Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2020. – Т. 41. – С. 29-45
DOI: 10.31861/mhpi2020.41.29-45

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2020. – Volume. 41. – pp. 29-45
DOI: 10.31861/mhpi2020.41.29-45

УДК 351.746:007](71)

© Іванна Макух-Федоркова [1]

Сучасні інформаційні виклики та формування кібернетичної стратегії Канади

У статті досліджується питання кібербезпеки Канади, характеризується комплекс заходів нормативно-правового, військово-політичного характеру щодо формування канадської стратегії інформаційної політики та механізмів захисту системи національної безпеки країни.

Характеризуються програмні документи, спрямовані на удосконалення кібербезпеки Канади та опрацьовані директиви, які вплинули на модернізацію збройних сил країни, активну 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 інформаційного простору. Наголошується на міжнародній співпраці Канади в плані захисту національного простору країни, консолідація зусиль з блоком НАТО і його членами у стримуванні Росії. Проаналізована медична місія канадських лікарів у допомозі українськими військовослужбовцям, а також розкривається значення канадської допомоги у боротьбі з кремлівською пропагандою в галузі кібербезпеки. Автор прийшла до висновку, що модернізація канадської економіки, державна фінансова підтримка, технологічні інновації, належна нормативно-правова база та партнерські зв'язки між усіма рівнями влади серйозним чином вплинули на створення стандартів в сфері системи національної безпеки Канади. В цьому важливу роль відіграє політика формування захисту кіберсередовища, що спрямована на покращення інтересів канадців і національної економіки.

Ключові слова: кібербезпека, інформаційна безпека, канадські національні інтереси, інформаційна стратегія, національна безпека, комп'ютерні системи, критична інфраструктура.

Contemporary Information Challenges and the Formation of Canada's Cybernetic Strategy

The article examines the issue of Canada's cybersecurity and also characterizes a set of normative acts, that have a military and political pattern regarding the formation of Canada's strategy for informational policy and the National Security protection mechanism.

The article contains program documents that are presented in order to improve Canada's cybersecurity and elaborate directives that influenced the country's armed forces modernization, active participation in peacekeeping and counterterrorism operations in crisis regions around the world. It is shown that Canada's cybersecurity strategy allows protecting the integrity of government systems and national critical assets, effectively fighting against cybercrime and protect Canada's citizens with their daily usage of informational space. It emphasized Canada's international cooperation in protecting the country's national space, consolidating efforts with NATO block and its members in order to restrain Russia. The medical mission of Canadian doctors that assisted Ukrainian servicemen was also analyzed, as well as the importance of Canadian assistance in combating "Kreml" propaganda in the cybersecurity field. The author concluded that the modernization of Canada's economy, governmental support, technological innovation, proper regulatory framework and partnerships between all levels of government had a serious impact on the creation of Canada's national security system standards. Cybersecurity policies, which are aimed at improving the interests of Canadians and the national economy, play an important role in this process.

[1] Кандидат політичних наук, доцент кафедри міжнародної інформації Чернівецького національного університету імені Юрія Федьковича, Україна. E-mail: ivanna.makuch7@gmail.com: https://orcid.org/0000-0003-2198-8727.

Keywords: cybersecurity, information security, Canadian national interests, information strategy, national strategy, computer systems, critical infrastructures.

Постановка проблеми. На сучасному етапі динамічне формування глобального інформаційного простору пов'язано, з одного боку, з наданням людству небачених раніше інформаційних можливостей, а з іншого – з виникненням нових загроз. Адже виник новий феномен – «кібербезпека», з якою пов'язані такі поняття, як «кіберзлочинність», «кібертероризм», «кібервійни». Практично усі розвинені країни світу та провідні міжнародні організації працюють над організацією безпечного функціонування національних інформаційних інфраструктур та формуванням відповідних концепцій кібербезпеки. 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 удосконалення 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. Вивчення канадського досвіду дасть змогу не лише заповнити прогалини нормативно-правової бази України в інформаційній сфері, а й скорегувати подальші напрямки розвитку кібербезпеки, заходів спрямованих на нейтралізацію та запобігання усіх загроз.

Аналіз останніх досліджень та публікацій. Аналізуючи основні підходи канадського уряду у формуванні кібернетичної стратегії, варто виділити важливі програмні документи, які регламентують структуру органів державної влади та провінційних урядів Канади в сфері забезпечення політики безпеки, а саме: Політика національної безпеки Канади (Securing an Open Society: Canada's National Security Policy, 2004)[2], Національна стратегія та План дій у галузі життєво важливої інфраструктури (National Strategy for Critical Infrastructure, Action Plan for Critical, 2011)[3], План дій Канада - США в галузі життєво важливих об'єктів інфраструктури (Canada-United States Action Plan for Critical Infrastructure, 2010)[4], Канадська Стратегія з кібербезпеки для сильної та успішної Канади (Canada's Cyber Security Strategy for a strong and more prosperous Canada, 2010)[5] та План дій стратегії кібербезпеки на 2010-2015 рр. (Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2011)[6]. Також канадським урядом було прийнято низку Законів, що регулюють питання, пов'язані з кібербезпекою: Закон «Про боротьбу зі спамом» (Anti-

[2] Securing an Open Society: Canada's National Security Policy (2004), available at: http: // www.defense-aerospace.com/article-view/reports/38677/canada%E2%80%99s-national-security-policy-%282004%29.html (accessed 17/02/2020).

[3] National Strategy for Critical Infrastructure, Action Plan for Critical Infrastructure (2011), available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx (accessed 12/02/2020).

[4] Canada-United States Action Plan for Critical Infrastructure (2010), available at: https: // www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx (accessed 17/02/2020).

[5]Canada's Cyber Security Strategy. (2018), available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (accessed 19/02/2020).

[6] Action Plan 2010-2015 for Canada's Cyber Security Strategy (2015), available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf. (accessed 15/02/2020).

Spam Act)[7], Постанова «Про безпеку електронних підписів» (Secure Electronic Signature Regulations)[8], Постанова «Про захист електронної комерції» (Electronic Commerce Protection Regulations)[9], Закон «Про електронні документи за захист персональних даних» (Personal Information Protection and Electronic Documents Act)[10]. Ще в 1985 році було прийнято Кримінальне законодавство у сфері кіберзлочинності «Положення Кримінального кодексу»[11]. Також варто зазначити, що дана проблема була об'єктом наукової зацікавленості як вітчизняних[12], так і зарубіжних науковців [13].

В даній статті поставлено за **мету** проаналізувати стратегію кібербезпеки Канади та визначити пріоритетні напрямки розвитку канадської системи інформаційної безпеки. Для досягнення поставленої мети використовувався порівняльний аналіз, елементи структурно-функціонального та системного підходу в аналізі кібернетичної системи Канади. Відповідно до поставленої мети було сформульовано такі **завдання:** дати оцінку політиці Канади щодо захисту кіберпростору; розкрити нормативно-правові та програмні документи реалізації кібербезпеки Канади; охарактеризувати співробітництво канадського уряду в рамках Північноатлантичного альянсу щодо заходів підвищення кіберзахисту на національному рівні.

Виклад основного матеріалу дослідження. 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

[7] Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) available at: http://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html (accessed 15/02/2020).

[8] Secure Electronic Signature Regulations (SOR/2005-30) (2005), available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html (accessed 19/02/2020).

[9] Electronic Commerce Protection Regulations (CRTC) (SOR/2012-36) (2014), available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2012-36/page-1.html. (accessed 15/02/2020).

