СОЦИАЛЬНАЯ СТРУКТУРА, СОЦИАЛЬНЫЕ ИНСТИТУТЫ И ПРОЦЕССЫ
SOCIAL STRUCTURE, SOCIAL INSTITUTES AND PROCESSES

УДК 316.77: 316. 324.8 **DOI: 10.18413/2408-9338-2018-4-3-0-3**

Бердник Е. А.

Рефлексируемые риски сетевых коммуникаций (результаты онлайн опроса российской молодежи)

Белгородский государственный национальный исследовательский университет
ул. Победы, 85, г. Белгород, 308015, Россия
k_berdnik@inbox.ru

Статья поступила 1 августа 2018 г.; Принята 2 сентября 2018 г.; Опубликована 30 сентября 2018 г.

Аннотация. В статье осуществлена ревизия новейших рисков и угроз, связанных с технологизацией информационно-коммуникативной сферы, а также представлены основные направления научного теоретизирования в указанной области. Особое внимание уделено рассмотрению новых вызовов, которые еще не нашли своего отражения в качестве таковых ни в научном сообществе, ни в политико-правовых документах Российской Федерации, таких как: технологии анализа Больших данных, переход от «социального Web» (Web 2.0) к «когнитивному Web» (Web 3.0), технологии дополненной реальности, трансмедийная трансляция контента. Делается вывод о том, что наличие обозначенных рисков в процессе сетевых коммуникаций молодежи обуславливает необходимость формирования практик их успешной нейтрализации и минимизацию их негативного воздействия. В этой связи в статье актуализируется эмпирический анализ рефлексивной оценки молодыми людьми собственной безопасности в процессе сетевых коммуникаций. Представлены результаты онлайн анкетирования молодых российских пользователей социальной сети «Вконтакте», на основании которых делается вывод о том, что большая часть молодых людей склонна не фиксировать или игнорировать риски и угрозы в процессе сетевых коммуникаций, отмечая, что сталкиваются с последними редко или практически никогда. Подтверждается гипотеза о дифференцированном восприятии молодыми людьми своей безопасности в Сети, которое коррелирует с их социально-демографическими показателями и ценностными установками.

Ключевые слова: сетевые коммуникации; информационно-коммуникативные риски; информационная безопасность; технологизация информационной сферы; Большие данные; когнитивный Web; молодежь.

Информация для цитирования: Бердник Е. А. Рефлексируемые риски сетевых коммуникаций (результаты онлайн опроса российской молодежи) // Научный результат. Социология и управление. 2018. Т. 4, N 3. С. 29-44. DOI: 10.18413/2408-9338-2018-4-3-0-3.

Ekaterina A. Berdnik

Reflected risks of network communications (the Russian youth online survey results)

Belgorod State National Research University
85 Pobedy St., Belgorod, 308015, Russia
k_berdnik@inbox.ru

Received on August 1, 2018; Accepted on September 2, 2018; Published September 30, 2018

Abstract. The author revises the latest risks and threats associated with technologization of the information and communication sphere, and presents the main directions of scientific theorization in this area. Special attention is paid to the new challenges, which have not yet been reflected as threats in the scientific community or in the political and legal documents of the Russian Federation, such as: Big Data analysis technologies, the transition from the "social Web" (Web 2.0) to the "cognitive Web" (Web 3.0), the augmented reality technologies, and transmedia content delivery. It is concluded that the presence of identified risks in the young people network communication process necessitates their neutralization practices formation and negative impact minimization. In this regard, the article actualizes the empirical analysis of young people's reflexive evaluation of their own safety in the network communications process. The article presents the results of the online survey involving young Russian users of the social network "Vkontakte". The survey enabled to draw a conclusion that the majority of young people tend not to fix or to ignore risks and threats in the network communications process, noting that they rarely or almost never faced the latter. The author confirms the hypothesis of young people's safety in the Network differentiated perception, which correlates with their socio-demographic indicators and values.

Keywords: network communications; information and communication risks; information security; technologization of information and communication sphere; Big Data; cognitive Web; youth.

Information for citation: Berdnik, E. A. (2018), "Reflected risks of network communications (the Russian youth online survey results)", *Research Results. Sociology and management*, 4 (3), 29-44, DOI: 10.18413/2408-9338-2018-4-3-0-3.

Введение (Introduction). Бурное развитие информационно-коммуникативных технологий последние пятьдесят лет обуславливает необходимость выработки новых правил существования и взаимодействия в условиях беспрецедентной прозрачности, транспорентности и транзитивности современного мира. Все чаще на международных площадках обсуждаются вопросы будущего человеческой цивилизации в новых технологических условиях, а также этические нормы, выработка которых необходима для безопасного существования человека в транспорентном сетевом мире, наполненном роботами, при этом на первый план выдвигается оценка «человекомерных» эффектов технологизации информационно-коммуникативных процессов.

В научном сообществе также предпринимаются попытки осмысления экзистенциальной угрозы, вызванной технологическим развитием, становлением глобального сетевого информационного-коммуникативного пространства с функционирующими в нем роботами и искусственным интеллектом, тотальной транспорентностью социальных взаимодействий, а также снижением эффективности государственного управления. Так, швейцарский

ученый-футуролог Герд Леонхард в своей книге «Технология против человечности» (Leonhard, 2016) пытается предсказать риски существования человека в полностью оцифрованном сетевом мире. Автор настаивает на создании Глобального этического совета по цифровым вопросам (Global Digital Ethics Council) и формулирует глобальный манифест киберэтики, в котором отстаиваются права человека на то, чтобы оставаться натуральным (т.е. не размещать технологии внутри своего тела для пользования публичными сервисами и социального взаимодействия); быть неэффективным (иметь возможность быть медленнее, чем технические системы), отключаться от сетей, оставаться анонимным, иметь возможность нанимать людей вместо роботов.

