УДК 327.5
JEL Classification: D 780; F 420

Гусейнова Сура

ПИТАННЯ ЗОВНІШНЬОПОЛІТИЧНОГО ВИМІРЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті аналізуються проблеми формування механізму щодо забезпечення міжнародної інформаційної безпеки в умовах глобалізаційних викликів і загроз. Автор доводить, що проблематика міжнародної інформаційної безпеки трансформувалася з чисто технологічної у військово-політичну і стала одним з ключових мегатрендів світової політики.

Справедливо відзначається, що технологічний дизайн дозволяє забезпечити нейтральність інтернет-технологій, які об'єднують одночасно безліч локальних мереж. Підкреслюючи те, що особливу небезпеку тут представляє так звана «мережева нейтральність», яка передбачає, що провайдери зобов'язані надавати доступ всім користувачам до всіх ресурсів на рівних умовах, блокувати трафік того чи іншого сайту або стягувати додаткову плату за збільшену швидкість доступу.

Відзначається, що з огляду на інтенсивне зростання конфліктного потенціалу в світі і посилюється протиборство в глобальному інформаційному просторі, зростають ризики використання міжнародними акторами інформаційно-комунікаційних технологій в досягненні своїх геополітичних цілей шляхом маніпулювання суспільною свідомістю на глобальному рівні.

Основний нормативною базою в цій області автор вважає, прийнятої Генасамблеєю ООН у вересні 2015 р резолюції «Перетворення нашого світу: Порядок денний в галузі сталого розвитку на період до 2030 р» мета №9, де пов’язано вдосконалення ІКТ зі стійким розвитком всієї світової спільноти . В умовах Четвертої промислової революція відбувається конвергенція технологій, яка розмиває кордони між фізичною, цифровою та біологічною сферами як у віртуальному просторі, так і в реальній практиці світової

взаємодії.

Відповідно розширюється і трансформується простір виконання державами зовнішньополітичних завдань у вирішенні проблем підтримки міжнародної інформаційної безпеки.

У статті досліджується діяльність Групи урядових експертів ООН з інформаційної безпеки. Вперше описується дискурс загроз конвергенцій нано, біо, інфо та когнітивних технологій NBIC в політико-стратегічних і соціально-медійних напрямках.

Ключові слова: виклики, міжнародна та інформаційна безпека, зовнішня політика, вимір, світова політика, ризики.

Huseynova Sura

QUESTIONS FOR FOREIGN POLICY DIMENSION OF INFORMATION SECURITY

The article analyzes the problems of forming a mechanism for ensuring international information security in the context of globalization challenges and threats. The author argues that the problems of international information security have transformed from a purely technological to a military-political one and have become one of the key megatrends of world politics.

It is rightly noted that the technological design allows to ensure the neutrality of Internet technologies that simultaneously unite many local networks. Emphasizing that the special danger here is the so-called “network neutrality”, which implies that providers are obliged to provide access to all users to all resources under equal conditions, block the traffic of a particular site or charge extra for increased access speed.

It is noted that, given the intensive growth of the conflict potential in the world and the growing confrontation in the global information space, the risks of using information and communication technologies by international actors to achieve their geopolitical goals by manipulating public consciousness at the global level are increasing.

The author considers the resolution “Transforming our world:

the Sustainable Development Agenda for the period up to 2030" as the main regulatory framework in this area in September 2015, which aims to improve ICT with the sustainable development of the entire global community. Under the conditions of the Fourth Industrial Revolution, there is a convergence of technologies that blurs the boundaries between the physical, digital and biological spheres both in the virtual space and in the actual practice of global interaction. Accordingly, the space for the fulfillment by states of foreign policy tasks in solving problems of maintaining international information security is expanding and transforming.

The article explores the activities of the UN Group of Governmental Information Security Experts. For the first time, the discourse of threats to convergence of nano, bio, info and cognitive technologies of NBIC is described in political-strategic and social-media directions.

***Key words*:** challenges, international, information, security, foreign policy, measurement, global politics, risks.

Гусейнова Сура

ВОПРОСЫ ВНЕШНЕПОЛИТИЧЕСКОГО ИЗМЕРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье анализируются проблемы формирования механизма по обеспечению международной информационной безопасности в условиях глобализационных вызовов и угроз. Автор доказывает, что проблематика международной информационной безопасности трансформировалась из чисто технологической в военно-политическую и стала одним из ключевых мегатрендов мировой политики.

Справедливо отмечается, что технологический дизайн позволяет обеспечить нейтральность интернет-технологий, объединяющих одновременно множество локальных сетей. Подчеркивая то, что особую опасность здесь представляет так называемая «сетевая нейтральность», которая предполагает, что провайдеры обязаны предоставлять доступ всем пользователям ко всем ресурсам на равных условиях, блокировать трафик того

или иного сайта или взимать дополнительную плату за увеличенную скорость доступа.

