим прорывом можно назвать топологическое моделирование трудноформализуемых объектов, каковым является феномен радикализации, с применением наряду с Web Mining и AI, методов и технологий сетевой топологии [11; 21; 25; 22]. Прикладная значимость моделирования сетевой топологии заключается в том, что это позволяет отразить степень близости, влияния, посредничества между топосами (общие темы, повестка и др.) и установить связанность сетевых акторов в процессе радикализации.

Методы и материалы

Методология данного исследования выстроена на основе применения двух групп методов, с доказанной эффективностью применения в исследованиях онлайн-радикализации:

1. Векторизация текстов [34; 48; 45; 63; 69; 38]. Целью данной группы методов является трансформация неструктурированной или слабоструктурированной текстовой информации в числовую, пригодную для сравнения, форму. За счет этого решаются задачи оценки «сходства» текстов и обсуждаемых тем, а также поиска значимых для отдельных идеологических платформ терминов и именованных объектов. Наиболее часто используемой является статистическая мера значимости слов *tf-idf*, к преимуществам которой можно отнести простоту и понятность реализации, а также высокую интерпретируемость получаемых результатов. К прочим применяемым методам этой группы относятся *word2vec* и *bag of words*. К основным сопутствующим сложностям относятся вопросы формирования выборок текстов для анализа, и в случае применения машинного обучения – обучающих и тестовых выборок.

2. Применение специализированных словарей. Несмотря на хорошо известные недостатки использования ключевых слов и словосочетаний в задачах прямого поиска целевого контента, а именно – большая размерность поисковой выдачи, а также высокая доля ложных и случайных результатов, потенциально эффективным является использование специализированных словарей особенно в сочетании с другими методами [55; 14; 15; 35; 30; 71]. Под словарями мы понимаем упорядоченные и формализованные знания относительно значимости для отдельных идеологических платформ и сообществ: а) ключевых слов, характеризующих именованные объекты: места, персоналии, события и даты; б) терминов, включая жаргонизмы и сленг; в) тегов, явно маркирующих сообщение как целевое. При этом, можно выделить два основных подхода к составлению словарей: экспертный и *wisdom of the crowds* (мудрость толпы). Экспертный способ не требует детальной характеристики. Словарь в этом случае является результатом работы одного или нескольких экспертов, специализирующихся на определенной предметной области. Эффективное использование экспертного словаря требует наличия четких правил и инструментария для его первичного составления, оценки качества и изменения содержимого.

Подход *wisdom of the crowds* основывается на допущении «большинство не может ошибаться». В практическом смысле подход выражается в анализе множества сообщений, маркированных пользовательскими тегами. Таким образом, обладая знанием о целевых и значимых тегах, можно не только статистически оценивать распространение контента и реакцию на него, но и составлять обучающие и тестовые выборки данных. В последнем случае, сопутствующими задачами будут определение репрезентативности выборки и оценка ошибки разметки выборки.

Метод векторизации текстов ранее уже был успешно апробирован в наших исследованиях оценки взаимосвязей сообществ социально активных отцов, аффилированных с организациями «Союз Отцов» и «Совет отцов», и сообществ с признаками радикализации, относящихся к различным идеологическим платформам, на открытых данных социальной сети «ВКонтакте»¹ [7; 6; 9]. Применение специализированных словарей также уже было успешно апробировано в наших исследованиях ультраправой радикализации [40; 39].

Распространенная практика в российских исследованиях онлайн-радикализации сводится к решению задачи выявления взаимосвязей отдельных онлайн-сообществ или их кластеров на оценке степени их сходства по подписчикам, либо по лингвистическим маркерам. Такой подход ограничен в прогнозировании новых связей между сообществами, фактически «путей» радикализации.

В представленной работе мы сосредоточились на совмещении двух групп методов. Это позволит проверить, насколько эффективно будет такое применение для изучения неявных, скрытых связей между онлайн-сообществами без признаков радикализации и онлайн-сообществами с признаками радикализации. Результаты представлены в виде социальных графов, сформированных по принципам общности подписчиков, сходства значимых слов, контекстного сходства на базе *doc2vec* модели.

Характеристика выборки анализируемых данных

Для моделирования сетевой топологии отобраны 160 онлайн-сообществ социальной сети ВКонтакте без признаков радикализации, условно разделяемые на три класса:

1. Сообщества лидеров мнений.
2. Сообщества волонтерских организаций.
3. Фанатские сообщества, включая фанатов популярной культуры (видеоигры, музыка, художественные и анимационные фильмы), спортивных команд и мероприятий.

¹ Ильдарханова Ч. И., Савельев А. О., Вильнин А. Д. [и др.]. Социологическое исследование «Сетевые взаимодействия социально активных отцов: норма и отклонение (анализ социальных сетей профильных НКО)»: Свидетельство о государственной регистрации базы данных № 2021621866 Российская Федерация. Заявка № 2021621733 от 24.08.2021, опублик. 03.09.2021 (дата обращения: 20.09.2023).

Общая численность не уникальных подписчиков онлайн-сообществ по всей выборке составила 16 698 375 учетных записей¹.

Сообщества лидеров мнений отбирались согласно рейтингу наиболее популярных блогеров, сформированному ВКонтакте на дату начала исследования.

Сообщества волонтеров и фанатов были отобраны экспертным образом из поисковых результатов ВКонтакте. При этом приоритетом для включения в итоговый список для анализа обладали сообщества с наибольшим количеством подписчиков при наличии актуальных на дату начала отбора публикаций и комментариев.

Возрастной диапазон подписчиков, указавших свой возраст, преимущественно составляет от 15 до 35 лет. В отдельных случаях он выходит за пределы молодежного возраста, превышая его верхнюю планку. Отметим, что возраст указывается подписчиками по их усмотрению и не является обязательным при регистрации. В равной мере он может быть вообще проигнорирован, или сфальсифицирован. По всей выборке анализируемых сообществ возраст не указан у 63% подписчиков, по классу «лидеры мнений» – у 55%, в сообществе «волонтеров» – у 65%, «фанатов» – у 63%.

Среднее количество ежедневно публикуемых сообщений в онлайн-сообществах распределено следующим образом: «лидеры мнений» – 2,69; «волонтеры» – 5,94; «фанаты» – 2,17. Подробные данные о каждом проанализированном сообществе представлены в Базе Данных [2].

Для каждого из сообществ был выявлен перечень из 29 наиболее значимых слов. Значимые слова определены на основе статистической меры *tf-idf*. Мера значимости слова («вес») пропорциональна частоте его употребления в корпусе текстов отдельного онлайн-сообщества и обратно пропорциональна частоте его употребления в корпусе русскоязычных текстов, включающем художественные произведения, новостные сообщения, открытые публикации в социальных медиа. Поиск и объединение слов-синонимов не выполнялись.

Результаты выявления значимых слов сгруппированы по классам рассматриваемых онлайн-сообществ и представлены в виде «облака слов» на рисунках 1–3 по классам «лидеры мнений», «волонтеры» и «фанаты» соответственно. Наиболее частые значимые слова по каждому из классов начертаны шрифтом большего размера и помещены ближе к центру.

Отметим, что подобный метод выявления значимых слов чрезвычайно чувствителен к исходным данным. На примере рисунка 6 видно, что значительную часть дискурса в сообществах «волонтеров» составляли обсуждения, связанные с объявлением «года волонтера». В смысловом поле дискурса фанатов предсказуемо расположились сюжеты, связанные с командами и проходящими состязаниями. А в среде лидеров мнений обсуждение строится вокруг масштаба и значимости их влияния. Как видно, ни одно из трех сообществ никак не демонстрирует признаков радикализации. Рассмотрим их более подробно в контексте взаимосвязей.

¹ *Примечание авторов:* это часть данных исследования [2].



Рис. 1. Облако значимых слов онлайн-сообществ «лидеры мнений»
Figure 1. Meaningful word cloud of online communities "opinion leaders"



Рис. 2. Облако значимых слов онлайн-сообществ «волонтеры»
Figure 2. Meaningful word cloud of online communities "volunteers"



Рис. 3. Облако значимых слов онлайн-сообществ «фанаты»
 Figure 3. Meaningful word cloud of online communities “fans”

Топологический анализ сетевых сообществ

Для оценки наличия взаимосвязей рассматриваемых не радикальных онлайн-сообществ и онлайн-сообществ с признаками радикализации были сформированы соответствующие социальные графы. Перечень онлайн-сообществ с признаками радикализации сформирован в рамках ранее выполненных исследований [4] и включает 259 активных на момент проведения исследования онлайн-сообществ.