Профессор Оксфордского университета, директор Института будущего человечества, философ Ник Бостром также анализирует угрозы и риски существования человеческой цивилизации в новых технологических условиях (Бостром, 2016). При этом источником существенных опасностей автор называет искусственный интеллект, который может превратиться в суперинтеллект со своими потребностями, целями и будет конкурировать с человеком за доступ к ресурсам. Нейтрализацию обозначенных угроз автор предлагает осуществлять по пути совершенствования средств контроля над сетевыми технологиями, а также, в противовес Герду Леонхарду, отстаивает идею использования технологических достижений для улучшения умственных и физических возможностей человека и обеспечения конкурентоспособности в роботизированном мире.

Траектории социализации и становления подрастающего поколения в новой сетевой информационно-коммуникативной реальности также вызывают много вопросов. Так, российский социолог, директор Фонда «Общественное Мнение» Лариса Паутова отмечает, что «поколение z», пришедшее на смену «поколению y» после 2000-х г.г., имеет ряд характерных черт (Исследователь 2.0: трансформация профессии в цифровую эпоху, 2017). К ним можно отнести следующее: индивидуализм, стремление к самореализации и поиску «дзен» в противовес карьерному росту любой ценой, отсутствие опыта жизни без интернета, социальных сетей и мобильной связи, потоковое сознание и поверхностность при работе с информацией, новый уровень коммуникабельности, тяга к волонтерству и социальной активности. При этом из уст исследователя звучит предупреждение к подрастающему поколению о необходимости конкурирования с роботами и искусственным интеллектом в будущем.

В этой связи актуализируется анализ восприятие молодыми людьми своей собственной безопасности в процессе сетевой информационно-коммуникативной деятельности, так как именно рефлексивное отношение к сетевым рискам и угрозам является неотъемлемым шагом на пути их нейтрализации.

Методология и методы (Methodology and methods). Перед тем как обратиться к анализу восприятия молодыми людьми собственной безопасности в Сети, осуществим ревизию новейших рисков и угроз, связанных с технологизацией информационно-коммуникативной сферы, а также рассмотрим основные направления научного теоретизирования в указанной области.

Как было отмечено, проблематика информационно-коммуникативных рисков все чаще возникает в повестке обсуждений международных организаций. Так, в ноябре 2016 г. в ООН была принята Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», соавторами которой выступили 80 государств из всех регионов мира. В Резолюции приветствуется созыв новой Группы правительственных экспертов ООН по международной информационной безопасности, основной задачей которой «является выработка правил ответственного поведения государств в информационном пространстве» (Генассамблея

ООН приняла резолюцию по информационной безопасности, 2016). Генеральная Ассамблея ООН выступила с призывом о формировании глобальной культуры кибербезопасности и создании национальных программ повышения осведомленности и распространения знаний среди детей и индивидуальных пользователей (Резолюция, принятая Генеральной Ассамблеей ООН, 2009).

В последнем докладе Римского клуба также затрагиваются проблемы цифровизации современного мира, при этом авторы отмечают разрушительный характер данного процесса (Von Weizsäcker and Wijkman, 2018). Последнее обстоятельство связано с тем, что все чаще цифровые технологии используются для обхода правил и регулятивных механизмов, а в цифровом мире также возникают монополии и гангстерские конгломераты, при этом значительно возрастает потребление таких ресурсов как энергия, металлы, вода и др. «Нет сомнения, что все положительные вещи, связанные с ИКТ и цифровыми технологиями, при рассмотрении их прямых последствий с точки зрения устойчивости, вызывают отрицательные эффекты первого порядка» (Von Weizsäcker and Wijkman, 2018: 46).

В Доктрине информационной безопасности Российской Федерации (Доктрина информационной безопасности Российской Федерации, 2016) отмечается, что современные информационные технологии приобрели трансграничный характер. В этой связи защита национальных интересов в данной сфере предполагает, наряду с остальным, сохранение суверенитета РФ в информационном пространстве, обеспечение безопасности в области культуры, а также неприкосновенность частной жизни при использовании информационно-коммуникативных технологий. В Доктрине указывается, что возможности новейших информационно-коммуникативных технологий все чаще используются для информационно-психологического воздействия с целью дестабилизации внутриполитической и социальной ситуации в государствах. Вместе с тем «наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей» (Доктрина информационной безопасности Российской Федерации, 2016). При этом стратегическая стабильность в мире разрушается из-за стремления ряда стран использовать технологическое превосходство для доминирования в информационном пространстве.

Несмотря на то, что документы стратегического планирования РФ достаточно полно отображают риски и угрозы в информационной сфере необходимо обратить внимание на новые вызовы, которые еще не нашли своего отражения в качестве таковых ни в научном сообществе, ни в политико – правовых документах РФ.

1. ***Технологии Big Data Analysis*** – социально-экономический феномен, который связан с появлением новых технологических возможностей для анализа огромного количества данных (Что такое Big Data, 2017). Существует несколько определений того, что же такое Big Data (Большие данные), но в общем под ними понимают структурированные и неструктурированные данные огромных объёмов, которые оставляют пользователи о себе в Сети (Савельев, 2015). Вместе с тем, технологии Big Data Analysis на основе систем искусственного интеллекта позволяют осуществлять сегментацию пользователей в Сети, группировку по моделям поведения, что открывает новые возможности для маркетингового и социально-политического воздействия на пользователей через персонализированную рекламу. Так, выступая на Международном Конгрессе по кибербезопасности в Москве 6 июля 2018 года, глава Сбербанка России Герман Греф отметил, что кража цифровых следов и доступ к цифровому образу в Сети – это угроза для граждан, а Большие данные пользователей становятся важнейшим активом и объектом

противоборства. При этом применение систем искусственного интеллекта, моделей психоаналитики, построение графовых связей между данными, полученными из открытого Интернета делает доступной личную информацию кому угодно (Международный конгресс по кибербезопасности, 2018).

Примером такого использования в политике может служить предвыборная кампания Д. Трампа, которая, как выяснилось, осуществлялась на основе таргетированной рекламы пользователям социальных сетей, разработанной кампанией Cambridge Analytica. Последняя хранила и анализировала данные более чем о 51 млн. граждан, имеющих страницы в Facebook, в большинстве случаев – без их ведома и согласия. По признанию директора компании Александра Никса, на основе этих данных составлялись «психографические портреты» и оказывалось влияние на избирателей в ходе президентской кампании 2016 года в США (Rosenberg, 2018).

