# ВВЕДЕНИЕ

Популярность социальных сетей, равно как и возможности информационного воздействия через них на массы людей, стремительно возрастают. Так, например, согласно корпоративной отчетности компании Facebook за второй квартал 2016 года число людей, которые заходят в Facebook хотя бы один раз в месяц, составило 1,712 миллиарда к 30 июня текущего года. При этом порядка 1,1 миллиарда человек заходят в Facebook каждый день [1]. Несмотря на то, что онлайновые социальные сети уже привлекли к себе огромное количество пользователей, их число продолжает расти. Показательной является динамика количества активных пользователей наиболее популярной в нашей стране социальной сети ВКонтакте: в начале 2014 года среднее число посетителей в день составляло более 58 миллионов, в начале 2015 года — более 68 миллионов, а в 2016 году — порядка 78 миллионов пользователей ежедневно. Зарегистрировано на сайте ВКонтакте более 380 миллионов пользователей, из которых более 80 миллионов заходят на сайт каждый день [2].

В отличие от традиционной Web-технологии, основу которой составляет контент, в онлайновых социальных сетях в качестве главного компонента выступают сами пользователи. Они присоединяются к сети, публикуют свой собственный контент и создают связи с другими пользователями. Эта базовая структура связей типа пользователь-пользователь облегчает онлайн-взаимодействие, поиск других пользователей со схожими интересами, а также размещение контента, который был ранее сгенерирован [3].

Одним из предназначений социальных сетей является распространение контента. В онлайновых социальных сетях может распространяться контент различного характера, в том числе деструктивный: призывающий к разжиганию межнациональной и межконфессиональной розни, экстремизму, сепаратизму и др. Согласно п. 43 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31 декабря 2015 года №683 «О стратегии национальной безопасности Российской Федерации» одной из основных угроз государственной и общественной безопасности является деятельность, связанная с использованием информационных и коммуникационных технологий для

распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе. Еще одной угрозой, которая рассматривается в Стратегии национальной безопасности является инспирирование «цветных революций» [4].

Неслучайно в новой редакции Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ № 646 от 5 декабря 2016 года, среди основных угроз информационной безопасности отмечается расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. Отмечается наращивание информационного воздействия на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей. При этом в современном мире наилучшей средой для проведения информационно-психологических атак являются онлайновые социальные сети [5].

Современный характер «цветных революций» в большинстве своем проявляется в применении цифровых технологий, относящихся сегодня к информационному оружию и влекущих за собой мобилизацию общественного протеста, используемого для «высокотехнологичного сноса» политической элиты. Как правило, начальная фаза современных «цветных революций» — «twitter-революция», для осуществления которой, в первую очередь, необходимо иметь достаточное количество активных продвинутых пользователей в социальных сетях Twitter, Facebook, Вконтакте. Для осуществления наращивания социальной базы, которая формирует психологическую среду для реализации информационной составляющей «цветной twitter-революции» простому обывателю достаточно иметь доступ в сеть Интернет и подходящий гаджет. Анализ событий, произошедших в последние годы на территории постсоветского пространства, Ближнего Востока и Азии, показывает, что цифровые технологии «цветных революций» в настоящее время популярны, эффективны и с широким охватом применяются для смены действующего режима власти. Современная власть, стремящаяся сохранить суверенность, должна иметь в своем распоряжении набор инструментов, ограничивающих (сводящих к минимуму) эффективность манипулятивного воздействия «мягкой силы». Государствам необходимо разработать и применять

те сетевые структуры, которые могут эффективно противодействовать проявлению манипуляций в цифровом пространстве, работать в том же операционном поле, что и их противники [6].

Таким образом, онлайновые социальные сети, обладающие чрезвычайной популярностью, являются одним из основных инструментов информационно-психологического воздействия на значительную часть населения, в большей части на молодежь. Необходимость противодействия угрозам информационной безопасности, которые могут быть реализованы через онлайновые социальные сети, подтверждена Стратегией национальной безопасности и Доктриной информационной безопасности Российской Федерации, что указывает на значительную актуальность исследования эпидемических информационных процессов в онлайновых социальных сетях, которые являются взвешенными неоднородными сетями.

