АНАЛИЗ СОЦИАЛЬНЫХ СЕТЕЙ

ИСКУССТВЕННЫЕ ПРОФИЛИ «ВКОНТАКТЕ» И ИХ ВЛИЯНИЕ НА СОЦИАЛЬНУЮ СЕТЬ ПОЛЬЗОВАТЕЛЕЙ

***Аделя Динаровна Кавеева*[a]*, *Константин Евгеньевич Гурин*[b]**

[a] Казанский федеральный университет, Казань, Россия
[b] Удмуртский государственный университет, Ижевск, Россия

Цитирование: Кавеева А.Д., Гурин К.Е. (2018) Искусственные профили «ВКонтакте» и их влияние на социальную сеть пользователей. *Журнал социологии и социальной антропологии*, 21(2): 214–231. https://doi.org/10.31119/jssa.2018.21.2.8

Аннотация. Статья посвящена проблеме поддельных аккаунтов (фейков) в социальных онлайн-сетях и возникающим из-за них искажениям данных о структуре сетевых взаимодействий между пользователями. Фейки создают дополнительный «шум» в данных, что затрудняет исследование сети как социального пространства. Вмешательство фейков оставляет отпечаток как на структуре сети, так и на ее свойствах. Оценка числа и влияния фейков имеет значение и для формирования выборок из сетей, поскольку анализ полных сетей зачастую невозможен в силу их размеров.

Цель статьи — оценка влияния поддельных аккаунтов на характеристики локальной сети дружбы между пользователями сайта «ВКонтакте» на примере жителей Ижевска. Авторы выделяют ключевые характеристики, по которым можно распознать фейк, и представляют опыт создания на их основе классификатора для определения того, является ли аккаунт пользователя подлинным или нет. Для создания классификатора был применен алгоритм случайного леса. Сравнение топологии исследуемой сети до и после удаления из нее фейковых аккаунтов демонстрирует, на изменение каких именно сетевых метрик влияет наличие в сети профилей, не являющихся подлинными. Так, было установлено, что по мере удаления фейков наименее интегрированные участники теряют связь с основной частью сети и происходит рост числа ее компонент. Таким образом, фейки служат сильными концентраторами связей, распределенными по всей сети, завышая наблюдаемые уровни ассортативности и транзитивности.

Ключевые слова: анализ социальных сетей, «ВКонтакте», анализ данных в R, фейк, поддельный аккаунт, онлайн-сообщества.

* Автор для связи. E-mail: adele.kaveeva@mail.ru

Введение

В течение последних лет онлайн социальные сети испытывают экспоненциальный рост как в регистрации профилей, так и в социальных взаимодействиях. Эти сети позволяют людям делиться различной информацией — новостями, фотографиями, видео, мнениями и другими личными данными. Однако их быстрый рост вызвал и резкий рост вредоносных действий, включая спам, создание поддельных учетных записей, фишинг и распространение вредоносных программ (Adewole et al. 2017: 41). Так, по оценкам Facebook, 8,7 % зарегистрированных в этой социальной сети учетных записей (что составляет 83,09 млн) не принадлежат реальным пользователям, и еще около 1,5 % (14,32 млн) принадлежат пользователям, которые могут распространять вредоносное содержимое (Fire et al. 2014). При этом разработка эффективной системы обнаружения, которая может идентифицировать вредоносные аккаунты, а также их подозрительное поведение в социальных сетях, была и остается сложной задачей.

Поддельные аккаунты (фейки) могут использоваться для того, чтобы подавить реальных пользователей и подорвать отношения доверия в социальной сети путем различных вредоносных действий — рассылки спама, сбора частных данных и др. (Chen et al. 2014). Снабжая фейковые аккаунты характеристиками (фотографией, персональной информацией о себе), их создатели имитируют реальных пользователей. Эта имитация построена на изначально большем доверии пользователей таким же «обычным людям», как они сами, в противовес доверию к СМИ и другим институциональным агентам, которые могут быть ангажированы в пользу тех или иных социально-политических сил, товаров и услуг.

Креси и соавторы отмечают, что фейки превратились в многомиллионный бизнес, они выставляются на продажу для тех, кто хочет повысить репутацию своего аккаунта. Их исследование показывает, что профили знаменитостей, политиков и популярных организаций демонстрируют подозрительное увеличение среди их подписчиков поддельных аккаунтов (Cresci et al. 2015). Такие действия зачастую могут нанести ущерб репутации и иметь далеко идущие последствия и риски для социальной сети. Примеры использования фейков в политических кампаниях и создании политического имиджа (в том числе «черный пиар» конкурентов) описаны в работе Л. Давыдова (Davydov 2016).

