Методика выявления каналов распространения информации в социальных сетях*

А. А. Проноза¹, Л. А. Виткова¹, А. А. Чечулин¹, И. В. Котенко¹, Д. В. Сахаров²

¹ Санкт-Петербургский институт информатики и автоматизации
Российской Академии наук, Российская Федерация,
199178, Санкт-Петербург, 14-я линия В. О., 39

² Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича, Российская Федерация,
193232, Санкт-Петербург, пр. Большевиков, 22, корп. 1

Для цитирования: Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. Т. 14. Вып. 4. С. 362–377. <https://doi.org/10.21638/11702/spbu10.2018.409>

Целью работы является разработка методики выявления каналов распространения информации в социальных сетях. Предложенная методика базируется на формировании базы знаний о связях между пользователями и группами, интерактивном отображении путей распространения информации и визуальном анализе полученных результатов для определения источников и ретрансляторов информации. Взаимосвязи пользователей и групп в социальной сети позволяют строить графы связности, а факты передачи информации через эти каналы дают возможность устанавливать пути распространения контента. В статье приведены результаты экспериментов, подтверждающих применимость описанной методики.

Ключевые слова: социальная сеть, визуализация, защита от информации, нежелательная информация, граф связей, визуальная аналитика.

1. Введение. Современные проблемы в области информационно-психологической безопасности общества и государства требуют от специалистов выработки новых методик в области мониторинга и противодействия угрозам, исходящим из информационного пространства социальных сетей.

Современные социальные сети — не только средство общения, но и инструмент для извлечения знаний о субъектах и объектах в социальных сетях, о связях между пользователями и группами. Кроме того, это удобная платформа для анализа данных о распространении информации. Современные исследования, например «Социальные сети в России: цифры и тренды», свидетельствуют о том, что количество «пишущих» авторов только в мае 2017 г. в социальной сети «ВКонтакте» составило 25.7 млн человек, при этом они создали около 310 млн сообщений [1].

Одной из задач анализа информационных потоков является обнаружение ретрансляторов, каналов распространения и источников информации. Анализ каналов распространения информации в социальных сетях позволяет выявить основные информационные потоки, содержащие нежелательный контент, что, несомненно, относится к актуальным задачам. В данной статье предложена методика выявления ка-

* Работа выполнена при частичной финансовой поддержке Российского научного фонда (проект № 18-71-10094).

© Санкт-Петербургский государственный университет, 2018

налов распространения информации. Она включает в себя несколько этапов: на первом — реализуется алгоритм сбора данных из социальных сетей; на втором — происходят предобработка неструктурированных данных, сортировка, анализ ретрансляторов и контента; на третьем — осуществляются визуальное представление и анализ данных, полученных из социальных сетей.

С помощью информации о репостах в публичных сообществах социальной сети созданная методика позволяет установить наиболее вероятные источники ввода информации. На основе данных о репостах и просмотрах информационных объектов методика дает возможность отобразить пути распространения информации по социальной сети и их характеристики. Такое представление помогает оператору выделить из множества полученных данных основные пути распространения информации.

Новизна предложенной методики состоит в разработке новых алгоритмов сбора данных об информационных объектах и отображения результатов, позволяющих эффективно проводить визуальный анализ информации. Предположим, что такая методика может применяться для повышения уровня защищенности пользователей социальных сетей от информационно-психологического воздействия.

Необходимо отметить, что при визуализации каналы распространения информации одновременно являются и средой передачи, и объектами, обладающими собственными характеристиками. Так, взаимосвязи объектов в социальной сети дают возможность строить графы, а визуализированный путь распространения информации через одни и те же ретрансляторы — выявлять пути контента.

Основной вклад исследования определяется повышением уровня защищенности информационного пространства социальных сетей за счет интеллектуального анализа каналов распространения информации. Осведомленность о путях распространения поможет оказывать противодействие целенаправленным вбросам информации.

В статье также проведен краткий обзор работ в области анализа социальных сетей, подходов, использующих графы взаимосвязей, а также обзор современных работ по визуализации данных. Применимость предлагаемой методики подтверждается результатами экспериментов.

Статья организована следующим образом. В п. 2 дан обзор литературы, посвященной анализу социальных сетей и использованию методов визуализации. Предлагаемая методика выявления каналов распространения информации описана в пп. 3 и 4. В п. 5 приведены результаты проведенных экспериментов и пример визуального анализа распространения информации. В п. 6 проанализированы результаты, выявлены их достоинства, недостатки и области возможного применения. В п. 7 подведены итоги и определены направления дальнейших исследований.

2. Обзор релевантных работ. Настоящая статья является продолжением предыдущих работ авторов, в которых были предложены методы выявления и противодействия нежелательной информации на отдельных веб-страницах сети Интернет. Общий подход к классификации веб-страниц был рассмотрен в [2]. Такой подход был основан на анализе различных аспектов веб-страниц для определения тематической направленности. Основным аспектом, который использовался для установления категории, был текст веб-страницы. Однако в результате экспериментов авторы пришли к выводу, что текст не подходит для анализа таких категорий веб-сайтов как, например, «новости», «блоги» и «социальные сети». Это обусловлено тем, что веб-страницы данных категорий могут содержать одновременно тексты, посвященные различной тематике. Для выявления таких категорий было предложено применять структурные особенности веб-страниц [3]. Общий подход, объединяющий анализ тек-

стового содержимого, структурных особенностей и URL-адреса, представлен в [4]. Он позволяет с достаточно высокой точностью определять категорию веб-страницы, что было доказано результатами экспериментов. Однако при работе с категорией «социальные сети» было обнаружено, что важной информацией являются не только категория конкретного информационного объекта (сообщения, группы и т. д.), но и пути распространения данной информации. Выявление источников и ретрансляторов информации значительно повышает эффективность методов противодействия.

