УДК 35.1

Сагайдак О. В.

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ГЛОБАЛІЗАЦІЙНИХ ВИКЛИКІВ

Periculum in mora (небезпека у зволіканні)
Тіт Лівій

Сьогодні світ перебуває на новому етапі свого розвитку – інформаційному. Тому, питання інформаційної безпеки та політики дуже актуальне, а особливо для України, бо як це не прикро, у цих питаннях ми програємо. На жаль, ми далеко відстали від могутніх геополітичних та геоекономічних суб'єктів міжнародних відносин і навіть від сусідів у сфері захисту національних інформаційних інтересів нашої держави.

Що ж таке інформація? Поняття інформації є дискусійним. Це явище має багато визначень залежності від контексту. У Законі України «Про інформацію» під інформацією розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та довколишньому природному середовищі [1]. Це досить влучне визначення, але суто правове. У розумінні багатьох експертів, інформація – це повідомлення, незалежно від форми його подання [2].

Що насправді являє собою нове інформаційне суспільство? Концепція інформаційного суспільства є одним з різновидів теорії постіндустріального суспільства, основу якої заклали З. Бжезинський, Д. Белл, У. Мартін, О.Тоффлер, Е. Гідденс, К. Ясперс, Р. Коен, А. Турен, Г. Кан, А. Дракер, Ф. Уебстер та ін. Згідно з даною концепцією головним фактором у розвитку суспільства є виробництво та використання науково-технічної й іншої інформації. Якщо розглядати суспільство, як зміну стадій, то з позицій прибічників даної концепції виникнення інформаційного суспільства пов'язано з домінуванням інформаційного сектора економіки, «четвертого». Він йде наступним за сільським господарством, промисловістю та сферою економічних послуг. Питаннями інформаційної безпеки України займаються В.А. Ліпкан, В.М. Бегма, О.О. Остроухов, Ю.Є. Максименко, В.П. Малинка, К.В. Рубель, В.А. Кормич, В.М. Петрик, О.М. Андрєєва та ін.

Метою цієї публікації є окреслення змісту та тенденцій розвитку моделі інформаційної безпеки України, на доктринальному рівні розкрити зміст сучасних тенденцій і глобалізаційних викликів у сфері інформаційних технологій впливу на масову свідомість.

«Спочатку була «перша хвиля», яку можна назвати «сільськогосподарською цивілізацією». Від Китаю та Індії до Беніну і Мексики, від Греції до Риму виникали та занепадали цивілізації, внаслідок їхніх зіткнень народжувалося багато строкатих картин. Та за

розбіжностями ховалися фундаментальні спільні риси. Земля була основою економіки, життя, культури, сімейної організації та політики. Панував простий розподіл праці та існував чіткий розподіл каст та класів: знать, духовенство, воїни, ілоти, раби та кріпаки. Влада була авторитарною. Соціальне походження людини обумовлювало його місце в житті. Економіка була децентралізована, а тому кожна община виробляла більшу частину того, чого потребувала. Триста років тому – плюс-мінус півстоліття – відбувся вибух, ударні хвилі якого пройшли всією планетою. Цей вибух – промислова революція. «Друга хвиля» змінила інститути та спосіб життя мільйонів… До середини 20 століття сили «першої хвилі» були розбиті і на землі запанувала «індустріальна цивілізація». Але ненадовго, бо з її перемогою розпочалася нова – третя за рахунком – «хвиля». Вона принесла з собою нові інститути, відносини, цінності» [3].

Як вважає професор У. Мартін, під інформаційним суспільством треба розуміти «розвинуте постіндустріальне суспільство», що виникло перш за все на Заході. Не випадково таке суспільство затверджується перш за все в Японії, США та ЄС, де сформувалось постіндустріальне суспільство. У. Мартіном було зроблено спробу дати йому основні характеристики за такими критеріями:

