DOI 10.36622/VSTU.2022.25.4.002
УДК 519.766.4:004.032.26

ВЫЯВЛЕНИЕ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ В СОЦИАЛЬНЫХ СЕТЯХ НА ИХ РАННИХ СТАДИЯХ

В.А. Минаев, А.Н. Рабчевский, Я.Р. Мустакимова

В статье представлены и исследованы на эмпирических материалах схемы проведения информационных операций в социальных сетях. Для выявления признаков информационных операций проведен анализ в сети ВКонтакте потоков деструктивного контента, содержащего около 130 тысяч информационных сообщений. Показано, что признаками информационных операций выступают увеличивающееся количество публикаций близкого по смыслу целевого контента, высокая частота публикаций, небольшой временной интервал между публикациями, стремление к максимальному охвату аудитории. Выявлена высокая начальная частота публикаций дубликатов, распространяемых несвязанными между собой пользователями, как общее свойство, присущее информационным операциям. Предложено использовать это свойство как признак информационных операций. Исследования показали, что методика, использующая этот признак, позволяет выявлять информационные операции на самых ранних стадиях, что приводит к сокращению времени принятия решений о мерах противодействия им и повысить эффективность информационного противодействия. Этапы методики выявления информационных операций включают: сбор массива публикаций по заданному информационному поводу; выявление информационных треков с аномально высокой начальной частотой вбросов дубликатов; проверку треков на предмет релевантности; формирование списка треков с признаками информационных операций; анализ связей пользователей, опубликовавших дубликаты в отобранных треках; формулирование итогового вывода о том, является ли конкретный информационный повод информационной операцией.

Ключевые слова: информационные войны, информационные операции; распознавание признаков, дубликаты публикаций, частота публикаций.

Введение

Развитие информационных и телекоммуникационных технологий привело к тому, что противостояние между противоборствующими сторонами на международной арене перешло на уровень информационных войн. Согласно Конвенции об обеспечении информационной безопасности ООН [1] информационная война – это «межгосударственное противоборство в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам».

Основным средством ведения указанных войн являются информационные операции, которые предпринимаются для достижения информационного превосходства путем воздействия на информационные системы противника с одновременной защитой собственных информационных систем и инфраструктуры [2]. В результате выполнения информационных операций решаются задачи:

– достижения максимального охвата аудитории деструктивным контентом;

– вовлечения наибольшего количества пользователей в какое-либо деструктивное событие или социальное явление;

– побуждения пользователей к практическим деструктивным действиям в реальном мире, например, их привлечение к участию в протестных акциях.

Объектами воздействия информационных операций являются как общество в целом (гражданское население, его социальные группы, в частности, личный состав силовых структур), так и его государственные, экономические и социальные институты.

Такое воздействие производится в виде массированной психологической обработки для дестабилизации общества и государства. Социальные сети и мессенджеры при этом стали основным полем боя в информационных войнах.

На рис. 1 представлена типовая схема активной фазы информационной операции в социальной сети ВКонтакте.

Размещение контента производится с помощью публикации постов на сайтах пользователей и их сообществ, либо комментариев под контентом, размещенным другими пользователями.

