

Е. Н. Каменская, Н. К. Дедюлина

КОНТЕНТНЫЕ УГРОЗЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА

Аннотация. В статье рассматриваются контентные угрозы информационно-психологической безопасности человека в условиях цифровизации общества. Авторы анализируют характерные особенности негативного информационно-психологического воздействия, классифицируют виды контентных угроз и критерии их вредоносности. Особое внимание уделяется фейковой информации, её эволюции, способам распространения и методам распознавания. Исследуется влияние деструктивного контента на традиционные духовно-нравственные ценности российского общества. На основе проведённого анализа предлагаются подходы к повышению устойчивости личности и социальных групп к контентным угрозам.

Ключевые слова: информационно-психологическая безопасность, контентные угрозы, фейковая информация, деструктивное воздействие, традиционные ценности, цифровизация, медиаграмотность, информационные риски.

Для цитирования: Каменская, Е. Н. Контентные угрозы информационно-психологической безопасности человека / Е. Н. Каменская, Н. К. Дедюлина // Труды Ростовского государственного университета путей сообщения. – 2025. – № 4. – С. 47–52. – DOI 10.46973/1818-5509_2025_4_47.

Современный человек является активным социальным субъектом, взаимодействующим в информационном пространстве с другими людьми и нуждающийся в притоке информации из различных источников. Такими источниками являются личный опыт и общение, книги, СМИ, Интернет, социальные сети и др. При этом наблюдается увеличение доли информации, получаемой человеком из информационных источников, чем из личного опыта. Он становится более зависимым от информационных ресурсов и цифровых технологий.

Информационные риски представляют опасность сознанию и здоровью пользователей (опасный контент, неприемлемое поведение, ощущения безнаказанности, анонимности собственных действий в Интернете, вовлечение в деструктивное поведение, потребление недостоверной информации и т.д.).

Контентное негативное информационно-психологическое воздействие представляет собой влияние негативного контента, когда прямая коммуникация людьми не осуществляется (например, распространение порнографического контента, фото- и видеоматериалов насилия, террористических действий) [2].

Характерные черты угроз информационно-психологической безопасности [2]:

- 1) наличие латентного периода начала негативного информационно-психологического воздействия и сложности в его обнаружении, идентификации,
- 2) возможности изменения территориального масштаба воздействия,
- 3) сложный многоуровневый характер воздействия,
- 4) отсутствие точности в прогнозе эффективности влияния на человека, социальные группы, возможности сопротивления человека (социальной группы) благодаря имеющимся механизмам психологической защиты и навыкам, полученным в ходе обучения технологиям устойчивости к негативным информационно-психологическим воздействиям,

5) значительное снижение или даже блокирование негативного эффекта информационно-психологического воздействия в зависимости от информированности человека (социальной группы), негативное влияние на государственное управление.