Дальнейший обзор структурирован следующим образом: в начале рассматриваются подходы к анализу социальных сетей, основанные на потоковых методах и на концепции социально-сетевого анализа (Social network analysis, SNA); далее приведен анализ исследований, направленных на визуализацию больших данных.

В работе [5] установлено, что анализ недостающих узлов в связях, которые возникают или только могут возникнуть в социальных сетях, может повысить эффективность прогнозов и моделирования развития событий. При этом авторы [5] опираются на анализ нечетко структурированных динамических систем, хотя для визуализации также используют граф, но цель проанализировать потоки или улучшить качество представления информации на графе перед собой не ставят.

Среди исследований, направленных на анализ взаимосвязей объектов, стоит выделить работы коллектива Института системного программирования РАН [6, 7]. В них предложен стек технологий для анализа объектов социальных сетей. Основными компонентами стека являются компоненты поиска неявных сообществ пользователей, идентификации пользователей различных социальных сетей, определения демографических атрибутов, измерения информационного влияния между пользователями в социальных сетях, а также генерации графов, визуализирующих структуры сообществ пользователей.

Авторы [8] выявили связь между объектами социальной сети и проанализировали закон распределения связей между узлами. Они показали, что узлы в сетях связаны асимметрично, для социальной сети справедливо распределение узлов по числу связей в виде степенного закона (безмасштабное распределение узлов по числу связей), т. е. в такой сети отсутствуют узлы с типичным числом связей (Scale-free networks). Также значимые научные работы — это исследования взаимовлияния объектов социальной сети (в том числе подходы, основанные на использовании понятий «структурные пустоты» и «информационный купол» [9], «информационные каскады» [10] и др.).

Активно развивается такое направление как социально-сетевой анализ (SNA). Это способ изучения социальных сетей как набора сущностей, между которыми есть определенные отношения. В SNA величина позитивной корреляции узла социальной сети характеризуется такими индикаторами как степень (degree), собственный вектор (eigenvector), мера близости (closeness) и центральность к посредничеству (betweenness-centrality). Таким образом, в процессе анализа выделяют наиболее популярные (влиятельные) узлы и их связи с другими объектами. В [11] описана социальная связанность с использованием трех различных индексов: центральная степень (Degree centrality) как показатель распределения уровня власти и влияния в сети, близость узла к центру сети и его взаимосвязь с центром других узлов.

Была выдвинута гипотеза о том, что в социальной сети пользователей можно разбить на кластеры неформальной организации и визуализировать по кластерам [12]. Визуализация на основе кластеризации повышает уровень восприятия информации при получении графа из социальной сети, позволяет разбить граф по определенным

категориям (цветовым группам) и выделить основные направления связи объектов. При этом стоит отметить, что в этой работе введены в сетевом взаимодействии ключевые понятия «владелец», «проектировщик» и «подрядчик».

В статье [13] предложен подход к автоматизированному анализу президентских выборов в США с помощью технологий больших данных и сетевого анализа. В результате работы разработанного парсера строится сеть с положительными и отрицательными гранями между субъектами и формируется визуальная карта распространения информации об основных кандидатах предвыборной гонки и их разделения в социальной сети.

Сочетание анализа контента, СМИ, журналов и анализа социальных сетей для изучения социального взаимодействия рассмотрено в [14]. Предлагаемый авторами метод может быть также использован для анализа информационных каналов и прогнозирования путей противодействия вредоносному воздействию.

Авторы [15] считают, что люди погружены в социальную сеть и технологии, и говорят о необходимости анализа больших, гетерогенных, данных. В настоящее время очень популярны исследования в области визуализации представлений больших данных. Например, С. В. Мельман и др. [16] предлагают технологию создания системы визуализации больших объемов синоптических данных, применяя распределенные и гетерогенные (параллельные/гибридные) вычисления.

Решения для кластерного анализа и визуализации больших объемов данных рассмотрены в [17], где предложена система, предназначенная для загрузки, нормализации и анализа входных данных, проведения кластерного анализа, визуализации и сохранения его результатов.

В. Авербух и Д. Манаков [18] утверждают, что для визуализации больших объемов данных необходимо использование дополнительных аппаратных и программных средств компьютерной графики. Требуются анализ и моделирование поведения пользователей, оценка и измерение качества визуальных и интерактивных систем.

Таким образом, по мере того, как масштабы социальных медиа и количество пользователей растут, анализ социальных сетей становится важным инструментом для экспертов и исследователей в области социальных вычислений. Информационное воздействие часто оказывается через страницы пользователей в их постах. Визуализация путей распространения может помочь частично автоматизировать анализ информационных потоков и повысить уровень защищенности информационного пространства социальных сетей.

Анализ современного состояния работ показывает, что они в основном направлены на изучение качественных или количественных характеристик связей узлов в социальных сетях, кластеризацию полученных данных, систематизацию и хранение. При этом задача исследования каналов распространения информации для повышения уровня защищенности пользователей социальных сетей от информационно-психологического воздействия сейчас не ставится. Потому визуальный анализ каналов распространения информации весьма актуален в области социальных сетей и информационной безопасности.

3. Сбор данных. Сбор, предварительная обработка и организация хранения данных являются важнейшим этапом при изучении социальных сетей. На данном этапе решаются одновременно несколько технических задач, таких как обход блокировок со стороны социальной сети, нормализация данных, проектирование подсистемы хранения и др. В качестве комплексного решения возникающих трудностей может использоваться кэширование собираемой информации, которое позволит снизить на-

грузку на социальную сеть при проведении повторных исследований, уменьшая тем самым число блокировок с ее стороны.