[10] Personal Information Protection and Electronic Documents Act (2000), available at: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html (accessed 6/02/2020).

[11] Criminal Code (R.S.C., 1985, c. C-46) (2019), available at: http://laws-lois.justice.gc.ca/eng/acts/C-46/ (accessed 16/02/2020).

[12] Варунц Л. (2017), «Роль Королівської канадської кінної поліції в реалізації правоохоронної функції держави», режим доступу: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/4066/Rol%20Korolivskoi%20kanadskoi%20kinnoi%20politsii%20u%20realizatsii %20pravookhoronnoi%20funktsii%20derzhavy_Varunts_2017.pdf?sequence=1 (дата перегляду: 05.02.2020); Канада дозволила постачання летальної зброї Україні (2017), режим доступу: https://www.unian.ua/politics/2296904-kanada-dozvolila-postachannya-letalnoji-zbroji-ukrajini.html (дата перегляду: 01.02.2020); Канадські пластичні хірурги безкоштовно оперуватимуть українських військових у Львові (2019), режим доступу: https://zaxid.net/kanadski_plastichni_hirurgi_bezkoshtovno_operuvatimut_ukrayinskih_viyskovih_u_lvovi_n1490547 (дата перегляду: 06.02.2020); Чеховська М., Марченко М. (2014). «Досвід Канади у формуванні політики інформаційної безпеки», *Порівняльне аналітичне право,* № 7, с. 145-147, режим доступу: http://www.pap.in.ua/7_2014/42.pdf (дата перегляду: 15.02.2020).

[13] Гунина А. (2014), «Политика Канады в сфере обеспечения информационной безопасности», режим доступа: http://www.scienceforum.ru/2014/676/5473 (дата просмотра: 04.02.2020); Никифорова Н. (2013), «Аналитический обзор критериев информационной безопасности ведущих зарубежных стран (США, Канада, Европейский союз)», режим доступа: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf. (дата просмотра: 04.02.2020); Blanchfield M. "Canada Doing More Than Just Military Spending for NATO: Trudeau" (2017), available at: https://torontosun.com/2017/02/17/canada-doing-more-than-just-military-spending-for-nato-trudeau/wcm/530e6c0e-29b9-4d16-9be6-7a27a9b8f2f2 (accessed 10/02/2020); Martin Rudner (2001), "Intelligence and information superiority in the future of Canadian defense policy", Ottawa, "The Norman Paterson School of International Affairs Carleton University", 31 s. available at: https://www3.carleton.ca/csds/docs/occasional_papers/npsia-24.PDF (accessed 13/02/2020); Major H.A.B. Apostoliuk (2013), Communication unification: the need for Canadian armed forces institutional communications. Canadian forcer College, 101 s. available at: https://www.cfc.forces.gc.ca/259/290/299/286/apostoliuk.pdf (accessed 17/02/2020).

захисті кіберпростору[14] 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»[15]. 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 (Canadian Forces – 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 CF. 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[16]. 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»[17]. 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[18].

Поштовхом до розробки власної доктрини InfoOps для CF 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)[19]. В цьому документі зазначалося про сучасні підходи НАТО спрямовані на

[14] Стратегия кибербезопасности Канады (2014), режим доступа: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf; Strategiya kiberbezopasnosti Kanadyi (дата просмотра: 04.02.2020).

[15] Макух-Федоркова І. (2016), «Критерії канадської системи інформаційної безпеки», «UChoice: 4P» Ukrainian Choice: Public Policy, Politics, Psychology: матеріали ІІ міждисциплінарної науково-практичної конференції, Одеса, Жовтень 08, 2016, Одеська юридична академія, сс. 46-49.

[16] Department of Defense Directive (2006), August 14, № 3600.1 available at: http://www.acqnotes.com/Attachments/DoD%20Directive%203600.01%20Information%20Operations%2023%20May%202011.pdf (accessed 16/02/2020).

[17] Ibid.

[18] Martin Rudner (2001), "Intelligence and information superiority in the future of Canadian defense policy", Ottawa, "The Norman Paterson School of International Affairs Carleton University", 31 s. available at: https://www3.carleton.ca/csds/docs/occasional_papers/npsia-24.PDF (accessed 13/02/2020).

[19] 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

«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 The Multinational Information Operations Experiment (MNIOE)[20]. 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 CF 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)[21], 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)[22].

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 (Canadian Forcer Information Operations Group, CFIOG)[23]. 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 (Canadian Forces Electronic Warfare Centre – CFEWC), Центр радіоелектронної розвідки (Canadian Forces Signals Intelligence Operation Centre – 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

(2010), available at: https://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf (accessed 13/02/2020).

[20] The Multinational Information Operations Experiment (MNIOE) within the Multinational Experiment (MNE). Integration of a Multinational CD&E Project (2004), available at: https://www.act.nato.int/images/stories/events/2011/cde/rr_mnioe.pdf (accessed 20/02/2020).

[21]Psychological operations (2004), available at: https: //www.psywar.org/psywar/reproductions/CF_Psychological_Operations_Joint_Doctrine.pdf (accessed 3/02/2020).

[22] Major H.A.B. Apostoliuk (2013), Communication unification: the need for Canadian armed forces institutional communications. Canadian forcer College, 101 s. available at: https://www.cfc.forces.gc.ca/259/290/299/286/apostoliuk.pdf (accessed 17/02/2020).

[23] Canadian Forcer Information Operations Group, CFIOG (2017), available at: https://canadianforces.wordpress.com/cfiog (accessed 10/02/2020).

персоналу забезпечує усю необхідну їм технічну і логістичну підтримку. Девізом станції стали слова pacermpetere, що означає «дослідження світу». При цьому найстаріша канадська станція збору даних радіотехнічної інформації CFS Leitrim 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 CF 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[24]. 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»[25].

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)[26]. 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 кіберінцидентам (CCIRC). Даний центр має мандат для

[24] Гунина А. (2014), «Политика Канады в сфере обеспечения информационной безопасности», режим доступа: http://www.scienceforum.ru/2014/676/5473 (дата просмотра: 04.02.2020).

[25] Никифорова, Н. Аналитический обзор критериев информационной безопасности ведущих зарубежных стран (США, Канада, Европейский союз). URL: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf (дата просмотра: 04.02.2020).

[26] Department of defense trusted computer system evaluation criteria (1985), available at: http:// access: http://csrc.nist.gov/publications/history/dod85.pdf (accessed 11/02/2020).

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[27]. Стратегія кібербезпеки Канади повинна закріпити інформаційні системи країни, особливо в критично важливих секторах інфраструктури, забезпечити підтримку економічного зростання та захисту канадців[28]. 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.