Социальные графы построены по принципу общности подписчиков, сходства значимых слов по *tf-idf*, контекстного сходства на базе *doc2vec* модели [5], оценивающей каждое слово по окружающим его словам.

На рисунках 4-6 представлены фрагменты графов «общие подписчики», «значимые слова», «контекстное сходство». Черным цветом обозначены онлайн-сообщества с признаками радикализации, желтым – сообщества «лидеры мнений», синим – «волонтеры», красным – «фанаты», зеленым – нейтральные сообщества различной тематической направленности (новостные, сообщества организаций, региональные).

Граф «общие подписчики» в основной своей части демонстрирует однородные, плотные, малосвязанные друг с другом кластеры онлайн-сообществ. Оценить степень влияния радикальных сообществ на не радикальные на основе данных только об общих подписчиках без дополнительного анализа размещаемого контента не представляется возможным.

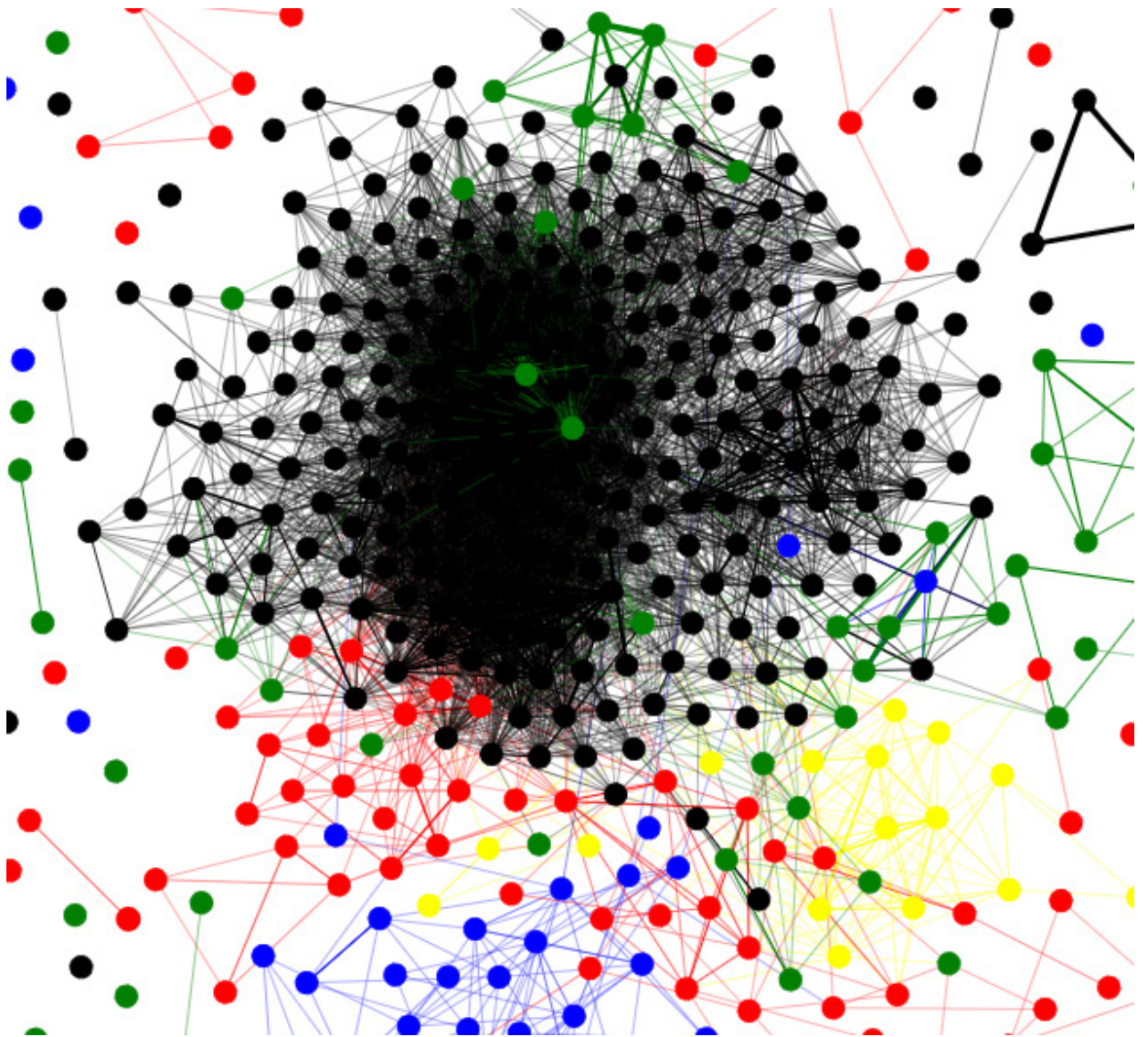


Рис. 4. Фрагмент социального графа онлайн-сообществ «общие подписчики»
Figure 4. Fragment of the social graph of online communities "total subscribers"

Для построения графа «значимые слова» текстовое содержание каждого из рассмотренных онлайн-сообществ было векторизовано с целью количественной оценки сходства между текстами, циркулирующими в разных сообществах (рис. 6). Парно было рассчитано косинусное расстояние между полученными векторами онлайн-сообществ. Расстояние находится в пределах от 0 до 1, где 1 означает абсолютное совпадение векторов. Граф, представленный на рисунке 6, получен путем отрисовки ребер между узлами-сообществами, если косинусное расстояние между ними больше или равно 0,6. Анализ графа показывает наличие устойчивых связей отдельных онлайн-сообществ «лидеров мнений», «волонтеров» и «фанатов» с онлайн-сообществами,

имеющими признаки радикализации. С учетом особенностей описанной методики выявления значимых слов полученные данные можно интерпретировать как наличие пересекающейся повестки. При этом следует учесть, что сходство между узлами и наличие соответствующих связей может быть результатом одной из трех «сил» различной природы, описываемых в сетевом анализе: влияния (связанные узлы с течением времени становятся схожи), гомофилии (похожие узлы со временем устанавливают связи) и внешнего воздействия (например, общественно значимое событие является причиной временного совпадения тематической повестки узлов вне зависимости от наличия связей между ними). Эти «силы» определяют значение ассортативности сети – меры, отражающей тенденцию схожих узлов к объединению.

Принцип построения графа «контекстное сходство» аналогичен способу построения предыдущего графа за исключением использованного метода для векторизации текстового контента сообществ – doc2vec. В общем виде, doc2vec оценивает сходство между словами по окружающему их контексту. То есть, слова считаются «схожими», если их окружают одни и те же слова. Косинусное расстояние повторно использовано для оценки степени сходства онлайн-сообществ. Между узлами отрисована грань, если косинусное расстояние равно или превышает 0,6. Полученный таким образом граф (рис. 6) демонстрирует наличие явно выраженных тематических кластеров сообществ. Экспертиза результатов показала, что doc2vec позволяет выявлять наличие устойчивых, легко интерпретируемых связей между онлайн-сообществами, основанных на общих смыслах и тематических нарративах. Например, кластер А целиком состоит из онлайн сообществ волонтеров-зоозащитников, включая сообщества приютов для животных. Кластер Б состоит из сообществ волонтеров медиков и региональных сообществ волонтеров. Кластер В включает исключительно сообщества футбольных фанатов, а кластер Г – музыкальных фанатов направления «k-POP». Это означает, что внутри названных кластеров контент не только однороден, но и полностью соответствует тематике этих сообществ.

Наиболее разнородным оказался кластер Д, объединивший сообщества спортивных фанатов, АнтиФа, Alt-Right и националистические онлайн-сообщества. Попадание сюда же представителей нейтральных сообществ (цвет: зеленый) может быть результатом ошибки в работе метода doc2vec из-за малого количества представленного в них текстового контента.

Использование doc2vec как способа оценки сходства онлайн-сообществ показало наиболее релевантные задачам исследования результаты. Так, с помощью этого метода из неупорядоченного множества связей можно выделить тематические кластеры, раскрыть которые не удастся на основании данных об общих подписчиках. Причина в том, что разные сообщества могут иметь одинаковых подписчиков. Так, на социальном графе проявилось вкрапление нейтральных сообществ в «гнездо» радикальных, а радикальных – в сеть тематических, не радикальных (лидеров мнений, волонтеров, фанатов) (рис.4). Поэтому метод анализа сообществ по подписчикам не может быть признан валидным для практического применения в исследованиях онлайн радикализации, исключая частные случаи задач моделирования информационной диффузии.

