УДК 323(71):316.77-049.5

І.І. Макух-Федоркова

ФОРМУВАННЯ СТРАТЕГІЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ЗБРОЙНИХ СИЛ КАНАДИ

У статті досліджується національна безпека Канади та характеризується комплекс заходів військово-політичного керівництва країни щодо розвитку канадської стратегії інформаційних операцій.

Проаналізовані директиви, які вплинули на модернізацію збройних сил країни та активна участь у миротворчих і контртерористичних операцій в кризових регіонах світу. Показано, що стратегія кібербезпеки Канади дозволяє захистити цілісність урядових систем і національних критичних активів, ефективно боротися з кіберзлочинами та захищати канадців при щоденному використанні ними кіберпростору. Автор прийшла до висновку, що модернізація канадської економіки та технологічні інновації серйозним чином вплинули на створення стандартів в сфері системи національної безпеки Канади.

Ключові слова:*кібербезпека, інформаційні операції, національна безпека, інформаційні технології, комп'ютерні системи, канадська інформаційна інфраструктура.*

Той, хто здобув сто перемог у ста поєдинках, – не герой; геройство – підкорити військо противника без боротьби. (Сунь-Дзи «Мистецтво війни»[4, с. 100]).

На сучасному етапі потоки інформації виходять за рамки національного суверенітету та інтегруються у світовий інформаційний простір, поряд із стрімким зростанням об'ємів інформації людство зіткнулося ще й із збільшенням могутності технічних засобів їх обробки та передачі. Саме динамічний розвиток інформаційних технологій та підвищена ефективність всієї інформаційної інфраструктури сучасного глобалізованого суспільства створили цілий комплекс проблем у світовій політиці, перш за все у сфері міжнародної та національної безпеки. Удосконалення комп'ютерних мереж, супутникового зв'язку, а також інтенсивний розвиток нових ІТ- технологій серйозним чином впливає на відносини як між країнами на світовому рівні, так і між іншими членами інформаційного суспільства. За останні 20 років в результаті широкого застосування новітніх інформаційних технологій у світі склалася нова розстановка сил, яка суттєвим чином змінила не тільки характер загроз, але й засоби збройної боротьби, форми і способи їхнього протистояння. В цих умовах проблема інформаційної безпеки в сучасному світі стає однією з самих актуальних, особливо важливою урядовою реалізацією є створення стратегії безпеки кіберсистем Канади. Кібербезпека Канади є лише одним із елементів тих ініціатив, які направлені на захист національних інтересів. Канадський уряд вносить зміни у законодавство, модернізує повноваження правоохоронних органів і забезпечує порядок, при якому технологічні інновації не можуть застосовуватися якщо вони ухиляються від законодавчого контролю. Актуальність даної проблеми не викликає жодних сумнівів, адже останніми роками Україна живе в стані гібридної війни з Російською Федерацією, а реалізація стратегії захисту кіберпростору є одним з надважливих національних питань.

Стратегія національної безпеки та комплекс інформаційних операцій збройних сил Канади стали предметом дослідження в основному зарубіжних дослідників [11; 12; 14; 10],

проте зустрічаються також наукові розвідки і серед російських науковців [1; 3; 9]. В даній статті поставлено за мету висвітлити стратегію національної безпеки Канади та охарактеризувати комплекс заходів військово-політичного керівництва країни щодо розвитку канадської стратегії інформаційних операцій.

Важливо зазначити, що канадська економіка в значній мірі опирається на Інтернет, адже об'єм продажу через мережу складає близько 63 млрд. дол., а 87 % канадських підприємств використовують Інтернет для забезпечення комерційної діяльності. Уряд Канади на сьогоднішній день пропонує громадянам більше 130 послуг в електронному вигляді, в тому числі заповнення податкових декларацій, кредитних заявок. Відповідно успіх Канади у захисті кіберпростору є гордістю країни і вважається величезним національним досягненням, адже спрямований на захист національних інтересів. Варто нагадати, що в 1993 році спеціалістами Центру безпеки, що входили в структуру відомства Канади були розроблені «Канадські критерії безпеки комп'ютерних систем», які на сьогоднішній день взяті за основу в багатьох інших країнах. Ще в 1990 році під егідою Міжнародної організації по стандартизації було розпочато роботу по створенню стандарту в сфері оцінки безпеки інформаційних технологій. Розробка цього стандарту мала наступні цілі: уніфікація національних стандартів в сфері оцінки безпеки ІТ; підвищення рівня довіри до оцінки безпеки ІТ; скорочення витрат на оцінку безпеки ІТ на основі взаємного визнання сертифікатів. В червні 1993 року організації по стандартизації і забезпеченню безпеки США, Канади, Великобританії, Франції, Німеччини та Нідерландів об'єднали свої зусилля в рамках проекту по створенню єдиної системи критеріїв оцінки безпеки ІТ. Цей проект отримав назву «Спільні критерії» [2, с. 47]. Стратегія кібербезпеки Канади дозволяє захистити цілісність урядових систем і національних критичних активів, ефективно боротися з кіберзлочинами та захищати канадців при щоденному використанні ними кіберпростору.