Важливо наголосити, що підхід до забезпечення кіберпростору Канаду є спільною роботою країн-партнерів – США, Великої Британії Австралії та Нової Зеландії. Саме ці країни входять до альянсу «Five Eyes» і проводять колективну радіотехнічну розвідувальну діяльність. Відомо, що 17 квітня 2017 р. США та Британія звинуватили РФ у новій масштабній кібератаці. Саме впродовж 2017 році спецслужби США затримали рекордну кількість російських хакерів Цілями кіберзлочинців були ключові пристрої, які дозволяють встановлювати з'єднання з Інтернетом – маршрутизатори, комутатори та файрвори. Як повідомляє CBC News (2018), ця подія заставила зібратися у Лондоні голів урядів Канади, Британії, Австралії та Нової Зеландії та обговорити стратегію протидії російським кібератакам[29]. Прем'єр-міністр Канади Ж. Трюдо зазначив, що федеральний уряд і Управління безпеки дуже серйозно ставиться до захисту кіберпростору країни. В інтерв'ю він зазначив, що важливу роботу в сфері безпеки і розвідки здійснює CSE (Communications Security Establishment, Організація безпеки зв'язку). Дана організація надає технічну і оперативну допомогу Королівській канадській кінній поліції, федеральним правоохоронним органам та органам безпеки, в тому числі Канадському агентству прикордонних служб і Канадському управлінню безпеки. В розмові прем'єр-міністр зазначив, що протягом п'яти років уряд лібералів планує виділити 507 мільйонів доларів на удосконалення стратегії кібербезпеки, зокрема більша частина коштів буде спрямована на розширення спектру діяльності CSE та створення федерального центру кібербезпеки. При цьому уряд наділив службу розвідки повноваженнями, які дозволяють проводити кібер операції не тільки оборонного, але і наступального характеру[30]. Таким чином, у межах реалізації спільних заходів щодо забезпечення безпеки кіберсередовища Канада активно взаємодіє не тільки з країнами-партнерами, але й постійно зацікавлена у просуванні власних інтересів у сфері кібербезпеки на міжнародних форумах, зокрема G 8, НАТО, ООН.

В НАТО регулярно вживаються заходи з метою вдосконалення захисту мереж зв'язку й інформаційних систем Альянсу, а також надається допомога окремим державам-членам щодо підвищення кіберзахисту на національному рівні. З метою запобігання і реагування на загрози у

[27] Гунина А. (2014), «Политика Канады в сфере обеспечения информационной безопасности», режим доступа: http://www.scienceforum.ru/2014/676/5473 (дата просмотра: 04.02.2020).

[28] Стратегия кибербезопасности североамериканских электрических сетей (2016), режим доступа: http://digitalsubstation.com/blog/2016/12/16/vypushhena-strategiya-kiberbezopasnosti-severo-amerikanskih-elektricheskih-setej/ (дата просмотра: 01.02.2020).

[29] Trudeau talks Russian cyberattacks with Five Eyes counterparts (2018), available at: https://www.cbc.ca/news/politics/trudeau-five-eyes-russia-cyberattacks-1.4625386 (accessed 21/02/2020).

[30] Ibid.

кіберпросторі, в НАТО здійснюється цілодобовий захист мереж. Цю функцію покладено на Агенцію НАТО з питань інформації і комунікацій. Окрім цього, надається консультативна допомога партнерам, орієнтована на індивідуальні потреби кожної країни. Саме на ці та інші військові потреби необхідне серйозне фінансування, тому під час виступу в Брюсселі на саміті НАТО Д. Трамп зазначив, що країни-учасники не витрачають достатньо коштів на підтримку колективної оборони альянсу і запропонував не тільки виконувати це зобов'язання, але й негайно довести оборонні витрати до 2 % ВВП[31]. Зауважимо, що внески Канади складали 1,23 % ВВП, тому прем'єр-міністр Канади Джастін Трюдо офіційно заявив, що буде збільшувати витрати на підтримку колективної обороноздатності НАТО. Вже під час свого візиту до Німеччини в лютому 2017 р., канадський прем'єр-міністр зазначив, що Канада і ФРН виконають найскладнішу роботу в НАТО «Ми будемо збільшувати (внесок Канади в обороноздатність альянсу) як в грошових коштах, так і у вигляді виконання (інших) своїх зобов'язань»[32]. А вже в червні 2017 р. було опубліковано доповідь Міністерства національної оборони Канади, в якій зазначалось про підняття витрат на оборону більше аніж на 70 % протягом наступних десяти років – з 18,9 млрд. дол. в 2016-2017 рр. до 32,7 млрд. дол. в 2026-2027 рр.[33]. Важливо наголосити, що в листопаді 2017 року відбулись 10-ті найбільш масштабні навчання у сфері кіберзахисту у світі під назвою «Кіберкоаліція». У них взяли участь понад сімсот представників з 25 країн-членів Альянсу, комерційні компанії та наукова спільнота. Ці щорічні навчання мали на меті здійснити підготовку персоналу і випробувати в дії спроможність фахівців у галузі кіберзахисту з усього Альянсу, а також вжити необхідних заходів для забезпечення мереж НАТО і національних мереж[34].

Варто нагадати, що ще в березні 2014 р. Канада одна з перших ввела санкції проти російських, українських політичних діячів та організацій у зв'язку з приєднанням Росією Криму. Одночасно з цим відбувалася консолідація блоку НАТО і розвиток співробітництва між його членами з метою стримування Росії. Саме Канада стала помітним учасником цих процесів. Зовнішньополітичний курс Ліберальної партії Канади, що був представлений напередодні виборів 2015 р. містив обіцянку відновити лідерські позиції країни в світі і представляв Канаду в ролі відповідального міжнародного актора, політика якої має сприяти миру і процвітанню в глобальному масштабі[35]. В документі висловлювалась точка зору про те, що необхідно активізувати участь країни в миротворчих операціях ООН, не скорочувати витрати на оборону, більше уваги приділяти проблемам збройних сил, виконувати військові зобов'язання в Центральній і Східній Європі. В останньому пункті про військові зобов'язання в Центрально-Східній Європі мова йшла про участь канадських військових в двох міжнародних операціях – місії REASSURANCE та місії UNIFIER[36].

Операція REASSURANCE була узгоджена Північноатлантичним альянсом 16 квітня 2014 р. у відповідь на входження Криму до складу РФ. Суть її полягала у комплексі заходів військового характеру, націлених на посилення гарантій безпеки держав-членів НАТО, що розміщені в Центральній і Східній Європі, стримування агресивних дій Росії, зміцнення колективної оборони. Вказані заходи передбачали патрулювання прикордонних повітряних і морських просторів, проведення військових навчань і демонстрацію сили, дії, спрямовані на підвищення оперативності союзних військ. Авіація і кораблі ВМФ країни прийняли активну участь в цій місії, проте особливо відзначилась присутність 200 канадських військовослужбовців на ротаційній основі в

[31] Jeremy Diamond Trump scolds NATO allies over defense spending (2017), available at: https://edition.cnn.com/2017/05/25/politics/trump-nato-financial-payments/index.html (accessed 16/02/2020).
[32] Blanchfield M. "Canada Doing More Than Just Military Spending for NATO: Trudeau" (2017), available at: https://torontosun.com/2017/02/17/canada-doing-more-than-just-military-spending-for-nato-trudeau/wcm/530e6c0e-29b9-4d16-9be6-7a27a9b8f2f2 (accessed 10/02/2020).
[33] Strong, Secure, Engaged. Canada's Defense Policy (2017), Minister of National Defence, 113 p. available at: http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf (accessed 11/02/2020).
[34] Щорічний звіт Генерального секретаря (2017), режим доступу: https:// www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_03/20180905_SG_AnnualReport_2017_ukr.pdf (дата перегляду: 15.02.2020).
[35] Real Change (2015), "A New Plan for a Strong Middle Class" available at: https: //www.liberal.ca/files/2015/10/New-plan-for-a-strong-middle-class.pdf (accessed 9/02/2020).
[36] Ibid

Польщі в період з 2014 по 2017 р.[37]. Міністерство національної оборони / Збройні сили Канади 18 травня 2018 р. підписали технічну угоду з Міністерством внутрішніх справ України, а також важливим фактом є те, що 18 березня 2019 р. уряд Канади продовжив операцію UNIFIER до кінця березня 2022 р.[38]. Заява щодо продовження участі Оттави в даній операції викликала гостру критику зі сторони РФ. Так, представник Посольства РФ в Канаді заявив, що це «не сприяє внутрішньо українському політичному процесу, включаючи передбачуваний мінськими угодами діалог між Києвом і Донбасом»[39].

