Элмахжуб Абдалла Омар Абдалла, асп.
Киевский национальный университет имени Тараса Шевченко, Киев, Украина

ЭСКАЛАЦИЯ ЛИВИЙСКОГО КРИЗИСА В 2019 ГОДУ И ПОЛИТИКА КЛЮЧЕВЫХ МЕЖДУНАРОДНЫХ АКТОРОВ ПО ЕГО УРЕГУЛИРОВАНИЮ

Проанализированы геополитические интересы и позиции международных акторов, привлеченных к решению кризиса в государстве Ливия. Сделан вывод, что основными мотивами внешних сил относительно их участия в урегулировании ситуации в стране являются важное геостратегическое расположение Ливии, ее огромные нефтяные запасы и значительные разведанные запасы природного газа в ливийском секторе Средиземного моря, а основными игроками на "ливийском поле" являются, с одной стороны, Европейский Союз и США, с другой – Россия, Объединенные Арабские Эмираты и Египет. Особую позицию в вопросе решения ливийского кризиса занимает член НАТО – Турция. В геополитическом соревновании названных выше международных акторов, по мнению автора, и будет решена судьба Ливии.

Ключевые слова: ливийский кризис, гражданская война, Ливийская национальная армия, Правительство национального согласия, геополитические интересы, международные акторы, посредническая война.

УДК 327:[351.746:316.77-049](73)(045)

М. Гринчук, асп.
Київський національний університет імені Тараса Шевченка, Київ, Україна

КОМУНІКАТИВНА СКЛАДОВА БЕЗПЕКОВОЇ ПОЛІТИКИ США: ПОЛІТИКО-ПРАВОВИЙ АСПЕКТ

Розглянуто основні аспекти комунікативної сфери в процесі забезпечення національної безпеки урядом Сполучених Штатів Америки. Проаналізовано низку законодавчо-правових актів США у сфері інформаційно-комунікативного забезпечення безпекової політики. Виявлено, що політичні комунікації та одна з найбільш глобальних загроз національної безпеки США, тероризм, нерозривно пов'язані. Підкреслено важливість кібербезпеки як невід'ємного елемента забезпечення національної безпеки загалом.

Ключові слова: комунікації, національна безпека США, інформаційно-комунікативні технології.

Постановка проблеми. Стрімкий розвиток інформаційно-комунікативних технологій призвів до того, що на сьогоднішній день неможливо уявити ефективне регулювання будь-якої сфери без залучення відповідних комунікативних та інформаційних заходів. Особливо це стосується політичної сфери, яка потребує залучення передових технологій у даній галузі задля можливості конкурування на міжнародній арені та забезпечення національної та міжнародної безпеки. Навмисний або випадковий вплив на інформаційні ресурси, що включають у себе як власне інформацію, так і технології, може обернутися серйозною загрозою для національної безпеки держави.

Сполучені Штати Америки як один з найбільш могутніх політичних, економічних і військових акторів сучасних міжнародних відносин мають досить розвинену систему комунікацій у політичній сфері, включаючи також безпекову. Багато в чому міць США зумовлена активним розвитком і впровадженням інформаційних та комунікативних технологій у різні сфери суспільного життя.

Мета статті – розглянути та проаналізувати основні аспекти комунікативного процесу уряду Сполучених Штатів Америки у сфері безпекової політики та визначити роль і значущість даного напряму. Дослідження передбачає вивчення базової законодавчої та правової бази уряду США у сфері забезпечення міжнародної та національної безпеки.

Аналіз останніх досліджень і публікацій. Проблематика інформаційно-комунікативних технологій та їх взаємозв'язок із політичною сферою вже досліджувались низкою зарубіжних і вітчизняних вчених. Одними з основних зарубіжних вчених, що зробили вагомий внесок у розвиток даної сфери, є С. Бьорд, Д. Джонс, С. Джонсон, Д. Мерфі, К. Халлаген, Д. Гольцхаузен та ін. Серед українських вчених можна відзначити С. Даниленка, Г. Почепцова, М. Ожевана, М. Рижкова, Є. Макаренко, О. Шевченко, Н. Піпченко та ін.