Отметим, что в Российской Федерации данная сфера информационно-коммуникативной отрасли еще не получила своего правового регулирования. Но уже вырисовывается два направления такой регуляции:

- государственная монополия на сбор больших пользовательских данных и торговлю ими, государство – хранитель цифрового образа страны;

- свободный сбор данных «data-брокерами» и их коммерческое использование. Именно такой вариант подготавливается Медиа-коммуникационным союзом в разработанном им «Инфокоммуникационном кодексе» (Нагорная, 2018).

2. Развитие технологий анализа Больших Данных обуславливает ***переход от «социального Web» (Web 2.0) к «когнитивному Web» (Web 3.0).*** Основная цель Web 3.0 – помочь пользователю сориентироваться в океане информации и найти нужный контент, т.е. предоставлять персонализированную информацию, что достигается благодаря когнитивным агентам, обладающим знаниями, способностью к самообучению, а также характеризующиеся человекоподобным поведением в Сети (Дрожжинов, Райков, 2017). Такого рода агентов еще называют «интеллектуальными агентами» т.к. они представляют собой программные продукты, действующие на основе интеллектуального анализа данных и искусственного интеллекта (Яковлев, 2018). Их функционирование также связано с угрозой сбора пользовательской информации, а также запрограммированным под определенные задачи человекоподобным поведением в Сети, например, распространение определенной информации, поддержание дискуссий и т.д. Все чаще в общественном дискурсе появляются понятия «бот» (сокращение от «робот»), «чат-бот», «ферма ботов», «детский сад ботов», «бот-сети» и т.д. Осязаемость рисков, связанных с деятельностью ботов подтверждает разработка закона в штате Калифорния, который будет обязывать ботов признаваться, что они боты. «Использование бота для общения или взаимодействия с другим лицом в Калифорнийском сегменте Интернета с намерением ввести другого человека в заблуждение относительно его искусственной идентичности с целью заведомо обмануть человека для стимулирования покупки или продажи товаров и услуг в коммерческой сделке или влияния на голосование на выборах должно быть незаконно. Лицо, использующее бота, не несет ответственности в соответствии с настоящим разделом, если лицо раскрывает, что это бот» – отмечается в законопроекте (Legislative counsel's digest, 2018).

3. Поступательное внедрение ***технологий дополненной реальности***, которые позволяют вносить цифровой контент в реальный мир в режиме реального времени также несет определенные риски в отсутствие должного регулирования со стороны государства. Примером такого рода технологий могут служить певцы-голограммы или «вокалоиды», которые набирают все большую популярность. Если в России и США используются голограммы реальных

певцов (В. Цоя, М. Джексона и др.), то в Азии колоссальную популярность завоевали именно «вокалоиды» – придуманные персонажи, с синтезированным голосом.

Так виртуальный статус не мешает собирать полные стадионы с миллионами поклонников китайской голограмме в стиле аниме Ло Тяньи. Вместе с тем, Коммунистическая партия Китая обязала разработчиков голограммы, компанию Shanghai Wangcheng, включить в репертуар «острые социальные вопросы и позитивные ценности, чтобы распространять их среди молодого поколения». Уже появились первые видео, на которых голограмма поёт гимн КНР «Марш добровольцев». В настоящее время компания Shanghai Wangcheng занимается производством виртуальных персонажей для китайских государственных органов и неправительственных организаций с целью донести необходимую им информацию до молодого поколения (Бовдунов, 2017).

Отметим, что подобное использование новейших технологий в Китае получает двоякие оценки мирового сообщества: с одной стороны, указывается на отсутствие свободы, информационный тоталитаризм, проводятся аналогии с Большом братом; с другой – отмечается цивилизационная субъектность Китая, которая позволяет ассимилировать любую новейшую социальную технологию или любое технологическое устройство без внесения изменений в основу своего культурного ядра.

Вместе с тем, следует признать, что технологии дополненной реальности обладают колоссальными возможностями по воздействию на механизмы нормативно-ценностной регуляции и формирования жизненных стратегий в молодежной среде, что требует более внимательного отношения к ним со стороны государства.

4. Новая философия подачи контента, возникшая на базе новейших медийных платформ – ***трансмедийное повествование*** – также может стать существенным фактором дестабилизации информационно-коммуникативного пространства. Суть последней заключается в том, что повествование (история) раскрывается через вербальную и невербальную коммуникации, с использованием разных медиасредств (видео, фото, изображения) и медиплатформ (телевидение, мобильное приложение, YouTube-канал, Vkontakte и др.). Американский теоретик медиа Г. Дженкинс концептуализирует трансмедийное повествование как «процесс, при котором отдельные части истории доставляются аудитории по различным каналам с целью создания единого целостного ее представления» (Jenkins, 2011). Главной особенностью является то, что истории не повторяются в разных формах повествования, а, наоборот, дополняют друг друга с целью конструирования цельного информационного пространства. Такой способ подачи информации позволяет добиться субъективности восприятия с помощью многомерности, гиперссылочности. При этом повествование осуществляется от лица нескольких героев, а не из одного источника или от одного журналиста, а у потребителя есть возможность воспринимать информацию по индивидуальной траектории. Кроме того, создается эффект присутствия путем переплетения повествования с помощью текста, аудио-, видеоинформации, а также новейших технологий. В результате трансмедийные истории обретают сегодня все большую популярность, благодаря возможности создания картины вымышленного мира, стирая при этом границу между реальным и виртуальным. Вместе с тем, подобная форма подачи контента открывает широкие возможности для манипулирования общественным мнением, распространения «фейк-ньюз», создания псевдознания.

Так, группа американских исследователей во главе с Джошуа Интроном проанализировала то, как люди объединяют онлайн информацию в псевдознание (Introne et al., 2018). Авторы обнаружили, что ложные повествования (нарративы) не просто передаются от человека к человеку в социальных сетях, а строятся из разрозненных

фрагментов информации, получаемой из нескольких источников, постепенно становясь частью правдоподобной реальности и псевдознанием.