Що стосується міжнародної операції UNIFIER, то це ще один приклад реалізації Канадою стратегії «лояльного союзника» поряд з Сполученими Штатами і Великобританією. Про участь в цій операції Канада оголосила 14 квітня 2015 р. і ці дії спрямовувалися на організацію додаткової підготовки і навчання українських військових. Канадські військовослужбовці розмістилися на Яворівському полігоні у Львівській області і від початку роботи місії за допомогою фахівців Канади вишкіл пройшли понад 5 тисяч військовослужбовців Збройних Сил України[40]. Більше того, Канада внесла Україну до списку країн, яким дозволено поставляти летальну зброю. За даними Canada Gazette метою цього кроку є «підтримка двосторонніх відносин Канади з Україною» та надання можливості «канадським експортерам подавати заявку на експорт певних видів стрілецької зброї, забороненої зброї та заборонених пристроїв в Україну»[41]. Канада включила Україну до Контрольного переліку країн, яким дозволено поставку автоматичної зброї, а Сполучені Штати Америки санкціонували безпекову допомогу українській державі. Адже Дональдом Трампом було підписано оборонний бюджет на 2018 р., в якому передбачалося 350 млн. дол. для надання безпекової допомоги Україні та заходи щодо протистояння російській агресії[42]. Важливо також підкреслити, що за роки збройного протистояння на Сході України відбулося сім медичних місій лікарів з Канади. Канадські хірурги здійснювали пластичні операції учасникам АТО та військовослужбовцям, а групу лікарів очолював відомий професор пластичної хірургії університету Торонто Олег Антонишин. Він регулярно з 2014 року приїздить до України для проведення операцій постраждалим внаслідок російсько-української війни[43]. Також Канада виділяла кошти Україні для боротьби з кремлівською пропагандою, а саме в галузі кібербезпеки. Співпраця між Україною та Канадою в галузі кібербезпеки дозволяє перейняти провідний досвід протистояння втручанню у демократичні процеси – зазначила кореспонденту Укрінформ міністр закордонних справ Канади Христя Фріланд[44]. Більше того, «Високопоставлений американський чиновник нещодавно сказав мені, що Україна – це російська лабораторія для дослідження ворожого втручання, тому взаємодія з Україною дає США змогу зрозуміти, що відбувається, і як захистити власну країну. Канада вважає так само» – сказала Х.Фріланд[45].

Співпраця між США і Канадою в плані захисту національного простору помітна і в тому, що останнім часом обидві країни планують розширити свою взаємодію в сфері протиповітряної

[37] Operation REASSURANCE (2018), available at: https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-reassurance. html (accessed 9/02/ 2020).

[38]Operation UNIFIER available at: https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-unifier.html (accessed 10/02/2020).

[39] Решение Канады продлить военную миссию в Украине разгневало Кремль» (2017), режим доступа: https://enovosty.com/news_politics/full/834-reshenie-kanady-prodlit-voennuyu-missiyu-v-ukraine-razgnevalo-kreml (дата просмотра: 04.02.2020).

[40] У Міжнародному центрі миротворчості та безпеки на Яворівському полігоні відбулась урочиста церемонія передачі повноважень операції «Unifier» (2018), режим доступу: https://www.ukrinform.ua/rubric-ato/2544619-misia-unifier-kanadski-vijskovi-proveli-rotaciu-v-ukraini.html (дата перегляду: 05.02.2020).

[41]Canada Gazette OTTAWA (2017), December 13, Vol. 151, №. 25. available at: http://gazette.gc.ca/rp-pr/p2/2017/2017-12-13/pdf/g2-15125.pdf. (accessed 16/02/2020).

[42]Канада дозволила постачання летальної зброї Україні (2017), режим доступу: https://www.unian.ua/politics/2296904-kanada-dozvolila-postachannya-letalnoji-zbroji-ukrajini.html (дата перегляду: 01.02.2020).

[43] Канадські пластичні хірурги безкоштовно оперуватимуть українських військових у Львові (2019), режим доступу: https://zaxid.net/kanadski_plastichni_hirurgi_bezkoshtovno_operuvatimut_ukrayinskih_viyskovih_u_lvovi_n1490547 (дата перегляду: 06.02.2020).

[44] Канаді є чого повчитися в Україні (2020), режим доступу: https://www.ukrinform.ua/rubric-technology/2678577-kanadi-e-cogo-povcitisa-v-ukraini-friland.html (дата перегляду: 09.02.2020).

[45]Там само

оборони (ППО) та в кіберпросторі. Свідченням цьому є спільний контроль NORAD (система повітряно-космічної оборони США і Канади, яка була створена в 1958 р.) повітряного простору Північної Америки. У зв'язку з тим, що постійно наростає загроза виникнення кібератак та втручання в північноамериканський повітряний простір військовими лідерами США і Канади було прийнято рішення спільними зусиллями модернізувати оборонну сферу NORAD[46]. Крім того, 19 січня 2017 р. Генсек НАТО Столтенберг зазначив, що кількість хакерських атак на мережі НАТО зросла на 60 %. У зв'язку з цим, Канаді та іншим країнам НАТО потрібно адаптуватися і застосувати більш активні заходи у протистоянні кібератакам зі сторони Росії. Як результат, Альянс прийняв план дій щодо використання кіберпростору в якості оперативного середовища і 8 листопада 2017 р. в Брюсселі узгодили створення нового командного центру щодо операцій в кіберпросторі[47]. Результатом продуманої роботи канадського уряду в цьому напрямку є створення нового спеціального органу по захисту кібернетичного простору. «Канадський центр кібербезпеки стане головним джерелом офіційної інформації та радою для канадських підприємців, власників і операторів критичної інфраструктури і всіх канадців. Експерти Центру будуть співпрацювати з партнерами в академічній і приватній сферах з метою боротьби із складними кібернетичними викликами, які виникають перед Канадою», – заявили в Міноборони[48].

