Современная Европа, 2022, № 6, с. 112–125

УДК 39.019.5

ЦИФРОВЫЕ СМИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОПЫТ ЕВРОСОЮЗА

© 2022 НУГМАНОВА Карлыгаш Жандильдиновна*
Доктор политических наук, профессор
Президент международного центра геополитического прогнозирования «Восток-Запад». Казахстан, Алматы, ул. Е 607, 4
E-mail: *politassoc@mail.ru.*

© 2022 КАГАЗБАЕВА Эльмира Маратовна*
Кандидат политических наук, доцент
Казахский университет международных отношений и мировых языков имени Абылай хана. Казахстан, Алматы, ул. Муратбаева, 200
E-mail: *Kagazbaeva.e@gmail.com*

Поступила в редакцию 10.06.2022
После доработки 27.08.2022
Принята к публикации 09.09.2022

Аннотация. В ближайшей перспективе цифровые средства массовой информации станут основным первоисточником информации для населения любого государства, следовательно роль цифровых медиа в процессе обеспечения информационной безопасности будет значительной. Цифровые СМИ в Европейском союзе являются важным политическим инструментом. Угрозу информационной безопасности ЕС представляют транснациональные сетевые новые медиа. Цель исследования – рассмотреть опыт Евросоюза в регулировании цифровых средств массовой информации в аспекте информационной безопасности. В статье проанализирована политика ЕС по борьбе с фейками и дезинформацией, показаны основные тенденции в сфере развития новых медиа, на основе концепции общества сетевых структур М. Кастельса. Анализ развития цифровых СМИ и политики ЕС в области обеспечения информационной безопасности позволяют сделать вывод, что дилемма, безопасность или свобода, решается в пользу безопасности, возрастает роль институтов ЕС в регулировании интернет-пространства, цифро-

вых СМИ, цифровой конфиденциальности, защиты фундаментальных прав человека и создании единого европейского цифрового пространства.

Ключевые слова: цифровая политика, цифровые СМИ, социальные сети, информационная безопасность, коммуникация, информационный суверенитет, дезинформация, гражданское общество.

DOI: 10.31857/S0201708322060080

EDN: gqfhyx

Актуальность статьи обусловлена, во-первых, необходимостью научного анализа роли цифровых средств массовой информации в обеспечении информационной безопасности, во-вторых, деятельностью современных СМИ, которая зачастую обусловлена интересами государства или собственниками крупных медиахолдингов, что ставит под сомнение достоверность и качество представленной информации. В-третьих, цифровые медиа вызывают широкий интерес, особенно у молодежи. Быстрый доступ к информации, способность устанавливать быстрые контакты между людьми и развивать отношения и бизнес привлекают большинство пользователей в качестве дополнительных преимуществ. Однако злоумышленники также пользуются преимуществами социальных сетей и их действия представляют существенную угрозу национальной безопасности. Цель исследования – рассмотреть опыт Евросоюза по регулированию цифровых средств массовой информации в аспекте информационной безопасности.

Медийное пространство представляет собой сферу распространения массовой информации, которая передается субъектами, наделенными обществом полномочиями и правами передачи информации. Сегодня оно является многофункциональным политическим и социальным институтом, обладающим институциональным статусом в сфере политики с большим политическим и социальным потенциалом.

Американский исследователь Р. Нойман в 1991 г. ввел в научный оборот понятие «новые медиа» (*new media*) как «новый формат средств массовой информации, которые доступны на цифровых устройствах и подразумевают активное участие пользователей в создании и распространении контента» [Neuman, 1991: 51].

Развитие цифровых СМИ привело к глобальным трансформациям информационного общества, изменению статуса аудитории: человек, потребляющий информацию, одновременно становится и потребителем, и производителем информации. Американский ученый Э. Тоффлер в работе «Третья волна» впервые использует понятие «просьюмер» (*prosumer*), означающее производителя и потребителя в одном лице [Тоффлер, 1999: 76]. Оно отражает направление развития деятельности цифровых СМИ. Просьюмеры занимаются распространением информационных материалов цифровых СМИ, выполняют социально-креативную функцию, выступают в роли медиакритиков информационного контента, а также могут давать индивидуальную оценку ресурсу [Кастельс, 2016].

