DOI 10.36622/VSTU.2022.25.4.007
УДК 004.056

ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС МОНИТОРИНГА МОЛОДЕЖНОЙ ИНТЕРНЕТ-АУДИТОРИИ

Д.Г. Плотников, И.А. Боков, А.А. Остапенко, С.В. Лихобабин, Р.Д. Бурцев, А.А. Сиделев

В работе рассматриваются принципы разработки программно-технического комплекса (ПТК) мониторинга молодежной интернет-аудитории социальных сетей для обмена контентами. Разрабатываемое прикладное программное обеспечение позволяет изучить сетевое пространство, а также оценить риски, связанные с деструктивной деятельностью пользователей подросткового возраста. Авторы обращают внимание читателя на острую необходимость наличия инструментария автоматизированного исследования молодежной аудитории интернет-пространства в плане реакции подростков на учащающиеся информационно-технологические атаки Запада. При этом предлагаются соответствующие проектные решения в отношении структуры входных и выходных данных ПТК, его модулей парсинга, классификации и баз данных. Результаты работы ПТК обязательно должны подвергаться глубокой аналитической обработке, выводы которой могут служить основой для адекватных профилактических мероприятий как в отношении рисковых тематических групп социальных сетей, так и отдельных их пользователей, склонных к девиантному поведению. Особо эффективной следует считать работу по оперативному противодействию фейкам (по возможности адресно) для наиболее рисковых категорий молодежной аудитории регионального социо-информационного пространства.

Ключевые слова: социальный сети, деструктивный контент, мониторинг, Netepidemic, риск.

Введение

Около 85% населения Российской Федерации является пользователями сети «Интернет», в том числе 68% являются активными пользователями различных тематических социальных сетей [1], где деструктивный контент наибольшее влияние оказывает на молодежную аудиторию сообществ, средний возраст которой варьируется в интервале 15-21 год, а в отношении некоторых медиа-сетей, в том числе для TikTok и Likee, может начинаться с детского возраста [2,3].

При этом риски влияния деструктивного контента на молодежную аудиторию в первую очередь связаны с рядом психологических особенностей исследуемой группы, в том числе: неокрепшим сознанием; попытками подражать своим «интернет-кумирам»; абсолютному доверием информации, циркулирующей в сети, в том числе сфальсифицированным историческим фактам; попыткам противопоставления себя обществу и отрицания сложившихся моральных, этических ценностей и устоев [4]. В этом случае мониторинг молодежной аудитории социальных сетей позволит в первую очередь выявить на ранних этапах и предотвратить девиаций поведения, таких как: отрицание семейных ценностей, попытки оправдания и реабилитации экстремисткой деятельности; разжигание национальной и религиозной розни, осуществление общественно-опасных деяний, направленных на нарушение интересов личности, общества и государства [5-7].

Исходные данные

Исходные данные мониторинга можно условно разделить на две обособленные категории: объекты мониторинга, настройки классификатора контента.

Основным объектом мониторинга выступает ареал молодежной аудитории региона, который может быть представлен различными способами, но наибольшую точность позволит достичь набор идентификаторов персонифицированных аккаунтов пользователей в исследуемых социальных сетях.

Набор идентификаторов позволяет установить однозначное соответствие между аккаунтом в социальной сети и реальной личностью, что позволит исключить коллизии, которые могут возникнуть, если ареал будет состоять из открытых персональных данных пользователей, которые не всегда позволяют верифицировать связь предполагаемого аккаунта с его владельцем (например, наличие в ареале однофамильцев, использование «ников» или псевдонимов).

Адекватной для анализа структурой ареала выступает набор кортежей для каждого пользователя, содержащих его идентификаторы в различных социальных сетях.

Формирование идентификаторов может производиться различными способами, в том числе посредством изучения открытой информации о пользователях, осуществивших аутентификацию через социальные сети в различных информационных ресурсах, образовательных платформах, маркет-плейсах и т.п.