Що стосується захисту канадських громадян на внутрішньому рівні, то основним органом, який координує роботу в сфері боротьби з тероризмом, захист критичної інфраструктури, забезпечення кібербезпеки та транспортної безпеки є Міністерство громадської безпеки Канади. Важливо зазначити, що саме це Міністерство тісно співпрацює з національними й міжнародними організаціями у межах глобального співробітництва із захисту життєво важливої інфраструктури та інформації, а також боротьби із кіберзлочинністю[49]. Більше того, Міністерство громадської безпеки Канади також забезпечує проведення суспільно-просвітницьких і пропагандистських заходів з метою інформування громадян про можливі потенційні ризики та інформує про комплекс дій, які вони можуть застосувати, щоб захистити себе та свої родини в кіберпросторі. Досвід із протидії кіберзагрозам має Канадська організація з Комунікаційної Безпеки, вона посилює власний потенціал для визначення й виявлення загроз, забезпечує інформацією зовнішню розвідку та служби кібербезпеки, реагує на кіберзагрози й напади на урядові мережі та системи інформаційних технологій[50]. Національним законодавством визначено, що суб'єктом забезпечення кібербезпеки країни є Канадська служба безпеки й розвідки, яка аналізує і досліджує внутрішні й міжнародні загрози безпеки Канади. Крім того, Королівська канадська кінна поліція є відповідальним органом у забезпеченні кібербезпеки. Слід наголосити, що Королівська канадська кінна поліція відіграє важливу роль у здійсненні правоохоронної функції держави, а саме: забезпечує державну політику боротьби зі злочинністю, громадський порядок, сприяє запобіганню та припиненню правопорушень; здійснює профілактичні заходи з метою попередження, виявлення, припинення та розкриття злочинів; бере участь у наукових, кримінологічних і соціологічних дослідженнях, розробці відповідних державних програм щодо боротьби зі злочинністю та охорони правопорядку; здійснює на договірній основі функції муніципальної чи провінційної поліції у відповідних регіонах, реагує на потреби тих людей, яким у силу якихось обставин необхідна термінова допомога[51]. Діяльність поліції Канади направлена на різно-

[46] Canadian, U.S. military leaders agree on framework to retool NORAD (2019), available at: https://www.cbc.ca/news/politics/norad-canada-us-military-1.5240855(accessed 15/02/2020).

[47] NATO and Canada adapting to new and evolving cyber threats (2017), available at: https://www.cbc.ca/radio/thehouse/nato-and-canada-adapting-to-new-and-evolving-threats-1.4405551/nato-and-canada-adapting-to-new-and-evolving-cyber-threats-1.4408307 (accessed 12/02/2020).

[48] Канада создала новый центр по кибербезопасности (2018), режим доступа: https://news.finance.ua/ru/news/-/435888/kanada-sozdala-novyj-tsentr-po-kiberbezopasnosti (дата просмотра: 04.02.2020).

[49] Чеховська М., Марченко М. (2014). «Досвід Канади у формуванні політики інформаційної безпеки», *Порівняльне аналітичне право,* № 7, с. 145-147, режим доступу: http://www.pap.in.ua/7_2014/42.pdf (дата перегляду: 15.02.2020).

[50] Там само.

[51] Варунц Л. (2017), «Роль Королівської канадської кінної поліції в реалізації правоохоронної функції держави», режим доступу: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/4066/Rol%20Korolivskoi%20kanadskoi%20kinnoi%20politsii%20u%20realizatsii%20pravookhoronnoi%20funktsii%20derzhavy_Varunts_2017.pdf?sequence=1 (дата перегляду: 05.02.2020).

бічний розвиток відносин з якомога більшим суспільним колом через засоби масової інформації, консультативні зустрічі з представниками громадськості, взаємовідносини з різноманітними органами влади і управління, громадськими організаціями, окремими громадянами. Поліція є важливим партнером у співтоваристві відомств, що займаються боротьбою зі злочинністю та забезпеченні дотримання прав людини[52]. Серед пріоритетних напрямків взаємодії поліції з громадськістю необхідно виділити: встановлення партнерських взаємовідносин, консультації з населенням з метою визначення проблем, які хвилюють відповідну громаду та вироблення адекватної стратегії дій, підзвітність громаді за свою діяльність. Більше того, відповідно до Закону про Королівську канадську кінну поліцію, розслідує підозри про внутрішні та міжнародні злочинні діяння проти канадських критичних інформаційних мереж й інфраструктури.

На внутрішньому рівні постійно розробляються нові Закони спрямовані на забезпечення кібербезпеки, формуються законодавчі ініціативи та виділяються фінансові ресурси. Позитивним досвідом є те, що Канада має давню історію взаємодії державного і приватного секторів у напрямку реалізації економічної і національної безпеки. Ця спільна співпраця забезпечується за рахунок взаємного обміну точною та своєчасною інформацією щодо кіберзагроз, відпрацьовуються методи захисту та інші передові практики. Згідно даних Статистичного агентства Канади протягом 2017 року канадські приватні компанії витратили на кібербезпеку 14 млрд. дол.[53]. Із цієї суми 8 млрд. дол. було витрачено на зарплати експертів й консультантів, 4 млрд. дол. було вкладено у оновлення відповідного програмного забезпечення та обладнання, а решта 2 млрд. були спрямовані на інші методи захисту[54]. Важливо зазначити, що протягом 2018 року кібернетичної атаки зазнала кожна п’ята канадська кампанія.

Напрямки кібернетичної безпеки Канади спрямовані на підтримку партнерських відносин центрального уряду з урядами провінцій і приватним сектором задля забезпечення важливих кіберсистем поза межами федерального уряду, а також розробка комплексу заходів посилення особистої безпеки громадян Канади в кіберпросторі. Урядом Канади вже прийнято закон, який регламентує боротьбу з крадіжками особистих даних. Скандал щодо незаконного використання персональних даних британською компанією Cambridge Analytica за сприяння американської компанії Facebook став каталізатором реформування інформаційного законодавства Канади у відповідності до сучасних цифрових викликів. Доречно нагадати, що інцидент щодо незаконного використання персональних даних компанією Cambridge Analitica виник ще в 2017 році після несподіваної для багатьох аналітиків перемоги Дональда Трампа у президентських перегонах у США. При цьому журналістами був виявлений зв'язок між Cambridge Analytica, Facebook і членами команди новообраного президента США. Тому ще наприкінці 2018 року Канада внесла поправки до Закону про конфіденційність, який регулює обробку персональних даних федеральними інституціями та Закону про захист персональних даних та електронні документи, який діє в приватному секторі. Інші законодавчі ініціативи реалізуються урядом у напрямі зміцнення потенціалу правоохоронних органів з метою розслідування та кримінального переслідування кіберзлочинності, зокрема шляхом визнання кримінальним злочином використання комп’ютерної системи для сексуальної експлуатації дітей; співпраця з провайдерами Інтернет-послуг можливості використання систем перехоплення та допомога поліції в забезпеченні вихідними даними ідентифікації клієнта, оскільки ця інформація є важливою для боротьби з онлайн злочинцями[55]. Окрім Королівської канадської кінної поліції відповідальними органами у сфері кібербезпеки є Центр реагування на надзвичайні ситуації у кіберпросторі (Canadian Cyber Incident Response Centre), Офіс омбудсмена з питань персональних даних (Office of the Privacy Commissioner of Canada) та Управління захисту важливих об’єктів інфраструктури та готовнос-

[52] Варунц Л. (2017), Вказ. пр.

[53] Impact of cybercrime on Canadian businesses (2017), available at: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm?HPA=1 (accessed 14/02/2020)

[54] У Канаді за рік витратили 14 млрд. дол. на кібербезпеку (2018), режим доступу: https://www.ukrinform.ua/rubric-world/2559084-u-kanadi-za-rik-vitratili-14-milardiv-na-kiberbezpeku.html (дата перегляду: 06.02.2020).

[55] Чеховська М., Марченко М. (2014). «Досвід Канади у формуванні політики інформаційної безпеки», *Порівняльне аналітичне право,* № 7, с. 145-147, режим доступу: http://www.pap.in.ua/7_2014/42.pdf (дата перегляду: 15.02.2020).

ті до надзвичайних ситуацій Міністерства державної безпеки (Office of Critical Infrastructure Protection and Emergency Preparedness)[56].