По мнению казахстанских исследователей Э.М. Кагазбаевой и Б. Алмырза, просьюмеры играют важную роль в создании и содержательном наполнении цифровых СМИ. В частности, эта тенденция прослеживается в таких развитых странах, как Соединенные Штаты, Канада и Британия. Например, в создании контента информационно-новостных интернет-ресурсов *Digg.com, Tremr.com, Articlebiz.com* участвуют зарегистрированные пользователи. Таким образом, просьюмеры являются эффективным инструментом для цифровых медиа и одновременно выступают создателями, рецензентами и потребителями контента. Благодаря просьюмерам аудитория цифровых СМИ, в отличие от традиционных, расширяется очень быстро. Они также имеют возможность влиять на формирование общественного мнения. В этом кроется большая опасность, поскольку цифровые медиа теряют контроль над управлением аудиторией, и любая информация может привести к непредсказуемым последствиям [Кагазбаева, Алмырза, 2021: 11].

Основными политическими акторами на современном этапе являются социальные сети, которые встроены в процесс общественного порядка. Сетевое сообщество – это интерактивная среда, в которой происходит обмен информацией между пользователями социальных сетей и блогосферы, влияющая на формирование общественного мнения. В ней формируются новые группы и контргруппы политических сетевых сообществ, которые способствуют принятию политических решений. На этих платформах организуется политический диалог и обсуждение [Мирошниченко, 2013: 207].

Широкое распространение Интернета привело к тому, что потребители информации получили возможность не только использовать механизмы для производства новостей, но и платформу для их распространения [Балуев, 2013: 610]. На технологическую сторону социальных медиа обращает внимание американский исследователь Б. Солис. Наиболее распространенная форма социальных сетей – это способ, которым пользователи открывают, читают и комментируют новости, информацию и контент. Это сплав социальных элементов и передовых технологий, которые превращают монологи в диалоги [Solis, Breakenridge, 2009: 19]. Испанский социолог М. Кастельс определил взаимодействие в социальных медиа как новую форму массовой самокоммуникации [Кастельс, 2016: 74]. Сети коммуникации обладают следующими чертами: открытостью, централизованностью, саморазвитием, автономностью [Castells, 2001: 13].

Взаимосвязь политического процесса и развития новых медиа проанализирована в статье И. Скрипка «Электронные СМИ и социальные сети в политике: европейский опыт», в которой автор сделал вывод, что цифровые СМИ меняют поведение как политиков, так и избирателей: «Фактически полноценное участие кандидата или партии в политическом процессе невозможно, если они не представлены в интернете» [Скрипка, 2021: 8].

Развитие цифровых СМИ в Евросоюзе

Для европейских граждан СМИ являются основным источником получения информации по вопросам интеграционной тематики, инструментом по налаживанию

гражданского взаимодействия, источником утверждения европейской идентичности. В Евросоюзе создан новый тип средств массовой коммуникации – компания *Euronews*, которая ведет трансляцию на нескольких языках и создает единую повестку для интеграционного образования. *Euronews* в 2016 г. открыл новый канал *Africanews*, который доступен на английском и французском языках на территории 33 стран Африки. В *Euronews* входят 6 радиостанций и 14 национальных сайтов. Канал доступен на 5 континентах. Он активно проводит политику продвижения в социальных сетях, на интернет-платформах. Особенность *Euronews* заключается в проводимой политике мультикультурализма и расширении медийного плюрализма при сохранении главной цели – построения единой Европы.

В период с 2010 по 2018 гг. Интернет переместился с 4 позиции на 2, опережая радио и печатную прессу. Самой популярной социальной сетью в Европе является *Facebook*[1]. По данным американских исследователей, к цифровым СМИ относятся официальные и институциональные веб-сайты ЕС, информационные веб-сайты, сайты социальных сетей, различные блоги и веб-сайты видеохостингов [Mourao et al., 2015: 3].

Социальные медиа, к которым можно отнести блоги, социальные сети, новостные сайты, являются новым видом коммуникации и обладают управленческим потенциалом. Они являются инструментом политического влияния, благодаря техническому развитию их аудитория с каждым разом растет. Особую ценность социальные медиа представляют для политического пиара. Наибольшую популярность в европейском истеблишменте получила социальная сеть *Twitter*. Европейские политические лидеры, используя её технологические возможности, формулируют свой политический курс, осуществляют электронную форму публичной коммуникации и влияют на политическое поведение электората. Пространство социальных медиа становится полем информационной борьбы политических деятелей за внимание и доверие избирателей.

В декабре 2020 г. Европейская комиссия приняла План действий в области средств массовой информации (2021–2027 гг.), целью которого является поддержка перехода традиционных СМИ на онлайн-платформы. В ЕС существует высокий спрос на новостной контент в Интернете. Так, более 70% европейцев один раз в неделю используют Интернет для доступа к новостям, 45% получают доступ к ним каждый день [KEA, 2021: 21]. Для поддержания европейских цифровых СМИ в 2018 г. был принят Закон о цифровых рынках, согласно которому были введены жесткие правила защиты онлайн-данных пользователей. Европейцская цифровая политика направлена на то, чтобы помешать крупным технологическим платформам (*Meta*[2]*, Microsoft, Amazon* и другие) использовать сервисы и ресурсы для борь-

[1] С 4 марта 2022 г. социальная сеть *Facebook* заблокирована Роскомнадзором на территории РФ.