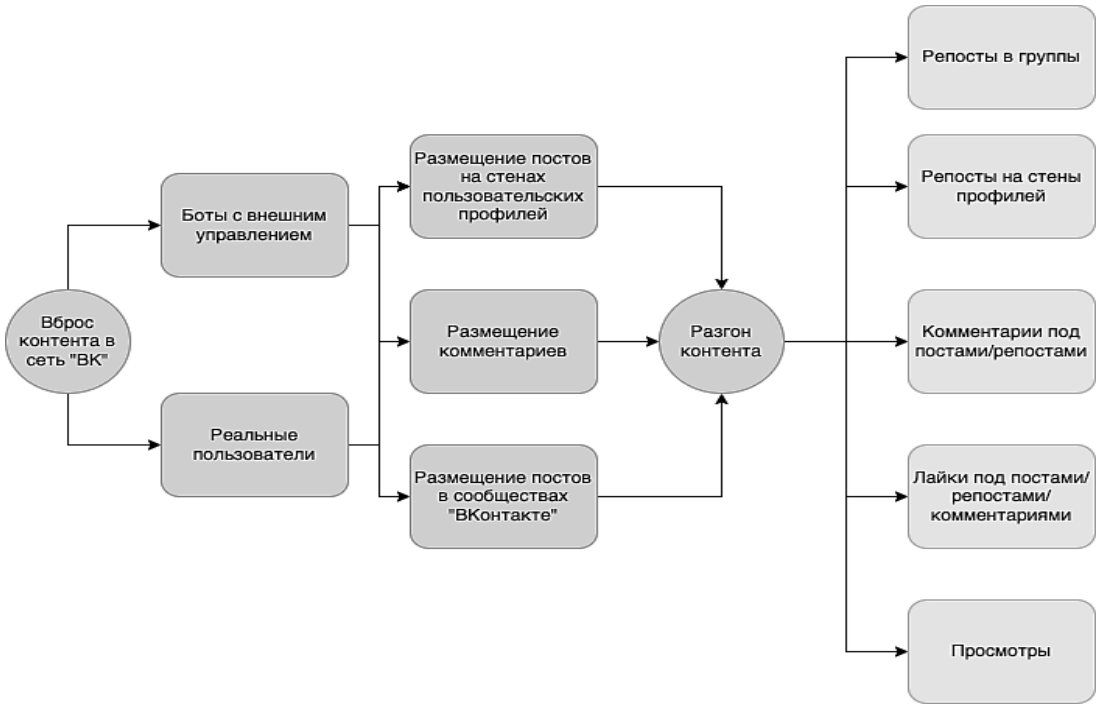

Рис. 1. Схема активной фазы информационной операции

В любом случае, для начала процесса распространения целевого контента необходимо сформировать в социальной сети первоисточник – пост. Первоисточник может содержать любую информацию (в том числе – ссылки на контент, размещенный в других социальных сетях, видеохостингах, сайтах и т.д.). Пост может быть размещен как реальным пользователем, так и ботом.

В зависимости от стратегии активной фазы информационной операции первоисточник может быть как открытым (к примеру, YouTube канал), так и скрытым – первичный пост, как правило, удаляется после начала распространения информации с целью затруднения последующего расследования инцидента.

Кроме того, стратегия активной фазы информационной операции может предполагать наличие множества первоисточников. Для активизации распространения контента используются репосты, комментарии, лайки и просмотры.

Особенностью реализации активной фазы информационных операций является применение технологической «накрутки» показателей контента с целью вывода его в тренды социальной сети.

Если в результате «накрутки» целевой контент попадает в тренды социальной сети, то доверие к нему повышается, и реальные пользователи более активно репостят, комментируют, просматривают и лайкают его, ускоряя распространение информации.

Основным элементом противодействия информационным операциям является их выявление. Таким образом, задача разработки методов, алгоритмов и программных средств, предназначенных для выявления информационных операций, является весьма актуальной.

Типовая информационная операция включает фазу вброса и фазу «разгона» контента. Очевидно, что детектирование информационной операции в фазе вброса контента позволяет существенно сократить время реагирования на нее и организовать противодействие ей на ранней стадии, не позволяя противнику достичь своих целей. В статье исследуются методы выявления

признаков, позволяющих распознавать информационные операции на ранних стадиях.

Методы выявления информационных операций

Изучению характерных признаков информационных операций посвящен ряд работ. Так, в [3] указано, что признаком информационной операции является повторение новостей и комментариев к ним. При этом чем меньше похожести на первичную новость, тем больше вероятность того, что повтор является частью спланированной операции. Основными значимыми параметрами для выявления информационных операций в этом случае, по мнению авторов, являются частота подачи материала, относящегося к заданной теме, значимость источника и охват населения.

В [4] указывается, что признаками начала информационной операции являются рост числа суррогатов в негативных высказываниях.

Основной особенностью информационных операций, по утверждению [5], являются экспрессивный и оперативный характер действий, организованных с использованием технологий Интернет.

В [6, 7] указывается, что особенностями информационных операций является наличие большого количества нечетких дубликатов и небольшой интервал времени их публикации.

Таким образом, основными признаками информационных операций выступают:

– увеличивающееся количество публикаций близкого по смыслу целевого контента,

– высокая частота публикаций,

– небольшой временной интервал публикаций,

– стремление к максимальному охвату аудитории.

