УДК 327

Кира ГОДОВАНЮК

КИБЕРБЕЗОПАСНОСТЬ И БОРЬБА С ДЕЗИНФОРМАЦИЕЙ: ОПЫТ ВЕЛИКОБРИТАНИИ

Аннотация. *После референдума 2016 г. правительство Великобритании предприняло ряд мер, направленных на обновление международной повестки. По мнению британского истеблишмента, передовой опыт Соединённого Королевства в противодействии киберугрозам, иностранному вмешательству и в борьбе с дезинформацией может обеспечить ему особый статус не только в отношениях со странами-единомышленниками в Европейском союзе и НАТО, но и за пределами Евро-Атлантики. В статье проанализированы британские инициативы в регулировании информационного контента, в том числе Белая книга Великобритании «О вреде онлайн» и глобальная конференция по свободе СМИ, (Лондон, июль 2019 г.). Автор делает вывод о том, что правительство считает источниками гибридных угроз страны-нарушители либерального миропорядка.*

Ключевые слова*: Великобритания, Б. Джонсон, кибербезопасность, кибератаки, дезинформация, «фейковые новости», гибридные угрозы, социальные медиа, Европейский союз, НАТО, Россия, брекзит.*

Кибербезопасность – внутрибританский контекст

С развитием интернет-технологий изменились не только источники и характер общественных угроз, но и форма управления международными отношениями (появление «облачной», сетевой или твиттер-дипломатии и пр.). Одновре́менно многие страны, включая Великобританию, приступили к разработке комплекса мер по противодействию угрозам в информационной среде.

Ещё в 2011 г. на Мюнхенской конференции по безопасности глава Форин Офиса У. Хейг заявил, что «Британия намерена активно содействовать поиску ответов на глобальные киберугрозы и с этой целью будет сотрудничать с союзниками в Вашингтоне, Берлине, Париже и Канберре»[1].

В ноябре того же года правительство опубликовало первую Национальную стратегию кибербезопасности[2]. С 2016 г. в Соединённом Королевстве действует обновлённая пятилетняя стратегия, в которой кибератаки признаны крупнейшей угрозой национальной безопасности во всех её аспектах, включая экономику[3]. В документе сформулирована амбициозная цель – сделать Великобританию неуязвимой по отношению к современным

© ***Годованюк Кира Анатольевна*** – кандидат политических наук, старший научный сотрудник Центра британских исследований Отдела страновых исследований Института Европы РАН. ***Адрес***: 125009, Москва, ул. Моховая, д. 11, стр. 3. ***E-mail***: kira.godovanyuk@gmail.com.

DOI: http://dx.doi.org/10.15211/vestnikieran420198792

[1] Security and freedom in the cyber age - seeking the rules of the road. Speech to the Munich Security Conference, Foreign Secretary William Hague. February 2011. URL: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road (дата обращения: 01.08.2019).

[2] Cyber Security Strategy. The new Cyber Security Strategy was published on 25 November 2011. URL: https://www.gov.uk/government/publications/cyber-security-strategy (дата обращения 1.08.2019).

[3] National Cyber Security Strategy 2016 to 2021. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (дата обращения: 01.08.2019).

угрозам в цифро-вой среде, а британские инициативы – моделью для глобальных усилий по киберзащите.

В правительственном документе обозначены ключевые государственные цели: укрепить потенциал IT-компаний по противодействию хакерским атакам (специальные меры защиты – *Defend*), укрепить возможности правоохранительных органов для борьбы с киберпреступниками (меры отражения – *Deter*), развитие кибернавыков специалистов технологических компаний (меры развития – *Develop*). Важная задача – создать партнёрство между государственными структурами и технологическими предприятиями, наладить взаимный обмен данными, а также поощрять совместные усилия бизнеса, общественности, частного сектора и институтов гражданского общества по противодействию хакерским атакам. На перечисленные меры Кабинет выделил 1,9 млрд ф.ст. (срок реализации – 2021 г.).

В рамках новой стратегии в 2016 г. был создан Национальный центр кибербезопасности (НЦК), в задачи которого вошла реализация программы «Активная киберзащита»[1].

В обзоре возможностей национальной безопасности Соединённого Королевства за 2018 г. отмечено, что «злонамеренная кибердеятельность выходит за пределы государственных границ, усложняется и становится всё более опасной»[2]. В правительственном документе высказано предположение, что по мере того, как повседневная жизнь будет переходить в онлайн сферу, государственные институты и обычные граждане будут ощущать возрастающую зави-симость от технологий, которые, в свою очередь, весьма уязвимы к «злонамеренным действи-ям» «безответственных стран». Руководство Соединённого Королевства исходит из того, что глобальные угрозы в киберпространстве требуют глобальных ответов, которые способны най-ти страны-единомышленники (like-minded countries) в ЕС и НАТО[3]. Лондон намерен выступить «страной-спонсором» диалога между ними как в Евро-Атлантике, так и за её пределами.