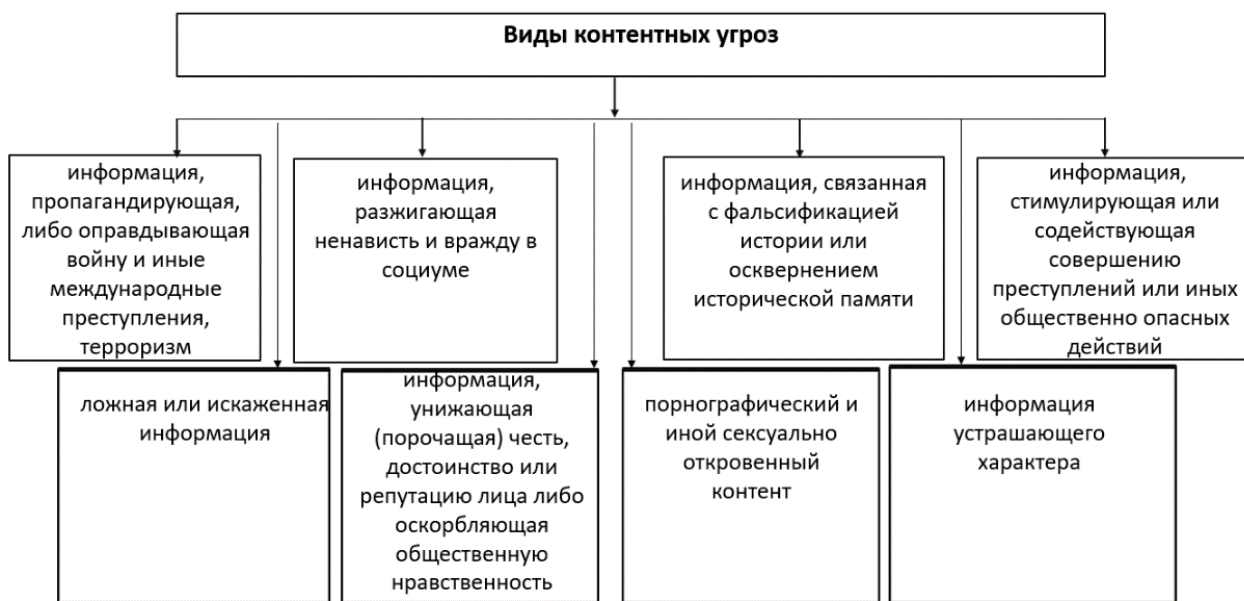


Рис. 1. Виды контентных угроз

Контентные угрозы включают виды информации с вредным, опасным негативным контентом, основной источник которых является массмедиа. Виды контентных угроз отражены на рис. 1, каждая, из которых, отличается специфическим механизмом деструктивного информационно-психологического воздействия, направленного на человека и социальную группу [2].

Критерии вредоносности контентных угроз (рис. 2).

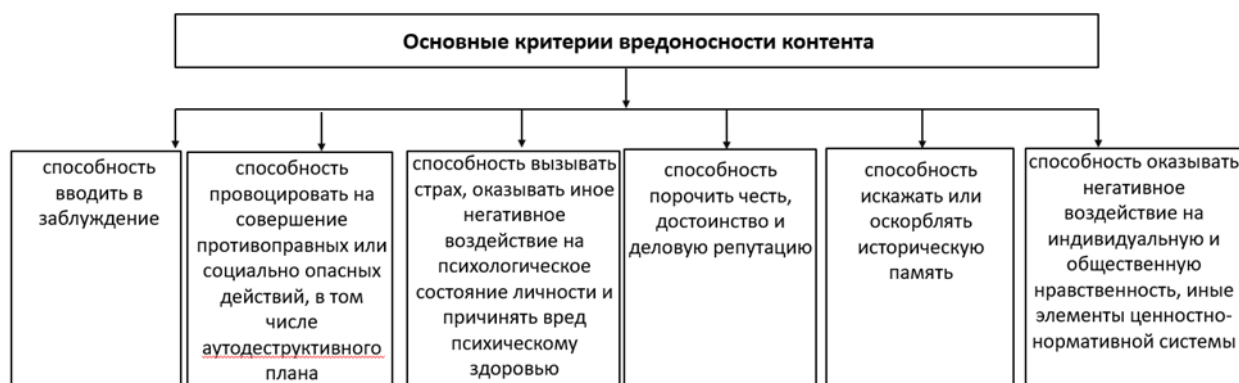


Рис. 2. Критерии вредоносности контента

В настоящее время обострилась проблема распространения фейков, передающих ложную информацию. Фейковый контент включает недостоверную текстовую информацию, фото-, видео-, аудиоматериалы, сайты и аккаунты в социальных сетях, содержащие недостоверные данные.

Одним из первых фейков в истории считается методика защиты страуса от опасности (спрятать голову в песок), стартовавший благодаря Плинию Старшему еще в Древнем Риме.

Приведем несколько примеров фейков. В 1990 г. свидетельства о терроризме в Кувейте, полученные от девочки Наиры, представляет собой первый спланированный,

постановочный политический фейк. Пример еще одного политического фейка, первого с распространением через сеть Интернет: утверждение о существовании плана Югославии «Подкова» по осуществлению этнических репрессий в Косово. Далее политический фейк в 2003 г. о существовании у Ирака оружия массового поражения с демонстрацией образцов химического оружия К. Пауэллом на Совете Безопасности ООН, который стал поводом вторжения американцев в Ирак. Примером неполитического фейка в 1998 г. является утверждение британского врача Э. Уэйкфилда о влиянии прививки от кори на развитие аутизма у детей, последствиями которого стали массовые отказы родителей вакцинировать детей и результатом вспышки кори (2006 и 2008), приведшие к гибели детей.

Эволюция средств массовой информации непосредственно связана с продвижением и отчасти фейковой информации, поскольку захватывающие сюжеты привлекают внимание людей и расширяют аудиторию издания или канала, увеличивают число просмотров. Фейки возродились с новой силой, благодаря появлению сети Интернет и его возможностей в быстром и легком распространении информации. Цели распространения фейков могут варьироваться от развлекательных до мошеннических и политических (рис. 3) [1].

