DOI 10.36622/1682-7813.2024.27.4.002
УДК 004.94:327

ВЫЯВЛЕНИЕ И ТИПОЛОГИЗАЦИЯ КРИМИНАЛЬНЫХ СУБЪЕКТОВ В СОЦИАЛЬНЫХ МЕДИА

В.А. Минаев, А.С. Толпыгин, К.А. Кузьмина

В статье рассматривается проблема выявления субъектов в социальных медиа, способных оказывать значительное негативное влияние на других пользователей. Основной акцент сделан на применении методов кластеризации для разделения пользователей на группы и последующего расчета центров влияния в каждом кластере. Методика направлена на решение задач, связанных с предупреждением киберпреступлений – выявление потенциально опасных сегментов аудитории, определение векторов распространения негативного контента, прогнозирование возможного перехода пользователей между кластерами. Предложенный подход включает этапы предварительной обработки данных, преобразования их в числовой формат, стандартизации и выбора модели кластеризации. Особое внимание уделено измерения рейтинговых показателей пользователей - количество связей (друзей), публикаций; уровень активности, в том числе – криминальной. В итоге создается информационно-аналитический комплекс, позволяющий эффективно определять центры влияния в социальных медиа. Результаты имеют потенциал для практического применения в борьбе с киберугрозами, обеспечивая поддержку правоохранительных органов и служб безопасности при решении задач мониторинга и анализа онлайн-сообществ.

Ключевые слова: киберпреступность, терроризм, экстремизм, социальное медиа, типологизация, идентификация лидеров.

Введение

Современный мир характеризуется массовым вовлечением населения и организаций в информационное взаимодействие посредством мобильных средств коммуникации. Это позволяет абонентам постоянно находиться на связи друг с другом и общаться в различных информационных средах, получать информацию из множества источников и мгновенно ею делиться (ретранслировать).

При этом все более значимое место в жизни общества и человека занимают социальные сети и мессенджеры – социальные медиа (СМ). Применяясь сначала в качестве преимущественно носителя развлекательного контента, сегодня они превратились в одно из важнейших средств коммуникации людей.

Сегодня многие проводят в сетях и мессенджерах не менее 4 часов в сутки [3], тратя время как на бытовое общение, так и на получение новой информации в сфере своих интересов, изучение новостей, просмотр видео и прослушивание музыки

Постоянно изменяющаяся информационная среда, к сожалению, стала благоприятной для связи организованных преступных группировок (ОПГ). Это могут быть как мошенники [1, 2], вымогающие обманом средства у граждан, так организации экстремистской, и террористической направленности, которые используют её для скрытного информационного взаимодействия при организации, координации противоправных действий и управлении ими.

Задача выявления такого взаимодействия в настоящее время не имеет достаточно эффективных способов решения. А если учитывать возможности в применении средств криптографии и стеганографии, то решение данной задачи многократно усложняется.

Социальные медиа позволяют получать данные, подчас весьма конфиденциальные, о конкретных людях и событиях. Заполняя информацию о себе на различных сайтах, порталах и других «Интернет-собирателях», человек дает доступ к ней неограниченному кругу лиц. Более того, нет средств контроля и

ограничения в распространении опубликованной информации. Она публикуется другими пользователями без уведомления её владельца, а СМ при таких операциях допускают получение дополнительных сведений о той или иной личности. Таким образом, скрыть критически значимую информацию о себе в современных условиях весьма непросто. Также не просто выявить распространителей информации, которые применяют современные технологии, чем гарантируют себе анонимность действий в СМ, скрывая факт принадлежности страницы или аккаунта конкретному лицу.

Как следствие, возможность обеспечения анонимности, сложность отслеживания скрытных действий и ограничения распространения личной информации, простота формирования фейковой информации значительно влияют на рост криминальной активности и потенциальных возможностей преступного мира в социальных медиа, начиная от мелких правонарушений до осуществления террористической деятельности, вербовки, обучения, финансирования экстремистов.

