УДК [002:004.056.5]:316.3/4(045)

О. В. СОСНІН
Г. В. ГРУШОВА

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА ЯК АКТУАЛЬНА ПРОБЛЕМА СУЧАСНОСТІ

Розглядається і розкривається поняття міжнародної інформаційної безпеки та процесів, пов'язаних із забезпеченням міжнародної інформаційної безпеки. Акцентується увага на основних моделях міжнародної інформаційної безпеки. Розкривається сутність основних загроз у сучасних міжнародних інформаційних відносинах. Обгрунтовується висновок, чим важлива міжнародна інформаційна безпека.

Ключові слова: *міжнародна інформаційна безпека, глобалізація комунікації, інформаційна зброя, інформаційне протиборство, інфосфера, інтернет, соціальні мережі, інфоінфраструктура.*

Соснин А.В., Грушовая А.В. **Международная информационная безопасность, как актуальная проблема современности**

Рассматривается и раскрывается понятие международной информационной безопасности и процессов, связанных с обеспечением международной информационной безопасности. Акцентируется внимание на основных моделях международной информационной безопасности. Раскрывается сущность основных угроз в современных международных информационных отношениях. Обосновывается вывод, чем важна международная информационная безопасность.

Ключевые слова: *международная информационная безопасность, глобализация коммуникации, информационное оружие, информационное противоборство, инфосфера, интернет, социальные сети, инфоинфраструктура.*

Sosnin Oleksandr, Grushova Ganna. **International information security as an urgent issue of our time**

© *СОСНІН Олександр Васильович* – доктор політичних наук, професор
© *ГРУШОВА Ганна Володимирівна* – магістр Інституту міжнародних відносин Національного авіаційного університету

Discusses and explains the concept of international information security and processes associated with ensuring international information security. Focuses on the major models of international information security. The essence of the main threats in modern international relations. The conclusion is grounded on importants of international information security.

Key words: *international information security, globalization of communication, information weapons, the informational confrontation, InfoSphere, the Internet, social networks, pointdexter.*

Наше покоління є свідком глобального процесу переходу до інформаційного суспільства, незалежного від рівня розвитку соціальних структур. Незважаючи на те, що роль інформаційних процесів у суспільстві знаходиться в прямій залежності від економічного, культурного і політичного рівня країн, процес інформатизації дедалі більше охоплює всі країни і континенти.

Як наслідок сучасний етап розвитку суспільства характеризується тріумфальною ходою інформаційно – телекомунікаційних інновацій, які змінюють вигляд світу і людини. Стає зрозуміло, що неможливо забезпечувати економічне зростання і розвиток, швидке і якісне виконання державою своїх функцій без широкого використання швидкозростаючих інформаційних технологій. Як зазначається в Доповіді ЮНЕСКО «Інформаційні та комунікаційні технології в понятті розвиток: перспективи ЮНЕСКО», інформаційні та комунікаційні технології дають можливість драматичним чином трансформувати, надавати людям новий вид засобам, для організації власного життя, взаємодії між собою, участі в різних сферах суспільного життя. Ці технології формують основу для радикальної зміни від індустріальних до постіндустріальних визначень розвитку[1].

З таких умов, забезпечення сталого розвитку виносять на порядок денний обговорення поняття «інформаційна безпека» як глобальної і актуальної проблеми. Вона посідає особливе місце в структурі міжнародної інформаційної політики, визначаючи суперчності сучасного етапу розвитку, коли вплив інформаційних чинників досяг такого рівня і гостроти, що поставлено під загрозу забезпечення світового порядку, реалізація стратегій становлення глобального інформаційного суспільства, навіть саме існування цивілізації. Інформаційна безпека як чинник міжнародних відносин, вплив якої має універсальний характер на поведінку акторів міжнародних відносин. До того ж трансформація самої сутності понять проблеми безпеки після закінчення «холодної війни» і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах інформаційної складової міжнародної безпеки[2].

Міжнародну інформаційну безпеку слід розглядати в контексті проблеми, що сприяє створенню ефективних гарантій миру як для окремої країни, так і для всього світового співтоваривства.