Основні результати дослідження. У широкому сенсі безпека визначається як незагрозливий стан.Тривалий час безпека передбачала відсутність війни, а загрози мали переважно військово-політичний характер. Однак із часом поняття безпеки зазнало суттєвих змін. Відбулося розширення суб'єктної та предметної сфер безпеки. Наприклад, у ролі суб'єктів міжнародної безпеки наразі виступають не тільки держави, а й нові актори – терористичні мережі, транснаціональні злочинні угруповання, приватні військові компанії. Також з'явились нові невійськові загрози – екологічна, економічна, інформаційна та ін. Утім, забезпечення національної безпеки є одним із пріоритетних завдань, що поставлені перед державою. Державна безпека – це захищеність інтересів особистості, суспільства і держави від різноманітних загроз у всіх сферах життєдіяльності. Сполучені Штати Америки під національною безпекою розуміють стан захищеності держави від ворожих актів чи інших втручань, у тому числі від внутрішніх загроз. Звичайно, ефективне здійснення безпекової політики неможливе без налагодженої системи комунікацій.

Політичні комунікації відіграють одну з ключових ролей у даному питанні. Під політичними комунікаціями розуміється система цілеспрямованого і багатофункціонального інформаційного обміну та взаємодії між суб'єктами і об'єктами політики, за допомогою яких забезпечуються вироблення і прийняття рішень, стратегічне планування, формування громадської думки та реалізація політичних цілей і завдань, у тому числі у сфері національної та військової безпеки [1]. Зростання ролі засобів масової інформації як засобу реалізації сучасної політичної влади є помітною тенденцією функціонування політичної комунікації в забезпеченні військової безпеки держави. У сучасному світі саме масова політична комунікація забезпечує трансляцію і взаємообмін інформацією між політичною і соціальною системами, а засоби масової інформації є найважливішим політичним інститутом. Одна з найбільш глобальних загроз національної безпеки США, тероризм, нерозривно пов'язаний із політичними комунікаціями, адже терористи здатні впливати на державу через створення громадської думки, що формується за допомогою комунікацій. Держава, що втрачає контроль над політичними комунікаціями, стає вразливою щодо інформаційного впливу ззовні. У цих умовах терористи набувають здатності мати вирішальний вплив на прийняття важливих державних рішень, у тому числі у військово-політичній

сфері. Якщо визначити комунікацію як обмін інформацією між двома або більше індивідами або групами, то комунікативний аспект терористичної діяльності можна описати як процес обміну інформацією між терористичною організацією та її внутрішньою і зовнішньою аудиторіями. До зовнішньої аудиторії терористів можна віднести державні влади, силові структури, представників ЗМІ та громадських організацій, а також потенційно нових терористів і прихильників. Як засіб передання повідомлень терористи використовують самі теракти (завдяки резонансу в ЗМІ), розсилки комюніке в редакції, роботу в соціальних мережах і на інтернет-форумах, свої власні сайти та багато іншого. Усі ці заходи включаються в комунікативну стратегію, кінцевою метою якої може бути зміна державного законодавства, зміщення політичного лідера чи примушення влади до прийняття вигідних для терористів рішень. Тому антитерористичні структури також мають використовувати новітні методи комунікації задля мінімізації впливу терористів у інформаційному просторі. Заходи інформаційної протидії тероризму можуть включати використання кризових комунікацій та превентивної інформаційно-комунікативної діяльності [2].

Задля забезпечення безпеки уряд Сполучених Штатів Америки також приділяє велику увагу стратегічним комунікаціям. Визначення даному терміну можна знайти в документі під назвою "Національні рамки стратегічних комунікацій" (National Framework for Strategic Communications), де визначено, що стратегічні комунікації є синхронізацією слів та дій, а також цілеспрямованими зусиллями з комунікацій та взаємодії з цільовими аудиторіями [3]. У Держдепартаменті функціонує Управління стратегічних комунікацій (Office of Strategic Communications and Outreach), яке підтримує Бюро міжнародної безпеки і нерозповсюдження шляхом відповідних зусиль у сфері публічної дипломатії, зв'язків із громадськістю та взаємодії з конгресом [4]. У системі підрозділів, що функціонують під загальним керівництвом заступника Держсекретаря з питань громадської дипломатії та зв'язків з громадськістю, з 2011 по 2016 рік діяв Центр стратегічних антитерористичних комунікацій (Center for Strategic Counterterrorism Communications), завданням якого була координація міжнародних комунікацій уряду США у сфері боротьби з тероризмом і екстремізмом. Починаючи з 2016 року, його функції виконує Центр глобальної взаємодії (Global Engagement Center), метою якого є координація дій уряду США з боротьби з пропагандою і дезінформацією іноземних держав і терористичних організацій [5].