По данным Генеральной прокуратуры Российской Федерации, из общего числа зарегистрированных преступлений за 2023 год, которое составило 1,8 миллиона, более четверти были совершены с использованием интернета. К ним относятся преступления в соцсетях и мессенджерах, телефонные мошенничества, хищения средств с банковских карт, преступления с использованием электронных платежных систем для онлайн покупок, преступления в даркнет, хакерские преступления. За прошедший год число зарегистрированных IT-преступлений выросло на треть, а IT-мошенничеств – на 40%. Важно отметить, что о многих таких инцидентах пострадавшие предпочитают не сообщать [4].

Согласно майским данным 2024 года доля киберпреступлений по сравнению с аналогичным периодом прошлого года выросла почти до двух пятых среди всех преступлений [2, 5].

Очевидно, что в связи с усилением негативных тенденций такого рода важно не только совершенствование работы правоохранительных органов по раскрытию и расследованию такого рода высокотехнологичных преступлений, но и существенная активизация их предупреждения в социальных медиа.

Принимая во внимание, что поведение в СМ различается в зависимости от целей пользователей, повысить эффективность выявления социально-опасных и криминальных элементов в сети представляется возможным, основываясь на их типологизации, которая, в свою очередь, основывается на анализе множества характеристик – социальный статус, психоэмоциональное состояние, образ жизни, степень преступной активности и других.

Ключевые вопросы предупреждения киберпреступлений

Основная задача состоит в выявлении таких субъектов в СМ, которые могут в наибольшей степени негативно влиять на других пользователей. В основу решения задачи положена гипотеза о том, что их можно разделить на кластеры, в центрах которых находятся пользователи, которые имеют наибольшее влияние на остальных, попавших в конкретный кластер. Решение основной задачи, помимо сбора данных и применения к ним классических алгоритмов кластеризации предполагает проведение анализа данных статистическим методами.

Исследование статистических характеристик позволяет решить и сопутствующие задачи, позволяющие расширить сведения о выделенных кластерах и центрах влияния в них. В качестве примеров можно привести задачу выявления типичных характеристик пользователей в кластере, задачу выявления пользователей, находящихся в группе риска и/или склонных к переходу в сферу негативного влияния, описания характера противоправной деятельности, определения наиболее вероятных направлений перехода между кластерами.

Важное требование, выдвигаемое к используемым данным – это возможность измерения важности, рейтинга пользователя в сети, отражаемого такими признаками, как количество друзей, подписчиков, публикуемых изображений, активность

пользователя на собственной странице и внутри сообщества. Указанная задача решается путем кластеризации элементного наполнения социальных сетей, сетевых сообществ и поведения подписчиков [6, 7].

На данный момент существует ряд решений для анализа характеристик сообществ в различных социальных сетях. Преимущественно они реализованы применительно к зарубежным сетям – Instagram, Twitter, Facebook и LinkedIn. Данные решения поддерживают функции мониторинга активности, планирования, аналитических исследований и поиска нужного контента.

Для решения задачи выделено несколько этапов:

1. *Формирование и предварительная обработка данных* для приведения их к виду, соответствующему требованиям моделей кластеризации. Перед построением моделей кластеризации пользователей выполняется предварительный анализ. Для этого производится:

– изучение имеющейся информации, предполагающее анализ данных – их значений, типов, полноты представления.

Все это позволяет осуществить корректную обработку данных для построения качественных моделей:

– удаление избыточных и ошибочных данных. В качестве избыточных данных выделяются дубликаты, а ошибочных - пропуски в собранной информации;

– реиндексацию данных для корректного объединения различных таблиц.

2. *Преобразование данных* путем приведения всех их типов к числовым. При этом важно учитывать, что модели кластеризации, как правило, используют расстояния между объектами как критерий или метрику для разделения.

3. *Стандартизация данных*.

Нестандартизированные данные трудно использовать для обучения модели. Для того, чтобы избежать этого, необходимо их стандартизировать. Сделать это нужно путем приведения каждого признака к нулевому среднему значению и единичному среднеквадратичному отклонению (СКО) по формуле:

$$x' = \frac{x - \mu}{\sigma},$$

где x' – стандартизированное значение признака,

x – исходное значение признака,

μ – среднее значение по признаку,

σ – СКО по признаку.