[2] 21 марта 2022 г. Тверской районный суд г. Москвы признал *Meta Platforms Inc*. экстремистской организацией и запретил деятельность компании на территории РФ.

бы с конкурентами и привлечения пользователей. В случае нарушения закона предусмотрен штраф в размере до 20% от дохода компании[1].

Политика ЕС в области обеспечения информационной безопасности, борьба с фейками и дезинформацией

Рассмотрим основные теоретические подходы к понятию «национальная безопасность». Российский исследователь А.И. Поздняков ввел в научный оборот аксиологический подход, в котором национальная безопасность определяется как защищенность национальных ценностей, национального достояния от значимого ущерба [Поздняков, 2013: 47]. Похожая позиция прослеживается у ряда западных исследователей. Например, У. Липпман писал: «Государство находится в состоянии безопасности, когда ему не приходится приносить в жертву свои законные интересы с целью избежать войны и когда оно в состоянии при необходимости защитить эти интересы путем войны» [Lippman, 1943: 5]. Аналогичных взглядов придерживается А. Уолферс, который в 1962 г. отмечал, что безопасность в объективном смысле определяется отсутствием угроз приобретенным ценностям, в субъективном смысле – отсутствием боязни, что эти ценности могут подвергнуться нападению [Wolfers, 1962: 150].

Ряд исследователей исходят из системно-философского подхода к определению национальной безопасности, который акцентирует внимание на сохранении целостности, устойчивости, стабильности страны, государства, общества как социальной системы при деструктивных воздействиях на нее.

Другие ученые, например О.А. Бельков, определяют национальную безопасность как состояние, тенденции развития и условия жизнедеятельности нации, гарантирующие ее выживание, свободное, независимое функционирование при сохранении фундаментальных институтов и ценностей [Бельков, 2004: 92].

Таким образом, национальная безопасность – это совокупность всех усилий, предпринимаемых для защиты суверенитета и заветных ценностей нации. Она повышает уровень жизни людей, а также обеспечивает свободу граждан от всех форм угрозы жизни и имуществу.

В условиях информационной эпохи одним из важных звеньев обеспечения национальной безопасности является информационная безопасность. Во многих развитых странах обеспечением последней занимаются силовые структуры, в том числе министерства обороны. Обеспечение национальной безопасности в информационной сфере связано с обеспечением информационно-психологической безопасности. В теории информационно-психологической войны одним из объектов выступают духовные ценности, а пропаганда образов массовой культуры является средством поражения объекта. Каналами доставки деструктивной информации могут выступать массмедиа. В обозримом будущем цифровые СМИ станут основны-

[1] Satariano A. E.U. Takes Aim at Big Tech's Power With Landmark Digital Act. The New York Times. 24.03.2022. URL: https://www.nytimes.com/2022/03/24/technology/eu-regulation-apple-meta-google.html (дата обращения: 13.07.2022)

ми первоисточниками информации для населения любого государства, следовательно роль цифровых массмедиа в процессе обеспечения национальной безопасности будет значительной.

Понятие «информационная безопасность» рассматривается на следующих уровнях: технологическом, общественно-информационном и политическом. С технологической точки зрения информационная безопасность представляет собой предотвращение угроз разрыва передачи данных и подмены информации или сообщений, борьбу с угрозами хакерских атак, хищениями. На данном уровне между экспертным сообществом и национальными управлениями специальных служб по противодействию преступлениям в киберпространстве обеспечено взаимопонимание и сотрудничество. Сложность представляют следующие два уровня. В частности, общественно-информационный уровень рассматривает вопросы распространения контента, т.е. информации в сети. Безопасность на данном уровне подразумевает смысловую безопасность, связанную с наличием альтернативных точек зрения в информационном пространстве. В зависимости от идеологических ценностей государства инакомыслие воспринимается как состояние небезопасности. Политический уровень является продолжением общественно-социального с добавлением оценки возможностей иностранного влияния на национальные политические процессы [Леви, 2018: 377].

Ряд государств, например Финляндия, Словакия, Чехия, в своих документах не отражают политические и внешнеполитические риски угроз кибербезопасности, а воспринимают ее с точки зрения технологических угроз. Стратегия информационной безопасности Германии является наиболее проработанной. В ней акцент сделан на развитие двух направлений – уголовные преступления в цифровом мире и обеспечение безопасности базовых функциональных сервисов [Гасанова, 2016: 246].