Информация, поступающая из социальной сети, имеет разнородную структуру с разными степенями вложенности, которая может со временем существенно изменяться. Возможность хранить слабоструктурированные данные — важнейшее требование к подсистеме хранения. Алгоритм сбора данных, в свою очередь, выполняет запросы к социальной сети только в случаях отсутствия информации в хранилище или потери ее актуальности.

Сбор данных для решения задачи обнаружения каналов распространения информации в социальной сети и их кэширование требуют огромного количества ресурсов, если основываться лишь на информационном наполнении объектов социальной сети. Например, для поиска каналов распространения изображения может потребоваться выгрузить и сравнить между собой все изображения, опубликованные в социальной сети, чтобы затем выстроить их в хронологическом порядке по дате публикации и выявить тем самым канал распространения. Однако на практике реализовать такой подход крайне сложно, поэтому при формировании алгоритма сбора данных целесообразно основываться на функциональных возможностях социальной сети, чем на содержании опубликованных объектов.

Социальная сеть может быть представлена как совокупность взаимосвязанных объектов Z . Примерами объектов могут служить пользователь, сообщество, пост, вложение и т. д., а примерами связей между объектами — одноуровневые отношения (состоят «в друзьях», состоят в сообществе и т. п.) и отношения вложенности (пост содержит вложение, профиль пользователя включает ссылку на родственника и т. п.). На самом высоком уровне представления объектами социальной сети являются ее пользователи U и сообщества G , при этом

$$U \cup G \subseteq Z.$$

Под пользователем будем понимать объект, имеющий персональную страницу, закрепленную за определенным аккаунтом (человеком), под сообществом — самостоятельный комплексный объект социальной сети, обладающий собственными страницами. Пользователи могут создавать и участвовать в сообществах. Будем также подразумевать, что информационное наполнение страниц пользователей и страниц сообществ происходит по схожим принципам.

Отметим, что в ходе этапа сбора данных информация об отношениях вложенности между объектами заранее известна и автоматически помещается в хранилище вместе с самими объектами.

Рассмотрим в качестве связи между объектами отношение «репост», реализованное во многих социальных сетях. Два объекта q_s и q_d находятся в отношении «репост» $q_s R q_d$, если произведено непосредственное копирование объекта q_s в объект q_d штатными средствами социальной сети, с сохранением ссылок как на факт копирования, так и на исходный объект. При этом можно утверждать, что $q_s \in q_d$. В таком случае объект q_s называется источником копирования, а объект q_d — приемником. В зависимости от конкретной социальной сети история копирования может быть сохранена и представлена различными способами.

Наличие в отношениях «репост» обязательных ссылок на исходный объект и факт копирования позволяют прийти к выводу, что данный вид отношений является одним из наиболее эффективных способов выявления каналов распространения информации в социальных сетях.

Таким образом, целью алгоритма сбора данных для анализа каналов распространения информации в социальных сетях будет сбор сведений об объектах, состоящих в отношении «репост».

Более формально алгоритм сбора данных можно описать следующим образом. Пусть функция $Q(u)$ определяет все источники копирования множества объектов $\{q_s\} \subset u$:

$$Q(u) = \{q_s \mid \exists q_d \in u : q_s R q_d\}, \quad u \in Z.$$

Например, результатом работы функции $Q(u)$ на «стене» страницы в социальной сети «ВКонтакте» стали бы все записи пользователей или сообществ, которые объект u хотя бы единожды «репостили».

Определим алгоритм сбора данных следующим образом. Пусть $X \subseteq Z$ — множество исходных объектов социальной сети. На первом шаге алгоритма для каждого исходного объекта $u \in X$ следует выделить множество объектов Q_0 , являющихся источниками копирования:

$$Q_0 = \bigcup_{u \in X} Q(u).$$

На i -м шаге алгоритма для всего множества обнаруженных объектов Q_i при помощи рекуррентной функции F_i необходимо итеративно получать все объекты, состоящие в отношении «репост» с объектами, определенными на предыдущем шаге:

$$F_1(Q_0) = \bigcup_{q_i \in Q_0} R(q_i) = Q_1,$$

$$F_n(Q_{n-1}) = \bigcup_{q_i \in Q_{n-1}} F_{n-1}(q_i) = Q_n.$$

Алгоритм заканчивает свою работу на шаге n , если $F_n(Q_{n-1}) = \emptyset$.

Отметим, что в ходе работы алгоритма формируется также множество объектов $U' \subseteq Z$, представляющее собой пользователей или сообщества социальной сети, содержащие объекты q , которые, в свою очередь, состоят между собой в отношении «репост»:

$$U' = \left\{ u \in Z \mid \exists q \in u : q \in \bigcup_{i=0}^{n-1} Q_i \right\}.$$

Таким образом, можно построить направленный граф $N' = (U', E')$, в котором вершинами являются такие объекты социальной сети как пользователь или группа, а наличие ребра между ними определяется наличием в них объектов q_s и q_d , состоящих в отношении «репост»:

$$\forall u_s, u_d \in U' \exists (u_s, u_d) \in E' \leftrightarrow \exists q_s \in u_s \wedge q_d \in u_d : q_s R q_d.$$

В свою очередь, объект $q \in u$ может содержать совокупность информационных атрибутов $a \in I$ (текст поста, число просмотров, прикрепленный мультимедиа контент и т. п.). Объекты социальной сети, включающие информационные атрибуты, будем называть информационными. Множество всех информационных объектов $\tilde{Q}^u \subset u$ объекта $u \in Z$ составляет его информационное пространство:

$$\tilde{Q}^u = \{\tilde{q} \in u \mid \exists a : a \in I \wedge a \in \tilde{q}\}, \quad u \in Z.$$

Далее будет рассматриваться только текстовое наполнение информационного пространства объектов социальной сети.

