Детектирование бот-программ, имитирующих поведение людей в социальной сети «Вконтакте»

А.С. Алымов, В.В. Баранюк, О.С. Смирнова

Аннотация **– Статья посвящена вопросам детектирования бот-программ, имитирующих поведение людей в социальной сети «Вконтакте». В рамках этого направления рассмотрены типы социальных ботов, варианты их использования, а также актуальность выявления. В статье описаны методы профилактической защиты от социальных ботов, представлены существующие системы детектирования бот-программ, а также выявлены критерии, способствующие распознаванию бот-профилей в социальной сети «Вконтакте».**

Ключевые слова **– социальная сеть «Вконтакте»; социальный бот; бот-профиль; методы распознавания бот-программ.**

I. Введение

В настоящее время социальные сети приобретают все большую популярность, т.к. интегрируют практически все существующие интернет-источники, являются мощным инструментом самоорганизации общества и отдельных его групп, а также затрагивают практически все слои населения и эффективно структурируют пользователей по их интересам, политическим и религиозным взглядам. Статистика использования социальных сетей растет ускоренными темпами, вдвое быстрее, чем статистика использования поисковых порталов или электронной почты. Но, как и любая другая, стремительно развивающаяся эта сфера сопряжена с новыми рисками – ростом недоверия к собеседникам, за счет сомнения в их реальности. Одна из самых распространённых угроз доверию в социальных сетях – социальные боты [1, 2].

Статья получена 14.07.2016 г.

Исследование выполнено федеральным государственным бюджетным образовательным учреждением высшего образования «Московский технологический университет» (МИРЭА) за счет гранта Российского фонда фундаментальных исследований (проект №16-37-00492).

А.С. Алымов, МИРЭА (e-mail: alexey.alymov@gmail.com).

К.т.н., с.н.с., В.В. Баранюк, МИРЭА (e-mail: valentina_bar@mail.ru).

О.С. Смирнова, МИРЭА (e-mail: mail.olga.smirnova@yandex.ru).

II. Социальные боты

За последнее время социальные сети привлекли очень много различных участников общества, став не только средством общения, но и развлекательным хостингом, коммерческой площадкой с набором инструментов для эффективного распространения продукта, а также источником информации. Заинтересованные лица умело используют этот потенциал для достижения своих целей, в том числе и за счет социальных ботов, выдавая их за реальных пользователей.

Называют социальных ботов по-разному: боты (программы, имитирующие поведение человека), фейки (поддельные аккаунты, выдаваемые за реального пользователя) и т.д.

Социальные боты (бот-программы) – это часть программного обеспечения, которая предназначена для имитации поведения живого пользователя в социальных сетях. Они могут использоваться для выдачи себя за другого пользователя, путем хищения его персональных данных или для достижения иных целей в сети интернет, к примеру, для продвижения бренда или идеи, либо имитации интереса большого количества людей к обсуждению какой-либо темы.

III. Типы социальных ботов

Ошибочным мнением является то, что все боты одинаковы и имеют одинаковые цели. Простые пользователи обычно не вникают в особенности поведения бот-программ и не пытаются определить последовательность их действий, дабы не попасться на крючок. Проведя анализ поведения бот-программ, можно разделить ботов на два типа: автоматических, которые выполняют простые заранее заданные инструкции, и управляемых, которые отличаются от автоматических тем, что их действия контролируются оператором, который в полуавтоматическом режиме участвует в обсуждениях. Автоматические бот-программы позволяют автоматически ставить лайки (выражение одобрения к публикуемому материалу), делать репосты (способ делиться информацией, не меняя ее содержания). Продвинутые боты способны в автоматическом режиме заполнять профиль пользователя, вступать в различные сообщества и пытаться добавлять других пользователей в «друзья». Такие боты обычно используются для накруток

различных статистических показателей и распространения спам-сообщений. Успех управляемых ботов зависит от степени социализации и соблюдения правил социальной сети с целью недопущения аккаунта к блокировке. К так называемым управляемым ботам также относятся клонированные страницы (клоны) реальных пользователей, в том числе публичных персон [2].

Также заблуждением является убежденность в том, что достаточно легко получить большое число поддельных аккаунтов для проведения различных коммерческих, рекламных кампаний. Многие пользователи считают, что практически любой информационный вброс, раскрутки или навязывание мнения можно легко решить путем привлечения трафика заранее созданных или купленных профилей, а представители социально-политических организаций делают это чуть ли не каждый день.

Ботов можно разделить на несколько типов, но основных – два:

1) автоматически зарегистрированные аккаунты;

2) взломанные аккаунты, которые в свою очередь делятся по типу взлома:

– с ретрива (восстановление пароля на почту);

– с брута (подбор комбинаций пароля);

– с фейка (подставной страницы, копирующей оригинал).