В книге Й. Фаркаса «Постправда, фальшивые новости и демократия» сделан вывод, что новой угрозой информационной безопасности является дезинформация и постправда [Farkas, 2019: 155]. В последние годы в медиапространстве увеличилось количество фальшивых новостей — фейков. В медиасреде фейками называют поддельные тексты, фото, видео или аудиозаписи; поддельные страницы или блоги; искусственно созданную популярность личности, проекта, произведения по заданию заказчика с помощью интернет-ботов, фальшивых аккаунтов; ложную или частично искаженную информация о тех или иных событиях [Суходолов, Бычкова, 2017: 159].

Вопросам информационной безопасности Евросоюз уделяет особое внимание: с 1994 по 2004 гг. была реализована программа «Безопасный Интернет». С 2004 г. функционирует Европейское агентство информационной безопасности – *ENISA*. В 2006 г. был принят документ «О Стратегии безопасности информационного общества» [Киселева, 2018]. С 2017 г. в рамках *ENISA* функционирует агентство по обеспечению кибербезопасности с широкими полномочиями по контролю за интернет-пространством. В ЕС ведется работа по согласованию законов государств-членов в сфере кибербезопасности. Например, в апреле 2018 г. 22 европейские страны заключили Соглашение о создании единого цифрового рынка.

Весной 2017 г. ОБСЕ принял «Совместную декларацию о свободе выражения мнений и фальшивых новостях, ложной информации и пропаганде». В документе содержались общие принципы: со стороны государства возможны ограничения на свободу волеизъявления только в целях запрета пропаганды насилия, дискриминации и вражды; любые ограничения считаются законными только в том случае, если суд или независимый орган признал контент вещания незаконным. Для свободы волеизъявления благоприятными условиями являются содействие государством созданию независимых СМИ и четкая нормативно-правовая база для развития свободного, плюралистического вещательного сектора. Посредники, журналисты и органы массовой информации должны проявлять инициативу и сотрудничать в вопросах обеспечения свободы выражения мнения и блокировать дезинформацию и пропаганду. Гарантиями неприкосновенности частной жизни и гражданских свобод в ЕС являются законы: Конституции государств-членов, Хартия ЕС об основных правах, Директива 2002/58/ЕС (2002) о конфиденциальности и электронных средствах связи.

Брюссель выступает за отмену принципа сетевой нейтральности в интернет-пространстве в целях обеспечения информационной безопасности. Осенью 2017 г. Комитет Европарламента по гражданским правам проголосовал за положение, ограничивающее конфиденциальность и контроль пользователей интернет-компаний, но Еврокомиссия заявила, что после 2018 г. последние должны предоставлять доступ к пользовательским данным в течении 10 дней после получения запроса правоохранительных органов, независимо от того, где находится компания и где собираются данные[1].

Евросоюз в борьбе с дезинформацией использует следующие средства: информирование общественности, удаление онлайн-контента с помощью искусственного интеллекта, организация тренингов для СМИ и лидеров мнений, повышение медиаграмотности. Борьба с дезинформацией является важной частью противодействия гибридным угрозам. В 2016 г. была принята Общая рамочная программа ЕС по противодействию гибридным угрозам. Согласно этому документу между государствами ЕС возрос информационный обмен и улучшена координация по обеспечению стратегической коммуникации, а также было усилено сотрудничество по этим вопросам с НАТО[2]. В 2017 г. в Хельсинки ЕС совместно с НАТО создал Центр передового опыта по противодействию гибридным угрозам. «Был предложен общеевропейский Кодекс практики по борьбе с дезинформацией, по которому онлайн-платформы должны принимать меры вплоть до закрытия или демонетизации дезинформационных сайтов или профилей в социальных сетях» [Базаркина, 2021а: 131–132]. Кодекс был подписан всеми крупными транснациональными медиахолдингами и онлайн-платформами (одним из последних Кодекс подписал в 2020 г. *TikTok*). Государства-члены ЕС также являются участниками цифровой платформы

[1] Цензура в интернете: мировой опыт. URL: http://www.tadviser.ru/index.php (дата обращения: 13.07.2022)

[2] Security: EU strengthens response to hybrid threats. European Commission Presscorner. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_16 (дата обращения: 10.07.2021).

для обмена информацией о фейковых новостях – системы оповещения о дезинформации, которая начала функционировать с 18 марта 2019 г. В ее функции входит борьба с фейками и дезинформацией и координация деятельности членов ЕС в данной сфере[1].