- соціальний (інформація виступає як важливий стимулятор зміни якості життя, формується «інформаційна свідомість» за широкого доступу до інформації);
- політичний (свобода інформації, яка веде до активізації участі та консенсусу між різними прошарками суспільства (тут потрібно відмітити, що завдяки цьому стала можливою маніпуляція масової свідомості. Такий спосіб легітимізації влади та управління віднайшов своїх прихильників. Це й зрозуміло, бо відкритий примус («батіг») – це боляче, а «духовний наркотик» («пряник» маніпуляції) – приємно. Головною умовою підтримання такого порядку є свобода інформації та індивіда, яка дозволяє йому в кожному акті «війни» робити псевдораціональний вибір і укласти псевдовільний контракт. Неважливо, йдеться про здійснення покупки чи продажу робочої сили, тієї чи іншої гумової резинки чи програми на виборах) [4];
- економічний (інформація є ключовим фактором в економіці як ресурсу, послуги, товару, джерела надлишкової вартості та зайнятості (стала можливою глобалізація, поширення ринкових економічних відносин));
- технологічний (ключовий фактор – інформаційні технології, які широко використовуються у виробництві, системі освіти, побуті);
- культурний (визнання культурної цінності інформації через затвердження інформаційних цінностей в інтересах індивіда та суспільства в цілому (завдяки цьому відбулася «вестернізація», поширення «західних» цінностей – прим. автора)).

При цьому Мартін особливо підкреслює думку про те, що комунікація є ключовим елементом інформаційного суспільства [5; с. 115–123].

Інформаційна сфера є системоутворюючим фактором життя суспільства, що активно впливає на стан внутрішньо- та зовнішньополітичної, економічної, соціальної, оборонної та інших складових національної безпеки будь-якої держави. Вона суттєво залежить від організації інформаційної безпеки, а в ході науково-технічного прогресу така залежність буде лише посилюватися. Під інформаційною безпекою сьогодні розуміють стан захищеності національних інтересів в інформаційній сфері, що становлять сукупність збалансованих інтересів особистості, суспільства та держави («Доктрина інформаційної безпеки РФ» від 9 вересня 2000 року) [6]. Вона, з одного боку, є невід'ємною складовою кожної зі сфер забезпечення національних інтересів, а з другого – важлива самостійна сфера організації національної безпеки країни.

Тому сьогодні перед нашою країною стоїть проблема захисту національних інформаційних інтересів, досягнення інформаційної безпеки. Україна повинна бути у ритмі формування глобального інформаційного суспільства, щоб не залишитись на узбіччі сучасних цивілізаційних процесів.

Суб'єктами інформаційної безпеки є:

- держава, державні органи та структури, що займаються її забезпеченням на державному рівні (це можуть бути органи не тільки виконавчого механізму влади, а й законодавчого, судового);
- інституалізовані форми вироблення конкурентоспроможного інформаційного продукту [7; с. 52–53].

Технічні об'єкти інформаційної безпеки:

- інформаційні ресурси;
- інформаційна інфраструктура;
- інформаційні технології [8; с. 81–86].

Об'єкти інформаційної безпеки (беручи до уваги «Доктрину інформаційної безпеки РФ»):

- особа – її права та свободи в інформаційній сфері, техніка та свідомість;
- суспільство – його духовні цінності, засади солідарної діяльності;
- держава – її конституційний лад, ефективне функціонування, суверенітет [6].

Таким чином, можна виокремити три групи національних інтересів:

а) для людини:

реалізація прав і свобод людини і громадянина щодо одержання, використання, поширення, зберігання інформації; забезпечення права

людини на захист від маніпуляції індивідуальною свідомістю; захист права інтелектуальної власності, захист енергоінформаційної безпеки людини тощо;

б) для суспільства:

побудова інформаційного суспільства; забезпечення плюралізму засобів масової інформації; захист від маніпуляції масовою свідомістю; розвиток духовності, моральних засад, інтелектуального потенціалу українського народу, зміцнення психічного здоров'я нації.

в) для держави:

забезпечення інформаційного суверенітету; унеможливлення монополізації інформаційного простору; іноземними компаніями або транснаціональними корпораціями; створення конкурентоспроможних інформаційних технологій та технологій зв'язку; збереження та зміцнення науково-технологічного потенціалу; інтеграція України в європейський інформаційний простір; боротьба з інформаційною злочинністю тощо [9; с. 79–80].

Загрози інформаційній безпеці, з одного боку, є організаційний компонент системи державного управління, а з іншого – слугує індикатором ефективності її функціонування. Адже реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування даної системи, і навпаки. На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно *з* урахуванням того контексту, в якому вони виникають і проявляються. Найбільш небезпечною на даному етапі для розвитку українського суспільства є проведення інформаційних війн - крайньої форми інформаційного протиборства.

Інформаційне протиборство – це суперництво соціальних систем (країн, блоків країн) в інформаційній сфері впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті чого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку [9; с. 98].

За інтенсивністю, засобами, що використовуються, та масштабами виділяють такі ступені інформаційного протиборства: інформаційна експансія, інформаційна агресія, інформаційна війна.