Согласно международному Индексу кибербезопасности за 2018 г., Великобритания заняла первое место в рейтинге из 193 стран мира, которые предпринимают наиболее эффективные меры интернет-защиты[4].

Обвинения в адрес России

Британское правительство неоднократно обращало внимание союзников на «агрессивные действия в киберпространстве со стороны Северной Кореи, Ирана, Китая и РФ»[5].

С 2017 г. в Хельсинки начал работу Европейский центр передовых практик по противодействию гибридным угрозам, в работе которого принимают участие страны – члены Евросоюза и НАТО. В рамках указанной структуры британские эксперты ведут мониторинг угроз и проводят исследования по противодействию гибридным атакам, в том числе со стороны России.

По инициативе Лондона противодействие информационным и кибератакам – одна из ве-

[1] Active Cyber Defence – tackling cyber attacks on the UK. URL: https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk (дата обращения: 01.08.2019).
[2] National SecurityCapability Review. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf. P. 6 (дата обращения: 01.08.2019).
[3] Ibid P. 8.
[4] Global Cybersecurity Index (GCI) 2018. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf. P. 62 (дата обращения: 01.08.2019).
[5] Речь премьер-министра Великобритании на банкете лорда-мэра Лондона в 2017 г. URL: https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.ru (дата обращения: 01.08.2019).

дущих тем в двустороннем диалоге со странами Восточной Европы. Например, в ходе первого британо-польского саммита в декабре 2017 г. лидеры двух стран договорились усилить со-трудничество в борьбе с российской дезинформацией. В октябре 2018 г. власти Эстонии заявили о поддержке Соединённого Королевства и Нидерландов в отражении российских кибератак в связи с «делом Скрипалей» и якобы попытками взлома базы данных Организации по запрещению химического оружия[1].

Великобритания продвигает тематику интернет-угроз в отношениях с бывшими колониями. В частности, по итогам саммита Содружества в Лондоне весной 2018 г. британские власти выделили 15 млн ф.ст. на укрепление кибербезопасности в этих странах.

В апреле 2018 г. министерство внутренней безопасности и Федеральное бюро расследований США совместно с Национальным центром кибербезопасности Великобритании опубликовали техническое предупреждение о «вредоносной кибердеятельности российского правительства». По словам директора НЦК С. Мартина «Москва – мощный враг в киберпрост-ранстве, поэтому борьба с ней – главный приоритет Лондона и Вашингтона»[2].

В октябре 2018 г. в рамках расследования «дела Скрипалей»[3], которое власти Британии связывают с деятельностью российских спецслужб, НЦК представил данные о «вредоносной» активности РФ в интернет-пространстве. В обнародованных материалах указано: «атаки совершены в нарушение международного права с целью нанести вред, как обычным гражданам, так и государственным структурам и международным организациям».

По заявлениям администрации Солсбери, городские серверы и аккаунты подверглись массированным кибератакам из-за границы вскоре после отравления С. Скрипаля и его дочери. Согласно Центру правительственной связи Великобритании, источники этих атак в 90% случаев находились за пределами Соединённого Королевства[4].

Британские власти априори возлагают вину за «вредоносную деятельность» в киберпространстве на РФ. Глава Форин Офиса заявил, что «такой образ поведения Москвы свидетельствует о нежелании следовать международному праву и установленным правилам», а с помо-щью незаконной деятельности в интернете Россия стремится влиять на политические процес-сы в зарубежных странах[5].

В мае 2019 г. на конференции по вопросам киберзащиты стран Североатлантического альянса Дж. Хант подчеркнул, что Лондон располагает широкими возможностями противодействовать «злонамеренному вмешательству РФ в дела иностранных государств». По его словам, НЦБ Великобритании ранее передал 16 союзникам по НАТО данные о «российских хакерских угрозах»[6].

Разбирательства о «возможном вмешательстве Москвы в референдум о членстве в ЕС» не дали результатов, однако в британском обществе продолжились дискуссии о том, в какой степени социальные сети воздействуют на общественное мнение и политику[7]. В декабре

[1] Estonia supports UK, Netherlands informing about cyber-attacks. URL: https://news.err.ee/866506/estonia-supports-uk-netherlands-informing-about-cyber-attacks (дата обращения: 01.08.2019).
[2] Joint US UK statement on malicious cyber activity carried out by Russian government. URL: https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government (дата обращения: 01.08.2019).
[3] Ананьева Е.В., Годованюк К.А. Матрёшка «дела Скрипалей». Современная Европа, №3, 2018. С. 16-27.
[4] В Солсбери заявили о кибератаках из-за границы после отравления Скрипаля. URL: https://www.bbc.com/russian/news-48803006 (дата обращения: 01.08.2019).
[5] UK exposes Russian cyber attacks. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks дата обращения: 01.08.2019).
[6] NATO Cyber Defence Pledge conference: Foreign Secretary's speech. URL: https://www.gov.uk/government/speeches/foreign-secretary-speech-at-the-nato-cyber-pledge-conference (дата обращения: 01.08.2019)
[7] Facebook: No new evidence of Russian meddling in Brexit vote. URL: https://www.bbc.com/news/uk-politics-43229969 (дата обращения: 01.08.2019).