Профили, которые используют как реальные люди, так и бот-программы называют киборгами или аватарами [3]. Обычно такие профили имеют хорошие социальные связи.

По предназначению социальных ботов можно разделить на:

– новостных ботов – ботов, публикующих новости у себя в профиле. Используются для целенаправленного распространения информации;

– бот-программы, использующие сообщения реальных пользователей для того, чтобы быть похожими на них. Главная цель существования – создание информационных вбросов;

– игровых ботов, используемых в приложениях социальных сетей. Общаются с пользователями от имени реальных пользователей, в основном используются для имитации игровых действий в приложениях;

– ботов, участвующих в улучшении репутации путем увеличения количества друзей и связей.

IV. Актуальность выявления социальных ботов

В современном понимании, как было указано выше, социальные боты – это программы, созданные для имитации поведения людей в социальных сетях. На данный момент, запрограммированные пользователи создают немало проблем, как для обычных пользователей, так и для тех, кто применяет социальные сети для ведения маркетинговой кампании или проведения социальных исследований. Посредством эксплуатации бот-профилей в социальных сетях, сильно искажается информация о действительных предпочтениях и интересах пользователей порталов. Одна из основных целей использования бот-программ – распространение информации, как положительной, так и отрицательной относительного продвигаемой идеи, что мешает проведению SMM-анализа (Social media marketing – процесс привлечения трафика или внимания к бренду или продукту через социальные платформы), искажая информацию об интересе пользователей к проекту за счет «накрутки» количества участников в сообществах [4]. Поэтому следует определять какие пользователи социальной сети являются запрограммированными и уметь разделять поток данных на генерируемый ботами и человеком.

Последствиями массового распространения запрограммированных аккаунтов являются:

1) массовое хищение персональных данных;

2) снижение уровня доверия в социальных сетях;

3) информационные вбросы и создание ложных новостей;

4) необъективность результатов проведения SMM-анализа, голосований, социальных исследований.

V. Методы защиты от социальных ботов

Социальные сети практически не осуществляют действий по борьбе с бот-активностью, в основном все мероприятия по защите от бот-программ являются профилактическими:

– Captcha – это автоматически генерируемый тест-проверка, является ли пользователь человеком или компьютером. Представляет собой в подавляющем большинстве случаев искаженную надпись из букв и/или цифр. Они могут быть написаны в различных цветовых сочетаниях с применением шума, искривления, наложения дополнительных линий или произвольных фигур;

– Смс–верификация (смс-проверка) – проверка подлинности пользователя посредством отправки на номер смс с кодом подтверждения, который он должен затем ввести в нужное поле при регистрации или входе в систему;

– Rate limit – ограничение числа запросов к системе за определённое время.

VI. Существующие системы детектирования бот-программ

В настоящее время в открытых источниках доступно немного информации о программных средствах, способных распознавать бот-активность в социальных сетях. К самым популярным можно отнести системы Akismet, Vkontakte Antispam и «Исследовательский вес рунета».

Система Akismet, которая в автоматическом режиме обнаруживает спам-сообщения пользователей, постоянно развивается и обучается, что позволяет детектировать поведение сложных ботов, с которыми другие системы не могут справиться. Разработчики предоставляют бесплатное использование системы,

связно это с тем, что системе необходимо обучаться, чтобы коммерческие проекты могли уверенно использовать программный продукт на платной основе. Положительной стороной является то, что систему можно интегрировать в любую социальную сеть. Минусом является то, что цены на использование системы очень высокие.

Еще одним примером такой системы является программный продукт «Vkontakte Antispam», предназначенный для социальной сети ВКонтакте. Посредством его использования можно сократить количество спама в группах и публичных страницах социальных сетей, которыми управляет пользователь. В настоящее время в системе реализован функционал выявления и добавления бот-пользователей в чёрный список. Достоинством данной системы является ее направленность на обнаружение спам-сообщений, с последующим их удалением и добавлением автора в чёрный список. Необходимо отметить, что программное средство является бесплатным и довольно эффективным.

Рисунок 1 – Скриншот работы программного продукта «Исследовательский вес рунета»

«Исследовательский вес рунета» – это продукт, разрабатываемый отечественной группой аналитиков, разработчиков и исследователей. Их система в автоматическом режиме индексирует и анализирует профили пользователей таких социальных сетей как «Twitter» и «Вконтакте». В первую волну исследований каждый пользователь социальной сети проверялся по различным критериям, по окончании проверки каждому пользователю присваивался один из трех статусов: бот, неактивный (отсутствующий в системе более 28 дней), активный (см. рисунок 1). Заявлено, что корректность расчетов может проверить любой желающий, проанализировав свой собственный аккаунт в социальных сетях, но расшифровка результатов такого анализа (определенный статус каждого контакта из списка пользователя) пользователю не предоставляется и, соответственно, нет возможности проверить верность полученных данных.