У новому суспільстві і війни нові. Які ж війни переживатиме в майбутньому людство? Слід відмітити, що однозначної відповіді на ці питання нині немає, але існує декілька гіпотез. Найбільш поширена сьогодні гіпотеза відомого американського політолога, директора Інституту стратегічних досліджень при Гарвардському університеті – Семюеля Хантінгтона, висунута ним в 1993 році у відомій статті “Зіткнення цивілізацій”.

Він запевняє, що у XXI ст. основним джерелом конфліктів буде вже не ідеологія і не економіка. Найважливіші кодони, які розділяють людство і домінуючі причини конфліктів, будуть визначатися культурою. Нація-держава залишиться головною дійовою особою у міжнародних справах, але

найбільш значущі конфлікти глобальної політики будуть розгортатися між націями і групами націй, що належать до різних цивілізацій. Зіткнення цивілізацій стане домінуючим фактором світової політики. Лінії розлому між цивілізаціями – це і є лінії майбутніх фронтів. За Хантінгтоном, ідентичність на рівні цивілізацій буде в подальшому розвитку людства все більш значущою, обличчя світу значною мірою формуватиметься в ході взаємодії семи-восьми великих цивілізацій. До них належать західна, китайська, японська, ісламська, індуїстська, православно-слов'янська, латиноамериканська і, можливо, африканська (в стадії формування). Україні Хантінгтон відводить особливе місце, бо вона лежить на лінії розлому між трьома цивілізаціями: західною, православно-слов'янською та ісламською [10].

Сьогодні вже йдеться про початок ери воєн «сьомого покоління», інформаційних воєн Це війни з використанням маніпуляцій індивідуальною та масовою свідомістю, нейрон-лінгвопрограмування, діяльність проти системи управління суперника, кібернетична, економічна боротьба, боротьба з використанням хакерів, власне військова боротьба з використанням високоточної керованої зброї, переваг свого геополітичного та геоекономічного становища, здобутків операції проти волі нації та національних культур («політика подвійних стандартів», маніпулятивна пропаганда, «переписування історії», метод «ставлення опонента в становище сторони, що виправдовується») та ін. «PR»-заходів.

Інформаційна війна – це є найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї). Вперше термін «інформаційна війна» начебто з'явився у наш час наприкінці 80-х років XX століття. Він став результатом плідної праці теоретиків збройних сил США і став уживаним після вдало проведеної роботи по знищенню СРСР. Насправді першими це зробили китайці. Що стосується іншого розуміння – технічного, то тут обов'язковою умовою є те, що ведення інформаційної війни є результатом узгодженої діяльності з використання інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності [9; с. 99].

У безконтактних війнах «інформаційне протиборство» або «інформаційна війна» (крайній прояв протиборства) є законним і є боротьбою сторін у перевазі в кількості, якості та швидкості отримання, аналізу і використання інформації. Зрозуміло, що цей вид протиборства, як і інші його види в безконтактних війнах, вже зараз мають дві чітко визначені складові: оборонну та наступальну(ударну).

Оборонна – захист власної інформаційної інфраструктури від впливу конкурента, організація безпеки власних інформаційних ресурсів.

Для оборонної складової в дистанційних безконтактних війнах можуть використовуватися такі форми та способи організації безпеки власних інформаційних систем та ресурсів як оперативне та стратегічне маскування, фізичний захист об'єктів інформаційної інфраструктури, дезінформація, радіоелектронна боротьба та ін.

Наступальна (атакуюча) складова – дезорганізувати та зламати інформаційну інфраструктуру суперника, розладнати процес оперативного управління його силами та ресурсами. Для ударної складової характерні наступні способи боротьби: стратегічне маскування, дезінформація, радіоелектронне протиборство, фізичне знищення об'єктів інформаційної інфраструктури, «атаки» на комп'ютерні мережі супротивника, «інформаційна експансія», «інформаційна агресія», «інформаційні удари» [11].

Інформаційна експансія — це діяльність для досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою:

1. поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;
2. витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;
3. збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ;
4. нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і т. п. [9; с. 98].

Інформаційна агресія – це незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих сферах його діяльності шляхом обмеженого та локального за своїм масштабом застосування сили. Ознаки інформаційної агресії:

1. виключення із засобів інформаційної дії найбільш небезпечних видів, що не дозволяють надійно контролювати масштаби завданого збитку – інформаційної зброї;
2. обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційної дії (агресія зачіпає інформаційний простір держави-жертви не цілком, а тільки його частину);
3. обмеження за метою (переслідує локальну, приватну мету) і часу (як правило, агресія припиняється після повного досягнення агресором усієї поставленої конкретної мети й рідко набуває затяжного характеру), а також по силах і засобах, що залучаються [9; с. 98-99].