Dos2vec также может быть применим для автоматизированной классификации онлайн-сообществ. Однако из-за нейросетевой природы метода и необходимости обучения модели на исходном корпусе текстов, данный подход является наиболее ресурсоемким с точки зрения вычислительных мощностей. Сложность экспоненциально возрастает по мере включения в выборку новых онлайн-сообществ.

Также следует учитывать, что наличие связей между онлайн-сообществами, выявленными на основе «значимых слов» и «контекстного сходства», следует интерпретировать именно как сходство, а в отдельных случаях как значительную общность дискурса, но не как фактическое взаимопроникновение на уровне активности отдельных пользователей. Однако, общность дискурса, в свою очередь, практически может послужить основой «проникновения» радикальных нарративов.

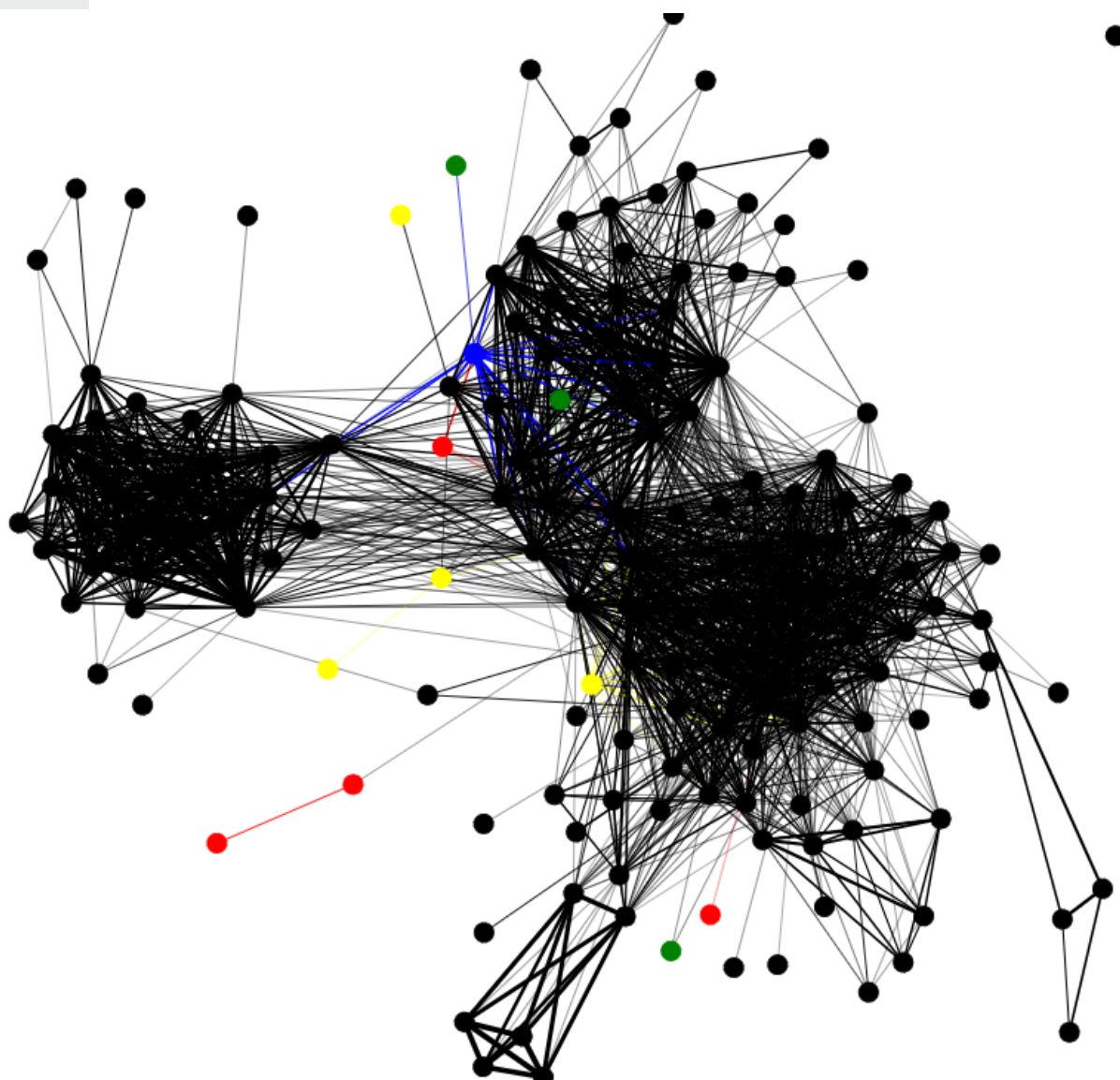


Рис. 5. Фрагмент социального графа онлайн-сообществ «значимые слова»
Figure 5. Fragment of the social graph of online communities “meaningful words”

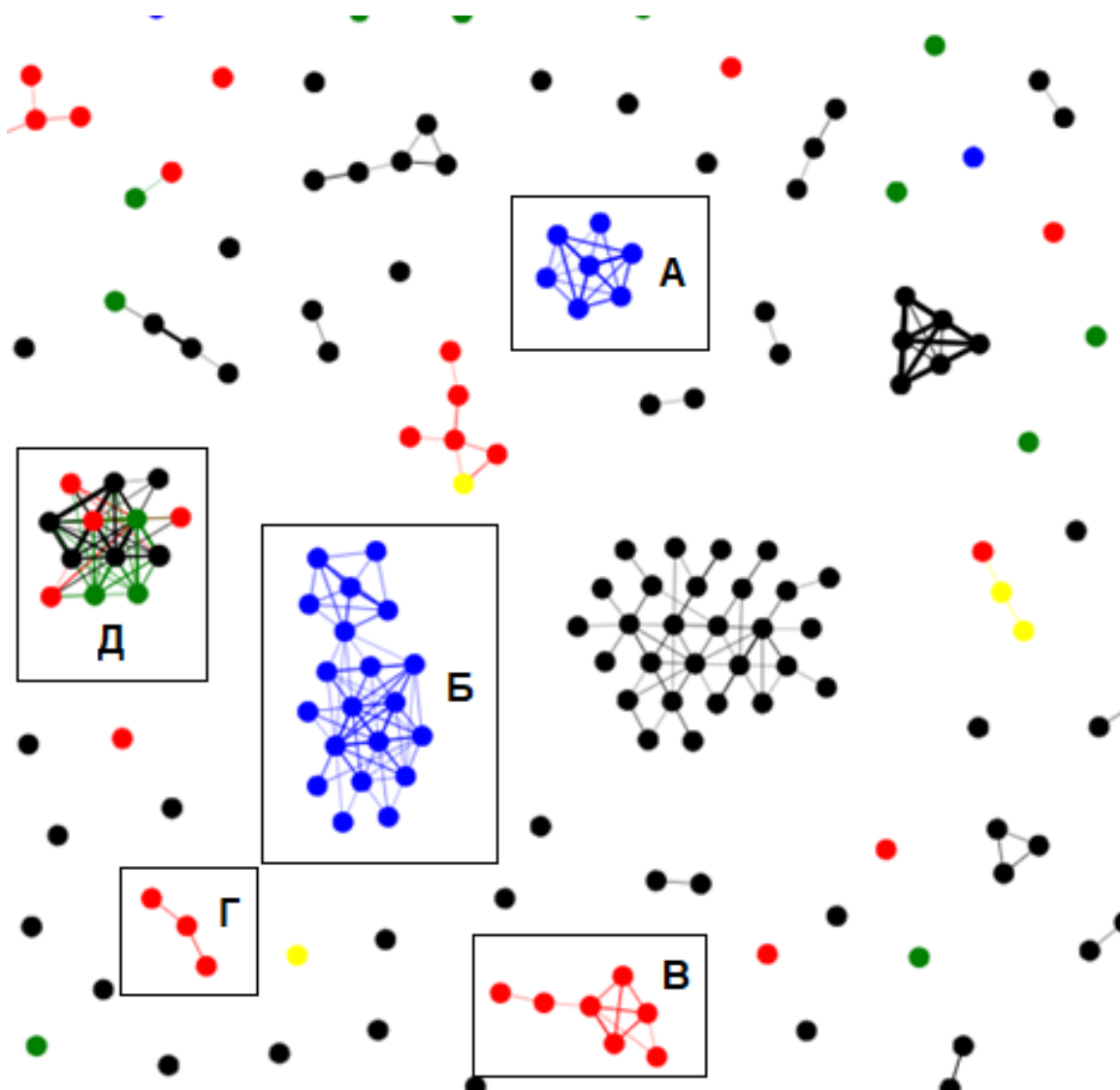


Рис. 6. Фрагмент социального графа онлайн-сообществ «контекстное сходство»
 Figure 6. Fragment of the social graph of online communities "contextual similarity"

На возможность использования результатов анализа социальных сетей в разработке профилактических мероприятий и выработке мер противодействия радикализации молодежи значительным образом влияет уже упомянутый «парадокс больших данных». Он заключается в том, что, с одной стороны, имеется действительно экстраординарное количество информации и соответствующие инструменты ее извлечения, но, с другой стороны, данных может быть все еще недостаточно для целей каждого отдельно взятого исследования. Особенно сильно это сказывается при переходе на уровень «социального атома» – отдельной учетной записи, которая может не содержать никаких данных, характеризующих пользователя. Более того, отсутствует гарантия того, что и указанные данные достоверны.