2018 г. Комитет по международным делам Палаты лордов порекомендовал правительству «координировать с союзниками работу по противодействию российским дезинформационным кампаниям и гибридным атакам»[1].

«Фейковые новости» и дезинформация

Помимо традиционных СМИ сегодня возрастает влияние интернет- и социальных медиа, что позволяет политически ангажированной или ложной информации напрямую достигать пользователей.

По мере обострения отношений по линии Россия-Запад и перехода «противостояния» в информационную среду, оппоненты Москвы интерпретируют распространение недостоверной информации как инструмент «подрывной», «злонамеренной» и «ревизионистской» деятельности России. Политический истеблишмент коллективного Запада исходит из аксиомы, что Москва стремится разобщить либеральные общества с помощью организованных кампаний по распространению ложных новостей.

Комитет Палаты общин по цифровым технологиям, культуре, СМИ и спорту рекомендовал британскому руководству отказаться от выражения «фейковые новости», а оперировать понятиями «дезинформация» или «недостоверная информация»[2].

В апреле 2019 г. правительство приняло Белую книгу «О вреде онлайн»[3], в которую, по рекомендации депутатов, включило требование к технологическим компаниям по защите интересов пользователей (Duty of care). Данная норма устанавливает ответственность социальных медиа за информационный контент и вскоре должна быть инкорпорирована в британское законодательство.

Власти Великобритании отмечают, что технологические компании, которые обеспечивают работу социальных сетей, не просто представляют собой платформу для общения, но не-сут ответственность за «вредный» контент, опубликованный пользователями. Ещё один важный аспект, на который обращают внимание государственные структуры, – контроль иност-ранного влияния на демократический процесс, включая избирательные кампании.

Правительство Соединённого Королевства выделило типы «вредоносной деятельности» (types of harm), которые подпадают под действие закона. Наряду с террористическим контентом, детской порнографией, информацией, разжигающей ненависть, буллизмом и прочими видами противоправных деяний обозначено распространение дезинформации. Этим понятием обозначают «намеренное создание и распространение недостоверного онлайн контента, который способен нанести вред личным, политическим или финансовым интересам».

Отныне социальные сети будут обязаны обмениваться информацией об иностранном вмешательстве на своих сайтах, проверять сертификаты безопасности, удостоверяющие подлинность учётных записей. Защиту от дезинформации в долгосрочной перспективе, по мнению Лондона, обеспечит высокий уровень цифровой грамотности населения, которая должна быть включена в базовую образовательную программу наряду с чтением, письмом и математикой. Конечная цель – изменить подход людей к обмену информацией в интернете.

[1] UK foreign policy in a shifting world order. December 2018. URL: https://publications.parliament.uk/pa/ld201719/ldselect/ldintrel/250/250.pdf. P. 24.
[2] Disinformation and «fake news»: Final Report. House of Commons Digital, Culture, Media and Sport Committee. 14 February 2019. URL: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf. P. 10 (дата обращения: 01.08.2019).
[3] On-Line Harm White Paper. 2019 г. URL: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#executive-summary (дата обращения: 01.08.2019).

На основе изученных данных был разработан комплекс мер против дезинформации «Противодействие» (RESIST), который предусматривает шесть шагов: обнаружение, ранее предупреждение, ситуационное осмысление, анализ её воздействия, стратегическую коммуникацию, отслеживание последствий[1].

Очевидно, что методы противодействия недостоверной информации должны сочетаться с принципами свободы слова, а также с задачей сохранить доверие между СМИ, общест-вом и государством. Именно с этой целью 10-11 июля 2019 г. в Лондоне под эгидой британского правительства и министерства иностранных дел Канады состоялась первая глобальная конференция по защите свободы СМИ[2]. Российские информационные агентства RT и Sput-nik, которые власти Соединённого Королевства неоднократно обвиняли в распространении «фейковых новостей» и «пропаганды», не были допущены на конференцию.

По итогам форума глава внешнеполитического ведомства Канады Х. Фриланд и её британский коллега объявили о создании коалиции стран-единомышленников, которые намерены сотрудничать в структурах ООН, контактных группах, а также при помощи специального Фонда защиты свободы СМИ с целью обеспечить достоверный информационный контент.