При передаче информации от источника распространения дальше по цепочке можно наблюдать факт «затухания» или «искажения» первоначальной информации. Для исследования этого феномена сбор данных об объектах социальной сети должен включать также сбор сведений об их информационном пространстве. Схема алгоритма сбора данных об отношениях «репост» между объектами социальной сети приведена на рис. 1.

Для оценки степени искажения информации по мере перемещения исходного объекта по цепочке распространения необходимо подвергнуть собранные данные предварительной обработке. В качестве механизма обработки текстового наполнения информационных объектов предлагается использовать метод вычисления ключевых слов, реализованный, например, в системе по созданию русскоязычного корпуса для автоматического перефразирования и поиска синонимов «ParaPhraser» [19].

Рис. 1. Схема алгоритма сбора данных

Формально алгоритм предобработки информационного пространства объектов может быть записан следующим образом.

Пусть $K(\tilde{Q}^u)$ — функция вычисления k ключевых слов по информационному пространству объекта $u \in Z$. Параметр k может иметь произвольные значения и задается вместе с набором входных данных X перед началом исследования.

На первом шаге следует вычислить ключевые слова для всех n информационных пространств исходных объектов:

$$K^S = K(\tilde{Q}^{u_1} \cup \dots \cup \tilde{Q}^{u_n}), \quad u_i \in X.$$

На втором шаге ключевые слова рассчитываются для каждого информационного пространства объекта приемника:

$$K^d = K(\tilde{Q}^d), \quad d \in U' \setminus X.$$

Степень сохранения изначального контекста P^d в информационном пространстве объекта приемника d определяется по формуле

$$P^d = \frac{|K^d \cap K^S|}{|K^S|}.$$

Полученное в результате применения алгоритма значение P^d указывает на степень схожести информационных пространств источников и приемников. Далее, для наглядности, указанная величина будет представлена в процентах.

Алгоритм сбора и предварительной обработки данных позволяет получить информацию о каналах распространения информации, построенных на штатных функциональных возможностях социальной сети. Все данные могут быть сохранены в любом NoSQL-хранилище для последующей обработки. Однако в сыром виде собранная информация крайне затруднительна для понимания и анализа человеком.

4. Визуализация. Для изучения результатов, полученных по окончании этапа сбора данных, целесообразно разработать графическую схему, предоставляющую возможность проведения их визуального анализа.

Существует множество способов графического представления связанных разнородных объектов [20], однако для отображения объектов социальной сети и их взаимосвязей целесообразно использовать граф, вершинами которого являются пользователи или группы, а ребрами — наличие отношения «репост» между входящими в них объектами (вес ребра определяется количеством таких отношений между двумя объектами, направление ребра — от источника к приемнику).

Визуализация в виде графа предоставляет множество атрибутов для повышения информативности изображения: форма, размер, цвет вершины, толщина и направление ребра и т. п. При необходимости дополнительная информация может быть также представлена в подписях к вершинам. Заметим, что все показатели, вычисляемые для объектов социальной сети, зависят от временного интервала — периода проведения исследования.

При помощи собранных данных можно также вычислить дополнительные показатели, имеющие значение для информационного насыщения визуализации.

Информационный атрибут «количество просмотров» $Views(u)$ дает численное представление об аудитории, обратившей внимание на соответствующие объекты $\tilde{Q}^u$ пользователя u , и может быть определен по формуле

$$Views(u) = \frac{\sum_{j=1}^k V(\tilde{q}_j)}{K}, \quad \tilde{q} \in \tilde{Q}^u.$$

Чем больше среднее число просмотров $Views(u)$, тем на большую аудиторию оказывает влияние объект u социальной сети.

Другим важным показателем объекта u социальной сети может быть уникальность генерируемого им контента, вычисляемая как отношение числа информационных объектов $\tilde{Q}_s^u$, состоящих в отношении «репост» с другими информационными объектами, к общему числу информационных объектов:

$$Unique(u) = \frac{\tilde{Q}_s^u}{\tilde{Q}^u}.$$

Этот показатель помогает установить, является ли данный объект социальной сети источником, потребителем, агрегатором или ретранслятором информации.

В качестве количественного показателя $Flow(u_1, u_2)$, оценивающего информационные потоки между двумя объектами социальной сети, предлагается использовать следующую величину, равную разности числа взаимных «репостов»:

$$\begin{aligned}\tilde{Q}_s^{u_1} &= \{q_i \mid \exists q_j \in u_2 : q_j \text{ } R \text{ } q_i\}, \\ \tilde{Q}_s^{u_2} &= \{q_i \mid \exists q_j \in u_1 : q_j \text{ } R \text{ } q_i\}, \\ Flow(u_1, u_2) &= |\tilde{Q}_s^{u_1}| - |\tilde{Q}_s^{u_2}|.\end{aligned}$$

От знака показателя $Flow(u_1, u_2)$ будет зависеть направление информационного потока.

Также в настоящей работе предложен метод, позволяющий найти показатель P^u , определяющий фактор «затухания» исходной информации в информационном пространстве объекта u социальной сети. С помощью данного показателя можно установить, насколько изменяется контекст информационного пространства объектов социальной сети по мере движения информационных объектов по цепочке отношений «репост».