Для распознавания информационных операций используют классический подход, когда анализируется число сообщений определенной направленности в некотором промежутке времени. Если их количество больше определенного порогового значения, делается вывод о наличии признаков проведения информационной операции. Недостатком такого подхода является эмпирический характер оценки порогового значения, которое зависит от многих факторов.

Наряду с классическим подходом, применяется анализ динамических свойств информационных потоков [8–11]. Для анализа зависимости объемов информационных потоков от времени в [12] рассматривается анализ временных рядов как реализация стохастического процесса, а также корреляционный анализ, анализ Фурье, вейвлет-анализ, корреляция с шаблоном, фрактальный анализ. Подобные подходы отчасти решают задачу выбора пороговых значений, однако имеют общий недостаток. Он состоит в том, что необходим анализ сообщений за достаточно продолжительный промежуток времени, что не позволяет выявлять информационные операции на ранних стадиях.

В работе [6] делается вывод, что выявление информационных операций возможно в момент достижения максимального значения частоты публикаций нечетких дубликатов. В указанной работе в качестве признаков информационных операций используются некоторые метрики центральности и их соотношения для графов, состоящих из сообщений (вершин) и их взаимосвязей (ребер).

Однако предложенный в ней метод не лишен недостатков. А именно, на выявление информационной операции требуется существенное время, включающее время ее активной фазы, а также время, необходимое на сбор и обработку информации. Кроме того, использование в качестве признака информационной операции нечетких дубликатов накладывает повышенные требования к средствам их выявления.

Следует отметить, что с учетом времени, прошедшего с момента публикации данной работы, исследуемая область несколько изменилась, характеризуясь тем, что современные организаторы информационных операций уже не считают нужным маскироваться. Поэтому наряду с нечеткими дубликатами в информационных операциях широко используются четкие дубликаты. При этом потоки нечетких дубликатов формируют тренд в виде конкретного информационного повода, а потоки четких

дубликатов прямо указывают на организованный целенаправленный характер их организации, а значит в большей мере являются признаком информационной операции [13].

Достижение целей информационной операции возможно только в случае обеспечения максимального охвата аудитории в минимальные сроки. Логично предположить, что при проведении информационной операции должен наблюдаться одновременный массовый вброс целевого контента через множество каналов.

При построении временного ряда, соответствующего такому массовому вбросу, следует ожидать аномально высокую начальную частоту публикации дубликатов.

Исходя из такого положения, измерение начальной частоты публикации дубликатов и выявление ее аномальных значений позволяет существенно сократить период времени, необходимый для идентификации информационных операций.

Обсуждение результатов

Предметом исследования в настоящей статье являются информационные потоки публикаций в социальной сети ВКонтакте.

Будем использовать следующие термины: *инфоповод* – поток информационных сообщений по общей тематике, публикуемых в социальной сети; *информационный трек* – поток сообщений, опубликованных в социальной сети, состоящий из дубликатов, отсортированных в единый временной ряд.

Цель настоящей работы – исследовать процессы распространения деструктивной информации в социальной сети ВКонтакте на предмет выявления признаков целенаправленной организованной деятельности в виде информационных операций.

В соответствии с поставленной целью разработана и официально зарегистрирована программа «Информационный трек-детектор», которая выявляет в общем информационном потоке четкие дубликаты, сортирует их по времени публикации, объединяет в отдельные информационные треки, анализирует начальную частоту публикации дубликатов в каждом треке и формирует данные об информационных треках с аномально высокой начальной частотой публикации дубликатов.

Выходные данные программы для каждого инфоповода представляются в виде графика, сводной таблицы и набора таблиц для каждого информационного трека, включающих содержание дубликатов и ссылки на страницы, на которых они опубликованы.

С помощью указанной программы проанализированы наиболее известные инфоповоды «Жыве Беларусь», связанный с протестными настроениями на выборах президента республики Беларусь, а также инфоповод «Дворец Путина», название которого говорит само за себя.

На рис. 2 представлен сводный график изменения количества дубликатов по инфоповоду «Жыве Беларусь» с начала момента информационной операции.

Цифрами обозначены номера информационных треков, которые представляют интерес для интерпретации в качестве информационных операций. По вертикальной оси указано количество опубликованных дубликатов, а по горизонтальной – временные отметки.

На данном графике присутствуют треки с высокой начальной частотой публикации дубликатов, имеющие значительный охват по сравнению с другими, за исключением 16421, который представляет набор дубликатов с картинками различного содержания.