Таким образом, результаты любых исследований, базирующихся на анализе данных множества учетных записей и не содержащие никаких количественных или качественных оценок точности полученных результатов и доказательств репрезентативности выборки, следует подвергать сомнению.

В то же время, рассмотрение в качестве базовой единицы анализа онлайн-сообществ, а не отдельных пользователей, позволяет судить о неявных, но возможных связях в рамках отдельно взятых сообществ как микро-социумов, сформировавшихся на базе общности интересов молодежи. Оценить же в точности каждую наметившуюся связь не представляется возможным. Следовательно, результаты, полученные только на основе открытых данных социальных медиа, могут быть использованы в качестве одного из возможных источников информации для понимания процесса радикализации в молодежной среде.

Заключение

Итак, результаты проведенного исследования позволяют оценить преимущество методов *tf-idf* и *doc2vec* для моделирования сетевой топологии и оценки контентного сходства различных онлайн-сообществ – имеющих признаки радикализации и не имеющих таковых. Во-первых, результаты, полученные с помощью этих методов, способствуют более глубокому осмыслению невыраженных связей между сообществами и оценке сходства/различия внутри и между кластерами онлайн сообществ. Используемые методы открывают перспективы для изучения природы ассортативности в наблюдаемой сети и выработки соответствующих регулятивных мер. При этом меры противодействия деструктивному воздействию на молодежь, включенную в онлайн сообщества, должны разрабатываться в зависимости от причин, обусловивших ассортативность.

Во-вторых, сделать более обоснованный вывод о наличии связей между сообществами. Если анализ по подписчикам и ключевым словам дает картину сетевой топологии с наличием прямых связей между радикальными и не радикальными сообществами, рисуя весьма поверхностную картину тотальной радикализации рассматриваемых онлайн сообществ, тем самым упрощая и искажая реальность, то совмещение методов *tf-idf* и *doc2vec* позволяет этого избежать. В результате оценки контентного сходства, произведенного на основе метода *doc2vec* представление о связях внутри/между сообществами становится более близкими к реальности.

Для принятия адекватных управленческих решений в равной мере важно выявление латентных признаков радикализации, но также и понимание отсутствия этих признаков там, где их, действительно, нет. Поэтому в изучении такой социально чувствительной проблемы как радикализация важно учитывать валидность инструментария. Это повысит обоснованность как научных выводов, так и практических мер.

Отмечая необходимость сочетания методов исследования, обратим внимание еще на один метод – структурно-таксономического моделирования, который позволяет анализировать механизмы регулирования тех или иных процессов путем выявления латентных связей между ними. С его помощью становится возможным моделирование смыслового пространства

реальности молодежи, в том числе выявление места радикальных смысловых установок в более широком контексте саморегуляции жизнедеятельности молодежи.

Разделяя идею перспективности применения Data Science, необходимо подчеркнуть, что критически важным элементом работы с ее технологиями, методами и инструментами является понимание не только открывающихся возможностей, но и существенных ограничений. Абсолютизация данных, полученных на основе анализа социальных сетей, способна привести к ошибкам как в социальной диагностике, так и в принятии управленческих решений. В силу самой природы онлайн-радикализации выработка профилактических мер противодействия этому процессу должна опираться на понимание особенностей молодежи и природы ее экстремальности, а также всего комплекса предпосылок, запускающих эскалацию процесса радикализации. А это по-прежнему выводит на первый план фигуру исследователя, обладающего фундаментальными знаниями об особенностях молодежи как социально-демографической группы и механизмах, регулирующих взаимодействия молодых людей друг с другом и с обществом.

Библиографический список

1. Ахременко А. С., Стукал Д. К., Петров А. П. Сеть или текст? Факторы распространения протеста в социальных медиа: теория и анализ данных // Полис. Политические исследования. 2020. № 2. С. 73–91. DOI: 10.17976/jpps/2020.02.06; EDN: APZWMB.

2. Карпова А. Ю., Кузнецов С. А. и др. Метод поиска изображений с признаками ультраправой радикализации в социальных медиа на основе нейросетевой классификации // Системы управления и информационные технологии. 2023. № 1(91). С. 59–64. DOI: 10.36622/VSTU.2023.91.1.012; EDN: KGWMLC.

3. Карпова А. Ю., Савельев А. О. Возможности и границы применения технологий Big Data для изучения онлайн-радикализации // Третьи декабрьские социально-политические чтения «Как живешь, Россия?». Вызовы пандемии, парламентские выборы и стратегическая повестка дня для общества и государства: Матер. науч.-практич. конф. М.: ФНИСЦ РАН, 2022. С. 67–78. EDN: ZXFWGV.

4. Карпова А. Ю., Савельев А. О. и др. Ультраправая радикализация: методика автоматизированного выявления угроз методами web mining // Вестник РФФИ. Гуманитарные и общественные науки. 2020. № 5(102). С. 30–43. DOI: 10.22204/2587-8956-2020-102-05-30-43; EDN: BEZTTC.

5. Карпова А. Ю., Савельев А. О. и др. Изучение процесса онлайн-радикализации молодежи в социальных медиа (междисциплинарный подход) // Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 3(157). С. 159–181. DOI: 10.14515/monitoring.2020.3.1585; EDN: CXJJUW.

6. Карпова А. Ю., Савельев А. О., Кузнецов С. А. Трансформация социальных практик ответственного отцовства в девиантные формы социальной активности // Векторы благополучия: экономика и социум. 2021. № 4(43). С. 107–118. DOI: 10.18799/26584956/2021/4(43)/1130; EDN: DDROPU.

7. Карпова А. Ю., Ширыкалов А. М. Разработка метода оценки схожести коллекций текстов с использованием их векторных представлений, полученных методом doc2vec // Молодежь и современные информационные технологии: Сб. тр. XVIII Междунар. науч.-практ. конф. Томск: ТПУ, 2021. С. 75–76. EDN SWSZVQ.

8. Кузнецов С. А., Карпова А. Ю., Савельев А. О. Методы и технологии интеллектуализации поиска деструктивного и радикального контента в социальных медиа: анализ современного состояния // Вестник компьютерных и информационных технологий. 2023. Т. 20. № 4(226). С. 39–48. DOI: 10.14489/vkit.2023.04.pp.039-048; EDN: EVCQQC.

9. Савельев А. О., Карпова А. Ю., Кузнецов С. А. Подход к оценке взаимосвязей сообществ социальных медиа на базе тематического сходства текстового контента (на примере сообществ социально активных отцов и сообществ с признаками радикализации) // Казанский экономический вестник. 2022. № 1(57). С. 96–103. EDN: DNZYVS.

10. Соколова Т. В., Чеповский А. М. Задача анализа профилей пользователей социальных сетей // Ситуационные центры и информационно-аналитические системы класса 4i для задач мониторинга и безопасности (SCVRT2017): Тр. Междунар. науч. конф. Москва–Протвино: ИФТИ, 2017. С. 198–201. EDN: YSHYDJ.

11. Стукал Д. К., Ахременко А. С., Петров А. П. Аффективная политическая поляризация и язык ненависти: созданы друг для друга? // Вестник РУДН. Сер.: Политология. 2022. Т. 24. № 3. С. 480–498. DOI: 10.22363/2313-1438-2022-24-3-480-498; EDN: VLTQRN.

12. Чупров В. И., Зубок Ю. А. Молодежный экстремизм: сущность, формы проявления, тенденции. М.: Academia, 2009. 320 с. EDN: SUFKBZ.