4. *Выбор и программная реализация модели кластеризации*.

5. *Разработка информационно-аналитического программного комплекса*, на базе которого определяются центры влияний в СМ.

В основу разработки модели и программно-аналитического комплекса положено предположение, что изучаемое Интернет-сообщество можно разделить на кластеры, центры которых представляют пользователи, наибольшим образом влияющие на других пользователей.

Определим СМ, наиболее подходящее для решения поставленной задачи кластеризации. Учтем при этом наиболее популярные СМ в России, представленные в табл. 1 [5].

Таблица 1

Популярность социальных медиа в РФ

Социальное медиа	Доля пользователей, %
WhatsApp	87
YouTube	75
ВКонтакте	62
Telegram	55
Одноклассники	42

Исходя из анализа табл.1, среди социальных медиа для решения задачи выбрана социальная сеть ВКонтакте, что объясняется:

– относительно б*о*льшим количеством персональных данных пользователей в ней;

– наибольшей доступностью данных для анонимных пользователей;

– сравнительным удобством сбора статистических данных об Интернет-сообществах;

– открытым API (applications program interface).

Построение модели кластеризации и анализ результатов

Для кластеризации имеющихся данных необходимо построить адекватную модель по определению количества кластеров и их центров, соответствующих наиболее влиятельным пользователям. В отношении полученных данных применена одна из наиболее популярных моделей кластеризации *K-means*, требующая определения количества кластеров для разделения данных. Оптимальное значение количества кластеров выбиралось на основе «правила локтя», заключающегося в анализе графика изменения среднего внутрикластерного расстояния.

В итоге выбрано такое количество кластеров, которое находится в точке резкого изменения среднего расстояния до их центра (рис. 1). В нашем случае оно оказалось равным семи.

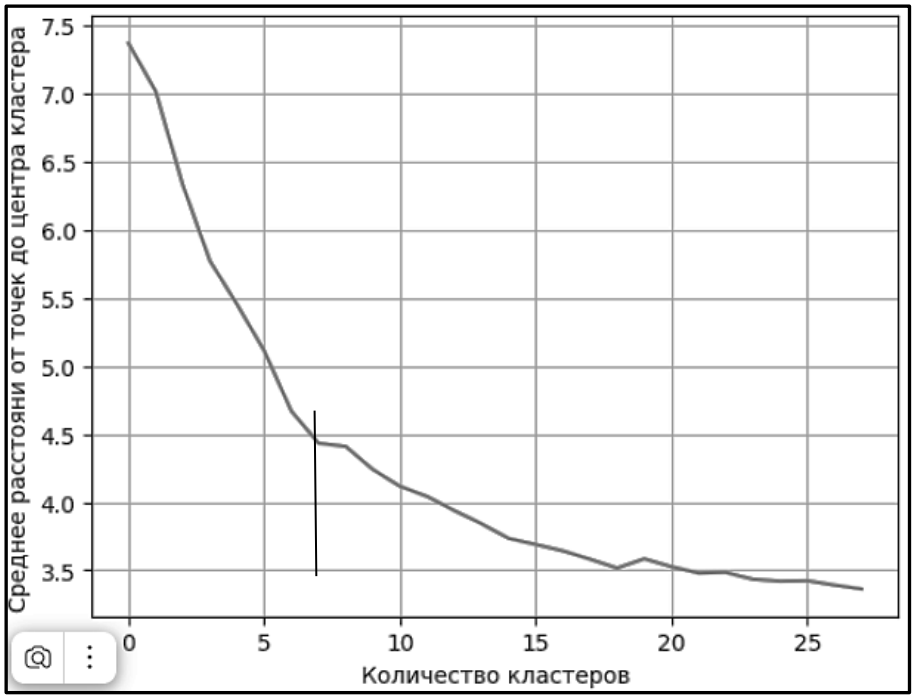

Рис. 1. Среднее расстояние до центра кластеров в зависимости от их количества

Избрание социальной сети ВКонтакте позволило получить необходимые данные о пользователях, которые преобразованы в нужный формат и стандартизованы для использования в модели кластеризации, позволившей выделить различающиеся кластеры пользователей, указать центры кластеров, отражающие максимумы влияния на сетевые сообщества со стороны тех пользователей, которые попали в центры. Исходя из «правила локтя» выявлено семь характерных кластеров.

