Санкт-Петербургский государственный университет

БЕЛЕНКОВ Даниил Вадимович

Выпускная квалификационная работа

Проблемы эффективности информационной политики Европейского союза в контексте общей европейской внешней политики

Уровень образования: высшее

Направление *41.04.05 «Международные отношения»*

Основная образовательная программа *ВМ.5565 «Мировая политика»*

Научный руководитель:
профессор кафедры мировой политики,
доктор политических наук,
Маркушина Наталья Юрьевна

Рецензент:
Начальник отдела обеспечения
международного и межрегионального
сотрудничества СПБГБУ
«Координационный центр научно-
технических и образовательных программ»
Карпенко Александр Михайлович

Санкт-Петербург
2020

Оглавление

Введение

В мировой политике сегодня особое развитие получают отношения в информационной сфере. Эта область все чаще становится полем взаимодействия и противостояния. Информация и массовые коммуникации все больше становятся ресурсом влияния. Для акторов в международных отношениях стало очевидным, что коммуникации могут быть самостоятельным средством по достижению своих целей. Проблема безопасности стала важным вопросом в информационной политике стран и объединений. Информационное пространство дало расширенные возможности взаимодействия между собой людям, государственным и наднациональным учреждениям, коммерческим и некоммерческим организациям.

Хорошим примером развития информационной политики является Европейский союз. Эта сфера особенно развивалась в союзе с начала 2000-х и имела разные направления на протяжении 20 лет. Это связано с возникавшими в разное время внутренними и внешними вызовами. Сфера внешней информационной политики получила сильный стимул к развитию в результате неудачи в информационном противостоянии с Россией по вопросу украинского кризиса. Украина является сферой столкновения интересов России и Европейского союза. В данной работе рассмотрен информационный аспект. Это также интересный пример отношений государства и объединения государств в конкретном сегменте – информационном. В работе проводится кейс-стади, где разбираются подходы Европейского союза и России к действиям в информационном пространстве. В связи с этим также необходимо оценить, насколько это равнозначные акторы. Дальнейшее развитие этой сферы – хороший пример ответа интеграционного объединения на информационные угрозы и адаптации к новым условиям.

На повестке в последние годы возник вопрос вмешательства третьих сторон в европейские процессы, а главным инициатором вмешательства называют Россию. Развитие информационных технологий, появление огромного числа каналов трансграничных массовых коммуникаций привело не только к облегчению и разнообразию полезных коммуникаций, но и возможности использования информационной среды для оказания скрытого влияния в целях достижения внешнеполитических интересов. Объекты критической информационной инфраструктуры, избирательные системы, убеждения населения, сферы социальной напряженности – все это угрожаемые области, которые могут подвергаться воздействию через средства коммуникации.

Проблема информационной безопасности актуальна для всех стран-членов союза. Поэтому предотвращение информационных угроз является задачей не только отдельных государств, но и наднациональных органов. С этой целью развиваются и функционируют

общеевропейские учреждения кибербезопасности, стратегических коммуникаций и защиты от гибридных угроз. Членство большинства стран Европейского союза в НАТО обеспечивает безопасность от непосредственно военных действий, однако операции по влиянию информационными средствами к таковым не относятся, но могут нанести значительный ущерб в социально-политическом отношении. Европейский союз стал развивать собственные структуры информационной безопасности, сотрудничая при этом с НАТО в обмене опытом и информацией об угрозах. Остается актуальным вопрос, насколько возможно использование этой системы за границами союза для оказания влияния.

Тема актуальна ввиду повышения интереса в мировой политике к возможности использования новостей и сообщений в социальных сетях в целях внешней политики. В силу сохранения российско-европейских противоречий на фоне ряда напряженных моментов, в числе которых присоединение Крыма, катастрофа МН 17, дело Скрипалей, возможное вмешательство в выборы европейских стран, можно проследить, какие факторы могут влиять на приоритеты информационной политики.

Цель исследования: выявить проблемные сферы в существующей системе информационной безопасности и определить потенциальные направления ее дальнейшего развития в условиях внешних угроз европейским общественно-политическим процессам.

Поставлены следующие задачи:

- определить основные для исследования категории и теоретическую основу;

- выявить связь внешней информационной политики и борьбы с дезинформацией;

- проанализировать эффективность системы информационной безопасности Европейского союза;

- провести сравнительный анализ оценок и подходов к вопросу деятельности сторон в информационном поле в рамках украинского кризиса.

Предмет исследования: информационная политика Европейского союза.

Объект исследования: общая европейская внешняя политика.

Использованные общенаучные методы: сравнительный анализ, системный метод. Сравнительный анализ необходим для выявления общих и различных черт в национальной информационной политике и политике интеграционного объединения. Системный метод позволил определить возможности системы информационной безопасности Европейского союза и сделать предположения о дальнейших направлениях ее развития. Использован также специальный метод – анализ документов, позволяющий проследить основные черты в развитии информационной политики и выявить проблемы в ходе украинского кризиса.

Для определения перспектив развития ситуации по украинскому вопросу проведен контент-анализ.

Научная новизна диссертационного исследования состоит в анализе отношений в информационной сфере по вопросу Украины и оценке действий Европейского союза на основе российских и европейских исследований.

Степень научной разработанности темы невысока. Существует мало российских публикаций, которые бы объективно и непредвзято рассматривали ответ Европейского союза на внешние угрозы, а также действия сторон в информационном поле на фоне украинского кризиса. Принятие Европейским парламентом резолюции о противодействии пропаганде и создание East SratCom обычно рассматриваются как агрессия и безосновательные нападки в отношении России. Среди европейских публикаций многие описывают российскую систему по оказанию информационного влияния и систему Европейского союза для борьбы с дезинформацией, но мало связывают ее с внешней политикой.

Для формирование категориального аппарата особенно полезными были работы Кучерявого М.М. и Курышевой Ю.В. Эти авторы подробно рассмотрели ключевые черты акторов информационной политики и их задачи.

Для изучения основ информационной политики России были использованы российские документы стратегического планирования: Стратегия развития информационного общества, Доктрина информационной безопасности, Стратегия развития отрасли информационных технологий, Стратегия национальной безопасности, Концепция внешней политики.

При анализе успехов и проблем в информационной политике Европейского союза и оценке российских действий полезными были публикации Европейского института проблем безопасности, Фонда Маршалла и Фонда Карнеги. В них с разной степенью негативной риторики в отношении России описаны главные этапы в становлении системы и основные перспективы для развития. Некоторые аналитические публикации были подготовлены специалистами из США, что подчеркивает вовлеченность этой страны в европейские процессы в части безопасности. Исследования этих же учреждений, а также Гаагского центра стратегических исследований помогли проследить развитие отношения Европейского союза к информационному противостоянию по вопросу Украины.

Также использовано большое количество официальных документов Европейского союза, которые были необходимы для определения черт европейской информационной политики: резолюции, регламенты и директивы Европарламента, сообщения Европейской

комиссии. Все они отражают официальную политику союза и поэтому представляют большую ценность.

Важными документами для определения ключевых черт современной информационной политики были План действий по борьбе с дезинформацией и Свод правил по дезинформации 2018 года. Эти документы были приняты в основном для обеспечения безопасности европейских выборов и независимости убеждений граждан. Они определили основные положения по работе с социальными сетями и открыли возможности для взаимодействия между наднациональным и негосударственным секторами в части защиты от дезинформации.

Необходимыми для анализа европейского подхода к информационным угрозам были такие документы, как Общие принципы по борьбе с гибридными угрозами, Стратегия кибербезопасности, Резолюция о противодействии пропаганде, Сообщение Европейской комиссии о борьбе с дезинформацией, План действий по стратегическим коммуникациям. Все они придерживаются одного нарратива – необходимость борьбы с дезинформацией и дают оценку текущей ситуации, а некоторые из документов дали начало многим инициативам, как, например, учреждение East StratCom.

Использована информация с официальных сайтов Европейского союза, Европейской комиссии, Европейской службы внешнего действия, ENISA, где также отражена официальная позиция Европейского союза.

Также использованы новостные публикации российских и европейских информационных ресурсов, публикации с официального сайта Российского института стратегических исследований и EUvsDISINFO.

Работа состоит из введения, трех глав, в каждой из которых по три параграфа, заключения и списка источников и литературы.

Глава 1

Концептуальная основа категории информационной политики

§1.1 Понятийные подходы к информационной политике

Всю область информационной политики можно разделить на два больших направления: компьютерные системы и содержательная часть. Первая касается передачи, обработки и хранения информации, баз данных, доступа к данным, функционирования компьютерных систем, защиты данных пользователей. Вторая – сообщений, транслируемых на население через СМИ, социальные сети, официальные заявления, научно-аналитические исследования.

Необходимо определиться с тем, как в данной работе будут пониматься ключевые понятия:

информационный суверенитет – самостоятельность субъекта отношений в информационной сфере в проведении внутренней и внешней информационной политики и способность обеспечить безопасность собственного информационного пространства;

информационная политика – целенаправленная деятельность субъекта отношений в информационной сфере по достижению внутриполитических и внешнеполитических целей через регулирование и организацию технической и содержательной составляющих информационного пространства;

информационное противоборство – состояние отношений субъектов в информационной сфере, характеризующееся соперничеством и являющееся следствием стремления как минимум одного из субъектов к достижению внешнеполитических целей средствами воздействия в информационном пространстве[1].

Понятие информационной войны представляется неуместным для использования в контексте невоенного противостояния. Информационная война предполагает нанесение физического ущерба информационной инфраструктуре, атаки в цифровой среде на объекты критической инфраструктуры, возможность человеческих жертв, нарушение военных и гражданских коммуникаций. Некоторые средства информационной войны могли быть использованы в ходе присоединения Крыма: нарушение связи, захват объектов. Это

[1] Беленков Д.В., Гюлазян П.А., Мазлумян Д.Э. Информационный суверенитет России и Европейского союза, информационная политика и информационное противоборство: сущность и содержание // Международный студенческий научный вестник, №5 2018

понятие используется зачастую журналистами, соответствующие разделы и теги можно увидеть на сайтах новостных ресурсов[2].

Изначальный термин «Information warfare» использовался министерством обороны США с 1992 года в отношении радиоэлектронной борьбы. В 1996 году в отчете корпорации «Рэнд» MR-6610OSD был использован термин «Strategic Information Warfare», с тех пор он понимается в военно-стратегическом и политическом смысле[3]. В 1998 году в США была введена в действие доктрина информационных операций. В ней «Information Warfare» понималось как комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе открытого военного конфликта полностью парализовало бы инфраструктуру управления противника[4].

Формулировку «информационное противоборство» лучше использовать в связи с тем, что противоборство имеет более широкое значение, чем война. Противоборство, в отличие от войны, не обязательно направлено на принуждение к принятию условий побежденной стороной.

Одной из задачи информационной политики является поддержание информационного суверенитета, то есть обеспечение информационной безопасности. Субъект может осуществлять это через развитие информационной инфраструктуры, определение угроз и создание соответствующей законодательной базы. По поводу информационной безопасности Ерофеева Н.В. дает следующее определение: «Способность государства, организации, личности, а также технической и информационной системы или конструкции обеспечить необходимые информационные ресурсы для поддержания их устойчивого функционирования в любых сложных условиях существования и развития, а также их способность противодействовать возникающим опасностям и угрозам по отношению к информационным ресурсам, техническим источникам информации, компьютерным и другим различным сетям передачи и обмена информации между техническими устройствами и конкретными потребителями»[5]. Также можно сказать, что

[2] Захарова сообщила о характере ответов России на информационную агрессию // сайт РИА новости URL: https://www.rbc.ru/rbcfreenews/5daafa179a7947060acaa0da

[3] Гриняев С.Н. Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. №8, 2001

[4] Иванов С.А. Информационная война: сущность и основные формы проявления // Известия АлтГУ. 2013. №4 (80). URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-suschnost-i-osnovnye-formy-proyavleniya

[5] Ерофеева Н.В. Современные информационные войны и их влияние на политическую стабильность государства // PolitBook. 2015. №2. URL: https://cyberleninka.ru/article/n/sovremennye-informatsionnye-voyny-i-ih-vliyanie-na-politicheskuyu-stabilnost-gosudarstva (дата обращения: 3.04.2018)

это состояние защищенности информационной сферы от угроз технического и содержательного характера.

Возможность быть актором в информационной среде определяется наличием информационного суверенитета. По мнению А.А. Ефремова, государственный суверенитет в информационном пространстве, с точки зрения права, заключается в возможности регулирования информационного пространства через национальное и международное право[6].

М.М. Кучерявый выделяет ряд возможных внешних угроз суверенитету:

- деятельность зарубежных структур, направленная против суверенной власти;
- доминирование отдельных политических сил в информационном пространстве;
- терроризм;
- формирование агрессивных концепций информационного противоборства в отдельных странах. [7]

Согласно Д.С. Артамонову, информационный суверенитет заключается в сочетании контроля государства над своей информационной сферой и защитой ее от угроз, таких как информационные войны и кибератаки[8]. Вместе с тем в понятии информационного суверенитета выделяется ряд составляющих: цифровой суверенитет, медийный суверенитет, идеологический суверенитет, ментальный (культурный) суверенитет, интеллектуальный суверенитет (образование и наука), репутационный суверенитет (имидж). Все эти составляющие объединены необходимостью обеспечения защиты со стороны государства. Более грубо можно было бы разделить сферы суверенитета на техническую и идеологическую составляющие[9]. Все то же самое может быть применимо и в отношении союза, ставящего среди своих целей формирование собственного защищенного информационного пространства. Таким образом, суверенитет обеспечивается защитой от угроз.

Еще одна важная категория – стратегические коммуникации. Соответствующее направление внешней политики есть в национальных и союзных политиках. Они

---

[6] Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. №1. URL: https://cyberleninka.ru/article/n/formirovanie-kontseptsii-informatsionnogo-suvereniteta-gosudarstva

[7] Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира. // Управленческое консультирование. 2015. №2 (74). URL: https://cyberleninka.ru/article/n/gosudarstvennaya-politika-informatsionnogo-suvereniteta-rossii-v-usloviyah-sovremennogo-globalnogo-mira

[8] Артамонов Д.С. Информационный суверенитет, теоретический аспект // Материалы VIII Международного Конституционного Форума, посвященного 80-летию Саратовской области. 2017 стр.16-20

[9] Зорина Е.Г. Информационный суверенитет современного государства и основные инструменты его обеспечения // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2017 №3 стр.345-348

охватывают любую коммуникационную деятельность организации и страны. Все действия могут восприниматься целевой аудиторией и способствовать формированию общего представления. Один из исследователей RAND Кристофер Пол дал такое определение стратегическим коммуникациям: «Скоординированные действия, сообщения, образы и другие виды оповещения и вовлеченности, направленные на информирование, влияние и убеждение определенных аудиторий в поддержку целей государства»[10]. Такое определение отвечает контексту международных отношений в информационной среде.

§1.2 Анализ национальной и союзной концепций

В данном параграфе рассмотрена информационная политика Европейского союза в сравнении с российской информационной политикой, выделены одинаковые и разные черты. Таким образом, можно будет сделать вывод вообще о схожести и различиях информационных политик страны и объединения стран, а также вывод о том, можно ли рассматривать отношения Европейского союза и России в информационной сфере.

В этой связи можно утверждать о наличии информационного суверенитета Европейского союза по двум причинам:

во-первых, наличие обширного наднационального законодательства по вопросу отношений в информационной сфере;

во-вторых, явно выраженное в Европейском союзе восприятие угрозы собственному информационному пространству извне, что в некоторой мере определяет его границы и как минимум дает основания говорить о его существовании.

Ipso facto можно утверждать, что оба рассматриваемых субъекта способны проводить собственную информационную политику, а значит могут подвергаться сравнению.

Во-вторых, необходимо понимать, что Европейский союз не является государством, но высокоинтегрированным объединением государств. Информационное пространство союза следует рассматривать как совокупность информационных систем и потоков информации всех стран-членов в той части, что затрагивает общеевропейские интересы и которые подвергаются наднациональному регулированию. Страны-члены являются основными производителями информации как в материальной части, так и в виртуальной,

[10] Богданов С.В. Стратегические коммуникации: концептуальные подходы и модели для государственного управления // Государственное управление. Электронный вестник. 2017. №61. URL: https://cyberleninka.ru/article/n/strategicheskie-kommunikatsii-kontseptualnye-podhody-i-modeli-dlya-gosudarstvennogo-upravleniya

а общий их интерес в информационной сфере находит отражение в решениях наднационального уровня. Европейский союз является не столько самостоятельным актором, сколько суммой интересов всех членов в сфере обеспечения безопасности и единообразия в информационной сфере. В связи с этим существуют учреждения, действующие в общесоюзных интересах.

Для начала можно рассмотреть государственную информационную политику Российской Федерации с позиции обеспечения информационной безопасности, учитывая то, что одной из главных функций государства во внешнеполитическом отношении является обеспечение национальной безопасности и сохранение собственного суверенитета.