13. Akram M., Nasar A. Systematic Review of Radicalization through Social Media // Ege Academic Review. 2023. Vol. 23(2). P. 279–296. DOI: 10.21121/eab.1166627; EDN: JFWLSR.

14. Alvari H., Sarkar S., Shakarian P. Detection of Violent Extremists in Social Media // 2nd International Conference on Data Intelligence and Security (ICDIS). South Padre Island, TX, USA, 2019. P. 43–47. DOI: 10.1109/ICDIS.2019.00014.

15. Araque O., Iglesias C. A. An Approach for Radicalization Detection Based on Emotion Signals and Semantic Similarity // IEEE Access. 2020. Vol. 8. P. 17877–17891. DOI: 10.1109/access.2020.2967219.

16. Binder J. F., Kenyon J. Terrorism and the internet: How dangerous is online radicalization? // Frontiers in Psychology. 2022. Vol. 13. DOI: 10.3389/fpsyg.2022.997390; EDN: RGSYY.

17. Borum R. Radicalization into Violent Extremism I: A Review of Social Science Theories // *Journal of Strategic Security*. 2012. Vol. 4(4). P. 7–36. DOI: 10.5038/1944-0472.4.4.1.
18. Borum R. Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research // *Journal of Strategic Security*. 2012. Vol. 4(4). P. 37–62. DOI: 10.5038/1944-0472.4.4.
19. Borum R. Rethinking radicalization // *Journal of Strategic Security*. 2012. Vol. 4(4). P. 1–6. URL: <https://digitalcommons.usf.edu/jss/vol4/iss4/1> (дата обращения: 15.12.2023).
20. Borum R. Understanding the terrorist mind-set // *FBI Law Enforcement Bulletin*. 2003. Vol. 72(7). P. 7–10.
21. Clancy T., Addison B., Pavlov O., Saeed Kh. Contingencies of Violent Radicalization: The Terror Contagion Simulation // *Systems*. 2021. Vol. 9(4). Article 90. DOI: 10.3390/systems9040090.
22. Das S., Biswas A. The Ties that matter: From the perspective of Similarity Measure in Online Social Networks // *ArXiv*. 2022. DOI: 10.48550/arXiv.2212.10960.
23. de la Roche R. S. Why is collective violence collective? // *Sociological Theory*. 2001. Vol. 19(2). P. 126–144. DOI: 10.1111/0735-2751.00133.
24. Deem A. The Digital Traces of #whitegenocide and Alt-Right Affective Economies of Transgression // *International Journal of Communication*. 2019. Vol. 13. P. 3183–3202.
25. Derbas N., Dusserre E. et al. Eventfully Safapp: hybrid approach to event detection for social media mining // *Journal of Ambient Intelligence and Humanized Computing*. 2020. Vol. 11(1). P. 87–95. DOI: 10.1007/s12652-018-1078-7; EDN: VCUFZA.
26. Ducol B. A Radical sociability: in defense of an online/offline multidimensional approach to radicalization // *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected* / Ed by M. Bouchard. N. Y.: Routledge, 2015. P. 82–104.
27. Expressions of Radicalization: Global Politics, Processes and Practices / Ed. by K. Steiner, A. Onnerfors. Cambridge: Palgrave Macmillan, 2018. 526 p. DOI: 10.1007/978-3-319-65566-6.
28. Ferrara E. Contagion dynamics of extremist propaganda in social networks // *Information Sciences*. 2017. Vol. 418–419. P. 1–12. DOI: 10.1016/j.ins.2017.07.030.
29. Floridi L. Hyperhistory and the philosophies of information policies // *The Onlife Manifesto* / Ed. by L. Floridi. L.: Springer, 2015. P. 51–63. DOI: 10.1007/978-3-319-04093-6_12.
30. Francisco M., Castro J. L. A fuzzy model to enhance user profiles in microblogging sites using deep relations // *Fuzzy Sets and Systems*. 2020. Vol. 401. P. 133–149. DOI: 10.1016/j.fss.2020.05.006.

31. Garcet S. Understanding the psychological aspects of the radicalization process: a sociocognitive approach // *Forensic Sciences Research*. 2021. Vol. 6(2). P. 115–123. DOI: 10.1080/20961790.2020.1869883.
32. Gezha V. N., Kozitsin I. V. The Effects of Individuals' Opinion and Non-Opinion Characteristics on the Organization of Influence Networks in the Online Domain // *Computers*. 2023. Vol. 12(6). Article 116. DOI: 10.3390/computers12060116.
33. Greenberg K. J. Counter-radicalization via the internet // *The Annals of the American Academy of Political and Social Science*. 2016. Vol. 668(1). P. 165–179. DOI: 10.1177/0002716216672635.
34. Grover T., Mark G. Detecting Potential Warning Behaviors of Ideological Radicalization in an Alt-Right Subreddit // *Proceedings of the International AAAI Conference on Web and Social Media*. 2019. Vol. 13. P. 193–204. DOI: 10.1609/icwsm.v13i01.3221.
35. Hall M., Logan M. et al. Do Machines Replicate Humans? Toward a Unified Understanding of Radicalizing Content on the Open Social Web // *Policy & Internet*. 2020. Vol. 12. P. 109–138. DOI: 10.1002/poi3.223.
36. Hamm M., Spaaj R. Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies. Washington DC: US Department of Justice, 2015. URL: <https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf> (дата обращения: 15.12.2023).
37. Horgan J. From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism // *The Annals of the American Academy of Political and Social Science*. 2008. Vol. 618(1). P. 80–94. DOI: 10.1177/0002716208317539; EDN: JLEUBT.
38. Ishfaq U., Khan H. U., Iqbal S. Identifying the influential nodes in complex social networks using centrality-based approach // *Journal of King Saud University. Computer and Information Sciences*. 2022. Vol. 34(10). P. 9376–9392. DOI: 10.1016/j.jksuci.2022.09.016; EDN: DKHGZY.
39. Karpova A. Yu., Kuznetsov S. A. et al. An online scan of extreme-right radicalization in social networks (the case of the Russian social network VKontakte) // *Journal of Siberian Federal University. Humanities and Social Sciences*. 2022. Vol. 15. № 12. P. 1738–1750. DOI: 10.17516/1997-1370-0948; EDN: IGVUQA.
40. Karpova A., Savelev A. et al. Method for detecting far-right extremist communities on social media // *Social Sciences*. 2022. Vol. 11. № 5. Article 200. DOI: 10.3390/socsci11050200; EDN: EFNFLP.
41. Kozitsin I. V. A general framework to link theory and empirics in opinion formation models // *Scientific Reports*. 2022. Vol. 12(1). Article 5543. DOI: 10.1038/s41598-022-09468-3; EDN: VVQEUT.
42. Kozitsin I. V. Opinion dynamics of online social network users: a micro-level analysis // *The Journal of Mathematical Sociology*. 2023. Vol. 47(1). P. 1–41. DOI: 10.1080/0022250X.2021.1956917; EDN: BHVFFM.