Феррара с соавторами встраивают проблему существования искусственных профилей в онлайн социальных сетях в еще более широкий социальный контекст. Авторы считают обнаружение таких пользователей

(«социальных ботов») важной исследовательской задачей, поскольку фейки могут проникать в политический дискурс, манипулировать фондовым рынком, раздувать панику во время чрезвычайных ситуаций и распространять дезинформацию, что влечет за собой эрозию доверия к социальным сетям (Ferrara et al. 2016). «Социальные боты» также могут препятствовать продвижению общественной и государственной политики, создавая видимость низового движения или способствуя сильной поляризации политической дискуссии в интернете (Conover et al. 2011).

Для социологического анализа сетей также большой интерес представляет вопрос, как наличие фейков влияет на выборки. Социальные сети пользователей таких площадок, как Facebook, ВКонтакте и других, — это гигантские графы с множеством узлов и ребер. Сбор и анализ настолько крупных сетей часто затратен или невозможен (в том числе в силу политики конфиденциальности). Уже с 1970-х гг. исследователи обсуждают способы формирования выборочных совокупностей из сетей (Granovetter 1976; Frank 1978). Репрезентативная выборка должна сохранять такие свойства исходной сети, как плотность, структура сообщества, распределение степеней, коэффициент кластеризации и другие, однако различные виды выборок дают неодинаковые результаты в различных исследовательских ситуациях. Некоторые работы посвящены применению и сравнению различных выборочных методов для сетей (см., напр.: Leskovec, Faloutsos 2006; Ahmed et al. 2013; Blagus et al. 2017; Wagner et al. 2017). Так, основными методами формирования выборок из сетей являются выборка по узлам, выборка по ребрам, метод случайного блуждания и метод снежного кома. Подробное описание выборочных методов для сетей не составляет цель настоящей работы. Однако, поскольку фейки могут влиять на показатели сетей и смещать их, уместно выявлять поддельные аккаунты перед формированием выборочной совокупности.

Обнаружение фейков в социальных сетях

Увеличение числа искусственных аккаунтов и их вмешательство не остается незамеченным на уровне топологии социальной сети, которую формируют пользователи. Это приводит к искажению картины взаимодействий реальных пользователей и может повлечь некорректность выводов относительно характеристик сети, которые делают исследователи на основе сетевого анализа.

Например, сетевая визуализация в работе Феррары и соавторов иллюстрирует вмешательство «социальных ботов» в онлайн-дебаты в Twitter относительно политики вакцинации в Калифорнии, США. На графе сети ретвитов размер узлов-фейков гораздо больше, чем размер узлов, репре-

зентирующих подлинные аккаунты, что отражает влияние пользователя — число ретвитов его поста (Ferrara et al. 2016: 98). Очевидно, что удаление искусственных аккаунтов из этой сети существенно изменило бы ее структуру, дав исследователю более корректную информацию о распространении темы только среди реальных агентов. Однако выявление фейков представляет собой сложную задачу, для решения которой существуют различные подходы (поведенческий анализ, теория графов, машинное обучение) и предлагаются различные алгоритмы (Boshmaf et al. 2011; Cao et al. 2012; Zhu et al., Xiao et al. 2012; Adewole et al. 2017 и др.).

Поведенческий подход основан на мониторинге поведения пользователя и на уверенности в том, что люди обычно ведут себя иначе, чем фейки, поэтому обнаружение подобного поведения приведет к их выявлению (El Azab et al. 2016). А. Алымов и соавторы, анализируя возможности детектирования поддельных аккаунтов в российской сети «ВКонтакте», выделяют два типа признаков для их выявления: статичные и поведенческие. Так, к статичным относятся такие признаки, как полнота заполнения профиля, число друзей (у фейков их больше, чем у среднего пользователя), количество комментариев от друзей (у фейка практически отсутствуют), наличие рекламного контента и др. Поведенческие признаки отражают различные формы активности, например скорость комментирования, которая у искусственных аккаунтов гораздо выше (Алымов и др. 2016: 57–59). Слабым местом поведенческого подхода является то, что если фейк не злоупотребляет различными платформами, используя некоторую базовую информацию профиля, его будет сложно обнаружить.

Теория графов — распространенная перспектива в исследованиях фейков. Например, Конти с соавторами анализирует граф социальной сети в динамике для обнаружения тех, кто создает поддельные профили для олицетворения реальных людей, а затем взаимодействует с их друзьями (Conti et al. 2012). Многие исследователи применяют алгоритмы машинного обучения для обнаружения спама в онлайн социальных сетях. Например, Файер и др. (Fire et al. 2012) используют аномалии топологии, деревья решений и наивные классификаторы Байеса для идентификации спамеров и поддельных профилей.

Некоторые работы в этой области исходят из того, что фейки группируются в кластеры и есть возможность обнаружить такие группы взаимосвязанных искусственных аккаунтов (см., напр.: Xiao et al. 2015). Однако чаще можно наблюдать противоположную картину. Так, на примере китайской социальной сети Renren было обнаружено, что соседи поддельных аккаунтов состоят в основном из реальных пользователей.