Вопросы борьбы с фейками были рассмотрены в Плане действий в сфере развития европейской демократии, принятом зимой 2020 г., и в Законе о цифровых услугах[2]. В Плане 2020 г. были обозначены следующие направления по борьбе с дезинформацией: 1) разработка общей методологии и инструментария ЕС по противодействию иностранному вмешательству и распространению дезинформации; 2) повышение медиаграмотности населения ЕС и поддержка инновационных проектов гражданского общества по борьбе с дезинформацией[3]. Таким образом, в ЕС созданы нормативно-правовая база и аналитические институты по противодействию дезинформации в интернет-пространстве. В этом вопросе институциональные структуры ЕС сотрудничают с гражданским обществом, частными компаниями, а также с НАТО.

Следует отметить, что понятие информационной безопасности стало шире и распространяется на сферу электронной коммуникации, цифровых СМИ и киберпространства в целом. Государства по-разному понимают информационную безопасность. Президент Франции Э. Макрон осенью 2018 г. на международном форуме, посвященном развитию Интернета, предложил «Парижский призыв к обеспечению доверия и безопасности в киберпространстве», состоящий из девяти направлений сотрудничества, среди которых необходимо упомянуть задачи по противодействию преступным действиям в Интернете, рост и укрепление безопасности цифровой продукции, невмешательство в избирательные процессы, а также защиту от кибернаемничества и других преступных действий со стороны различных акторов.

Анализ документов по обеспечению безопасности ЕС показал, что страны Союза большое внимание уделяют технологическому сотрудничеству. Для координации данной деятельности в 2005 г. была создано Европейское агентство по сетевой и информационной безопасности, в задачу которого входят координация и обеспечение безопасности инфраструктурных объектов и сетей, решение вопросов, связанных с киберпреступностью, и разработка стратегий кибербезопасности в ЕС.

По мнению российского исследователя Д. Базаркиной, государства ЕС «гиперполитизируют» противодействие гибридным угрозам и «используют для оправдания санкционного давления, усиления военных блоков или массированных инфор-

[1] Шейко Ю. В ЕС запустили систему оповещения о дезинформации. Deutsche Welle. 18.03.2019. URL: https://www.dw.com/ru/в-ес-запустили-систему-оповещения-о-дезинформации (дата обращения: 13.07.2022) (28 марта 2022 г. Deutsche Welle (Германия, Kurt-Schumacher-Strasse 3, 53113 Bonn) включено Минюстом России в реестр иностранных средств массовой информации, выполняющих функции иностранного агента.)

[2] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. COM/2020/825 final.

[3] Digital Services Act – Questions and Answers. European Commission Presscorner. 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/QAND (дата обращения: 10.07.2021)

мационных кампаний против политического оппонента» на фоне углубления экономической конкуренции и политических противоречий между государственными акторами [Базаркина, 2021b: 133].

Цифровые СМИ являются ведущими субъектами национальной безопасности в связи с возрастающей ролью информации и возможностью ее использования в целях нанесения ущерба национальным интересам. Фейковые новости в зависимости от целей создания представляют опасность в условиях развития информационных технологий. Неконтролируемое распространение фейков способно спровоцировать «информационные теракты». В 2017 г. ЕС создало новое специализированное подразделение *«East Stratcom»* для противодействия угрозе кибератак и фейковых новостей.

На формирование общественного мнения влияние оказывают корпорации *Microsoft, YouTube, Facebook* (деятельность в России запрещена), *Apple*, им принадлежит одна треть глобального трафика. Как показали события «войны» Д. Трампа с интернет-холдингами, в демократических политических системах социальные сети являются важными инструментами контроля и регулирования общественного мнения в политической конкуренции. Изучая опыт демократических стран, мы приходим к выводу, что существует объективная необходимость в развитии альтернативных социальных сетей – государственных интернет-платформ. Необходимо также осуществлять контроль над Интернетом и правовое регулирование данной сферы.

Основатель *Facebook* (деятельность в России запрещена) М. Цукерберг после президентских выборов в США в 2016 г. предложил меры по борьбе с дезинформацией: 1) отключать сайты, распространяющие фейковые новости; 2) отключать от монетизации вышеуказанные сайты; 3) использовать механизмы искусственного интеллекта для обнаружения дезинформации и видеотрансляций со сценами насилия[1]. Платформа также предоставляет программы для обучения журналистов и пользователей по обнаружению дезинформации в социальных сетях[2]. По словам руководителя Социал-демократической партии Германии Т. Оппермана, вышеуказанные меры транснациональных медиахолдингов недостаточны, в связи с чем он предложил наказывать крупными штрафами интернет-платформы, которые распространяют фейковые новости и дезинформацию. Многие политики Германии заявили, что наряду с создателями и распространителями фейков социальные сети также должны нести часть ответственности за их распространение[3]. Из стран ЕС наиболее эффективно с выявлением фейковых новостей справляется Германия. В частности, там запустили механизм выявления дезинформации, ложных новостей, а у пользователей есть возможность обратиться к независимому фактчекеру *Correctiv*. В слу-