В табл. 1 представлены характеристики информационных треков по инфоповоду «Жыве Беларусь».

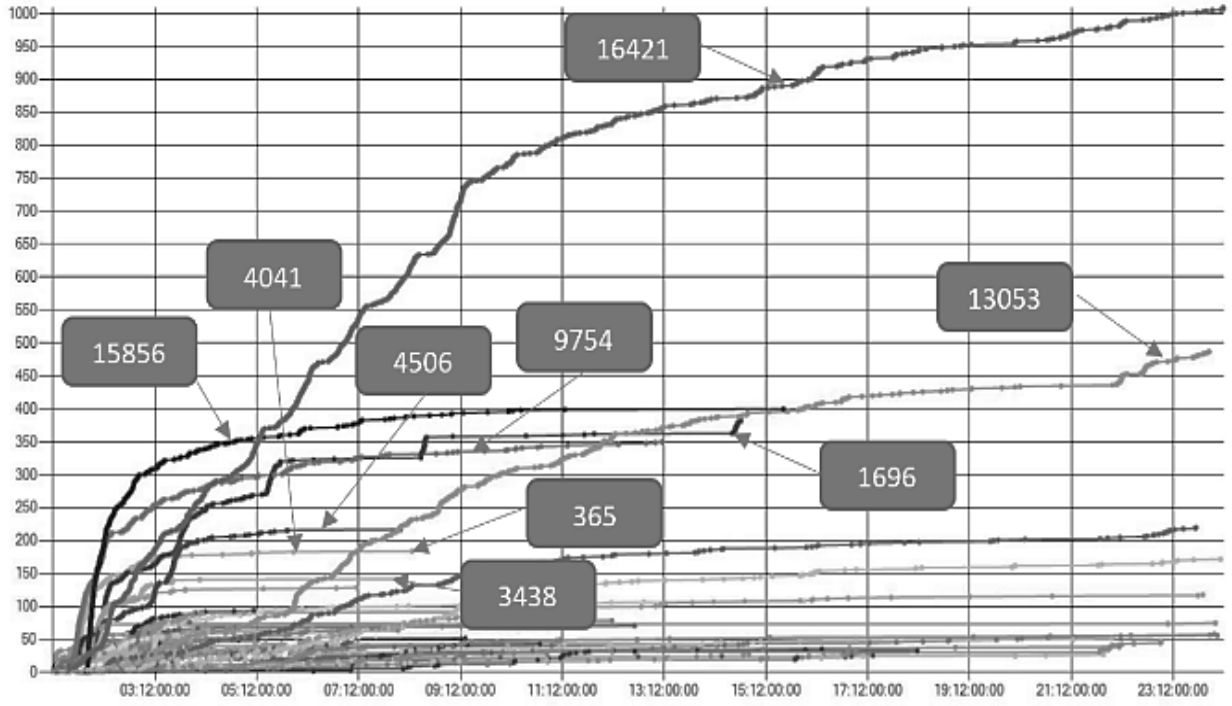

Рис. 2. Сводный график информационных треков по инфоповоду «Жыве Беларусь» (скриншот программы «Информационный трек-детектор»)

Таблица 1

Фрагмент сводной таблицы по инфоповоду «Жыве Беларусь»

Номер трека	**Общее количество дубликатов**	**Период публикации первых 10 дубликатов, мин**
16421	1009	47
13053	487	41
15856	400	16
1696	382	12
9754	350	23
4506	217	10
365	184	19
3438	142	08
4041	129	06

Из анализа рис. 2 и табл. 1 можно сделать вывод, что 7 из 9 информационных треков обладают признаками информационной операции. Применительно к ним первые 10 дубликатов опубликованы в период до 23 минут, что явно не соответствует сложившимся параметрам обычных информационных потоков.

На рис. 3 и в табл. 2 представлены график информационных треков и фрагмент сводной таблицы по инфоповоду «Дворец Путина».

В инфоповоде «Дворец Путина» период публикации первых 10 дубликатов короче (до 9 мин), чем в предыдущем инфоповоде.

Очевидно, что вероятность стихийной публикации полностью идентичного контента десятью различными пользователями в течение первых 4 минут (трек 1712) практически равна нулю. То есть в действительности наблюдался организованный одновременный массовый вброс целевого контента, который однозначно интерпретируется как признак информационной операции.