Иными словами, фейки не образуют кластер, они хорошо интегрированы в более широкую социальную сеть (Zhu et al. 2012). Исследования также показывают, что поддельные аккаунты добавляют друзей по методу «снежного кома»: начиная с популярных пользователей, они постепенно добавляют все больше рядовых пользователей, вскоре оказываясь интегрированными в социальную сеть как обычные участники (Yang et al. 2011).

Для борьбы со спамом сайты социальных сетей позволяют пользователям сообщать о мошеннических профилях или действиях. В работе Фримана (Freeman 2017) обсуждаются возможности выявления фейков силами пользователей социальных сетей, а именно: действительно ли некоторые пользователи (так называемые «доверенный набор») лучше определяют поддельные аккаунты, чем другие? Фриман обнаружил, что участники, демонстрирующие измеримые, повторяемые навыки в идентификации поддельных профилей, существуют, но редки (не более 2,4 %). Таким образом, любой надежный «доверенный набор» пользователей слишком мал, чтобы иметь заметное влияние на показатели вредоносных действий в социальных сетях.

При выборе алгоритма обнаружения для настоящего исследования мы опирались на работу исследователей из LinkedIn (Xiao et al. 2015). Для обучения классификатора для обнаружения фейков в LinkedIn авторы использовали и сравнивали алгоритмы случайного леса, логистической регрессии и метод опорных векторов. Было обнаружено, что алгоритм случайного леса дает лучшие результаты для всех показателей (показатель AUC на тестовой выборке составил 0,98). В связи с этим в нашем исследовании мы также используем алгоритм случайного леса для создания классификатора фейков в российской социальной сети «ВКонтакте».

Поддельные аккаунты «ВКонтакте»: постановка задачи и данные

В работе мы разрабатываем классификатор для обнаружения поддельных аккаунтов в онлайн социальной сети «ВКонтакте», используя алгоритм случайного леса. «ВКонтакте», будучи самым популярным российским сайтом (Similar Web 2017), представляет собой социальное поле для коммуникации, поддержания социальных связей и формирования социального капитала. По причине популярности этой площадки в сеть проникают агенты, которые стремятся использовать ее как экономический инструмент или в иных целях, создавая сеть поддельных профилей. Исследовательский интерес авторов сосредоточен на том, как такое вмешательство отражается на топологии и свойствах сети пользователей «ВКонтакте». Мы предлагаем способ выявления искусственных аккаунтов на

примере сети дружеских связей г. Ижевска. Выявление и удаление фейков позволяет скорректировать сеть пользователей и оценить влияние, которое искусственные аккаунты оказывают на сеть.

Исследовательские вопросы статьи:

1. Влияет ли удаление обнаруженных поддельных аккаунтов на сплоченность сети (модулярность)?

2. Какую роль фейки играют в интеграции слабо вовлеченных в сеть пользователей?

3. Как удаление фейков влияет на распределение дружеских связей в сети (иными словами, как изменяются показатели ассортативности и транзитивности в сети после удаления фейков)?

Мы предполагаем, что удаление из сети аккаунтов, с высокой вероятностью являющихся фейковыми, повлияет на наблюдаемые сетевые метрики. Метрики, рассчитываемые для сетей пользователей, дают информацию о том, насколько сплоченным является сообщество, содержит ли оно подгруппы, какие узлы (т.е. пользователи) в ней имеют наибольший вес и значение, как и за счет каких участников происходит расширение сети и распространение информации.

К значимым в данной статье метрикам сетевого анализа относятся следующие:

- размер сети — число «узлов» или «вершин» (пользователей);
- средняя длина пути между двумя любыми участниками сети;
- распределение степеней (т.е. числа связей, которыми пользователь связан с другими);
- ассортативность — тенденция узлов с одинаковой степенью образовывать связи друг с другом. Ассортативность означает, что пользователи объединены связями с теми, у кого схожее с ними количество друзей;
- транзитивность — доля закрытых «триад», где все трое связаны между собой («друг моего друга — мой друг»);
- модулярность — свойство, характеризующее степень кластеризации узлов, когда внутри кластера плотность сети высокая, а между кластерами — низкая; и др.

Локальная сеть жителей г. Ижевска была выбрана в качестве пробной площадки для создания и применения классификатора. Выбор Ижевска обусловлен как проживанием одного из авторов в этом городе, так и относительной простотой сбора данных в силу небольших размеров сети (по данным на 1 июля 2017 г., на сайте «ВКонтакте» зарегистрировано 507 748 ижевских аккаунтов). С помощью алгоритма поиска жителей, в том

числе и не указавших город проживания, была собрана база пользователей жителей Ижевска на сайте «ВКонтакте». Всего сеть включила 600 315 пользователей и 23 113 тыс. дружеских связей.

Объектом исследования стала локальная сеть дружеских связей в социальной онлайн-сети «ВКонтакте» на примере г. Ижевска, а предметом — топология этой сети под влиянием искусственных аккаунтов. Таким образом, целью данного исследования является определение изменений характеристик сети при удалении пользователей, с высокой вероятностью являющихся фейками. Для достижения исследовательской цели были поставлены и реализованы следующие задачи:

1. Определение характеристик, по которым можно распознать фейк.
2. Создание классификатора на основе характеристик пользователя для определения того, является ли аккаунт пользователя фейковым или нет.
3. Оценка влияния удаления наиболее вероятных аккаунтов-фейков на топологию локальной сети и ее характеристики.