В другом исследовании, предпринятом К. Старбирд, было установлено, что множество альтернативных новостных изданий действуют совместно, чтобы продвигать более широкую систему политических убеждений, которая сплетена из ложных повествований, вытекающих из текущих событий (Starbird, 2017). При этом различные сайты играют разные роли в обнародовании ложных повествований, причем некоторые из них используются в качестве доказательной базы, в то время как другие объединяют доказательства для создания более насыщенных историй.

Таким образом, подобный способ подачи контента, который стал возможен благодаря новейшим ИКТ, требует своего дальнейшего изучения с точки зрения его рискогенности и манипулятивного потенциала.

В целом, обобщая ревизию новейших рисков и угроз, связанных с технологизацией информационно-коммуникативной сферы необходимо обозначить основные направления научного теоретизирования в указанной области. Так научный подход к данной проблеме позволяет сформулировать различные ее уровни и направления. В первую очередь отметим, что сущность информационно-коммуникативных рисков и угроз, а также проблем информационной безопасности социальных субъектов сводится к «защите информации и защите от информации», что определяет развитие двух базовых направлений, связанных: 1) с разработкой технической базы для обеспечения устойчивости программного обеспечения информационных сетей и сохранения конфиденциальности, целостности информации (технологический подход); 2) с выявлением, оценкой последствий, нейтрализацией, а также защитой от негативной, неадекватной, манипулятивной информации (контентный подход) (см. напр., Владимирова, 2011; Наберушкина, Бердник, 2016). Научное рассмотрение проблемы информационной безопасности и анализа информационно-коммуникативных рисков и угроз в вертикальной плоскости позволяет выявить различные уровни ее проявления. Так, макроуровень затрагивает вопросы устойчивости, управляемости и воспроизводимости социальных систем в новых информационно-коммуникативных условиях, на мезоуровене актуализируются обозначенные вопросы в рамках различных социальных групп и организаций. При этом микроуровень отражает проблемы обеспечения информационной безопасности личности в пространстве сетевых коммуникаций, без решения которых невозможно дальнейшее стабильное существование системообразующих структур общества. Вместе с тем исследование вопросов информационной безопасности, нейтрализации информационно-коммуникативных рисков и угроз в различных сферах и отраслях общественной жизни (политической, экономической, социальной, духовно-культурной) отражает горизонтальную плоскость указанной проблемы.

Значительный интерес представляют научные наработки в сфере изучения информационно-коммуникативного среза бытия современной молодежи. При этом по мере осмысления воздействия сетевых коммуникаций на социализационные процессы и выбор жизненных стратегий исследователи все чаще обращаются к эмпирическому анализу рискогенности сетевых коммуникаций, а также к исследованию вопросов обеспечения информационной безопасности молодых людей (Бердник, 2018). На основании проведенных в этой области исследований можно выделить следующие группы рисков и угроз, с которыми сталкиваются молодые люди в процессе сетевых коммуникаций (см. напр. Морозова, 2016):

- технологические – вирусное ПО, утечка персональных данных, взломы аккаунтов и т.д.;
- экономические – несанкционированное снятие денежных средств, финансовое мошенничество, вирусный маркетинг;

- психофизиологические – расстройства памяти, сна, низкая физическая активность, интернет-зависимость и т.д.;
- когнитивные – рассредоточенность внимания, трудности с запоминанием, пониманием, прочтением текстовой информации;
- контентные – материалы явно содержащие незаконную, деструктивную информацию;
- манипулятивные воздействия – материалы, скрыто содержащие информацию для воздействия на мотивацию и поведение пользователей;
- негативная коммуникация – нежелательные контакты «кибербуллинг» или кибертравля, киберпреследования, «груминг» или сексуальные домогательства в Сети;
- самоизоляция – отказ от социальной жизни.

Наличие обозначенных рисков в процессе сетевых коммуникаций молодежи делает необходимым минимизацию их негативного воздействия, а также формирование практик их успешной нейтрализации. Решение данных вопросов, по нашему мнению, неразрывно связано с осознанием рискогенности сетевого пространства и учетом данного обстоятельства при осуществлении информационно-коммуникативной деятельности в Сети. Вместе с тем методологической базой исследования стали идеи о социальной конструируемости риска, обусловленности его восприятия ценностными, социокультурными установками социальных субъектов, которые детально разработаны в работах М. Дуглас, А. Вилдавски, К. Дейк и др. (Вилдавски, Дейк, 1994; Дуглас, 2000; Чупров, Зубок, Уильямс, 2003). При этом тезис о том, что риск социально конструируем, а значит, его оценка не свободна от ценностей, стал важным отличием социокультурного подхода в современной рискологии.

Указанные методологические основания позволили выдвинуть гипотезу о наличии дифференцированного восприятия собственной безопасности и сетевых рисков в молодежной среде, которое коррелирует с социально-демографическими характеристиками и ценностными установками молодых людей. Для прояснения обозначенных вопросов нами было предпринято эмпирическое исследование в январе – июле 2017 года на основе онлайн анкетирования. В качестве генеральной совокупности исследования были выбраны российские пользователи социальной сети «Вконтакте». Рекрутирование осуществлялось посредством рассылки личных сообщений и размещения постов в различных сообществах с предложением пройти по ссылке социологического исследования, размещенного в сети Интернет с помощью специализированной автоматической формы google. forms. Сформированная по результатам опроса выборка составила 300 человек и отразила основные социально-демографические характеристики молодых российских пользователей Сети от 14 до 29 лет. Целью предпринятого эмпирического исследования было выявление рефлексивной оценки молодыми людьми собственной безопасности в процессе сетевых коммуникаций, а также проверка гипотезы о дифференцированном восприятии информационно-коммуникативных рисков, в корреляции с социально-демографическими характеристиками и ценностными установками молодых людей.

Научные результаты и обсуждение (Research results and discussion).

В ходе исследования было установлено, что на вопрос «Насколько безопасно Вы ощущаете себя в Сети?» молодые респонденты отвечают весьма неоднозначно (рис. 1).