Уместно настройки классификатора контента подразделить на [5-7]:

− категории контента — наиболее популярные в исследуемом ареале тематические группы, тематики контентов, в том числе деструктивных;

− библиотеки ключевых слов для каждой категории контента. Библиотеки ключевых слов и словосочетаний, характеризующие настроения (привязанности, устремления, ожидания, опасения и т.п.) автора аккаунта. Психологи и правоохранители должны регулярно актуализировать данную библиотеку с учетом складывающихся риск-реалий в области социальной безопасности;

− набор признаков, позволяющих классифицировать контент по степени опасности его автора, что открывает возможности применения превентивных мер, упреждающих террористические и прочие экстремистские акты в регионе;

− массивы данных (датасеты), в перспективе позволяющие использовать технологии искусственного интеллекта при классификации контента.

Модули и компоненты

Для мониторинга его структурно функциональная схема состоит из набора модулей. Рассмотрим каждый из этих модулей более подробно.

Модуль парсинга

Первичную обработку данных мониторинга должен проводить модуль парсинга.

Парсинг должен осуществляться в режиме многопоточности и многопроцессорности, что позволит наиболее оптимально использовать вычислительные ресурсы, тем самым избежать состояний «простоя» и «блокировки». Число необходимых потоков можно определить, зная точную мощность ареала и оценку границ допустимого времени, затрачиваемого на сканирование.

Элементарный поток содержит набор компонентов, каждый из которых создает сканер аккаунтов, сообществ и публикаций для каждой из исследуемой социальной сети. Необходимость написания уникального парсера под каждую сеть обусловлена типом представленных данных, особенностями API и ее тематической направленностью.

Структуру парсеров уместно рассмотреть на примере парсинга самой популярной российской социальной сети «Вконтакте» [5, 6].

В этом контексте потребуется разработать четыре отдельных парсера под различные сущности, используемые в социальной сети:

− парсер информации о пользователе. Данный компонент обязан собрать общую информацию, размещенную на странице пользователя. В первую очередь представляет интерес информация из блока «Обо мне», в котором чаще всего пользователи указывают свои увлечения, политические и религиозные предпочтения, любимые книги, фильмы, игры. Сбор подобных данных необходим как для определения первичного круга интересов пользователя, так и для своевременной актуализации ареала;

− парсер публикаций пользователя, размещенных на его странице. В социальной сети «Вконтакте» пользователь может

размещать на своей странице контент любых типов и категорий. Тематика данного контента представляет наибольший интерес для исследования, так как, в отличие от публикаций сообщества, можно утверждать, что контент на личной странице пользователя был им замечен и произвел информационно-психологическое воздействие на пользователя;

− парсер сообществ пользователя. Данный парсер должен собрать информацию о сообществах, страницах за контентом которых наблюдает текущий пользователь, и более точно сформировать его круг интересов;

− парсер публикаций в сообществах [5].

Очевидно, последовательный сбор информации менее оптимален по сравнению с алгоритмами параллельного сбора [6], однако повысить производительность можно, используя архитектуру «конвейера».

Суть конвейерной архитектуры заключается в работе циклами. На каждой итерации цикла (не считая первые 3 итерации после первого запуска модуля) одновременно будет функционировать каждый из парсеров, что позволит повысить эффективность работы по сравнению с последовательным сканированием в 4 раза (за один цикл будет производиться сбор информации о четырех отдельных пользователях).

В целях повышения эффективности, должен быть формализован механизм, позволяющий определить проводилось ли сканирование конкретного сообщества в рамках анализа интересов другого пользователя, и в случае, если сканирование уже было произведено, осуществить переход к следующему сообществу. Данная задача может быть решена введением дополнительных метрик.

На выходе модуля парсинга каждый объект исследования в качестве атрибутов будет иметь набор публикаций, сообществ, статусов и иной информации из различных социальных сетей (набор данных может варьироваться как и в зависимости от сети, так и цели исследования), позволяющих наиболее полно описать его круг интересов, что в свою очередь необходимо для оценки рисков деструктивного влияния, оказываемого на пользователя.