Применяя представленные показатели, можно выделить следующие типы объектов социальной сети, участвующих в информационном взаимодействии:

- источник информации — объект, содержащий высокую долю уникального контента и являющийся отправной точкой для информационного наполнения других объектов сети;
- ретранслятор информации — объект с низкой долей уникального контента, который воспроизводится другими участниками информационного обмена;
- агрегатор информации — объект, размещающий чужой контент при большом охвате аудитории;
- потребитель информации — объект, активно размещающий на своей странице заимствованный контент, не пользующийся большим интересом у аудитории и не имеющий дальнейшего распространения.

Поскольку при визуализации данных необходимо соблюдать баланс между информативностью и простотой восприятия выводимых данных [21], следует разработать схему визуального представления данных и использовать методы для их фильтрации.

В табл. 1 приведен набор предлагаемых к отображению показателей и соответствующие характеристики графа для их представления.

Таблица 1. Метрики визуальной аналитики и способы их представления

Характеристика	Показатель
Вершина (размер)	Среднее число просмотров
Вершина (форма)	Тип объекта
Вершина (цвет)	Уникальность генерируемого контента
Вершина (подпись)	Оценка изменения контента
Ребро (толщина / вес)	Информационный поток
Ребро (направление)	Направление информационного воздействия
Ребро (цвет)	Уникальность генерируемого контента

Направление ребра может означать либо информацию об источнике и приемнике объектов, либо указывать на направление информационного воздействия одного объекта на другой. Далее под направлением ребер графа подразумевается информационное воздействие источника информации на ее приемник.

Описанный подход к визуализации позволяет отобразить в понятной форме все элементы схемы распространения информации. Основанный на графах метод представления информационных потоков дает возможность визуально устанавливать основные источники и ретрансляторы информации, выявлять пути ее распространения, а также открывает возможности для выработки алгоритма дальнейшего противодействия распространению потенциально опасной информации.

5. Эксперименты. Для оценки эффективности представленных алгоритмов и информативности их работы приведем результаты экспериментов, в которых поставлена задача при помощи визуальной аналитики выявить следующие объекты: источники информации, ее потребители, агрегаторы и ретрансляторы, каналы распространения и точки, в которых происходит ее «затухание».

Эксперименты проводились на базе социальной сети «ВКонтакте» как наиболее популярной социальной площадке в российском сегменте Интернета. Как исходные данные для экспериментов был выбран ряд сообществ и пользователей, тем или иным образом связанных с поклонением Кришне.

В качестве временного интервала t взято 7 дней до момента проведения расчетов. Далее для всего информационного пространства исходных данных, составляющего 125 646 знаков, подсчитаны ключевые слова. В связи с имевшимися на момент проведения экспериментов техническими ограничениями шаг 3 алгоритма сбора данных выполнялся начиная с групп, вошедших в исходные данные.

Общий вид графа отношений «репост» приведен на рис. 2 (см. URL: <http://comsec.spb.ru/img/papers/vestnik/>). Для упрощения визуального представления общей картины произведена фильтрация конечных вершин, которые не являются источниками информации для других объектов социальной сети, форма вершин не зависит от типа источника, а также убраны надписи к вершинам.

Рис. 2. Граф отношений «репост»

Представленный граф дает целостную картину информационных потоков между объектами социальной сети. Для более очевидного примера рассмотрим подграф, показанный на рис. 3 (см. URL: <http://comsec.spb.ru/img/papers/vestnik/>).

Рис. 3. Подграф отношений «репост»

Для обозначения типа объекта u социальной сети используется форма вершины. В частности, в изучаемом подграфе форма «ромб» относится к сообществам («Центр общ...», «Культурный...», «Харе Кришн...» и т. д.), а форма «круг» — к пользователям («Serg Nigri...», «Евгений Ка...», «Анастасия...» и др.).

Размер вершины определяет среднее число просмотров сообщений на «стене» пользователя или группы. На рис. 3 наибольшим охватом аудитории обладают сообщества «Центр общ...», «Культурный...», «Центр Веди...», «Харе Кришн...» и др.

Цвет вершины описывает уникальность контента, генерируемого пользователем или сообществом. Чем ближе цвет вершины к ярко-зеленому, тем более уникальным контентом обладает объект социальной сети. Вершины красного цвета содержат в основном копии («репосты») сообщений из других источников. Отметим, что при окрашивании вершин используется целый диапазон цветов, от зеленого к красному, и, таким образом, вершины, содержащие равное число уникальных постов и «репостов», имеют коричневый цвет. В частности, к вершинам с наиболее уникальным контентом можно отнести сообщества «Центр общ...», «НРИСИМХ...», «Харинома в...», «Фестиваль...» и «Экологичес...». Наименее уникальным контентом обладают почти все представленные в подграфе пользователи и сообщества «Общение с...», «Прославлен...» и др. Пользователь «Юрий Губанов», а также сообщества

«Центр Веди...», «Культурный...» и «Akhandha Na...» публикуют как новый контент, так и заимствованный из других источников.

Используемая цветовая схема применима и для связей — цвет ребер повторяет цвет вершины-источника и указывает на уникальность распространяемого контента. Из приведенного подграфа видно, что основными источниками информации являются сообщества «Центр обще...» и «НРИСИМХ...», в то время как сообщество «Харе Кришн...» — агрегатор контента. К потребителям информации следует отнести пользователей «Евгений Ка...», «Светлана Г...», «КарунаНидх...» и др.

Ретранслятором в приведенном подграфе является пользователь «Ольга Скор...», заимствующая информацию от сообщества «НРИСИМХ...» и транслирующая ее пользователю «Светлана Г...» и сообществам «Общение с ...» и «Прославлен...». Отметим, что, несмотря на большое число заимствований, данный пользователь также производит собственный контент.