Для реалізації розробленої в США Концепції інформаційної війни на державному рівні виділяються шість основних складових:

1) боротьба з системами управління супротивника;

2) боротьба на основі розвідувальних технологій, електронна боротьба;
3) економічна інформаційна боротьба;
4) психологічна боротьба;
5) кібернетична боротьба;
6) боротьба з використанням хакерів.

Для вирішення завдань інформаційного протиборства створюються відповідні органи управління, сили та засоби. Так, у ЗС США керівництво захистом інформаційної інфраструктури покладено на управління інформаційних систем МО. Для організації та ведення наступальних заходів ІБ усі види ЗС мають власні центри. Центр ІБ сухопутних військ створений у 1994 році, міститься у форті Белвуар (штат Вірджинія). Аналогічний центр ВМС, також створений у 1994 р., розташовано у форті Мід (штат Меріленд). Центр ІБ Військове – Повітряних Сил створений ще раніше в 1993 р., на авіабазі Келі (м. Сан-Антоніо, штат Техас). Дії цих центрів координуються створеним у січні 1995 р. центральним органом МО США - виконавчим комітетом з питань ІБ, головне завдання якого полягає в прискоренні «розроблення та досягнення цілей ІБ». Аналогічні структури створюються і в стратегічних об'єднаннях. Продовжується також розвиток органів ІБ і по вертикалі. Структури психологічних операцій в США створені у межах ЦРУ та МО, а саме в об'єднаному командуванні спеціальних операцій. Принципові рішення з питань проведення психологічних операцій приймає воєнно-політичне керівництво США в особі Президента, уряду та Конгресу. Президент, як верховний головнокомандувач, здійснює загальне керівництво психологічними операціями через раду національної безпеки та міністерство оборони, а оперативне керівництво – через Комітет начальників штабів.

А як справи з питаннями інформаційної безпеки в наших найближчих сусідів? У Війську Польському завдання чинити інформаційно-психологічного вплив на війська і населення супротивника для досягнення політичних, військових і пропагандистських цілей покладено на центральну групу психологічних дій (ЦГПД) (місце дислокації – м. Бидгощ). Центральна група психологічних дій складається зі штабу, а також з інформаційно-аналітичних, теле- і радіомовних, редакційно-видавничих і тилових підрозділів. Особовий склад лише кадровий. Середній вік польських фахівців психологічних операцій 32 роки. Більшість з них володіє декількома іноземними мовами, у тому числі англійською – не менш 75% військовослужбовців. Практично весь командний склад стажувався в структурах психологічних операцій натовських армій, має досвід роботи в штабах об'єднання збройних сил альянсу різного рівня, брав участь у миротворчих операціях. Відповідно до планів генерального штабу щодо подальшої

реорганізації ЗС Польщі на 2003–2008 роки, передбачається включити ЦГПД до складу національних сил спеціальних операцій, які планують сформувати, а на основі її керівного складу створити в структурі ГШ управління психологічної боротьби.

До останнього часу Росія не мала власної державної концепції з проблем інформаційного протиборства. Деякі російські фахівці вважають, що саме її відсутність була одним із факторів розпаду СРСР і поразки у «холодній війні». «Доктрина інформаційної безпеки Росії» була підписана президентом Російської Федерації лише у вересні 2000 року, її головною особливістю є врахування інтересів трьох основних об'єктів національної безпеки: особи, суспільства та держави. Забезпечення інформаційної безпеки та впровадження основних положень Доктрини здійснюється Управлінням інформаційної безпеки при Раді безпеки РФ. Її експерти вважають, що для забезпечення інформаційної безпеки Російської Федерації необхідно створити особливий координаційний орган. Цей орган матиме право контролювати розробку, а також застосування інформаційної зброї, здійснювати нагляд за роботою міжвідомчого аналітичного центру з проблем інформаційно-психологічних технологій на базі ФСБ, МВС, ЗС та Ради безпеки РФ [9; с. 102–107].