Для забезпечення національної безпеки та захисту інтересів держави за кордоном військово-політичне керівництво Канади приділяє значну увагу розвитку сил спеціальних операцій (ССО). Збройні сили Канади (CanadianForces – CF) незважаючи на свою відносно незначну чисельність є одними з найближчих союзників Збройних сил США, адже поділяють концепцію свого сусіда щодо максимального розширення інформаційного простору для військових наступальних, оборонних та пропагандистських дій. Прийняття Міністерством оборони США у 2006 р. Директиви стратегічних інформаційних операцій В 3600.1 серйозним чином вплинуло на модернізацію ЗС Канади. Адже у цьому документі вперше чітко визначалися основні завдання і функції інформаційних операцій, комплексне застосування засобів радіоелектронної боротьби, операції в інформаційно-комунікаційних мережах, психологічні операції, військова дезінформація та оперативна безпека [8]. В документі зазначалося, що інформаційні операції проводяться «з метою інформаційного впливу, введення в оману, порушення роботи комп'ютерних систем, викривлення інформації, дезорганізація баз даних та позбавлення противника можливості їх використовувати, вилучення інформації із комп'ютерних систем і баз даних ворога при одночасному забезпеченні захисту своєї інформації та інформаційної інфраструктури» [8]. Варто зазначити, що ще в квітні 1999 р. на 50-ій сесії НАТО у Вашингтоні було оголошено про нові оборонні можливості з використанням передових технологій як складової частини розвитку сил Північноатлантичного союзу. В 2007 році актуалізувалася національна концепція інформаційних операцій Армії Канади (InfoOps), яка знайшла своє відображення в Стратегії формування канадських Збройних сил до 2020 року [12].

Поштовхом до розробки власної доктрини InfoOps для ЗС Канади було бажання національних військових контингентів стати активними учасниками миротворчих і контртерористичних операцій в кризових регіонах світу, що проводилися в багатонаціональному форматі під егідою НАТО і Євросоюзу. Саме нова стратегічна концепція оборони і безпеки членів Північноатлантичного договору була сформульована в декларації Ліссабонського саміту і зафіксована в пресс-релізі PR/CP 0155 (2010) [10]. В цьому документі зазначалося про сучасні підходи НАТО спрямовані на «підвищення рівня ефективності в нових світових умовах, проти нових загроз з новими можливостями і новими партнерами». Про серйозність підходів країн-членів НАТО до розробки концепції інформаційних операцій свідчить створення багатонаціонального форуму для спеціалістів в сфері стратегічних комунікацій та інформаційних війн під назвою TheMultinationalInformationOperationsExperiment (MNIOE) [13]. Основна його мета полягала у виробленні спільних підходів щодо концептуального розуміння поняття інформаційні операції. В ході цієї місії була задекларована структура розвитку концепції InfoOps. Канада увійшла до складу міжнародної робочої групи MNIOE поряд з Австралією, Францією, Німеччиною, Великобританією і США. Діяльність групи координується збройними силами Німеччини, а також постійними представниками є Австрія, Португалія, Фінляндія, Нова Зеландія і Швеція. Ініціатива створення MNIOE є спробою поглибленого вивчення принципів, процедур, інструментів і методів проведення InfoOps, які можуть бути застосовані в умовах багатонаціональних операцій. Основним документом InfoOps в інформаційних операціях коаліції є Біла книга. Серед основних стратегічних цілей інформаційного PR – супроводження військово-політичних дій країн-членів НАТО в миротворчих і антитерористичних операціях є: формування позитивного іміджу збройних сил НАТО в очах національної та світової громадськості та нейтралізація інформаційно-психологічними засобами країн, що займають негативну позицію по відношенню до дій НАТО в зонах військового конфлікту. До цілей оперативно-тактичного рівня відносять: дискредитацію урядів і політичних груп ворогуючої сторони в очах власного народу і світової громадської думки, деморалізацію особистого складу збройних сил противника, спонукання військовослужбовців до дезертирства та дій непідкорення, протидію поширенню чуток і дезінформації. Задля формування конкретних параметрів політики і діяльності ЗС Канади в цьому напрямку спеціалісти НАТО склали відповідний документ в англійській та французькій версії під назвою «Ієрархія документів Збройних сил Канади в сфері інформаційних операцій». Ціла низка документів присвячена проблемам психологічних операцій (код сертифікованого документа B-GJ-005-313/FP-010 [13]), військово-громадянського співробітництва (CIMIC) в умовах миру, надзвичайних ситуацій, а також взаємодії зі службою зв’язків з громадськістю (код документів B-GJ-005-361/FP-000 [5]).