В ходе исследования по множеству исходных данных подсчитаны их ключевые слова при помощи сервиса [19]. В качестве примера затухания информации рассмотрим следующий канал распространения информации: «Харе Кришн...» — «Анастасия...» — «Ольга Золо...». В табл. 2 приведены ключевые слова, подсчитанные для каждого информационного объекта, а также доля содержания в них исходных слов. Представленные данные позволяют предположить об изменении контекста заимствованной информации по мере ее появления на «стенах» других пользователей. Это позволяет говорить о затухании исходной информации.

Таблица 2. Пример затухания информации

Объект	Ключевые слова	Доля, %
«Харе Кришн...»	Кришна, шри, экадаши, господь, падмини, прабхупад, госвами, шрила, харя, бхакти, божество, пурушоттам, вриндаван, всевышний, джаганнатх	100
«Анастасия...»	Кришна, прабхупад, шрила, харя, шри, госвами, господь, божество, ребенок, сваи, бхакти, чайтанья, служение, совершенство, бог	60
«Ольга Золо...»	Кришна, харя, прабхупад, рама, шрила, вриндаван, радхи, божество, сваи, гопи, повелитель, господь, шри, махараджа, бхактиведанта	53

Таким образом, визуальный анализ дает возможность находить основные информационные потоки и выделять ключевые узлы в сети передачи информации (источники, потребители, агрегаторы и ретрансляторы). Дополнительные сведения, отображаемые в надписях к вершинам, помогают установить отличие информационной повестки конкретного объекта социальной сети от исходной.

6. Анализ полученных результатов. В данной работе представлена методика выявления каналов распространения информации в социальных сетях. Предполагается, что она позволит получать информацию о каналах распространения нежелательной информации, каналов информационно-психологического воздействия с выделением источников, ретрансляторов, агрегаторов и потребителей.

Отправной точкой для сбора информации и визуализации каналов ее распространения является отношение «репост» между двумя информационными объектами, которое фиксируется средствами самой социальной сети. В то же время при таком подходе из поля зрения исчезают сообщения-клоны, подготовленные пользователями вручную и появляющиеся в социальной сети за их авторством. Этот способ распространения информации значительно менее удобен, но дает преимущество пользовате-

лям, желающим оставаться «в тени» и в то же время распространять нежелательный контент.

Остается открытым вопрос, связанный с определением входных данных для алгоритма анализа распространения информации. Имея лишь общее представление о потенциально опасных источниках информации, необходимо неоднократно применять предложенный алгоритм, с учетом сведений, полученных на предыдущей итерации, для выявления истинных центров и путей распространения информации.

Обнаружение источников, ретрансляторов, агрегаторов и потребителей информации не позволяет вычислять информационные вбросы, осуществляемые, как правило, децентрализованно при помощи ботов. Это, в свою очередь, ограничивает область применения и целевую аудиторию предлагаемого подхода.

Представление информации с использованием графа может оказаться неинформативным в случае с большими объемами информации. Для этого следует выработать универсальный комплекс мер по снижению связности графа, выделению его ключевых узлов, получению деталей по требованию.

Однако, несмотря на вышеперечисленные недостатки, данная методика, по нашему мнению, перспективна при исследовании целевой аудитории, на которую направлен информационный поток. Например, методика дает возможность изучать поведенческие факторы в течение заданного периода в информационном пространстве объекта, динамика которых позволит оценить прирост аудитории и вовлеченность объектов информационного воздействия.

7. Заключение. Непосредственной областью применения предложенной методики является информационная безопасность государства: повышение уровня защищенности от информационно-психологического воздействия в социальных сетях, анализ атакуемой аудитории, выявление путей распространения информации, обнаружение источника вброса информации.

Полученные результаты позволяют проводить исследования в области визуального анализа социальных сетей. Также разработанная методика может быть использована не только для задач защиты пользователей; так, например, в маркетинге она поможет прогнозировать эффективность рекламных компаний, оценивать скорость реакции рынка на продукт, вовлеченность. Кроме того, у оператора появится возможность отслеживать «затухание» информации по мере ее удаления от ключевых источников распространения.

В дальнейших исследованиях планируется провести серию дополнительных экспериментов, направленных на анализ информационных потоков вокруг групп с запрещенным законодателем контентом. Также перспективным является внедрение тепловых карт вовлеченности. В настоящее время изучаются возможности совмещения текущей модели визуализации информационных потоков с картой вовлеченности объектов воздействия.

Кроме того, представляется важным классифицировать типы узлов распространения информации, отделить агитационные источники от простых трансляторов. Выявление признаков таких узлов позволит проводить сегментацию объектов социальных сетей и повысить эффективность противодействия вредоносному воздействию.

Литература

1. Социальные сети в России, лето 2017: цифры и тренды. URL: <https://www.cossa.ru/289/166387/> <https://www.slideshare.net/Taylli01/2017-77172443> (дата обращения: 20.08.2018).

