Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2022. – Т. 45. – С. 29-40
DOI: 10.31861/mhpi2022.45.29-40

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2022. – Volume. 45. – pp. 29-40
DOI: 10.31861/mhpi2022.45.29-40

УДК 351.86:004](71)

© Іванна Макух-Федоркова [1]

Нормативно-правові основи формування політики кібербезпеки Канади

У статті досліджується питання нормативно-правового регулювання політики кібербезпеки Канади, а також подається оцінка основним етапам формування кібернетичного законодавства. Характеризуються програмні документи, спрямовані на удосконалення кібербезпеки Канади та опрацьовані директиви, які позитивно впливають на розвиток системи національної безпеки. Наголошується на прийнятті двох Національних стратегій кібербезпеки та показано важливість інших законодавчих ініціатив щодо захисту цілісності урядових систем, національних критичних активів, методів і форм боротьби з кіберзлочинами та механізмів захисту канадців при щоденному використанні ними інформаційного простору.

Зосереджується увага на міжнародній інтеграції Канади в сфері кібербезпеки та співпраці в плані захисту національного простору з країнами-партнерами в сучасних умовах. Авторка прийшла до висновку, що канадська законодавча та виконавча влада швидко реагує на інформаційні виклики та створює гнучке правове законодавство, яке націлена на попередження загроз в майбутньому. Адже Канада однією з найперших почала розробляти нормативно-правову базу для забезпечення кібербезпеки, постійно удосконалює законодавчі ініціативи та виділяє фінансові ресурси. Позитивним досвідом є те, що канадська держава у реалізації національної безпеки поєднує взаємодію державного і приватного секторів. Ця спільна співпраця проявляється у забезпеченні взаємного обміну своєчасною інформацією щодо кіберзагроз, відпрацьовуються методи захисту та інші передові практики.

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

Regulatory Framework for Canada's Cybersecurity Policy

The article examines the issue of regulatory regulation of cybersecurity policy in Canada, and also considers an assessment of the main stages of cyber law formation. It describes policy documents that aim to improve Canada's cybersecurity and develop directives that have a positive impact on the development of the national security system. It emphasizes the adoption of two National Cyber Security Strategies and highlights the importance of other legislative initiatives to protect the integrity of government systems, national critical assets, methods and forms of combating cybercrime and protecting Canadians in their daily use of information space.

The focus is on Canada's international integration in the field of cybersecurity and cooperation in the field of national space protection with partner countries in modern conditions. The author concludes that the Canadian legislature and executive are responding quickly to information challenges and creating flexible legal legislation aimed at preventing future threats. After all, Canada was one of the first to develop a regulatory framework for cybersecurity, constantly improving legislative initiatives and allocating financial resources.

Characterizing the specifics of the legal framework of Canadian cyber law, it should be noted that the authorities are making great efforts to change the law, modernize the powers of law enforcement agencies and ensure an order that prevents evasion of legal control over criminal activities online. The

[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.

Canadian criteria for computer systems security are the basic standards of information security and are highly recognized by the international community.

Internationally, Canada's cybersecurity is developed through the Five Eyes Alliance and is closely linked to US, UK, Australian and New Zealand policy priorities, providing access to intelligence from around the world and providing a high level of protection against cyber security. attacks. Canada has one of the world's best institutional systems for information policy, including the creation of a single information space, the functioning of e-government, free access to information, government regulation of the media, and most importantly clear regulation of all information relations and processes

The positive experience is that the Canadian state has a long history of cooperation between the public and private sectors in the field of economic and national security. This joint cooperation is ensured through the mutual exchange of accurate and timely information on cyber threats, protection methods and other best practices.

Keywords: cybersecurity, cyber threats, cyberspace, cybercrime, information security, Canadian national interests, national security, computer systems, critical infrastructure.

Постановка проблеми. Розвиток інформаційних технології та штучного інтелекту призвели до виникнення загроз в кіберпросторі, адже сучасний технологічний рівень породжує нові виклики, відповідно, підштовхує провідні країни світу до посилення політики безпеки. Використання цифрових технологій в різних сферах діяльності сприяє поширенню кіберзлочинності, яка негативно впливає на систему державного управління, завдає шкоди сферам життєдіяльності країни та зменшує довіру до державної системи управління в цілому. Саме ці нові інформаційні виклики несуть загрозу суверенітету та територіальній цілісності, адже кіберзлочинність посилює суперечності між державами. З метою реалізувати свої геополітичні інтереси, світові центри впливу ведуть активну боротьбу за поділ кіберпростору. Як зазначено в проєкті Стратегії кібербезпеки України (2021-2025), «кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, які управляють такими об'єктами»[2]. В умовах сучасних гібридних та військових загроз, які виникли перед Україною надзвичайно важливим є вивчення та аналіз досвіду Канади в сфері забезпечення політики національної безпеки. Адже канадська держава стала першою країною у світі, яка визнала важливість медіаосвіти та зробила її обов'язковою шкільною дисципліною. Це дає змогу сформувати необхідні знання та навички у боротьбі з дезінформацією і маніпуляцією, розрізняти достовірну інформацію від фейкової, а також захищати як особистий, так і суспільний кіберпростір. Сформований рівень медіа освіти розширився до кіберграмотності та усвідомленості, що сприяє тісній взаємодії між громадянами та правоохоронними органами. Досвід формування нормативно-правової бази канадської політики в сфері кібербезпеки дає змогу оцінити рівень українського законодавства та вжити необхідних заходів щодо удосконалення безпекових питань з метою нейтралізації сучасних інформаційних загроз та викликів.

