Минаев В.А.,

доктор технических наук
Московский Ордена почета университет МВД России им. В.Я. Кикотя

Коломина А.В.

Московский Ордена почета университет МВД России им. В.Я. Кикотя

Модели распространения дискредитирующей информации в социальных медиа (обзор)

Социальные медиа формируют среду для реализации разнообразных угроз, направленных на дискредитацию сотрудников организаций и самих организаций. Это актуализирует задачу выявления дискредитирующих кампаний на ранних стадиях их формирования. Ключом к решению данной задачи является математическое моделирование как самих дискредитирующих кампаний, так и признаков их проявления.

Взгляды специалистов позволяет определить дискредитацию как стратегическую технологию информационно-психологического воздействия, реализуемую в киберпространстве и направленную на разрушение доверия, авторитета и деловой репутации путем целенаправленного распространения деструктивной информации манипулятивного характера.

Цель статьи – систематизировать современные методологические подходы и математические модели, применяемые для исследования распространения дискредитирующей информации, и выявить перспективные пути моделирования.

Основные определения

Анализ научных работ позволяет выявить сущность дискредитации через процессы манипулирования общественным сознанием. Так, Г.Г. Почепцов[1] раскрывает ее как технологию информационно-психологического воздействия, направленного на «размытие» или целенаправленное разрушение позитивного имиджа того или иного индивида или организации. В.С. Овчинский[2] подчеркивает, что дискредитация ключевых фигур выступает стандартным инструментом ослабления национальной безопасности и конкурентной борьбы, направленным на деморализацию общества или его отдельных групп.

В работе А.С. Овчинского, К.К. Борзунова и С.О. Чеботаревой[3] дискредитация идентифицируется как ключевой элемент управления в условиях гибридных угроз в системе системообразующих координат (доверие, авто-

[1] Почепцов Г.Г. Информационные войны. М.: Алгоритм, 2015. 254 с.

[2] Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М.: Книжный мир, 2014. 352 с.

[3] Овчинский А.С., Борзунов К.К., Чеботарева С.О. Информационные координаты. Управление. Противоборство. Безопасность. М.: Горячая линия – Телеком, 2025. 280 с.

ритет, репутация), воздействие на которые позволяет управлять массовым сознанием.

Применительно к цифровой среде выделяются следующие формы дискредитации:

пропаганда – систематическое распространение информации, формирующей у целевой аудитории негативное восприятие объекта дискредитации;

клевета – распространение фейковой информации с целью подрыва репутации;

научная манипуляция – применение псевдонаучных данных или результатов экспертиз, вырванных из исходного контекста и подающихся в искаженном виде с целью развития скептического отношения к объекту.

Обзор подходов к моделированию процесса дискредитации

1. *Моделирование инсайдерских угроз* – ключевое направление для решения задач дискредитации, поскольку инсайдер, обладая легитимным доступом к конфиденциальной информации, зачастую выступает не только ее источником, но и активным распространителем, что многократно усиливает репутационные риски. В работе «System Dynamics Based Insider Threats Modeling»[1] применяется системно-динамическое моделирование для анализа мотивационных факторов инсайдеров. Модель включает ключевые переменные Expectations (ожидания), Sense of Achievement (чувство достижения), Disgruntlement (недовольство) и позволяет строить причинно-следственные диаграммы, иллюстрирующие связи между этими переменными и мерами контроля за ними со стороны организации. Имитационные эксперименты показывают, как «ленивый» менеджмент и рост ожиданий сотрудника приводят к инсайдерской атаке, и демонстрируют, как модель повышает вероятность обнаружения таких угроз.

Обзорные исследования[2] отражают критическую важность комплексного учета триады «человеческий фактор – технологическая среда – организационные механизмы». В качестве технологической основы моделирования предлагается использовать такую платформу машинного обучения как Система анализа поведения пользователей и сущностей, а также Систему управления информацией и событиями безопасности. Отметим, что используемые в них модели фокусируются на внутренних аспектах безопасности и слабо учитывают интеграцию внутренних угроз с внешними координированными кампаниями в социальных медиа.

[1] Yang S.- C., Wang Y.- L. System Dynamics Based Insider Threats Modeling // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2015. Vol. 6. № 3. Pp. 61-81. DOI: 10.22667/JOWUA.2015.09.31.061.

[2] Mazzarolo G., Jurcut A.D. Insider threats in Cyber Security: The enemy within the gates // European Cybersecurity Journal. 2020. Vol. 6, Issue 1. Pp. 71-79; CERT Insider Threat Team. Unintentional Insider Threats: A Foundational Study. CMU/SEI-2013-TN-022, 2013. P. 73.

2. *Агент-ориентированное моделирование* и методы теории социального влияния – подход, детально разработанный в исследовании[1] и представляющий собой комплексную агент-ориентированную модель механизмов социального влияния в социальных сетях.