Тема исследования социальных сетей является достаточно популярной, свидетельством чему является ряд научно-исследовательских работ [7—29], включая: изучение их метрик [10—13] и структурного анализа социальных сетей; описание [14—18] эпидемических процессов в социальных сетях, в которых традиционно используются аналоговые модели; оценку информационных рисков в социальных сетях [19, 20] и их эпистойкости [21]; вопросы [22, 23] иммунизации и автоматического выявления сообществ [24—26].

Традиционно при описании эпидемических процессов используются аналоговые модели, основанные на дифференциальных уравнениях [14—18]. Однако, анализ указывает на несовершенство этих моделей и наличие целого ряда существенных противоречий.

1. Упомянутая выше аналоговая модель используется для описания эпидемического процесса, который по своей природе является дискретным: количество элементов в системе, как и число зараженных или не зараженных вершин являются дискретными параметрами. В связи с этим, логичным является построение моделей с дискретными по своим значениям переменными.
2. При моделировании различных процессов, в том числе эпидемических, важной является возможность остановки эксперимента в необходимый момент времени и осуществления коррекции защиты по ходу процесса. Аналоговая модель принципиально не позволяет вносить такие изменения в параметры системы. Дискретная модель предусматривает такую возможность, благодаря чему можно провести более

глубокий анализ информационной эпидемии, задавая новые условия на требуемом шаге эксперимента.

3. Особенностью информационной диффузии в онлайновых социальных сетях является репостинг — многократное размещение записи оригинального поста на собственной странице с указанием автора. Дело в том, что благодаря репостам участники социальной сети могут неоднократно подвергаться воздействию одного и того же контента. Дискретная модель позволяет учесть это явление и более адекватно предсказать результаты распространения того или иного контента.
4. Информационные атаки зачастую бывают распределенными. Так, при инфицировании онлайновой социальной сети вполне возможна инъекция деструктивного контента в несколько сетевых элементов одновременно. Дискретная модель, в отличие от аналоговой, позволяет одновременно описывать возникновение эпидемии с несколькими очагами заражения, в том числе в различных слоях сети, что позволяет проследить динамику информационного эпидемического процесса в зависимости от степеней вершин, которые были инфицированы в гетерогенной сети.
5. В онлайновых социальных сетях, как и во всем современном мире, действует закон конкуренции. В связи с этим вопрос противоборства контентов является актуальным при моделировании эпидемического информационного процесса. В аналоговых моделях этот фактор учесть не представляется возможным, в то время как дискретная модель открывает перспективы описания процессов противоборства различных контентов одновременно.

Таким образом, дискретная модель эпидемического процесса имеет ряд преимуществ перед аналоговой. Указанные достоинства заключается не только в более адекватном описании процесса с помощью дискретной модели, но и в более широких ее возможностях с точки зрения анализа и прогнозирования результатов на всевозможных его стадиях и вариантах.

Изложенное выше дает основание утверждать, что проблема повышения защищенности информационных процессов в онлайновых социальных сетях при распространении в них деструктивных контентов представляется чрезвычайно актуальной, а связанные с этим вопросы создания методического обеспечения дискретного вероятностного моделирования возникающих в данном случае эпидемических процессов, его алгоритмизации и реализации в виде программного инструментария автоматизации прогнозных

расчетов, включая комплексный риск-анализ наиболее популярных социальных сетей, имеют значительную не только научную, но и практическую ценность.

Указанной проблематике посвящена настоящая монография, авторы которой выражают благодарность Е.В. Шварцкопф, Е.С. Соколовой, Д.А. Савинову, Д.В. Гусеву, Е.А. Автоновой, Е.В. Гусеву, А.О. Девяшину, К.В. Зайцеву, Р.К. Бабаджанову и В.А. Кургузкину за помощь в подготовке рукописи к публикации.