Зважаючи на глобальність складових інформаційної безпеки, розвинуті країни вже давно розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту структур критично залежних від інформації. В 1996 році проблему міжнародної іфнормаційної безпеки було винесено на політичний та міжнародно-правовий рівень:

Концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 рік)

У спільному комюніке зустрічі на найвищому рівні США-Російська Федерація у 1997 році було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної кладової глобального процесу інформатизації

На 52-ій сесії ГА ООН було консенсумом прияйнято Резолюцію 53/70 від 4 грудня 1998 року, де зазначалося, що міжнародна спільнота визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у світі, пропонувалося державам-членам ООН розглянути конкретну типологію інформаційних загроз, визначити критерії проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем, внести пропозиції до комплексної доповіді Генерального секрктаря ООН для створення міжнародного механізму протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн[3].

Міжнародна інформаційна безпека визначається як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільности від реальних і потенційних інформаційних загроз[4].

Інформаційна безпека, як поняття в міжнародних відносинах залежно від його використання розглядається у декількох ракурсах. У найзагальнішому вигляді- інформаційна безпека- це стан захищенності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави[5].

Визнання проблеми інформаційної безпеки в міжнародних відносинах обумовлюється чинниками глобалізації комунікації, то у більшості індустріально розвинутих країн проводяться дослідження і розробки нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними реурсами потенційного противника, а за

необхідності прямо впливати на них. За даними аналітичних центрів США, розробки такої зброї ведуться в 12- країнах світу: для порівняння розробки в галузі ядерної зброї проводяться у 20 країнах; в деяких країнах завершено розробку засобів інформаційного протиборства (війни) з можливим противником як в умовах воєнних конфліктів різної інтенсивності, так і в мирний час на стратегічному, оперативному, тактичному рівнях та в польових умовах з метою захисту національної інфосфери від агресії і несанкціонованого втручання; в розвинутих країнах концепція інформаційної війни є складовою воєнної доктрини, що обумовлює спеціальну підготовку особового складу і окремих підрозділів для проведення інформаційних операцій; практика міжнародних регіональних та етнічних конфліктів виявила унікальність застосування інформаційної зброї для впливу на міжнародне співтоваривство та для боротьби за геополітичні інтереси[6].

В свою чергу, необхідно розуміти, що не може бути інформаційної безпеки без застосування спеціальних технічних засобів та методів для захисту інформації від несанкціонованого доступу.

Інформаційна безпека складається на тлі зростання вимог до організаційної сфери і включає в себе сукупність організаційних, соціально-економічних, правових заходів, спрямованих на забезпечення стабільності суспільства і держави.

Довгий час була поширена точка зору, що Інтернет – це децентралізована гнучка інформаційна система, і управління, а тим більше контроль над нею неможливий.

Однак Інтернет, як і будь-яка технічна система, потребує координації для зв'язкової роботи в глобальному масштабі. В Інтернеті є декілька технічних «точок контролю». Це насамперед система доменних імен та інтернет-адрес, вироблення параметрів інтернет-протоколів. Зараз контроль над простором імен і адрес Інтернету, а також координацію робіт з вироблення параметрів інтернет-протоколів здійснює приватна некомерційна організація ICANN (Internet Corporation for Assigned Names and Numbers), зареєстрована в штаті Каліфорнія і підкоряється законам США. Подібна ситуація не може не викликати заклопотаності у інших держав, що виступають за інтернаціоналізацію функцій ICANN і передачу їх Міжнародному союзу електрозв'язку, спеціалізованої організації «сім'ї ООН».

При цьому управління Інтернетом включає в себе не тільки технічну координацію, а й більш широке коло питань, пов'язаних із захистом прав людини в Інтернеті, захистом прав інтелектуальної власності, протидією злочинності та інш. Згідно з визначенням Робочої групи ООН з питань управління Інтернетом, таке управління «представляє собою розробку і застосування урядами, приватним сектором і грома-

дянським суспільством, при виконанні ними своєї відповідної ролі, загальних принципів, норм, правил, процедур прийняття рішень і програм, регулюючих еволюцію і застосування Інтернету[7].