Наприкінці 2009 року в газ. «Дзеркало тижня» було надруковано статтю вже колишнього Голови Служби зовнішньої розвідки України Миколи Маломужа «Про стратегію подолання загроз національній безпеці України на початку XXI століття». Про інформаційну та соціальну безпеку нашої країни ним були заявлено таке: «Треба сформулювати й активно реалізовувати в Україні інтеграційну гуманітарну політику, яка має включати формування сучасної української ідентичності, єдиного інформаційного простору, гнучке розв'язання мовного питання, відмову від нав'язування поглядів з принципових питань гуманітарної політики (міжконфесійних відносин, ставлення до історичного минулого Вітчизни), з яких у суспільстві немає єдності. Паралельно створити дійову загальнодержавну систему протидії іноземним інформаційним впливам на українське суспільство із залученням ресурсів національних міністерств та відомств, спеціальних служб, неурядових і громадсько-політичних організацій, державних і комерційних дослідницьких та аналітичних структур, ЗМІ тощо» [12]. Це вселяє оптимізм, бо якщо в ЗМІ надруковано статтю такого службовця ще й з такого питання як інформаційна безпека України, то не все у нас в цьому напрямку втрачено. В тій статті аналізується взагалі стан речей в сфері національної безпеки нашого суспільства і розглядається аспект не лише інформаційної, а й соціальної та гуманітарної, науково-технічної, економічної, зовнішньополітичної та внутрішньополітичної, державної, енергетичної, воєнної безпеки (тобто всіх складових безпеки нації). В статті ним було зроблено влучні та актуальні висновки по кожній з складових цієї безпеки. Прикро, що про це говорять журналісти, кадрові

офіцери, а наші політики стосовно питань забезпечення національних інтересів переважно відмовчуються.

Лише на 17 році незалежності було прийнято «Стратегію національної безпеки» Указом Президента України від 12 лютого 2007 року №105/2007[13]. «Доктрину інформаційної безпеки» не прийнято й по цей день. Це є причиною неналежного ідеологічного та організаційно-правового оснащення органів держави, котрі реалізують її політику в цій сфері. Прийняття «Доктрини інформаційної безпеки України» повинно надати нового стратегічного імпульсу діяльності органів державної влади, а також певною мірою інститутів громадянського суспільства в організації інформаційної безпеки України, формуванні і реалізації державної інформаційної політики. За доктриною (в якій буде закріплено основні принципи вирішення даної проблеми), повинні бути розроблені концепція – сукупність правових норм,які визначать напрямки діяльності; стратегія, яка визначить інформаційні цінності,засоби і методи протидії загрозам; програма – сукупність правових норм, які будуть безпосередньо регулювати діяльність суб'єктів організації інформаційної безпеки; і план інформаційної безпеки України – деталізація діяльності в конкретній ситуації.

Останні події – питання по о. Тузла, газовий конфлікт, втрата частини чорноморського шельфу в районі о. Зміїний, питання стосовно гирла р. Дунай – доводять, що Україна програє свою інформаційну війну. Головною проблемою України в сфері організації інформаційної безпеки сьогодні є відсутність якісного конкурентоздатного інформаційного продукту, який би поширювався на нашій території та на теренах інших суб'єктів міжнародних відносин. Констатую, що ми програємо сучасну інформаційну війну,а в геополітиці, як і в спортивних змаганнях, рахуються тільки з лідерами, сильними світу цього. Ми, на жаль, якщо й не аутсайдери, то в цьому плані все одно плентаємося у хвості планети всієї. Тому, нагадаю дуже влучні слова Тіта Лівія «Periculum in mora» (небезпека у зволіканні).

Таким чином, в умовах становлення української державності, демократизації суспільного життя та формування цивілізованої ринкової системи господарювання забезпечення національної безпеки нашої держави набуває особливої ваги. Національна безпека України – це спосіб самозбереження народу України, який досяг рівня організації і національного буття у формі незалежної держави. Це один із чинників, що забезпечує його державно-організоване існування, вільний саморозвиток, надійний захист інтересів від зовнішніх і внутрішніх загроз.