[1] Facebook Starts Taking Measures Against Fake News. URL: http://www.vedomosti.ru/technology/ articles/2016/12/16/669946 (дата обращения: 10.01.2022)

[2] Голицына А. Журналисты помогут Facebook бороться с фейками. Ведомости. 11.01.2017. URL: http://www.vedomosti.ru/technology/articles/2017/01/11/672608-zhurnalisti-pomogut-facebook (дата обращения: 12.01.2022)

[3] В Германии могут начать штрафовать Facebook. URL: https://ria.ru/world/20161216/1483846152.html. (дата обращения: 25.01.2022)

чае подтверждения фейковой новости распространители получают предупреждение [Kuchler, 2017].

Заключение

Страны ЕС стоят перед выбором между безопасностью и свободой в вопросе регулирования деятельности цифровых СМИ. Одна из ценностей демократии – это конфиденциальность. Обеспечение национальной безопасности посредством наблюдения за Интернетом не должно осуществляться в ущерб частной жизни и гражданским свободам. Некоторые корпорации и государства могут легко вмешиваться в жизнь других стран через информационное пространство, программное и аппаратное обеспечение. Политические манипуляции на фоне растущей геополитической напряженности могут привести к угрозе ограничения или даже к полному закрытию киберпространства отдельных стран. В текущей ситуации возрастает роль регулирования цифровой конфиденциальности и защиты фундаментальных прав человека.

В целях создания эффективной модели управления общественным мнением и обеспечения информационного суверенитета Евросоюз предпринимает следующие меры: развивает новые информационные технологии управления, проводит исследования основных медиатрендов и медиапредпочтений граждан ЕС в целях определения основных направлений информационной работы, развивает деятельность, направленную на укрепление конкурентоспособности европейских СМИ посредством поощрения конкуренции внутри информационного пространства.

СПИСОК ЛИТЕРАТУРЫ

Балуев Д. Г. (2013) Политическая роль социальных медиа как поле научного исследования. *Образовательные технологии и общество*. № 2. С. 604–616.

Базаркина Д.Ю. (2021a) Эволюция подхода Европейского Союза к борьбе с дезинформацией. *Власть*. № 6. С. 130–138.

Базаркина Д. (2021b) Эволюция подходов к противодействию гибридным угрозам в стратегическом планировании ЕС. *Современная Европа*. № 6. С. 133–143. DOI: http://dx.doi.org/10.15211/soveurope62021133143

Бельков О.А. (2004) Понятийно-категориальный аппарат концепции национальной безопасности. *Безопасность: информационный сборник*. № 3. С. 91–94.

Гапич А.Э., Лушников Д.А. (2010) *Технологии «цветных революций»*. РИОР, Москва, Россия. 132 с.

Гасанова В.С. (2016) Киберпреступления в международном праве: понятие, содержание и меры регулирования. *Юридическая наука: история, современность, перспективы. Сборник материалов VII международной научно-практической конференции, посвященной Дню российской науки*. Международный юридический институт, Москва, Россия. С. 244–248.

Кастельс М. (2016) *Власть коммуникации*. ГУ ВШЭ, Москва, Россия. 564 с.

Кагазбаева Э.М., Алмырза Б. (2021) Концептуальные основы исследования цифровых СМИ в аспекте национальной безопасности. *Известия КазУМОиМЯ имени Абылай хана. Серия Международные отношения и регионоведение.* № 4 (46). С. 7–18. DOI: 10.48371/ISMO.2021.46.4.001.

Киселева Н.В. (2018) Формирование организационно-правовых основ политики информационной безопасности: опыт Европейского Союза. *Академический вестник Ростовского филиала РТА.* № 2(31). С. 95–103.

Леви Д.А. (2018) Безопасность и риски политической дефрагментации киберпространства. *Азимут научных исследований: экономика и управление.* Т. 7. № 4(25). С. 375–378.

Мирошниченко И.В. (2013) *Сетевой ландшафт российской публичной политики*. Просвещение-Юг, Краснодар, Россия. 295 с.

Поздняков А.И. (2013) Сравнительный анализ основных методологических подходов к построению теории национальной безопасности. *Национальные интересы: приоритеты и безопасность*. № 21(210). С. 46–53.

