3. Вінничук Н. Ю. Становлення та розвиток опозиції як політичного інституту// Політологічний вісник. Збірник наук. праць. – 2006. – Вип. 21. – С. 28-36.
4. Вінничук Н. Ю. Типологія політичної опозиції// Політичний менеджмент. – 2007. – № 3 (24). – С. 51-59.
5. Висоцький О. Ю. Демократія як інструмент легітимаційної політики // Грані. – Д., 2006. – № 4. – С. 113-117.
6. Лапаева В. В. Права и многопартийность в современной России. – М.: Норма, 1999. – С. 17-18.
7. Лебедев В. А., Киреев В. В. Конституционно-правовые аспекты взаимодействия демократического государства и политических партий // Конституционное и муниципальное право. – 2009. – № 2. – С. 2-5.
8. Оппозиция политическая // http://mirslovarei.com/content_pol/OPPOZICIJA-POLITICHESKAJA-1240.html
9. Павленко Р. Опозиція: права і повноваження // Людина і політика. – 2002. – № 4. – С. 3-10.
10. Побочий І. А. Влада та опозиція: конфліктний аналіз взаємовідносин // Грані. – 2007. – № 1. – С. 115-119.
11. Проект Закону України "Про опозиційну політичну діяльність" від 16.05.2005р. № 2007-1. // http://search.ligazakon.ua/l_doc2.nsf/link1/ed_2005_05_16/JD1JR01A.html#
12. Political institutions in the United Kingdom by David Judge. – Oxford University Press, 2005. – 323p.
13. Political Oppositions in Western Democracies. /edited by Robert A. Dahl – Yale University, 1966. – 458p.
14. Politics, Law and Social Change. Selected essays of Otto Kirchheimer. / edited by Frederic S. Burin and Kurt L. Shell. – Columbia University Press. New York and London, 1969. – 483p.

Піщевська Е. В., ОНУ ім. І. І. Мечникова

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СУЧАСНОМУ СВІТІ

В данной статье анализируется информационная безопасность в контексте проблем национальной безопасности. Уточняется соотношение понятий "национальная безопасность" и "информационная безопасность", рассматривается сущность информационного противоборства в современном мире.

This article analyzes the information security in the context of national security issues. We improve relations between the concepts "national security" and "information security", is considered the essence of information confrontation in the modern world.

Актуальність даної статті полягає в тому, що на сучасному етапі основними реальними і потенційними погрозами інформаційній безпеці є прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожує сталому і безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Зросли зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також через Інтернет [1].

Мета статті – проаналізувати інформаційну безпеку в контексті проблем національної безпеки.

Завдання статті: дослідити співвідношення понять "національна безпека" і "інформаційна безпека", розглянути сутність інформаційного протиборства на сучасному світі.

Як відомо, вперше в політичному лексиконі поняття "національна безпека" було використане в посланні президента Т. Рузвельта Конгресу США в 1904 р., де він обґрунтував приєднання зони Панамського каналу до національних інтересів Сполучених Штатів Америки. Даний факт з'явився поштовхом в науковому осмисленні національних інтересів в контексті національної безпеки [2]. Тому невипадково деякі з дослідників-юристів підкреслюють політичне походження даного поняття, "що, з одного боку, обумовлює його нерозривний зв'язок з державною діяльністю і державною політикою, а з іншого – створює певні труднощі при правовому регулюванні пов'язаних з нею питань через декларативність та нестабільність деяких її аспектів" [3].

Уперше поняття "національна безпека" та "національні інтереси" на законодавчому рівні були визначені в "Концепції (основах державної політики) національної безпеки Україні", яка була прийнята Верховною Радою Україні [4]. У ній визначається, що захист національної безпеки є однією з найважливіших функцій держави. У цьому контексті інформаційна безпека, як невід'ємна складова національної безпеки, потребує свого забезпечення на державному рівні, оскільки протягом усієї історії розвитку людства інформація розглядалася як важливий військовий, політичний, економічний і соціальний фактори, що значною мірою обумовлює розвиток держави, суспільства і особистості в конкретних історичних умовах [5].