На сьогоднішній день в країнах НАТО існує ціла низка спеціальних підрозділів, які з певною метою здійснюють прямий психологічний вплив на світову громадську думку. Для практичної реалізації завдань інформаційно-пропагандистського характеру і військово-політичних акцій канадського уряду, в структурі Збройних сил Канади було сформовано спеціальний підрозділ, який набув поширення в західних військових колах як Група інформаційних операцій (CanadianForcerInformationOperationsGroup, CFIOG) [6]. Він є основним підрозділом психологічної війни збройних сил Канади зі штаб квартирою в м. Літрим (Онтаріо). Група складається із: штабу, центру засобів електронної боротьби, центру мережних операцій, центру радіоелектронної розвідки, військо-технічної станції.

Основна місія CFIOG полягає в розробці, координації та здійсненні інформаційних операцій для забезпечення сприятливих можливостей діяльності Міністерства національної оборони і канадських Збройних сил. Саме цей підрозділ діє в тісній взаємодії з такими службами і підрозділами, як Центр засобів електронної боротьби (CanadianForcesElectronicWarfareCentre – CFEWC), Центр радіоелектронної розвідки (CanadianForcesSignalsIntelligenceOperationCentre – CFSOC), Об'єднаний інформаційно-розвідувальний координаційний центр (JIIFC). Усі перелічені вище структури реалізовуються безпосередньо на станції CFS в Літримі, яка зі штатом майже 500 військовослужбовців і 29 осіб громадянського персоналу забезпечує усю необхідну їм технічну і логістичну підтримку. Девізом станції стали слова racermpetere, що означає «дослідження світу». При цьому найстаріша канадська станція збору даних радіотехнічної інформації CFSLeitrim входить в глобальну систему «Ешелон» і використовується для пошуку вогнищ тероризму, контролю наркотрафіка, а також для політичної і дипломатичної розвідки.

Варто зазначити, що за останні десятиліття ефективність участі Групи інформаційних операцій ЗС Канади в складі коаліційних сил в миротворчих акціях справляє неоднозначне ставлення. З одного боку, очевидним є той факт, що Канада не в повній мірі включилась в битву на інформаційних фронтах, але з іншого боку – її військовослужбовці активно адаптуються до умов і збільшують власний потенціал можливостей. У той же час канадська держава докладає багато зусиль не тільки до розвитку стратегій спеціальних інформаційних операцій, але й до удосконалення системи інформаційної безпеки країни.

Одним з основних завдань в сфері інформаційної безпеки є розробка критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки. Тому ще в 1993 році спеціалістами Центру безпеки, що входили в структуру відомства Канади були розроблені «Канадські критерії безпеки комп'ютерних систем», які на сьогоднішній день взяті за основу в багатьох інших країнах [1].В даному контексті варто нагадати, що в 1990 році під егідою Міжнародної організації по стандартизації було розпочато роботу по створенню стандарту в сфері оцінки безпеки інформаційних технологій. Розробка цього стандарту мала наступні цілі: уніфікація національних стандартів в сфері оцінки безпеки IT; підвищення рівня довіри до оцінки безпеки IT; скорочення витрат на оцінку безпеки IT на основі взаємного визнання сертифікатів. В червні 1993 року організації по стандартизації і забезпеченню безпеки США, Канади, Великобританії, Франції, Німеччини та Нідерландів об'єднали свої зусилля в рамках проекту по створенню єдиної системи критеріїв оцінки безпеки IT. Цей проект отримав назву «Спільні критерії» [3].