Особлива увага урядом США приділяється кібербезпеці як невід'ємному елементу забезпечення національної безпеки в цілому. У доповіді Комісії з кібербезпеки у 2008 році прямо підкреслювалось, що нездатність США захистити кіберпростір є однією з найбільших проблем національної безпеки. А у 2013 році вперше, згідно з "Оцінкою глобальних загроз розвідувального співтовариства США" (Worldwide Threat Assessment of the US Intelligence Community), кіберзагроза стала головним пріоритетом національної безпеки США, випередивши загрозу номер один останньої декади – тероризм [6]. У 2018 році президент США Дональд Трамп підписав "Національну стратегію кібербезпеки", попередні версії якої були опубліковані у 2003 та 2011 роках. У документі, зокрема, зазначається, що адміністрація уповноважує Міністерство внутрішньої безпеки на забезпечення безпеки федеральних міністерських та відомчих мереж, за винятком систем національної безпеки, Міністерства оборони і систем розвідувального співтовариства. До необхідних заходів, у тому числі, належить забезпечення Міністерства внутрішньої безпеки відповідним доступом до відомчих інформаційних систем з метою кібербезпеки, яке також може вести діяльність і давати розпорядження щодо захисту систем від ризиків [7].

Звичайно, соціальні мережі також є надзвичайно важливим аспектом комунікацій у сфері забезпечення безпекової політики. Передусім ідеться про захист від дезінформації та забезпечення доступу громадян до актуальної та достовірної інформації, адже неправдива інформація може завдати істотної шкоди всьому суспільству. У 2006 році було створено Команду з цифрових зовнішніх контактів (Digital Outreach Team), до завдань якої входила участь у дискусіях із питань зовнішньої політики США з користувачами популярних сайтів арабською та перською мовами, а також урду. Згідно з інформацією Бюро міжнародних програм, місія команди полягає в роз'ясненні зовнішньої політики США і боротьбі з дезінформацією. Доречі, подібні відділи були створені також у Міністерстві оборони, ЦРУ і Агентстві міжнародного розвитку. Їх представники моніторять дискусії у всіх можливих міжнародних і національних соціальних мережах та формують відповідні реакції на негативну інформацію про США [8]. На офіційному сайті Департаменту внутрішньої безпеки Сполучених Штатів Америки є окремий розділ, присвячений соціальним мережам, де користувачі можуть легко знайти інформацію стосовно офіційних акаунтів Департаменту в таких сервісах, як Twitter, Facebook, Flickr, Instagram, LinkedIn та ін. [9].

У системі взаємовідносин інформаційно-комунікативних технологій та національної безпеки особливе місце займає проблема інформаційної безпеки, породжена значною мірою процесами бурхливого розвитку новітніх технологій і формуванням інформаційного суспільства. У Національному плані захисту інфраструктури (National Infrastructure Protection Plan) поняття інформаційної безпеки визначається як комплекс заходів, спрямованих на захист комп'ютерів, цифрових даних і мереж від несанкціонованого доступу і дій, пов'язаних із маніпулюванням, крадіжкою, псуванням, блокуванням, знищенням умисно або випадково [10].

