[Електронний ресурс]. – Режим доступу : http://www.medialaw.kiev.ua/laws/laws_international /105/.

7. ARTICLE 29 – DATA PROTECTION WORKING PARTY. WP 37. Working Document. Privacy on the Internet – An integrated EU Approach to On-line Data Protection, adopted on 21st November 2000 [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf.

8. International Working Group on Data Protection in Telecommunications. Report and Guidance on Data Protection and Privacy on the Internet "Budapest – Berlin Memorandum" [Електронний ресурс]. – Режим доступу : http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf?1200577389.

9. ВГО "УАЗПД". Звіт за результатами громадського моніторингу "Забезпечення прозорості та відкритості обробки персональних даних на веб-ресурсах" [Електронний ресурс]. – Режим доступу : http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf.

10. ВГО "УАЗПД". Декларація "За недоторканість приватного життя в Інтернеті" [Електронний ресурс]. – Режим доступу : http://uapdp.org/images/1016%202012%20.pdf.

Аннотация: В статье проанализирован отечественный и европейский опыт урегулирования вопроса обработки и защиты персональных данных в сети Интернет, обозначены проблемные вопросы и пути дальнейшего развития законодательства Украины на основе европейского опыта.

Ключевые слова: обработка и защита персональных данных, усовершенствование законодательства, иностранный и отечественный опыт, интернет.

Abstract: The domestic and European experience on processing and protection of personal data in Internet is analyzed in the article. The optimal ways of its development in Ukraine on European experience are suggested.

Key words: processing and protection of personal data, improvement of legislation, foreign and domestic experience, Internet.

УДК 35.746.1

СОЛОДКА Олена Маркіянівна

СУЧАСНІ ТЕНДЕНЦІЇ МІЖНАРОДНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Постановка проблеми. Глобальні інтеграційні процеси в умовах інформаційної революції впливають на формування нової системи міжнародних відносин, що характеризуються розмитістю державного суверенітету, збільшенням політичної та економічної взаємозалежності суб'єктів міжнародного співробітництва, необхідністю реалізації міжнародних стратегій цивілізаційного розвитку на різних рівнях взаємодії. Процеси глобалізації мають неоднозначні наслідки. З одного боку, вони забезпечують взаємозв'язки у межах світу, сприяють демократизації глобального управління, відкривають нові можливості для збалансованого розвитку регіонів і держав; з іншого – технологічні зміни формують нові типи поляризації у сучасному світі, що призводить до асиметрії міжнародного розвитку.

Становлення інформаційного суспільства дає змогу не лише будувати більш ефективне та розвинене громадянське суспільство, але

й надає нових імпульсів традиційним загрозам як національній, так і світовій безпеці загалом. Стрімке впровадження інформаційних технологій у всі сфери життя, глобалізація інформаційних відносин зумовлюють світову тенденцію до перенесення протиправної діяльності у віртуальний простір.

З огляду на транскордонність проблем забезпечення інформаційної безпеки сьогодні це питання є одним із перших на порядку денному сучасного світового співтовариства.

Розробкою питань забезпечення інформаційної безпеки, загроз інформаційній безпеці займаються вітчизняні та зарубіжні науковці, а саме Є.А.Макаренко, М.А.Ожеван, М.М.Рижков, Д.В.Дубов, О.Ю.Запорожець та інші, проте стрімкий розвиток сучасного інформаційного суспільства безупинно дає новий матеріал для подальших досліджень.

Таким чином, актуальність дослідження зумовлена потребою наукового аналізу та узагальнення змісту сучасних умов забезпечення міжнародної інформаційної безпеки.

Мета статті – визначити сучасні тенденції міжнародної політики забезпечення інформаційної безпеки.

Для реалізації мети слід вирішити такі *завдання,* спрямовані на: виокремлення особливостей забезпечення інформаційної безпеки на міжнародному рівні; визначення пріоритетів у забезпеченні міжнародної інформаційної безпеки.

Міжнародну безпеку слід розглядати як політику, що сприяє створенню ефективних гарантій миру як для окремої держави, так і для всього світового співтовариства.