VII. Критерии распознавания бот-профилей в социальной сети «ВКонтакте»

В детектировании социальных ботов существует одна сложность – невозможно однозначно определить является ли пользователь ботом или нет. Связано это с тем, что однозначный ответ может дать лишь сам владелец пользовательского профиля. Исходя из этого, необходимо оперировать понятиями нечеткой логики. В таком случае, проектируемая система оценки близка, по сути, к скоринговой системе, принятие решения в которой осуществляется по совокупности некоторых, заранее определённых, признаков, а не по одному показателю. Реализовывать саму систему необходимо только после определения перечня показателей и оценки их весомости в суммарной оценке критериев определения бот-профилей.

Методы определения бот-профилей можно разделить на две категории – на анализ информации, получаемой во время присутствия пользователя на страницах социальной сети (онлайн анализ), и на анализ информации, размещенной пользователем на своей персональной странице (оффлайн анализ). Соответственно, все полученные в результате такого анализа признаки будут подразделяться на статичные и поведенческие.

VIII. Статичные признаки определения бот-профилей

К статичным признакам относят характеристики данных, используемых для оформления аккаунта и некоторые особенности его ведения – полнота заполнения данных профиля и т.п. В этом случае данными для анализа являются фотографии, выложенные пользователем, публичные сообщения, персональная информация, например, дата рождения или место проживания и т.д. По этим данным можно определить принадлежит ли анализируемый профиль реальному человеку.

Заблокированный профиль – блокировка пользователей в социальной сети практически всегда происходит из-за использования сторонних программ, осуществляющих спам-деятельность.

Верифицированный аккаунт – признаком такого аккаунта является галочка рядом с именем пользователя (рисунок 2). Такой статус аккаунта предоставляется в основном известным личностям, чьи профили абсолютно точно принадлежат реальному человеку.

Рисунок 2 – Скриншот верифицированного аккаунта

Количество друзей – среднестатистический пользователь социальной сети имеет обычно в друзьях 20-200 пользователей. В то время как у большинства бот-профилей в друзьях насчитывается порой и более нескольких тысяч друзей. При этом не стандартной является ситуация, если у человека нет друзей, пусть и виртуальных, но при этом он активно общается (комментирует посты). Поэтому также интересен не только сам показатель числа друзей, а его соотношение с длительностью существования аккаунта, числом публикаций и числом комментариев (входящих и исходящих).

Количество подписчиков – не вызывающее подозрение количество людей, которые подписаны на пользователя – не более 300 человек.

Полнота заполнения полей профиля – когда регистрируют ботов, то обычно стараются заполнить минимум данных, чтобы избежать лишних затрат времени. Если ботов регистрируют с помощью программных средств, то поля заполняются по максимуму.

Аватар пользователя – если на аватаре (графическое представление пользователя) стоит изображение с рекламой стороннего проекта и другие фотографии отсутствуют, то, скорее всего, это будет бот, созданный для проведения рекламных акций какого-либо продукта. Если аватар пользователя не уникальный или если у пользователя нет аватара, то это будет считаться признаком бот-профиля.

Использование некорректного имени – использование в имени не имен – один из признаков бот-активности. Это косвенный признак, который может использоваться только в комплексе с другими выявленными признаками как дополнительный фактор.

Публикации пользователя – если пользователь ничего сам не пишет, а только комментирует чужие записи или репостит (копирует) их на свою страницу, то это еще один признак бот-активности. Нередко для имитации активности профиля делаются такие публикации, но в большинстве случаев они не являются уникальными. В таком случае используют показатель соотношения личных постов пользователя (самостоятельных записей на странице) к общему числу постов (в том числе репостов и чужих записей) на его странице.

Активность пользователя – резкие скачки активности пользователя по наполнению профиля контентом также могут свидетельствовать о действиях бот-программы, которые, к примеру, чаще всего наполняют страницу только при ее создании. Также интересным для анализа показателем является соотношение активности пользователя (число, период формирования постов, комментариев) к продолжительности существования его аккаунта. Если, например, аккаунт зарегистрирован недавно, но при этом на его странице уже несколько тысяч записей или комментариев, это вызывает сомнения.

Для выявления подобных аномальных случаев рассчитывается средняя активность пользователя, (количество постов в месяц, количество комментариев в месяц и т.д.), периоды повышенной активности, соотношение активности пользователя к продолжительности существования его аккаунта и т.д.

Количество комментариев от друзей пользователя – если у пользователя на странице практически нет активности других пользователей, то, скорее всего, это бот-профиль.

Вредоносные ссылки – наличие в статусе и контактах пользователя ссылок на ресурсы из черного списка таких сервисов как, Google, Yandex, Yahoo и т.д., предоставляющие черные списки вредоносных сайтов.

