СОЦИАЛЬНЫЕ СЕТИ И КИБЕРПРЕСТУПНОСТЬ

Норкулова Гавхаршодбегим Алишер кизи

https://doi.org/10.5281/zenodo.8076593

Отказавшись от анонимности, которая ранее была типична для онлайн-общения, миллиарды людей устремились на сайты социальных сетей, где участники создают и поддерживают личные профили, которые они связывают с профилями других участников. Образовавшаяся в результате сеть “друзей” или “контактов”, имеющих схожие интересы, бизнес-цели или академические курсы, заменила для многих людей, особенно молодежи, устаревшие концепции сообщества. Самые простые социальные сети позволяют друзьям комментировать профили друг друга, отправлять личные сообщения внутри сети и перемещаться по расширенной сети друзей, видимой в профиле каждого участника. Более продвинутые сети позволяют участникам улучшать свои профили с помощью аудио- и видеоклипов, а некоторые открывают исходный код своего программного обеспечения, чтобы сторонние разработчики могли создавать приложения или виджеты — небольшие программы, которые запускаются на странице профиля участника. Эти программы включают в себя игры, викторины, инструменты для обработки фотографий и новостные ленты. В лучшем случае сайт социальной сети функционирует как творческий улей, где пользователи и разработчики подпитываются желанием друг друга видеть и быть замеченными. Критики, однако, рассматривают эти сайты как грубые конкурсы популярности, в которых “опытные пользователи” стремятся к наименьшему общему знаменателю в стремлении приобрести как можно больше друзей. Учитывая, что миллиарды уникальных посетителей пользуются многими подобными сайтами по всему миру, безусловно, можно наблюдать обе крайности — часто в пределах одной и той же группы “друзей”.

Платформы социальных медиа стали основными источниками новостей и информации для значительной части населения. Простота обмена и распространения информации на этих платформах привела к быстрому распространению фальшивых новостей, что делает крайне важным понимание их влияния на общество и кибербезопасность.

Также в данной работе рассматривается распространение фальшивых новостей. Фальшивые новости способны манипулировать общественным мнением, подрывать доверие к институтам и способствовать социальным беспорядкам. Изучая динамику распространения фальшивых новостей в

сетях социальных медиа, данное исследование может дать представление о факторах, способствующих их широкому распространению.

Распространение фальшивых новостей в социальных сетях может иметь значительные последствия для кибербезопасности. Оно может привести к распространению вредоносных программ, фишинговых атак и краже личных данных, создавая риски для отдельных людей, организаций и даже национальной безопасности. Понимание этих последствий необходимо для разработки эффективных стратегий кибербезопасности.

Фальшивые новости способны формировать общественный дискурс, влиять на выборы и усугублять социальные разногласия. Изучая мотивы создания и распространения фальшивых новостей в социальных сетях, данное исследование может способствовать более глубокому пониманию их влияния на общество .

Онлайн-платформы должны брать на себя ответственность за предоставляемые ими информацию. Платформы социальных сетей играют решающую роль в борьбе с распространением фальшивых новостей. Анализ эффективности текущих технологических и политических мер, реализуемых этими платформами, может дать представление об их ответственности и необходимости совершенствования стратегий борьбы с фальшивыми новостями и защиты пользователей.

Также большую роль играет осведомленность и образование пользователей. Понимание поведения пользователей, когнитивных предубеждений и общественных факторов, связанных с потреблением и распространением фальшивых новостей, может помочь в разработке образовательных инициатив, способствующих развитию критического мышления, медиаграмотности и ответственного поведения в Интернете.

Список исп. литературы:

1. Goodman, Marc D. and Brenner, Susan W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, Vol. 10, No. 2, 139-223.

2. International Telecommunication Union (ITU). (2012). Understanding cybercrime: Phenomena, challenges and legal response.

3. Maras, Marie-Helen. (2014). Computer Forensics: Cybercriminals, Laws and Evidence, second edition. Jones and Bartlett.