Проблеми глобальної безпеки посідають особливе місце у структурі міжнародної інформаційної політики, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світового порядку, реалізацію стратегій становлення глобального інформаційного суспільства. Глобальна безпека як чинник міжнародних відносин, вплив якого має універсальний характер і врахування якого в діяльності міжнародного співтовариства, та в зовнішній політиці окремих держав призводить до радикальних змін, до трансформації самої сутності проблеми безпеки, потребує перегляду концептуальних принципів функціонування міжнародних та національних інститутів, а також врахування в нових доктринах інформаційної складової міжнародної безпеки [1].

На думку експертів, всі держави зіштовхнуться з проблемами, які суттєво вплинуть на політику, економіку, соціальну та культурну сферу в усіх країнах світу. Вважається, що подальший розвиток інформаційних і комунікаційних технологій сприятиме зміні економічних і політичних можливостей держав [2].

Відмінність сучасного етапу розвитку комунікаційної діяльності від попереднього полягає у тому, що за останні десятиріччя створено комунікаційний канал, який є принципово новим матеріально-технічним засобом її здійснення. Його називають простором комп'ютерних комунікацій, кіберпростором або віртуальною реальністю. На думку Е.Гіденса, "кіберпростір – це простір взаємодії, утворений глобальною мережею комп'ютерів, з яких складається інтернет" [3]. Він передає повідомлення у фізичному просторі та астрономічному часі з небаченою раніше швидкістю та легкістю, що дає змогу значно інтенсифікувати процес руху смислів у суспільстві в національному та міжнародному масштабах. У цьому аспекті кіберпростір є засобом розширення можливостей інформаційного простору, ефективне використання якого стає сучасною парадигмою суспільного розвитку.

Концепція забезпечення кібернетичної безпеки в сучасних умовах заснована на аналізі глобальних проблем і містить два важливих висновки: перший – людство зіткнулося із серйозною загрозою інформаційній безпеці, яка виявляється в кібернетичних атаках; другий – спроби пошуку шляхів виходу з цієї ситуації змушують світове співтовариство аналізувати ризики та своєчасно їм протидіяти.

Особливо важливо вирішити кілька принципових проблем (передусім на міжна-

родному рівні), що унеможливлюють формалізацію безпекової політики в кіберпросторі: досі відсутні системні міжнародні нормативно-правові документи, які б чітко давали визначення кіберпростору та всіх похідних від нього елементів безпекового характеру; не визначено правовий статус кіберпростору; відсутній консенсус на міжнародному рівні щодо правил поведінки в кіберпросторі; відсутня загальноприйнята методологія оцінювання наслідків кіберзлочинів та їх належність до міжнародних норм і правил (зокрема щодо визнання кібератаки як акту війни) [4].

Питання кіберзлочинності стали на порядку денному у Давосі (Всесвітній економічний форум–2012). Зазначено, що персональні дані – це новий товар, який пропонує кіберзлочинність, а також те, що розвиток інтернет-технологій призвів до розповсюдження матеріалів, що містять дитячу порнографію.

Крім цього, на початку червня 2013 року колишній американський співробітник ЦРУ та Агентства національної безпеки США Е.Сноуден передав журналістам секретні матеріали, які викривали діяльність американських спецслужб, що займалися масовим стеженням за громадянами як США, так й інших країн. 19 міжнародних правозахисних організацій подали позов проти АНБ та звернулися до урядів країн ЄС із закликом захистити європейців від шпигунських програм. Справа Сноудена вдруге, після історії із Wikileaks, вивела на серйозний рівень дискусію про проблему співвідношення таких понять, як безпека держави, свобода слова та право на приватність громадян.

Відтак, міжнародні організації та інститути, неурядові асоціації, країни-члени, країни-партнери міжнародних організацій активізують обговорення актуальних проблем міжнародних відносин, зумовлених глобалізацією комунікації, з метою формування спільної стратегії та узгодження політичних рішень в умовах становлення інформаційного суспільства.

Зокрема, суттєвих змін зазнала політика НАТО з питань кіберзахисту, що зумовлено зростанням кількості та якості атак у кіберпросторі на інформаційні системи, критично важливі об'єкти інфраструктури НАТО, а також країн-членів Альянсу.