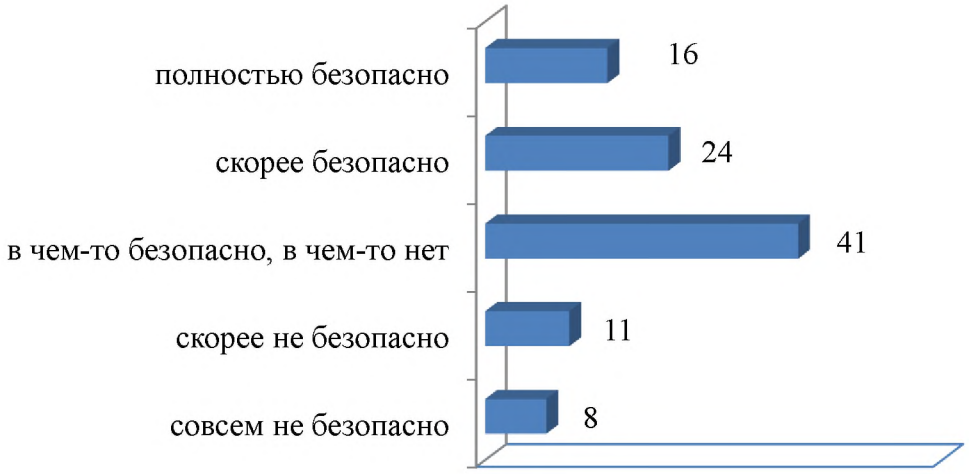

Рис. 1. Распределение ответов на вопрос
«Оцените, насколько безопасно Вы ощущаете себя в Сети?», %
Fig. 1. Distribution of answers to the question «Assess, how safe you feel online», %

Из полученных данных видно, что в целом 40% опрошенных ощущают себя безопасно в Сети, 41% – все же сомневается в своей безопасности и только 19% – чувствуют себя небезопасно в Сети. Подобное распределение отражает, по нашему мнению, тенденцию к игнорированию существующих рисков и угроз в процессе сетевых коммуникаций. Данный вывод подтверждает и распределение ответов на вопрос о частоте столкновения с нижеперечисленными рисками и угрозами (табл. 1).

Как видно из таблицы альтернатива «часто» и «иногда» были наименее выбираемыми. Свое столкновения с нижеперечисленными рисками и угрозами молодые люди описывают понятиями «редко» и «практически никогда». Вместе с тем полученные данные идут вразрез с результатами предпринятого нами анализа контента социальных медиа, где было установлено, что негативный контент встречается в более чем в половине, предложенной молодым людям информации (Бердник, 2018).

Таблица 1

Распределение ответов на вопрос: «Оцените, как часто Вы сталкиваетесь со следующими сетевыми рисками и угрозами?» (где 4 – часто, 3 – иногда, 2 – редко, 1 – практически никогда)

Table 1

Distribution of answers to the question «Assess, how often you face the following network risks and threats?» (4 – often, 3 – sometimes, 2 – rarely, 1 – almost never)

Ранг	Информационно-коммуникативные риски	Средние значения
1	Негативный контент	2
2	Технологические	1,9
3	Манипулятивное воздействие	1,7
4	Психофизиологические	1,7
5	Когнитивные	1,6
6	Негативная коммуникация	1,3
7	Самоизоляция	1,2
8	Экономические	1

Таким образом, можно сделать вывод о том, что молодые люди склонны не замечать или игнорировать информационно-коммуникативные риски сетевых коммуникаций, в целом ощущая себя безопасно в Сети.

Вместе с тем, в контексте нашего исследования значительный интерес представляли социально-демографические характеристики и ценностные установки молодых людей, которые имеют различное восприятие информационно-коммуникативных рисков и угроз. Для изучения данного аспекта, на основании вопроса «Оцените, насколько безопасно Вы ощущаете себя в Сети» нами были выделены две группы респондентов: «осторожные» – ребята которые чувствуют себя небезопасно в Сети (19% ответивших на вопрос); «смелые» молодые люди, которые чувствуют себя в безопасности в процессе сетевых коммуникаций (40% ответивших на вопрос). Отметим, что интерес представляли именно полюсные группы респондентов, так как их сравнение дает более четкую картину различий. Анализ изучаемых характеристик в выделенных группах позволил выявить статистически значимые различия в социально-демографических показателях и ценностных установках респондентов[1].

Охарактеризуем социально-демографические показатели в выделенных группах. Как видно из таблицы 2 «смелые» ребята моложе (в среднем им 17 лет), соответственно у них ниже уровень образования (среднее общее/среднее профессиональное), но выше материальное положение. В то же время «осторожные» молодые люди старше (около 21 года), они, либо окончили средние профессиональные учебные заведения, либо являются студентами высших учебных заведений, при этом отмечают, что денег в основном хватает только на самое необходимое. Вместе с тем по признаку «Пол» не было обнаружено статистически значимых различий, т.е. восприятие своей безопасности в Сети не зависит от пола респондентов.

Таблица 2

Социально-демографические характеристики в выделенных группах:
возраст (метрическая переменная); уровень образования (где 1 – неоконченное среднее, 2 – среднее общее, 3 – среднее профессиональное; 4 – высшее бакалавриат/неоконченное, 5 – магистратура\специалитет, 6 – аспирантура, ученая степень); материальное положение (1 – денег не хватает на самое необходимое, 2 – все деньги расходуются на покупку вещей первой необходимости, 3 – хватает на все, кроме товаров длительного пользования, 4 – живем обеспеченно, но не можем осуществить крупные покупки, 5 – можем позволить практически все)

Table 2

Socio-demographic characteristics in the selected groups:
age (metric variable); education level (1 – incomplete secondary, 2 – secondary, 3 – vocational; 4 – bachelor's degree /incomplete, 5 – master's degree/ specialist, 6 – postgraduate, PhD); financial situation (1 – money is not enough for bare essentials, 2 – all the money is spent on bare essentials, 3 – enough for all, except durable goods, 4 – live securely, but cannot make large purchases, 5 – can afford almost everything)

Социально-демографические характеристики	Средние значения		Статистическая значимость различий (95% доверительный интервал) *Sig*
	«осторожные»	«смелые»	
Возраст	21	17	0,004
Уровень образования	3,7	2,5	0,003
Материальное положение	2,8	3,2	0,004

[1]Статистическая значимость различий устанавливалась с помощью Т-тестов для независимых выборок в программе SPSS.

