

Цифровая личность как фактор социальной коммуникации: актуальные вопросы

Научный руководитель – Гладченко Ирина Алексеевна

Цзя Шуюэ

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра международной коммуникации, Москва, Россия

E-mail: 15502473805@163.com

Как новый тип представления идентичности в цифровую эпоху, цифровая личность постепенно становится важным фактором социальной коммуникации, который нельзя игнорировать. Цифровая личность не только отражает идентификационные характеристики людей в киберпространстве, но и влияет на социальное взаимодействие людей и методы распространения информации. Однако с широким распространением цифровой идентификации возник ряд проблем, таких как конфиденциальность и безопасность, проверка подлинности и цифровой разрыв. Эти проблемы не только угрожают цифровым правам и интересам отдельных лиц, но и создают проблемы для здорового развития социальных коммуникаций. Поэтому исследования роли цифровой личности в социальной коммуникации и проблем, с которыми она сталкивается, имеют огромное значение для содействия гармоничному развитию общества в эпоху цифровых технологий.

«Цифровая личность - это человек, который обладает свободой, сформированной цифровой грамотностью, осознанно создает свой цифровой образ на основе соблюдения нормативных норм и этических ценностей, несет персонализированную ответственность за сохранность данных и содержание цифрового контента, соблюдает правила кибербезопасности, имеет цифровой профиль для реализации личностных потребностей и гражданских прав, контролирует свой цифровой след и адекватно относится к цифровым инновационным преобразованиям» [1]. Цифровая личность обладает такими характеристиками, как множественность, динамика и пластичность. Эти характеристики делают цифровую личность сложным и гибким фактором социальной коммуникации, который не только предоставляет новые возможности для самовыражения и социального взаимодействия, но и создает множество проблем.

Формирование цифровой личности зависит от сбора и анализа больших объемов персональных данных, что увеличивает риск утечки личной информации. Такие проблемы, как злоупотребление данными и кража личных данных, становятся все более серьезными, угрожая цифровой безопасности и правам отдельных лиц. Второй вопрос - это вопрос проверки подлинности. Использование систем управления идентификационными данными в качестве систем управления рисками создает ситуацию, в которой безопасность снижается, поскольку действительно опасные пользователи будут представлены или аутентифицированы как обладающие явно безопасными идентификационными данными [5]. Виртуальный характер цифровой личности облегчает подделку личных данных и распространение ложной информации. Вопрос о том, как создать эффективный механизм цифровой аутентификации, стал ключом к поддержанию целостности сети и социального порядка. Наконец, существует проблема цифрового неравенства. Такого рода неравенство не только усугубляет социальную дифференциацию, но и может еще больше увеличить разрыв в реальном обществе.

Учитывая проблемы, с которыми сталкивается цифровая личность в социальной коммуникации, необходимо принять множество контрмер. Это включает в себя совершенствование законов и нормативных актов о защите данных, совершенствование технологий

защиты данных и повышение осведомленности о защите персональных данных. В то же время для создания методики защиты цифровой личности нужно понимать, что является этой цифровой личностью в конкретном контексте, какие атрибуты в нее входят. Отсутствие единого определения, которое задало бы условия приравнивания конкретного набора данных к цифровой личности, также является проблемой [3]. Также необходимо усовершенствовать механизм проверки подлинности. Этого можно достичь за счет разработки надежной технологии цифровой идентификации личности, создания кросс-платформенной системы оценки кредитоспособности и усиления надзора и правоприменения в киберпространстве. Цифровой кодекс должен объединить в единую инфраструктуру комплексное регулирование развития IT-технологий и инфраструктуры связи и формировать общую систему правовых норм для этих отраслей, в основе которой должна быть обеспечена безопасность личности гражданина [2]. Наконец, следует предпринять усилия по продвижению цифровой инклюзивности. Правительству и связанным с ним организациям следует разработать политику, направленную на обеспечение справедливого распределения цифровых ресурсов и оказание необходимой поддержки и обеспечения справедливого развития цифрового общества. Также важным аспектом является исследование роли цифровой личности в формировании и распространении дипфейков. Дипфейк превратился из развлекательной технологии в опасное цифровое оружие. Современный цифровой человек находится в состоянии выбора дальнейшего движения либо к цифровому апокалипсису, либо к гуманистическому ренессансу [4].

Являясь важным фактором социальной коммуникации в эпоху цифровых технологий, цифровая личность не только предоставляет новые возможности для самовыражения и социального взаимодействия, но и создает ряд проблем. В будущем, с развитием технологий и улучшением социального познания, цифровая личность будет играть все более важную роль в социальной коммуникации и способствовать построению гармоничного и инклюзивного цифрового общества.

Источники и литература

- 1) Бороненко Т.А., Кайсина А.В., Федотова В.С. Цифровая грамотность цифровой личности: к вопросу об уточнении понятий // Инновационные проекты и программы в образовании. 2020. №4 (70). URL: <https://cyberleninka.ru/article/n/tsifrovaya-gramotnost-tsifrovoy-lichnosti-k-voprosu-ob-utochnenii-ponyatiy> (Дата обращения: 26.06.2022).
- 2) Лукошкин А.А. Цифровая безопасность личности в условиях развития цифрового права // Образование и право. 2024. №1.
- 3) Осанова А.С., Жукова М.Н. О проблемах обеспечения безопасности цифровой личности // Актуальные проблемы авиации и космонавтики. 2021.
- 4) Савушкина М.А. Дипфейк как цифровое оружие гибридной войны // Вестник ОмГУ. 2024. №4.
- 5) Camp L. "Digital identity," in IEEE Technology and Society Magazine. Vol. 23.(3). Pp. 34-41. Fall 2004. doi: 10.1109/MTAS.2004.1337889.