Отмечается, что учитывая интенсивный рост конфликтного потенциала в мире и усиливающееся противоборство в глобальном информационном пространстве, возрастают риски использования международными актерами информационно-коммуникационных технологий в достижении своих геополитических целей путем манипулирования общественным сознанием на глобальном уровне.

Основной нормативной базой в этой области автор считает, принятой Генассамблеей ООН в сентябре 2015 г. резолюции «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 г.» цель №9, где связывается совершенствование ИКТ с устойчивым развитием всего мирового сообщества. В условиях Четвертой промышленной революция происходит конвергенция технологий, которая размывает границы между физической, цифровой и биологической сферами как в виртуальном пространстве, так и реальной практике мирового взаимодействия. Соответственно расширяется и трансформируется пространство выполнения государствами внешнеполитических задач в решении проблем поддержания международной информационной безопасности.

В статье исследуется деятельность Группы правительственных экспертов ООН по информационной безопасности. Впервые описывается дискурс угроз конвергенций нано, био, инфо и когнитивных технологий NBIC в политико-стратегических и социально-медийных направлениях.

Ключевые слова: вызовы, международная и информационная безопастность, внешняя политика, измерение, мировая политика, риски.

DOI: 10.32680/2409-9260-2019-3-266-73-84

Постановка проблемы. На современном этапе Интернет выступает глобальным виртуальным электронный рынком, который не разделяют ни территориальные, ни временные границы. Несомненно, пользователи разных

регионов мира имеют свои особенности и различия, которые учитываются при составлении программ воздействия, но именно Интернет способствует реализации политических стратегий с четко выраженными географическими регионами, с учетом временных зон и специфики аудитории. Доминантой назначения Интернет технологий становится реализация национальных интересов, определяемая их возможностью влиять на политические решения, управлять массовым сознанием путем концентрированного информационного воздействия на социум как в национальных, так и в глобальных параметрах.

Анализ последних исслдований и публикаций. Значимость Интернета как ключевой инфраструктуры информационной безопасности подтверждается масштабами его использования. Число пользователей Интернета постоянно увеличивается – если в начале 2008 г. насчитывалось 1.4 млрд. пользователей, то в 2017 г. уже 3.7 млрд. человек, то есть почти половина всего населения [1].

Информационные ресурсы отдельных пользователей все чаще хранятся в так называемых «серверных фермах». Облака создают и предоставляют для размещения данных такие гиганты информационного рынка, как Google, Apple, Microsoft, Amazon и Facebook. В результате Интернет приобретает трансграничную архитектуру, все материалы которой хранятся у по сути в нескольких странах, в основном в США. Распространение «облачных» технологий хранения и обработки данных позволяет получить максимальный доступ к самым секретным материалам, что вызывает новые угрозы международной и национальной информационной безопасности.

Для понимания тех угроз, которые процессы информатизации привносят в систему международных отношений, необходимо отметить сложную и неоднородную макросистему Интернета, объединяющую значительное количество информационных сетей. Масштабы покрытия Интернета, влияние сети на мировое сообщество дают возможность полагать большинству экспертов что дальнейшее

развитие данной структуры без какого-либо урегулирования и контроля невозможно [2]. Существуют так же экспертные заключения о том, что мониторинг деятельности пользователей — это целенаправленное ограничение их свобод и конституционных прав. На данный момент существуют три основные державы в контексте разрешения проблем кибер безопасности – это Китай, Россия и Соединенные Штаты. Не секрет, что эти страны отличаются как по своим позициям в вопросах безопасности, так и по степени открытости Интернет-пространства.

Формулировка цели статьи. В статье рассматриваются вопросы внешнеполитического измерения информационной безопасности с целью рассмотрения механизма по обеспечению международной информационной безопасности в условиях глобализационных вызовов и угроз.

Изложение основного материала исследования.

Технологический дизайн позволяет обеспечить нейтральность интернет- технологий, объединяющих одновременно множество локальных сетей. Особую опасность представляет так называемая «сетевая нейтральность», которая предполагает, что провайдеры обязаны предоставлять доступ всем пользователям ко всем ресурсам на равных условиях, блокировать трафик того или иного сайта или взимать дополнительную плату за увеличенную скорость доступа. Концепция сетевого нейтралитета была введена в США в 2015 году при личной поддержке президента Барака Обамы. Однако в мая 2018 года Федеральная комиссия по связи (FCC) на слушаниях в Конгрессе США доказала угрозы сетевого нейтралитета не только для информационной, но и всей национальной безопасности страны. Более 80 тыс. веб-сайтов, включая платформы интернет-гигантов Facebook, Amazon и Google, приняли участие в онлайн-протесте против плана Комиссии по коммуникациям отменить принцип сетевой нейтральности. Тем не менее несмотря на широчайший общественный протест с 11 июня 2018 года в США не действует принцип сетевого нейтралитета как мера, обеспечивающая национальную безопасность именно США, так

как высокий уровень сетезависимости США создает ситуацию, когда Америке угрожают и технологически менее развитые страны [3].