Анализ ответов на вопрос «С какого возраста Вы начали пользоваться виртуальными социальными сетями» в выделенных группах показал, что «осторожные» ребята начинают пользоваться социальными сетями преимущественно в 14 лет, в то время как средний возраст начала сетевой деятельности «смелых» ребят составляет 12 лет.

Отвечая на вопрос, с какими рисками молодые люди сталкиваются чаще всего, «осторожные» отмечают, что чаще сталкиваются с технологическими рисками, в отличие от «смелых» (табл. 3). Можно предположить, что рискогенность сетевого пространства, ребятами, которые ощущают себя небезопасно в Сети, в целом связывается с технологическими угрозами (вирусным ПО, утечкой персональных данных, взломы аккаунтов и др.). При этом контентные риски не актуализируются ни «осторожными», ни «смелыми» респондентами.

Таблица 3

Распределение в выделенных группах ответов на вопрос «Как часто Вы сталкиваетесь со следующими сетевыми рисками и угрозами?» (где 4 – часто, 3 – иногда, 2 – редко, 1 – практически никогда, 0 – трудно сказать)

Table 3

Distribution of answers in the selected groups to the question «Assess, how often you face the following network risks and threats? » (4 – often, 3 – sometimes, 2 – rarely, 1 – almost never)

Риски	Средние значения		Статистическая значимость различий (95% доверительный интервал) *Sig*
	«осторожные»	«смелые»	
Технологические	2,5	1,7	0,003
Психофизиологические	1,6	1,6	0,982
Экономические	1,2	1,3	0,599
Когнитивные	1,5	1,6	0,280
Негативный контент	2	2,1	0,082
Манипулятивное воздействие	1,7	1,8	0,257
Нежелательные контакты	1,3	1,2	0,480
Самоизоляция	1	1,2	0,121

Анализ ценностных установок в выделенных группах (табл. 4), несмотря на схожесть ценностных ориентаций, показал дифференцированное отношения к материальному благополучию – для «смелых» ребят оно оказалось самым ценным, более значимым для них оказалось и участие в общественной жизни, в решении общественных проблем.

Таблица 4

Распределение в выделенных группах ответов на вопрос «Насколько ценно лично для Вас …?» (где, 3 – ценно, 2 – отчасти ценно, отчасти нет, 1 – совсем не ценно, 0 – трудно сказать)

Table 4

Distribution of answers in the selected groups to the question «How valuable is to you ……» (3 – valuable, 2 – partly valuable, partly not, 1 – not valuable, 0 – hard to say)

Ценности	Средние значения		Статистическая значимость различий (95% доверительный интервал) *Sig*
	«осторожные»	«смелые»	
1. Интересная творческая работа	2,5	2,6	0,982
2. Материальное благополучие	2,5	3	0,003
3. Хорошие отношения с окружающими людьми	2,6	2,7	0,599
4. Возможность приносить пользу людям	2,4	2,2	0,280
5. Участие в общественной жизни, в решении общественных проблем	2	2,6	0,005
6. Образованность, знание	2,7	2,6	0,257
7. Личное спокойствие, отсутствие неприятностей	2,5	2,7	0,480
8. Семейное благополучие	2,6	2,7	0,121
9. Здоровье	2,6	2,6	0,468
10. Полноценный отдых, интересные развлечения	2,6	2,6	0,438
11. Высокое служебное и общественное положение	2,3	2,3	0,846
12. Приобщение к литературе и искусству	2,2	2,3	0, 321
13. Экологическая безопасность	2,3	2,2	0,798
14. Взаимопонимание с родителями, старшим поколением	2,6	2,5	0,035
15. Личная свобода независимость в суждениях и действиях	2,5	2,4	0,176
16. Возможность развития, реализации своих талантов	2,4	2,5	0,736
17. Экономическая независимость	2,5	2,4	0,067
18. Бытовой комфорт	2,4	2,4	0,198
19.Свободный доступ к Интернет	2,4	2,3	0,054

Резюмируя проведенное эмпирическое исследование можно сделать вывод о том, что большая часть молодых людей склонна не фиксировать или игнорировать риски и угрозы в процессе сетевых коммуникаций, отмечая, что сталкиваются с последними редко или практически никогда. Вместе с тем, подтверждена гипотеза о дифференцированном восприятии молодыми людьми своей безопасности в Сети, которое коррелирует с их социально-демографическими показателями и ценностными установками. «Смелые» молодые люди в целом моложе (менее 18 лет), они

раньше начинают пользоваться виртуальными социальными сетями, при этом материальное благополучие и участие в решении социальных проблем являются приоритетными для них. В то же время «осторожные» молодые люди старше (им более 20 лет), образованность и знание для них стоят на первом месте. Примечательно то, что основную угрозу своей безопасности в Сети они связывают с технологическими рисками (вирусным ПО, хищением персональных данных, взломами аккаунтов и др.). При этом контентные риски не актуализированы ни в одной из выделенных групп.

Заключение (Conclusions). Таким образом, налицо недостаточная информированность российской молодежи о современных вызовах и угрозах в информационно-коммуникативной сфере. Данное обстоятельство требует выработки совместных подходов всех заинтересованных сторон – государственных структур, родительских ассоциаций, образовательных организаций представителей гражданского общества, НКО, поставщиков Интернет-услуг, администраторов популярных онлайн-сервисов. Их взаимодействие позволит создать единую нормативно-правовую базу по защите и регулированию информационно-коммуникативной деятельности молодых людей в сети Интернет, разработать просветительскую федеральную программу, которая решит задачи повышения осведомленности и получения навыков по обеспечению информационной безопасности с учетом новейших вызовов и угроз в этой сфере, инициировать всероссийские научные исследования по анализу стратегий родительского контроля, изучению онлайн-активности подрастающего поколения, оценке ими собственной безопасности в Сети, сформировать систему рейтингования безопасных ресурсов в виртуальном пространстве, поставщиков Интернет-услуг, а также программных средств обеспечения безопасности в Сети.