Основные функции государства в этом направлении:

- анализ и прогнозирование угроз;

- разработка мер и механизмов обеспечения информационной безопасности в случае угрозы;

- организация работы законодательных и исполнительных органов по реализации мер, направленных на нейтрализацию угроз;

- организация работы органов государственной власти с общественными организациями и гражданами и определение правовых механизмов по противодействию возможным угрозам;

- контроль деятельности СМИ в рамках закона;

- разработка норм федерального законодательства в сфере информационной безопасности, определение юридической квалификации акциям в информационном пространстве;

- участие в разработке норм международного права;[11]

Концептуальные основы информационной политики РФ следует изучать через анализ основных документов стратегического планирования в информационной сфере.

Для данной работы интересны следующие документы:

- Стратегия развития информационного общества РФ;

- Доктрина информационной безопасности РФ;

- Стратегия развития отрасли информационных технологий в РФ на 2014-2020 годы и на перспективу до 2025 года;

- Стратегия национальной безопасности РФ;

[11] Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В.Б. Вепринцев, А.В. Манойло, А.И. Петренко, Д.Б. Фролов; под ред. А.И. Петренко. – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2011. – 495с.

- Концепция внешней политики РФ.

Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы[12] основывается, среди прочего, на Стратегии национальной безопасности и Доктрине информационной безопасности РФ. В ней учтены положения Окинавской хартии 2003 года, Декларации принципов построения информационного общества 2003 года, Плана действий Тунисского обязательства 2005 года.

Что интересно, уже в общих положениях можно увидеть такую формулировку, как «традиционные российские духовно-нравственные ценности». Она же встречается и в других документах, относящихся к политике в информационной сфере. То есть, согласно им, предполагается соблюдение таких ценностей в информационном пространстве как коммуникативной среде. Отметим сразу, что в европейских документах не прослеживается стремлений создать «европейских дух», «традиционные ценности» или что-нибудь подобное.

Следует обратить внимание и на такое понятие, как «объекты критической информационной инфраструктуры», подразумевающее наиболее важные объекты информационной инфраструктуры, в первую очередь нуждающиеся в обеспечении защиты: транспорт, связь, энергетика, топливная, атомная, ракетно-космическая, химическая и прочая промышленность, сфера здравоохранения и др. В вопросах, касающихся обеспечения национальной безопасности, им отводится значимое место как в России, так и ЕС.

В целом можно назвать следующие основные направления информационной политики, вытекающие из этой стратегии:

- обеспечение повсеместного доступа к сети Интернет;

- противодействие учащающимся кибератакам;

- содействие развитию информационного общества;

- производство собственных информационно-коммуникационных технологий (ИКТ) и как можно более широкое их использование взамен импортных, на чем сделан особый акцент;

- недопущение влияния на собственное население извне в информационной сфере;

- повышение международного имиджа РФ в культурной и гуманитарной сферах;

- контроль информации в российском сегменте сети Интернет;

- повышение сознательности граждан в информационной сфере;

[12] Указ Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” URL: http://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 13.02.2020)

- увеличение количества полезной медиапродукции российского производства;

- развитие традиционных средств вещания;

- совершенствование нормативно-правовой базы в информационной сфере.

Этот документ наиболее полно отражает приоритеты российской информационной политики. Схожие положения прослеживаются в прочих документах стратегического планирования.

Один из наиболее важных документов, определяющих основы информационной политики и информационной безопасности - Доктрина информационной безопасности РФ[13]. Текущая ее версия была принята 5 декабря 2016 года. До этого она утверждалась лишь в 2000 году, так что за все 16 лет концептуальные основы информационной безопасности РФ не претерпевали изменений.

Под обеспечением информационной безопасности в ней подразумевается «осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно- технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления».

В Доктрине напрямую констатируется наличие угрозы применения средств информационно-психологического воздействия со стороны неназванных иностранных государств, направленного на дестабилизацию политического положения целых регионов мира.

Стратегия развития отрасли информационных технологий в РФ на 2014-2020 годы и на перспективу до 2025 года[14] - основной документ, определяющий направления развития технической сферы информационного пространства (информационной среды). В общих положениях Стратегии сказано, что «реализация Стратегии будет способствовать обеспечению информационной безопасности и высокого уровня обороноспособности страны, в том числе за счет создания современных средств реагирования и предупреждения глобальных информационных угроз».

Стратегия национальной безопасности[15] - базовый документ в вопросе национальной безопасности РФ. В качестве одной из угроз в ней обозначено

[13] Доктрина информационной безопасности РФ, утверждена Указом Президента РФ от 5 декабря 2016 г. №646 URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 13.02.2020)

[14] Стратегия развития отрасли информационных технологий в РФ на 2014-2020 годы и на перспективу до 2025 года, утверждена распоряжением Правительства РФ от 1 ноября 2013 г. №2036-р URL: http://minsvyaz.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014-2020_2025.pdf (дата обращения: 13.02.2020)

[15] Указ Президента РФ от 31.12.2015 №683 «О Стратегии национальной безопасности Российской Федерации» URL:

информационное давление, осуществляемое со стороны США и их союзников, упоминаются информационные инструменты борьбы за влияние. Идет также речь о поддержке Европейским союзом «антиконституционного государственного переворота на Украине». Констатируется усиливающееся противоборство в глобальном информационном пространстве, рост преступности в информационной сфере. В Стратегии предусмотрено использование информационных мер для обеспечения безопасности.

Еще один документ, представляющий интерес - Концепция внешней политики РФ[16]. Как и в Стратегии, в Концепции уделяется внимание растущему влиянию информационного фактора и возможностям использования «мягкой силы».

В Концепции в числе общих задач ставится необходимость улучшения российского международного имиджа информационными средствами, что вполне логично для Концепции внешней политики, если говорить о задачах внешней информационной политики. Согласно Концепции, Россия принимает участие в обеспечении информационной безопасности как на национальном, так и международном уровне, в том числе через ООН. Информационные средства упоминаются здесь большей частью в контексте борьбы с терроризмом.

Отдельный раздел Концепции, пусть и всего из трех пунктов, посвящен такому важному вопросу, как информационное сопровождение внешнеполитической деятельности РФ. В нем говорится об использовании Россией ИКТ для обеспечения информационной безопасности, влияния на общественное мнение за рубежом, усиления российских СМИ, обеспечение доступа каждого человека к объективной информации.

Основываясь на этих документах, можно обозначить некоторые черты, присущие информационной политике России:

- явный акцент на обеспечение безопасности, защиты от внешних и внутренних угроз как для критической информационной инфраструктуры, так и для информационного поля;

- предусматривается возможность использования инструментов информационной политики для достижения внешнеполитических целей;

- информационная политика носит стратегический характер и увязывается с национальными интересами;

- в качестве одной из целей стоит повышения имиджа России за рубежом;

---

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=191669&fld=134&dst=1000000001,0&rnd=0.07402217045154613#05568460818294072 (дата обращения: 15.02.2020)

[16] Концепция внешней политики РФ, утверждена Президентом Российской Федерации В.В. Путиным 30 ноября 2016 г. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2542248 (дата обращения: 15.02.2020)

- на стратегическом уровне рассматриваются как развитие информационной инфраструктуры, так и контроль за информационным полем, то есть в целом стратегия информационной политики многогранна;

- вместе с тем концептуальные основы информационной политики недостаточно глубоко разработаны, актуализация происходит редко, в повестке дня информационные инструменты рассматриваются только как инструмент направленного влияния.

Понятие информационной политики не столь популярно в европейском дискурсе. Информационная составляющая видится присущей любой проводимой политике. Информационная политика рассматривается в качестве связей с общественностью в более широком понимании. Михаэль Брюггеманн использует термин «информационная политика» применительно к средствам и целям информирования и коммуникации политического института (в частности – Европейской комиссии). Он выделяет в ней три элемента: первый касается прав и конкретных вопросов доступа к информации и документам, иначе говоря, прозрачность; второй – профессиональные связи с общественностью, что может порой осуществляться через PR агентства; третий – политическая риторика, коммуникативная деятельность политиков. Все это, вместе взятое, образует информационную политику института[17].

Что касается внутренней информационной политики ЕС, зафиксированной в официальных документах, то акцент обычно делается на аудиовизуальной сфере как части единого цифрового рынка[18].

Статья 167 Договора о Европейском союзе предполагает поддержку сотрудничества стран-членов в следующих вопросах:

- продвижение знаний и распространение истории и культуры европейских народов;

- сохранение культурного наследия европейского значения;

- некоммерческие культурные обмены;

- поддержка изобразительного и литературного творчества, включая аудиовизуальный сектор[19].

Под аудиовизуальными медиа услугами в Директиве по аудиовизуальным медиа услугам понимаются услуги, предоставляемые поставщиком с целью информирования, развлечения или образования широкой публики посредством электронных

[17] Brüggemann, M. How the EU constructs the European Public Sphere: Seven strategies of information policy // Javnost. - 2005 №12 (2), pp. 57-74.

[18] Ibrus, I. The EU Digital Single Market as a mission impossible: Audio-visual policy conflicts for Estonia // International Journal of Digital Television. – 2016 vol.7 №1. pp.23-28

[19] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Charter of Fundamental Rights of the European Union URL: https://europa.eu/european-union/sites/europaeu/files/eu_citizenship/consolidated-treaties_en.pdf#nameddest=article167 (дата обращения: 15.02.2020)

коммуникационных сетей. Различают традиционные аудиовизуальные услуги (телевидение) и услуги по запросу (программы по выбору потребителя в данный момент)[20].

В Директиве ставятся следующие цели:

- создание одинаковых условий в странах-членах для развития аудиовизуальных медиа;

- защита детей и потребителей;

- сохранение медиаплюрализма;

- борьба с ненавистью на почве расовых и религиозных различий;

- сохранение культурного разнообразия;

- независимость национальных медиа-ресурсов[21].

С 2006 года функционирует Исполнительное агентство Европейской комиссии по образованию, культуре и аудиовизуальным материалам (the Education, Audiovisual and Culture Executive Agency; EACEA). Оно отвечает за ряд программ в сфере образования, культуры, аудиовизуальных материалов, спорта, гражданства и волонтерства, включая программы «Creative Europe» и «Erasmus+»[22].

И для России, и для Европейского союза информационная безопасность является важной составляющей информационной политики. Союз в этом неплохо преуспел. Одним из наиболее ранних и важных документов, определяющих основы информационной безопасности, было Сообщение «Сетевая и информационная безопасность: предложения для подхода европейской политики»[23] 2001 года. В нем понятие сетевой и информационной безопасности определено как «способность сети или информационной системы противостоять с определенным уровнем стойкости случайным событиям или намеренным действиям, которые угрожают доступности, подлинности, целостности или конфиденциальности хранящейся или передаваемой информации и связанным с ними служб, к которым может быть осуществлен доступ с помощью этих сетей и систем».

В Сообщении указывалось, что оно является первым шагом на пути к обеспечению информационной безопасности в ЕС. В нем представлен ряд предложений по ответу на

[20] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance) URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013 (дата обращения: 15.02.2020)

[21] Audiovisual and Media // Official website of the European Union URL: https://europa.eu/european-union/topics/audiovisual-media_en (дата обращения: 15.02.2020)

[22] About EACEA, European Commission website URL: https://eacea.ec.europa.eu/about-eacea_en (дата обращения: 15.02.2020)

[23] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions “Network and Information Security: Proposal for a European Policy Approach” Brussels, 6.6.2001 URL: https://www.steptoe.com/images/content/4/8/v1/485/811.pdf] (дата обращения: 15.02.2020)

различные угрозы: перехват информации, неавторизованный доступ к компьютерным сетям, нарушение работы сетей, использование вредоносного ПО и его маскировка, природные катаклизмы и непреднамеренные действия.

В 2001 году был принят Регламент о защите прав граждан при обработке персональных данных институтами и органами Сообщества и свободном обращении таких данных[24]. В нем среди прочего учреждалась должность Европейского наблюдателя по защите данных, который назначается на пятилетний срок.

Директива 2002 года о частной жизни и электронных коммуникациях[25] затрагивает обеспечение равного уровня среди стран-членов по защите персональных данных в секторе электронных коммуникаций. Она также стала одним из первых основных документов в системе информационной безопасности.

Важным этапом в формировании европейской системы информационной безопасности было издание в 2006 году Сообщения Европейской комиссии «Стратегия безопасности информационного общества «Диалог, партнерство и расширение возможностей»[26]. В Стратегии обозначена важность создания единого европейского информационного пространства. Она является продолжением политики, обозначенной в Сообщении 2001 года, и охватывает три направления: специфические меры по защите сети и информации, нормативное регулирование электронных коммуникаций, борьба с киберпреступлениями.

С целью повышения защищенности критической инфраструктуры, в 2009 году Европейская комиссия издает Сообщение «Защита Европы от крупномасштабных кибератак и сбоев: повышение готовности, безопасности и устойчивости»[27].

---

[24] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data URL: https://edps.europa.eu/sites/edp/files/publication/reg_45-2001_en.pdf (дата обращения: 20.02.2020)

[25] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058 (дата обращения: 20.02.2020)

[26] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. A strategy for a secure Information Society “Dialogue, partnership and empowerment”. Brussels, 31.52006. COM(2006) 251 final. URL: http://ec.europa.eu/information_society/doc/com2006251.pdf (дата обращения: 20.02.2020)

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400} URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0149 (дата обращения: 20.02.2020)

Среди учреждений, призванных бороться с киберпреступлениями, необходимо также отметить Европейский центр киберпреступлений, созданный в 2013 году и входящий в структуру Европола (ЕС 3) [28].

Здесь также нельзя не упомянуть Общий Регламент по защите информации (GDPR), принятый 27 апреля 2016 года и вступивший в силу 25 мая 2017 года[29].

Регламент касается как европейских организаций, так и тех, что взаимодействуют с ними. Он пришел на смену Директиве о защите людей в вопросе обработки и передачи личной информации 1995 года[30], которая уже не соответствовала современным требованиям и не смогла предотвратить фрагментации в процессе защиты информации в Союзе: уровень защиты такой информации разнился по странам-членам. Регламент определяет единые правила по работе с личной информацией, ее обработке и передаче.

Итак, можно назвать основные черты информационной политики ЕС:

- стремление обеспечить безопасность личных данных пользователей;
- обеспечение информационной инфраструктуры совместными усилиями;
- учреждение специальных экспертных органов на наднациональном уровне;
- акцент на информационной безопасности, а не формировании имиджа или повышении «мягкой силы».

Можно сделать вывод о том, что в сравнении с Россией Европейский союз нигде не фиксирует стремление к оказанию внешнего влияния. Внешняя информационная политика может сводиться к деятельности в сфере цифровой политики с целью поддержки демократии за границами ЕС или участию в разработке международных соглашений по защите данных. Возможно использование инструментов вроде распространения информации по возможностям обхода блокировки онлайн-ресурсов государством или поддержки активистов и их обучение в навыках работы с цифровой информацией и кибербезопасности[31]. Однако, судя по официальным документам, во внешней политике нет нарратива по достижению каких-то целей информационными средствами, если не говорить о безопасности. Единственное, что можно отметить в этой связи, — это Резолюция

[28] About European Cybercrime Centre – EC3 // Europol website URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата обращения: 20.02.2020)
[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525205207301&uri=CELEX:32016R0679 (дата обращения: 27.02.2020)
[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (дата обращения: 27.02.2020)
[31] Łukasz Antoni Król Digital foreign policy: how digital tools can further Europe's foreign policy goals // European View (2016) 15:133-144

Европарламента 2012 года о стратегии цифровой свободы во внешней политике ЕС[32], которая призывает Еврокомиссию как можно скорее разработать такую стратегию. Резолюция обозначила стремление союза к поддержке цифровой свободы в третьих странах.

Информационная политика Европейского союза большей частью на протяжении всего существования этого направления касается киберсферы. Внутренняя информационная политика сводится к регулированию медиапродукции. Союз не ставит цели защиты информационно-психологической сферы, как это делает Россия, и не делает серьезных шагов по формированию европейской идентичности через инфополе. В этой сфере Европейский союз лишь пытается защититься от fake news посредством их разоблачения и дискредитации информационных ресурсов.

В последнее время в целях повышения безопасности Европейский союз все больше усилий вкладывает в развитие стратегических коммуникаций для борьбы с гибридными угрозами, то есть борьбу с дезинформацией. Кибербезопасность получила больший акцент на защите европейских выборов от иностранного вмешательства.

Таким образом, Европейский союз может быть приравнен к государству в отношениях по вопросу информационной политики, поскольку:

- имеет собственную информационную инфраструктуру;
- проводит стратегическое планирования в информационной сфере;
- обладает информационным суверенитетом;
- стремится защититься от информационных угроз и имеет соответствующие учреждения.