Создание классификатора для обнаружения фейков

Для создания классификатора необходимо было в первую очередь сформировать обучающую выборку. С этой целью была собрана информация с 37 пользователей — жителей Ижевска. Им необходимо было указать, кто из их друзей и подписчиков знаком им лично, а кто из них добавился или пытался добавиться в друзья, но не знаком с ними и/или является продавцом некоторых товаров или услуг через сайт «ВКонтакте». Таким образом была получена выборка ижевчан для построения классификатора, содержащая после удаления дубликатов и пересечений 6252 настоящих аккаунта и 2293 фейка.

Сбор данных об этих пользователях был осуществлен при помощи языка программирования R и библиотеки VKR, разработанной Д. Сорокиным (GitHub 2016). Пакет VKR содержит набор функций, позволяющих обращаться к сайту «ВКонтакте», выгружать и анализировать данные о пользователях и сообществах.

Для полученной выборки пользователей была собрана информация о заполнении определенных полей в профиле (место жительства, пол, дата рождения, школа и вуз обучения, политические, религиозные взгляды, наличие партнера, указание девичьей фамилии) и информация о типе устройства, с которого пользователь заходил в сеть в последний раз. Также были рассчитаны сетевые и поведенческие метрики пользователей: уровень транзитивности, число друзей и подписчиков в сети, общее число друзей и подписчиков, доля ижевчан среди друзей и подписчиков

пользователя, центральность по собственному значению векторов, число отправленных пользователем заявок в друзья, не получивших подтверждения, число групп, в которых состоит пользователь, и групп, популярных среди ижевчан (с более чем 500 ижевчанами). Было также установлено, в каком сегменте сети по размеру находится пользователь (ранг размера его кластера, полученного в результате разбивки графа). Как видно из перечня собранных признаков, они содержат как статичные, так и поведенческие признаки.

Для создания модели, определяющей, является ли пользователь фейком или нет, был применен алгоритм случайного леса. Случайный лес строит множество деревьев, извлекая из обучающих данных случайные подвыборки и рассчитывая, за какой класс по каждому наблюдению проголосовало больше деревьев. Случайный лес не требует преобразования и предположений о распределении признаков, не чувствителен к лишним переменным. Однако, как и другие методы статистического обучения, он склонен к переобучению, что требует от исследователя разбиения выборки на обучающую и тестовую. В результате алгоритм из 1000 деревьев был построен на основе двух третей базы, а треть была применена для проверки на переобучение.

На тестовой выборке алгоритм верно распознал 92 % пользователей (15,2 % фейков были распознаны как реальные пользователи, а 5,7 % реальных пользователей были ложно распознаны как фейки). Показатель AUC, оцененный на данных тестовой выборки, составляет 0,954, что указывает на высокое качество распознавания как реальных, так и искусственных аккаунтов. Построение моделей на основе алгоритма XGBoost и логистической регрессии с регуляризацией показали аналогичные результаты.

Применение классификатора к локальной дружеской сети ижевчан «Вконтакте»

Разработанный классификатор был применен к сети дружеских связей пользователей «ВКонтакте», проживающих в Ижевске. Были изучены следующие показатели сети: размеры графа, число связных компонент (так как классификатор был собран через алгоритм блуждания по графу, без удаления фейков была всего одна связная компонента), ассортативность, транзитивность, модулярность и число подгрупп в наибольшей связной компоненте. Также проверялась корреляция между показателями центральностей в сетях до и после удаления фейков, а именно центральности по числу друзей (*degree centrality*) и по собственному значению векторов (*eigenvector centrality*). Кроме того, в процессе построения сети

дружбы отслеживались изменения в распределении числа дружеских связей пользователей (среднее значение, медиана, первый и третий квартиль, первый и последний квантиль).

Поскольку ошибка классификатора на разных уровнях различается, был проведен ряд замеров с разным пороговым уровнем показателя доли деревьев, проголосовавших за «фейк», для определения принадлежности к этому классу. Были рассчитаны значения от 1 (т.е. включение всего графа) до 0,7 (исключение всех пользователей, за отнесение которых к классу «фейк» проголосовало 70 и более процентов деревьев), с шагом в 1 % по результату классификатора. На каждом шаге строилась сеть, удалялись фейки и замерялись сетевые метрики (табл. 1).

В результате проведенных тестов было определено, что по мере удаления аккаунтов, с большой вероятностью являющихся фейками, наименее интегрированные участники теряют связи с основной частью сети, что выражается в росте числа компонент. Также сеть значительно уменьшается в размерах. Сплоченность основной части сети, выраженная в показателе модулярности, не изменяется по мере удаления фейковых аккаунтов, однако число кластеров внутри наибольшей связной компоненты сокращается, что объясняется отсоединением малых кластеров от связной компоненты. Следовательно, фейковые аккаунты не влияют на сплоченность/разобщенность в сети.