Варто наголосити, що канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria) були розроблені в 1993 р. спеціалістами із Центру безпеки відомства безпеки зв'язку Канади (Canadian System Security Centre Communication Security Establishment). В цьому розробленому документі відчувається сильний вплив «Оранжевої книги» і Федеральних критеріїв безпеки. Доречно нагадати, що критерії безпеки комп'ютерних систем (TCSEK Trusted Computer System Evaluation Criteria) вперше були сформульовані розробниками Міністерства оборони США в документі, що отримав назву «Оранжева книга» (1983) (по кольору видання) [7]. Концепції і функціональні вимоги, що були сформульовані в цьому документі, стали основним орієнтиром для розробки в майбутньому стандартів безпеки. В «Оранжевій книзі» було запропоновано три критерії безпеки, а саме: політика безпеки, аудит і коректність та безперервність захисту. Це була перша спроба створення єдиного для розробників,

споживачів і спеціалістів по сертифікації стандарту безпеки. Однак специфіка розробки документа була розрахована переважно на комп'ютерні системи військового призначення (при цьому в основному на операційні системи), тому в 1992 році спеціалісти Національного інституту стандартів і технологій США і Агентство національної безпеки США врахували усі недоліки Оранжевої книги та розробили Федеральні критерії безпеки інформаційних технологій, що на сьогодні є однією із важливих складових Американського федерального стандарту по обробці інформації.

Інформаційна система Канади постійно тестується на стан безпеки та проводиться контроль по захисту інформації від зовнішнього впливу. З метою посилення ефективності діяльності підрозділів Міністерства оборони проводиться робота з групою інформаційних операцій Канадських збройних сил. Свідченням успішного розвитку канадської інформаційної інфраструктури було створення в 2005 році Центру по кібер-інцидентам (CCIRC). Даний центр має мандат для боротьби із загрозами і нападами на критичну інфраструктуру цілодобово сім днів на тиждень. Важливим рішенням було прийняття в 2010 році канадської стратегії кібербезпеки, яка включає в себе такі аспекти: захист урядових систем; забезпечення безпеки канадських громадян в онлайн середовищі; контроль кібернетичної системи країни за межами федерального уряду [1]. Стратегія кібербезпеки Канади повинна закріпити інформаційні системи країни, особливо в критично важливих секторах інфраструктури, забезпечити підтримку економічного зростання та захисту канадців [9]. Слід зазначити, що вказана стратегія побудована на трьох основних принципах: забезпечити довіру канадців до державних інформаційних систем при роботі уряду з їх особистою і корпоративною інформацією, а також при наданні електронних послуг громадянам. Уряд намагається захистити канадський суверенітет і забезпечити кіберзахист національної безпеки та економічні інтереси; співробітництво з провінціями і територіями, а також приватним сектором. Уряд Канади надає підтримку кіберініціативам та всіляко підтримує важливі сектори інфраструктури, а канадські дослідники працюють над прогнозуванням та оперативною ліквідацією кіберзагроз, вносять пропозиції раціонального використання кіберпростору в національних інтересах Канади; канадський уряд підтримує міжнародні зусилля по розробці і реалізації глобального режиму управління кібербезпекою, адже Канада бере участь у створенні потенціалу кібербезпеки в менш розвинених країнах спільно із зарубіжними партнерами, і в такий спосіб долучається до посилення глобальної системи кіберзахисту. Стратегія кібербезпеки Канади дозволяє захистити цілісність урядових систем і національних критичних активів, ефективно боротися з кіберзлочинами і захищати канадців при щоденному використанні ними кіберпростору.

Підсумовуючи варто наголосити, що останніми роками в Канаді створюються усі передумови для переходу до якісно нової моделі розвитку, яка базується на освіті, інноваціях та надійній політиці в сфері безпеки. Ці зміни обумовлені необхідністю пріоритетного розвитку наукоємких галузей виробництва країни, а також завдяки постійному удосконаленню інформаційної політики, яка включає в себе єдиний інформаційний простір, систему електронного урядування, вільний доступ до інформації, державне регулювання ЗМІ, розвиток Інтернету, нормативне регулювання всіх інформаційних відносин і процесів, переведення більшості державних послуг в електронний варіант. Якість інформаційної безпеки Канади визнана усім міжнародним співтовариством і відзначається, що канадські критерії безпеки комп'ютерних систем є надійними і досконалими національними стандартами інформаційної безпеки. Варто

відзначити, що важливу роль в цьому процесі відіграла активність канадського уряду в напрямку фінансування інноваційній діяльності країни, адже за останні роки створена комплексна система фондів інноваційного розвитку, таких як Канадський фонд інновацій, Фонд нових ініціатив, Фонд передових технологій, Фонд лідерських можливостей та ін. І найголовнішим є те, що приймаючи програму створення інноваційного суспільства канадський уряд, виходив з того, що в інноваційний процес мають бути залучені усі прошарки канадського суспільства, які в тісному взаємозв'язку і при фінансовій підтримці держави можуть забезпечити входження Канади в п'ятірку найбільш розвинутих в науково-технічному плані країн.

