УДК 321

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРОВІДНИХ КРАЇНАХ СВІТУ

FEATURES PROVIDING INFORMATION SECURITY IN THE WORLD LEADING COUNTRIES

Олефір І.В.,
аспірант кафедри суспільно-політичних наук,
глобалістики та соціальних комунікацій
Відкритого міжнародного університету розвитку людини «Україна»

У статті йдеться про інформатизацію суспільства як про глобальний процес, який потребує глибокого та продуманого підходу до його трансформації. У зв'язку з тим, що рівень розвитку та інформатизації країн світу різний, це веде до цифрового відставання одних країн від інших, що підвищує інформаційну небезпеку. При цьому такі провідні країни, як США та країни-члени Європейського Союзу, останнім часом приділяють значну увагу питанням забезпечення інформаційної безпеки, яку вони поставили на провідне місце у системі забезпечення національної безпеки. Якщо США веде політику більш наступального характеру з метою попередити інформаційні небезпеки, які можуть становити загрозу державі у будь-якій точці земної кулі, то країни ЄС намагаються виробити надійні підходи до захисту свого інформаційного середовища та громадян. Україні необхідно вибудовувати свою систему забезпечення інформаційної безпеки відповідно до європейських кран на основі двосторонньої та багатосторонньої співпраці.

Ключові слова: інформаційна безпека, інформаційні війни, гібридна війна, інформаційне середовище.

В статье говорится об информатизации общества как о глобальном процессе, требующем глубокого и продуманного подхода к его трансформации. В связи с тем, что уровень развития и информатизации стран мира разный, это ведет к цифровому отставанию одних стран от других, повышает информационную опасность. При этом такие ведущие страны, как США и страны-члены Европейского Союза, в последнее время большое внимание уделяют вопросам обеспечения информационной безопасности, которую они поставили на ведущее место в системе обеспечения национальной безопасности. Если США ведет политику более наступательного характера с целью предупредить информационные опасности, которые могут представлять угрозу государству в любой точке земного шара, то страны ЕС пытаются выработать надежные подходы к защите своего информационного пространства и граждан. Украине необходимо выстраивать свою систему обеспечения информационной безопасности в соответствии с европейскими странами на основе двустороннего и многостороннего сотрудничества.

Ключевые слова: информационная безопасность, информационные войны, гибридная война, информационная среда.

This article is about informatization of society as a global process, which requires a thorough and thoughtful approach to its transformation. Due to the fact that the level of development and informatization of the countries in the world is different, it leads to the digital lag of some countries behind others, which increases the information danger. At the same time, such leading countries as the United States and the European Union member states have recently paid considerable attention to the issues of information security which they have put in the leading place in the system of providing national security. While the US leads a more aggressive policy in order to prevent information dangers that could pose a threat to the state anywhere in the world, the EU countries are trying to develop reliable approaches to protect their information environment and citizens. Ukraine needs to build up its information security system in accordance with the European countries and on the basis of the bilateral and multilateral cooperation.

Key words: information security, information wars, hybrid war, information environment.

Постановка проблеми. Інформатизація суспільства у розвинених країнах світу – це глобальний процес, який не може бути здійснений одним кроком або рішенням уряду тієї чи іншої країни.

Зважаючи на важливість і складність цих перетворень, цей процес потребує глибокого та продуманого підходу до трансформації суспільства.

Як показав аналіз результатів формування інформаційного суспільства, країни демонструють неоднакові рівні життя різних груп населення, але виграють від процесів інформатизації ті країни, які є активними їх учасниками. Між розвиненими країнами і країнами, які не встигають за сучасними темпами розвитку, збільшується цифровий розрив. Монополія на інтелектуальну власність у виробництві товарів і послуг перетворюється на основну потребу провідних виробничих процесів.

Разом із тим, інформаційні технології породжують і нові види небезпек, які пов'язані перш за все з захистом інформаційних ресурсів.

Аналіз останніх досліджень і публікацій. Провідними вітчизняними дослідниками, які займаються проблемами інформаційної безпеки, є: В.М. Бебик, В.А. Ліпкан, Є.В. Магда, Г.Г. Почепцов, Г.В. Хоружий, І.С. Чиж та ін.

Формулювання цілей статті (постановка завдання). Мета роботи полягає у визначенні особливостей забезпечення інформаційної безпеки у провідних країнах світу.