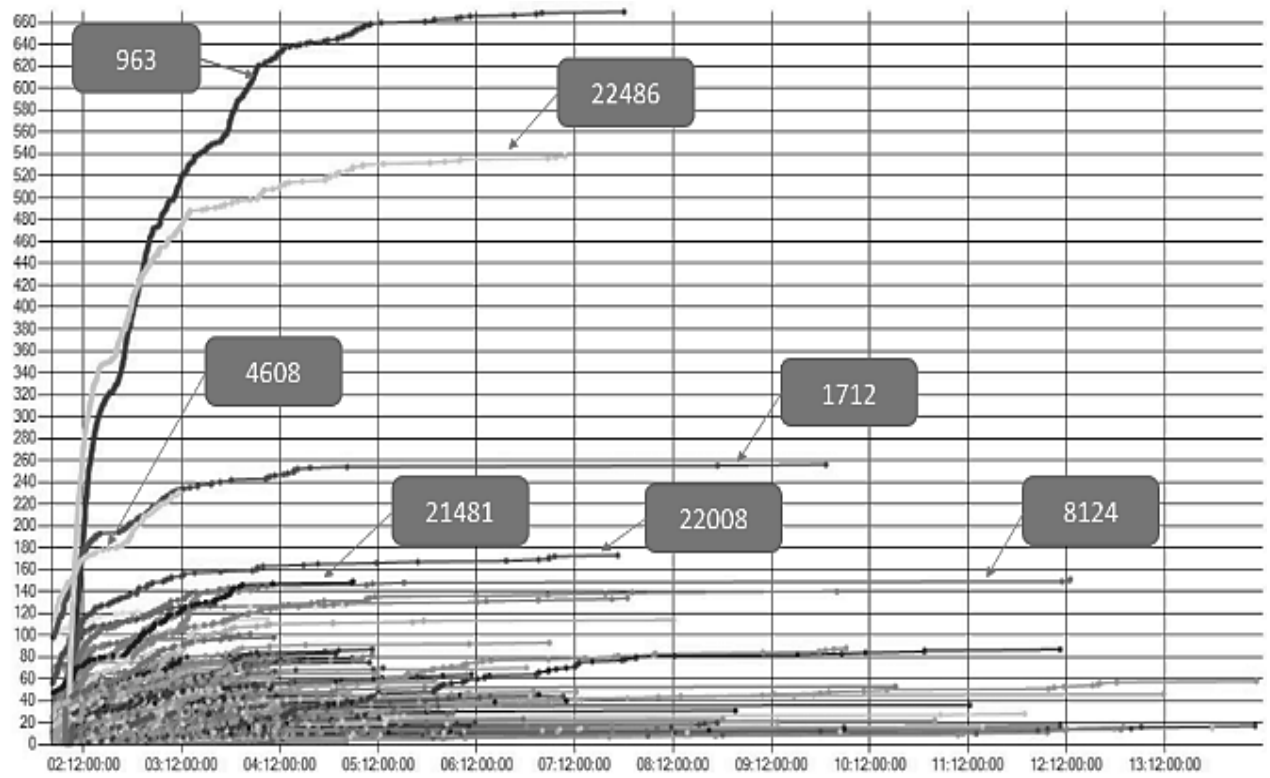

Рис. 3. Сводный график информационных треков по инфоповоду «Дворец Путина» (скриншот программы «Информационный трек-детектор»)

Таблица 2

Фрагмент сводной таблицы по инфоповоду "Дворец Путина"

Номер трека	**Общее количество дубликатов**	**Период публикации первых 10 дубликатов, мин**
963	670	6
22486	538	6
1712	256	4
4608	231	9
22008	173	42
8124	151	8
1973	142	7

То же касается и других представленных информационных треков с аномальными характеристиками.

В обоих инфоповодах сочетание высокой начальной частоты публикаций дубликатов и массового охвата аудитории можно интерпретировать как признаки проведения информационной операции.

С целью выявления особенностей проведения информационных операций, реализуемых в пространстве социальных сетей выполнен анализ операции «Дворец Путина». В результате сформирована общая схема информационной операции «Дворец Путина» (рис. 4).