Влияние фейков на интеграцию слабо вовлеченных пользователей в сеть ниже, чем влияние случайно взятого аккаунта. Такой вывод был получен в результате сравнения сети, полученной при удалении аккаунтов с 70%-м пороговым значением модели, и 30 сетями, построенными со случайным удалением узлов, количественно эквивалентным удаленным искусственным аккаунтам. В сетях со случайным удалением узлов минимальное число компонент в сети составило 7336, что в 2,5 раза превышает число компонент, остающееся после удаления фейков.

По мере удаления снижается уровень ассортативности и транзитивности в сети. Таким образом, фейки служат сильными концентраторами связей, распределенными по всей сети, завышая тем самым наблюдаемые уровни ассортативности и транзитивности. Этот вывод подкрепляется и сравнением с сетями со случайно удаленными участниками, где параметры сети меньше отличаются от полного графа.

По мере удаления фейковых аккаунтов из сети изменяются показатели локальной транзитивности для конкретных пользователей (корреляция Спирмена между метриками для полной сети и скорректированной по конкретным узлам опускается до 0,98) и показатели центральности по собственному значению векторов (до 0,97). По мере удаления фейков

Таблица 1

Сетевые метрики, рассчитываемые по мере удаления из сети аккаунтов, отнесенных классификатором к классу «фейк»

Пороговый процент фейков, выше которого аккаунт исключается из сети	**100**	**95**	**90**	**85**	**80**	**75**	**70**
Число аккаунтов в сети	600 315	594 897	579 011	562 185	546 020	529 462	511 297
Число связей в сети	23 113 829	22 539 385	21 470 725	20 472 632	19 593 964	18 811 865	18 195 034
Число связных компонент	1	443	1230	1972	2543	2909	2893
Число узлов в наибольшей связной компоненте	600 315	594 432	577 751	560 174	543 430	526 509	508 362
Модулярность наибольшей связной компоненты	0,40	0,40	0,40	0,41	0,41	0,40	0,41
Число кластеров в наибольшей связной компоненте	185	120	216	104	93	78	52
Ассортативность сети	0,16	0,16	0,16	0,16	0,15	0,13	0,12

Пороговый процент фейков, выше которого аккаунт исключается из сети	**100**	**95**	**90**	**85**	**80**	**75**	**70**
Транзитивность сети	0,09	0,09	0,09	0,09	0,08	0,07	0,07
Среднее число дружеских связей	77	76	74	73	72	71	71
Первый дециль числа дружеских связей	2	2	2	2	2	3	3
Первый квартиль числа дружеских связей	6	6	6	7	8	9	10
Медиана числа дружеских связей	28	28	29	30	31	33	35
Третий квартиль числа дружеских связей	84	83	84	84	85	86	87
Девятый дециль числа дружеских связей	173	170	168	166	165	164	164

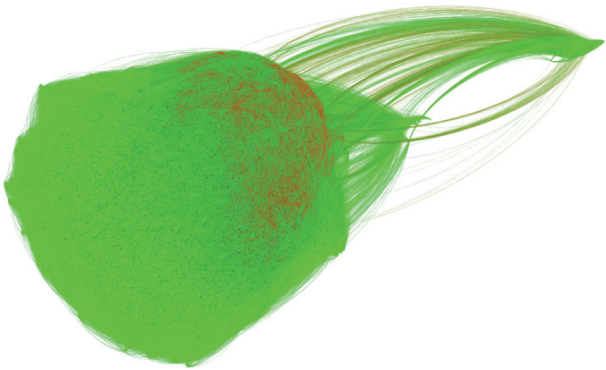

Рис. 1. K-ядро графа пользователей Ижевска (при k=75)

среднее число дружеских связей и девятый дециль распределения снижаются, а непараметрические показатели распределения (за исключением девятого дециля) растут. Это объясняется тем, что фейки чаще становятся либо хабами (но ограниченными максимальным числом друзей в 10 тысяч), либо, наоборот, слабо включенными в сеть аккаунтами. Соответственно, распределение числа дружеских связей у пользователей сильно деформируется по мере включения фейковых аккаунтов в анализ.

На рисунке 1 изображено k-ядро* графа пользователей Ижевска (при k=75), содержащее 86 523 узлов (пользователей) и 10 860 487 ребер (отношений дружбы между пользователями). Зеленые узлы обозначают настоящих пользователей, а красные — поддельные профили. Если хотя бы один из концов является поддельным, то ребро красного цвета.