Список литературы

Бердник Е. А. Контентные риски в поле сетевой культуры молодежи (на примере анализа сообществ «Вконтакте») // Человек. Общество. Инклюзия. МГГЭУ, 2018. № 1 (33). С. 12-30.

Бовдунов А. Цифровой дракон: как Китай строит общество тотального контроля с помощью интернет-технологий // RT на русском. 31.12.2017 г. URL: https://russian.rt.com/world/article/466304-kitai-kontrol-internet-tehnologii (дата обращения: 15.08.2018).

Бостром Н. Искусственный интеллект. Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. М.: Манн, Иванов и Фербер, 2016. 496 с.

Вилдавски А., Дейк К. Теории восприятия риска: кто боится, чего и почему? // Thesis: теория и история экономических и социальных институтов и систем. 1994. № 5. С. 268-276.

Владимирова Т. В. Сетевые коммуникации как источник информационных угроз // Федеральный образовательный портал «Экономика. Социология. Менеджмент». 2011 г. URL: http://ecsocman.hse.ru/data/2011/09/20/1267451215/Vladimirova.pdf (дата обращения: 10.09.2018).

Генассамблея ООН приняла резолюцию по информационной безопасности // Информационное агентство ТАСС. 02.11.2016 г. URL: https://tass.ru/politika/3754890_(дата обращения: 11.09.2018).

Доктрина информационной безопасности Российской Федерации от 05.12.2016 г. URL: https:// rg.ru/ 2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 06.09.2018).

Дрожжинов В. И., Райков А. Н. Веб-технологии, искусственный интеллект и когнитивное правительство // Современные информационные технологии и ИТ-образование. 2017. Т. 13. № 2. С. 153-169. URL: https://cyberleninka.ru/article/v/veb-tehnologii-iskusstvennyy-intellekt-i-kognitivnoe-pravitelstvo (дата обращения: 14.09.2018).

Дуглас М. Чистота и опасность: анализ представлений об осквернении и табу. М.: Канон-Пресс-Ц: Кучково поле, 2000.

Международный конгресс по кибербезопасности / Выступление Г. Грефа на пленарной сессии, 06.07.2018 г. URL: https://icc.moscow/translyatsii.html (дата обращения: 12.09.2018).

Международный социологический марафон «Исследователь 2.0: трансформация профессии в цифровую эпоху» / Выступление Л. Паутовой, 12.12.2017 г. URL: https://www.youtube.com/watch?v=v7aWcvUFeBQ (дата обращения: 11.09.2018).

Морозова А. А. Основные виды рисков медиапотребления в социальных сетях: на примере «Вконтакте» // Журналистика цифровой эпохи: как меняется профессия: материалы междунар. науч.-практ. конф.: к 80-летию журналист. образования на Урале и 75-летию фак. журналистики Урал. ун-та, Екатеринбург, 14-15 апр. 2016 г.; М-во образования и науки РФ, Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина. Екатеринбург, 2016. С. 117-120.

Наберушкина Э. К., Бердник Е. А. Социокультурные аспекты информационной безопасности в сетевом обществе // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. Белгород, 2016. № 17 (237). С. 90-99.

Нагорная М. Бизнес-сообщество обсуждает идею создания Инфокоммуникационного кодекса // Адвокатская газета. 17.01.2018 г. URL: https://www.advgazeta.ru/novosti/biznes-soobshchestvo-obsuzhdaet-ideyu-sozdaniya-infokommunikatsionnogo-kodeksa/_(дата обращения: 10.09.2018).

Резолюция, принятая Генеральной Ассамблеей 21.12.2009 г. URL: https://undocs.org/ru/A/RES/64/211_(дата обращения: 02.09.2018).

Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43-66.

Что такое Big data: собрали всё самое важное о больших данных // Образовательные материалы Rusbase. 16.05.2017 г. URL: https://rb.ru/howto/chto-takoe-big-data/ (дата обращения: 04.09.2018).

Чупров В. И., Зубок Ю. А., Уильямс К. Молодежь в обществе риска; Рос. акад. наук, Ин-т соц.-полит. исслед., М-во образования РФ, Департамент по молодеж. политике. 2-е изд. М.: Наука, 2003. 230 с.

Яковлев К. Интеллектуальные агенты // Постнаука. 10.09.2018 г. URL: https://postnauka.ru/video/88720 (дата обращения: 15.09.2018).

Introne J., Yildirim, I. G., Iandoli, L., Decook, J., Elzeini, S. How people weave online information into pseudoknowledge // Social Media+Society. 2018. № 4 (3). URL: http://journals.sagepub.com/doi/full/10.1177/2056305118785639 (дата обращения: 15.09.2018).

Jenkins H. Transmedia 202: Further Reflections // Confessions of an Aca-Fan. Los Angeles, 2011. URL: http://henryjenkins.org/blog/2011/08/defining_transmedia_further_re.html (дата обращения: 15.01.2018).

Legislative counsel's digest: SB 1001, Hertzberg. Bots: disclosure. 05. 02.2018 г. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001 (дата обращения: 15.09.2018).

Leonhard, G. Technology vs. Humanity: The Coming Clash Between Man and Machine (Futurescapes). USA: Fast Future Pablishing ltd., 2016.

Rosenberg, M. Cambridge Analytica Suspends C.E.O. Amid Facebook Data Scandal // The New York times. 20 March 2018. URL: https://www.nytimes.com/2018/03/20/world/europe/cambridge-analytica-ceo-suspended.html?action=click&module=Top%2520Stories&pgtype=Homepage (дата обращения: 12.09.2018).

Starbird K. Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on Twitter // Proceedings of the International AAAI Conference on Web and Social Media. 2017. URL: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15603 (дата обращения: 15.09.2018).

Von Weizsäcker E. U., Wijkman A. Come On! Capitalism, Short-termism, Population, and the Destruction of the Planet. New York: Springer, 2018.