Інтернет сьогодні – невід'ємна частина повсякденного реальності, він трансформує всі сфери життя суспільства і держави – політику, економіку, культуру. Виклики і загрози, що існують оффлайн, переносяться в онлайн-середовище. Без управління Інтернетом неможливо забезпечити його безпеку, стабільне функціонування, інноваційний розвиток. Тому управляти Інтернетом необхідно.

На міжнародному рівні технічна координація здійснюється в рамках ICANN, але окремі питання, такі як захист прав інтелектуальної власності в Інтернеті, вирішуються в рамках міжнародних організацій, зокрема, СОТ і ВОІВ. Деякі питання вирішуються на рівні окремих держав.

Часто під керуванням Інтернетом мають на увазі цензуру, яка має місце в багатьох країнах, однак управління Інтернетом включає в себе набагато більш широке коло питань.

Багато країн давно займаються політикою захисту інформаційних потоків та систем- не тільки як джерел державних секретів, але і як джерел економічного прибутку. Франція, наприклад, відзначилися у створенні власного сегменту Інтернету на французькій мові. Вона взяла під свій контроль прибутковий ринок комп'ютерної техніки, програмного забезпечення та інформаційних потоків на всьому франкомовному просторі. Відомий досвід Китаю, який досяг суттєвого економічного росту за рахунок переорієнтації інформаційних потоків та акамуляції капіталів в інформаційній сфері[8].

Соціальні мережі сьогодні носять великі масиви інформації про користувачів, які, звичайно, становлять інтерес не тільки для державних спецслужб, а й для рекламодавців.

Найчастіше соціальні мережі змушені надавати чутливу інформацію про своїх користувачів спецслужбам, причому мова йде не тільки про такі країни, як Китай, який широко відомий своєю обмежувальною політикою в Інтернеті, але і США, а також низці країн ЄС.

Після подій 11 вересня 2001 року в США були прийняті закони, що обмежують безпеку користувачів Інтернету на користь безпеки держави. В цілому, це було позитивно сприйнято суспільством, так як складно забезпечити особисту безпеку в умовах, коли безпека держави під загрозою.

При цьому важливо, витримати правильний баланс, адже надмірне посилення державного контролю в Інтернеті, обмеження свободи в мережі здатні підірвати властивий Інтернету інноваційний потенціал і

тим самим обмежити можливі вигоди від розвитку онлайн-середовища, що сприяє економічному зростанню.

Слід підкреслити, що стратегії глобального інформаційного протиборства лежать в основі аналітичних розробок дослідницьких інституцій різних країн, метою яких є саме забезпечення інформаційного лідерства у сфері міжнародної безпеки. За результатами досліджень аналітики виділяють такі моделі системи глобальної інформаційної безпеки:

Модель А- створення абсолютної ситеми захисту країни-інформаційного лідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній іфнормаційній війни, змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером. При цьому може бути використано ситему жорстокого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Модель В- створення значної переваги державами-потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту державами-протиника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз.

Модель С- наявність кількох країн-інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Модель D- всі конфліктуючі сторони використовують транспорантність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами(політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій.

Модель Е- протиборство світової спільности та міжнародної організованої злочинності, здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в дослідженні Національної ради розвідки США «Mapping the global future»- 2020 у версії «Коло страху» («Cycle

of fear»), яка є найбільш песимістичним сценарієм майбутнього світової спільноти[9].

Заборонити розробку та використання інформаційної зброї неможливо. Обмежити зусилля багатьох країн з формування єдиного глобального інформаційного простору також нереально. Проте цілком можливо підписати розумні погодження, які б опиралися на міжнародне право та мінімізували загрозу застосування інформаційної зброї.

Концепція міжнародної інформаційної безпеки визначає критичні структури, які, в першу чергу, зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства.

У політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення.