Суходолов А.П., Бычкова А.М. (2017) «Фейковые» новости как феномен современного медиапространства: понятие, виды, назначение, меры противодействия. *Вопросы теории и практики журналистики*. Т. 6. № 2. С. 143–169.

Скрипка И. (2021) Электронные СМИ и социальные сети в политике: европейский опыт. *Современная Европе*. № 4. С. 184–193. DOI: http://dx.doi.org/10.15211/soveurope42021184193

Тоффлер Э. (1999) *Третья волна*. АСТ, Москва, Россия. 464 с.

Castells M. (2001) T*he Internet Galaxy: Reflections on the Internet, Business, and Society.* Oxford University Press, Oxford, UK. 292 p.

Farkas J. (2019) *Post-Truth, Fake News and Democracy*. Routledge, N.Y., USA. 305 p.

KEA (2021) *Research for CULT Committee – Europe's media in the digital decade*. European Parliament, Policy Department for Structural and Cohesion Policies, Brussels, Belgium. 40 p. DOI: 10.2861/63848

Kuchler H. (2017) Facebook rolls out fake-news filtering service to Germany. *Financial Times*. 15.01. URL: https://www.ft.com/content/75796bce-d9dd-11e6-944b-e7eb37a6aa8e (accessed: 02.09.2022)

Lippman W. (1943) *US Foreign Policy: Shield of the Republic*. Little, Brown and Co., Boston, USA. 177 p.

Mourao R.R., Yoo J., Geise S., Araiza J.A., Kilgo D.K., Chen V., Johnson T.J. (2015) Online News, Social Media, and European Union Attitudes: A Multidimensional Analysis. *International Journal of Communication*. Vol. 9(24). Pp. 3199–3222.

Neuman R. (1991) *The Future of the Mass Audience*. Cambridge University Press, Cambridge, UK. 180 p.

Solis B., Breakenridge D.K. (2009) *Putting the Public Back in Public Relations: How Social Media Is Reinventing the Aging Business of PR*. Pearson Education Inc., Upper Saddle River, USA. 352 p.

Wolfers A. (1962) *Discord and Collaboration: Essays on International Politics*. The Johns Hopkins University Press, Baltimore, USA. 283 p.

Digital Media Provision of Information Security: the EU's Experience

K.Zh. Nugmanova*
Doctor of Sciences (Politics), Professor
President of the International Center of Geopolitical Forecasting «East-West»
4, E 607 Street, Nur-Sultan, Kazakhstan
***E-mail:** politassoc@mail.ru*

E.M. Kagazbaeva**
Candidate of Sciences (Politics), Associate Professor
of Abylai Khan Kazakh University of International Relations and World Languages
200, Muratbaeva Street, Almaty, Kazakhstan
****E-mail:** Kagazbaeva.e@gmail.com*

Abstract. Mass media can be a channel for destructive information**.** In the short term, digital media will become the main primary source of information for the population of any state, hence the role of digital media in the information security process will be significant. Digital media in the European Union is a factor of political influence and power. Transnational online and new media, some of which have destructive effects in the media system, threaten the European Union's information security. The purpose of this study is to review the experience of the European Union in regulating digital media from a national security perspective. The authors analyse the European Union's anti-fraud and disinformation policy; show the main trends in the development of new media, based on the concept of M. Castells network structures society. The analysis of the development of digital media, the European Union's policy in the field of information security leads to the conclusion that the dilemma of security or freedom is resolved in favor of security. The role of the European Union institutions in regulating Internet, digital media, digital privacy, protection of fundamental human rights and the creation of a single European digital space is increasing.

Key words: digital policy, digital media, social networks, information security, interests, communication, information sovereignty, disinformation, fakes, civil society.

DOI: 10.31857/S0201708322060080

EDN: gqfhyx

REFERENCES

Baluev D.G. (2013) Politicheskaya rol' social'nih media kak pole nauchnogo issledovaniya. [The political role of social media as a research field]. *Obrazovatel'nie tehnologii I obshestvo*, no. 2, pp. 604–616 (in Russian).

Bazarkina D.U. (2021a) Evoluciya podhoda Evropeiskogo Soyuza k bor'be s dezinformaciei [The evolution of the European Union's approach to combat disinformation], *Vlast*, no. 6, pp. 130–138. DOI: http://dx.doi.org/10.15211/soveurope62021133143 (in Russian).

Bazarkina D. (2021b) Evolyuciya podhodov k protivodejstviyu gibridnym ugrozam v strategicheskom planirovanii ES [There is an evolution of approaches to countering hybrid threats in strategic planning]. *Sovremennaya Evropa*, no. 6, pp. 133–143, (in Russian).