Виклад основного матеріалу дослідження. Однією з перших країн, що почала розбудову інформаційного суспільства, були Сполучені Штати Америки. Ті умови розвитку інформаційних технологій, які утворилися у другій половині XX ст., дали США змогу випередити весь світ у питаннях інформатизації та перетворити інформаційні технології на стратегічний ресурс. Оскільки у США інформаційна інфраструктура найбільше пов'язана з інформаційною безпекою, політика держави у цій сфері стала пріоритетною у забезпеченні національної безпеки.

Маючи наймогутнішу армію, яка забезпечена найновішою технікою, Сполучені Штати Америки виділяють значні кошти на забезпечення інформаційної безпеки, щоб запобігти завданню колосальної шкоди як окремим державним об'єктам, так і усій країні загалом.

Потужний поштовх у розробці та впровадженні інформаційних технологій у суспільне життя у США спричинило закінчення «холодної» війни, яке призвело до скорочення витрат на оборону. Це могло б призвести до відставання військових технологій від громадянських. Для того щоб уникнути такої ситуації, США здійснили реформу військових закупівель, яка мала на меті збільшити витрати на дослідження і розробки через скорочення військового виробництва і зробити пріоритетною галуззю модернізацію військово-технічної системи [3, с. 150]. Військова продукція та нове озброєння для армії мали відповідати стандартам, які використовувалися у громадському секторі [10].

Також широке поширення здобули технології подвійного застосування. Закупівлі продукції некомерційного сектору приділялася особлива увага. Через розширення урядом США хвильових діапазонів для комерційного мобільного зв'язку шляхом скорочення діапазонів, які використовувалися військовими, відбулося збільшення кількості споживачів продукції бездротового зв'язку. Потреба у мобільному з'єднанні стала причиною продажу вільних частот на аукціоні, а це дало змогу державі отримувати кошти від продажу ліцензій на ринку.

Незважаючи на те, що військова міць США найбільша за інші країни і жодна інша держава не почне проти них війну, є небезпеки терористичних атак, які можуть бути реалізовані будь-якими особами, які мають комп'ютери.

З метою забезпечення національної безпеки США започаткували політику, що спрямована на встановлення контролю не лише над національним простором США, але й розширенням можливостей свого впливу на інші країни.

Мета збройних сил США – перевага інформаційних систем порівняно з іншими країнами. Заради цього США об'єднали роботу космічного та стратегічного управлінь. Космічні ресурси відіграють визначальну роль у попередженні загроз та здійсненні превентивних дій. Це дає змогу США володіти максимальною інформацією про своїх можливих супротивників.

Інформаційні технології та космічні розробки допомагають зрозуміти та відстежити супротивника, виявити його ворожі наміри на ранніх стадіях та знешкодити потенційні загрози. Такі можливості відсувають традиційні методи ведення збройної боротьби на друге місце. Основою сьогоднішніх воєнних операцій є інформаційні технології, за допомогою яких США можуть знешкоджувати ворогів, руйнуючи їхні інформаційні системи. Інформація про супротивника, його місцезнаходження, військовий потенціал дають змогу застосовувати проти нього як традиційну зброю, так і інформаційну.

Із метою ефективної реалізації таких завдань у США було затверджено «План дій по розвитку інформаційних операцій» [8, с. 23]. Він визначав такі основні особливості стримування супротивника:

– застосування усіх можливих засобів при стримуванні супротивника;

– здійснення впливу на командування супротивником;

– порушення намірів супротивника;

– максимальний контроль інформаційно-телекомунікаційних мереж супротивника.

З цього випливає, що США забезпечують свою інформаційну безпеку шляхом попередження дій потенційного супротивника. Через наявність технологічної переваги, якою володіють США, країна має змогу отримувати, обробляти та використовувати інформацію, одночасно перешкоджаючи супротивнику здійснювати подібні речі. Це дає змогу США досягати військової переваги у невійськовий час.

Європейський Союз у забезпеченні своєї інформаційної безпеки пішов дещо іншим шляхом. Хоча найбільшою небезпекою для ЄС стала російська пропаганда, яка почала проявляти свою агресивність, починаючи з 2014 р., але заходи із забезпечення інформаційної безпеки реалізовувалися ЄС з початку формування інформаційної системи.

Ще з 1950-х рр. країни-члени ЄС почали виокремлювати інформаційні загрози та небезпеки як важливий складник інформаційного суспільства. Лісабонський договір 2009 р. перевів усі юридичні документи та заходи, які відповідали за забезпечення інформаційної безпеки, в юридичні норми ЄС [11, с. 42].