Література

1. Закон України «Про інформацію» від 02.10.92, ВВР, 1992, N 48. http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.
2. Федеральный закон «Об информации, информационных технологиях

и о защите информации» от 27.07.2006 г. № 149-ФЗ http://www.systema.ru/inc/bkard.php?Id=97653. **3. Тоффлер Э**. Третья волна. – М.: АСТ, 2004. http://www.gumer.info/bibliotek_Buks/Culture/Toffler/_Index.php. **4. С.Г.Кара-Мурза** "Манипуляция сознанием" http://www.kara-murza.ru/books/manipul/manipul_content.htm. **5. Мартин У**. Дж. Информационное общество (Реферат) // Теория и практика общественно-научной информации. Ежеквартальник / АН СССР. ИНИОН; Редкол.: Виноградов В. А. (гл. ред.) и др. – М., 1990. – № 3. – С. 115–123. **6. «Доктрина** информационной безопасности РФ» подписана Президентом РФ от 9 сентября 2000 г. http://www.justice4.net/law_miscellaneous_2.php. **7. Петрик В. М.,** Кузьменко. А. М., Остроухов В. В. Соціально-правові основи інформаційної безпеки: Навчальний посібник – К.: Росава, 2007. – 496 с. **8. Бегма В.М.,** Малинка В.П., Рубель К. В. Концептуальные подходы к определению категориально-понятийного аппарата информационной безопасности Украины / Национальная безопасность: украинское измерение: щокв. наук. сб. / Совет нац. безопасности и обороны Украины, Ин-т пробл. нац. безопасности; Редкол.: Горбулин В.П. (Голов. ред.) [И др.]. – К., 2008. – Вип.1 (20-21). – С. 81–86. **9. Ліпкан В.А.,** Максименко Ю.Є. Інформаційна безпека України в умовах Євроінтеграції: Навчальний посібник – К.: КНТ, 2006. – 279 с. **10. Хантингтон С.** Столкновение цивилизаций. – М.: АСТ, 2003. http://grachev62.narod.ru/hantington/content.htm. **11. Слипченко В. И.** Войны шестого поколения. Оружие и военное искусство будущего. – М.: Вече, 2002. http://www.pseudology.org/colonels/War6Genaration/index.htm. **12. Маломуж М.** Про стратегію подолання загроз національній безпеці. України на початку XXI століття // Дзеркало тижня № 46 (774) 28 листопада – 4 грудня 2009. http://www.dt.ua/1000/1550/67893/ **13. Указ** Президента України № 105/200 «Про Стратегію національної безпеки України» від 12 лютого 2007 року. www.president.gov.ua/documents/5728.html

Сагайдак О. В. Інформаційна безпека України в умовах глобалізаційних викликів

Розглянуто загальні засади побудови національної системи інформаційної безпеки. Узагальнено світовий досвід щодо державної політики протидії інформаційним загрозам і атакам. Взято за методологічну основу дослідження теорію „третьої хвилі” О. Тоффлера задля розкриття змістовних ознак інформаційного суспільства (суспільства знань). Досліджено фактори впливу на інформаційний простір держави, докладно проаналізовано концептуальні засади майбутньої Доктрини інформаційної безпеки України та ін.

Ключові слова: інформація, інформаційна безпека, інформаційні загрози, інформаційні війни, інформаційне суспільство, національна безпека, постіндустріальне суспільство.

Сагайдак О. В. Информационная безопасность Украины в условиях глобализационных вызовов

Рассмотрены общие принципы построения национальной системы информационной безопасности. Обобщен передовой опыт стран мира в вопросах противодействия информационным угрозам и атакам. За методологическую основу исследования выбрана теория «третей волны» О. Тоффлера с целью выявления существенных составляющих информационного общества (общества знаний). Исследованы факторы воздействия на информационное пространство государства, детально проанализированы концептуальные основы будущей Доктрины информационной безопасности Украины и т. д.

Ключевые слова: информация, информационная безопасность, информационные угрозы, информационные войны, информационное общество, национальная безопасность, постиндустриальное общество.

Sagaidak O. V. Information security of Ukraine under conditions of globalization challenges.

The general principles for constructing a national system of information security are reviewed. Here summarized the best practices of the world in the sphere of information threats and attacks. For the methodological basis of research selected the theory of "third wave" by Toffler to identify the essential components of an information society (knowledge society). The factors which influence on the information space of the state are reviewed and the conceptual foundations of the future Information Security Doctrine of Ukraine are analyzed in details, etc.

Key words: information, information security, information threats, information war, information society, national security, post-industrial society.

УДК 316

Швирков О. І.

ІНФОРМАЦІЙНА ЕРА ТА МЕРЕЖЕВІ СТРУКТУРИ: НОВІ МОЖЛИВОСТІ ДЛЯ ЖІНКИ

Бізнес сьогодні – це висококонкурентне середовище, що потребує від людини сильної волі, високих енерго- та розумових затрат, та й просто немалої фізичної сили та витривалості. Особливо це стосується малого та середнього бізнесу, де конкуренція особливо