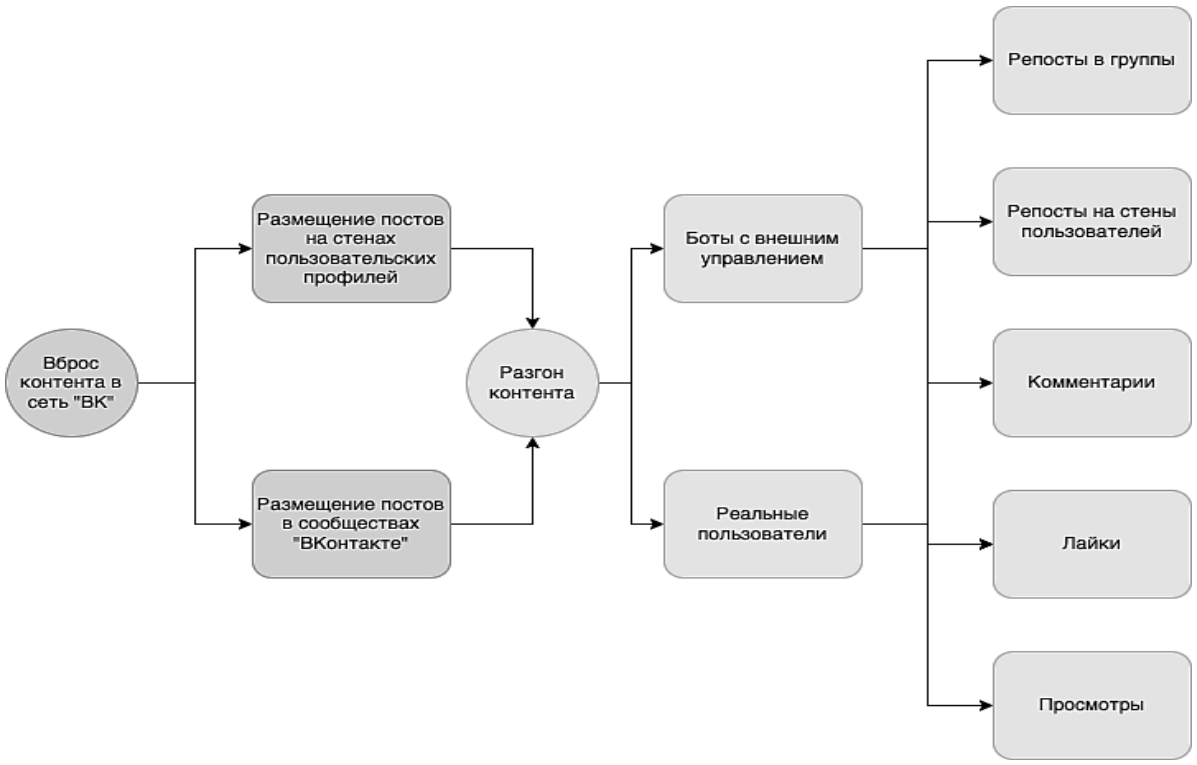

Рис. 4. Общая схема информационной операции по инфоповоду «Дворец Путина»

Видно, что схема активной фазы практически схожа с типовой схемой, приведенной на рис. 1.

Детальный анализ показал, что целью информационной операции «Дворец Путина» являлось достижение максимальных показателей охвата аудитории.

На рис. 5 представлен график частоты публикации дубликатов самого массового информационного трека 963 инфоповода «Дворец Путина».

Рис. 5. График частоты вброса дубликатов в информационной операции «Дворец Путина»

Из рис. 5 следует, что в начальной фазе информационной операции (первые 3 часа) частота публикации дубликатов максимальна. Это свидетельствует в пользу того, что измерение указанной частоты является ключевым элементом выявления начала информационной операции.

Наши исследования подтвердили, что информационные треки с высокой начальной частотой публикации, как правило, имеют гораздо большее количество дубликатов, чем те, которые не идентифицируются как признаки информационной операции.

Высокая начальная частота публикации дубликатов в совокупности с их аномальным количеством является явным признаком информационной операции. Однако такой вывод может быть и ложным в том случае, если все пользователи, опубликовавшие дубликаты в начале предполагаемой информационной операции связаны между собой в сети как друзья или подписчики.

Поэтому прежде, чем делать вывод о том, имеет ли информационный трек признаки информационной операции, необходимо проанализировать социальные связи пользователей, опубликовавших дубликаты.