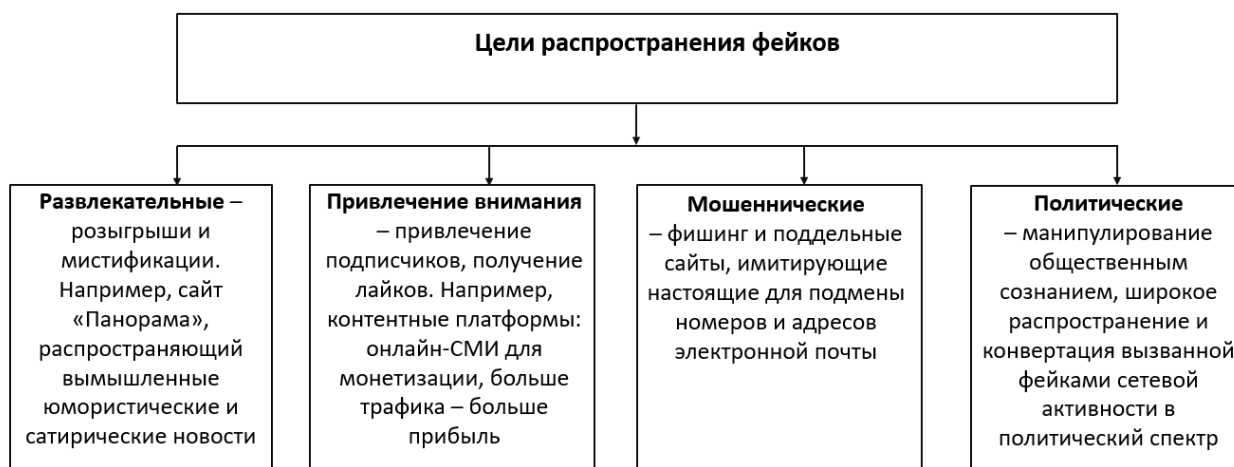


Рис. 3. Цели распространения фейков

Цифровизация информационных технологий стала причиной появления искусственно созданных видео- и аудиозаписей посредством нейросетей, абсолютно похожих на оригинал. Медиафайлы, включающие фото-, видео-, аудиоматериалы, полученные данным способом, или дипфейки, основанные на синтезе изображения или голоса человека с применением искусственного интеллекта часто применяется при финансовых мошеннических операциях.

Фейки в зависимости от уровня достоверности информации разделяются на следующие виды:

1. Фейки, основанные на реальных событиях, с добавлениями фальшивых деталей и обстоятельств, которые оказывают на пользователя эмоциональное давление и подводят к желательным выводам для распространения нужных идей, провокации споров, разжигания дискуссий.

2. Частичные фейки содержат сведения, не имеющие фактической значимости, которые включают фрагментарные достоверные сведения в сочетании с недостоверными. Такие сообщения используют для подмены новостной повестки, текущей обстановки, например, сообщения из жизни шоу-бизнеса.

3. Полные фейки содержат фальшивые, ложные сообщения. Такие сообщения не имеют информационной значимости, их целью является формирование отношения к теме фейка и провоцирование тиражирования обсуждения этой темы в социальных сетях и интернет-пространстве.

Распространение фейков охватывает большие аудитории благодаря использованию следующих инструментов [1]:

1. Задействование квази-СМИ или сайтов, изображающих интернет-СМИ, посвященные определенным темам, которые автоматически наполняются соответствующими тематике новостями, позаимствованными с похожих информационных ресурсов. Создается иллюзия работы реальных средств массовой информации, имитация посещаемости сайта и его продвижение в поисковых системах. При этом отсутствуют собственные авторские материалы площадки или демонстрируется их минимальное количество.

2. Применение одноразовых страниц или сайтов, имитирующих известные веб-сайты СМИ, онлайн платформы, сетевые издания. При этом учетные записи домена раскрывают данный сайт-фальшивку датой регистрации сайта и информацией о владельцах или сокрытие этой информации.

3. Имитирование известных средств массовой информации для постоянного распространения долгосрочных фейков с помощью псевдо-источников системы одноразовых страниц. При этом первый псевдо-источник помещается на иностранный хостинг для имитации достоверности.

Естественное распространение информации осуществляется при концентрической передаче данных из первоисточников и транслируется недолго, если не появляются новые подробности.

Искусственное распространение информации осуществляется по цепочке между связанными профилями, не охватывающими большие аудитории по отдельности, но вместе создающие иллюзию глобальности. В этом случае трансляция будет длительной.

Для распознавания фейкового текста необходимо:

- 1) отметить факты и соотнести заголовок и содержание информационного материала;
- 2) затем провести проверку источника (информационная история источника, количество опубликованных на ресурсе материалов, качество материалов, авторство);
- 3) найти подтверждающую информацию, используя независимые, достоверные источники, компетентные в данной сфере;
- 4) оценить скорость распространения данной информации (целенаправленное распространение информации чаще всего отличается ее высокой скоростью передачи);
- 5) проанализировать, какую психологическую реакцию вызывает сообщение, кому это может быть выгодно и в чем смысл сообщения (передача информации или эмоциональное воздействие),
- 6) изучить детально фотоматериалы, цитаты, ссылки на источники.