В умовах інформатизації суспільства повсякденним стало прагнення певних суб'єктів до одноосібного володіння інформаційними ресурсами, засобами і технологіями та їх використання з метою задоволення власних інтересів і протидії інтересам імовірних конкурентів у економічній, політичній, військовій та інших сферах. Інформаційно-комунікативні технології при цьому можуть бути використані для формування і реалізації відповідних загроз інтересам конкурентів. У процесі забезпечення національної безпеки Сполучені Штати Америки приділяють значну увагу регламентації функціонування комп'ютерних та інших інформаційних систем. Основою забезпечення кібербезпеки у США є існування потужної технологічної бази. У 2018 році Рада національної безпеки США запропонувала розгорнути на території країни швидкісну телекомунікаційну мережу п'ятого покоління (5G) для протидії загрозі з боку Китаю [11]. Раніше у Стратегії національної безпеки адміністрації президента США Дональда Трампа, опублікованій 18 грудня 2017 року, Китай був визнаний державою-ревізіоністом, що загрожує безпеці США [12]. Тому в березні 2020 року Сполучені Штати Америки оприлюднили Національну стратегію захисту 5G (National Strategy for 5G Security). У документі представлено "бачення президента США щодо розвитку та управління надійною комунікативною інфраструктурою 5G разом із партнерами та союзниками" [13].

Останнім часом занепокоєння щодо безпеки інформаційного простору викликають умови, за яких проходитимуть вибори нового президента США у 2020 році. У березні 2020 року спеціальна Комісія з питань кіберпростору (Cyberspace Solarium Commission) опублікувала

доповідь щодо безпеки у цифровому середовищі, у якому було запоновано призначити урядового координатора з питань кібербезпеки, а також застосовувати на виборах прості й перевірені технології, зокрема голосування паперовими бюлетенями [14]. Експерти також відзначили значне зростання інтернет-шахрайства. Були випадки, коли зловмисники розсилали фішингові повідомлення, що містили різноманітні посилання з приблизно таким повідомленням: "Дізнайтесь, як захиститися від коронавірусу". Насправді ж дані посилання ведуть на сторінки тих, хто має намір отримати доступ до ваших особистих даних [15]. Ураховуючи стратегічне значення інформаційних ресурсів у сучасному світі, проблема безпеки інформації стала пріоритетом внутрішньополітичного регулювання і міжнародних відносин. Підтвердженням цього є той факт, що 15 травня 2019 року президент США Дональд Трамп підписав указ "Про забезпечення безпеки поставок інформаційно-комунікативних технологій і послуг", який дозволить його адміністрації блокувати іноземним технологічним компаніям можливості ведення бізнесу в США, якщо вони загрожують національній безпеці. Президент також зазначив, що іноземні противники все частіше створюють і використовують уразливості в інформаційно-комунікативних технологіях, де зберігається і передається величезна кількість конфіденційної інформації. Дональд Трамп також звернув увагу на те, що необхідно мати чітке уявлення про загрози, з якими доведеться стикатися, і бути готовим зробити все необхідне для протидії цим загрозам [16].

Висновок. Отже, ефективне здійснення безпекової політики дійсно неможливе без налагодженої системи комунікацій, що забезпечені політичними, інституційними та правовими складовими. Вони мають відображати прагнення держави до зміцнення інформаційної безпеки та збереження демократичних цінностей. Ключову роль у даному питанні відіграють політичні комунікації, втрата контролю над якими робить країну вразливою щодо інформаційного впливу ззовні. Також важливу роль у здійсненні комунікативної функції безпекової політики США відіграє функціонування таких служб, як Управління стратегічними комунікаціми, Центр стратегічних антитерористичних комунікацій, Команди з цифрових зовнішніх контактів тощо. Очевидним також є факт, що кіберпростір є невід'ємним елементом забезпечення національної безпеки в цілому і потрібно докладати зусиль щодо його захисту. Підтримка лідерства США у сфері інформаційно-комунікативних технологій розглядається американським керівництвом як один із ключових компонентів глобальної інформаційної переваги, що є важливим елементом забезпечення національної безпеки. Досвід Сполучених Штатів Америки з використання новітніх технологій у сфері забезпечення національної безпеки також може бути корисний іншим країнам. Для більш ефективного забезпечення безпекової політики державам необхідно освоювати нові канали комунікацій, такі як інтернет-форуми, блоги, чати, які терористи та їхні покровителі вже давно використовують для просування вигідних їм ідей. При цьому необхідно враховувати специфіку мережевої аудиторії та вміти вести дискусію зрозумілою їй мовою.