43. LaFree G. Lone-Offender Terrorists // *Criminology and Public Policy*. 2013. Vol. 12(1). P. 59–62. DOI: 10.1111/1745-9133.12018.
44. Lara-Cabrera R., Pardo A. G. et al. Measuring the Radicalisation Risk in Social Networks // *IEEE Access*. 2017. Vol. 5. P. 10892–10900. DOI: 10.1109/access.2017.2706018; EDN: GFVVFJT.
45. Lee D.-H., Kim Y.-R. et al. Fake News Detection Using Deep Learning // *Journal of Information Processing Systems*. 2019. Vol. 15(5). P. 1119–1130. DOI: 10.3745/JIPS.04.0142.
46. McCauley C., Moskalenko S. Mechanisms of Political Radicalization: Pathways Toward Terrorism // *Terrorism and Political Violence*. 2008. Vol. 20(3). P. 415–433. DOI: 10.1080/09546550802073367.
47. Moghaddam F. M. The staircase to terrorism: A psychological exploration // *American Psychologist*. 2005. Vol. 60(2). P. 161–169. DOI: 10.1037/0003-066X.60.2.161.
48. Mussiraliyeva S., Bolatbek M. et al. On detecting online radicalization and extremism using natural language processing // *21st International Arab Conference on Information Technology*. Giza, 2020. P. 9300086. DOI: 10.1109/ACIT50332.2020.9300086; EDN JNULVZ.
49. Neumann P. R. The trouble with radicalization // *International Affairs*. 2013. Vol. 89(4). P. 873–893. DOI: 10.1111/1468-2346.12049.
50. Petrov A. Countering Fake News with Contagious Inoculation and Debunking: A Mathematical Model // *2022 15th International Conference Management of large-scale system development (MLSD)*. Moscow, 2022. P. 1–4. DOI: 10.1109/MLSD55143.2022.9933991.
51. Petrov A., Akhremenko A., Zheglov S. Dual Identity in Repressive Contexts: An Agent-Based Model of Protest Dynamics // *Social Science Computer Review*. 2023. Vol. 41(6). P. 2249–2273. DOI: 10.1177/08944393231159953; EDN: LPVEKT.
52. Petrov A., Proncheva O. Modeling propaganda battle: Decision-making, homophily, and echo chambers // *Communications in Computer and Information Science*. 2018. Vol. 930. P. 197–209. DOI: 10.1007/978-3-030-01204-5_19; EDN: WTYCBE.
53. *Radicalization and Variations of Violence. New Theoretical Approaches and Original Case Studies* / Ed. by D. Beck, J. Renner-Mugono. Springer, 2023. 212 p. DOI: 10.1007/978-3-031-27011-6.
54. Renström E. A., Bäck H., Knapton H. M. Exploring a pathway to radicalization: The effects of social exclusion and rejection sensitivity // *Group Processes & Intergroup Relations*. 2020. Vol. 23(8). P. 1204–1229. DOI: 10.1177/1368430220917215.
55. Rowe M., Saif H. Mining Pro-ISIS Radicalisation Signals from Social Media Users // *Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016)*. 2016. Vol. 10(1). P. 329–338. DOI: 10.1609/icwsm.v10i1.14716.

56. Sharif W., Mumtaz S. et al. An empirical approach for extreme behavior identification through tweets using machine learning // *Applied Sciences*. 2019. Vol. 9(18). Article 3723. DOI: 10.3390/app9183723; EDN: VKLQVT.
57. Siebl T. *Digital transformation: survive and thrive in an era of mass extinction*. N. Y.: Rosetta Books, 2019. 256 p.
58. Smith L. G., Wakeford L. et al. Detecting psychological change through mobilizing interactions and changes in extremist linguistic style // *Computers in Human Behavior*. 2020. Vol. 108. Article 106298. DOI: 10.1016/j.chb.2020.106298.
59. Tang L., Liu H. *Community Detection and Mining in Social Media*. Morgan & Claypool Publishers, 2010. 138 p. DOI: 10.1007/978-3-031-01900-5.
60. Tausch N., Bode S., Halperin E. Emotions in Violent Extremism // *Handbook of the Psychology of Violent Extremism* / Ed by M. Obaidi, J. Kunst. Cambridge University Press, 2024.
61. *The Routledge handbook of terrorism research* / Ed. by A. Schmid. L.: Routledge, 2011. 736 p.
62. Thompson R. Radicalization and the Use of Social Media // *Journal of Strategic Security*. 2011. Vol. 4. P. 167–190. DOI: 10.5038/1944-0472.4.4.8.
63. Tsapatsoulis N., Djouvas C. Opinion Mining From Social Media Short Texts: Does Collective Intelligence Beat Deep Learning? // *Frontiers in Robotics and AI*. 2019. Vol. 5. P. 138. DOI: 10.3389/frobt.2018.00138.
64. Valentini D., Lorusso A. M., Stephan A. Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization // *Frontiers in Psychology*. 2020. Vol. 11. P. 524. DOI: 10.3389/fpsyg.2020.00524.
65. Wadhwa P., Bhatia M. P. S. An approach for dynamic identification of online radicalization in social networks // *Cybernetics and Systems*. 2015. Vol. 46(8). P. 666. Whittaker J. Rethinking Online Radicalization // *Perspectives on Terrorism*. 2022. Vol. 16(4). P. 27–40. URL: <https://www.jstor.org/stable/27158150> (дата обращения: 15.12.2023).
66. Whittaker J. Rethinking Online Radicalization. *Perspectives on Terrorism*, 2022: 16(4): 27–40. Accessed 15.12.2023. URL: <https://www.jstor.org/stable/27158150>.
67. Winter Ch., Neumann P. et al. Online extremism: research trends in internet activism, radicalization, and counter-strategies // *International Journal of Conflict and Violence*. 2020. Vol. 14. P. 1–20. DOI: 10.4119/ijcv-3809.
68. Wojcieszak M. Carrying online participation offline: mobilization by radical online groups and politically dissimilar offline ties // *Journal of Communication*. 2009. Vol. 59(3). P. 564–586. DOI: 10.1111/j.1460-2466.2009.01436.x.

69. Xu G., Meng Y. et al. Sentiment Analysis of Comment Texts Based on BiLSTM // IEEE Access. 2019. Vol. 7. P. 51522–51532. DOI: 10.1109/ACCESS.2019.2909919.

70. Zafarani R., Abbasi M. A., Liu H. Social Media Mining: An Introduction. Cambridge University Press, 2014. 332 p. DOI: 10.1017/CBO9781139088510.

71. Zareie A., Sheikhahmadi A. et al. Finding influential nodes in social networks based on neighborhood correlation coefficient // Knowledge-Based Systems. 2020. Vol. 194. Article 105580. DOI: 10.1016/j.knosys.2020.105580.

Получено редакцией: 19.02.24

СВЕДЕНИЯ ОБ АВТОРАХ

Зубок Юлия Альбертовна, доктор социологических наук, профессор, заместитель директора по научной работе, Институт социологии ФНИСЦ РАН; руководитель центра социологии молодежи, Институт социально-политических исследований ФНИСЦ РАН

Карпова Анна Юрьевна, доктор социологических наук, профессор Школы общественных наук, Национальный исследовательский Томский политехнический университет

Савельев Алексей Олегович, кандидат технических наук, доцент Инженерной школы информационных технологий и робототехники, Национальный исследовательский Томский политехнический университет

DOI: 10.19181/vis.2024.15.1.2

Practical Network Topology in the Study of Online Radicalisation of Youth: Opportunities and Limitations

Yulia A. Zubok

Institute of Sociology of FCTAS RAS, Moscow, Russia;

Institute of Socio-Political Research of FCTAS RAS, Moscow, Russia

uzubok@mail.ru

ORCID: 0000-0002-3108-2614

Anna Yu. Karpova

National Research Tomsk Polytechnic University, Tomsk, Russia

belts@tpu.ru

ORCID: 0000-0001-7854-1438

Aleksei O. Savelev

National Research Tomsk Polytechnic University, Tomsk, Russia

sava@tpu.ru

ORCID: 0000-0002-7466-6142

For citation: Zubok Yu. A., Karpova A. Yu., Savelev A. O. Practical network topology in the study of online radicalisation of youth: opportunities and limitations. *Vestnik instituta sotziologii*. 2024. Vol. 15. No. 1. P. 13–42. DOI: 10.19181/vis.2024.15.1.2; EDN: VWSNFH.

Abstract. The paper presents key approaches to understanding and researching radicalisation, as well as the opportunities and limitations of applying some research methods to model network topology and assess content similar-

ity of online communities. Today, Web Mining and AI methods and technologies are often applied in research on social networks and youth participation in them. However, the question how these approaches can be effectively used to study online radicalisation remains open. The answer to this question should increase the explanatory and predictive power of computational models for detecting and predicting radicalisation in the online space. In much of the Russian research on online radicalisation, a common approach has been to reduce the task of identifying the interconnectedness of individual online communities or clusters of them to assessing the degree of similarity in terms of subscribers or linguistic markers. This approach is limited in predicting new connections between communities and justifying radicalisation pathways, but is relevant in modelling information diffusion. In this paper, the authors aim to demonstrate the possibilities and limitations of applying the tf-idf, doc2vec methods to assess the content similarity of online communities without signs of radicalisation and online communities with signs of radicalisation. This approach allowed the authors to identify communities with a significant tendency to unite (to establish direct links). The paper presents the results of the comparative study in the form of social graphs formed according to the principles of subscriber commonality, similarity of significant words, and contextual similarity based on the doc2vec model. The social graph based on doc2vec method performed better in terms of clustering of online communities as well as interpretability of the results. This is crucial for detecting and predicting radicalisation online, as it opens the prospect of exploring the nature of assortativity in the observed network.