Авторами проведен анализ связей между пользователями, опубликовавшими первые 10 дубликатов в каждом информационном треке. Согласно схеме, представленной на рис. 5, вброс целевого контента осуществлялся в виде постов или в виде репостов. Соответственно были проанализированы графы связей постеров для одних информационных треков и репостеров – для других.

На рис. 6 представлены графы связей указанных пользователей для информационных треков по инфоповоду «Дворец Путина».

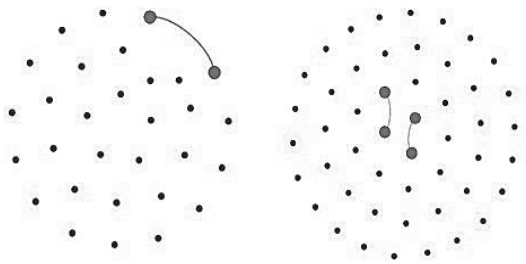

Рис. 6. Графы связей постеров и репостеров по инфоповоду «Дворец Путина»

Анализ обоих графов показывает практически полное отсутствие связей между пользователями, опубликовавшими первые 10 дубликатов за короткий промежуток времени в информационных треках, идентифицированных как признак информационной операции. Отсутствие связей со всей очевидностью указывает на целенаправленный, организованный вброс целевого контента, выступая дополнительным признаком информационной операции.

Исходя из изложенного, этапы методики выявления информационных операций могут выглядеть следующим образом:

– сбор массива публикаций по заданному информационному поводу;

– выявление информационных треков с аномально высокой начальной частотой вбросов дубликатов;

– проверка треков на предмет релевантности;

– формирование списка треков с признаками информационных операций;

– анализ графов связей пользователей, опубликовавших дубликаты в отобранных треках;

– формулирование вывода о том, является ли конкретный инфоповод информационной операцией.

Заключение

При подготовке статьи проведен анализ информационных потоков деструктивного контента, содержащего около 130 тысяч информационных сообщений. Выявлена высокая начальная частота публикации четких дубликатов, распространяемых несвязанными между собой пользователями, как общее свойство, присущее информационным операциям. Это свойство положено в основу методики выявления последних.

Как следует из графика, представленного на рис. 5, эта методика позволяет выявлять информационные операции в первые часы после их начала, что является очень хорошим результатом.

Исследования показали, что этот период может варьироваться в зависимости от конкретной информационной операции, ее мощности, уровня подготовки и других характеристик. Но в целом предложенная в статье методика позволяет выявлять информационные операции на самых ранних стадиях, сокращая время на принятие решений по противодействию деструктивным операциям в социальных сетях и повышая эффективность указанных решений.

В статье проанализированы информационные операции, реализованные по различным сценариям. Один из сценариев отличался тем, что вместо использования

большого количества четких дубликатов вбрасывались небольшие порции нечетких дубликатов, распространяемых в очень короткие промежутки времени ботами (не больше одной секунды).

В этой связи необходимо провести дополнительные исследования характеристик нечетких дубликатов и пользователей, их опубликовавших, на предмет того, не являются ли они ботами. В случае выяснения того, что публикация четких или нечетких дубликатов осуществляется с высокой начальной частотой не связанными между собой ботами, это будет еще одним дополнительным признаком информационной операции. Совокупность же приведенных в статье и дополнительных признаков даст возможность повысить точность детектирования информационных операций

Список литературы

1. Концепция Конвенции ООН об обеспечении международной информационной безопасности / Совет Безопасности Российской Федерации. URL: http://www.scrf.
gov.ru/security/information/document112/
(Дата обращения: 21.10.2022).

2. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века / С. И. Макаренко. Санкт-Петербург: Наукоемкие технологии, 2017. 546 с.

3. Расторгуев С. П. Информационные операции в сети Интернет / С. П. Расторгуев, М. В. Литвиненко, под. общ. ред. А. Б. Михайловского. Москва: АНО ЦСОиП, 2014. 128 с.

4. Нежданов И. Ю. Технологии информационных войн в интернете / Российский союз молодых ученых. URL:http://bash.rosmu.ru/activity/attach/
events/1283/01.pdf (Дата обращения: 21.10.2022).

5. Еременко В. Т. Информационное противоборство в социотехнических системах / В. Т. Еременко, П. Н. Рязанцев. Орел: ОГУ имени И.С. Тургенева, 2016. 209 с.