Для опознавания фейкового изображения необходимо:

- 1) исследовать его уникальность с помощью сервиса поиска по картинкам;
- 2) найденные изображения проанализировать (оценить похожие, проверить даты публикации дубликатов);
- 3) проверить метаданные картинки (дата, время создания и последней обработки, данные геолокации), применив стандартные средства Windows.

Внешнее разрушительное контентное информационно-психологическое воздействие приводит к идеологическому подрыву традиционных российских духовно-нравственных ценностей, усугублению демографической ситуации в стране, культивированию деструктивной идеологии, «включая культивирование эгоизма, вседозволенности, безнравственности, отрицание идеалов патриотизма, служения Отечеству, естественного продолжения жизни, ценности крепкой семьи, брака, многодетности, созидательного труда, позитивного вклада России в мировую историю и культуру, разрушение традиционной семьи с помощью пропаганды нетрадиционных сексуальных отношений» [3].



Рис. 4. Традиционные ценности

В современном российском обществе одним из важных вопросов на текущий момент является сохранение традиционных ценностей (рис. 4), представляющих собой моральные принципы, закладывающие основы мировоззрения россиян, которые передаются из поколения в поколение, и на базе которых формируется общероссийская гражданская идентичность и единое культурное пространство страны.

Список литературы

1. Основы безопасности жизнедеятельности / Под ред. Ю. С. Шойгу / Ю. С. Шойгу, Е. Н. Байбарина, В. А. Зув. – М., «Просвещение», 2024. – 256 с.
2. Смирнов, А. А. Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации. Монография / А. А. Смирнов. – СПб.: Издательство «Русь», 2022. – 272 с.
3. Указ Президента РФ от 9 ноября 2022 г. № 809 “Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей”.

References

1. Fundamentals of Life Safety / Ed. by Yu. S. Shoigu / Yu. S. Shoigu, E. N. Baibarina, V. A. Zuev. – M., "Education", 2024. – 256 p.
2. Smirnov, A. A. Formation of a system of legal support for information and psychological security in the Russian Federation. Monograph / A. A. Smirnov. – St. Petersburg: Rus Publishing House, 2022. – 272 p.
3. Decree of the President of the Russian Federation of November 9, 2022 No. 809 “On approval of the Fundamentals of State Policy for the Preservation and Strengthening of Traditional Russian Spiritual and Moral Values”.

E. N. Kamenskaya, N. K. Dedyulina

CONTENT THREATS TO INFORMATION AND PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL

Abstract. The article examines content threats to the information and psychological security of individuals in the context of societal digitalization. The authors analyze the characteristic features of negative information and psychological influence, classify types of content threats, and define criteria for their maliciousness. Special attention is paid to fake information, its evolution, dissemination methods, and recognition techniques. The influence of destructive content on the traditional spiritual and moral

values of Russian society is investigated. Based on the conducted analysis, approaches to enhancing the resilience of individuals and social groups to content threats are proposed.

Keywords: information and psychological security, content threats, fake information, destructive influence, traditional values, digitalization, media literacy, information risks.

For citation: Kamenskaya, E. N. Content Threats to Information and Psychological Security of the Individual / E. N. Kamenskaya, N. K. Dedyulina// Trudy Rostovskogo gosudarstvennogo universiteta putej soobseniya. – 2025. – № 4. – P. 47–52. – DOI 10.46973/1818-5509_2025_4_47.

Сведения об авторах

Каменская Елена Николаевна

ФГАОУ ВО «Южный федеральный университет» (ЮФУ),
Институт компьютерных технологий и
информационной безопасности,
кафедра «Психологии и безопасности
жизнедеятельности»,
д.п.н., профессор,
e-mail: kamenskyaen@sfedu.ru

Дедюлина Нина Константиновна

ФГАОУ ВО «Южный федеральный университет» (ЮФУ),
Институт компьютерных технологий и
информационной безопасности,
Студент

Information about the authors

Kamenskaya Elena Nikolaevna

Southern Federal University (SFU),
Institute of Computer Technology and
Information Security,
Chair «Psychology and Life Safety»,
Doctor of Pedagogical Sciences, Professor,
e-mail: kamenskyaen@sfedu.ru

Dedyulina Nina Konstantinovna

Southern Federal University(SFU),
Institute of Computer Technology and
Information Security,
Student