2. *Kotenko I. V., Chechulin A. A., Shorov A. V., Komashinsky D. V.* Analysis and evaluation of web pages classification techniques for inappropriate content blocking // 14th Industrial Conference on Data Mining, LNAI. New York e. a.: Springer-Verlag, 2014. Vol. 8557. P. 39–54.
3. *Novozhilov D. A., Kotenko I. V., Chechulin A. A.* Improving the categorization of web sites by analysis of Html-Tags Statistics to Block inappropriate content // 9th Intern. Symposium on Intelligent Distributed Computing. New York e. a.: Springer-Verlag, 2016. P. 257–263.
4. *Kotenko I. V., Chechulin A. A., Komashinsky D. V.* Categorisation of web pages for protection against inappropriate content in the Internet // Intern. Journal of Internet Protocol Technology. 2017. Vol. 10(1). P. 61–71.
5. *Zadeh L., Abbasov A., Shahbazova S.* Fuzzy based techniques in human like processing of social network data // Intern. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. Singapore: World Scientific, 2015. Vol. 23 (Suppl. 1). P. 1–14.
6. *Gomzin A., Kuznetsov S.* Methods of construction of socio-demographic profiles of Internet users // Programming and Computer Software Journal. Moscow: ISP RAS, 2015. Vol. 27(4). P. 129–144.
7. *Drobyshevskiy M., Korshunov A., Turdakov D.* Parallel modularity computation for directed weighted graphs with overlapping communities // Programming and Computer Software Journal. Moscow: ISP RAS, 2016. Vol. 28(6). P. 153–170.
8. *Barabasi A., Bonabeau E.* Scale-free networks // Scientific American Journal. 2003. Vol. 288(5). P. 50–59.
9. *Zhang E., Wang G., Gao K., Zhao X., Zhang Y.* Generalized structural holes finding algorithm by bisection in social communities // 6th Intern. Conference on Genetic and Evolutionary Computing. 2013. P. 276–279.
10. *Liu Q., Zhang L.* Information cascades in online reading: an empirical investigation of panel data // Library Hi Tech Journal. 2016. Vol. 32(4). P. 687–705.
11. *Opsahl T., Agneessens F., Skvoretz J.* Node centrality in weighted networks: Generalizing degree and shortest paths // Social Networks Journal. 2010. Vol. 32(3). P. 245–251.
12. *Hickethier G., Tommelein I. D., Lostuvali B.* Social network analysis of information flow in an IPD-project design organization // 21st Annual Conference of the Intern. Group for Lean Construction. 2013. P. 315–324.
13. *Sudhahar S., Veltri G., Cristianini N.* Automated analysis of the US presidential elections using Big Data and network analysis // Big Data & Society Journal. 2015. Vol. 2(1). P. 1–28.
14. *Martinez A., Dimitriadis Y., Rubia B., Gomez E., de la Fuente P.* Combining qualitative evaluation and social network analysis for the study of classroom social interactions // Computers & Education Journal. 2003. Vol. 41(4). P. 353–368.
15. *Lazer D., Pentland A. S., Adamic L., Aral S., Barabasi A. L.* Life in the network: the coming age of computational social science // Science Journal. New York: NIH Public Access, 2009. Vol. 323(5915). P. 721.
16. *Melman S., Bobkov V., Cherkashin A.* Technology and system visualization of large amounts of synoptic data // Journal Information Science and Control Systems. 2015. Vol. 3(45). P. 63–71.
17. *Hornostal O.* System of cluster analysis and visualization of big data // Intern. Scientific Journal Internauka. 2016. Vol. 1(6). P. 22–24.
18. *Averbukh V., Manakov D.* Analysis and visualization of “big data” // Intern. Scientific Conference Parallel Computational Technologies. 2015. P. 332–340.
19. ParaPhraser.ru: Перифразирование и синонимизация текста. URL: www.paraphraser.ru (дата обращения: 20.08.2018).
20. *Kolomeec M. V., Gonzalez-Granadillo G., Doynikova E. V., Chechulin A. A., Kotenko I. V., Debar H.* Choosing models for security metrics visualization // Computer Network Security. Lecture Notes in Computer Science. New York e. a.: Springer-Verlag, 2017. Vol. 10446. P. 75–87.
21. *Kolomeec M. V., Chechulin A. A., Pronoza A. A., Kotenko I. V.* Technique of data visualization example of network topology display for security monitoring // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2016. Vol. 7(1). P. 41–57.

Статья поступила в редакцию 26 июня 2018 г.

Статья принята к печати 25 сентября 2018 г.

Контактная информация:

Проноза Антон Александрович — аспирант; pronoza@gmail.com

Виткова Лидия Андреевна — науч. сотр.; iskinlidia@gmail.com

Чечулин Андрей Алексеевич — канд. техн. наук, вед. науч. сотр.; chechulin@comsec.spb.com

Котенко Игорь Витальевич — д-р техн. наук, проф.; ivkote@comsec.spb.com

Сакхаров Дмитрий Викторович — канд. техн. наук, доц.; d.sakharov@rkn.gov.ru

Methodology for disseminating information channels analysis in social networks*

A. A. Pronoza¹, L. A. Vitkova¹, A. A. Chechulin¹, I. V. Kotenko¹, D. V. Sakharov²

¹ St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 39, 14 Line V. O., Saint Petersburg, 199178, Russian Federation

² The Bonch-Bruевич St. Petersburg State University of Telecommunication, 22-1, Bolshevikov pr., Saint Petersburg, 193232, Russian Federation

For citation: Pronoza A. A., Vitkova L. A., Chechulin A. A., Kotenko I. V., Sakharov D. V. Methodology for disseminating information channels analysis in social networks. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2018, vol. 14, iss. 4, pp. 362–377. <https://doi.org/10.21638/11702/spbu10.2018.409> (In Russian)

The aim of the investigation was to develop a methodology for disseminating information channels analysis in social networks. The proposed methodology is based on the three steps. The first one is the formation of a knowledge base with information about the relationships between users and groups. The second one is the interactive mapping of information dissemination paths, and the third one is related to the visual analysis of the results obtained in previous steps. The interconnections of users and groups in the social network allow one to form the connectivity graphs, and the facts of information transfer through these channels make it possible to identify the ways of content distribution. The results of experiments that confirm the applicability of the proposed methodology are also presented in the paper.