Висновки. Підсумовуючи варто наголосити, що останніми роками в сучасному світі кібернетичні загрози набувають безпрецедентного поширення, стають дедалі складнішими і руйнівними за своїми наслідками. У найгіршому випадку кібернапад може вивести з ладу інфраструктуру країни, паралізувати урядові структури, підірвати демократичний устрій, серйозним чином вплинути на обороноздатність збройних сил. Враховуючи швидкість і складність сучасних кібератак на державні, корпоративні та приватні ресурси, потрібно постійно моніторити ситуацію та інвестувати в сферу кіберпростору, що в майбутньому гарантуватиме як сталий економічний розвиток, так і належне забезпечення рівня національної безпеки. 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. На внутрішньому рівні інформаційна політика Канади та система інформаційної безпеки спрямована на забезпечення захисту цілісності державних систем і критично важливих активів країни. Важливим елементом роботи є постійне підвищення поінформованості громадян, суспільства та урядовців щодо необхідності реалізації заходів з кібербезпеки, а також заохочення застосовувати технології, необхідні для протистояння кіберзагрозам. Позитивними тенденціям в цьому напрямку передувала цілеспрямована реформаторська політика уряду, належне фінансування та прийняття низки як нормативно-правових, так і програмних документів. Як зазначалося вище, програмним документом у сфері забезпечення кібербезпеки є План дій щодо реалізації кібербезпеки Канади, прийнятий ще в 2010 до 2015 рр. Кінцевою метою цього документу був захист кіберсередовища в інтересах канадців і національної економіки. Враховуючи світові зовнішні виклики Міністерство оборони ініціювало створення в 2017 р. Канадського центру кібербезпеки. Канадський уряд велику увагу приділяє співробітництву в рамках Північноатлантичного альянсу, продовжує нарощувати оборонні витрати та приймати активну участь в зміцненні «східного флангу» НАТО. Відомим фактом є те, що за останні роки Альянс вжив низку заходів спрямованих на вдосконалення інформаційних систем та мереж зв'язку, а також надав допомогу державам-членам щодо підвищення кіберзахисту на національному рівні. Канада дотримується цієї стратегії так як розглядає цю співпрацю оптимальним способом забезпечення безпеки і зміцнення міжнародного іміджу країни. Важливим моментом також є те, що в документах, які регламентують діяльність у сфері кібербезпеки та виступають передумовою реалізації практичних підходів у забезпеченні безпекової політики країни є співпраця усіх зацікавлених сторін: уряду, провінцій, представників бізнесу і громадян у спільній партнерській діяльності. Тому пріоритетними напрямами є розвиток і захист канадської інформаційної інфраструктури, удосконалення послуг і продукції в сфері інформаційної безпеки, підвищення обізнаності громадськості щодо он-лайн безпеки, захист урядових інформаційних систем.

Список в джерел

1. Варунц Л. (2017), «Роль Королівської канадської кінної поліції в реалізації правоохоронної функції держави», режим доступу: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/4066/Rol%20Korolivskoi%20kanadskoi%20kinnoi%20politsii%20u%20realizatsii%20pravookhoronnoi%20funktsii%20derzhavy_Varunts_2017.pdf?sequence=1 (дата перегляду: 05.02.2020).

2. Гунина А. (2014), «Политика Канады в сфере обеспечения информационной безопасности», режим доступа: http://www.scienceforum.ru/2014/676/5473 (дата просмотра: 04.02.2020).

[56] Cyber wellness Profile Canada (2012), available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Canada.pdf (accessed 16/02/2020)

3. Канада дозволила постачання летальної зброї Україні (2017), режим доступу: https://www.unian.ua/politics/2296904-kanada-dozvolila-postachannya-letalnoji-zbroji-ukrajini.html (дата перегляду: 01.02.2020).

4. Канадські пластичні хірурги безкоштовно оперуватимуть українських військових у Львові (2019), режим доступу: https://zaxid.net/kanadski_plastichni_hirurgi_bezkoshtovno_operuvatimut_ukrayinskih_viyskovih_u_lvovi_n1490547 (дата перегляду: 06.02.2020).

5. Канаді є чого повчитися в Україні (2020), режим доступу: https://www.ukrinform.ua/rubric-technology/2678577-kanadi-e-cogo-povcitisa-v-ukraini-friland.html (дата перегляду: 09.02.2020).

6. Канада создала новый центр по кибербезопасности (2018), режим доступа: https://news.finance.ua/ru/news/-/435888/kanada-sozdala-novyj-tsentr-po-kiberbezopasnosti (дата просмотра: 04.02.2020)

7. Макух-Федоркова І. (2016), «Критерії канадської системи інформаційної безпеки», «UChoice: 4P» Ukrainian Choice: Public Policy, Politics, Psychology: матеріали ІІ міждисциплінарної науково-практичної конференції, Одеса, Жовтень 08, 2016, Одеська юридична академія, сс. 46-49.

8. Никифорова Н. (2013), «Аналитический обзор критериев информационной безопасности ведущих зарубежных стран (США, Канада, Европейский союз)», режим доступа: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf (дата просмотра: 04.02.2020).

9. Решение Канады продлить военную миссию в Украине разгневало Кремль» (2017), режим доступа: https://enovosty.com/news_politics/full/834-reshenie-kanady-prodlit-voennuyu-missiyu-v-ukraine-razgnevalo-kreml (дата просмотра: 04.02.2020).

10. Стратегия кибербезопасности североамериканских электрических сетей (2016), режим доступа: http://digitalsubstation.com/blog/2016/12/16/vypushhena-strategiya-kiberbezopasnosti-severo-amerikanskih-elektricheskih-setej/ (дата просмотра: 01.02.2020).

11. Стратегия кибербезопасности Канады (2014), режим доступа: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf; Strategiya kiberbezopasnosti Kanadyi (дата просмотра: 04.02.2020).

12. Сунь-Дзи (2017), «Мистецтво війни», Видавництво Старого Лева, Львів, 100 с.

13. У Канаді за рік витратили 14 млрд. дол. на кібербезпеку (2018), режим доступу: https://www.ukrinform.ua/rubric-world/2559084-u-kanadi-za-rik-vitratili-14-milardiv-na-kiberbezpeku.html (дата перегляду: 06.02.2020).

14. У Міжнародному центрі миротворчості та безпеки на Яворівському полігоні відбулась урочиста церемонія передачі повноважень операції «Unifier» (2018), режим доступу: https://www.ukrinform.ua/rubric-ato/2544619-misia-unifier-kanadski-vijskovi-proveli-rotaciu-v-ukraini.html (дата перегляду: 05.02.2020).

15. Чеховська М., Марченко М. (2014). «Досвід Канади у формуванні політики інформаційної безпеки», *Порівняльне аналітичне право,* № 7, с. 145-147, режим доступу: http://www.pap.in.ua/7_2014/42.pdf (дата перегляду: 15.02.2020).

16. Щорічний звіт Генерального секретаря (2017), режим доступу: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_03/20180905_SG_AnnualReport_2017_ukr.pdf (дата перегляду: 15.02.2020).

17. Action Plan 2010-2015 for Canada's Cyber Security Strategy (2015), available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf. (accessed 15/02/2020).

18. Blanchfield M. "Canada Doing More Than Just Military Spending for NATO: Trudeau" (2017), available at: https://torontosun.com/2017/02/17/canada-doing-more-than-just-military-spending-for-nato-trudeau/wcm/530e6c0e-29b9-4d16-9be6-7a27a9b8f2f2 (accessed 10/02/2020).