Keywords: social network, community, radicalisation, network topology, tf-idf, doc2vec

References

1. Akhremenko A. S., Stukal D. K., Petrov A. P. Network or text? Factors of protest dissemination in social media: theory and data analysis. *Polis. Politicheskie issledovaniya*, 2020: 2: 73–91 (in Russ.). DOI: 10.17976/jpps/2020.02.06; EDN: APZWMB.
2. Karpova A. Y., Kuznetsov S. A. et al. Method for searching images with signs of ultra-right radicalization in social media based on neural network classification. *Sistemy upravleniya i informacionny'e texnologii*, 2023: 1(91): 59–64 (in Russ.). DOI: 10.36622/VSTU.2023.91.1.012; EDN: KGWMLC.
3. Karpova A. Yu., Savelev A. O. Opportunities and boundaries of Big Data technologies for the study of online radicalization. In Third December socio-political readings “How you live, Russia?”. Challenges of the pandemic, parliamentary elections and strategic agenda for society and the state. Moscow, FNISC RAN, 2022: 67–78 (in Russ.). EDN: ZXFWGV.
4. Karpova A. Y., Savelev A. O. et al. Ultra-right radicalization: methodology of automated threat detection by web mining methods. *Vestnik RFFI. Gumanitarnye i obshchestvennye nauki*, 2020: 5(102): 30–43 (in Russ.). DOI: 10.22204/2587-8956-2020-102-05-30-43; EDN: BEZTTC.
5. Karpova A. Y., Savelev A. O. et al. Studying Online Radicalization of Youth through Social Media (Interdisciplinary Approach). *Monitoring obshchestvennogo mneniya: ekonomicheskie i social'nye peremeny*, 2020: 3(157): 159–181 (in Russ.). DOI: 10.14515/monitoring.2020.3.1585; EDN: CXJJUW.
6. Karpova A. Y., Savelev A. O., Kuznetsov S. A. Transformation of social practices of responsible fatherhood into deviant forms of social activity. *Vektory blagopoluchiya: ekonomika i socium*, 2021: 4(43): 107–118 (in Russ.). DOI: 10.18799/26584956/2021/4(43)/1130; EDN: DDROPU.
7. Karpova A. Yu., Shirykalov A. M. Development of a method for evaluating the similarity of text collections using their vector representations obtained by the doc2vec method. In Youth and Modern Information Technologies. Tomsk, TPU, 2021: 75–76 (in Russ.). EDN: SWSZVQ.
8. Kuznetsov S. A., Karpova A. Yu., Savelev A. O. Methods and technologies of intellectualization of search for destructive and radical content in social media: analysis of the current state. *Vestnik kompyuternyh i informacionnyh texnologij*, 2023: 4(226): 39–48 (in Russ.). DOI: 10.14489/vkit.2023.04.pp.039-048; EDN: EVCQQC.
9. Savelev A. O., Karpova A. Yu. A. Approach to the assessment of interconnections of social media communities on the basis of thematic similarity of textual content (on the example of communities of socially active fathers and communities with signs of radicalization). *Kazan Economic Bulletin*, 2022: 1(57): 96–103 (in Russ.). EDN: DNZYVS.
10. Sokolova T. V., Chepovsky A. M. The task of analyzing social network user profiles. In Situation centers and *information-analytical systems of class 4i for monitoring and security tasks (SCVRT2017)*. Moscow–Protvino, IFTI, 2017: 198–201 (in Russ.). EDN: YSHYDJ.

11. Stukal D. K., Akhremenko A. S., Petrov A. P. Affective political polarization and hate speech: created for each other? *Vestnik RUDN. Ser.: Politologiya*, 2022: 3: 480–498 (in Russ.). DOI: 10.22363/2313-1438-2022-24-3-480-498; EDN: VLTQRN.
12. Chuprov V. I., Zubok Yu. A. Molodezhnyj ekstremizm: sushhnost, formy proyavleniya, tendencii [Youth extremism: essence, forms of manifestation, trends]. Moscow, Academia, 2009: 320 (in Russ.). EDN: SUFKBZ.
13. Akram M., Nasar A. Systematic Review of Radicalization through Social Media. *Ege Academic Review*. 2023. Vol. 23(2). P. 279–296. DOI: 10.21121/eab.1166627; EDN: JFWLSR.
14. Alvares H., Sarkar S., Shakarian P. Detection of Violent Extremists in Social Media. In 2nd International Conference on Data Intelligence and Security (ICDIS). South Padre Island, TX, USA, 2019: 43–47. DOI: 10.1109/ICDIS.2019.00014.
15. Araque O., Iglesias C. A. An Approach for Radicalization Detection Based on Emotion Signals and Semantic Similarity. *IEEE Access*, 2020: 8: 17877–17891. DOI: 10.1109/access.2020.2967219.
16. Binder J. F., Kenyon J. Terrorism and the internet: How dangerous is online radicalization? *Frontiers in Psychology*, 2022: 13. DOI: 10.3389/fpsyg.2022.997390; EDN: RGSMYY.
17. Borum R. Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, 2012: 4(4): 7–36. DOI: 10.5038/1944-0472.4.4.1.
18. Borum R. Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research. *Journal of Strategic Security*. 2012: 4(4): 37–62. DOI: 10.5038/1944-0472.4.4.
19. Borum R. Rethinking radicalization. *Journal of Strategic Security*, 2012: 4(4): 1–6. Accessed 15.12.2023. URL: <https://digitalcommons.usf.edu/jss/vol4/iss4/1>
20. Borum R. Understanding the terrorist mind-set. *FBI Law Enforcement Bulletin*, 2003: 72(7): 7–10.
21. Clancy T., Addison B. et al Contingencies of Violent Radicalization: The Terror Contagion Simulation. *Systems*, 2021: 9(4): 90. DOI: 10.3390/systems9040090.
22. Das S., Biswas A. The Ties that matter: From the perspective of Similarity Measure in Online Social Networks. *ArXiv*, 2022. DOI: 10.48550/arXiv.2212.10960.
23. de la Roche R. S. Why is collective violence collective? *Sociological Theory*, 2001: 19(2): 126–144. DOI: 10.1111/0735-2751.00133.
24. Deem A. The Digital Traces of #whitegenocide and Alt-Right Affective Economies of Transgression. *International Journal of Communication*, 2019: 13: 3183–3202.
25. Derbas N., Dusserre E. et al. Eventfully Safapp: hybrid approach to event detection for social media mining. In *Journal of Ambient Intelligence and Humanized Computing*, 2020: 11(1): 87–95. DOI: 10.1007/s12652-018-1078-7; EDN: VCUFZA.
26. Ducol B. A Radical sociability: in defense of an online/offline multidimensional approach to radicalization. *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected*. Ed by M. Bouchard. New York, Routledge, 2015: 82–104.
27. Expressions of Radicalization: Global Politics, Processes and Practices. Cambridge, Palgrave Macmillan, 2018: 526. DOI: 10.1007/978-3-319-65566-6.
28. Ferrara E. Contagion dynamics of extremist propaganda in social networks. *Information Sciences*, 2017: 418–419: 1–12. DOI: 10.1016/j.ins.2017.07.030.
29. Floridi L. Hyperhistory and the philosophies of information policies. *The Onlife Manifesto*, 2015: 51–63. DOI: 10.1007/978-3-319-04093-6_12.
30. Francisco M., Castro J. L. A fuzzy model to enhance user profiles in microblogging sites using deep relations. *Fuzzy Sets and Systems*, 2020: 401: 133–149. DOI: 10.1016/j.fss.2020.05.006.
31. Garcet S. Understanding the psychological aspects of the radicalization process: a sociocognitive approach. *Forensic Sciences Research*, 2021: 6(2): 115–123. DOI: 10.1080/20961790.2020.1869883.
32. Gezha V. N., Kozitsin I. V. The Effects of Individuals' Opinion and Non-Opinion Characteristics on the Organization of Influence Networks in the Online Domain. *Computers*, 2023: 12(6). DOI: 10.3390/computers12060116.
33. Greenberg K. J. Counter-radicalization via the internet. *The Annals of the American Academy of Political and Social Science*, 2016: 668(1): 165–179. DOI: 10.1177/0002716216672635.