Модуль классификатора

Модуль классификации должен осуществлять наиболее важный этап мониторинга - выявление деструктивного контента и определения уровня его влияния на массовое сознание молодежной аудитории интернет-пространства.

Задачами модуля является:

− выявление контента с признаками деструктивности.

− классификация контента по заданным категориям деструктивности.

− классификация контента по уровню его влияния на сознание пользователей.

− распределение пользователей по ареалам вовлеченности по отношению к контенту.

Данные задачи могут быть решены с применением двух принципиально разных методов выявления и классификации деструктивного контента.

Первый метод заключается в глубоком лингвистическом анализе, основанном на сравнении текста с наборами ключевых слов, позволяющих отнести его к конкретной категории. Преимуществом данного метода является относительная простота реализации. Для успешного функционирования классификатора достаточно создать библиотеку словарей ключевых терминов и провести сравнение словарей с заранее обработанным исходным текстом публикации [5].

Классификация на основе словарей позволяет достаточно точно определять категорию деструктивного контента, однако словари требуют периодической актуализации психологами и сотрудниками правоохранительных органов. Другим критерием успешности метода является само содержание словарей и метод анализа сложных конструкций речи, таких как словосочетания, цельные предложения, фразеологизмы и иные литературные приемы.

При этом существенным недостатком является ориентированность метода на текстовую информацию, что не актуально на этапе развития стриминговых платформ и

видеохостингов. Для расширения метода на графическую, аудио- и видеоинформацию требуется написание дополнительных, промежуточных модулей распознавания текста на фотографиях, генерации субтитров и речевых преобразователей [8,9]. Кроме этого, метод абсолютно не может быть применен, если на изображении или в видеозаписи нет надписей, разговоров. Способом решения данной проблемы могут послужить внешние сервисы, позволяющие получать описание изображений в текстовом виде, однако это существенно замедляет работу программно-технического комплекса и зачастую требует дополнительных материальных ресурсов.

Используются также методы на основе средств машинного обучения. Суть данных методов заключается в обучении модели классификации на основе заранее размеченного датасета, которым может выступать набор текстов, изображений, аудиозаписей, видеороликов различной направленности с заранее указанной категорией деструктивности [10].

Достоинством метода является его универсальность для различных типов данных, однако существует ряд недостатков, таких как: слабая расширяемость; необходимость периодического переобучения модели; необходимость создания и грамотной разметки датасета, содержащего тысячи единиц классифицированных контентов и сам процесс обучения модели.

Весьма эффективен «Наивный байесовский классификатор». Это простой вероятностный классификатор, основанный на применении теоремы Байеса со строгими (наивными) предположениями о независимости. Метод позволяет определить вероятность, с которой контент относится к определенной категории. При этом точность метода существенно зависит от выборки данных, на которой производилось обучение.

Зачастую при оценке параметров для наивных байесовых моделей используют метод максимального правдоподобия. Другими словами, можно работать с наивной байесовской моделью, не веря в байесовскую вероятность и не используя байесовские методы. Несмотря на очень упрощенные условия, наивные байесовские классификаторы часто работают намного лучше нейронных сетей во многих сложных жизненных ситуациях [11,12].

Достоинством наивного байесовского классификатора является малое количество данных, необходимых для обучения, оценки параметров и классификации.

Далее классифицированный по категориям деструктивности контент необходимо также разделить по влиянию этого контента на сознание молодежной аудитории пользователей. Для этого необходимо совместно с психологами разработать и ввести ряд метрик, которые позволят создать «шкалу опасности» контента. Оценка опасности должна включать в себя не только предположение об опасности конкретной категории относительно иных, но и учитывать: тип представления этого контента; время публикации; аудиторию сообщества или число связанных аккаунтов, если контент был размещен на личной странице пользователя; реакции пользователей сообщества или владельцев связанных с пользователем аккаунтов на публикацию.

Для повышения точности оценка должна формироваться на различных этапах анализа и пересматриваться в течении «времени жизни» публикации, так как в динамике опасность контента может существенно меняться. Интегральные оценки опасности контента, его дискретные характеристики и ареалы пользователей (в зависимости их от вовлеченности) позволяют принять решение о противодействии и сформировать персональные и групповые информационно-психологические портреты пользователей.