На думку українського ученого Б. Корміч, "національна безпека представляє собою стан захищеності гарантованих законодавством розумів життєдіяльності держави, суспільства та окремої особини від внутрішніх та зовнішніх загроз. Підтримання національної безпеки

є важливим напрямком державної діяльності, що актуалізується в залежності від наявності та ступеня відповідних загроз" [6].

Український дослідник Ю. Максименко пропонує визначати національну безпеку як результат управління реальними чи / та потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави [7].

У цілому, до основних проблем, які несуть ризики й загрози національній безпеці Україні, експерти відносять такі явища, властиві багатьом державам, як: боротьба за енергоресурси, техногенні катастрофи, міжнаціональні й міжконфесійні конфлікти, тероризм, наркоторгівля, організована злочинність і корупція, нелегальна міграція, торгівля людьми, демографічні проблеми тощо. Особливу загрозу становлять тенденції консолідації національних і міжнародних злочинних угруповань, об'єднання кримінальної злочинності з націоналістичними й екстремістськими угрупованнями.

Активізація терористичної діяльності, яка все більше набуває глобального характеру, посилює небезпеку для будь-якої окремо взятої країни і пов'язується переважно з міжнаціональними й міжконфесійними конфліктами й сепаратистськими рухами. Терористичні організації перетворилися на інструмент досягнення певних політичних цілей і, дуже часто, високоприбуткового злочинного бізнесу. Повсякчасна загроза міжнародного тероризму трансформувалася в один з основних викликів світовій цивілізації [8].

Перехід ряду держав в постіндустріальну фазу суспільного розвитку сприяє швидкому розвитку комунікативних технологій, що підсилює потребу в боротьбі за здобуття якісної інформації. Новий вигляд безпеки – інформаційна безпека. Її відмінність від інших складових національної безпеки в нематеріальності. Таким чином, на державному рівні виникає потреба в додаткових матеріальних витратах з боку компетентних органів влади в її перевірці. Як відзначають дослідники, "інформаційна складова не може існувати поза цілями загальної національної безпеки, так само як і національна безпека не буде всеохоплюючою без інформаційної безпеки" [9].

Інформаційна сфера є в даний час системообразующей сферою життя суспільства. З цієї причини вона активно впливає на стан політичної, економічної сфери, а також інших складових національної безпеки. У політичній сфері все більшої значущості набуває інформаційно-психологічна дія з метою формування стосунків в суспільстві, його реакції на процеси, що відбуваються. У економічній сфері зростає уразливість економічних структур від невірогідності,

запізнювання і незаконного використання економічної інформації. У сфері духовного життя виникає небезпека розвитку в суспільстві за допомогою електронних засобів масової інформації агресивної споживчої ідеології, поширення ідей насильства і нетерпимості та інших негативних дій на свідомість і психіку людини [10].

Як показує практика останніх років, чим вище активність громадян, організацій або держав в кіберпросторі, тим перед суспільством гостріше встають проблеми забезпечення своєї інформаційної безпеки. І сьогодні є всі підстави вважати, що національна безпека країн залежатиме від забезпечення інформаційної безпеки. По мірі ж інтенсифікації технічного прогресу і посилення "електронної співпраці" держав, ця залежність постійно зростатиме [11].

Як вважає військовий експерт С. Гріняєв, сьогодні істотна доля всіх суперечностей між державами перенесена в інформаційну сферу. Дана обставина привела до трансформації підходів до поняття "військової сили". На зміну "грубій силі" зброї приходить "м'яка сила" переконання і психологічної маніпуляції. Реалізація цього принципу вимагає перегляду підходів до формування військової стратегії нової епохи. Домінуюча роль інформації і інформаційних технологій, а також орієнтація на парирування принципово нових погроз інформаційної епохи, змусили керівництво деяких західних країн, і перш за все США, активніше упроваджувати нові концепції будівництва озброєних сил [12].