Ключевым методологическим достижением работы Альфа является формализация двух типов социального влияния, основанного на гипотезах из социологии и социальной психологии[2]: нормативное влияние – стремление индивида к конформности под давлением группы; информационное влияние – основанное на принятии компетентности и доверия к источнику информации. Данный подход представляет собой концептуальную основу для исследования механизмов формирования общественного мнения. Однако, будучи сосредоточенной на индивидуальных восприятиях и парных взаимодействиях, используемая в нем модель демонстрирует ограниченные возможности в исследовании полномасштабных дискредитирующих кампаний по дискредитации, где существенную роль играют нелинейные связи.

В качестве примера интеграции агент-ориентированного подхода с аналитическим анализом выступает работа[3]. Применяемые в нем модели характеризуются динамическим мнением и гетерогенной активностью. Динамика мнения каждого агента описывается дифференциальным уравнением, которое учитывает социальное влияние от его соседей во времени. Ключевым механизмом является взаимодействие агентов со схожими взглядами, взаимно усиливающее их убеждения. При этом агенты предпочитают взаимодействовать с теми, чьи мнения близки к их собственным, что приводит к самоорганизации сети вокруг общих позиций.

3. *Стохастические модели распространения информации*, часто реализуемые с помощью библиотек Python (NetworkX, NDLib), оперируют вероятностными закономерностями на уровне популяции.

Классической здесь является модель Дейли-Кендала[4], в которой популяция делится на три группы (невовлеченные, распространители, прекратившие распространять), а динамика описывается системой стохастических переходов с интенсивностями, пропорциональными попарным взаимодействиям между группами.

[1] Alf H. Identifikation von Influentials in virtuellen sozialen Netzwerken. Berlin: Technische Universität Berlin, 2018. 210 p.

[2] Deutsch, Morton/Gerard, Harold B. (1955): A study of normative and informational social influences upon individual judgment // Journal of Abnormal and Social Psychology, 51 (3): C. 629-636.

[3] Baumann F., et al. Modeling Echo Chambers and Polarization Dynamics in Social Networks // Physical Review Letters. 2020. Vol. 124. № 4. Pp. 45-68.

[4] Daley D.J., Kendal D.G. 1965 Stochastic rumors, J. Inst. Maths Applics 1, p. 42.

Модель в работе[1] представляет собой стохастическую модель распространения слухов в сложных сетях, объединяющую модель Маки-Томпсона (вариант модели Дейли-Кендала) и модель SIR (распространение эпидемий). Модель учитывает неоднородность сети и ключевые механизмы прекращения распространения – прекращение при контакте и спонтанное забывание.

Модели в работах[2] добавляют механизмы прекращения распространения, не связанные с контактами. В частности, в работе «The stochastic evolution of rumors within a population» представлена комплексная модель, вводящая дополнительный класс агентов-«инкубаторов». В этой модели распространители могут спонтанно терять интерес к распространяемой информации и переходить в класс «угасших».

Стохастические модели полезны для прогнозирования масштаба и скорости распространения, но не объясняют, почему происходит распространение, не отражают детально социально-психологические механизмы вовлечения.

4. *Системно-динамическое моделирование*.

Классический подход системной динамики, основанный Дж. Форрестером[3] и реализуемый в AnyLogic и других имитационных платформах, позволяет моделировать нелинейные обратные связи в системе на макроуровне.

В прикладном аспекте методы системной динамики адаптированы и развиты в серии работ российских исследователей[4], посвященных моделированию распространения манипулятивного контента и информационного противоборства.

В работе «Имитационные эксперименты с моделью информационно-психологических воздействий на массовое сознание» представлена базовая системно-динамическая модель влияния информационно-психологических воздействий (ИПВ) на массовое сознание, реализованная в среде AnyLogic.

---

[1] Nekovee M., Moreno Y., Bianconi G., Marsili M. Theory of Rumour Spreading in Complex Social Networks // Physica A: Statistical Mechanics and its Applications. 2007. Vol. 374. № 1. Pp. 457-470. DOI: 10.1016/j.physa.2006.07.017.

[2] Dauhoo, M. Z., Juggurnath, D., & Badurally Adam, N. R. (2016). The stochastic evolution of rumors within a population. Mathematical Social Sciences, 82, Pp. 85–96. https://doi.org/10.1016/j.mathsocsci.2016.06.003; Li M. The stochastic evolution of a rumor spreading model with two distinct inhibiting and attitude adjusting mechanisms... // Physica A: Statistical Mechanics and its Applications. 2020. Vol. 562. Pp. 61-81.

[3] Forrester J.W. Industrial Dynamics. Cambridge: MIT Press, 1961. 464 p.