Коннектор к базам данных

Коннектор к базам данных должен сгенерировать набор необходимых таблиц (в базе данных) и осуществить операции чтении и записи моделей пользователей. Из-за сложной и неоднородной структуры выходных данных применение базы данных одного типа не представляется возможным. По этой причине необходимо разработать архитектуру набора баз данных, которая будет включать в себя как реляционные базы данных (под управлением различных СУБД),

так и не реляционные базы данных для хранения информации о связях и кластерах сущностей. Наиболее оптимальным решением будет использование графовых баз данных (в дополнение к реляционным).

Отсюда следует организация самого модуля, который должен состоять из нескольких компонентов, обеспечивающих низкоуровневый доступ к каждому типу СУБД. С использованием нескольких баз данных так же возникает требование к организации и управлению процесса чтения-записи, которые могут быть решены введением в структуру блока управления потоками чтения и записи, функция которого заключается в разделении общего потока чтения-записи между несколькими базами данных, тем самым, предотвращая дублирование, потери данных, коллизии при записи однотипных данных. При необходимости на блок управления может быть возложена обязанность создания резервных копий всех таблиц и подключение к нему графического интерфейса для обработки данных экспертами.

Выходные данные

Выходным данными мониторинга являются:

− автоматизированная модель молодежного контингента, которая в интерактивном режиме позволит в различных социальных ракурсах и разрезах оценивать настроения, устремления, ожидания и др. грядущих поколений;

− прогностические оценки динамики характеристик социо-информационного пространства, прежде всего в его сегменте пользователей революционного возраста;

− в ходе анализа возникает ряд побочных данных, которые напрямую не влияют на данное исследование, однако могут быть использованы в дальнейших разработках по тематикам анализа социально-информационного пространства (например, статистика сообществ, попавших в исследование, данные о времени наибольшей и наименьшей активности пользователей, о продолжительности интереса к публикации в зависимости от типа их представления). Кроме того, выходные данные могут варьироваться в зависимости от типа социальной сети.

Заключение

Результаты работы нацелены на автоматизированной исследование предпочтений молодежной интернет-аудитории с перспективой реализации соответствующих мер по противостоянию или же поддержки в отношении как тематических групп, так и каждого пользователя в отдельности. Однако главной задачей мониторинга является риск-анализ воздействия деструктивов на психику наиболее подверженной влиянию аудитории, что позволит вовремя выявить возможные проблемы отдельных интернет-пользователей и с помощью квалифицированных психологов предотвратить совершение общественно-опасных деяний.

Практическую актуальность результатов настоящей работы объективно усиливают нарастающие риски деструктивного управления молодежью через ресурсы социо-информационного пространства. Именно поэтому подходы авторов легли в основу создания программно-технического комплекса автоматизированного мониторинга вышеуказанных ресурсов, которое в настоящее время реализуется в рамках проекта «Безопасный Интернет» [5-7].

Авторы выражают глубокую благодарность кафедре систем информационной безопасности Воронежского государственного технического университета, а также – исполнителям проекта «Безопасный Интернет» за предоставление актуального материала и полезные консультации по тематике и результатам настоящей работы.

В свете развития предлагаемого подхода и его практического применения уместно рассмотреть следующие вопросы. По большому счету, мы сегодня занимаемся «информационным разминированием». В течение десятков лет через СМИ и социальные сети в нашем сознании размещались психологические заряды (в том числе замедленного действия), изготавливаемые на Западе с целью