Заключение

Изучение локальных, городских сетей интернет-пользователей требует от исследователя учета таких недостатков больших данных, как их возможная неполнота и недостоверность. Если к первому типу недостатков можно отнести случайный или умышленный пропуск пользователем заполнения части данных о себе (например, города проживания), то второй связан в первую очередь с наличием в сетях большого количества искусственных аккаунтов, создающих «шум» в данных. Неполнота и недостоверность данных влекут за собой изменения в топологии сети и сме-

* K-ядро — показатель, помогающий определить небольшие связанные ключевые области в сети. Чтобы быть включенным в k-ядро, объект должен быть связан с другими объектами в группе, число которых равно или больше числа k.

щение сетевых характеристик, поэтому уместно использовать методы корректировки сети (ее дополнение недостающими данными о пользователях или, напротив, «чистку» от фейков). К способам обнаружения поддельных аккаунтов относится предложенный в статье классификатор, основанный на алгоритме случайного леса.

Предложенный нами классификатор верно распознает 92 % пользователей (15,2 % фейков были неверно распознаны как реальные пользователи, 5,7 % реальных пользователей были распознаны как фейки). В его основу легли как статичные, так и поведенческие признаки для выявления подлинности профиля: информация о заполнении полей в профиле, сетевые и поведенческие метрики (транзитивность, число друзей и подписчиков, членство в группах, местоположение в сегменте сети и др.).

Работа подтверждает выводы предшествующих исследований других сайтов социальных сетей о том, что искусственные аккаунты хорошо интегрированы в сеть реальных пользователей. Стремясь к большему числу связей, они добавляют друзей по принципу снежного кома. Более того, они служат концентраторами связей в сети: по мере удаления поддельных аккаунтов наименее интегрированные участники теряют связи с основной частью сети, что выражается в росте числа компонент, а сама сеть значительно уменьшается в размерах. В сети фейки чаще становятся либо хабами, либо, наоборот, слабо включенными в сеть аккаунтами. Соответственно, распределение числа дружеских связей у пользователей сильно деформируется по мере включения фейковых аккаунтов в анализ. Наличие фейковых аккаунтов завышает и наблюдаемые уровни ассортативности (склонности образовывать дружеские связи с теми, кто имеет схожее число друзей) и транзитивности (доли закрытых триад, где все трое являются друзьями). Таким образом, значительное число искусственных профилей, за которыми не стоят реальные пользователи, действительно имеет влияние на топологию сети и, следовательно, то, как в ней будет распространяться информация. Поэтому корректное исследование тех или иных процессов, а также структуры сетей на сайтах социальных сетей должно предваряться выявлением и удалением из них поддельных аккаунтов.

Тематика фейковых агентов в сети сама по себе представляет научный интерес и имеет перспективы для дальнейших исследований. Рост числа фейков и их реальное влияние как на структуру сети, так и на процессы распространения информации внутри нее отражают современные тенденции развития онлайн-сообществ, оказывая непосредственное влияние и на действительность вне Интернета. Несмотря на то что в настоящей статье поддельные аккаунты рассматриваются как «шум» в данных, фей-

ки могут быть объектом исследования сами по себе. Большая вариативность способов поведения, которую демонстрируют искусственные агенты, определяет и разнообразие способов их изучения и подходов к нему. В частности, за пределами статьи остались вопросы идентичности и ситуации, в которых реальные люди создают поддельные аккаунты с целью презентации себя с иной, нежели в реальной жизни, стороны. В таких ситуациях фейк — это способ проигрывания иных социальных ролей и сценариев (в том числе девиантных), недоступных индивиду в офлайне, что может выступать в качестве значимого социализирующего фактора. При таком подходе к проблеме могут быть применены классические социологические теории, например драматургия И. Гофмана.

Благодарность

Авторы статьи выражают благодарность Дмитрию Сорокину (университет ИТМО), разработавшему библиотеку VKR для языка программирования R, с помощью которой были собраны данные для исследования. Работа выполнена при поддержке Программы повышения конкурентоспособности Казанского (Приволжского) федерального университета.

Литература

Алымов А.С., Баранюк В.В., Смирнова О.С. (2016) Детектирование ботпрограмм, имитирующих поведение людей в социальной сети «ВКонтакте». *International Journal of Open Information Technologies,* 8: 55–60.

Adewole K.S., Anuar N.B., Kamsin A., Varathan K.D., Razak S.A. (2017) Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications*, 79: 41–67. https://doi.org/10.1016/j.jnca.2016.11.030.

Ahmed N. K., Neville J., and Kompella R. (2013) Network Sampling: From Static to Streaming Graphs. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 8(2), Article 7. https://doi.org/10.1145/2601438

Blagus N., Šubelj L., Bajec M. (2017) Empirical comparison of network sampling: How to choose the most appropriate method? *Physica A: Statistical Mechanics and its Applications*, 477: 136–148. https://doi.org/10.1016/j.physa.2017.02.048.

Boshmaf Y., Muslukhov I., Beznosov K., and Ripeanu M. (2011) The Socialbot Network: When Bots Socialize for Fame and Money. *Proceedings of the 27th Annual Computer Security Applications Conference*: 93–102.

Cao Q., Sirivianos M., Yang X., Pregueiro T. (2012) Aiding the Detection of Fake Accounts in Large Scale Social Online Services. *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation:* 1–15.