Так, у маніфесті, замовником якого був центр кіберзахисту НАТО (створений в 2008 р. у Таллінні), країнам НАТО рекомендовано відповідати військовими ударами на держави, кібератаки з боку яких будуть призводити до смерті громадян або серйозних руйнувань критичної інфраструктури. Таким чином, кібератаки прирівнюються до військових дій.

У цьому ж документі міститься визначення збройного військового конфлікту: "міжнародний збройний конфлікт виникає щоразу, коли ведуться військові дії, які можуть включати або бути обмежені кібероперераціями між двома або більшою кількістю держав", а також є положення присвячені методам реагування на атаки на важливі об'єкти інфраструктури, до яких належать дамби, греблі, атомні електростанції, руйнування яких може призвести до загибелі населення [5].

Не залишається осторонь питань протидії кіберзагрозам і Європейський Союз. В Європейському Союзі інформаційна та мережева безпека полягає у захисті особистої інформації про відправників і одержувачів, захисті інформації від несанкціонованих змін, захисті від несанкціонованого доступу до інформації і створенні надійного джерела постачання обладнання, послуг та інформації [6].

Згідно із звітом Європолу "The EU Serious and Organized Crime Threat Assessment (SOCTA) 2013" на території Європейського Союзу знешкоджено 3600 злочинних угруповань, які через мережу Інтернет вчинювали економічні злочини [7].

У січні 2013 року в Європолі відкрито Європейський центр по боротьбі з кіберзлочинністю (European Cyber Crime Centre (EC3), який став координаційним центром ЄС у боротьбі з кіберзлочинністю. Мандат діяльності Центру включає боротьбу із такими видами кіберзлочинності: злочини, вчинені організованими групами для отримання

злочинних доходів, зокрема, on-line-шахрайство; злочини, які завдали серйозної шкоди жертві, зокрема сексуальна експлуатація дітей; злочини, які завдали шкоди критично важливій інфраструктурі та інформаційним системам в ЄС.

Процес глобалізації призвів до змін цінностей у світовій системі. Перше місце посіли цінності демократичного суспільства. Все більше уваги приділяється правам людини та їх захисту.

За результатами опитування, що проводилося у всіх країнах ЄС, перше місце серед ідеалів посіли права людини (37%), мир (35%), демократія (34%), верховенство закону (22%), повага до інших культур (17%), солідарність (15%), повага до життя людини (14%), рівність (13%), особиста свобода (11%), толерантність (10%), самовираження (4%), і на останньому місці у переліку цінностей – релігія, яка важлива для 3% опитаних [8].

Одним із невід'ємних і важливих прав людини у сучасному інформаційному суспільстві є свобода слова та забезпечення доступу до інформації, адже виникнення права на інформацію зумовлене зростанням інтересу як до самої інформації, так і до її змісту.

Сьогодні як у правовій науці, так і в законодавстві сформувалися два підходи до трактування права на інформацію. У межах вузького підходу право на інформацію визначається тільки як право на одержання (доступ) до інформації, тобто як відносне право. Широкий підхід передбачає віднесення до права на інформацію усіх видів суб'єктивних прав, спрямованих на інформацію чи на здійснення дій із нею [9].

Комітет ООН із прав людини у 2011 році провів дворічні консультації про те, яким чином інтерпретувати право на "свободу думок і їх вираження", гарантоване статтею 19 Міжнародного пакту про громадянські і політичні права. У заході взяли участь більше ніж 70 неурядових організацій, а також урядів, національних правозахисних організацій та учених, основними темами були:

– значення свободи вираження поглядів та інформації як "метаправа", на якому ґрунтуються інші права;

– зобов'язання урядів захищати свободу слова і забезпечувати доступність інформації;

– право журналістів та інших осіб на поширення інформації, а також право громадян на отримання інформації;

– визнання мінливого характеру сучасних засобів масової інформації, а також розвитку технологій;

– важливість незалежності засобів масової інформації [10].