§1.3 Приоритеты информационной политики в рамках общей европейской внешней политики

Общая европейская внешняя политика (ОЕВП) – инструмент выработки общего внешнеполитического курса всего ЕС. Для принятия важных решений в сфере внешней политики необходимо единогласие всех стран-членов ЕС. При этом важно учитывать, что такая политика не заменяет национальные политики европейских стран. Европейский союз – не государство, он не отменяет существования суверенных стран с их собственной политикой. Это отдельное наднациональное образование, необходимое для защиты общих

[32] European Parliament resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI)) // URL: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0470&language=EN (дата обращения: 27.02.2020)

интересов стран-членов. Евроинтеграция с передачей части суверенитета странами на наднациональный уровень происходит лишь в той мере, которая будет рациональна для всех стран-членов. В случае с информационной политикой они будут влиять друг на друга. Специфической внешней информационной политики у Европейского союза нет: она может быть выражена в «мягкой силе» или ответе на угрозы. Современная информационная политика может носить оборонительный характер в отношении внешних гибридных угроз.

Внешняя информационная политика не ставит перед собой масштабных целей. Тем не менее, союз выступает в качестве актора в международной информационной среде, уже хотя бы учитывая его разоблачения fake news в зарубежных источниках. Более того, общеевропейские СМИ, ведущие вещание на зарубежье, подчиняются европейской информационной политике. Информационная политика Европейского союза и ОЕВП согласованы в слабой мере. Интеграция в этих сферах будет возможной только в том случае, если страны члены сочтут это рациональным. В скором времени не предвидится значительных интеграционных скачков, однако восприятие угрозы извне может повлиять на этот узкий сегмент европейской политики. Здесь затронута важная категория, требующая рассмотрения – внешняя информационная политика. Она объединяет действия, находящиеся на стыке информационной и внешней политики.

Внешняя информационная политика служит для достижения внешнеполитических целей через воздействие на зарубежное общество информационными средствами. Среди таких целей могут быть создание положительного имиджа собственной страны, формирование негативного отношения зарубежной общественности к собственному правительству, дестабилизация политической обстановки, оказание международного давления, обеспечение поддержки собственной позиции на международной арене, проведение кибератак с целью получения информации или дезорганизации работы информационных систем и др. Так к средствам внешней информационной политики может быть отнесено информационное противодействие/противоборство, а также обеспечение информационной защиты от внешних угроз. Следует отметить, что при оговоренной самостоятельности Европейского союза как субъекта информационной политики к нему будут применимы те же утверждения, что справедливы для государства. В данной работе к внешним информационным действиям относятся как действия в содержательной сфере, так и в отношении информационных систем. Информационные системы можно определить как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[33]. Эти действия разумно включить в

[33] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 10.03.2020)

понятие внешней информационной политики, если рассуждать и от обратного: Европейский союз проводит единую политику в обеспечении защиты от атак на сети и информационные системы[34]. Сетевую и информационную безопасность определяют как способность сети или информационной системы противостоять с высоким уровнем надежности случайным событиям или умышленным действиям, которые угрожают доступности, аутентичности, целостности или конфиденциальности хранимой или передаваемой информации и связанным с ней сервисам, к которым можно получить доступ с помощью этих сетей или информации[35]. При этом подразумеваются угрозы как внутренние, так и внешние.

Информационная безопасность представляется существенной составляющей информационной политики. Ее следует понимать в двух плоскостях: во-первых, информационная безопасность заключается в защищенности информационной среды, при которой она нормально функционирует; во-вторых, защищенность национальных интересов в информационной сфере (интересы государства, личности, общества). Основополагающая задача государства в информационной сфере в этом смысле – соблюдение конституционных прав человека и гражданина[36]. Если опустить здесь национальный аспект, то такое определение будет применимо и к образованию вроде Европейского союза, причем будут соблюдены все те же принципы и задачи, присущие государству: обеспечение соблюдения прав и свобод собственного населения, защита от внешнего вмешательства и др.

Внешняя политика субъекта может строиться в русле сотрудничества, агрессии, противодействия, защиты и т.д. Если говорить о негативных проявлениях международного взаимодействия, то среди них следует назвать информационное противоборство, информационную войну и информационную безопасность. Последнее мы отнесли к этой категории, поскольку оно является ответом субъекта в информационном пространстве на возникающие угрозы, которые были перечислены выше.

---

[34] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524931018994&uri=CELEX:32013L0040 (дата обращения: 10.03.2020)

[35] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions “Network and Information Security: Proposal for a European Policy Approach” Brussels, 6.6.2001 URL: https://www.steptoe.com/images/content/4/8/v1/485/811.pdf (дата обращения: 10.03.2020)

[36] Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В.Б. Вепринцев, А.В. Манойло, А.И. Петренко, Д.Б. Фролов; под ред. А.И. Петренко. – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2011. – 495с.

О деятельности Европейского союза как актора в дипломатических отношениях свидетельствует обширная сеть зарубежных представительств. Представительства есть более чем в 140 странах и организациях по всему миру[37].

ОЕВП начала свое существование лишь с 1993 года, когда вступил в силу Маастрихтский договор о Европейском союзе. Тем не менее, говорить о проведении единой политики безопасности в принципе уместно в отношении еще Западноевропейского союза (ЗЕС) (до 1954 года - Западного союза). Учреждение этой организации иллюстрирует то, что непосредственным стимулом к началу процесса европейской интеграции в послевоенное время был вопрос обеспечения безопасности и недопущения новых конфликтов. Возникла необходимость проведения общей оборонной политики. Однако это не исключает важности экономической составляющей, выраженной в критической необходимости восстановления Европы после опустошительной войны, что было в большей степени выражено в заключении договора о Европейском объединении угля и стали, носившем больше черт, присущих Европейскому экономическому сообществу и Европейскому союзу.

Западный союз – военно-политическая организация, созданная в 1948 году для проведения совместной согласованной оборонной политики европейскими государствами. Он ставил перед собой следующие основные цели: создать устойчивую основу для экономического восстановления Западной Европы; оказывать взаимную помощь странам-членам в противодействии любой агрессии извне; продвигать единство и поддерживать позитивную интеграцию в Европе[38]. Впоследствии Западный союз должен был стать главным инструментом проведения общей политики безопасности[39]. Интересно отметить, что началом европейской интеграции принято считать создание сообщества экономического характера – Европейского объединения угля и стали, что позже привело к интеграции в политической сфере. Дата оглашения декларации Шумана до сих пор отмечается как День Европы. Что важно, для обоих случаев причиной (в одном случае – основной, в другом – неотъемлемой) послужила проблема безопасности. Судить об этом можно из Декларации Шумана: «Чтобы мир мог быть обеспечен, необходимо, чтобы существовала Европа… Установленные таким образом совместные производственные связи будут означать, что любая война между Францией и Германией отныне станет не

[37] EU in the World // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/area/geo_en (дата обращения: 20.03.2020)
[38] Shaping of a Common Security and Defence Policy // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/5388/shaping-common-security-and-defence-policy_en (дата обращения: 20.03.2020)
[39] Авдеенко Е.Г. От Маастрихта к Амстердаму: стратегия ФРГ в области общей внешней политики, безопасности и обороне в Европе // Вестник Челябинского Государственного Университета №22 (237) 2011 стр112-121

только немыслимой, но и практически невозможной»[40]. Это заявление отражает наиболее насущную на тот момент для европейцев проблему – недопущение новых войн.

Западный союз был непосредственно следствием восприятия реальной угрозы со стороны Германии европейскими государствами – Францией и Великобританией. Еще в марте 1947 года их представители подписали в Дюнкерке военный союз. Примечателен он тем, что явился точкой отсчета для интеграции в сфере безопасности в Европе. На основе Дюнкеркского договора в 1948 году был создан Западный союз (Брюссельский пакт), в который вошли страны Бенилюкса, Великобритания и Франция. Впоследствии часть членов Пакта вошла и в НАТО. Тем не менее, союз продолжил свое существование, что явилось проявлением недоверия европейских стран к США и неуверенности в том, что они будут готовы пойти против ядерной державы – СССР. Наличие собственного оборонительного потенциала должно было гарантировать защищенность, обеспеченную европейцами и в интересах европейцев. В 1954 году было подписано Парижское соглашение, расширявшее Западный союз и переименовавшее его в Западноевропейский союз. В 1957 году ЗЕС оказался в непосредственном подчинении НАТО, так что, по сути, он сохранил лишь номинальные функции, ведь он даже не имел собственного контингента войск, но лишь сводился к наложению оборонных обязательств на стран-участниц[41].

Впоследствии это образование стало связующим звеном между Европейским сообществом и НАТО. В 1987 году в Гааге на сессии Совета министров ЗЕС был принят документ «Платформа по проблемам европейской безопасности», который и был посвящен согласованию европейской политики безопасности с общей политикой безопасности НАТО.

После подписания Лиссабонского договора все функции ЗЕС были включены в сферу деятельности ЕС, в 2011 году ЗЕС перестал существовать.

Это позволяет нам утверждать, что европейское объединение началось вследствие возникновение общей повестки безопасности. В то время Европа стремилась избавиться от внутренних угроз. Как опасность послужила стимулом к объединению, так она может послужить и теперь для углубления интеграции в сфере общей оборонительной политики, которая «перельется» и на внешнюю политику, и на информационную политику, и на прочие сферы.

---

[40]Декларация от 9 мая 1950 года, оглашенная Робером Шуманом, министром иностранных дел, в Париже, на Кэ д'Орсэ в салоне часов // История европейской интеграции. Хрестоматия в 3-х частях. Ч 1. История Европейских сообществ Составители: Браницкий А.Г., Леушкин Д.В. – Н. Новгород: Нижегородский госуниверситет, 2014 стр9-12

[41] Лобанов Р.О. Динамика взаимоотношений Западноевропейского союза и НАТО по вопросам военно-политической безопасности Европы в 1954-2002 гг // Локус: люди, общество, культуры, смыслы №4 2012 стр74-85

Согласно Договору о Европейском союзе, Основные направления ОЕВП определяются Европейским советом и Советом Европейского союза, которые принимают единогласные решения. Рассматривая Маастрихтский договор с изменениями, внесенными согласно Амстердамскому договору, Верховный представитель по иностранным делам и политике безопасности обеспечивает претворение в жизнь принятых решений и представляет союз на мировой арене.

Во внешней политике Европейский союз как наднациональное формирование определяет общие ориентиры, принимает решения по действиям и позиции, устанавливает порядок реализации решений, а также укрепляет сотрудничество государств-членов в проведении общей внешней политики.

Европейским советом определяются стратегические интересы, цели и общие ориентиры.

Совет Европейского союза непосредственно разрабатывает политику и принимает необходимые решения на основании ориентиров, определенных Европейским советом.

Согласование любого вопроса по общей внешней политике и политике безопасности, представляющего общий интерес, осуществляется в рамках Европейского совета и Совета Европейского союза[42].

В соответствии с Ниццким договором 2000 года Европейским советом был учрежден ряд органов для более эффективного осуществления общей политики безопасности и обороны. Среди них Комитет по политическим вопросам и вопросам безопасности, Военный комитет, Комитет по гражданским вопросам и управлению кризисами, Политико-военная группа, Директорат по управлению кризисами и планированию, Военный штаб, Отдел гражданского планирования и управления, Европейское оборонное агентство, Колледж европейской безопасности и обороны, Институт по исследованиям в сфере безопасности, Спутниковый центр, Центр операций[43]. Вместе с тем в рамках Совета существует Европейское оборонное агентство, выявляющее оперативные потребности и участвующее в разработке европейской политики в отношении потенциалов и вооружений.

В 2004 году было создано Агентство по управлению и оперативному взаимодействию на внешних границах стран-членов Европейского союза (Фронтекс). В 2016 году его заменило Агентство по охране границ и береговой линии (также Фронтекс).

---

[42] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Charter of Fundamental Rights of the European Union URL: https://europa.eu/european-union/sites/europaeu/files/eu_citizenship/consolidated-treaties_en.pdf#nameddest=article167 (дата обращения: 15.02.2020)

[43] CSDP structure, instruments and agencies // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/5392/csdp-structure-instruments-and-agencies_en (дата обращения: 20.03.2020)

В соответствии с Лиссабонским договором действует Европейская служба внешнего действия. Ее главная задача – усиление взаимодействия с национальными парламентами стран-членов в сфере внешнего действия и в особенности в сфере внешней политики и обороны[44].

В целом в сфере единой внешней политики, согласно Маастрихтскому договору, союз ставит перед собой следующие задачи:

1) защита своих ценностей, основных интересов, укрепление безопасности, независимости и целостности;

2) укрепление и поддержание демократии, верховенства права, прав человека и принципов международного права;

3) сохранение мира, предотвращение конфликтов и укрепление международной безопасности;

4) поддержка развивающихся стран;

5) поддержание интеграции всех стран в мировую экономику, включая такой метод, как запрещение наложения ограничений в международной торговле;

6) сохранение экологии, обеспечение устойчивого развития;

7) помощь странам, пострадавшим от бедствий;

8) продвижение международной системы, основанной на многостороннем взаимодействии и глобальном управлении.

Внешняя информационная политика связана с политикой по ответу на гибридные угрозы. Так, Центр по анализу гибридных угроз, созданный в 2016 году в структуре Европейской службы внешнего действия, ведет мониторинг открытой и закрытой информации о возможных угрозах, в том числе касающихся киберсферы и стратегических коммуникаций[45].

Из этого видно, что Европейский союз имеет развитую дипломатическую и оборонную системы, позволяющие эффективно осуществлять внешнюю политику и политику безопасности и рассматривать его в качестве самостоятельного актора в международных отношениях. Соответственно, союз предстает и единым актором, ответственным за действия в информационном пространстве. Стоит учитывать и то, что такие страны, как США расценивают кибератаки на критическую информационную

[44] European Parliament legislative resolution of 8 July 2010 on proposal for a Council decision establishing the organization and functioning of the European External Action Service // URL: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0280&language=EN&ring=A7-2010-0228 (дата обращения: 30.03.2020)

[45] Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats, a European Union response // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата обращения: 12.04.2020)

инфраструктуру как военную агрессию. ЕС практикует лишь оборонительные действия в цифровом пространстве. Так или иначе, Европейский союз обладает потенциалом для проведения операций в цифровой среде.

Глава 2

Практические аспекты современной информационной политики Европейского союза

§2.1 Развитие информационной политики в документах и учреждениях Европейского союза

В данном разделе Европейский союз рассматривается в качестве самостоятельного актора в проведении информационной политики, обладающим некоторыми признаками информационного суверенитета. Европейский союз имеет собственное регулируемое информационное пространство. Его наполнение в основном состоит из контента национальных СМИ, работающих, в том числе, в общеевропейских масштабах, а также материалов в соцсетях. Однако, помимо регулирования информационного пространства в рамках единой аудиовизуальной политики, Европейский союз осуществляет меры в информационном пространстве с целью поддержания безопасности своих граждан и либеральных демократических устоев. Это касается как деятельности террористических организаций, так и третьих стран и внутренних субъектов. В информационной политике последних нескольких лет основное место занимали угрозы со стороны других стран и внутренних политических сил.

Наибольший интерес для исследования представляет политика кибербезопасности и борьба с дезинформацией. За последние пять лет именно этот сегмент информационной политики Европейского союза развивался наиболее интенсивно, что во многом связано с настороженным восприятием внешней информационной политики России и ростом международной напряженности вокруг Украинского кризиса. Согласно опросам, проведенным Европейской комиссией в 2017-208 годах, 85 процентов европейцев считают, что фейковые новости являются в их стране актуальной проблемой, а 68 процентов признались, что по крайней мере раз в неделю сталкиваются с ложными сообщениями[46].

На повестке долгое время был вопрос возможного вмешательства в европейские выборы в 2019 году[47]. В частности, в число мер, призванных защитить выборы, вошли защита персональных данных, прозрачность предвыборных онлайн-кампаний, кибербезопасность, укрепление европейского сотрудничества и обеспечение надлежащих

[46] Fact Sheet on Tackling the Spread of Disinformation Online // URL: https://ec.europa.eu/digital-single-market/en/news/factsheet-tackling-online-disinformation (дата обращения: 30.03.2020)

[47] 10 ways the EU is fighting disinformation, Medium website, author European Commission // URL: https://medium.com/@EuropeanCommission/10-ways-the-eu-is-fighting-disinformation-f07fca60e918 (дата обращения: 30.03.2020)

санкционных мер для политических партий. Эти положения опираются на основные на сегодняшний день регулирующие документы в сфере онлайн-безопасности, вступившие в силу в 2018 году, среди которых Общий регламент о защите персональных данных и Свод правил[48]. Стоит отметить, что Европейская комиссия в значительной мере опирается на гражданское общество в вопросах контроля за информационной сферой, что проявляется в опросах, регулярном информировании и поддержке негосударственных наблюдательных центров.