Ще у 2001 р. було видано Повідомлення «Мережева та інформаційна безпека: пропозиції по переходу для європейської політики». Цей документ зазначав основні тенденції, які були присутніми у системі забезпечення інформаційної безпеки.

Цей документ закріплює за інформацією та комунікаціями ключове місце серед факторів сучасного економічного та соціального розвитку. Через це питання інформаційної безпеки виноситься на перше місце в сучасному світі. Інформаційна безпека стосується усіх учасників комунікаційного процесу державної влади, приватних осіб та бізнесу.

З метою захисту від основних загроз інформаційної безпеки Європейський Союз сформував низку заходів:

1) підвищення освіченості населення в інформаційній сфері (створення і реалізація освітніх програм, обмін новітніми технологіями тощо);

2) створення системи попередження та інформування через взаємозв'язок аварійних служб та підвищення їх професіоналізму;

3) технологічна підтримка новітніх розробок у галузі забезпечення інформаційної безпеки;

4) створення законодавства в інформаційній сфері;

5) співпраця країн-членів у сфері вироблення спільних рішень щодо забезпечення безпеки державних установ та урядових організацій;

6) міжнародна співпраця країн із міжнародними організаціями у сфері інформаційно-комунікаційних технологій.

Після формування теоретичних положень європейської політики забезпечення інформаційної безпеки Європейська Комісія та інші установи ЄС почали їх втілення.

Велику увагу ЄС приділив боротьбі з кіберзлочинністю. Так, у 2007 р. ЄС видав Повідомлення «На шляху до загальної політики по боротьбі з кіберзлочинністю» [1, с. 108]. Основною його метою була поєднати роботу правоохоронних органів, держави та бізнесу у сфері боротьби з кіберзлочинами і забезпечити міжнародну співпрацю у цій сфері.

Оскільки у руках приватного сектору знаходиться велика частина інформаційної інфраструктури, то він, насамперед, має бути зацікавлений у боротьбі з кіберзлочинністю.

ЄС залучає до співпраці у цій сфері інші країни, які не є членами співтовариства.

Проводячи роботу серед власних громадян, ЄС зазначає, що мешканці Союзу мають використовувати ті технології, які вже перевірені. Усі користувачі інтернету мають бути захищені онлайн.

Тому, щоб максимально захистити громадян в інформаційному середовищі, необхідно реалізувати такі заходи:

1) підвищити рівень збирання та обробки інформації;

2) реалізувати технології захисту від кібератак;

3) створити єдину європейську базу з кіберзлочинністю;

4) реалізувати заходи і програм, які забезпечують боротьбу з кіберзлочинністю на міжнародному рівні;

5) розробляти засоби з інформування користувачів про порушення систем безпеки;

6) проводити навчальні заходи з підготовки та боротьби з можливими загрозами кібербезпеці;

7) запроваджувати гарячі лінії, які б змогли приймати інформацію про кіберзлочини.

На відміну від США, ЄС вживає заходів із захисту своїх мереж і громадян від негативних впливів, які можуть надійти з інформаційних мереж. Основну свою роботу ЄС зосереджує на захисті користувачів від онлайн-загроз та попередженні кібератак. Для того, щоб ці заходи стали ефективними, завдання Євросоюзу полягає в організації відповідної роботи на загальноєвропейському, міжнародному та національному рівнях. Оскільки ЄС не претендує на світового гегемона та не проводить політики активної присутності в усьому світі, він не ставить собі за мету контроль за діяльністю різних країн та угрупувань, які можуть бути потенційними супротивниками.

Найбільшу загрозу інформаційній безпеці ЄС протягом останніх років становить Росія. Це веде до погіршення внутрішньополітичної ситуації в певних країнах-членах ЄС, виникнення серйозних непорозумінь на наднаціональному рівні.

Після застосування санкцій до Російської Федерації Німеччина стала першочерговим об'єктом російських кібератак та пропаганди. Російська пропаганда має успіх. Мета Росії – послаблення єдності європейських кран. Європейські установи разом із НАТО почали вживати заходів із протидії російській пропаганді. Будь-яка проблема європейської політики опрацьовується Росією та доноситься до європейських громадян із негативного боку.

Через це у 2014 р. ЄС створив робочу групу, яка б вивчала можливості опору російській пропаганді [6, с. 7].

До цього питання долучилася і Україна, оскільки вона найбільше потерпає від російської пропаганди.

В Україні ситуація дещо інша, оскільки вона потрапила під вплив російської інформаційної агресії з перших днів незалежності. Нині інформаційна агресія Росії переросла у гібридну війну [5].