расчеловечивания российского общества. В первую очередь это минирование было ориентировано на неокрепшую психику молодого человека, который в отсутствие жизненного опыта и наличии юношеского максимализма при упущениях в его воспитании склонен к девиантному поведению. Этот фактор использовался различными иноагентами для «раскачивания лодки» нашего общества через акции протеста и неповиновения. Несмотря на многочисленные предостережения специалистов, государство до недавнего времени не уделяло должного внимания этой проблеме. Состоявшиеся наконец блокировки прозападных интернет-платформ несколько разрядили обстановку. Однако мины замедленного действия, размещенные до этого в молодежном сознании, продолжают работать, и их нужно обезвреживать. Для этого необходим мониторинг общественного сознания с использованием автоматизированных инструментариев, позволяющих оперативно и масштабно (желательно в реальном масштабе времени) анализировать информационно-психологические риски успеха деструктивного воздействия на различные категории отечественной молодежи, прежде всего в отношении старшеклассников и студентов. Настоящая работа в основном ориентирована на первое подмножество. Вместе с тем, предлагаемый инструментарий может быть развит и для студенческой интернет-аудитории.

Одним из сложнейших этапов мониторинга студенческой аудитории является процесс идентификации персональных аккаунтов в социальных сетях. В наиболее популярных сетях присутствует ряд штатных возможностей, позволяющих скрывать личные профили как от других пользователей, так и от специализированных автоматизированных систем. Среди факторов, усложняющих процесс идентификации, также стоит выделить высокую степень дисперсии в параметрах выборки: возраст, регион рождения, проживания, интересы, социальные группы. Из-за перечисленных особенностей не представляется возможным использовать методы машинного обучения в парсерах и классификаторах, так как большинство описанных методов основываются на анализе коэффициентов схожести по заранее определенным векторам.

Одним из немногих признаков, который позволяет идентифицировать большую часть множества студентов могут служить корпоративные сообщества в социальных сетях, такие как сообщества ВУЗов, отдельных факультетов, студенческих организаций как конкретного учебного заведения, так и региона в целом.

Поиск в привязке к студенческим сообществам в социальных сетях, позволяет значительно повысить точность идентификации аккаунтов при использовании минимального объема персональных данных (необходимыми являются: имя, фамилия, учебное заведение, остальные параметры лишь позволяют незначительно повысить точность идентификации при возникновении коллизий). Важной особенностью данного метода поиска является простая программная реализация алгоритма.

Другой особенностью данной аудитории, позволяющей облегчить процесс идентификации аккаунтов, является высокая степень связности элементов данного множества, что позволяет, идентифицировав одного пользователя, рекурсивно проанализировать связи его аккаунта (подписки, подписчики, сообщества, друзья, комментарии к публикациям других пользователей и ссылки на аккаунты в других социальных сетях) тем самым обнаружить или верифицировать аккаунты других элементов исследуемого множества.

Однако данная задача требует глубокого изучения структуры каждой конкретной социальной сети, с полным описанием ее функциональных элементов, типов связей для определения максимального уровня глубины рекурсии, позволяющего использовать алгоритм наиболее эффективно и в то же время снизить процент повторного сканирования одних и тех же аккаунтов.

Подобный алгоритм позволяет проводить идентификацию аккаунтов и для других множеств пользователей, обладающих высокой связностью между собой, однако использование рекурсии

требует тщательной проработки архитектуры приложения из-за необходимости высоких объемов вычислительных ресурсов, существенно возрастающих с мощностью искомого множества.