Keywords: social network, visualization, protection against information, inappropriate information, connection graph, visual analytics.

References

1. *Sotsial'nie seti v Rossii, leto 2017: tsifry i trendy* [Social networks in Russia, summer 2017: figures and trends]. URL: <https://www.cossa.ru/289/166387/> <https://www.slideshare.net/Taylli01/2017-77172443> (accessed: 20.08.2018). (In Russian)
2. Kotenko I. V., Chechulin A. A., Shorov A. V., Komashinsky D. V. Analysis and evaluation of web pages classification techniques for inappropriate content blocking. *14th Industrial Conference on Data Mining*, LNAI. New York e. a., Springer-Verlag Publ., 2014, vol. 8557, pp. 39–54.
3. Novozhilov D. A., Kotenko I. V., Chechulin A. A. Improving the categorization of web sites by analysis of html-tags statistics to block inappropriate content. *9th Intern. Symposium on Intelligent Distributed Computing*. New York e. a., Springer-Verlag Publ., 2016, pp. 257–263.
4. Kotenko I. V., Chechulin A. A., Komashinsky D. V. Categorisation of web pages for protection against inappropriate content in the Internet. *Intern. Journal of Internet Protocol Technology*, 2017, vol. 10(1), pp. 61–71.
5. Zadeh L., Abbasov A., Shahbazova S. Fuzzy based techniques in human like processing of social network data. *Intern. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*. Singapore, World Scientific Publ., 2015, vol. 23 (Suppl. 1), pp. 1–14.
6. Gomzin A., Kuznetsov S. Methods of construction of socio-demographic profiles of Internet users. *Programming and Computer Software Journal*. Moscow, ISP RAS Publ., 2015, vol. 27(4), pp. 129–144.
7. Drobyshevskiy M., Korshunov A., Turdakov D. Parallel modularity computation for directed weighted graphs with overlapping communities. *Programming and Computer Software Journal*. Moscow, ISP RAS Publ., 2016, vol. 28(6), pp. 153–170.

* The work is at partial supported by Russian Found of Fundamental Research (project N 18-71-10094 mol-a).

8. Barabasi A., Bonabeau E. Scale-free networks. *Scientific American Journal*, 2003, vol. 288(5), pp. 50–59.
9. Zhang E., Wang G., Gao K., Zhao X., Zhang Y. Generalized structural holes finding algorithm by bisection in social communities. *6th Intern. Conference on Genetic and Evolutionary Computing*, 2013, pp. 276–279.
10. Liu Q., Zhang L. Information cascades in online reading: an empirical investigation of panel data. *Library Hi Tech Journal*, 2016, vol. 32(4), pp. 687–705.
11. Opsahl T., Agneessens F., Skvoretz J. Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks Journal*, 2010, vol. 32(3), pp. 245–251.
12. Hicketier G., Tommelein I. D., Lostuvali B. Social network analysis of information flow in an IPD-project design organization. *21st Annual Conference of the Intern. Group for Lean Construction*, 2013, pp. 315–324.
13. Sudhahar S., Veltri G., Cristianini N. Automated analysis of the US presidential elections using Big Data and network analysis. *Big Data & Society Journal*, 2015, vol. 2(1), pp. 1–28.
14. Martinez A., Dimitriadis Y., Rubia B., Gomez E., de la Fuente P. Combining qualitative evaluation and social network analysis for the study of classroom social interactions. *Computers & Education Journal*, 2003, vol. 41(4), pp. 353–368.
15. Lazer D., Pentland A. S., Adamic L., Aral S., Barabasi A. L. Life in the network: the coming age of computational social science. *Science Journal*. New York, NIH Public Access, 2009, vol. 323(5915), p. 721.
16. Melman S., Bobkov V., Cherkashin A. Technology and system visualization of large amounts of synoptic data. *Journal Information Science and Control Systems*, 2015, vol. 3(45), pp. 63–71.
17. Hornostal O. System of cluster analysis and visualization of big data. *Intern. Scientific Journal Internauka*, 2016, vol. 1(6), pp. 22–24.
18. Averbukh V., Manakov D. Analysis and visualization of “big data”. *Intern. Scientific Conference Parallel Computational Technologies*, 2015, pp. 332–340.
19. *ParaPhraser.ru: Perefrazirovanie i sinonimizatsia teksta* [Paraphrasing and synonymy of text — ParaPhraser.ru]. URL: www.paraphraser.ru (accessed: 20.08.2018). (In Russian)
20. Kolomeec M. V., Gonzalez-Granadillo G., Doynikova E. V., Chechulin A. A., Kotenko I. V., Debar H. Choosing models for security metrics visualization. *Computer Network Security. Lecture Notes in Computer Science*. New York e. a., Springer-Verlag Publ., 2017, vol. 10446, pp. 75–87.
21. Kolomeec M. V., Chechulin A. A., Pronoza A. A., Kotenko I. V. Technique of data visualization example of network topology display for security monitoring. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2016, vol. 7(1), pp. 41–57.

Received: June 26, 2018.

Accepted: September 25, 2018.

Author's information:

Anton A. Pronoza — Postgraduate Student; pronoza@gmail.com

Lidia A. Vitkova — Research Fellow; iskinlidia@gmail.com

Andrey A. Chechulin — PhD in Technics, Leading Research Fellow; chchulin@comsec.spb.com

Igor V. Kotenko — Dr. Sci. in Technics, Professor; ivkote@comsec.spb.com

Dmitry V. Sakharov — PhD in Technics, Associate Professor; d.sakharov@rkn.gov.ru