Для наглядной демонстрации принципов работы модели и программного комплекса представим набор данных о подписчиках сообщества в СМ ВКонтакте.

Для отображения рейтинга пользователя в сети нами выбраны показатели и соответствующие им типы данных, представленные в табл. 2.

На предварительно обработанных данных проведена кластеризация пользователей и для образованных групп пользователей применяются различные методы анализа, позволяющие всесторонне исследовать проблему влияния центров на прочие субъекты и возможности распространения негативной информации, а также осуществления противоправной деятельности.

Таблица 2

Собранные характеристики пользователей и соответствующие им типы данных

Характеристика пользователя	Тип данных
Имя	Строковый
Фамилия	Строковый
Удаленная страница	Логический
День рождения	Целочисленный
Месяц рождения	Целочисленный
Год рождения	Целочисленный
Количество друзей	Целочисленный
Город	Строковый
Количество подписчиков	Целочисленный
Количество подписок	Целочисленный
Наличие главного фото	Логический
Количество отметок «нравится» на главном фото	Целочисленный

Для идентификации социально-опасных субъектов учитывались следующие признаки, отражающиеся в публикуемом контенте и указывающие на мотивы субъектов:

Экономические мотивы:

– Качество: материальная выгода.

– Признак: низкий социально-экономический статус, финансовые трудности.

Эмоциональные мотивы:

– Качество: сильные эмоции (злоба, ревность, страх, месть).

– Признак: импульсивность действий, отсутствие долгосрочного планирования.

Морально-этические мотивы:

– Качество: ощущение борьбы за правду, моральные убеждения.

– Признак: идеологические или политические мотивы, чувство справедливости.

Психологические мотивы:

– Качество: психологические внутренние потребности, бессознательные желания.

– Признак: отсутствие осознания своих поступков, наличие психических расстройств.

В совокупности с личностными характеристиками уточнен характер лиц с криминальными наклонностями.

Импульсивность:

– Качество: эмоциональная нестабильность, склонность к агрессивному поведению.

– Признак: незапланированные, спонтанные действия социально-опасного и криминального характера, вызванные сильными эмоциями.

Расчетливость:

– Качество: холодный расчет, планирование.

– Признак: долгосрочная подготовка социально-опасных действий, стремление минимизировать риски.

Анализ:

1. Расчет среднеквадратичного отклонения (СКО) позволяет оценить кучность классов, относительно каждого признака. Так как многие алгоритмы кластеризации используют или могут использовать СКО при отнесении экземпляров к тому или иному классу, данный показатель наиболее информативен при оценке влияния конкретного признака на распределение по кластерам. При анализе СКО в совокупности с медианными значениями или значениями центров, могут быть выявлены характерные значения признаков для каждого кластера.

2. Расчет медианных значений по каждому признаку для каждого кластера позволяет оценить их различие по принимаемым характеристиками пользователей значениям. Данная информация позволяет сформировать портрет типичного пользователя, входящего в данный кластер.

3. Значения признаков для центров кластеров несут в себе основную информацию о всех представителях кластера. Подробный смысловой анализ публикаций пользователя и личной информации может помочь выделить характер распространяемой информации, направление противоправной деятельности, каналы распространения информации.

4. Анализ минимальных и максимальных значений расстояний до соседних кластеров для центра каждого кластера позволяет выдвинуть предположения о сходстве между кластерами по всем признакам сразу и определить наиболее вероятные векторы

переходов пользователей из одного кластера в другой.