Для защиты выборов Европейское агентство по кибербезопасности (ENISA) издало руководство для стран-членов по обеспечению надлежащего уровня технической безопасности. Руководство имеет рекомендательный характер и разбирает реальные кейсы небезопасности электоральных систем[49]. Такая политика была спровоцирована, в том числе, сообщениями о вмешательстве в президентские выборы в США 2016 года со стороны России, а также в выборы во Франции в 2017 году. Под «вмешательством» Европейская комиссия подразумевает ряд действий: от взлома почтовых ящиков и обрушения веб-сайтов посредством DDoS атак до вмешательства в электоральные системы и финансирование политических сил[50].

ENISA является основным ведомством в Европейском союзе, занимающимся вопросами киберезопасности, причем как в технической части, так и в вопросах координации сил и средств и информирования населения[51]. Оно было учреждено регламентом от 10 марта 2004 года[52]. Агентство было создано с целью повышения способности ЕС предотвращать угрозы информационной безопасности и отвечать на случаи нападения в цифровой среде. По численности – одно из наиболее малых агентств ЕС. Сейчас оно позиционирует себя как центр обеспечения кибербезопасности в Европе[53]. Учредительный Регламент от 2004 года был дополнен Регламентом 2013 года[54]. В соответствии с ним, перед агентством стоят цели:

---

[48] Free and fair European elections, State of the Union, European Commission, 12 September 2018 // URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf (дата обращения: 30.03.2020)

[49] Compendium on Cyber Security of Election Technology, NIS Cooperation Group July 2018 // URL: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf (дата обращения: 30.03.2020)

[50] Joanna Świątkowska European Cybersecurity Journal, volume 3 (2017), issue 3 // URL https://www.ria.ee/sites/default/files/content-editors/kuberturve/ecj_volume3.issue3_extract_past.pdf

[51] About ENISA, European Union Agency for Cybersecurity website // URL: https://www.enisa.europa.eu/about-enisa (дата обращения: 30.03.2020)

[52]European Commission, Evaluation of the EU decentralised agencies in 2009 Volume III – Individual Agencies URL: https://europa.eu/european-union/sites/europaeu/files/docs/body/agency_level_findings_en.pdf (дата обращения: 30.03.2020)

[54] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 URL: https://ccdcoe.org/sites/default/files/documents/EU-130521-ENISA.pdf (дата обращения: 30.03.2020)

1) Поддержание высокого экспертного уровня;

2) Содействие органам ЕС в формировании политики в отношении сетевой и информационной безопасности;

3) Содействие органам и странам-членам ЕС в проведении политики, необходимой для соответствия требованиям к сетевой и информационной безопасности в рамках европейского законодательства;

4) Содействие ЕС и странам-членам в повышении способности и готовности к предотвращению, распознаванию и ответу на проблемы и инциденты, связанные с информационной безопасностью;

5) Широкое взаимодействие с представителями публичного и частного сектора.

С 2010 года ENISA организует каждые два года общеевропейские учения Кибер Европа (Cyber Europe), которые проводятся в рамках Европейского союза и ЕАСТ. В ходе учений отрабатывается разрешение инцидентов в киберпространстве, затрагивающих публичный и частный сектор[55].

East StratCom является основной организацией в структуре институтов Европейского союза, противодействующим российской внешней информационной политике и вообще зарубежной дезинформации. Группа упоминается в различных документах, в том числе в резолюции по противодействию пропаганде третьих сторон[56]. В той же резолюции среди основных источников пропаганды и дезинформации отмечены российские учреждения и СМИ: Спутник, Россотрудничество, Русский мир и проправительственные СМИ.

Подразделение восточных стратегических коммуникаций призвано способствовать усилиям ЕС в сфере публичной дипломатии, внешнеполитической деятельности и политики безопасности. Создано оно было изначально только для опровержения дезинформации из России. Со временем StratCom стал также организацией, продвигающей коммуникации Европейского союза в странах Восточного партнерства и поддерживающей независимые СМИ. Восточная политика, урегулирование украинского кризиса и финансовая поддержка украинских реформ в 2015 году уже входили в число приоритетных внешнеполитических задач Европейской комиссии. С этим связано и начало активной борьбы с Российской дезинформацией[57]. Среди основных инструментов – взаимодействие

[55] ENISA meets cyber-experts to plan Cyber Europe 2018 // ENISA website https://www.enisa.europa.eu/news/enisa-news/enisa-meets-cyber-experts-to-plan-cyber-europe-2018 (дата обращения: 30.03.2020)

[56] European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)) // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584441630054&uri=CELEX:52016IP0441 (дата обращения: 02.04.2020)

[57] Conclusions – 19 and 20 March 2015, European Council // URL: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf (дата обращения: 02.04.2020)

с прессой, коммуникации в сети, доклады, статьи, аудиовизуальные материалы[58]. StratCom также осуществляет мониторинг российский проправительственных СМИ и издает при необходимости опровержения, систематизируя все случаи. Подготовленная ими информация широко цитируется. Так, среди ссылающихся на них СМИ - El Pais, Welt, Zeit, Independent, The Guardian, USA Today и др[59].

В марте 2015 года Еврокомиссия поручила Высокому представителю подготовить план действий по стратегическим коммуникациям – создание такой группы должно было стать первым шагом в борьбе с дезинформацией со стороны России[60].

План был подготовлен в июне 2015 года. Он определил основные направления деятельности для StratCom:

1) Повышение потенциала ЕС в стратегических коммуникациях;

2) Работа с партнерами и расширение сетей взаимодействия;

3) Коммуникационная деятельность по программам ЕС, проекты и деятельность в направлении стран Восточного партнерства;

4) Поддержание свободы СМИ и свободы выражения мнений;

5) Инициативы публичной дипломатии;

6) Развитие потенциала журналистов и медиа-акторов;

7) Поддержка плюрализма в русскоязычном медиапространстве;

8) Работа с гражданским обществом;

9) Повышение осведомленности, развитие критического мышления и продвижение медиаграмотности;

10) Укрепление взаимодействия между странами-членами по законодательному регулированию медиапространства[61].

В октябре 2019 года был подведен промежуточный итог эффективности ведомства. Согласно подсчетам, группа издала более 6500 случаев опровержения новостей на более чем 20 языках[62].

---

[58] Strategic Communications // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en (дата обращения: 02.04.2020)

[59] In the media // EUvsDisinfo website URL: https://euvsdisinfo.eu/in-the-media/

[60] European Council meeting (19 and 20 March 2015) – Conclusions URL: https://www.eesc.europa.eu/resources/docs/european-council-conclusions-19-20-march-2015-en.pdf (дата обращения: 02.04.2020)

[61] East StratCom Team. «Action Plan on Strategic Communication» URL: http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf (дата обращения: 02.04.2020)

[62] EUvsDisinfo: how to debunk over 6,500 disinformation cases in four years? // European Union External Action website URL: https://eeas.europa.eu/topics/countering-disinformation/68633/euvsdisinfo-how-debunk-over-6500-disinformation-cases-four-years_en (дата обращения: 12.04.2020)

Следующим шагом в обновлении системы информационной безопасности стала подготовка и публикация в Европейской комиссией в апреле 2016 года Совместного плана по отражению гибридных атак[63].

Как отмечается в документе, обстановка в странах Восточного и Южного партнерства создала новые угрозы, в разрешении которых Европейский союз должен выступить посредником. План опирается на изданную еще в 2013 году – до кризиса – Стратегию кибербезопасности, которая определила такие приоритеты, как повышение уровня устойчивости киберсферы, устранение киберпреступности, разработка стратегии цифровой безопасности с опорой на Общую политику безопасности и обороны, улучшение цифровой инфраструктуры, продвижение европейских ценностей[64]. Более современные стратегии делают больший акцент на онлайн сфере и социальных сетях. Так, в плане 2016 года по противодействию гибридным угрозам[65] в разделе стратегических коммуникаций упоминаются таргетированные кампании, направленные на социальную дестабилизацию. В документе присутствует и другой важный нарратив – создание системы мониторинга за сообщениями в сети. В части кибербезопасности план рекомендует углубить сотрудничество в работе групп по противодействию угрозам компьютерной безопасности (Computer security incident response team; CSIRTs), которые были созданы в соответствии с Директивой 2016 года о мерах по повышению уровня сетевой и информационной безопасности в Союзе[66]. В соответствии с той же Директивой была создана Группа взаимодействия по безопасности сети и информации, которая призвана координировать действия в киберсфере между странами, в том числе работу CSIRTs, способствовать обмену информацией, и которая состоит из представителей соответствующих министерств[67].

В соответствии с планом был впоследствии создан Центр передовых технологий по борьбе с гибридными угрозами, который тесно сотрудничает с НАТО. Необходимость такого сотрудничества даже обозначена в плане отдельно.

---

[63] Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats, a European Union response // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата обращения: 12.04.2020)

[64] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 (дата обращения: 12.04.2020)

[65] Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats a European Union response // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018 (дата обращения: 12.04.2020)

[66] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1521461913374&uri=CELEX:32016L1148 (дата обращения: 03.05.2020)

[67] NIS Cooperation Group, European Commission website // URL: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group (дата обращения: 03.05.2020)

В целом, изучив документ, можно отметить два основных направления деятельности Европейского союза в современной информационной политике: стратегические коммуникации и борьба с дезинформацией с одной стороны, с другой – кибербезопасность.

Через два года, в апреле, было опубликовано Сообщение по борьбе с дезинформацией в Интернете[68]. Примечательно, что документ был подготовлен с опорой на собственные общественные опросы и исследования от Евробарометра.

В сообщении отмечается, что европейское население столкнулось с большим числом случаев дезинформации. В документе утверждается, что Интернет становится все более важным источником новостей, и вместе с тем в нем растет количество дезинформации от внутренних и внешних акторов, что противоречит демократическим устоям и лишает население возможности делать осознанный выбор. Дезинформация признается частью гибридной войны, упоминается возможность использования средств информационной войны в российской военной доктрине, а российские кампании в информационной среде рассматриваются в качестве основной угрозы. Среди других возможных последствий дезинформации – снижение доверия науке и эмпирическим доказательствам.

В преддверии европейских выборов был также принят другой значимый документ – Свод правил по борьбе с дезинформацией[69]. Это первый случай, когда представители бизнеса добровольно согласились принять стандарты саморегуляции для борьбы с дезинформацией. Свод призван осуществить задачи, поставленные в Сообщении 2018 года. Среди методов были приняты обеспечение прозрачности рекламных политических кампаний, закрытие фейковых аккаунтов, а также демонетизация для распространителей дезинформации. К Своду присоединились Facebook, Google, Twitter, Mozilla и другие платформы. Впоследствии участники представляли Европейской комиссии отчеты по выявленным случаям дезинформации и заблокированным аккаунтам.

Во исполнение положений Сообщения 2018 года при содействии Европейской комиссии был создан Наблюдательный центр за социальными сетями (SOMA), который является платформой по наблюдению за СМИ и выявлению дезинформации в помощь Европейской комиссии. Участником может стать любой человек или организация в ЕС, вовлеченные в проверку фактов на подлинность. Платформа предоставляет различные технологические инструменты и возможность обмениваться данными по случаям

[68] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (дата обращения: 03.05.2020)

[69] Code of Practice on Disinformation, European commission website // URL: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (дата обращения: 03.05.2020)

дезинформации. Организация ставит перед собой задачи мониторинга, просвещения, экспертных рекомендаций, оценки результатов и координации усилий[70].

Следующий шаг, который предприняла Европейская комиссия, стал наиболее важным с точки зрения стратегии в борьбе с дезинформацией. Этим шагом стало принятие Плана действий против дезинформации в декабре 2018 года[71]. План определял дезинформацию как достоверно ложную или искаженную информацию, которая создается и распространяется с целью экономической выгоды или намеренного введения в заблуждение общественности, способную нанести вред обществу. В угрожаемые объекты включены, в первую очередь, демократические процессы. План снова отмечает в качестве приоритета в обеспечении безопасности борьбу с гибридными угрозами, частью которой являются стратегические коммуникации. В этом же пункте по вопросу гибридной угрозы есть отсылка к химической атаке в Солсбери, что дает основания утверждать о многоуровневой политике безопасности против российской угрозы, учитывая и то, что План делает акцент на работе StratCom и Европейской службы внешнего действия в восточном направлении. В контексте гибридной войны дезинформационные кампании связаны с кибератаками и взломом компьютерных сетей.

В Плане признается, что впервые угроза дезинформации с российской стороны в онлайн-среде возникла в 2015 году. Хотя Европейская комиссия признает также, что так или иначе кампании дезинформации проводят более тридцати стран, Россия лидирует в этом направлении, позволяя всем остальным перенимать успешный опыт.

Согласно Плану, для борьбы с дезинформацией страны-члены и институты ЕС должны быть вовлечены в работу на разном уровне: борьба с гибридными угрозами, киберугрозами, осуществление разведки и стратегических коммуникаций, защита данных, безопасности выборов и работа со СМИ. В целом, предлагаемые Планом действия основаны на четырех опорах: повышение способности Европейского союза в обнаружении и опровержении дезинформации; укрепление способности совместного реагирования на угрозы; мобилизация частного сектора; информирование граждан и повышение устойчивости населения к угрозам. План предполагает проведение всех необходимых мер перед майскими выборами 2019 года.

[70] About Us, SOMA website // URL: https://www.disinfobservatory.org/about-us/ (дата обращения: 03.05.2020)
[71] Joint Communication to the European parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation // URL: https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation (дата обращения: 03.05.2020)

В феврале 2019 года Совет Европейского союза опубликовал решения, где отметил важность предотвращения киберугроз для обеспечения честных и прозрачных выборов[72]. Среди прочего, документ обращает внимание на важность проведения перед выборами Недели медиаграмотности. В качестве организаций-партнеров определены G7 и NATO.

В июне 2019 года, уже после выборов, был опубликован отчет по осуществлению Плана действий[73]. Документ стал итоговым для всего процесса перестройки системы стратегических коммуникаций и борьбы с дезинформацией в условиях европейских выборов.

В нем отмечается, что предпринятые перед европейскими выборами действия в борьбе с дезинформацией оказались успешными. С января по июнь Стратком выявил и опроверг 1000 случаев дезинформации, что более чем в два раза больше по сравнению с аналогичным периодом предыдущего года. Бюджет, выделенный Европейской службе внешнего действия на стратегические коммуникации, был увеличен вдвое, а штат расширяется. Хотя Стратком не выявил зарубежных дезинформационных кампаний, нацеленных на европейские выборы, в отчете указывается на продолжающуюся дезинформационную активность со стороны России.

В отчете упоминается созданная в марте 2019 года Система быстрого реагирования. Она призвана обеспечить оперативное взаимодействие с G7, НАТО и онлайн-платформами по случаям дезинформации. На настоящий момент она используется для выявления ложных сведений по теме коронавируса, распространямых в Интернете, среди которых неверные способы лечения, которые могут вызвать тяжелые последствия для здоровья[74].

Согласно отчету, Google предпринял действия в отношении более чем 130 000 европейских аккаунтов, которые нарушили правила размещения рекламы. Facebook сообщил о 1,2 млн случаев нарушения правил размещения рекламы и контента и заблокировал 2,2 миллиарда фейковых аккаунтов, а также препятствовал работе полутора тысяч неевропейских и 658 европейских страниц, групп и аккаунтов, нацеленных на европейских граждан, и принял меры по повышению прозрачности рекламных кампаний. Twitter отклонил более 16000 рекламных объявлений, нацеленных на граждан Европейского союза.

---

[72] Conclusions of the Council and of the Member States on securing free and fair European elections // URL: https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf (дата обращения: 05.05.2020)

[73] Action Plan Against Disinformation, Report on Progress, June 2019 // URL: https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf (дата обращения: 05.05.2020)

[74] EU Rapid Alert System used amid coronavirus disinformation campaign, Euractiv website // URL: https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/ (дата обращения: 05.05.2020)

Среди прочих организаций, которым Европейский союз оказывает поддержку в борьбе с дезинформацией – SOMA и Международная сеть проверки фактов (International Fact-Checking Network), которая недавно запустила европейское отделение.

§2.2 Эффективность стратегических коммуникаций Европейского союза в информационном противостоянии

Европейскому союзу удалось выстроить обширный аппарат по информационной деятельности. Некоторые документы последних лет даже имеют стратегическое значение: План действий по борьбе с дезинформацией, Свод правил, План борьбы с гибридными угрозами. Были созданы новые учреждения межправительственного и неправительственного характера, способные проводить мероприятия по информационной защите в содержательной части: SOMA, RAS, Центр передовых технологий. StratCom удалось выявить огромное число фактов дезинформации. Европейский союз достиг главной цели – создать систему защиты европейских граждан и демократии от дезинформации. Тем не менее, результаты требуют критической оценки, поскольку представители бизнеса и органов Европейского союза в разной мере оценивают эффективность новой системы кооперации.