References

Berdnik, E. A. (2018), "Content risks in the field of youth network culture (on the example of "Vkontakte" communities analysis»)", *Human. Society. Inclusion*, 1 (33), 12-30. *(In Russian).*

Bovdunov, A. (2017), *Digital dragon: how China is building a total control society with the help of Internet technologies* [Online], available at: https://russian.rt.com/world/article/466304-kitai-kontrol-internet-tehnologii_(Accessed 15 September 2018). *(In Russian).*

Bostrom, N. (2016), *Iskusstvenny intellect. Etapy. Ugrozy. Strategii* [Superintelligence: Paths,

Dangers, Strategies], Translated by Filin S., Moscow, Russia. *(In Russian).*

Wildavsky, A. and Dake, K. (1994), "Theories of risk perception: who fears what and why?", *Thesis*, 5, 268-276. *(In Russian).*

Vladimirova, T. V. (2011), *Setevye kommunikatsii kak istochnik informatsionnyh ugroz* [Network communications as a source of information threats], The Federal educational portal "Economics. Sociology. Management" [Online], available at: http://ecsocman.hse.ru/data/2011/09/20/1267451215/Vladimirova.pdf (Accessed 10 September 2018). *(In Russian).*

The UN General Assembly adopted a resolution on information security (2016), [Online], available at: https://tass.ru/politika/3754890 (Accessed 11 September 2018). *(In Russian).*

The Russian Federation information security doctrine (2016), [Online], available at: https://rg.ru/ 2016/12/06/doktrina-infobezobasnost-site-dok.html (Accessed 6 September 2018). *(In Russian).*

Drozhzhinov, V. I. and Raikov, A. N. (2017), "Web technologies, artificial intelligence and cognitive government", *Modern information technologies and IT education,* 13 (2), 153-169. *(In Russian).*

Douglas, M. (2000), *Chistota i opasnost`: analiz predstavleniy ob oskvernenii i tabu* [Purity and Danger. An Analysis of the Concepts of Defilement and Taboo], Kanon-Press-Cz: Kuchkovo pole, Moscow, Russia. *(In Russian).*

International Congress on cybersecurity (2018), [Online], available at: https://icc.moscow/translyatsii.html (Accessed 12 September 2018). *(In Russian).*

International sociological marathon "Researcher 2.0: transformation of the profession in the digital age" (2017), [Online], available at: https://www.youtube.com/watch?v=v7aW-cvUFeBQ (Accessed 11 September 2018). *(In Russian).*

Morozova, A. A. (2016), "The main types of risks of media consumption in social networks on the example of "Vkontakte»", *Zhurnalistika cifrovoj ehpohi: kak menyaetsya professiya: materialy mezhdunar. nauch.-prakt. konf.: k 80-letiyu zhurnalist. obrazovaniya na Urale i 75-letiyu fak. zhurnalistiki Ural. un-ta,* Ekaterinburg, Russia, 117-120. *(In Russian).*

Naberushkina, E. K. and Berdnik, E. A. (2016), "Socio-cultural aspects of information security in a network society", *Belgorod State University Scientific Bulletin: Philosophy. Sociology. Law*, 17 (237), 90-99. *(In Russian).*

Nagornaya, M. (2018), "The business community discussing the idea of creating an Info-communication code" [Online], available at: https://www.advgazeta.ru/novosti/biznes-soobshchestvo-obsuzhdaet-ideyu-sozdaniya-infokommunikatsionnogo-kodeksa/ (Accessed 10 September 2018).

UN General Assembly Resolution (2009), [Online], available at: https://undocs.org/ru/A/RES/64/211_(Accessed 02 September 2018). *(In Russian).*

Savel'ev, A. I. (2015), "Personal data legislation application problems in the era of "Big data", *Law. Journal of the Higher School of Economics*, 1, 43-66. *(In Russian).*

What is Big data: we have collected the most important things about big data (2017), [Online], available at: https://rb.ru/howto/chto-takoe-big-data (Accessed 04 September 2018). *(In Russian).*

Chuprov, V. I., Zubok, Y. A. and Uil'yams, K. (2003), *Molodezh' v obshchestve riska* [Youth at risk society], Nauka, Moscow, Russia. *(In Russian).*

Yakovlev, K. (2018), *Intelligent agents* [Online], available at: https://postnauka.ru/video/88720_(Accessed 15 September 2018). *(In Russian).*

Introne, J., Yildirim, I. G., Iandoli, L., Decook, J., & Elzeini, S. (2018), "How people weave online information into pseudoknowledge", *Social Media+Society,* 4 (3), [Online], available at: http://journals.sagepub.com/doi/full/10.1177/2056305118785639 (Accessed 15 September 2018). *(In Russian).*

Jenkins, H. (2011), "Transmedia 202: Further Reflections", *Confessions of an Aca-Fan*, Los Angeles, USA. [Online], available at: http://henryjenkins.org/blog/2011-/08/defining_transmedia_further_re.html (Accessed 15 September 2018)

Legislative counsel's digest: SB 1001, Hertzberg. Bots: disclosure, (2018). [Online], available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001 (Accessed 15 September 2018).

Leonhard, G. (2016), *Technology vs. Humanity: The Coming Clash Between Man and Machine (Futurescapes)*, Fast Future Pablishing ltd., USA.

Rosenberg, M. (2018), "Cambridge Analytica Suspends C.E.O. Amid Facebook Data Scandal", *The New York times*, [Online], available at: https://www.nytimes.com/2018/03/20/world/europe/cambridge-analytica-ceo-suspended.html?action=click&module=Top%2520Stories&pgtype=Homepage (Accessed 12 September 2018).

Starbird, K. (2017), "Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on Twitter", in *Proceedings of the International AAAI Conference on Web and Social Media*, [Online], available at: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15603 (Accessed 12 September 2018).

Von Weizsäcker, E. U. and Wijkman, A. (2018), *Come On! Capitalism, Short-termism, Population, and the Destruction of the Planet*, Springer, New York, USA.

Конфликты интересов: у авторов нет конфликта интересов для декларации.

Conflicts of Interest: The authors have no conflict of interest to declare.

Бердник Екатерина Александровна, старший преподаватель кафедры международных отношений, зарубежного регионоведения и политологии Белгородского государственного национального исследовательского университета.

Ekaterina A. Berdnik, Senior Lecturer of the Department of International Relations, Foreign Regional Studies and Political Science, Belgorod State National Research University.