Список литературы

1. Интернет и соцсети в России в 2021 году — вся статистика. URL: https://www.web-canape.ru/business/internet-i-socseti-v-rossii-v-2021-godu-vsya-statistika/ (Дата обращения: 10.11.2021).
2. Статистика TikTok – 29 показателей [на конец 2021 года] URL: https://logotip.online/blog/statistika-tiktok/ (Дата обращения: 10.11.2021).
3. Likee – итоги 2019 года: Приложение, которое растет быстрее всего в мире. URL: https://youngspace.ru/internet/likee-itogi-2019 (Дата обращения: 10.11.2021).
4. Влияние социальных сетей на молодежь. URL: https://tjournal.ru/u/368803-dias-azimov/253418-vliyanie-socialnyh-setey-na-molodezh (Дата обращения: 10.11.2021).
5. Остапенко А.Г., Чапурин Е.Ю., Соколова Е.С., Зимницкий А.Г., Боков И.А., Программное обеспечение для мониторинга процессов восприятия и распространения деструктивного контента в социальных сетях. // Информация и безопасность. 2019. Т. 22. № 2. С. 188-205.
6. Железняк В.П., Чапурин Е.Ю., Боков И.А. Структурно-функциональная формализация процедур риск-мониторинга региональных пабликов. // Информация и безопасность. 2019. Т. 22. № 4. С. 573-586.
7. Остапенко А.Г., Боков И.А., Остапенко А.А., Лантюхов Н.М., Мирошниченко Т.Ю., Лихобабин С.В., Трубицын С.Д. Научно-технические результаты и перспективы реализации проекта «Безопасный интернет». // Информация и безопасность. 2021. Т. 24. № 2. С. 287-296.
8. Потапов А.С. Системы компьютерного зрения: учебное пособие. СПб: Университет ИТМО, 2016. 161 с.
9. 6 способов перевести аудио и видео в текст. URL: https://yagla.ru/blog/marketing/6-sposobov-perevesti-audio-i-video-v-tekst--2110m94955/ (Дата обращения: 10.11.2021).
10. Обзор методов классификации в машинном обучении с помощью Scikit-Learn. URL: https://tproger.ru/translations/scikit-learn-in-python/ (Дата обращения: 10.11.2021).
11. Наивный Байес, или о том, как математика позволяет фильтровать спам. URL: https://habr.com/ru/post/415963/ (Дата обращения: 10.11.2021).
12. Наивный байесовский классификатор. URL: https://ru.wikipedia.org/wiki/Наивный_байесовский_классификатор (Дата обращения: 10.11.2021).

Правительство Воронежской области
Government of the Voronezh region

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 28.04.2022

Информация об авторах

Плотников Денис Геннадьевич – канд. техн. наук, директор центра цифровой трансформации образования ВИРО им Н.Ф. Бунакова, e-mail: mnac@comch.

Боков Илья Александрович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Остапенко Александр Алексеевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Лихобабин Сергей Викторович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Бурцев Роман Дмитриевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Сиделев Алексей Ахмадович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

SOFTWARE AND HARDWARE COMPLEX FOR MONITORING THE YOUTH INTERNET AUDIENCE

D.G. Plotnikov, I.A. Bokov, A.A. Ostapenko, S.V. Likhobabin, R.D. Burtsev, A.A. Sidelev

The paper discusses the principles of developing a software and hardware complex (STC) for monitoring the youth Internet audience of social networks for the exchange of content. The developed application software allows you to explore the network space, as well as assess the risks associated with the destructive activities of adolescent users. The authors draw the reader's attention to the urgent need for tools for automated research of the youth audience of the Internet space in terms of the reaction of adolescents to the increasing information technology attacks of the West. At the same time, appropriate design solutions are proposed regarding the structure of the input and output data of the PTC, its modules for parsing, classification and databases. The results of the work of the PTK must necessarily be subjected to deep analytical processing, the conclusions of which can serve as the basis for adequate preventive measures both in relation to risky thematic groups of social networks and their individual users prone to deviant behavior. Particularly effective should be considered the work on operational counteraction to fakes (targeted if possible) for the most risky categories of the youth audience of the regional socio-information space.

Keywords: social networks, destructive content, monitoring, Netepidemic, risk.

Submitted 28.04.2022

Information about the authors
Denis G. Plotnikov – Cand. Sc. (Technical), Director of the Center for Digital Transformation of Education VIRO named after N.F. Bunakova, e-mail: mnac@comch.ru
Ilya A. Bokov – Student, Voronezh State Technical University, email: mnac@comch.ru
Alexander A. Ostapenko – Student, Voronezh State Technical University, e-mail: mnac@comch.ru
Sergey V. Likhobabin – Student, Voronezh State Technical University, e-mail: nmac@comch.ru
Roman D. Burtsev– Student, Voronezh State Technical University, e-mail: nmac@comch.ru
Alexey A. Sidelev– Student, Voronezh State Technical University, e-mail: nmac@comch.ru