В политической прогностике США уже практически с краха биполярной системы международных отношений разрабатываются сценарии «мировой информационной войны» как вполне вероятные вследствие агрессивного или иного враждебного использования как самой информации, так и современных информационно-коммуникационных технологий [4, 5, 6]. Учитывая интенсивный рост конфликтного потенциала в мире и усиливающееся противоборство в глобальном информационном пространстве, возрастают риски использования международными акторами информационно-коммуникационных технологий в достижении своих геополитических целей путем манипулирования общественным сознанием на глобальном уровне.

В принятой Генассамблеей ООН в сентябре 2015 г. резолюции «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 г.» цель №9 связывает совершенствование ИКТ с устойчивым развитием всего мирового сообщества. В условиях Четвертой промышленной революция (Industry 4.0) происходит конвергенция технологий, которая размывает границы между физической, цифровой и биологической сферами как в виртуальном пространстве, так и реальной практике мирового взаимодействия. Соответственно расширяется и трансформируется пространство выполнения государствами внешнеполитических задач в решении проблем поддержания международной информационной безопасности.

Цифровое развитие в глобальных масштабах формирует новые тенденции в обеспечении как информационной безопасности на национальном и международном уровне. Разработка и внедрение новейших когнитивных информационно-аналитических и геоинформационных систем в управление национальной безопасностью развитых стран вызвало обострение глобальной конкуренции. На Варшавском саммите Североатлантического

альянса в 2018г. отмечалось: «государства -члены НАТО вправе защищаться от нападения других стран, Это касается не только прямого вторжения солдатами в форме, но и атак, проводимых нетрадиционными способами - информационных операций, действий в киберпространстве» [7]. На Варшавском саммите была разработана новая стратегия усиления эффективности реагирования специальных военных сил альянса на нетрадиционные угрозы, в том числе, и в сфере информационной безопасности.

Наиболее эффективным ответом на информационную атаку противника считается метод «сдерживания геополитических соперников» [8, p.56], который проявляется в агрессивной демонстрации в информационном пространстве милитаристских возможностей, а при необходимости и применении военной силы. Острая проблема возможного «поигрывания технологическими мускулами» беспрецедентно обостряет международные отношения, выдвигая проблему баланса принципов «сдержек и противовесов» в качестве доминирующей в обеспечении безопасности. Сложность обозначенной проблемы подтвердила Группы правительственных экспертов ООН по достижениям в области информатизации и коммуникации, особо подчеркнув, что феномен стремительного развития ИКТ охватил сегмент международных отношений. [9]. Тем не менее, весьма показателен, на наш взгляд, сам факт того, что Группа, которая действует в разном составе с 2004 года, до настоящего времени так и не смогла определить направления международного сотрудничества в сфере информационно-коммуникационных технологий вследствие постоянного нарастания и трансформации угроз информационной безопасности.

Современные информационные ресурсы и информационная инфраструктура отличаются от других аналогичных объектов, регулируемых международном и национальном правом, уникальными свойствами делимости и воспроизводимости. Специфические пространственно-временные характеристики информационных ресурсов не ограничиваются пределами национальной территории и

формируют способность геополитического субъекта к устойчивому развитию. Потенциал подавления или снижения возможностей информационных ресурсов выступает предметом конкуренции на международной арене

Достижение геополитических конкурентных преимуществ в информационном пространстве в форме превосходства в информационных технологиях и производстве инновационной продукции невозможно без осуществления контроля над развитием всей глобальной инфраструктуры информационного пространства [10, с.26]. При этом в качестве основных категорий такого возможного контроля, обеспечивающего информационную безопасность суверенного государства, можно, как нам представляется, выделить следующие базовые индикаторы:

– продолжительность создания информационного продукта;

– уровень влияния информационного продукта на стратегическую стабильность и устойчивое развитие государства;

– создание условий для технологического лидерства государства в сфере ИКТ.

– следует отметить, что конкретными возможностями реализации контроля над развитием глобальной инфраструктуры информационного пространства располагают только те государства, которые способны создавать и производить:

– компоненты и комплектующие для обработки в заданных режимах информационных потоков;

– оборудование для формирования и функционирования информационных баз данных, современных средств коммуникаций и управления сетями связи;

– новейшие вычислительные процессоры и устройства мобильной связи;

– совместимые программные платформы и многое другое.