19. Canadian Forcer Information Operations Group, CFIOG (2017), available at: https://canadianforces.wordpress.com/cfiog (accessed 10/02/2020).

20. Canadian, U.S. military leaders agree on framework to retool NORAD (2019), available at: https:// www.cbc.ca/news/politics/norad-canada-us-military-1.5240855(accessed 15/02/2020).

21. Canada's Cyber Security Strategy. (2018), available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (accessed 19/02/2020).

22. Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) available at: http://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html (accessed 15/02/2020).

23. Canada-United States Action Plan for Critical Infrastructure (2010), available at: https: // www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx (accessed 17/02/2020).

24. Canada Gazette OTTAWA (2017), December 13, Vol. 151, №. 25. available at: http://gazette.gc.ca/rp-pr/p2/2017/2017-12-13/pdf/g2-15125.pdf. (accessed 16/02/2020).

25. Criminal Code (R.S.C., 1985, c. C-46) (2019), available at: http://laws-lois.justice.gc.ca/eng/acts/C-46/ (accessed 16/02/2020).

26. Cyber wellness Profile Canada (2012), available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Canada.pdf (accessed 16/02/2020).

27. Department of defense trusted computer system evaluation criteria (1985), available at: http:// access: http://csrc.nist.gov/publications/history/dod85.pdf (accessed 11/02/2020).

28. Electronic Commerce Protection Regulations (CRTC) (SOR/2012-36) (2014), available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2012-36/page-1.html. (accessed 15/02/2020).

29. Impact of cybercrime on Canadian businesses (2017), available at: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm?HPA=1 (accessed 14/02/2020).

30. Department of Defense Directive (2006), August 14, № 3600.1 available at: http://www.acqnotes.com/Attachments/DoD%20Directive%203600.01%20Information%20Operations%2023%20May%202011.pdf (accessed 16/02/2020).

31. Jeremy Diamond Trump scolds NATO allies over defense spending (2017), available at: https://edition.cnn.com/2017/05/25/politics/trump-nato-financial-payments/index.html (accessed 16/02/2020).

32. 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 (2010), available at: https://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf (accessed 13/02/2020).

33. Martin Rudner (2001), "Intelligence and information superiority in the future of Canadian defense policy", Ottawa, "The Norman Paterson School of International Affairs Carleton University", 31 s. available at: https: //www3.carleton.ca/csds/docs/occasional_papers/npsia-24.PDF (accessed 13/02/2020).

34. Major H.A.B. Apostoliuk (2013), Communication unification: the need for Canadian armed forces institutional communications. Canadian forcer College, 101 s. available at: https://www.cfc.forces.gc.ca/259/290/299/286/apostoliuk.pdf (accessed 17/02/2020).

35. National Strategy for Critical Infrastructure, Action Plan for Critical Infrastructure (2011), available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx (accessed 12/02/2020).

36. NATO and Canada adapting to new and evolving cyber threats (2017), available at: https://www.cbc.ca/radio/thehouse/nato-and-canada-adapting-to-new-and-evolving-threats-1.4405551/nato-and-canada-adapting-to-new-and-evolving-cyber-threats-1.4408307 (accessed 12/02/2020).

37. Operation UNIFIER available at: https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-unifier.html (accessed 10/02/2020).

38. Operation REASSURANCE (2018), available at: https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-reassurance.html (accessed 9/02/2020).

39. Personal Information Protection and Electronic Documents Act (2000), available at: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html (accessed 6/02/2020)

40. Psychological operations (2004), available at: https: //www.psywar.org/psywar/reproductions/CF_Psychological_Operations_Joint_Doctrine.pdf (accessed 3/02/2020)

41. Real Change (2015), "A New Plan for a Strong Middle Class" available at: https: //www.liberal.ca/files/2015/10/New-plan-for-a-strong-middle-class.pdf (accessed 9/02/2020).

42. Secure Electronic Signature Regulations (SOR/2005-30) (2005), available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html (accessed 19/02/2020).

43. Securing an Open Society: Canada's National Security Policy (2004), available at: http: // www.defense-aerospace.com/article-view/reports/38677/canada%E2%80%99s-national-security-policy-%282004%29.html (accessed 17/02/2020).

44. Strong, Secure, Engaged. Canada's Defense Policy (2017), Minister of National Defence, 113 p. available at: http:// dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf (accessed 11/02/2020).

45. The Multinational Information Operations Experiment (MNIOE) within the Multinational Experiment (MNE). Integration of a Multinational CD&E Project (2004), available at: https://www.act.nato.int/images/stories/events/2011/cde/rr_mnioe.pdf (accessed 20/02/2020).

46. Trudeau talks Russian cyberattacks with Five Eyes counterparts (2018), available at: https:// www.cbc.ca/news/politics/trudeau-five-eyes-russia-cyberattacks-1.4625386 (accessed 21/02/2020).

References

1. Varunts L. (2017), «Rol Korolivskoi kanadskoi kinnoi politsii v realizatsii pravookhoronnoi funktsii derzhavy», rezhym dostupu http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/4066/Rol%20Korolivskoi%20kanadskoi%20kinnoi%20politsii%20u%20realizatsii.%20pravookhoronnoi%20funktsii%20derzhavy_Varunts_2017.pdf?sequence=1 (data perehliadu: 05.02.2020).

2. Gunina A. (2014), «Politika Kanadyi v sfere obespecheniya informatsionnoy bezopasnosti», rezhim dostupa: http://www.scienceforum.ru/2014/676/5473 (data prosmotra: 04.02.2020).

3. Kanada dozvolyla postachannia letalnoi zbroi Ukraini (2017), rezhym dostupu: https://www.unian.ua/politics/2296904-kanada-dozvolila-postachannya-letalnoji-zbroji-ukrajini.html (data perehliadu: 01.02.2020)

4. Kanadski plastychni khirurhy bezkoshtovno operuvatymut ukrainskykh viiskovykh u Lvovi (2019), rezhym dostupu https://zaxid.net/kanadski_plastichni_hirurgi_bezkoshtovno_operuvatimut_ukrayinskih_viyskovih_u_lvovi_n1490547 (data perehliadu: 06.02.2020)

5. Kanadi ye choho povchytysia v Ukraini (2020), rezhym dostupu: https://www.ukrinform.ua/rubric-technology/2678577-kanadi-e-cogo-povcitisa-v-ukraini-friland.html (data perehliadu: 09.02.2020)

6. Kanada sozdala novyiy tsentr po kiberbezopasnosti (2018), rezhim dostupa https://news.finance.ua/ru/news/-/435888/kanada-sozdala-novyj-tsentr-po-kiberbezopasnosti (data prosmotra: 04.02.2020)

7. Makukh-Fedorkova I. (2016), «Kryterii kanadskoi systemy informatsiinoi bezpeky», «UChoice: 4P» Ukrainian Choice: Public Policy, Politics, Psychology: materialy II mizhdystsyplinarnoi naukovo-praktychnoi konferentsii, Odesa, Zhovten 08, 2016, Odeska yurydychna akademiia, ss. 46-49.

8. Nikiforova N. (2013), «Analiticheskiy obzor kriteriev informatsionnoy bezopasnosti veduschih zarubezhnyih stran (SShA, Kanada, Evropeyskiy soyuz)», rezhim dostupa: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf. (data prosmotra: 04.02.2020).