Б. Корміч вважає за необхідне пов'язувати національну безпеку та її інформаційну складову з функціонуванням держави, що створює ресурс захисту безпеки, і з розвитком системи міжнародного співробітництва задля створення безпечних умов для кожної держави [13].

Особливе місце в системі інформаційної безпеки займає інформаційне протиборство. Його особливість в тому, що воно ведеться державними органами інформаційної безпеки з формуваннями, що мають різне суспільне (державне) положення (фізичні особи, юридичні особи, суб'єкти міжнародного права) і які зловмисно створюють інформаційні погрози життєво важливим інтересам особи і суспільству. Ця обставина обумовлює значущість його цілей і ширший арсенал засобів, використованих для їх досягнення. У зміст інформаційного протиборства, окрім інформаційного забезпечення і інформаційного захисту, входить комплекс заходів інформаційної протидії, спрямованих на блокування інформації, яка цікавить різного роду зловмисників, і доведення до них помилкових відомостей.

Як відзначає С. Пірумов, "інформаційний простір практично став театром військових дій, де кожна з протиборчих сторін прагне отримати і як можна довше утримувати перевагу, а у разі потреби – розгромити противника. Стає очевидним, що сторона, яка не розуміє або недооцінює вказану обставину, приречена виявитися на узбіччі стовпового шляху цивілізаційного розвитку" [14].

Інформаційно-психологічні методи дії стають усе більш масштабними і політично результативними, і тому все частіше використовуються державами для досягнення своїх політичних цілей замість так званих "гарячих" воєн. У світовій практиці міждержавних відносин створюються умови не лише для послідовної трансформації озброєного протистояння в інформаційне протиборство, але і для перетворення її на самостійний напрям зовнішньої політики розвинених держав. Так, С. Гріняєв вважає, що цілі національної політики США досягатимуться шляхом ведення стратегічного інформаційного протиборства з використанням атакуючої інформаційної зброї. І тому все частіше останнім часом розглядаються не апаратно-програмні засоби дії на інформаційні системи і інформаційний ресурс противника, а засоби і методи маніпулювання інформацією. Це підтверджує аналіз робіт з даної тематики – в зарубіжній пресі останніми роками різко зросло число робіт по засобах і методах маніпулювання свідомістю (зокрема, по методах нейролінгвістичного програмування, гіпнозу та іншим методам дії), дослідженнях психології особи та ін. З'явилися ряд нових понять, наприклад – "реальна віртуальність", коли освітлення деякої події в пресі набуває більшої важливості, ніж ця подія [15].

Таким чином, інформаційне протиборство є сукупністю таких взаємин, в рамках яких одні суб'єкти шляхом активної дії на інформаційну сферу інших суб'єктів прагнуть отримати перевагу над іншою стороною на користь досягнення своїх політичних цілей.

Інформаційне протиборство є невід'ємною складовою політичних стосунків і основним інструментом політичного примусу і досягнення політичних цілей.

Не секрет, що Україна є одним з об'єктів сфери інформаційного протиборства. Серйозна дія на громадську думку в цілому і на конкретну особу окремо надають факти розсекречення важливих державних документів, різного роду підслухуючих пристроїв, передачі надсекретних архівних матеріалів в інші країни через популістські кон'юнктурні міркування. В результаті у українських громадян та і в державних структурах в цілому став складатися синдром інформаційної беззахисності.

Останніми роками ситуація значно змінилася. Проте, Україна залишається об'єктом дії західних країн в їх прагненні до світового лідерства. Нейтралізувати дію інформаційних погроз покликана єдина державна система інформаційної безпеки України.

Державна система інформаційної безпеки – це організаційне об'єднання державних органів, сил і засобів інформаційної безпеки, що здійснюють свої функції на основі закону і під контролем і захистом судової влади. У завдання цієї системи входить: виявлення і прогнозування появи дестабілізуючих чинників і інформаційних погроз життєво важливим інтересам особи, суспільства і держави; здійснення комплексу довготривалих і оперативних заходів по їх попередженню і усуненню; створення і підтримка сил і засобів забезпечення інформаційної безпеки [16].