Фонд Карнеги проводит оценку мероприятий по борьбе с дезинформацией в рамках программы партнерства по противодействию кампаниям по оказанию влияния[75]. Исследования Фонда направлены на разработку предложений по информационной политике, изучение принципов операций по оказанию влияния и укрепление партнерства с правительственными и неправительственными учреждениями. В мае 2018 года, еще до выборов, Фонд опубликовал исследование о российском вмешательстве и европейском ответе на фейковые новости и кибератаки[76]. Оно исходило из того, что электоральную систему следует рассматривать в качестве критической инфраструктуры. В исследовании освещены пять случаев вмешательства России в выбор в европейских странах. Отмечается, что воздействие происходило на разных уровнях: формирование предпочтений избирателей, влияние непосредственно на процесс голосования и на явку избирателей. Объектами воздействия являются СМИ, социальные сети, базы данных, каналы передачи информации, организации и ответственные лица. Соответственно и система

[75] Partnership for Countering Influence Operations, Carnegie Endowment for International Peace website // URL: https://carnegieendowment.org/specialprojects/counteringinfluenceoperations
[76] Erik Brattberg, Tim Maurer Russian Election Interference, Europe's Counter to Fake News and Cyber Attacks // Carnegie Endowment for International Peace, May 2018 URL https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

кибербезопасности должна выстраиваться с участием правительственных и неправительственных организаций и нацеливаться на эти направления. Современная система информационной безопасности Европейского союза позволяет принимать такие меры без отказа от электронных носителей, как это было в Нидерландах в 2017 году.

В марте 2020 года Фонд Карнеги также выпустил исследование по эффективности Свода правил[77]. В нем сообщается, что Свод привел к неоднозначным результатам, так что не все участники остались ими довольны, а доверие между правительствами, предприятиями, гражданским и научным обществами не было выстроено.

Достигнутые положительные эффекты не требовали значительных усилий. Среди них – распознавание и сбор политической рекламы с данными о кампаниях; открытость данных; распознавание неточной информации; развитие практики проверки фактов; подготовка журналистов по программам коммерческих платформ; повышение медиаграмотности благодаря деятельности платформ.

По многим направлениям, тем не менее, прогресс был незначительный:

Различный подход к проверке рекламы – платформы по-разному определяют отношение рекламы к вопросам политики, выборов, социальным вопросам. Соответственно принимаются разные меры по проверке рекламы на достоверность и по ее запрету.

Подробность данных – хотя информация по политической рекламе архивируется, данные по ней недостаточно глубокие. Более того, в отчетах платформы не конкретизировали все категории рекламы, которую они запретили, поэтому нет возможности оценить эффективность мер: была реклама коммерческой или политической, сгенерированной автоматически или созданной людьми, связанной с Европой или нет.

Оценка эффекта от мер – проблема, присущая в целом информационной сфере. Европейская комиссия была недовольна результатами отчетов платформ, а платформы были недовольны критериями. Ни одна из сторон, включая страны-члены Европейского союза, не смогли предоставить показательные и исчерпывающие данные. Более того, неизвестно, какой эффект могло бы произвести какое-либо из заблокированных рекламных сообщений. С точки зрения борьбы с политической рекламой, нарушающей правила, как с проблемой самой по себе эти меры действенны и могут измеряться количественно. Нарушение правил – это, прежде всего, сокрытие источника финансирования. Проблема оценки касается в целом влияния и операций по влиянию, и контрмер.

[77] James Pamment The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission // Carnegie Endowment for International Peace March 2020 URL: https://carnegieendowment.org/files/Pamment_-_EU_Code_of_Practice.pdf

Содействие исследованием – доступ ко многим данным закрыт, что влечет трудности для независимых исследователей. Тем не менее платформы размещают и регулярно обновляют библиотеки отклоненной и заблокированной рекламы.

Одна из рекомендаций Фонда – создание Европейской комиссией нормативной базы для деятельности платформ. Следует учитывать, что они стали не источником проблем, а жертвами. Комиссия уже принимала обязательный Общий регламент по защите данных, который действует на организации, даже находящиеся за пределами Европейского союза, но работающие с данными о европейцах. В отличие от него, Свод правил является добровольным соглашением, стороны сами взяли на себя обязательства предоставлять отчеты. Вероятно, дальнейшую политику стоит выводить за рамки Свода правил и включать в более масштабную стратегию по информационной безопасности – масштабнее, чем План действий о борьбе с дезинформацией. Скорее всего, следующие шаги будут выглядеть только как следующая фаза сотрудничества в рамках нового Свода правил, учитывающего ошибки первого. Международному сообществу, по мнению Фонда, следует использовать понятие «операции по влиянию». Хотя, возможно, это понятие может представляться слишком обширным и не исключать дипломатического, экономического, политического влияния: оно не фокусируется на информационной стороне проблемы.

Фонд Карнеги предлагает несколько мер: усилить взаимодействие, сфокусироваться на формировании общих понятий и потребностей, разработать методы оценки эффективности.

Фонд Маршалла также исследовал эту тему[78]. Он предлагает десять принципов, которые следует принять европейцам для борьбы с информационными угрозами: усилить взаимодействие для разработки мер по совместному противодействию иностранному вмешательству вместе с НАТО; защищать принципы и институты демократии, привлекать граждан к участию в политическом процессе; ужесточить меры противодействия; повышение прозрачности и отчетности в информационно-технологическом секторе при сохранении анонимности данных о пользователях; углубление взаимодействия с частным сектором; усиление контроля над финансовой активностью и предотвращение спонсирования операций в Европе; контроль над зарубежным инвестированием в критические секторы европейской экономики; поддержка местных и независимых СМИ; информирование населения об иностранном вмешательстве; деполитизация подхода к борьбе с иностранным вмешательством.

[78] Kristine Berzina, Nad'a Kovalcikova, David Salvo, Etienne Soula European Policy Blueprintfor Countering Authoritarian Interference in Democracies // German Marshall Fund of the United States, June 2019, 66pp

Европейскому союзу необходимо создать общеевропейский центр по борьбе с вмешательством. Следует назначить официальный орган, который координировал бы усилия разных структур и обмен данными. Национальным правительствам, в свою очередь, необходимо централизовать контроль над ответами на угрозы. Им также следует устранить уязвимости в финансовой системе, избирательной, политической и в киберсфере.

Не следует упускать из виду когнитивную устойчивость, то есть способность населения критически и грамотно воспринимать информацию. Среди европейского населения наибольшим доверием пользуются радио и телевидение, социальные сети – наименьшим, при этом показатели очень разнятся по странам. Так, если в Финляндии телевидению доверяют 78 процентов опрошенных, то в Греции – 23 процента[79]. Через выявление и опровержение дезинформации населению и повышение медиаграмотности можно сформировать способность самостоятельно отделять правдивые новости от ложных. При этом не следует проводить диктаторскую политику и запрещать какие-либо информационные каналы, поскольку это подрывает доверие к властям, если не идет речь об экстренных мерах. Поток информации должен быть открытым, но она вся должна проходить проверку на правдивость в структурах Европейского союза и непосредственно самими гражданами. Для союза до сих пор существует в восприятии угроза со стороны российских правительственных СМИ, прежде всего, канала Russia Today. Тем не менее, в этой сфере оценка результатов – очень сложный процесс. Пока можно опираться только на опросы и количество выявленных случаев дезинформации.

Как отмечается в отчетах, для Европейского союза возникали сложные ситуации с российским информационным влиянием: захват Крыма, учения НАТО в Прибалтике, дело Скрипалей, миграционный кризис, катастрофа MH17[80]. Благодаря им можно дать оценку эффективности стратегических коммуникаций Европейского союза и его способности отвечать на угрозы.

В целом, механизмы работы в информационном пространстве высоко развиты в Европейском союзе, однако их эффективность могла бы вырасти при более централизованной координации. Сейчас инициативы имеют ситуативный характер – на данный момент это было связано с прошедшими выборами. В соответствии с этим законодательно выстроена и система информационной безопасности – она направлена на защиту выборов и демократии, что не отвечает потребности в долгосрочной стратегии.

[79] Flemming Splidsboel Hansen Russian Hybrid Warfare, a Study of Disinformation // Danish Institute for International Studies, 2017 URL: https://www.jstor.org/stable/resrep17379.7

[80] Roderick Parkes, Daniel Fiott Protecting Europe: the EU's Response to Hybrid Threats // European Union Institute for Security Studies, 2019 URL: https://www.jstor.org/stable/resrep21143.7

Этот механизм может быть более универсальным. Силы и средства должны входить в одну структуру и координироваться одним ведомством. Наибольшая часть полномочий сосредоточена в Европейской службе внешнего действия, ей же должны быть подотчетны и остальные направления. Так, в структуре ведомства должен быть масштабный центр по борьбе с гибридными угрозами, в котором следует выделить два направления: стратегические коммуникации и кибребезопасность. Основой для первого может послужить East StratCom, для второго – ENISA. Сюда же должны входить Общественный центр наблюдения за СМИ, Система быстрого реагирования, Координационная группа для аудиовизуальных медиа сервисов (ERGA), компьютерные группы реагирования. Этот орган должен координировать и стратегию, и оперативные действия в ответ на возникающие угрозы вроде кибератак или выявления ложных сообщений. Также упростилось бы взаимодействие с социальными сетями и медиаплатформами. Одной из первых задач могла бы стать разработка общеевропейского понятийного аппарата, который бы использовался правительствами и негосударственными организациями. Этот же орган мог бы проводить информирование граждан союза о том, как выявлять ложные сообщения и осуществлять подготовку и набор в наблюдательный центр. В его полномочия могло бы входить и содействие государствам и компаниям в разработке и совершенствовании систем информационной безопасности.

При значительных масштабах этого подразделения и соответствующем объеме полномочий, оно могло бы обеспечить более высокую информационную безопасность для всего союза, учитывая и то, что тогда пропадает необходимость совершенствовать механизм обмена данными о дезинформации и кибератаках. При этом следует продолжать придерживаться политики прозрачности и открытости данных, что обеспечивает доверие населения.

§2.3 Политический аспект информационной сферы

Информационная политика Европейского союза последних пяти лет сосредоточилась на безопасности содержательной части информационного пространства. Нарратив обеспечения безопасности компьютерных четей и персональной информации о гражданах Европейского союза, берущий начало на рубеже 1990-х и 2000-х, также сохранился. В результате политика информационной безопасности стала частью политики отражения гибридных угроз, что относится к общей политике безопасности союза. В ней сформировались два устойчивые направления: отражение киберугроз и борьба с дезинформацией.

В документах неизменной угрозой остается Россия. Вокруг этой темы и выстраиваются стратегические коммуникации. Вопрос возможного российского вмешательства в дела стран Европейского союза находится между двумя событиями: украинский кризис и присоединение Крыма; европейские выборы 2019 года. Между этими двумя вехами прослеживается развитие информационной политики в части борьбы с дезинформацией. Если на раннем этапе российское вмешательство обозначалось словом «пропаганда», то со временем чаще стало использоваться понятие «дезинформация». Вероятно, в дальнейшем стратегические коммуникации и борьба с дезинформацией войдут в План действий по человеческим правам и демократии 2020-2024[81], поскольку все чаще эта деятельность связывалась с обеспечением честных и прозрачных выборов, так что главным объектом для защиты от российской угрозы станет европейская демократия и свобода выбора, основанного на достоверной и общедоступной информации.

Таким образом, внешняя информационная политика определяется внешними факторами в виде угроз со стороны других стран. Внешняя угроза заставляет представителей европейских стран требовать усиления структур по борьбе с дезинформацией, как это было, например, в Европарламенте в 2018 году[82]. Это еще раз подчеркивает, что информационная безопасность в отношении дезинформации проявляется только как реакция на угрозу и не исходит из стремления союза к оказанию внешнего влияния.

Для информационной политики Европейского союза в общем понимании есть ряд черт. Ю.В. Курышева связывает ее с процессом интеграции и необходимостью формирования общеевропейской идентичности и определяет ее как «информационно-коммуникационную деятельность институтов Европейского союза, которая направлена на создание и поддержку функционирования единого европейского культурно-информационного пространства». Она выделяет три группы принципов информационной политики:

1) в интересах общества в целом;
2) в интересах национальных государств;
3) в интересах Европейского союза [83].

---

[81] EU Action Plan on Human Rights and Democracy 2020-2024 Road Map // URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12122-EU-Action-Plan-on-Human-Rights-and-Democracy-2020-2024

[82] The influence of propaganda on EU countries, video of the plenary sitting 17-01-2018 // European Parliament EPTV website URL: http://www.europarl.europa.eu/ep-live/en/plenary/video?debate=1516197858767 (дата обращения: 21.05.2020)

[83] Курышева Ю. В. Принципы и стратегии информационной политики ЕС // Вестник СПбГУ. Язык и литература. 2007. №4-II. URL: https://cyberleninka.ru/article/n/printsipy-i-strategii-informatsionnoy-politiki-es

Согласно этому же исследователю, единой европейской публичной сферы не существует. Вопросы общеевропейского значения рассматриваются через национальные интересы. В конечном счете решения принимаются членами союза, в том числе в отношении своей информационной политики – действия союза не могут противоречить этим интересам. Однако стоит учитывать, что есть институты наднационального уровня, действующие в информационной сфере в общесоюзных интересах. Европейский союз как межнациональное образование действует в информационной сфере с целью углубления интеграции и создания европейской идентичности при сохранении информационной независимости стран-членов[84]. Внешняя информационная политика тем самым может служить цели формирования общеевропейской идентичности через создание образа внешнего врага, который угрожает всем странам-членам. Это может способствовать интеграции в оборонной сфере и расширению наднациональных органов. Такой результат, скорее всего, может являться не целью самой по себе, а следствием политики безопасности.

Для внешней информационной политики Европейского союза можно обозначить некоторые приоритеты:

- обеспечение безопасности в Европейском союзе, защита либеральной демократии и европейских выборов;

- поддержание свободной журналистики в странах Восточного партнерства;

- сотрудничество с другими объединениями и странами по вопросам информационной безопасности.

[84] Курышева Ю. В. Политика ЕС в информационной сфере: европейская идентичность и культурное разнообразие. Нравственный аспект в работе фотоагентства поставщика изображений // Вестник СПбГУ. Язык и литература. 2008. №1-II. URL: https://cyberleninka.ru/article/n/politika-es-v-informatsionnoy-sfere-evropeyskaya-identichnost-i-kulturnoe-raznoobrazie-nravstvenny

Глава 3
Информационная политика Европейского союза по украинскому кризису

§3.1 Европейское восприятие ситуации в информационном поле по вопросу украинского кризиса и присоединения Крыма

В отношении украинского кризиса было сделано немало публикаций как с Российской, так и с Европейской стороны. Подавляющие их число имело соответственно проевропейский и пророссийский характер в зависимости от происхождения. Целесообразным для данной работы представляется не выявлять, какие действительно действия предпринимались сторонами, а какое позиционирование они получили. Каждая сторона стремится оправдать свою политику через осуждение чужой. Европейские публикации направлены на дискредитацию российских информационных источников, распространяющих дезинформацию, с точки зрения европейских стран. Российские же публикации продвигают идею о нецелесообразности такой европейский риторики и определение ее как явно агрессивной. Поэтому данная глава разбита на два параграфа – первый посвящен европейским исследованиям, второй – российским. Оба параграфа рассматривают восприятие сторонами политики другой стороны, причем преимущественно в научном и аналитическом ключе. Нецелесообразно использовать в одном контексте материалы, обусловленные диаметрально противоположными внешнеполитическими интересами.

Противостояние в информационном пространстве имело наиболее явное проявление в ходе украинских событий 2014 года и присоединения Россией Крыма, которое сопровождалось информационной поддержкой. С этим было связано принятие Европейским парламентом резолюции о противодействии российской пропаганде, где в преамбуле об этом открыто заявляется[85], и создание East StratCom. Российские действия будут рассмотрены в этом разделе только с позиции воздействия на население Европы, включая Украину как страну Восточной Европы.

С тех самых пор единая политика Европейского союза была неизменной – непризнание в отношении Крыма и Севастополя: «18 марта 2014 года Российская Федерация незаконно аннексировала Автономную Республику Крым и город

[85] European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)) // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584441630054&uri=CELEX:52016IP0441 (дата обращения: 02.04.2020)

Севастополь»[86]. Союз обращается в этом вопросе к резолюции Генеральной Ассамблеи ООН от 27 марта 2014 года и к заключениям заседаний Европейского совета. Позиция неоднократно подтверждалась в выступлениях Верховного Представителя ЕС. В части информационной политики Европейский союз прежде всего отказался от поставок товаров и технологий телекоммуникационного сектора в Крым.

Со стороны России информационная поддержка присоединения Крыма непосредственно в ходе кризиса осуществлялась разными средствами, среди которых был и захват радио- и телевизионных станций 28 февраля 2014 года. Украинские военные не получили приказа открыть огонь и просто сдались; можно предположить, что причины были связаны с нарушенными коммуникациями, это отвечает концепции гибридной войны и связано с минимальными жертвами, но требует хорошего технического оснащения. Подавляющее большинство крымского населения приветствовало выход из состава Украины, что тоже не могло пройти без информационной подготовки, учитывая то, что план по присоединению Крыма был разработан задолго до этих событий[87].