Chen C.-M., Guan D., Su Q.-K. (2014) Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. *Information Sciences*, 289: 133–147.

Conover M., Ratkiewicz J., Francisco M., Gonçalves B., Menczer F. and Flammini A. (2011) Political polarization on Twitter. *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*: 89–96.

Conti M., Poovendran R., and Secchiero M. (2012) Fakebook: Detecting fake profiles in on-line social networks. *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*: 1071–1078.

Cresci S., Di Pietro R., Petrocchi M., Spognardi A., Tesconi M. (2015) Fame for sale: Efficient detection of fake Twitter followers. *Decision Support Systems*, 80: 56–71. https://doi.org/10.1016/j.dss.2015.09.003

Davydov L. (2016) On the Use of Social Networks as a Tool for Creating Political Authority's Image. *International Journal of Environmental & Science Education*, 11(18): 12423–12430.

El Azab A., Idrees A.M., Mahmoud A. M., Hefny H. (2016) Fake Account Detection in Twitter Based on Minimum Weighted Feature set. *International Scholarly and Scientific Research & Innovation*, 10(1): 13–18.

Ferrara E., Varol O., Davis C., Menczer F., and Flammini A. (2016) The Rise of Social Bots. *Communications of the ACM*, 59(7): 96–104. https://doi.org/10.1145/2818717.

Fire M., Kagan D., Elyashar A., Elovici Y. (2014) Friend or foe? Fake profile identification in online social networks. *Social Network Analysis and Mining*, 4(1): 1–23.

Fire M., Katz G., and Elovici Y. (2012) Strangers intrusion detection — detecting spammers and fake profiles in social networks based on topology anomalies. *ASE Human Journal*, 1(1): 26–39.

Frank O. (1978) Sampling and estimation in large social networks. *Social Networks*, 1: 91–101.

Freeman D.M. (2017). Can You Spot the Fakes? On the Limitations of User Feedback in Online Social Networks. *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*: 1093–1102. https://doi.org/10.1145/3038912.3052706.

Granovetter M. (1976) Network sampling: Some first steps. *American Journal of Sociology*, 81: 1267–303.

Leskovec J., Faloutsos C. (2006) Sampling from large graphs. *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM:* 631–636.

Wagner C., Singer P., Karimi F., Pfeffer J., and Strohmaier M. (2017) Sampling from Social Networks with Attributes. *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*: 1181–1190. https://doi.org/10.1145/3038912.3052665.

Xiao C., Freeman D. M., Hwa T. (2015) Detecting Clusters of Fake Accounts in Online Social Networks. *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security,* 91–101. https://doi.org/10.1145/2808769.2808779

Yang Z., Wilson C., Wang X., Gao T., Zhao B. Y., and Dai Y. (2011) Uncovering social network sybils in the wild. *Internet Measurement Conference*: 259–268.

Zhu Y., Wang X., Zhong E., Liu N., Li H., Yang Q. (2012) Discovering Spammers in Social Networks. *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence:* 171–177.

Источники

GitHub (2017) *Access to VK (Vkontakte) API via R* [https://github.com/Dementiy/vkR] (дата обращения: 31.08.2017).

Similar Web (2017) *Top Websites Ranking* [https://www.similarweb.com/top-websites] (дата обращения: 31.08.2017).

"VKONTAKTE" FAKE ACCOUNTS AND THEIR INFLUENCE ON THE USERS' SOCIAL NETWORK

***Adelia Kaveyeva*[a]*, *Konstantin Gurin*[b]**

[a] Kazan Federal University, Kazan, Russia
[b] Udmurt State University, Izhevsk, Russia

Citation: Kaveyeva A., Gurin K. (2018) Iskusstvennyye profili "VKontakte" i ikh vliyaniye na sotsial'nuyu set' pol'zovateley ["VKontakte" fake accounts and their influence on the users' social network]. *Zhurnal sotsiologii i sotsialnoy antropologii* [The Journal of Sociology and Social Anthropology], 21(2): 214–231 (in Russian). https://doi.org/10.31119/jssa.2018.21.2.8

Abstract. The paper deals with the fake accounts in online social networks and resulting data misrepresentation about the structure of network users' interactions. Fakes create an additional noise in the data; therefore investigation of the network as a social space becomes difficult. The intervention of fakes leaves a mark on both the network structure and on its properties. The estimation of the number and influence of fakes is also important for sampling large networks, since the analysis of complete networks is often impossible because of their size.

The aim of the present paper is the impact assessment of the fake accounts on the characteristics of a local friendship network between users of the VKontakte site (on the example of Izhevsk residents). The key characteristics recognizing a fake were emphasized. The design of the classifier (based on random forest algorithm) to determine the authenticity of the account was also presented. It was shown which network metrics in particular are affected by the presence of fake profiles by comparing the network topology before and after deleting the fake accounts from it. It was found, that as the

* Corresponding author. E-mail: adele.kaveeva@mail.ru

fakes are removed, the less integrated participants lose contact with the main part of the network and the number of its components increases. Thus, fakes represent strong link concentrators distributed throughout the network, overestimating the observed levels of assortativity and transitivity.