Разом із тим, спостерігається тенденція до посилення контролю з боку правоохоронних органів за контентом національного інформаційного простору, мережевим трафіком, засобами доступу до всесвітньої мережі, що свідчить про довгострокову тенденцію формування в мережі Інтернет класичних прав та обов'язків громадянина та держави, що існують в традиційній державі та формування своєрідних "цифрових суверенітетів". Розглядаючи цю тенденцію разом із можливістю зменшення рівня анонімності у всесвітній мережі (із уведенням "інтернет-паспорту" для користувачів), можна зазначити, що неоліберальний підхід до розуміння мережі Інтернет (так звана "Каліфорнійська ідеологія") зазнає кардинальних змін, а на зміну йому приходить "технореалізм" із його відношенням до ІКТ як "технологій подвійного призначення" та ключовою роллю держави у розвитку мережі Інтернет [11].

У Росії до середини 2014 року усі інтернет-провайдери змушені будуть встановити на свої мережі обладнання для запису і зберігання інтернет-трафіку терміном не менше 12 годин, і вся ця інформація буде доступна спецслужбам. Відтак, під контроль ФСБ потраплять телефонні номери, IP-адреси, імена облікових записів і адреси електронної пошти користувачів соціальних мереж. Подібна норма встановлена у законодавстві Китаю.

Як зазначають провайдери, деякі положення наказу порушують права, котрі гарантовані Конституцією, наприклад, права на недоторканність приватного життя, адже кожен має право на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень. Обмежувати ці

права можна лише на підставі судових рішень.

Висновки. З огляду на викладене встановлено, що чинниками, які впливають на забезпечення міжнародної інформаційної безпеки та визначають сучасні тенденції у цій сфері, є:

– прискорені темпи розробки і використання засобів несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем;

– постійні спроби неправомірного використання та завдання збитків інформаційним ресурсам іноземних держави;

– протиправні посягання на критичну інфраструктуру;

– дії, спрямовані на домінування в інформаційному просторі;

– цілеспрямований інформаційний вплив на населення іншої держави ведення інформаційних війн.

Співробітництво у сфері інформаційної безпеки потребує пошуку спільних рішень щодо протидії інформаційним і кіберзагрозам, вироблення міжнародних стратегій інформаційної безпеки щодо запобігання негативним інформаційним впливам, інформаційним війнам, протидії кібертероризму.

Список використаних джерел

1. Міжнародна інформаційна безпека: сучасні виклики та загрози / Є.А.Макаренко, М.А.Ожеван, М.М.Рижков та ін. – К. : Центр Вільної преси, 2006. – 916 с.

2. Столетов О.В. Тренди трансформації владних відносин у світовій політиці: smart power? / О.В.Столетов // Поліс. – 2009. – № 4. – С. 173–178.

3. Global trends 2025: The National Intelligence Council's. 2025 Project [Електронний ресурс]. – Режим доступу : http://www.dni.gov/nic/NIC_2025_project.html.

4. Дубов Д.В. Сучасні тенденції забезпечення кібербезпеки на міжнародному рівні / Д.В.Дубов // Стратегічні пріоритети. – 2011. – № 4 (21).

5. The Comprehensive National Cybersecurity Initiative. National Security Council [Електронний ресурс]. – Режим доступу : http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.

6. Запорожець О.Ю. Політика інформаційної безпеки в ЄС / О.Ю.Запорожець // Актуальні проблеми міжнародних відносин : зб. наук. праць. – К., 2009. – Вип. 87. – Ч. 2. – С. 36-45.

7. Макаренко Є.А. Європейська інформаційна політика : моногр. / Є.А.Макаренко. – К. : Наша культура і наука, 2000. – 368 с.

8. Європейські цінності: реальність чи міф? [Електронний ресурс]. – Режим доступу : http://www.radiosvoboda.org/content/article /25131805.html.

9. Марущак А.І. Доступ до інформації в Україні: питання правового регулювання / А.І.Марущак // Бюлетень Міністерства юстиції України. – 2006. – № .1 – С. 37.

10. Recommendation № R (94) (13) Measures to Promote Media Transparency, Council of Europe (Adopted by the Committee of Ministers on 22 November 1994).

11. Дубов Д.В. Сучасні тренди кібербезпекової політики: висновки для України: аналітична записка НІСД при Президентові України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/294/.

Аннотация: В статье рассматриваются особенности современных тенденций международной политики информационной безопасности.

Ключевые слова: международная политика, информационная безопасность, кибербезопасность.

Abstract: The article considers the features of modern trends on international information security policy.

Key words: international policy, information security, cybersecurity.