Операция по присоединению Крыма считается примером гибридной операции, проводимой государством. До этого, по убеждению европейских авторов, такие операции проводились только негосударственными организациями[88]. В гибридных операциях используются военные и невоенные методы, скрытые и открытые действия. Так, согласно европейским исследованиям, Россия применяла кампании по дезинформации, экономическое давление, скрытые военные действия, чтобы устроить нестабильность в Киеве и в отношениях Украины с Западом, сформировала образ фашистского государства и убеждение в угнетении части украинского населения.

Как у России, так и у западных стран были ключевые тезисы для официальных заявлений и материалов СМИ: для России – это право крымского населения на самоопределение; для Запада – нарушение Россией Устава ООН и Хельсинкского акта. Доведение этих тезисов до собственного населения было приоритетным в обеспечении поддержки и предотвращении внешнего информационного воздействия. В российском[89] и

[86] Сайт Европейской службы внешнего действия, Политика непризнания в отношении Крыма и Севастополя: справочная информация // URL: https://eeas.europa.eu/headquarters/headquarters-Homepage_ru/22972/Политика%20непризнания%20в%20отношении%20Крыма%20и%20Севастополя:%20справочная%20информация

[87] Anton Bebler “Frozen Conflicts” in Europe // Verlag Barbara Budrich, 2015 URL: https://www.jstor.org/stable/j.ctvdf0bmg.22

[88] Jan Joel Andersson Hybrid Operations: Lessons from the past // European Union Institute for Security Studies 2015 URL: https://www.jstor.org/stable/resrep06843

[89] Владимир Путин: Реакцию Запада на присоединение Крыма в Москве считают абсолютно неадекватной // сайт RT на русском URL: https://russian.rt.com/article/59878 (дата обращения: 24.05.2020)

европейском[90] информационном пространстве примеров достаточно. Россия при этом часто обращается к результатам референдума и до сих пор использует этот аргумент[91]. Однако, международным сообществом он не воспринимается как легитимный, при этом он остается единственным основанием для легитимности таких действий.

Как отмечают европейские исследователи, Россия в рамках информационного воздействия использовала фабрикацию фейковых новостей, онлайн-троллинг и помехи на радиочастотах[92]. Такие действия могут рассматриваться в качестве мер информационной войны в рамках гибридной. Украина со своей стороны вела работу по разоблачению фейковых новостей и блокировку различных каналов информации из России: телевизионные и радиоканалы, соцсети. Но это не помогло ни сформировать предпочтения крымского населения, ни оперативно среагировать на захват территории. То есть России удалось провести информационную кампанию на двух уровнях: формирование убеждений и оперативное нарушение коммуникаций.

Россия осуществляет информационное воздействие на европейское население в основном через каналы Russia Today и Sputnik, активное участие принимают фонд «Русский мир» и Россотрудничество. В формировании российского имиджа играет роль и такая крупная компания, как «Газпром». Так, он спонсирует европейские футбольные клубы и значимые спортивные события, например, Лигу Чемпионов UEFA. Более того, многоязычный европейский канал Euronews обвинялся в предвзятом пророссийском освещении событий 2014 года, несмотря на низкое участие России в финансировании канала. Украина в 2014 году отозвала лицензию на вещание Euronews на русском языке, а в 2015 году – и на украинском. В целом, Россия обладает достаточным ресурсом для продвижения своей повестки в Европе.

Однако, европейское население оказалось мало восприимчивым к российскому нарративу по теме Украины. Большинство продолжало возлагать вину за кризис на Россию и пророссийских сепаратистов, в то время как Россия обвиняла Украину и Запад.

От 15 до 20 процентов населения все же верили российским аргументам. В таких странах, как Франция и Великобритания доля обвинявших Россию была в пределах 40-45 процентов. В 2014 году наибольший рост негативного отношения к России среди европейских стран был отмечен в Германии и Польше – около 80 процентов населения.

---

[90] Die OSZE stößt an ihre Grenzen // DW website URL: https://www.dw.com/de/die-osze-stößt-an-ihre-grenzen/a-18107611 (дата обращения: 24.05.2020)

[91] Небензя назвал отправную точку произошедших в 2014 году событий в Крыму // RT на русском URL: https://russian.rt.com/world/news/748631-nebenzya-krym-rossiya (дата обращения: 24.05.2020)

[92] Sijbren de Jong, Tim Sweijs, Katarina Kertysova and Roel Bos Inside the Kremlin House of Mirrors, How Liberal Democracies Can Counter Russian Disinformation and Societal Interference // Hague Centre for Strategic Studies, 2017 URL: https://www.jstor.org/stable/resrep12585.10

Изменение восприятия России с позитивного на негативное в 2014 году по отношению к 2013 году было наиболее явным в Польше и Великобритании. Незначительным сдвигом выделяется Греция. Вместе с тем опросы населения стран Восточного партнерства показали, что негативное отношение к Европейскому союзу выросло с 13 процентов в 2012 году до 21 процента в 2014 году; выросла и доля убежденных в том, что Европейский союз не приносит в регион стабильность и мир. Среди украинского населения 57 процентов предпочли бы интеграцию с Европейским союзом, 16 процентов – с ЕАЭС, и это после присоединения Крыма, при этом есть сильное региональное разделение[93].

По этим данным можно заключить, что в целом Европейское население устойчиво к российскому информационному давлению, а европейские каналы достаточно независимы, чтобы формировать собственную повестку. Российское влияние в странах Восточного партнерства при этом дало ощутимые результаты и может считаться эффективным.

Во многом это связано с тем, какой курс присутствовал в местных СМИ и насколько у населения сформировано критическое мышление. В странах Европейского союза проводится регулярная работа с населением, хотя и в недостаточных масштабах. Тем не менее, есть недели медиаграмотности, а СМИ могут ссылаться на разоблачения фейковых новостей, которые публикует East StratCom. Вместе с тем такие данные дают основание полагать, что внешняя информационная Европейского союза на страны Восточного партнерства показывает невысокую эффективность, поскольку East StratCom и другие органы не ведут систематических масштабных кампаний, ориентированных на население этих стран, хотя он и работает с независимыми журналистами. Стоит учитывать постоянную работу Russia Today и Sputnik. В странах Восточной Европы осведомлены по вопросу возможной дезинформации и информационного влияния в их отношении, однако проявляют низкую обеспокоенность возможными последствиями[94].

Европейский союз не предпринимал внешних информационных действий в отношении Украины во время кризиса. Его собственное население устойчиво к российскому информационному влиянию. Каналы Russia Today и Sputnik ведут постоянную деятельность, но не пользуются высоким доверием в Европе. Европейские органы достаточно успешно справляются с дискредитацией российских информационных каналов. Хотя России удалось провести значимую работу в информационном пространстве Украины, на Европу не оказывалось влияния: эта сфера осталась перспективной для

[93] Antonio Missiroli, Jan Joel Andersson, Florence Gaub, Nicu Popescu and John-Joseph Wilkins Strategic Communications: East and South // European Union Institute for Security Studies (EUISS) 2016 URL: https://www.jstor.org/stable/resrep07092.5

[94] Michal Boksa Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures // German Marshall Fund of the United States 2019 URL: https://www.jstor.org/stable/resrep21238

дальнейшей работы. Очевидно, перед Россией на стояла задача предотвращения репутационных издержек в связи с присоединением Крыма и завоевания поддержки среди европейских стран, либо эти попытки оказались провальными.

Европейский союз воспринимает информационную угрозу со стороны России в двух аспектах: влияние на собственное население через дезинформацию и на ход выборов; влияние на общественное мнения в странах Восточного партнерства. Если в первом случае Европейский союз проводит успешную политику, то во втором – она почти отсутствует, в Европе есть только исследования о предпринятых Россией действиях. Однако, восприятие угрозы в этом направлении сохраняется. Вероятно, следует учитывать фактор влияния НАТО. Необходимость совместных действий Европейского союза и НАТО, в частности подразделений по стратегическим коммуникациям, прослеживается в ряде аналитических документов, прежде всего – в документах Фонда Маршалла. Стоит также не забывать, что СМИ стран Европейского союза также могут делать публикации в русском сегменте которые могут преследовать общесоюзные цели во внешней информационной политике и предоставлять альтернативную точку зрения[95].

§3.2 *Российская оценка стратегических коммуникаций Европейского союза по вопросу украинского кризиса*

В российском информационном и исследовательском пространстве доминирует убеждение, что Европейский союз ведет агрессивную и необоснованную информационную политику в отношении российских источников. При этом Россия терпит имиджевый ущерб от такой деятельности и не может добиться внешнеполитических целей. Это, в свою очередь, становится поводом для оценки европейского общественного мнения как предвзятого и неадекватного.

В европейских исследованиях отмечается, что Россия стремится использовать кризисные моменты в Европе, вроде миграционного кризиса или украинского, для разобщения европейского населения и снижения доверия к властям[96]. Эта же тема может быть обнаружена в российских публикациях, но с другим знаком[97]. К слову, европейские

[95] Информационная блокада Крыма – из личного опыта // сайт DW URL: https://www.dw.com/ru/информационная-блокада-крыма-из-личного-опыта/a-19174687 (дата обращения: 24.05.2020)
[96] Sijbren de Jong, Tim Sweijs, Katarina Kertysova and Roel Bos Inside the Kremlin House of Mirrors, How Liberal Democracies can Counter Russian Disinformation and Societal Interference // Hague Centre for Strategic Studies, 2017 URL: https://www.jstor.org/stable/resrep12585.10
[97] Европейцы не доверяют своим СМИ в освещении событий на Украине // РИА новости URL: https://ria.ru/20150421/1059731912.html (дата обращения: 24.05.2020)

СМИ также использовали в повестке моменты напряженности – например, проблему крымских татар.

В российском дискурсе начало активных мер Европейского союза по формированию системы защиты от дезинформации также связывается с Украинским кризисом, но вина за него возлагается на Запад[98]. Сам факт дезинформации при этом ставится под сомнение. В то что на Западе считают российской дезинформацией российские исследователи включают отдельные утверждения, публикации в СМИ, академические работы и внешнеполитическую риторику.

Среди инструментов Европейского союза, которыми он пытался воздействовать на информационную сферу по вопросу Украины, отмечают публикацию от имени ервокомиссара по вопросам торговли в 2014 году опровержения мифов об ассоциации Украина-Европейский союз, которые касаются России[99]. Опровержения касаются опасений, связанных с тем, что Украина может потерпеть экономические потери от ассоциации. В документе утверждается, что Украина получит рост торгового оборота и прибыли, но это не значит возможного вступления страны в союз. В том же году на сайте Европейской службы внешнего действия была опубликована брошюра с опровержением мифов о Восточном партнерстве, Украине и соглашении об ассоциации[100]. В ней опровергалось намерение союза расшатать социально-политическую обстановку на Украине. При этом отмечается, что союз и Россия вместе несут ответственность за мир в регионе. Референдум и присоединение Крыма еще раз обозначаются как нелигитимные, поскольку референдум должен был быть общеукраинским, а Крым является неотделимой частью Украины, согласно конституции страны. Сепаратисты в документе признаются экстремистами, при этом в брошюре сказано, что Россия уделяет им много внимания в медиапространстве. При этом в документе отрицается политический переворот на Украине и причастность Европы к процессам. В документе Россия упоминается довольно часто в информационном, экономическом и правовом отношениях.

В дальнейшем формат тезис-опровержение не раз использовался Европейским союзом. Можно предположить, что формат публикаций East StratCom был позаимствованы

[98] В.С. Царик Борьба с «российской дезинформацией» в публичном позиционировании западных институтов: анализ официальный сайтов НАТО и Европейского союза // Среднерусский вестник общественных наук №6 2019 URL: https://www.elibrary.ru/item.asp?id=41745626

[99] Myths about the EU–Ukraine Association Agreement. Setting the facts straight // The European Commission. – 2014. – 22 January. – URL: http://trade.ec.europa.eu/doclib/docs/2014/january/tradoc_152074.pdf (дата обращения: 24.05.2020)

[100] Fact sheet. Frequently asked questions about Ukraine, the EU's Eastern Partnership and the EU– Ukraine Association Agreement // EEAS. – 2014. – 14 June. URL: http://eeas.europa.eu/archives/delegations/ukraine/documents/virtual_library/myths_aa3_en.pdf (дата обращения: 25.05.2020)

именно оттуда. Преимущество такого подхода заключается в том, что работа происходит либо непосредственно с общественным мнением и доминирующими убеждениями, либо с информацией СМИ, которую необходимо опровергнуть, то есть повестка не создается искусственно, а это вызывает доверие. Перед структурами Европейского союза, тем не менее, не стоит цель завоевать доверие. Такая проблема есть у СМИ и социальных сетей, как показали опросы.

Таким образом, формат тезис-опровержение был задействован в продвижении европейского взгляда на украинские события и разоблачении мифов об ассоциации, причем еще в 2012-2013 годах.

Некоторые исследователи откровенно называют «информационной войной» против России ситуацию в информационном пространстве по вопросу Украины[101]. Авторы обвиняют западные СМИ в представлении ситуации в том свете, что война ведется якобы между Украиной и Россией. Тезис о российском вмешательстве позиционируется как абсурдный, российская позиция оценивается как четкая и направленная на невмешательство. В развязывании конфликта на Украине обвиняется абстрактный Запад.

Можно вообще говорить о наличии в российском дискурсе некоего нарратива об агрессивном Западе. Противостояние России и Европы редко выносится в самостоятельную тему. Речь скорее о противостоянии с США, которые олицетворяют все западные силы, враждебные России. Просто в этом общем контексте войны против мирной России теперь появилась информационная составляющая. Действия в информационном поле предпринимаются всеми сторонами, но кто-то может обвиняться в агрессивном использовании этих средств. Другой стороне якобы приходится адаптироваться к новым условиям ведения противоборства и разрабатывать оборонную информационную политику. Но если в Европе это действительно было реализовано, то в России это осталось в форме заявлений и обвинений в СМИ, примеры можно найти в том же RT[102]. В целом это можно объяснить тем, что Россия и так имеет достаточно обширный механизм работы в медиапространстве и обширные ресурсы, где можно публиковать опровержения.

Агрессивные действия Запада обуславливаются в российских публикациях его стремлением к подрыву влияния России, ослаблению ЕАЭС, а Украина является лишь инструментом. Продвигается идея, что Европейский союз создает видимость готовности принять Украину в числе стран-членов, хотя сам союз как раз утверждал обратное в своих

[101] Фролкин П.П., Шишкин Д.П. Информационная война против России и национализм на Украине как актуальная угроза национальной безопасности РФ // Информационная безопасность регионов 2014 №2 URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-protiv-rossii-i-natsionalizm-na-ukraine-kak-aktualnaya-ugroza-natsionalnoy-bezopasnosti-rf

[102] Американские СМИ о RT: Машина российской пропаганды обгоняет США // RT на русском URL: https://russian.rt.com/article/139367 (дата обращения: 26.05.2020)

коммуникациях. Отмечается, что сдвиг европейской и американской коммуникации с украинского населения на дискредитацию России произошел после крымского референдума. Исследователи выделяют ключевые тезисы в западных коммуникациях с того времени:

- Украина этнически ближе к Европе, чем России
- Евроинтеграция жизненно необходима Украине
- Таможенный союз подобен возврату в советское прошлое
- Россия – оккупант и угнетатель[103].

То есть таким образом Запад обвиняется в навешивании негативных ярлыков на Россию, что является чисто пропагандистским приемом. Вообще эмоциональной коммуникации свойственно обвинять кого-либо именно в ведении пропаганды, это прослеживается и в Российских, и в западных СМИ.

Популярной темой стали также ограничительные санкции в отношении России. Они коснулись российского медиапространства. Так, в октябре 2016 год Великобритания заблокировала счета канала Russia Today в Лондоне[104]. Это событие рассматривается не в контексте противостояния России и Европейского союза, а России и Великобритании. Основным моментом конфронтации России и Европейского союза называют принятие Европейским парламентом в 2016 году резолюции о противодействии пропаганде.

С российской стороны аналитики украинских событий и российского участия оценивают российскую политику как успешную, при этом ориентированной на распространение правды и вызвавшей движение национального возрождения. Так отмечают специалисты Российского института стратегических исследований[105]. При этом не идет речи об агрессивности в информационном пространстве Европейского союза в отношении России, но отдельных стран, в частности - Германии[106]. Политика России описывается как разъяснительная и оборонительная, в агрессивных действиях нет смысла. Специалисты утверждают даже, что России удалось после провала 2008 года в информационном противоборстве по вопросу Южной Осетии создать работающий

---

[103] Кошкин Р.П. Информационная война вокруг событий на Украине: геополитический анализ // Стратегические приоритеты 2015 №1 (5) URL: https://www.elibrary.ru/download/elibrary_23604876_39183480.pdf

[104] Лесь А.Ю. Влияние ограничительных санкций на российский сектор глобального медиапространства // Вестник Московского университета. Серия 27. Глобалистика и геополитика. 2016. №4. URL: https://cyberleninka.ru/article/n/vliyanie-ogranichitelnyh-sanktsiy-na-rossiyskiy-sektor-globalnogo-mediaprostranstva

[105] И.А. Николайчук Россия в зеркале мировых СМИ: что такое новая информационная война // сайт Российского института стратегических исследований URL: https://riss.ru/smi/21213/ (дата обращения: 26.05.2020)

[106] О. Назаров Интервью с И. Николайчуком: Стратегическая информационная операция может быть скоротечной, а может длиться годами // сайт Российского института стратегических исследований URL: https://riss.ru/smi/6696/ (дата обращения: 26.05.2020)

информационный аппарат и в итоге даже сформировать положительный имидж «вежливых людей» в Крыму.