Практическое применение

Описанный подход к выявлению в социальных медиа субъектов, способных оказывать негативное, в том числе – криминальное влияние на других пользователей, находит практическое применение для решения задач предупреждения действий криминального характера различной направленности. Решение сопутствующих задач позволяет расширять сферы применения, обеспечивая разделение подписчиков на группы с выявлением зависимостей между ними, интерпретировать характеристики каждой группы, определять каналы распространения деструктивной информации между группами и внутри них.

Одно из направлений – выявление и предотвращение финансовых преступлений на основе анализа больших данных и современных методов обработки информации. Поиск опасных паттернов и предотвращение финансовых преступлений на основе больших данных (отмывание денег, мошенничество, недобросовестная конкуренция, использование серых зон в регулировании, утечка конфиденциальной информации).

Применение описанного метода кластеризации может использоваться в задачах построения социальных графов членов террористических организаций или организаций по распространению запрещенных веществ и/или оружия. Методы интерпретации данных могут активно применяться в задачах выявления сегментов пользователей, наиболее подверженных негативному влиянию. Применение описываемых методов в связке с проведением семантического анализа контента пользователей и сообществ может применяться в задачах выявления оппозиционно настроенных личностей и их связей.

Следуя методологии, предложенной авторами в [8], возможно создание цифровых двойников клиентов для их изучения и управления кредитными рисками в финансово-кредитных организациях.

Цифровые двойники строятся на основе исследования цифровых следов, оставляемых пользователями в СМ. Даже незначительные, на первый взгляд, данные дают возможность делать выводы о поведении, мотивации и индивидуальных особенностях клиента, что, в конечном итоге, способствует автоматизации процессов оценки рисков и предотвращения мошенничества.

Практическое применение описанного подхода в каждом конкретном случае может потребовать адаптации и уточнения, но в целом основные шаги методики включают:

1.Исследование ключевых моделей и сценариев финансовых преступлений, таких как отмывание денег, мошенничество и утечки информации для определения ключевых характеристик и свойств, по которым оцениваются субъекты и может быть сделан вывод о принадлежности их к числу социально-опасным.

2.Разработка критериев и методов оценивания для автоматического поиска паттернов поведения, сигнализирующих о возможной принадлежности субъекта к числу социально-опасных.

3. Формирование наборов данных, необходимых для создания цифровых двойников

4. Построение моделей – цифровых двойников и насыщение их данными.

5. Анализ, типологизация субъектов, выявление социально-опасных действий в СМ.

6. Проверка достоверности и корректности результатов моделирования.

7. Принятие мер (при необходимости), разработка и реализация рекомендаций по повышению точности моделей.

Для выполнения указанных шагов разработано программное обеспечение, которое автоматически собирает данные в социальной сети ВКонтакте. Создан алгоритм разделения данных на кластеры и выделения их наиболее значимых характеристик. Программный комплекс успешно функционирует и применяется для анализа массивов пользователей СМ.

Реализованные в рамках программного комплекса функции кластеризации алгоритмами машинного обучения

позволяют для каждого кластера вычислять центры (субъектов) влияния.

Введенные нормы в российском законодательстве позволяют поставить под контроль средства коммуникаций, но при этом практика применения предполагает последействие в процедуре проведения расследования по результатам уже совершенных противоправных действий, последствия которых необратимы и выражаются не только экономически, а также в массовых человеческих жертвах.

Предлагаемый подход к решению поставленной задачи является превентивным (профилактическим) и предполагает изучение поведенческих особенностей субъектов и связей (возможно скрытых) между ними при осуществлении информационного взаимодействия. Это позволит в последствии выявить причинно-следственные связи между поведением субъектов и их интересами, которые его (поведение) определяют.

Для реализации подхода необходимо создание программного комплекса, в основу которого может быть положено разработанное ПО.

Заключение

В качестве дальнейшего развития реализованного подхода и улучшения качества решения классификационных задач можно выделить следующие направления:

– применение более детализированных моделей с улучшенными алгоритмами кластеризации;

– добавление новых признаков, характеризующих характеристики и информационное поведение пользователей внутри сетевого сообщества и их взаимодействие с другими участниками сети;

– сбор информации из других социальных медиа;

– отслеживание и анализ изменений в составе сообществ и распределении при кластеризации с течением времени.