Список використаних літератури

1. Гунина А. А. Политика Канады в сфере обеспечения информационной безопасности [Электронный ресурс] / А. А. Гунина // Студенческий научный форум - 2014 : VI Междунар. студ. науч. конф. – Режим доступа : http://www.scienceforum.ru/2014/676/5473 ; Gunina A. A. Politika Kanady v sfere obespecheniya informatsionnoy bezopasnosti [Elektronnyy resurs] / A.A. Gunina // Studencheskiy nauchnyy forum - 2014 : VI Mezhdunar. stud. nauch. konf. – Rezhim dostupa : http://www.scienceforum.ru/2014/676/5473

2. Макух-Федоркова І. І. Критерії канадської системи інформаційної безпеки / І.І. Макух-Федоркова // «UChoice: 4P» Ukrainian Choice: Public Policy, Politics, Psychology : матер. ІІ міждисциплін. наук.-практ. конф., м. Одеса, 8 жовтня 2016 р. – Одеса : Національний університет «Одеська юридична академія», 2016. – С. 46-49 ; Makukh-Fedorkova I. I. Kryterii kanadskoi systemy informatsiinoi bezpeky / I. I. Makukh-Fedorkova // «UChoice: 4P» Ukrainian Choice: Public Policy, Politics, Psychology : mater. II mizhdystsyplin. nauk.-prakt. konf., m. Odesa, 8 zhovtnia 2016 r. – Odesa : Natsionalnyi universytet «Odeska yurydychna akademiia», 2016. – S. 46-49.

3. Никифорова Н. М. Аналитический обзор критериев информационной безопасности ведущих зарубежных стран (США, Канада, Европейский союз) [Электронный ресурс] / Н.М. Никифорова // Безопасность информационных технологий. — 2013. — № 1. С. 66-70 – Режим доступа: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf ; Nikiforova N.M. Analiticheskiy obzor kriteriev informatsionnoy bezopasnosti vedushchikh zarubezhnykh stran (SShA, Kanada, Yevropeyskiy soyuz) [Elektronnyy resurs] / N. M. Nikiforova // Bezopasnost informatsionnykh tekhnologiy. — 2013. — № 1. S. 66-70 – Rezhim dostupa: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf

4. Сунь-дзи Мистецтво війни / Сунь-дзи. – Львів : Видавництво Старого Лева, 2017. – 105 с. ; Sun-dzy Mystetstvo viiny / Sun-dzy. – Lviv : Vydavnytstvo Staroho Leva, 2017. – 105 s.

5. Apostoliuk H. A. B. Communication unification: the need for Canadian armed forces institutional communications [Electronic resource] / H. A. B. Apostoliuk. – Mode of access : https://www.cfc.forces.gc.ca/259/290/299/286/apostoliuk.pdf

6. Canadian Forcer Information Operations Group, CFIOG [Electronic resource]. – Mode of access : https://canadianforces.wordpress.com/cfiog/

7. Department of defense trusted computer system evaluation criteria / December. 1985. [Electronic resource] – Mode of access : http://csrc.nist.gov/publications/history/dod85.pdf

8. Information Operations. DoD Directive 3600.01,Washington. 14.08.2006.

9. Joint United States-Canada Electric Grid Security and Resilience Strategy [Electronic resource] / Product of the Governments of the United States and Canada. – 2016. - Mode of access :

https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf

10. Lisbon summit declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon on 20 November 2010. Press release 20 November 2010 PR/CP(2010)0155 [Electronic resource] – Mode of access : https://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf

11. Psychological operations [Electronic resource] : Joint Doctrine Manual / MDN Canada. – Mode of access : https://www.psywar.org/psywar/reproductions/CF_Psychological_Operations_Joint_Doctrine.pdf

12. Rudner M. Intelligence and information superiority in the future of Canadian defense policy [Electronic resource] / M. Rudner. - Ottawa, Ontario, 2001. –Mode of access : https://www3.carleton.ca/csds/docs/occasional_papers/npsia-24.PDF

13. The Multinational Information Operations Experiment (MNIOE) within the Multinational Experiment (MNE) – Integration of a Multinational CD&E Project [Electronic resource] – Mode of access : https://www.act.nato.int/images/stories/events/2011/cde/rr_mnioe.pdf

Стаття надійшла до редакції 03.03.2019 р.