Сравнивая риторику европейских и российских научно-аналитических публикаций по вопросу украинского кризиса, можно сделать некоторые выводы. Обе стороны стремятся обвинить друг друга в агрессивных методах информационного воздействия и представить себя их жертвой. Тогда оборонительная информационная политика представляется обоснованной, а значит можно дискредитировать информационные источники противника. Обе сторон также говорят об успехе целенаправленной политики по формированию информационного аппарата. В России начало такой политики можно связать с созданием в 2005 году Russia Today, в Европейском союзе – East StratCom в 2015 году. И российские, и европейские исследователи и официальные лица называют политику своей стороны успешной, но при этом и для тех, и для других сохраняются информационные угрозы.

Можно сказать, что в Российском дискурсе нет явно негативного отношения к Европейскому союзу. Есть только негативные новости по отдельным странам. В отношении всего союза скорее прослеживается нарратив о его разобщенности: внутреннее недоверие, разные ценности, разное отношение населения к внешним событиям. Основной актор, противоречащий российским интересам – США, а европейские структуры тесно связаны с американскими ведомствами. В целом для такого подхода есть основания – действительно, есть много аналитических публикаций как американских по вопросу Европейского союза, так и совместных европейско-американских. В Европейском союзе и НАТО подразделения стратегических коммуникаций имеют сходства в целях и методах, они даже проводили совместные семинары и сотрудничают в обмене опытом и информацией[107]. С Российской стороны обвинения в адрес Европейского союза сводятся в основном к тезису о влиянии на убеждения украинцев о возможности евроинтеграции, хотя союз на самом деле проводил противоположную официальную политику.

В европейских публикациях очень сильный акцент делается на недавно сформированной системе ответа на информационные угрозы в части борьбы с дезинформацией. В научно-аналитических материалах, на официальных сайтах, в СМИ, в заявлениях официальных лиц Россия предстает информационным агрессором. Информационная политика представляется направленной и на Украину, и на европейское население и страны Восточного партнерства. Политика борьбы с дезинформацией всячески

[107] Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization // NATO website, Official texts URL: https://www.nato.int/cps/en/natohq/official_texts_138829.htm

поддерживается. Учитывая российские и европейские публикации, нельзя говорить об активной внешней информационной политике Европейского союза, которая бы продвигала какие-либо убеждения. Формат коммуникаций строится в духе тезис-опровержение и основывается на российской дезинформации. Хотя материалы East StratCom не отражают официальную политику Европейского союза, в документах все же Россия часто упоминается как агрессор.

В целом, можно заключить, что риторика обеих сторон строится на взаимном обвинении в агрессивной информационной политике.

§3.3 *Перспективы развития информационной политики в отношении Украины*

На основе текущей ситуации и общих приоритетов Европейского союза во внешней информационной политике можно утверждать, что украинский кризис уходит из внешней и внутренней информационной повестки Европейского союза. Приоритеты информационной безопасности смещаются в сторону защиты европейской демократии, однако останутся публикации для поддержания общественного мнения внутри и за рубежом. Актуальность события упала, вопрос российский дезинформации может существовать и без него. Пандемия и кризис, скорее всего, приведут к тому, что Европейский союз вообще будет сосредоточен на внутренних проблемах, поэтому не будет необходимости в информационной поддержке его позиции по Украине.

На сайте EUvsDISINFO[108], который ведет East StratCom, с 1 января по 31 мая этого года в опровержениях тег «Украина» встречался 345 раз. В 2019 году – 447, 2018 году – 145, 2017 году – 331, 2016 году – 439.

Таким образом, с 2016 года по 2018 количество публикаций по Украине сократилось в три раза. Рост публикаций в 2019 году в три раза по отношению к 2018 году можно связать с началом активной борьбы с дезинформацией по Плану действий, который был утвержден в конце 2018 года.

Общее количество публикаций с 1 января по 31 мая 2018 года было равно 400, по тегу «Украина» было 36 процентов из них. В 2019 общее количество публикаций за этот период равнялось 1020, по тегу «Украина» было 44 процента. В этом году общее количество публикаций составило 1354, по тегу «Украина» было 25 процентов. Доля публикаций с тегом Украина, таким образом, уменьшилась на 19 процентов к предыдущему году. При этом процент публикаций с тегом «Россия» в этом году равен 38 процентам, в прошлом

[108] Main page // EUvsDISINFO website URL: https://euvsdisinfo.eu

году – 42 процентам. Многие из них сейчас связаны с новостями о дезинформации со стороны России по поводу коронавируса.

Соответственно можно проследить несколько трендов. Во-первых, активность East StratCom в целом растет после спада активности в 2017 году, когда за пять месяцев было всего 678 публикаций. Во-вторых, доля новостей по Украине сокращается из-за отсутствия значимых инфоповодов и снижения интереса для внешней политики. В-третьих, Россия чаще упоминается в опровержениях.

Тема Украины может снова возникнуть в информационном поле в случае подвижек в переговорном процессе. Позиция Европейского союза по присоединению Крыма останется неизменной, если только сама Украина не признает его законным, что сомнительно. Однако в обзоре дезинформации от 28 мая 2020 года East StratCom отмечает, что наибольшую часть российской дезинформации сейчас занимает Украина, затем идет коронавирус, после него – Вторая Мировая война. В отчете также утверждается что Россия использует исторический ревизионизм, что связано с празднованием Дня Победы[109].

Позитивное возможное изменение ситуации в инфополе для Европейского союза – уменьшение количества дезинформации, поддержка украинским населением европейских инициатив, повышение лояльности населения стран Восточного партнерства.

Негативное – повышение агрессивности в риторике всех стран Восточного партнерства и России, заявления европейских политиков о нецелесообразности трат на систему борьбы с дезинформацией и поддержку инициатив по Восточному партнерству, увеличение количества fake news, радикализация отношения украинского населения к Европейскому союзу из-за бездействия.

Взвешенный прогноз – сохранение трендов на снижение упоминаний Украины и повышение упоминаний России в опровержениях дезинформации, продолжение курса по усилению системы борьбы с дезинформацией, возможна ее перестройка с большим подчинением Европейской службе внешнего действия, сдвиг усилий на внутренние проблемы на фоне кризиса и уход Украины в целом из повестки, сохранение курса на поддержку демократии внутри Европейского союза и в странах Восточного партнерства, продвижение общеевропейских ценностей внутри Европы, борьба с мифом о разделенной Европе, сотрудничество со стратегическими коммуникациями НАТО и США. Европейскому союзу необходимо поддерживать свою позицию по Украине в информационном поле, а также по Восточному партнерству в целом, поскольку в восточном направлении было приложено много усилий, поэтому будет поддерживаться его

[109] Back to Basics: Ukraine, Revisionism, and Russophobia // Disinfo Review, EUvsDISINFO website URL: https://euvsdisinfo.eu/back-to-basics-ukraine-revisionism-and-russophobia/

позитивный образ, но это направление не будет приоритетным. Политика будет сосредоточена на решении внутриевропейских проблем.

Единственный действенный способ для Европейского союза по вопросу Украины – продолжение опровержений любой дезинформации о Восточном партнерстве, украинской политике, отдельных личностях, боевых действиях, пересмотре истории, в том числе в украинских источниках. East StratCom необходимо стать более значимой информационной силой за счет повышения авторитета как источника, расширения связей с информационными агентствами в Европе, России и на Украине, проводить качественные опровержения и журналистские по значимым поводам, стремиться к увеличению упоминаемости в новостных ресурсах. В таком случае можно будет использовать это учреждение более эффективно и для разъяснения европейской политики и продвижения ценностей. Тем не менее, опровержение новости всегда отстает на шаг от самой новости, поэтому европейские национальные СМИ должны также придерживаться единых подходов в вопросах освещения внешней политики, а это в свою очередь в значительной степени зависит от политики самой страны. Поэтому Европейскому союзу важно окончательно определить, какие ценности разделяют все европейцы.

Заключение

Итак, основными понятиями, необходимыми для изучения информационной политики государства или объединения государств, были определены:

информационный суверенитет – самостоятельность субъекта отношений в информационной сфере в проведении внутренней и внешней информационной политики и способность обеспечить безопасность собственного информационного пространства;

информационная политика – целенаправленная деятельность субъекта отношений в информационной сфере по достижению внутриполитических и внешнеполитических целей через регулирование и организацию технической и содержательной составляющих информационного пространства;

информационное противоборство – состояние отношений субъектов в информационной сфере, характеризующееся соперничеством и являющееся следствием стремления как минимум одного из субъектов к достижению внешнеполитических целей средствами воздействия в информационном пространстве

стратегические коммуникации – скоординированная коммуникационная деятельность страны, направленная на формирование мнений и убеждений у целевой аудитории для осуществления внешнеполитических целей.

Официально Европейский союз признает наличие угроз, требующих ответа на наднациональном уровне в общесоюзном масштабе. Система органов Европейского союза позволяет проводить единую информационную политику как в аудиовизуальном внутреннем секторе, так и в стратегических коммуникациях. Это обусловлено осознанием всех стран-членов наличия угрозы.

Безусловно, Европейскому союзу удалось создать эффективную систему по борьбе с внешней дезинформацией за последние пять лет, что обеспечивает повышение общей безопасности союза в рамках общей внешней политики и политики безопасности. Стратегические коммуникации и борьба с гибридными угрозами подчиняются внешнеполитическому ведомству. Вместе с тем в информационной политике сохраняется нарратив по повышению безопасности компьютерных систем и защите персональных данных в том числе от внешних угроз, который развивается уже около 20 лет. Соблюдать требования союза обязаны все компании, которые работают с данными о европейцах, согласно Общему регламенту по защите персональных данных. Кибербезопасность – самостоятельная ветвь, которая иногда связывается с борьбой с дезинформацией в документах по борьбе с гибридными угрозами.

Таким образом, в политике информационной безопасности есть два основных направления: компьютерная безопасность и стратегические коммуникации. Деятельность

первой координируется в основном ENISA, второй – Европейской службой внешнего действия и East StratCom. Помимо этого, во втором направлении функционируют Наблюдательный центр за социальными сетями, европейская ветвь Международной организации проверки фактов, Система быстрого реагирования. Следует отметить важное направление деятельности этих двух сегментов – работа с населением, в которую входит информирование о защите от хищения персональных данных и формирование критического отношения к новостям.

В последние два года больше всего усилий было сосредоточено на защите выборов и демократии. Операции по влиянию, инициированные внешними странами, могут определить результат выборов. Тем самым действия в сфере массовых коммуникаций могут иметь последствия в политической сфере, в этом и состоит главная опасность. Сохраняется и возможность атак на компьютерные сети. Этим обусловлено сосредоточение усилий на защите выборов, однако европейский аппарат информационной безопасности может иметь намного более широкий функционал и работать в том числе на зарубежную аудиторию, что пока развито в невысокой степени. В основном это касается поддержки независимых журналистов. В дальнейшем возможно еще большее смещение вопросов информационной безопасности в сферу защиты демократии.

Все более активно используется дискредитация новостных источников, особенно российских. На результаты опровержений East StratCom могут ссылаться не только европейские СМИ. Следует ожидать дальнейшего развития этой организации.

Нельзя не отметить повышенного внимания к социальным сетям. В 2018 году были приняты План действий по борьбе с дезинформацией и Свод правил для социальных сетей. Документы подобного рода были приняты впервые в Европейском союзе, социальные платформы добровольно присоединились к Своду правил и приняли обязательство предоставлять отчеты по разоблачению политической рекламы.

Вмешательство в выборы посредством социальных сетей может происходить через распространение информации среди пользователей и внедрение в компьютерные сети. Они могут влиять на предпочтения избирателей, явку и процесс голосования и подсчета голосов. Есть ряд инструментов правового и программного характера, способных этому помешать. Однако важным остается вопрос выявления угроз и определения их источника. Главным инструментом является мониторинг финансирования рекламных компаний. Социальные сети, такие как Facebook и Twitter, имеют положения в своей политике, запрещающие некоторые рекламные сообщения политического характера, если источник финансирования рекламодателя не подтвержден. Можно предположить, что ошибки в сотрудничестве с социальными платформами будут учтены, и в будущем будет принят

новый свод правил, который бы более четко определял критерии для рекламы, способной оказать негативное влияние, а также будет более правильная оценка результатов, расширение доступа к информации об отклоненных рекламных кампаниях для исследователей и общепринятый понятийный аппарат для всего союза и сотрудничающих организаций.

Ситуация в информационной среде по вопросу украинского кризиса и присоединения Крыма была главным стимулом для развития содержательной информационной политики Европейского союза. Он был не готов к информационному противоборству, сфера стратегических коммуникаций тогда не воспринималась как угрожаемая и осуществлялась в основном за счет официальных представителей союза, значимых стратегических документов и учреждений не было, причем даже в течение года-двух после начала кризиса[110]. Изучение публикаций с европейской и российской стороны позволяет утверждать, что стороны не оказали ощутимого влияния друг на друга информационными средствами. Последующая исследовательская активность сводилась к взаимным обвинения. Россию обвиняли в агрессии, Европейский союз – в неадекватной реакции. Новостные сообщения придерживались таких нарративов, как право на самоопределение и аналогия с Косово с одной стороны, с другой – нелегитимность референдума и нарушение международного права. В будущем возможно сохранение трендов на снижение упоминаний Украины и повышение упоминаний России в опровержениях дезинформации, продолжение курса по усилению системы борьбы с дезинформацией, ее перестройка с большим подчинением Европейской службе внешнего действия, сдвиг усилий на внутренние проблемы на фоне кризиса, поддержка демократии, продвижение общеевропейских ценностей, борьба с мифом о разделенной Европе, сотрудничество со стратегическими коммуникациями НАТО и США. East StratCom необходимо стать более значимой информационной силой за счет повышения авторитета как источника, расширения связей с информационными агентствами в Европе, России и на Украине, проводить качественные опровержения и журналистские по значимым поводам, стремиться к увеличению упоминаемости в новостных ресурсах. Позиция по Восточному партнерству и Украине останется прежней, но восточное направление уйдет на второй план на фоне решения внутриевропейских проблем.

В общем можно заключить, что Европейский союз добился значимых успехов в переформатировании информационной политики для ответа на современные внешние угрозы, в том числе за счет ее смещения в сторону борьбы с дезинформацией, работы с

[110] Кремлевская пропаганда и тщетность борьбы с ней // сайт BBC русская служба URL: https://www.bbc.com/russian/features-38145898 (дата обращения: 26.05.2020)

социальными сетями и защиты демократии. Вместе с тем сохраняется большой потенциал для развития, в том числе за счет реструктуризации системы, ее централизации и расширения ее функций. Сфера международных отношений в информационной среде в целом перспективна для развития и дальнейших исследований. Опыт Европейского союза может стать полезным для других стран. Вероятно, на фоне повышения значимости повестки информационной безопасности в мировой политике увеличится объем сотрудничества стран в обмене опытом.