Обилие рекламных постов – если пользователь размещает на своей странице много рекламных сообщений, то это также выглядит странно и является признаком того, что профиль ведет бот-программа. В таком случае рассчитывается соотношение числа рекламных записей к общему числу записей.

IX. Поведенческие признаки определения бот-профилей

К поведенческим признакам относят те особенности пользовательского поведения, которые обычно не характерны реальным пользователям социальной сети [5]. На пример участие в искусственном продвижении контента указывает на то, что аккаунт, скорее всего, используется бот-программой. Зачастую пользователи сдают свой реальный аккаунт «в аренду» на своеобразных «биржах» для автоматизированного распространения какой-либо информации, но подобные случаи единичны. Другой вариант – «взлом» аккаунта реального пользователя. Но во всех подобных случаях этот профиль считается бот-профилем.

Скорость комментирования – нормальный человек не может оставлять комментарии со скоростью 1 комментарий в секунду. Как минимум нужно прочитать то, что комментируешь, сформулировать ответ и набрать его на клавиатуре. При самых лучших условиях на это уйдет около десяти секунд. По этой причине, более точным показателем является показатель, основанный на соотношении скорости комментирования к длине самого комментария.

Комментарии разных аккаунтов с одного IP за короткий промежуток времени**.** Речь идет о ситуации, когда в комментариях одной публикации (например, в

блоге) «оставили след» несколько аккаунтов за короткий промежуток времени и все с одного IP. Это явное указание на то, что управляются эти аккаунты с одного компьютера (сервиса) или через один прокси-сервер.

Содержание комментариев также может указывать на их программное происхождение, например, примитивные комментарии («+100500», «автар жжет», «кек»). Безусловно, это может написать и человек, а по тому это лишь косвенный признак. Другой вариант – комментарии «не в тему», когда содержание комментария не соответствует содержанию общения. Еще один вариант – точные дубли других комментариев, особенно, когда дублируется многократно (десятки, сотни дублей) за короткий промежуток времени. Но здесь нужно учитывать такое явление как цитаты. Достаточно примеров, когда некое короткое высказывание нравится публике, и его начинают распространять именно люди, просто дублируя его.

Поведение пользователя на странице – если человек перейдет по ссылке и ничего не произойдет, он, скорее всего, попытается перейти по ней еще раз, тогда как бот не будет этого делать.

Определение бот-профиля строится по значениям ряда критериев, каждый из которых по отдельности является лишь косвенно характеризующим признаком, при том что оценка их в совокупности повышает шанс обнаружения бот-программ, имитирующих поведение людей.

X. Заключение

На современном этапе развития информационных технологий разработка методов автоматического распознавания бот-программ является актуальной задачей, играющей важную роль в вопросах безопасности и решении ряда экономических и социальных проблем.

Использование программных средств детектирования бот-программ, имитирующих поведение людей, позволит уменьшить массовые хищения персональных данных, уровень недоверия в социальных сетях, количество информационных вбросов и ложных новостей, а также повысит объективность результатов проведения SMM-анализа, голосований, социальных исследований и т.д.

БИБЛИОГРАФИЯ

[1] Topmarketing.by Честное SMM-продвижение, выявляем аккаунты-боты в социальных сетях [Электронный ресурс] [Дата обращения: 20.02.2016]. Режим доступа: URL: http://topmarketing.by/internet-marketing/chestnoe-smm-prodvizhenie-vyyavlyaem-akkaunty-boty-v-socialnyx-setyax.html

[2] Лыфенко М.Д. Виртуальные пользователи в социальных сетях: Мифы и реальность: [Текст] / Лыфенко М.Д. // Вопросы кибербезопасности – 2014 – № 4 – с.1-4

[3] Zi Chu, Steven Gianvecchio, Haining Wang, Sushil Jajodia Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?// IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2012. —P.2-10.

[4] Градосельская Г. В. Сетевые измерения в социологии: Учебное пособие / Под ред. Г. С. Батыгина. — М.: Издательский дом «Новый учебник», 2004. — с. 3.

[5] Лаборатория Перспективных Разработок Автоопределение ботов [Электронный ресурс] [Дата обращения: 31.05.2016] Режим доступа: URL: http://www.ci2b.info/3-texnologii-iw/3-analiz-informacii/avtoopredelenie-botov/

Detection of bot programs that mimic the behavior of people in the social network "Vkontakte"

A.S. Alymov, V.V. Baranjuk, O.S. Smirnova

Abstract –The paper is devoted to the detection of bot programs that simulate people's behavior in social network «Vkontakte». During the research, we identified the types of social bots, types of their use, as well as the relevance of their detection. This article describes methods of protection against social bots, presents existing system software for bots recognition, as well as the identifying criteria to facilitate the recognition bot profiles in the social network «Vkontakte».

Keywords – social network «Vkontakte»; social bot; methods of bot recognition.