Розуміючи велике значення невоєнних методів перед силою зброї, Росія витрачає великі кошти на інформаційні ресурси. На Програму «Інформаційне суспільство» у 2011−2020 рр. видатки з російського бюджету мають становити 40,6 млрд дол. США. Зокрема, ця Програма включає поширення телепередач, які транслюються російськими ЗМІ по усьому світі [4].

Захищаючись від російської пропаганди, Україна має випрацювати власну модель інфор-

маційної безпеки, яка б змогла не лише розпізнавати негативні інформаційні впливи, але і вчасно їх знешкоджувати. Найбільше Росія маніпулює на наведеному нижче [9, с. 23]:

– завдавання шкоди іміджу України на міжнародній арені;

– зниження значимості України у геополітичному середовищі;

– висвітлення подій, які викривлюють та дестабілізують ситуацію;

– пропаганда меншовартості серед населення України;

– популяризація російської мови і зниження значення української, шляхом трансляції російськомовних фільмів, телепрограм, радіопередач.

Будуючи інформаційне суспільство, Україна має виробити модель власної інформаційної безпеки, з урахуванням міжнародного досвіду та аналізу інформаційної політики Росії, яка велася та буде вестися увесь час співіснування.

Інформаційна політика України має стосуватися внутрішніх і зовнішніх аспектів діяльності держави. Внутрішня інформаційна політика має бути спрямована на задоволення внутрішніх потреб у країні і суспільстві. Зовнішня політика має максимально забезпечувати просування інтересів України на міжнародній арені та формування позитивного іміджу [2, с. 110].

Як вважає більшість спеціалістів і дослідників інформаційного суспільства, адекватне використання інформації в розвиненому інформаційному середовищі сприяє формуванню інформаційної державної політики [7].

Висновки та перспективи подальших розвідок у цьому напрямі. З огляду на вищевикладене, можемо зазначити, що вплив на український інформаційний простір інших держав може здійснюватися через відсутність механізмів у забезпеченні її інформаційної безпеки. Тому система інформаційної безпеки України повинна мати аналогію з європейськими підходами та бути максимально інтегрованою в європейські безпекові мережі. Засоби масової інформації мають бути з'єднуючою ланкою між Європейським Союзом, європейськими цінностями, підходами, стилем життя та українським населенням. Оскільки в Україні спостерігається нерівномірне забезпечення інформаційними ресурсами населення, пріоритетним завданням, яке стоїть перед українською владою, є створення інформаційного середовища, яке б охоплювало усю територію України, а інформаційні продукти, які створюються в Україні, могли б поширюватися на міжнародному ринку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Европейское право. Право Европейского Союза и правовое обеспечение защиты прав человека: Учебник для вузов / Рук. авт. колл. и отв. ред. д.ю.н., проф. Л.М. Энтин. М.: Норма, 2007. С. 108−109.

2. Карпенко В.О. Інформаційна політика та безпека: [підручник] / В.О. Карпенко. К.: Нора-Друк, 2006. 320 с.

3. Роговский Е.Л. Создание военно-промышленного комплекса США. Экономика США / Под ред. В.Б. Супяна. СПб.: Питер, 2003. С. 386.

4. Російська пропаганда. URL: http://forum.pravda.com.ua/index.php?topic=786907.

5. Российская пропаганда завоевывала сердца и умы Евросоюза. URL: http://geopolitica.info/euobserver-rossiyskaya-propaganda-zavoevala-serdtsa-i-umy-evrosoyuza.html.

6. Хоружий Г. Російська гібридна пропаганда як складова «Гібридної війни». Освіта регіону. 2016. № 4. С. 6−15.

7. Чиж І.С. Україна: шлях до інформаційного суспільства. К.: Либідь, 2004. 287 с.

8. Шариков П.А. Политика США в области информационной безопасности: дис. … канд. полит. наук / Учреждение Российской Академии наук Институт США и Канады РАН, М. 2009. 215 с.

9. Шевчук П. Інформаційно-психологічна війна Росії проти України: як її протидіяти. «Демократичне врядування». Науковий вісник. 2014. Вип. 13. С. 23−28.

10. Шлыков В. Глобализация военной промышленности. Время новостей. 2006. № 15, 31 января.

11. Энтин Л.М. Право Европейського Союза. Новый етап эволюции: 2009−2010 годы. М.: Изд-во Аксиом, 2009. С. 42−46.