6. Потемкин А.В. Распознавание информационных операций в средствах массовой информации сети Интернет / А.В. Потемкин // Интернет-журнал Науковедение. 2015. № 3. Т. 7. С. 122.

7. Загорулько Ю. А. Выявление нечетких дубликатов при автоматическом формировании тематических коллекций документов на основе web-публикаций / Ю. А. Загорулько, Н. В. Саломатина, А. С. Серый, Е. А. Сидорова, В. К. Шестаков // Вестник НГУ. Серия: Информационные технологии. 2013. № 4. Т. 11. С. 59-70.

8. Kleinberg J. Temporal Dynamics of On-Line Information Streams // Data Stream Management. 2016. С. 221-238.

9. Корсо Д,. Гулли А., Романи Ф. Ранжирование потоков новостей / Материалы 14-й Международной конференции по Всемирной паутине, WWW 2005, Тиба, Япония, 10-14 мая 2005 г. С. 97-106.

10. Rakesh V. et al. Personalized recommendation of twitter lists using content and network information // Proceedings of the 8th International Conference on Weblogs and Social Media. 2014. № 1. Т. 30. С. 416-425.

11. Ландэ Д. В. Основы моделирования и оценки электронных информационных потоков / Д. В. Ландэ, В. Н. Фурашев, С. М. Брайчевский, А. Н. Григорьев. Киев: Инжиниринг, 2006. 176 с.

12. Додонов А. Г. Распознавание информационных операций / А. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук, С. В. Каденко, А. Н. Грайворонская. Киев: Инжиниринг, 2017. 282 с.

13. Минаев В. А. Системно-динамическое моделирование сетевых информационных операций / В. А. Минаев, М. П. Сычев, Е. В. Вайц, К. М. Бондарь // Инженерные технологии и системы. 2019. Т. 29. № 1. С. 20-39

Московский университет МВД России им. В.Я. Кикотя
V.Ya. Kikot Moscow University of the Russian Internal Affairs Ministry

Пермский государственный национальный исследовательский университет
Perm State National Research University

Поступила в редакцию 30.10.2022

Информация об авторах

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

Рабчевский Андрей Николаевич – канд. техн. наук, старший преподаватель кафедры информационной безопасности и систем связи, Пермский государственный национальный исследовательский университет, e-mail: ran@psu.ru

Мустакимова Яна Романовна – старший преподаватель кафедры информационной безопасности и систем связи, Пермский государственный национальный исследовательский университет, e-mail: mustakimovayr@gmail.com

RECOGNITION OF INFORMATION OPERATIONS IN SOCIAL NETWORKS ON THEIR EARLY STAGES

V.A. Minaev, A.N. Rabchevskiy, Y.R. Mustakimova

The article presents and investigates the schemes of information operations in social networks based on empirical materials. In order to identify the marks of information operations, an analysis was carried out on the VKontakte network of destructive content streams containing about 130 thousand informational messages. It is shown that the marks of information operations are an increasing number of target content publications similar in meaning, a high frequency of publications, a short time interval between publications, and the desire for maximum audience coverage. The high initial frequency of publications of duplicates distributed by unrelated users has been revealed as a common property inherent in information operations. It is proposed to use this property as a mark of information operations. Studies have shown that the technique using this mark allows identifying information operations at the earliest stages, which leads to a shortening of the decision-making time on measures to counteract them and to increase the effectiveness of information counteraction. The stages of the methodology for identifying information operations include: collecting an array of publications on a given information occasion; identifying information tracks with an abnormally high initial frequency of duplicate stuffing; checking tracks for relevance; forming a list of tracks with marks of information operations; analyzing the connections of users who have published duplicates in selected tracks; formulating a final conclusion that whether a specific information occasion is an information operation.

Keywords: information wars, information operations; marks recognition, duplicates of publications, frequency of publications.

Submitted 30.10.2022

Information about the authors

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

Andrey N. Rabchevskiy – Cand. Sc. (Technical), Senior Lecturer of the Department of Information Security and Communication Systems, Perm State National Research University, e-mail: ran@psu.ru

Yana R. Mustakimova – Senior Lecturer of the Department of Information Security and Communication Systems, Perm State National Research University, e-mail: mustakimovayr@gmail.com