Выводы

Великобритания занимает передовые позиции в сфере обеспечения кибербезопасности, что позволяет ей выдвинуть эту тематику как ключевую для глобальной повестки стран-единомышленников.

Лондон использует дискурс о кибератаках и гибридных угрозах со стороны России, а также потенциал противостоять им как козырь в переговорах с партнёрами по Европейскому союзу и НАТО. В среднесрочной перспективе данная тематика останется центральной на российском направлении, а также в диалоге по вопросам безопасности со странами Восточной и Северной Европы и Западных Балкан.

Дискурс о противодействии недостоверной информации в традиционных и социальных медиа помогает Великобритании объединить вокруг себя союзников на глобальном уровне (США, Канаду, Австралию и пр.) в рамках инициатив по защите либерального мирового порядка. Такие шаги отвечают курсу Лондона на «Глобальную Британию», способную, по замыслу брекзитёров, обеспечить Соединённому Королевству ведущие международные позиции после выхода из ЕС.

Новый глава Кабинета Б. Джонсон, очевидно, продолжит линию предыдущего правительства по регулированию информационного контента и мерам кибербезопасности. Так, 1 августа 2019 г. в британских СМИ были обнародованы данные о специальном подразделении британской армии, в задачи которого вошла борьба с гибридными угрозами и кибератакам, которые якобы «исходят от РФ» и различных террористических группировок[3].

Первым международным мероприятием с участием нового главы МВД П. Пател был

[1] RESIST: Counter-Disinformation Toolkit. URL: https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/ (дата обращения: 01.08.2019).

[2] Foreign Secretary sets out his vision to improve media freedom around the world. URL: https://www.gov.uk/government/speeches/foreign-secretary-sets-out-his-vision-to-improve-media-freedom-around-the-world (дата обращения: 01.08.2019).

[3] Cyber Warfare: Army Deploys «Social Media Warfare» Division To Fight Russia. URL: https://www.forbes.com/sites/zakdoffman/2019/08/01/social-media-warfare-new-military-cyber-unit-will-fight-russias-dark-arts/?ss=cybersecurity&fbclid=IwAR2j_7UEPuBQH_8rbKWn61MFJDpOMNliFZRn2xKbL38oxDVVGHfNhIznUtM#789571a24f6e (дата обращения: 01.08.2019).

саммит по вопросам безопасности Альянса «Пять глаз» (США, Великобритания, Канада, Австралия и Новая Зеландия) в Лондоне 29-31 июля. Союзники подтвердили намерение совместно противодействовать современным угрозам, источниками которых, в частности, выступают новейшие технологии, например мобильные системы пятого поколения и киберпространство[1].

Список литературы

Потемкина О.Ю. Проблема регулирования социальных сетей накануне выборов в Европейский парламент. Современная Европа, №2, 2019. С. 50-62.

References

Disinformation and «fake news»: Final Report. House of Commons Digital, Culture, Media and Sport Committee. 14 February 2019. URL: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Potemkina O.Yu. Problema regulirovaniya social'nyh setej nakanune vyborov v Evropejskij parlament. Sovremennaya Evropa, №2, 2019. S. 50-62.

Prince C., Sullivan J. The UK Cyber Strategy Challenges for the Next Phase. Royal United Services Institute for Defence and Security Studies. 2019. URL: https://rusi.org/sites/default/files/20190627_the_uk_cyber_strategy_web.pdf.

Cybersecurity and combating disinformation: UK case

Author. **Kira Godovanyuk**, Candidate of Sciences (Politics), Senior Research Associate at the UK Studies Center, Department of Countries Studies, Institute of Europe Russian Academy of Sciences. **Address**: 11-3, Mokhovaya str., Moscow, Russia, 125009; **E-mail**: kira.godovanyuk@gmail.com.

Abstract. In the aftermath of the EU membership referendum, the UK's government undertook some initiatives in order to update its international agenda. According to the British political establishment, the UK best practices in countering cyber threats, foreign meddlings and disinformation campaigns can ensure London's special status in cooperation with like-minded countries not only within the EU and NATO but beyond the Euro-Atlantic. The article considers British initiatives in information content regulations including recently adopted «Online Harms» White Paper and Global Conference on Mass Media Freedom hosted in London in July 2019. The author concluded that the majority of the measures by the UK government should be considered in the broader context of searching a new global role in countering hybrid threats. The latter, according to London, comes from the countries aiming to undermine the liberal world order.

Key words: Britain, B. Johnson, cyber security, cyber-attacks, disinformation, fake news, hybrid threats, social media, European Union, NATO, Russia, Brexit.

DOI: http://dx.doi.org/10.15211/vestnikieran420198792

[1] Home Secretary hosts «Five Eyes» security summit. URL: https://www.gov.uk/government/news/home-secretary-hosts-five-eyes-security-summit (дата обращения: 01.08.2019).