[4] Минаев В. А., Вайц Е. В., Грачева Ю. В. Имитационные эксперименты с моделью информационно-психологических воздействий на массовое сознание // Безопасность информационных технологий. 2017. Т. 24. № 2. С. 61-71; Минаев В.А., Сычев М.П., Вайц Е.В., Бондарь К.М. Системно-динамическое моделирование сетевых информационных операций // Инженерные технологии и системы. 2019. Т. 29. № 1. С. 20-39; Противодействие экстремистской идеологии в социальных медиа: математические модели и методы / В.А. Минаев, К.М. Бондарь и др.. Хабаровск: ДВЮИ МВД России, 2023. 232 с.; Минаев В.А., Корячко А.В., Коломина А. Системно-динамическая модель распространения дискредитирующей информации в социальных медиа // Вестник РГРТУ. 2025. № 93. С. 100-109.

Модель описывается системой дифференциальных уравнений, связывающих ключевые переменные:

S – количество лиц, способных принять идею ИПВ.

Y – количество лиц, принявших идею ИПВ.

$S_Y(t)$ – темп увеличения числа принявших идею.

$Y_S(t)$ – темп уменьшения числа принявших идею (забывание).

Модель включает следующие уравнения:

$$\begin{cases} \dfrac{dY}{dt} = S_Y(t) - Y_S(t) \\ \dfrac{dS}{dt} = Y_S(t) - S_Y(t) \\ S_Y(t) = \dfrac{S * (\alpha * Y + M * b)}{N} \\ Y_S(t) = g * Y \\ \alpha = p * k_0 * E \\ b = k_1 * k_2 \end{cases}$$

где: a – вероятность увлечения идеей при межличностном контакте, b – вероятность увлечения под воздействием средств массовой информации (СМИ), M – массовость СМИ, g – вероятность забывания, p – вероятность коммуникации на тему, k_0, k_1, k_2, n – параметры, регулирующие интенсивность контактов и восприятия.

В последующей работе – «Системно-динамическое моделирование сетевых информационных операций» – модель существенно развита. Предложена комплексная системно-динамическая модель информационного противодействия (ИПД), которая учитывает конкуренцию двух противоборствующих идей – негативной и позитивной. Данная модель описана в виде системы дифференциальных уравнений и реализована в имитационной системе AnyLogic.

Важным результатом, подтверждающим адекватность моделей, является их эмпирическая валидация. Авторы показывают высокую согласованность результатов моделирования со статистическими данными (коэффициент детерминации достигает 95%), а также высокую степень согласования (94%) между системно-динамической и агентной моделями, построенными для одних и тех же процессов. Модели использовались для анализа реальных ситуаций, таких как динамика распространения призывов к оппозиционным митингам в социальной сети «ВКонтакте».

Проведенный обзор позволяет заключить, что современный спектр моделей процессов дискредитации характеризуется разнообразием подходов и математического аппарата.

Агент-ориентированные модели раскрывают механизмы, описанные в теории социального влияния.

Стохастические модели, основанные на модификации моделей эпидемиологического типа, прогнозируют макродинамику процессов.

Системно-динамические модели через систему взаимосвязанных дифференциальных уравнений синтезируя ключевые процессы распространения дискредитирующей информации, учитывают нелинейные обратные связи.

Модели инсайдерских угроз интегрируют модели машинного обучения с моделями системной динамики.

Однако единая методологическая система моделей пока не реализована. Комплексная модель, которая бы объединила качества всех рассмотренных подходов, еще не обоснована и не построена.

Представляется, что наиболее адекватной инструментальной основой для решения такой актуальной задачи является системно-динамическое моделирование в имитационной среде типа AnyLogic. Ее использование позволит построить целостную модель, учитывающую взаимодействие человеческого фактора, технологической среды и институциональных ограничений, и обеспечивающую раннюю диагностику и активное противодействие дискредитирующим кампаниям в социальных медиа.

Макушко А.А.

Московский Ордена почета университет МВД России им. В.Я. Кикотя

Биометрические технологии в деятельности дорожной полиции

Используемые подразделениями ГИБДД автоматизированные системы (АС) обеспечивают сбор, обработку и хранение значительных объемов информации, в том числе персональных данных. Защита вышеуказанных сведений имеет первостепенное значение, так как неправомерный доступ к ним и их разглашение могут повлечь очень серьезные негативные последствия.

Одним из перспективных направлений повышения информационной безопасности данных при эксплуатации АС является использование биометрических технологий. Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» биометрические персональные данные – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Биометрия позволяет идентифицировать пользователей на основе их уникальных биологических характеристик (отпечатки пальцев, радужная оболочка глаза, голос, лицо и т. д). Внедрение биометрических методов защиты информации может значительно повысить надежность АС, эксплуатируемых в подразделениях ГИБДД.