Об'єктивно зростаюча глобальність інформаційної сфери наводить до того, що створювана інформаційно-комунікаційна інфраструктура країни і національні інформаційні ресурси виявляються об'єктами, вельмиуразливими щодо дій з боку геополітичних конкурентів, терористичних організацій, кримінальних груп і окремих зловмисників. З урахуванням цих чинників інформаційний розвиток України, який помітно відстає від провідних промислово-розвинених країн, повинен здійснюватися в рамках системної і збалансованої державної інформаційної політики, спрямованої на активну протидію інформаційній агресії. У зв'язку з цим уявляється необхідним розробити і ухвалити Закон Україні про інформаційну безпеку, відповідний Доктринам національної та інформаційної безпеки Україні.

Як випливає з Доктрини інформаційної безпеки України, діяльність органів виконавчої влади в сфері забезпечення інформаційної безпеки Україні має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за наступними головними напрямами: інформаційно-психологічному (зокрема щодо забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей); технологічного розвитку (зокрема щодо розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, обробки та поширення інформації; захисту інформації, зокрема щодо забезпечення конфіденційності, цілісності та доступності інформації, у тому числі технічного захисту інформації у національних інформаційних ресурсах від кібернетичних атак) [17].

Все вище зазначене дозволяє зробити висновок, що в забезпеченні інформаційної безпеки зацікавлена не лише держава, але і суспільство в цілому.

Сьогодні завданням першорядного значення слід вважати створення надійної системи інформаційної безпеки, яка повинна забезпечити захист як країни в цілому, так і кожного її громадянина від небажаних інформаційних дій. Зокрема, ця система повинна захистити населення країни від інформаційних дій, що зашкоджують об'єктивному сприйняттю дійсності, а також забезпечити захист вищого керівництва країни від недостовірної інформації, що затрудняє або робить неможливим ухвалення політичних або соціально-економічних рішень, адекватних реальній обстановці.

Головною інформаційною загрозою для держави є порушення режиму державної таємниці. В Україні інформація з обмеженим доступом поділяється на два різновиди – таємну і конфіденційну. Відповідно до Закону Україні "Про інформацію" до таємної інформації відносять такі відомості, розголошення яких завдає шкоди особі, суспільству і державі, та яка включає до свого складу державну або іншу визначену законом таємницю [18].

На цих підставах М. Галамба робить висновок, що захист інформації, віднесеної до конфіденційної і перш за все до державної таємниці, слід вважати невід'ємною складовою національної безпеки Україні. Іншими словами, можна стверджувати, що інформаційна безпека визначається як захищеність важливих інтересів особи, суспільства та держави в інформаційній сфері, за якою забезпечується використання інформації у інтересах її суб'єктів, сталий розвиток держави, виявлення, попередження і ліквідація загроз національним інтересам [19].

До тяжких наслідків веде також порушення безпеки інформаційних систем або телекомунікації, внаслідок чого відбувається "втеча" інформації.

Отже, можна зробити висновок, що в цілях інформаційної безпеки держави необхідне створення державної системи інформаційного протиборства, основним завданням якої має бути погоджена і цілеспрямована діяльність органів держави по протидії негативному інформаційному впливу.

Слід пам'ятати, що інформаційна безпека України знаходиться під постійною загрозою. А це означає необхідність розвитку ефективної системи техніко-технологічного захисту, який дозволить державі виробити адекватну відповідь на можливі погрози і виклики.

Література:

1. Рішення всеукраїнської науково-практичної конференції "Стан та вдосконалення безпеки інформаційно-телекомунікаційних систем (Коблево, 15-17 вересня 2009 р. [Електронний ресурс]. – Режим доступу: http://www.afa.biz.ua/news).
2. Варфоломеев М. Проблема национальной безопасности в современном политическом процессе / М. Варфоломеев // Власть. – 2008. – № 4. – С. 38.
3. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. … док. юрид. наук: Спеціальність 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / Б. А. Кормич. – Харків, 2004. – С. 14.
4. Постанова Верховної Ради України "Про Концепцію (основи державної політики) національної безпеки України" від 16 січня 1997 р. № 3/97 ВР // Голос України. – 1997. – 4 лютого. – С. 5.
5. Галамба М. Інформаційна безпека України: поняття, сутність та загрози / М. Галамба [Електронний ресурс]. – Режим доступу: http://www.nbu.gov.ua/infan/arxiv/arxiv0/2007/01/28).
6. Кормич Б. А. Указ. праця. – С. 15.
7. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки: автореф. дис. … канд. юрид. наук: спец. 12.00.01 – теорія та історія держави і права, історія політичних і правових учень / Ю. Є. Максименко. – Київ, 2007. – С. 9.
8. Горбулін В. Національна безпека України: загрози і виклики / В. Горбулін // Безпека та нерозповсюдження. – Вип. 3 (15). – К., 2006. – С. 54.
9. Галамба М. Указ. праця.
10. Ноговицын А. В центре внимания – информационная безопасность / А. В. Ноговицын [Електронний ресурс]. – Режим доступу: http://www.redstar.ru/2009/02/27_02/1_06.html.
11. Политические коммуникации / ред. А. И. Соловьев. – М.: Аспект Пресс, 2004. – С. 228.
12. Гриняев С. Россия в глобальном информационном обществе: угрозы, риски и возможные пути их нейтрализации / С. Гриняев [Електронний ресурс]. – Режим доступу: http://www.fondiv.ru/articles/3/335/.
13. Кормич Б. А. Указ. праця. – С. 15.
14. Пирумов В. С. Информационное противоборство. Четвертое измерение противостояния / В. С. Пирумов. – М.: Издательский дом "Оружие и технологии", 2003. – С. 544.
15. Гриняев С. Указ. праця.
16. Брандман Э. Информационная безопасность Российского общества в современных условиях / Э. Брандман // Власть. – 2007. – № 5. – С. 70-71.

17. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html.
18. Закон України "Про інформацію", прийнятий Верховною Радою України 2 жовтня 1992 року // Відомості Верховної Ради України. – 1992. – № 48, Із змінами від 06.04.2000, Відомості Верховної Ради. – 2000. – № 20.
19. Галамба М. Указ. праця.

Карагіоз Р. С., ПНПУ ім. К. Д. Ушинського

СУЧАСНІ ЗАСОБИ ДОСЯГНЕННЯ ПОЛІТИЧНОЇ ЗГОДИ

В статье рассматриваются современные механизмы и способы достижения политического согласия. Анализируются теоретические подходы к выработке данных способов и механизмов, проводится их классификация и выделяются основные принципы.

Modern mechanisms and ways of achievement of political consent are considered in article. Theoretical approaches to production such methods and mechanisms are analysed, their categorization and stand out basic principles are conducted.

Історія людства виробила безліч засобів, методів і принципів, що сприяють досягненню миру, формуванню політичної згоди серед таких груп. Так, Крисюн Н. А., поділяє механізми досягнення політичної згоди на дві групи: процесуальні та інституціональні [4, с. 112]. До процесуальних механізмів науковці відносять практику й принципи взаємодій між політичними лідерами, інститутами та об'єднаннями різних рівні. Це переговори, договори та угоди (пакти), "круглі столи", консенсуси, компроміси, толерантність, партнерство, співробітництво, довіра, примирення, погоджувальні комісії [2, с. 344]. Процесуальні механізми вторинні стосовно інституціональних [4, с. 113].

Інституціональні механізми політичної згоди – це набір специфічних способів і засобів впливу різноманітних інститутів на процес формування політичної згоди. На практиці процесуальні механізми досягнення політичної згоди часто використовують у сполученні один з одним, тому що вони внутрішньо взаємозалежні і випливають один з одного. До механізмів досягнення політичної згоди можна віднести різноманітні методи вирішення та врегулювання спорів та конфліктів, заснованих на мирних засобах. Загальновизнана класифікація засобів мирного врегулювання міжнародних суперечок міститься в статті 33 Уставу ООН, відповідно до якої держави зобов'язані вирішувати свої