



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

## СОЗДАНИЕ ИСКУССТВЕННЫХ НОВОСТЕЙ ДЛЯ МАНИПУЛЯЦИИ АЛГОРИТМАМИ ПОИСКОВЫХ СИСТЕМ

**Ворошилов Д.В.**

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: superdaniil2002@yandex.ru*

**В эпоху цифровой информации манипуляция алгоритмами поисковых систем стала инструментом влияния на общественное мнение. Создание искусственных новостей позволяет недобросовестным источникам продвигать ложные или искажённые сведения, влияя на информационную повестку. В статье рассматриваются методы создания и распространения фейковых новостей, их влияние на алгоритмы поисковых систем и механизмы борьбы с подобными манипуляциями, включая совершенствование алгоритмов ранжирования и развитие методов выявления недостоверного контента.**

Ключевые слова: Фейковые новости, манипуляция поисковыми системами, алгоритмы ранжирования, информационная безопасность, дезинформация, SEO-манипуляции.

## CREATING FAKE NEWS TO MANIPULATE SEARCH ENGINE ALGORITHMS

**Voroshilov D.V.**

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: superdaniil2002@yandex.ru*

**The manipulation of search engine algorithms has become a powerful tool for influencing public opinion in the digital age. The creation of fake news allows unreliable sources to promote false or distorted information, shaping the information landscape. This article explores the methods of creating and distributing fake news, their impact on search engine algorithms, and mechanisms for combating such manipulations, including improvements in ranking algorithms and the development of methods for detecting unreliable content.**

Keywords: Fake news, search engine manipulation, ranking algorithms, information security, disinformation, SEO manipulation.

### Введение

В современном мире интернет является основным источником информации для большинства людей, а поисковые системы играют ключевую роль в её распространении. Алгоритмы ранжирования, используемые такими системами, как Google и Yandex, определяют, какие страницы попадут в топ выдачи, а значит, какие сведения будут восприняты пользователями как наиболее достоверные. Однако эти алгоритмы не всегда способны отличить правдивый контент от фейкового, чем активно пользуются злоумышленники, создавая искусственные новости для продвижения определённых идей, манипуляции общественным мнением или даже для коммерческих целей.

Распространение фейковых новостей стало острой проблемой, поскольку дезинформация способна влиять на политические процессы, финансовые рынки и общественные настроения. Применяя различные SEO-техники, злоумышленники могут вывести ложную информацию в топ поисковой выдачи, тем самым увеличивая её доверие среди пользователей. Это делает проблему не просто актуальной, но и угрожающей информационной безопасности как отдельных пользователей, так и целых государств.

### **Создание искусственных новостей для манипуляции алгоритмами поисковых систем**

Фейковые новости создаются с целью влияния на общественное мнение или продвижения определённых интересов. Основной принцип заключается в том, чтобы подстроить контент под алгоритмы поисковых систем, обеспечив его видимость в топе поисковой выдачи. Для этого используются несколько методов, каждый из которых играет важную роль в процессе распространения ложной информации[1].

Один из ключевых инструментов для продвижения фейковых новостей — это SEO-оптимизация. Злоумышленники анализируют, какие ключевые слова и фразы чаще всего ищут пользователи, и включают их в текст, заголовки и метаописания своих материалов. Это позволяет обойти алгоритмы фильтрации и сделать ложную информацию максимально релевантной для поисковых систем. Кроме того, активно используются так называемые "контентные фермы" — сети сайтов, публикующие однотипные или переписанные статьи, увеличивающие индексруемость ложных сведений[2].

Ещё одним способом продвижения дезинформации является использование ботов и сетей фейковых аккаунтов в социальных сетях. Автоматизированные системы генерируют репосты, комментарии и лайки, создавая видимость популярности фейковой новости. В результате поисковые алгоритмы воспринимают материал как "актуальный" и поднимают его выше в результатах выдачи[3].

Кроме того, злоумышленники могут использовать взломанные или специально созданные сайты с высоким уровнем доверия, чтобы размещать там фейковый контент. Такие ресурсы, уже имея репутацию надёжных источников, способствуют распространению ложных сведений через поисковики, поскольку их материалы воспринимаются как заслуживающие доверия[4].

Одним из самых изощрённых методов является "петля подтверждения", когда несколько фейковых сайтов ссылаются друг на друга, создавая иллюзию достоверности информации. Поисковые алгоритмы, основанные на оценке ссылочной массы, могут принять такую информацию за правду, что приводит к её массовому распространению.

Чтобы бороться с подобными манипуляциями, поисковые системы разрабатывают всё более сложные алгоритмы проверки достоверности контента. Google, например, внедрил технологию E-E-A-T (Experience, Expertise, Authoritativeness, Trustworthiness — опыт, экспертиза, авторитетность, надёжность), которая оценивает не только содержание статьи, но и авторитетность источника. Однако злоумышленники находят способы обхода таких проверок, создавая псевдонаучные публикации или ссылаясь на якобы экспертные мнения[5].

Несмотря на все усилия поисковых систем, проблема фейковых новостей остаётся актуальной. Манипуляции алгоритмами могут оказывать влияние не только на общественное

мнение, но и на важные экономические и политические процессы. В связи с этим возникает необходимость в более жёстких мерах контроля за распространяемой информацией.

### **Заключение**

Создание искусственных новостей с целью манипуляции алгоритмами поисковых систем является серьёзной угрозой для информационной безопасности. Используя методы SEO, ботовые сети и поддельные источники, злоумышленники способны продвигать ложную информацию, создавая у пользователей ложное представление о реальности.

Поисковые системы, такие как Google и Yandex, активно разрабатывают механизмы борьбы с фейковыми новостями, внедряя алгоритмы, оценивающие достоверность источников и анализирующие поведенческие факторы пользователей. Однако борьба с дезинформацией остаётся сложной задачей, так как злоумышленники постоянно находят новые способы обхода фильтров.

Для эффективного противодействия распространению фейковых новостей необходим комплексный подход, включающий развитие технологий анализа контента, усиление контроля над источниками информации и повышение цифровой грамотности пользователей. В условиях стремительного роста цифровой информации осведомлённость о методах манипуляции данными становится ключевым фактором защиты от дезинформации.

### **Список литературы**

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Душин С. Е. и др. Синтез структурно-сложных нелинейных систем управления. – 2004.
4. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
5. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 92-101.

### **References**

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
2. Minyaev A. A. Method for evaluating the effectiveness of information security systems of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020). 2020. pp. 716-719.
3. Dushin S. E. et al. Synthesis of structurally complex nonlinear control systems. – 2004.

4. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
  5. Krasov A.V. et al. Current threats to information security in the field of healthcare and ophthalmology //Ophthalmosurgery. – 2022. – No. 4s. – pp. 92-101.
-