Keywords: social network analysis, VKontakte, data analysis using R, fake accounts, online communities.

Acknowledgements

The authors thank Dmitry Sorokin from ITMO University who developed 'VKR' package for R programming language. This research was financially supported by the Russian Government Program of Competitive Growth of Kazan Federal University.

References

Adewole K.S., Anuar N.B., Kamsin A., Varathan K.D., Razak S.A. (2017) Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications*, 79: 41–67. https://doi.org/10.1016/j.jnca.2016.11.030.

Ahmed N.K., Neville J., and Kompella R. (2013) Network Sampling: From Static to Streaming Graphs. *ACM Transactions on Knowledge Discovery from Data (TKDD),* 8(2), Article 7. https://doi.org/10.1145/2601438

Alymov A.S., Baranyuk V.V., Smirnova O.S. (2016) Detektirovaniye bot-programm, imitiruyushchikh povedeniye lyudey v sotsial'noy seti «VKontakte» [Detecting bot programs that mimic people's behavior in the social network "VKontakte"]. *International Journal of Open Information Technologies,* 8: 55–60 (in Russian).

Blagus N., Šubelj L., Bajec M. (2017) Empirical comparison of network sampling: How to choose the most appropriate method? *Physica A: Statistical Mechanics and its Applications*, 477: 136–148. https://doi.org/10.1016/j.physa.2017.02.048

Boshmaf Y., Muslukhov I., Beznosov K., and Ripeanu M. (2011) The Socialbot Network: When Bots Socialize for Fame and Money. *Proceedings of the 27th Annual Computer Security Applications Conference*, 93–102.

Cao Q., Sirivianos M., Yang X., Pregueiro T. (2012) Aiding the Detection of Fake Accounts in Large Scale Social Online Services. *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation:* 1–15.

Chen C.-M., Guan D., Su Q.-K. (2014) Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. *Information Sciences*, 289: 133–147.

Conover M., Ratkiewicz J., Francisco M., Gonçalves B., Menczer F. and Flammini A. (2011) Political polarization on Twitter. *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*: 89–96.

Conti M., Poovendran R., and Secchiero M. (2012) Fakebook: Detecting fake profiles in on-line social networks. *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*: 1071–1078.

Cresci S., Di Pietro R., Petrocchi M., Spognardi A., Tesconi M. (2015) Fame for sale: Efficient detection of fake Twitter followers. *Decision Support Systems*, 80: 56–71. https://doi.org/10.1016/j.dss.2015.09.003

Davydov L. (2016) On the Use of Social Networks as a Tool for Creating Political Authority's Image. *International Journal of Environmental & Science Education*, 11(18): 12423–12430.

El Azab A., Idrees A.M., Mahmoud A. M., Hefny H. (2016) Fake Account Detection in Twitter Based on Minimum Weighted Feature set. *International Scholarly and Scientific Research & Innovation*, 10(1): 13–18.

Ferrara E., Varol O., Davis C., Menczer F., and Flammini A. (2016) The Rise of Social Bots. *Communications of the ACM*, 59(7): 96–104. https://doi.org/10.1145/2818717.

Fire M., Kagan D., Elyashar A., Elovici Y. (2014) Friend or foe? Fake profile identification in online social networks. *Social Network Analysis and Mining*, 4(1): 1–23.

Fire M., Katz G., and Elovici Y. (2012) Strangers intrusion detection — detecting spammers and fake profiles in social networks based on topology anomalies. *ASE Human Journal*, 1(1): 26–39.

Frank O. (1978) Sampling and estimation in large social networks. *Social Networks*, 1: 91–101.

Freeman D.M. (2017). Can You Spot the Fakes? On the Limitations of User Feedback in Online Social Networks. *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*: 1093–1102. https://doi.org/10.1145/3038912.3052706.

Granovetter M. (1976) Network sampling: Some first steps. *American Journal of Sociology*, 81: 1267–303.

Leskovec J., Faloutsos C. (2006) Sampling from large graphs. *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM:* 631–636.

Wagner C., Singer P., Karimi F., Pfeffer J., and Strohmaier M. (2017) Sampling from Social Networks with Attributes. *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*: 1181–1190. https://doi.org/10.1145/3038912.3052665

Xiao C., Freeman D. M., Hwa T. (2015) Detecting Clusters of Fake Accounts in Online Social Networks. *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security,* 91–101. https://doi.org/10.1145/2808769.2808779

Yang Z., Wilson C., Wang X., Gao T., Zhao B. Y., and Dai Y. (2011) Uncovering social network sybils in the wild. *Internet Measurement Conference*: 259–268.

Zhu Y., Wang X., Zhong E., Liu N., Li H., Yang Q. (2012) Discovering Spammers in Social Networks. *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence:* 171–177.