Список литературы

1. Минаев В.А., Бондарь К.М., Рабчевский А.Н., Федорович В.Ю. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: Монография / Под ред. В.А. Минаева, К.М. Бондаря. Хабаровск: РИО ДВЮИ МВД России, 2023. 232 с.

2. Банк России. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. I квартал 2024 года. // URL: https://www.cbr.ru/statistics/ib/ review_1q_2024/ (дата обращения: 30.11.2024).

3. Емельяненко В. ВЦИОМ: Россияне тратят на соцсети до пяти часов в день. // URL: https://rg.ru/2023/08/10/vciom-polzovateli-socsetej-tratiat-na-nih-do-piati-chasov-v-den.html (дата обращения: 30.11.2024).

4. Каждое четвертое преступление в России совершают через Интернет. // URL: https://tass.ru/obschestvo/19669641 (дата обращения: 30.11. 2024).

5. В России доля киберпреступлений достигла 38% среди всех преступлений. // URL: https://tass.ru/obschestvo/20933305 (дата обращения: 30.11. 2024).

6. Ушкин С. Г., Сапон Н. В. Протестные группы в социальной сети ВКонтакте: кластеризация пользователей и их типологические особенности // Социология и управление. 2022. Т. 8. № 2. С. 97-111.

7. Social Media Clustering: How to Group and Segment Your Social Media Users Based on Similarities. URL: https://fastercapital.com/content /Social-Media-Clustering--How-to-Group-and-Segment -Your-Social-Media-Users-Based-on-Similarities.html (дата обращения: 30.11.2024).

8. Минаев В.А., Мазин А.В., Здирук К.Б., Куликов Л.С. Цифровые двойники объектов в решении задач управления // Радиопромышленность. 2019. № 3. С. 68-78.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia

Московский государственный технический университет имени Н. Э. Баумана
Bauman Moscow State Technical University

Поступила в редакцию 01.12.24

Информация об авторах

Минаев Владимир Александрович – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

Толпыгин Алексей Сергеевич – канд. техн. наук, доцент кафедры защиты информации Московского государственного технического университета имени Н. Э. Баумана, e-mail: tolpygin@bmstu.ru

Кузьмина Ксения Александровна – студентка кафедры защиты информации Московского государственного технического университета имени Н. Э. Баумана, e-mail: ksenon2512@gmail.com

IDENTIFICATION AND TYPOLOGIZATION OF CRIMINAL ACTORS IN SOCIAL MEDIA

V.A. Minaev, A.S. Tolpygin, K.A. Kuzmina

The article considers the problem of identifying subjects in social media that can have a significant negative impact on other users. The main focus is on the use of clustering methods to divide users into groups and then calculate the centers of influence in each cluster. This technique is aimed at solving a number of tasks related to the prevention of cybercrime, such as identifying potentially dangerous audience segments, determining vectors for the spread of negative content and predicting the possible transition of users between clusters. The proposed method includes the stages of data preprocessing, converting them into a numerical format, standardization and selection of the optimal clustering model. Special attention is paid to the need to measure user ratings, such as the number of friends, publications and activity level. As a result, an information and analytical system is being created that makes it possible to effectively identify centers of influence in social media. The developed approach has the potential for practical application in the fight against cyber threats, providing support to law enforcement and security services in monitoring and analyzing online communities.

Keywords: cybercrime, terrorism, extremism, social media, typologization, identification of leaders.

Submitted 01.12.24

Information about the authors

Vladimir A. Minaev – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V. Ya. Kikot Moscow University of the Internal Affairs Ministry, Moscow, e-mail: m1va@yandex.ru

Aleksei S. Tolpygin – Cand. Sc. (Technical), Associate professor of the Information Security Department of Bauman Moscow State Technical University, Moscow, e-mail: tolpygin@bmstu.ru

Ksenia Al. Kuzmina – Student of the Information Security Department of Bauman Moscow State Technical University, Moscow, e-mail: ksenon2512@gmail.com