В економічній сфері критичними є системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, системи управління в критично важливих для держави структурах(енергетика, комунікації, інформаційні мережі).

Досвід інформаційно-розвинутих країн свідчить, що економічні переваги грунтуються в сучасному світі на прогресивній інформаційній експансії, і саме ті країни які найбільше просунулися у напрямку інформаційної цивілізації, будуть переважати у світовій господарській системі та в міжнародній конкуренції з технологічно відсталими країнами та регіонами.

Феномен інформаційної безпеки в міжнародних відносинах обумовлюється стратегічною спрямованістю інформаційних впливів проти критично важливих структур життєдіяльності і функціонування міжнародного співтоваристваа, визнання їх в якості інформаційної зброї як нового глобального виду зброї масового ураження, катастрофічного за наслідками свого застосування, необхідністю створення міжнародного механізму протидії і попередження глобальних інформаційних війн в рамках політичної компетенції ООН, регіональних міжнародних організацій з проблем безпеки та оборони, політичних рішень на національному рівні.

Негативні наслідки деструктивного застосування інформаційних технологій злочинцями і терористами, а також окремими державами для вирішення військово-політичних завдань стосуються інтересів багатьох країн, набуваючи глобального характеру.

З вище викладеного можна зробити висновок, що міжнародна інформаційна безпека – стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі.

Всі питання забезпечення інформаційної безпеки держави, крім технічних засобів захисту інформації, повинні регулюватися, насамперед, нормами міжнародного права, так як засоби інформаційного впливу мають деструктивні наслідки не тільки для держави, проти якої вони спрямовані, а й для всієї світової спільноти.

1. *Федоров А.В.* Информационная безопасность в мировом политическом / Федоров А.В. – М. : МГИМО-Университет, 2006. – 220 с. **2.** *Міжнародна* інформаційна безпека: Сучасні виклики та загрози. –К. : Центр вільної преси, 2006. – С. 9. **3.** Там само. – С. 13-14. **4.** *Раймон А.* Мемауры: 50 лет размышления о политике / Раймон А. Memoires: 50 Ands de Reflexion Politique ; пер. с фр. Г.А. Абрамова, Л.Г. Лариновой.– М. : Ладомир, 2002.– 873с. **5**. *Юдін О.К.* Інформаційна безпека держави : навч. посіб. / О.К. Юдін, В.М. Богуш. – Х. : Консум, 2005. – С. 38. **6**. *Міжнародна* інформаційна безпека:Сучасні виклики та загрози – С. 15. **7**. *Доклад* рабочей группы по управлению Интернетом. – Шато де Босси, 2005. **8.** *Пухова Калерия.* Совбез занялся СМИ : Доктрина информационной безопасности может сработать против российских масс-медиа [Електронний ресур]. – Режим доступа : http://www.org.ng.ru/printed/8786. **9**. *Міжнародна* інформаційна безпека: Сучасні виклики та загрози [Текст].-К..:Центр вільної преси, 2006. – С. 147.

УДК 328.182

М. Д. ХОДАКІВСЬКИЙ

ПРОТИДІЯ ДИСКРИМІНАЦІЇ ЗА ОЗНАКОЮ СЕКСУАЛЬНОЇ ОРІЄНТАЦІЇ ТА ГЕНДЕРНОЇ ІДЕНТИЧНОСТІ В УКРАЇНІ*

На основі аналізу законодавства України у статті розглянуто політико-правові засади протидії дискримінації за ознакою сексуальної орієнтації та гендерної ідентичності, особливості цього процесу в сучасних політичних умовах.

Ключові слова: *дискримінація, сексуальна орієнтація, гендерна ідентичність.*

© *ХОДАКІВСЬКИЙ Михайло Дмитрович* – кандидат політичних наук, старший науковий співробітник Інституту держави і права ім. В. М. Корецького НАН України

* Стаття підготовлена в рамках планової теми відділу правових проблем політології «Політико-правові механізми запобігання ксенофобії та іншим видам дискримінації в Україні в контексті європейської інтеграції»