– по всем вышеперечисленным показателям доминантная роль принадлежит США, так как на ее

территории расположены штаб-офисы ведущих компаний IT-индустрии, представляющих более половины поставок информационных технологий во всем мире [11].

В обобщенном виде информационно- технологические угрозы современному мировому порядку и режиму международной безопасности проявляются в следующих направлениях

– в военно-политической сфере с целью реализации в виртуальном пространстве разного рода враждебных актов и агрессивных действии, попирающих императивные принципы международного права, такие, как территориальная целостность, нерушимость границ и дискредитирующих государственный суверенитет;

– в военно-информационной сфере с целью распространения вредоносных компьютерных программ и вирусов неконтролируемого доступа к информационным системам военно-стратегического и оборонного характера,

– в сфере государственного управления с целью неконтролируемого вмешательства в процесс функционирования критически важных объектов инфраструктуры суверенного государства, которое ведет к необратимым негативным изменениям, вплоть до разрушения экономики страны и жизнедеятельности ее населения;

– в медийной сфере с целью формирования деструктивных сетевых сообществ, пропагандирующих терроризм, экстремизм, сепаратизм, привлекающих сторонников этих антигуманных идеологий и вербующих участников незаконных вооруженных формирований;

– в сфере социально- политической стабильности с целью вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды насилия, расистских и ксенофобских идей.

Выводы. На основе анализа проблем формирования механизма по обеспечению международной информационной безопасности в условиях глобализационных вызовов и угроз, доказано, что проблематика международной информационной

безопасности трансформировалась из чисто технологической в военно-политическую и стала одним из ключевых мегатрендов мировой политики. При этом, технологический дизайн позволяет обеспечить нейтральность интернет-технологий, объединяющих одновременно множество локальных сетей. Обосновано, что особую опасность здесь представляет так называемая «сетевая нейтральность», которая предполагает, что провайдеры обязаны предоставлять доступ всем пользователям ко всем ресурсам на равных условиях, блокировать трафик того или иного сайта или взимать дополнительную плату за увеличенную скорость доступа. Отмечается, что учитывая интенсивный рост конфликтного потенциала в мире и усиливающееся противоборство в глобальном информационном пространстве, возрастают риски использования международными актерами информационно-коммуникационных технологий в достижении своих геополитических целей путем манипулирования общественным сознанием на глобальном уровне.

Литература

1. 118 Internet World Stats. Usage and population statistics. URL:www.internetworldstats.org
2. Цензура (контроль и анонимность) в интернете. Мировой опыт http://www.tadviser.ru/index.php
3. The US Senate votes in favor of restoring the FCC's net-neutrality rules/www.businessinsider.com/net-neutrality-2018
4. Andrew Krepinevich.7 Deadly Scenarios: A Military Futurist Explores the Changing Face of War in the 21st Century. Bantam, August 31, 2010
5. Baird D., Nordmann A. & Schummer J. (eds.), Discovering the Nanoscale, Amsterdam: IOS Press, 2004.
6. Dorothy E. Denning. Information Warfare and Security. Oxford. UK, 2005
7. Nato’s Warsaw summit is a test the west must pass. www.ft.com/content/f36c7b2a-3f7d-11e6-9f2c
8. Кларк Р., Найк Р. Третья мировая война. Какой она

будет? Высокие технологии на службе милитаризма. С-П., Питер, 2011.

9. Towards a secure cyberspace via regional cooperation.https://dig.watch/processes/ungge

10. Смирнов. А.И. Современные информационные технологии в международных отношениях. М., МГИМО-Университет, 2017.

11. The 25 Largest Internet Companies In The World www.worldatlas.com/articles/

8. Clark, R., Nike, R. (2011) *Tret'ya myrovaya voyna. Kakoy ona budet? Vыsokye tekhnolohyy na sluzhbe mylytaryzma. [The Third World War. What will it be? High technology in the service of militarism]*. St. Petersburg: Peter. [in Russian].

10. Smirnov, A.I. (2017) *Sovremennыe ynformatsyonnыe tekhnolohyy v mezhdunarodnыkh otnoshenyyakh [Modern information technology in international relations]*. Moscow: MGIMO-University. [in Russian].

25.04.2019

УДК 658:65.012.8
JEL Classification: D 830

Король Володимир

ОРГАНІЗАЦІЯ ПРОЦЕСУ ФОРМУВАННЯ АНАЛІТИЧНОЇ ІНФОРМАЦІЇ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті визначено елементи інформаційно-аналітичного забезпечення економічної безпеки промислових підприємств.

Виокремлено методичні способи, що застосовуються для інформаційного забезпечення системи економічної безпеки підприємства. Охарактеризовано особливості організації обліково-аналітичної діяльності на підприємстві.