Источники

1. Декларация от 9 мая 1950 года, оглашенная Робером Шуманом, министром иностранных дел, в Париже, на Кэ д'Орсэ в салоне часов // История европейской интеграции. Хрестоматия в 3-х частях. Ч 1. История Европейских сообществ Составители: Браницкий А.Г., Леушкин Д.В. – Н. Новгород: Нижегородский госуниверситет, 2014 стр9-12
2. Доктрина информационной безопасности РФ, утверждена Указом Президента РФ от 5 декабря 2016 г. №646 URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 13.02.2020)
3. И.А. Николайчук Россия в зеркале мировых СМИ: что такое новая информационная война // сайт Российского института стратегических исследований URL: https://riss.ru/smi/21213/ (дата обращения: 26.05.2020)
4. Концепция внешней политики РФ, утверждена Президентом Российской Федерации В.В. Путиным 30 ноября 2016 г. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2542248 (дата обращения: 15.02.2020)
5. О. Назаров Интервью с И. Николайчуком: Стратегическая информационная операция может быть скоротечной, а может длиться годами // сайт Российского института стратегических исследований URL: https://riss.ru/smi/6696/ (дата обращения: 26.05.2020)
6. Стратегия развития отрасли информационных технологий в РФ на 2014-2020 годы и на перспективу до 2025 года, утверждена распоряжением Правительства РФ от 1 ноября 2013 г. №2036-р URL: http://minsvyaz.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014-2020_2025.pdf (дата обращения: 13.02.2020)
7. Указ Президента РФ от 31.12.2015 №683 «О Стратегии национальной безопасности Российской Федерации» URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=191669&fld=134&dst=1000000001,0&rnd=0.07402217045154613#05568460818294072 (дата обращения: 15.02.2020)
8. Указ Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” URL: http://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 13.02.2020)
9. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 10.03.2020)
10. 10 ways the EU is fighting disinformation, Medium website, author European Commission // URL: https://medium.com/@EuropeanCommission/10-ways-the-eu-is-fighting-disinformation-f07fca60e918 (дата обращения: 30.03.2020)
11. About EACEA, European Commission website URL: https://eacea.ec.europa.eu/about-eacea_en (дата обращения: 15.02.2020)
12. About ENISA, European Union Agency for Cybersecurity website // URL: https://www.enisa.europa.eu/about-enisa (дата обращения: 30.03.2020)
13. About European Cybercrime Centre – EC3 // Europol website URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата обращения: 20.02.2020)
14. About Us, SOMA website // URL: https://www.disinfobservatory.org/about-us/ (дата обращения: 03.05.2020)
15. Action Plan Against Disinformation, Report on Progress, June 2019 // URL: https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf (дата обращения: 05.05.2020)

16. Audiovisual and Media // Official website of the European Union URL: https://europa.eu/european-union/topics/audiovisual-media_en (дата обращения: 15.02.2020)
17. Code of Practice on Disinformation, European commission website // URL: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (дата обращения: 03.05.2020)
18. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for a European Policy Approach" Brussels, 6.6.2001 URL: https://www.steptoe.com/images/content/4/8/v1/485/811.pdf] (дата обращения: 15.02.2020)
19. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. A strategy for a secure Information Society "Dialogue, partnership and empowerment". Brussels, 31.52006. COM(2006) 251 final. URL: http://ec.europa.eu/information_society/doc/com2006251.pdf (дата обращения: 20.02.2020)
20. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for a European Policy Approach" Brussels, 6.6.2001 URL: https://www.steptoe.com/images/content/4/8/v1/485/811.pdf (дата обращения: 10.03.2020)
21. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400} URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0149 (дата обращения: 20.02.2020)
22. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (дата обращения: 03.05.2020)
23. Compendium on Cyber Security of Election Technology, NIS Cooperation Group July 2018 // URL: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf (дата обращения: 30.03.2020)
24. Conclusions – 19 and 20 March 2015, European Council // URL: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf (дата обращения: 02.04.2020)
25. Conclusions of the Council and of the Member States on securing free and fair European elections // URL: https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf (дата обращения: 05.05.2020)
26. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Charter of Fundamental Rights of the European Union URL: https://europa.eu/european-union/sites/europaeu/files/eu_citizenship/consolidated-treaties_en.pdf#nameddest=article167 (дата обращения: 15.02.2020)
27. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1521461913374&uri=CELEX:32016L1148 (дата обращения: 03.05.2020)

28. Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058 (дата обращения: 20.02.2020)
29. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance) URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013 (дата обращения: 15.02.2020)
30. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524931018994&uri=CELEX:32013L0040 (дата обращения: 10.03.2020)
31. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (дата обращения: 27.02.2020)
32. East StratCom Team. «Action Plan on Strategic Communication» URL: http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf (дата обращения: 02.04.2020)
33. ENISA meets cyber-experts to plan Cyber Europe 2018 // ENISA website https://www.enisa.europa.eu/news/enisa-news/enisa-meets-cyber-experts-to-plan-cyber-europe-2018 (дата обращения: 30.03.2020)
34. EU Action Plan on Human Rights and Democracy 2020-2024 Road Map // URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12122-EU-Action-Plan-on-Human-Rights-and-Democracy-2020-2024
35. European Commission, Evaluation of the EU decentralised agencies in 2009 Volume III – Individual Agencies URL: https://europa.eu/european-union/sites/europaeu/files/docs/body/agency_level_findings_en.pdf (дата обращения: 30.03.2020)
36. European Council meeting (19 and 20 March 2015) – Conclusions URL: https://www.eesc.europa.eu/resources/docs/european-council-conclusions-19-20-march-2015-en.pdf (дата обращения: 02.04.2020)
37. The influence of propaganda on EU countries, video of the plenary sitting 17-01-2018 // European Parliament EPTV website URL: http://www.europarl.europa.eu/ep-live/en/plenary/video?debate=1516197858767 (дата обращения: 21.05.2020)
38. European Parliament legislative resolution of 8 July 2010 on proposal for a Council decision establishing the organization and functioning of the European External Action Service // URL: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0280&language=EN&ring=A7-2010-0228 (дата обращения: 30.03.2020)
39. European Parliament resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI)) // URL: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0470&language=EN (дата обращения: 27.02.2020)
40. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)) // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584441630054&uri=CELEX:52016IP0441 (дата обращения: 02.04.2020)
41. CSDP structure, instruments and agencies // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/5392/csdp-structure-instruments-and-agencies_en (дата обращения: 20.03.2020)

42. EU in the World // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/area/geo_en (дата обращения: 20.03.2020)
43. Shaping of a Common Security and Defence Policy // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/5388/shaping-common-security-and-defence-policy_en (дата обращения: 20.03.2020)
44. EUvsDisinfo: how to debunk over 6,500 disinformation cases in four years? // European Union External Action website URL: https://eeas.europa.eu/topics/countering-disinformation/68633/euvsdisinfo-how-debunk-over-6500-disinformation-cases-four-years_en (дата обращения: 12.04.2020)
45. Fact Sheet on Tackling the Spread of Disinformation Online // URL: https://ec.europa.eu/digital-single-market/en/news/factsheet-tackling-online-disinformation (дата обращения: 30.03.2020)
46. Fact sheet. Frequently asked questions about Ukraine, the EU's Eastern Partnership and the EU– Ukraine Association Agreement // EEAS. – 2014. – 14 June. URL: http://eeas.europa.eu/archives/delegations/ukraine/documents/virtual_library/myths_aa3_en.pdf (дата обращения: 25.05.2020)
47. Free and fair European elections, State of the Union, European Commission, 12 September 2018 // URL: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf (дата обращения: 30.03.2020)
48. James Pamment The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission // Carnegie Endowment for International Peace March 2020 URL: https://carnegieendowment.org/files/Pamment_-_EU_Code_of_Practice.pdf
49. Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats, a European Union response // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата обращения: 12.04.2020)
50. Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats a European Union response // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018 (дата обращения: 12.04.2020)
51. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 (дата обращения: 12.04.2020)
52. Joint Communication to the European parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation // URL: https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation (дата обращения: 03.05.2020)
53. Myths about the EU–Ukraine Association Agreement. Setting the facts straight // The European Commission. – 2014. – 22 January. – URL: http://trade.ec.europa.eu/doclib/docs/2014/january/tradoc_152074.pdf (дата обращения: 24.05.2020)
54. NIS Cooperation Group, European Commission website // URL: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group (дата обращения: 03.05.2020)
55. Partnership for Countering Influence Operations, Carnegie Endowment for International Peace website // URL: https://carnegieendowment.org/specialprojects/counteringinfluenceoperations
56. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18December 2000 on the protection of individuals with regard to the processing of personal

data by the Community institutions and bodies and on the free movement of such data URL: https://edps.europa.eu/sites/edp/files/publication/reg_45-2001_en.pdf (дата обращения: 20.02.2020)
57. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525205207301&uri=CELEX:32016R0679 (дата обращения: 27.02.2020)
58. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 URL: https://ccdcoe.org/sites/default/files/documents/EU-130521-ENISA.pdf (дата обращения: 30.03.2020)
59. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization // NATO website, Official texts URL: https://www.nato.int/cps/en/natohq/official_texts_138829.htm
60. Strategic Communications // European Union External Action website URL: https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en (дата обращения: 02.04.2020)

Новостные ресурсы

1. Американские СМИ о RT: Машина российской пропаганды обгоняет США // RT на русском URL: https://russian.rt.com/article/139367 (дата обращения: 26.05.2020)
2. Владимир Путин: Реакцию Запада на присоединение Крыма в Москве считают абсолютно неадекватной // сайт RT на русском URL: https://russian.rt.com/article/59878 (дата обращения: 24.05.2020)
3. Европейцы не доверяют своим СМИ в освещении событий на Украине // РИА новости URL: https://ria.ru/20150421/1059731912.html (дата обращения: 24.05.2020)
4. Информационная блокада Крыма – из личного опыта // сайт DW URL: https://www.dw.com/ru/информационная-блокада-крыма-из-личного-опыта/a-19174687 (дата обращения: 24.05.2020)
5. Кремлевская пропаганда и тщетность борьбы с ней // сайт BBC русская служба URL: https://www.bbc.com/russian/features-38145898 (дата обращения: 26.05.2020)
6. Небензя назвал отправную точку произошедших в 2014 году событий в Крыму // RT на русском URL: https://russian.rt.com/world/news/748631-nebenzya-krym-rossiya (дата обращения: 24.05.2020)
7. Back to Basics: Ukraine, Revisionism, and Russophobia // Disinfo Review, EUvsDISINFO website URL: https://euvsdisinfo.eu/back-to-basics-ukraine-revisionism-and-russophobia/
8. Die OSZE stößt an ihre Grenzen // DW website URL: https://www.dw.com/de/die-osze-stößt-an-ihre-grenzen/a-18107611 (дата обращения: 24.05.2020)
9. EU Rapid Alert System used amid coronavirus disinformation campaign, Euractiv website // URL: https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/ (дата обращения: 05.05.2020)
10. In the media // EUvsDisinfo website URL: https://euvsdisinfo.eu/in-the-media/
11. Main page // EUvsDISINFO website URL: https://euvsdisinfo.eu

Литература

1. Авдеенко Е.Г. От Маастрихта к Амстердаму: стратегия ФРГ в области общей внешней политики, безопасности и обороне в Европе // Вестник Челябинского Государственного Университета №22 (237) 2011 стр112-121
2. Артамонов Д.С. Информационный суверенитет, теоретический аспект // Материалы VIII Международного Конституционного Форума, посвященного 80-летию Саратовской области. 2017 стр.16-20
3. Беленков Д.В., Гюлазян П.А., Мазлумян Д.Э. Информационный суверенитет России и Европейского союза, информационная политика и информационное противоборство: сущность и содержание // Международный студенческий научный вестник, №5 2018
4. Богданов С.В. Стратегические коммуникации: концептуальные подходы и модели для государственного управления // Государственное управление. Электронный вестник. 2017. №61. URL: https://cyberleninka.ru/article/n/strategicheskie-kommunikatsii-kontseptualnye-podhody-i-modeli-dlya-gosudarstvennogo-upravleniya
5. Гриняев С.Н. Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. №8, 2001
6. Ерофеева Н.В. Современные информационные войны и их влияние на политическую стабильность государства // PolitBook. 2015. №2. URL: https://cyberleninka.ru/article/n/sovremennye-informatsionnye-voyny-i-ih-vliyanie-na-politicheskuyu-stabilnost-gosudarstva (дата обращения: 3.04.2018)
7. Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. №1. URL: https://cyberleninka.ru/article/n/formirovanie-kontseptsii-informatsionnogo-suvereniteta-gosudarstva
8. Захарова сообщила о характере ответов России на информационную агрессию // сайт РИА новости URL: https://www.rbc.ru/rbcfreenews/5daafa179a7947060acaa0da
9. Зорина Е.Г. Информационный суверенитет современного государства и основные инструменты его обеспечения // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2017 №3 стр.345-348
10. Иванов С.А. Информационная война: сущность и основные формы проявления // Известия АлтГУ. 2013. №4 (80). URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-suschnost-i-osnovnye-formy-proyavleniya
11. Кошкин Р.П. Информационная война вокруг событий на Украине: геополитический анализ // Стратегические приоритеты 2015 №1 (5) URL: https://www.elibrary.ru/download/elibrary_23604876_39183480.pdf
12. Курышева Ю. В. Политика ЕС в информационной сфере: европейская идентичность и культурное разнообразие. Нравственный аспект в работе фотоагентства поставщика изображений // Вестник СПбГУ. Язык и литература. 2008. №1-II. URL: https://cyberleninka.ru/article/n/politika-es-v-informatsionnoy-sfere-evropeyskaya-identichnost-i-kulturnoe-raznoobrazie-nravstvenny
13. Курышева Ю. В. Принципы и стратегии информационной политики ЕС // Вестник СПбГУ. Язык и литература. 2007. №4-II. URL: https://cyberleninka.ru/article/n/printsipy-i-strategii-informatsionnoy-politiki-es
14. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира. // Управленческое консультирование. 2015. №2 (74). URL: https://cyberleninka.ru/article/n/gosudarstvennaya-politika-informatsionnogo-suvereniteta-rossii-v-usloviyah-sovremennogo-globalnogo-mira

15. Лесь А.Ю. Влияние ограничительных санкций на российский сектор глобального медиапространства // Вестник Московского университета. Серия 27. Глобалистика и геополитика. 2016. №4. URL: https://cyberleninka.ru/article/n/vliyanie-ogranichitelnyh-sanktsiy-na-rossiyskiy-sektor-globalnogo-mediaprostranstva
16. Лобанов Р.О. Динамика взаимоотношений Западноевропейского союза и НАТО по вопросам военно-политической безопасности Европы в 1954-2002 гг // Локус: люди, общество, культуры, смыслы №4 2012 стр74-85
17. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В.Б. Вепринцев, А.В. Манойло, А.И. Петренко, Д.Б. Фролов; под ред. А.И. Петренко. – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2011. – 495с.
18. Политика непризнания в отношении Крыма и Севастополя: справочная информация // Сайт Европейской службы внешнего действия URL: https://eeas.europa.eu/headquarters/headquarters-Homepage_ru/22972/Политика%20непризнания%20в%20отношении%20Крыма%20и%20Севастополя:%20справочная%20информация
19. Фролкин П.П., Шишкин Д.П. Информационная война против России и национализм на Украине как актуальная угроза национальной безопасности РФ // Информационная безопасность регионов 2014 №2 URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-protiv-rossii-i-natsionalizm-na-ukraine-kak-aktualnaya-ugroza-natsionalnoy-bezopasnosti-rf
20. Царик В.С. Борьба с «российской дезинформацией» в публичном позиционировании западных институтов: анализ официальный сайтов НАТО и Европейского союза // Среднерусский вестник общественных наук №6 2019 URL: https://www.elibrary.ru/item.asp?id=41745626
21. Anton Bebler “Frozen Conflicts” in Europe // Verlag Barbara Budrich, 2015 URL: https://www.jstor.org/stable/j.ctvdf0bmg.22
22. Antonio Missiroli, Jan Joel Andersson, Florence Gaub, Nicu Popescu and John-Joseph Wilkins Strategic Communications: East and South // European Union Institute for Security Studies (EUISS) 2016 URL: https://www.jstor.org/stable/resrep07092.5
23. Brüggemann, M. How the EU constructs the European Public Sphere: Seven strategies of information policy // Javnost. - 2005 №12 (2), pp. 57-74.
24. Erik Brattberg, Tim Maurer Russian Election Interference, Europe’s Counter to Fake News and Cyber Attacks // Carnegie Endowment for International Peace, May 2018 URL https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf
25. Flemming Splidsboel Hansen Russian Hybrid Warfare, a Study of Disinformation // Danish Institute for International Studies, 2017 URL: https://www.jstor.org/stable/resrep17379.7
26. Ibrus, I. The EU Digital Single Market as a mission impossible: Audio-visual policy conflicts for Estonia // International Journal of Digital Television. – 2016 vol.7 №1. pp.23-28
27. Jan Joel Andersson Hybrid Operations: Lessons from the past // European Union Institute for Security Studies 2015 URL: https://www.jstor.org/stable/resrep06843
28. Joanna Świątkowska European Cybersecurity Journal, volume 3 (2017), issue 3 // URL https://www.ria.ee/sites/default/files/content-editors/kuberturve/ecj_volume3.issue3_extract_past.pdf
29. Kristine Berzina, Nad’a Kovalcikova, David Salvo, Etienne Soula European Policy Blueprintfor Countering Authoritarian Interference in Democracies // German Marshall Fund of the United States, June 2019, 66pp
30. Łukasz Antoni Król Digital foreign policy: how digital tools can further Europe’s foreign policy goals // European View (2016) 15:133-144

31. Michal Boksa Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures // German Marshall Fund of the United States 2019 URL: https://www.jstor.org/stable/resrep21238
32. Roderick Parkes, Daniel Fiott Protecting Europe: the EU's Response to Hybrid Threats // European Union Institute for Security Studies, 2019 URL: https://www.jstor.org/stable/resrep21143.7
33. Sijbren de Jong, Tim Sweijs, Katarina Kertysova and Roel Bos Inside the Kremlin House of Mirrors, How Liberal Democracies Can Counter Russian Disinformation and Societal Interference // Hague Centre for Strategic Studies, 2017 URL: https://www.jstor.org/stable/resrep12585.10