9. Reshenie Kanadyi prodlit voennuyu missiyu v Ukraine razgnevalo Kreml» (2017), rezhim dostupa: https://enovosty.com/news_politics/full/834-reshenie-kanady-prodlit-voennuyu-missiyu-v-ukraine-razgnevalo-kreml (data prosmotra: 04.02.2020).

10. Strategiya kiberbezopasnosti severoamerikanskih elektricheskih setey (2016), rezhim dostupa: http://digitalsubstation.com/blog/2016/12/16/vypushhena-strategiya-kiberbezopasnosti-severo-amerikanskih-elektricheskih-setej/ (data prosmotra: 01.02.2020).

11. Strategiya kiberbezopasnosti Kanadyi (2014), rezhim dostupa: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf; Strategiya kiberbezopasnosti Kanadyi (data prosmotra: 04.02.2020).

12. Sun-Dzy (2017), «Mystetstvo viiny», Vydavnytstvo Staroho Leva, Lviv, 100s.

13. U Kanadi za rik vytratyly 14 mlrd. dol. na kiberbezpeku (2018), rezhym dostupu: https://www.ukrinform.ua/rubric-world/2559084-u-kanadi-za-rik-vitratili-14-milardiv-na-kiberbezpeku.html (data perehliadu: 06.02.2020).

14. U Mizhnarodnomu tsentri myrotvorchosti ta bezpeky na Yavorivskomu polihoni vidbulas urochysta tseremoniia peredachi povnovazhen operatsii «Unifier» (2018), rezhym dostupu:

https://www.ukrinform.ua/rubric-ato/2544619-misia-unifier-kanadski-vijskovi-proveli-rotaciu-v-ukraini.html (data perehliadu: 05.02.2020).

15. Chekhovska M., Marchenko M. (2014). «Dosvid Kanady u formuvanni polityky informatsiinoi bezpeky», *Porivnialne analitychne pravo,* № 7, s. 145-147, rezhym dostupu: http://www.pap.in.ua/7_2014/42.pdf (data perehliadu: 15.02.2020).
16. Shchorichnyi zvit Heneralnoho sekretaria (2017), rezhym dostupu: https:// www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_03/20180905_SG_AnnualReport_2017_ukr.pdf (data perehliadu: 15.02.2020).
17. Action Plan 2010-2015 for Canada's Cyber Security Strategy (2015), available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf. (accessed 15/02/2020).
18. Blanchfield M. "Canada Doing More Than Just Military Spending for NATO: Trudeau" (2017), available at: https://torontosun.com/2017/02/17/canada-doing-more-than-just-military-spending-for-nato-trudeau/wcm/530e6c0e-29b9-4d16-9be6-7a27a9b8f2f2 (accessed 10/02/2020).
19. Canadian Forcer Information Operations Group, CFIOG (2017), available at: https://canadianforces.wordpress.com/cfiog (accessed 10/02/2020).
20. Canadian, U.S. military leaders agree on framework to retool NORAD (2019), available at: https:// www.cbc.ca/news/politics/norad-canada-us-military-1.5240855(accessed 15/02/2020).
21. Canada's Cyber Security Strategy. (2018), available at: http://www.publicsafety.gc.ca/ cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (accessed 19/02/2020).
22. Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) available at: http://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html (accessed 15/02/2020).
23. Canada-United States Action Plan for Critical Infrastructure (2010), available at: https: // www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx (accessed 17/02/2020).
24. Canada Gazette OTTAWA (2017), December 13, Vol. 151, №. 25. available at: http://gazette.gc.ca/rp-pr/p2/2017/2017-12-13/pdf/g2-15125.pdf. (accessed 16/02/2020).
25. Criminal Code (R.S.C., 1985, c. C-46) (2019), available at: http://laws-lois.justice.gc.ca/eng/acts/C-46/ (accessed 16/02/2020).
26. Cyber wellness Profile Canada (2012), available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Canada.pdf (accessed 16/02/2020).
27. Department of defense trusted computer system evaluation criteria (1985), available at: http:// access: http://csrc.nist.gov/publications/history/dod85.pdf (accessed 11/02/2020).
28. Electronic Commerce Protection Regulations (CRTC) (SOR/2012-36) (2014), available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2012-36/page-1.html. (accessed 15/02/2020).
29. Impact of cybercrime on Canadian businesses (2017), available at: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm?HPA=1 (accessed 14/02/2020).
30. Department of Defense Directive (2006), August 14, № 3600.1 available at: http://www.acqnotes.com/Attachments/DoD%20Directive%203600.01%20Information%20Operations%2023%20May%202011.pdf (accessed 16/02/2020).
31. Jeremy Diamond Trump scolds NATO allies over defense spending (2017), available at: https://edition.cnn.com/2017/05/25/politics/trump-nato-financial-payments/index.html (accessed 16/02/2020).
32. 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 (2010), available at: https://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf (accessed 13/02/2020).
33. Martin Rudner (2001), "Intelligence and information superiority in the future of Canadian defense policy", Ottawa, "The Norman Paterson School of International Affairs Carleton University", 31 s. available at: https: //www3.carleton.ca/csds/docs/occasional_papers/npsia-24.PDF (accessed 13/02/2020).

34. Major H.A.B. Apostoliuk (2013), Communication unification: the need for Canadian armed forces institutional communications. Canadian forcer College, 101 s. available at: https://www.cfc.forces.gc.ca/259/290/299/286/apostoliuk.pdf (accessed 17/02/2020).

35. National Strategy for Critical Infrastructure, Action Plan for Critical Infrastructure (2011), available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx (accessed 12/02/2020).

36. NATO and Canada adapting to new and evolving cyber threats (2017), available at: https://www.cbc.ca/radio/thehouse/nato-and-canada-adapting-to-new-and-evolving-threats-1.4405551/nato-and-canada-adapting-to-new-and-evolving-cyber-threats-1.4408307 (accessed 12/02/2020).

37. Operation UNIFIER available at: https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-unifier.html (accessed 10/02/2020).

38. Operation REASSURANCE (2018), available at: https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-reassurance.html (accessed 9/02/2020).

39. Personal Information Protection and Electronic Documents Act (2000), available at: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html (accessed 6/02/2020)

40. Psychological operations (2004), available at: https: //www.psywar.org/psywar/reproductions/CF_Psychological_Operations_Joint_Doctrine.pdf (accessed 3/02/2020)

41. Real Change (2015), "A New Plan for a Strong Middle Class" available at: https: //www.liberal.ca/files/2015/10/New-plan-for-a-strong-middle-class.pdf (accessed 9/02/2020).

42. Secure Electronic Signature Regulations (SOR/2005-30) (2005), available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html (accessed 19/02/2020).

43. Securing an Open Society: Canada's National Security Policy (2004), available at: http: // www.defense-aerospace.com/article-view/reports/38677/canada%E2%80%99s-national-security-policy-%282004%29.html (accessed 17/02/2020).

44. Strong, Secure, Engaged. Canada's Defense Policy (2017), Minister of National Defence, 113 p. available at: http:// dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf (accessed 11/02/2020).

45. The Multinational Information Operations Experiment (MNIOE) within the Multinational Experiment (MNE). Integration of a Multinational CD&E Project (2004), available at: https://www.act.nato.int/images/stories/events/2011/cde/rr_mnioe.pdf (accessed 20/02/2020).

46. Trudeau talks Russian cyberattacks with Five Eyes counterparts (2018), available at: https:// www.cbc.ca/news/politics/trudeau-five-eyes-russia-cyberattacks-1.4625386 (accessed 21/02/2020).