34. Grover T., Mark G. Detecting Potential Warning Behaviors of Ideological Radicalization in an Alt-Right Subreddit. In Proceedings of the International AAAI Conference on Web and Social Media, 2019: 13: 193–204. DOI: 10.1609/icwsm.v13i01.3221.
35. Hall M., Logan M. et al. Do Machines Replicate Humans? Toward a Unified Understanding of Radicalizing Content on the Open Social Web. *Policy & Internet*. 2020: 12: 109–138. DOI: 10.1002/poi3.223.
36. Hamm M., Spaaj R. Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies. Washington DC: *US Department of Justice*, 2015. Accessed 15.12.2023. URL: <https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf>
37. Horgan J. From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism. *The Annals of the American Academy of Political and Social Science*, 2008: 618(1): 80–94. DOI: 10.1177/0002716208317539; EDN: JLEUBT.
38. Ishfaq U., Khan H. U., Iqbal S. Identifying the influential nodes in complex social networks using centrality-based approach. *Journal of King Saud University. Computer and Information Sciences*, 2022: 34(10): 9376–9392. DOI: 10.1016/j.jksuci.2022.09.016; EDN: DKHGZY.
39. Karpova A. Yu., Kuznetsov S. A. et al. An online scan of extreme-right radicalization in social networks (the case of the Russian social network VKontakte). *Journal of Siberian Federal University. Humanities and Social Sciences*, 2022: 15: 12: 1738–1750. DOI: 10.17516/1997-1370-0948; EDN: IGVUQA.
40. Karpova A., Savelev A. et al. Method for detecting far-right extremist communities on social media. *Social Sciences*, 2022: 11: 5. DOI: 10.3390/socsci11050200; EDN: EFNFLP.
41. Kozitsin I. V. A general framework to link theory and empirics in opinion formation models. *Scientific Reports*, 2022: 12(1): 5543. DOI: 10.1038/s41598-022-09468-3; EDN: VVQEUT.
42. Kozitsin I. V. Opinion dynamics of online social network users: a micro-level analysis. *The Journal of Mathematical Sociology*, 2023: 47(1): 1–41. DOI: 10.1080/0022250X.2021.1956917; EDN: BHVFFM.
43. LaFree G. Lone-Offender Terrorists. *Criminology and Public Policy*, 2013: 12(1): 59–62. DOI: 10.1111/1745-9133.12018.
44. Lara-Cabrera R., Pardo A. G. et al. Measuring the Radicalisation Risk in Social Networks. *IEEE Access*, 2017: 5: 10892–10900. DOI: 10.1109/access.2017.2706018; EDN: GFVFJT.
45. Lee D.-H., Kim Y.-R. et al. Fake News Detection Using Deep Learning. *Journal of Information Processing Systems*, 2019: 15(5): 1119–1130. DOI: 10.3745/JIPS.04.0142.
46. McCauley C., Moskaleiko S. Mechanisms of Political Radicalization: Pathways Toward Terrorism. *Terrorism and Political Violence*, 2008: 20(3): 415–433. DOI: 10.1080/09546550802073367.
47. Moghaddam F. M. The staircase to terrorism: A psychological exploration. *American Psychologist*, 2005: 60(2): 161–169. DOI: 10.1037/0003-066X.60.2.161.
48. Mussiraliyeva S., Bolatbek M. et al. On detecting online radicalization and extremism using natural language processing. In 21st International Arab Conference on Information Technology. Giza, 2020: 9300086. DOI: 10.1109/ACIT50332.2020.9300086; EDN JNULVZ.
49. Neumann P. R. The trouble with radicalization. *International Affairs*, 2013: 89(4): 873–893. DOI: 10.1111/1468-2346.12049.
50. Petrov A. Countering Fake News with Contagious Inoculation and Debunking: A Mathematical Model. 2022 15th International Conference Management of large-scale system development (MLSD). Moscow, 2022: 1–4. DOI: 10.1109/MLSD55143.2022.9933991.
51. Petrov A., Akhremenko A., Zhiglov S. Dual Identity in Repressive Contexts: An Agent-Based Model of Protest Dynamics. *Social Science Computer Review*, 2023: 41(6): 2249–2273. DOI: 10.1177/08944393231159953; EDN: LPVEKT.
52. Petrov A., Proncheva O. Modeling propaganda battle: Decision-making, homophily, and echo chambers. *Communications in Computer and Information Science*, 2018: 930: 197–209. DOI: 10.1007/978-3-030-01204-5_19; EDN: WTYCBE.
53. Radicalization and Variations of Violence. New Theoretical Approaches and Original Case Studies. Ed. by D. Beck, J. Renner-Mugono. Springer, 2023: 212. DOI: 10.1007/978-3-031-27011-6.
54. Renström E. A., Bäck H., Knapton H. M. Exploring a pathway to radicalization: The effects of social exclusion and rejection sensitivity. *Group Processes & Intergroup Relations*, 2020: 23(8): 1204–1229. DOI: 10.1177/1368430220917215.

55. Rowe M., Saif H. Mining Pro-ISIS Radicalisation Signals from Social Media Users. In Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016). 2016: 10(1): 329–338. DOI: 10.1609/icwsm.v10i1.14716.
56. Sharif W., Mumtaz S. et al. An empirical approach for extreme behavior identification through tweets using machine learning. *Applied Sciences*, 2019: 9(18). DOI: 10.3390/app9183723; EDN: VKLQVT.
57. Siebl T. Digital transformation: survive and thrive in an era of mass extinction. New York, Rosetta Books, 2019: 256.
58. Smith L. G., Wakeford L. et al. Detecting psychological change through mobilizing interactions and changes in extremist linguistic style. *Computers in Human Behavior*, 2020: 108: 106298. DOI: 10.1016/j.chb.2020.106298.
59. Tang L., Liu H. Community Detection and Mining in Social Media. Morgan & Claypool Publishers, 2010: 138. DOI: 10.1007/978-3-031-01900-5.
60. Tausch N., Bode S., Halperin E. Emotions in Violent Extremism. Handbook of the Psychology of Violent Extremism. Cambridge University Press, 2024.
61. The Routledge handbook of terrorism research. London, Routledge, 2011: 736.
62. Thompson R. Radicalization and the Use of Social Media. *Journal of Strategic Security*, 2011: 4: 167–190. DOI: 10.5038/1944-0472.4.4.8.
63. Tsapatsoulis N., Djouvas C. Opinion Mining From Social Media Short Texts: Does Collective Intelligence Beat Deep Learning? *Frontiers in Robotics and AI*, 2019: 5: 138. DOI: 10.3389/frobt.2018.00138.
64. Valentini D., Lorusso A. M., Stephan A. Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization. *Frontiers in Psychology*, 2020: 11: 524. DOI: 10.3389/fpsyg.2020.00524.
65. Wadhwa P., Bhatia M. P. S. An approach for dynamic identification of online radicalization in social networks. *Cybernetics and Systems*, 2015: 46(8): 641–665. DOI: 10.1080/01969722.2015.1058665.
66. Whittaker J. Rethinking Online Radicalization. *Perspectives on Terrorism*, 2022: 16(4): 27–40. Accessed 15.12.2023. URL: <https://www.jstor.org/stable/27158150>.
67. Winter Ch., Neumann P. et al. Online extremism: research trends in internet activism, radicalization, and counter-strategies. *International Journal of Conflict and Violence*, 2020: 14: 1–20. DOI: 10.4119/ijcv-3809.
68. Wojcieszak M. Carrying online participation offline: mobilization by radical online groups and politically dissimilar offline ties. *Journal of Communication*, 2009: 59(3): 564–586. DOI: 10.1111/j.1460-2466.2009.01436.x.
69. Xu G., Meng Y. et al. Sentiment Analysis of Comment Texts Based on BiLSTM. *IEEE Access*, 2019: 7: 51522–51532. DOI: 10.1109/ACCESS.2019.2909919.
70. Zafarani R., Abbasi M. A., Liu H. Social Media Mining: An Introduction. Cambridge University Press, 2014: 332. DOI: 10.1017/CBO9781139088510.
71. Zareie A., Sheikhamadi A. et al. Finding influential nodes in social networks based on neighborhood correlation coefficient. *Knowledge-Based Systems*, 2020: 194: 105580. DOI: 10.1016/j.knosys.2020.105580.

The article was submitted on: February 19, 2024

INFORMATION ABOUT THE AUTHORS

Yulia A. Zubok, Doctor of Sociology Sciences, Professor, Deputy Director for Research, Institute of Sociology of FCTAS RAS; Head of the Center for Sociology of Youth, Institute of Socio-Political Research of FCTAS RAS

Anna Yu. Karpova, Doctor of Sociology Sciences, Professor, School of Social Sciences, National Research Tomsk Polytechnic University

Aleksei O. Savelev, Candidate of Engineering Sciences, Associate Professor, Division for Information Technology, National Research Tomsk Polytechnic University