Список використаних джерел:

1. Багиров Р. З. Политическая коммуникация как средство борьбы с международным терроризмом [Электронный ресурс] / Р. З. Багиров. – Режим доступа : https://cyberleninka.ru/article/n/politicheskaya-kommunikatsiya-kak-sredstvo-borby-s-mezhdunarodnym-terrorizmom.
2. Базаркина Д. Ю. Противодействие терроризму посредством коммуникаций: обобщение Европейского опыта [Электронный ресурс] / Д. Ю. Базаркина. – Режим доступа : https://cyberleninka.ru/article/n/protivodeystvie-terrorizmu-posredstvom-kommunikatsiy-obobschenie-evropeyskogo-opyta.
3. National Framework for Strategic Communication [Electronical recources]. – Access mode : https://www.hsdl.org/?abstract&did=27301.
4. Office of Strategic Communications and Outreach [Electronical recources]. – Access mode : https://www.state.gov/about-us-office-of-strategic-communications-and-outreach/.
5. Global Engagement Center [Electronical recources]. – Access mode : https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/.
6. Worldwide Threat Assessment of the US Intelligence Community [Electronical recources]. – Access mode : https://fas.org/irp/congress/2013_hr/031213clapper.pdf.
7. National Cyber Strategy of the United States of America [Electronical recources]. – Access mode : https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
8. Цветкова Н. А. Социальные сети в публичной дипломатии США [Электронный ресурс] / Н. А. Цветкова. – Режим доступа : https://cyberleninka.ru/article/n/sotsialnye-seti-v-publichnoy-diplomatii-ssha.
9. Social Media Directory [Electronical recources]. – Access mode : https://www.dhs.gov/social-media-directory.
10. National Infrastructure Protection Plan [Electronical recources]. – Access mode : https://www.cisa.gov/national-infrastructure-protection-plan.
11. Holland S. Trump security team sees building U.S. 5G network as option [Electronical recources] / S. Holland, P. Schroeder. – 2018. – Access mode : https://www.reuters.com/article/us-usa-trump-5g/trump-security-team-sees-building-u-s-5g-network-as-option-idUSKBN1FH103.
12. 2017 National Security Strategy of the United States of America. – 2017 [Electronical recources]. – Access mode : https://ge.usembassy.gov/2017-national-security-strategy-united-states-america-president/.
13. Vincent B. White House Releases National Strategy for 5G Security [Electronical recources] / Brandi Vincent // Nextgov. – 2020. – Access mode: https://www.nextgov.com/emerging-tech/2020/03/white-house-releases-national-strategy-5g-security/164109/.
14. Cyberspace Solarium Commission Report [Electronical recources]. – Access mode : https://www.fdd.org/analysis/2020/03/11/cyberspace-solarium-commission-report/.
15. Coronavirus phishing emails: How to protect against COVID-19 scams [Electronical recources]. – Access mode : https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html.
16. Executive Order on Securing the Information and Communications Technology and Services Supply Chain. – 2019 [Electronical recources]. – Access mode : https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Надійшла до редколегії 27.12.19

M. Grynchuk, PhD Stud.
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

COMMUNICATIVE COMPONENT OF THE US SECURITY POLICY: POLITICAL AND LEGAL ASPECT

The article describes key aspects of communication sphere in the process of maintenance of the US national security. A number of US laws and regulations in the sphere of information and communication technologies and security policy were analyzed. It was found that political communications and terrorism, which is considered to be one of the biggest threats to US national security, are integrally linked. As well, the importance of cybersecurity as an integral element of national security was emphasized.

Keywords: communications, US national security, information and communication technologies.

М. Гринчук, асп.
Киевский национальный университет имени Тараса Шевченко, Киев, Украина

КОММУНИКАТИВНАЯ СОСТАВЛЯЮЩАЯ БЕЗОПАСНОСТИ США: ПОЛИТИКО-ПРАВОВОЙ АСПЕКТ

Рассмотрены основные аспекты коммуникативной сферы в процессе обеспечения национальной безопасности правительством Соединенных Штатов Америки. Проанализирован ряд законодательно-правовых актов США в сфере информационно-коммуникативного обеспечения безопасности. Обнаружено, что политические коммуникации и одна из самых глобальных угроз национальной безопасности США, терроризм, являются неразрывно связанными. Подчеркнута важность кибербезопасности как неотъемлемого элемента обеспечения национальной безопасности в целом.

Ключевые слова: коммуникации, национальная безопасность США, информационно-коммуникативные технологии.