I.I. Makuch-Fedorkova

FORMATION OF THE NATIONAL SECURITY STRATEGY AND CANADIAN ARMED FORCES INFORMATION OPERATIONS

The article examines Canadian national security and describes a set of measures for military-political leadership in the country to develop the Canadian strategy of information operations. It should be recalled that in 1993, the specialists of the Center for Security, which were part of the Canadian office structure, developed "Canadian Computer Security Criteria", which today are based on many other countries. Back in 1990, under the auspices of the International Organization for Standardization, work was begun to establish a standard for the assessment of information technology security. The directives that influenced the modernization of the country's armed forces and active participation in peacekeeping and counterterrorist operations in the crisis regions of the world were analyzed.

The impetus for the development of its own InfoOps doctrine for the Canadian Armed Forces was the desire of national military contingents to become active participants in peacekeeping and counterterrorist operations in crisis regions of the world, held in a multinational format under the auspices of NATO and the European Union. Canada's information system is constantly tested for safety and controls are in place to protect information from external influences. In order to increase the effectiveness of the activities of the Ministry of Defense, the Canadian Armed Forces has been working with the information operations group. It is shown that Canada's cybersecurity strategy can protect the integrity of government systems and national critical assets, effectively fight cybercrime, and protect Canadians with their daily use of cyberspace. Evidence of the successful development of Canadian information infrastructure was the creation in 2005 of the Center for Cybercrime (CCIRC). The center has a mandate to deal with threats and attacks on critical infrastructure, and the Canadian government not only supports cyber-initiatives and strongly supports important infrastructure sectors, but also supports international efforts to develop and implement a global cyber security regime. After all, Canada is involved in building cyber security capabilities in less developed countries, in conjunction with foreign partners, and thus contributes to strengthening the global cyber defense

system. The author came to the conclusion that the modernization of the Canadian economy and technological innovation have seriously influenced the creation of standards in the field of national security of Canada. The quality of Canada's information security is recognized by the international community as a whole, and it is noted that Canadian security criteria for computer systems are robust and exemplary with national information security standards.

Key words: *cybersecurity, information operations, national security, information technologies, computer systems, Canadian information infrastructure.*

УДК 32:316.344.8(477)

О.В. Мендрін

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ПОЛІТИКИ ІДЕНТИЧНОСТІ В УКРАЇНІ

У статті проаналізовані запропоновані в українській політичній теорії моделі та підходи до визначення функцій, завдань, способів реалізації політики ідентичності. Робиться спроба порівняльної характеристики запропонованих як академічними інститутами та аналітичними центрами, так і окремими дослідниками концепцій імплементації такої політики, визначення її місця у системі функцій держави та інститутів громадянського суспільства.

Ключові слова: *макрополітична ідентичність, політика ідентичності, загальнонаціональна ідентичність, символічна політика, конструювання ідентичності, держава.*

Трансформаційні процеси в Україні, значною мірою обумовлені глобальними політичними змінами 90-х рр. XX ст., поряд із незавершеністю транзиту, суперечливістю і непослідовністю проведення реформ у соціальній та політичній сферах, також характеризувались й культурними, світоглядними, ціннісними зрушеннями. Водночас, складність посталих перед пануючими елітами, державою і суспільством завдань з опрацювання, переживання постімперського і, одночасно, постколоніального досвіду, відсутність суспільного консенсусу щодо сценарію майбутнього розвитку продовжують визначати рівень еволюції політичних процесів та інститутів в країні, стан демократії, вимагаючи прийняття системних рішень, що дозволили б сформувати і забезпечити перспективу розвитку України як держави.

Однією з істотних складових зазначеної трансформації стала зміна соціальної, політичної ідентичності громадян як всього пострадянського простору в цілому, так і України зокрема. Постала «криза ідентичності» вимагала певних дій задля свого подолання, «створення нової конструкції ідентичності, колективного «ми» знову створених пострадянських політій, скріпленого загальними символами і міфологемами, вписаними в проект колективного майбутнього», вироблення «символічних моделей інтерпретації та легітимації процесів, що відбуваються» [1, с.199]. Однак, «проблема громадянської ідентичності з часу проголошення незалежності перебувала поза сферою інтересів та пріоритетів держави» [2, с. 16], а самі спроби сформувати якусь нову, спільну для громадян України ідентичність «характеризувались суперечливістю, кон'юнктурністю,