Castells M. (2016) *The Power of Communication [The power of communication]*, GU VSHE, Moscow, Russia (in Russian).

Castells M. (2001) *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford, Oxford University Press, UK.

Gapich A.E., Lushnikov D.A. (2010) *Tehnologii «cvetnih revolucii [«Colour revolutions» technologies]*, RIOR, Moscow, Russia (in Russian).

Gasanova V.S. (2016) Kiberprestupleniya v mezhdunarodnom prave: ponyatie, soderzhanie i meri regulirovaniya [Cybercrime in international law: concept, content and regulation]. *Uridicheskaya nauka: istoria, sovremennost', perspektivi. Sbornik materialov VII mezhdunarodnoi nauchno-prakticheskoi konferencii, posvyashennoi Dnyu rossiiskoi nauki*, Mezhdunarodnyj yuridicheskij institut, Moscow, Russia, pp. 244–248 (in Russian).

Johan Farkas (2019) *Post-Truth, Fake News and Democracy*, Routledge, N.Y., USA.

Kagazbaeva E.M., Almyrza B. (2021) Conceptual foundations of digital media research in the aspect of national security, *Bulletin of Ablai Khan KazUIRandWL: Series «International relations and regiona studies*, no. 4 (46), pp. 7–18. DOI: 10.48371/ISMO.2021.46.4.001 (in Russian).

KEA (2021) *Research for CULT Committee – Europe's media in the digital decade*, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels, Belgium. DOI: 10.2861/63848

Kiseleva N.V. (2018) Formorovanie organizacionno-pravovih osnov politiki informacionnoi bezopasnosti: Opit Evropeiskogo Soyuza [Formation of the organizational and legal framework of the information policy: The European experience], *Akademicheskiy vestnik Rostovskogo filiala RTA*, no. 2(31), pp. 95–103 (in Russian).

Kuchler H. (2017) Facebook rolls out fake-news filtering service to Germany. *Financial Times*. 15.01. URL: https://www.ft.com/content/75796bce-d9dd-11e6-944b-e7eb37a6aa8e (accessed: 02.09.2022)

Levi D.A. (2018) Bezopasnost' i riski politicheskoj defragmentacii kiberprostranstva [Security and risks of political defragmentation of cyberspace], *Azimut nauchnyh issledovanij: ekonomika i upravlenie*, vol. 7, no. 4(25), pp. 375–378 (in Russian).

Lippman W. (1943) *US Foreign Policy: Shield of the Republic*. Little, Brown and Co., Boston, USA.

Miroshnichenko I.V. (2013) *Setevoi landshaft rossiiskoy publichnoi politiki [Russian Public Policy Network Landscape]*, Prosveshenie-Ug, Krasnodar, Russia (in Russian).

Mourao R.R., Yoo J., Geise S., Araiza J.A., Kilgo D.K., Chen V., Johnson T.J. (2015) Online News, Social Media, and European Union Attitudes: A Multidimensional Analysis, *International Journal of Communication*, vol. 9(24), pp. 3199–3222.

Neuman R. (1991) *The Future of the Mass Audience*, Cambridge University Press, Cambridge, UK.

Pozdnyakov A.I. (2013) Sravnitel'nyj analiz osnovnyh metodologicheskih podhodov k postroeniyu teorii nacional'noj bezopasnosti [Comparative analysis of the main methodological approaches to the construction of the theory of national security], *Nacional'nye interesy: prioritety i bezopasnost'*, no. 21(210), pp. 46–53 (in Russian).

Solis B., Breakenridge D.K. (2009) *Putting the Public Back in Public Relations: How Social Media Is Reinventing the Aging Business of PR*, Pearson Education Inc., Upper Saddle River, USA.

Sukhodolov A.P., Bychkova A.M. (2017) «Feikoviye» novosti kak fenomen sovremennogo mediaprostranstva: ponyatie, vidi, naaznachenie, meri protivodeystviya [«Fake» news as a phenomenon of modern media: concept, types, purpose, measures], *Voprosi teorii I praktiki zhurnalistiki*, vol. 6., no. 2, pp. 143–169 (in Russian).

Skripka I. (2021) Elektronnye SMI i social'nye seti v politike: evropejskij opyt [Electronic media and social networks in politics: European experience], *Sovremennaya Evrope*, no. 4, pp. 184–193. DOI: http://dx.doi.org/10.15211/soveurope42021184193 (in Russian).

Toffler E. (1999) *The Third Wave*, ACT, Moscow, Russia (in Russian).

Wolfers A. (1962) *Discord and Collaboration: Essays on International Politics*, The Johns Hopkins University Press, Baltimore, USA.