Аналіз останніх досліджень та публікацій. Аналізуючи нормативно-правову базу формування політики кібербезпеки Канади, варто виділити дві Національних стратегії кібербезпеки Канади: Стратегію кібербезпеки Канади (2010-2015)[3] та Національний план дій з кібербезпеки (2019-2024)[4]. Вказані документи є надзвичайно важливі, адже в них розкривається чіткий опис тактичних та стратегічних пріоритетів і завдань у сфері кіберзахисту. Також канадським уря-

[2] Проєкт Стратегії кібербезпеки України (2021-2025). Безпечний кіберпростір – запорука успішного розвитку країни. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (accessed: 13.02.2022).

[3] Action Plan 2010-2015 for Canada's Cyber Security Strategy. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf (accessed: 13.02.2022).

[4] National Cyber Security Action Plan (2019-2024) URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf (accessed: 13.02.2022).

дом було прийнято низку Законів, що регулюють питання, пов'язані з кібербезпекою: Закон «Про боротьбу зі спамом» (Anti-Spam Act)[5], Постанова «Про безпеку електронних підписів» (Secure Electronic Signature Regulations)[6], Постанова «Про захист електронної комерції» (Electronic Commerce Protection Regulations)[7], Закон «Про електронні документи за захист персональних даних» (Personal Information Protection and Electronic Documents Act)[8]. Ці документи та офіційна інформація із сайтів урядових структур, склали основу для аналізу та висновків з питань правового регулювання політики кібернетичної безпеки в Канаді. Проблематиці відносин Канади і США у сфері безпекової політики присвячена наукова стаття українського дослідника Артемчука Д.В.[9], а особливостям і методам забезпечення інформаційної безпеки на прикладі Канади, дослідження кандидата наук з державного управління Національного університету цивільного захисту України, Грабара Н.С.[10]. Серед зарубіжних дослідників, головні напрями співпраці у сфері кібербезпеки між США і Канадою охарактеризувала Луї С.[11].

В даній статті ставимо собі за **мету** проаналізувати нормативно-правові основи законодавства Канади в сфері кібернетичної політики та оцінити його можливості протидіяти сучасним інформаційним викликам. Відповідно до поставленої мети було сформульовано такі **завдання:** проаналізувати міжнародні аспекти співробітництва Канади в сфері кіберзахисту; оцінити специфіку канадського кібернетичного законодавства; розкрити основні напрями формування Національної стратегії кібербезпеки Канади.

Виклад основного матеріалу дослідження. На сучасному етапі не виникає жодних сумнівів наскільки сильно інформаційні технології інтегрувалися у наше повсякденне життя, бо суспільство перейшло у цифровий формат. І хоча кіберпростір приносить значні переваги, постійна залежність від нього створює нові загрози та вразливі моменти. Аналізуючи нормативно-правову базу, варто звернути увагу на те, що Канада є світовим лідером у політиці захисту інформаційного простору, законодавство вирізняється своєю гнучкістю, чітким контролем за дотриманням усіх норм і правил, а також покаранням порушників. Досвід цієї країни є показовим прикладом комплексного підходу до розробки основних питань правового та організаційного регулювання у сфері кіберзахисту.

В Канаді ще з 1946 р. створено Центр безпеки комунікацій (Communications Security Establishment, CSEC)[12] – спецслужба Канади, яка є підрозділом Міністерства національної оборони зі штаб-квартирою в Оттаві. Цей орган відповідає за зовнішню радіоелектронну розвідку, захист урядових електронних інформаційних і комунікаційних мереж, криптографію. На початку 2008 р. у відповідності з федеральною програмою ідентичності уряду Канади, федеральні відомства країни у своїй назві додали слово «Канада», Центр безпеки комунікацій отримав назву Центр безпеки комунікацій Канади (Communications Security Establishment Canada). CSEC займає унікальне місце в канадському розвідувальному співтоваристві, проводить роботу у сфері шифрування та крипто аналізу, забезпечує інформаційну безпеку структур уряду Канади та здійснює радіоелектронну розвідку. Також забезпечує технічну і оперативну допомогу Королівській канадській кінній поліції та іншим федеральним правоохоронним органам і силовим

[5] 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 15/02/2022).

[6] 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 19/02/2022).

[7] 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 15/02/2022).

[8] 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 6/02/2022).

[9] Артемчук, Д. (2020). Співробітництво США та Канади в сфері безпеки і оборони на сучасному етапі. *Наукові записки студентів та аспірантів,* с. 278-287. URL: https://eprints.oa.edu.ua/8291/1/32.pdf (дата перегляду: 1.03.2022).

[10] Грабар, Н. Формування культури кібербезпеки в суспільстві – актуальне завдання сучасності. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12389/1/stGrabar1.pdf (дата перегляду: 1.03.2022).

[11] Louie, C. (2017). U.S.-Canada Cybersecurity Cooperation. URL: https:// jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/(accessed: 16.02.2022).

[12] Communications Security Establishment URL: https://www.cse-cst.gc.ca/en (accessed: 16.02.2022).

структурам, в тому числі Канадській береговій охороні і Канадській адміністрації безпеки повітряного транспорту.

Для запобігання викраденню іншими державами секретної інформації, діяльності організованої злочинності та терористичних груп у кіберпросторі, Центр безпеки комунікацій постійно обмінюється розвідданими з Агентством національної безпеки США, а також державами-членами альянсу «Five Eyes»[13]. Забезпечення кіберпростору Канаду є спільною роботою таких країн-партнерів: США, Великої Британії Австралії та Нової Зеландії. Зазначені країни входять до альянсу «Five Eyes» і проводять колективну радіотехнічну розвідувальну діяльність. Рівень американської кіберрозвідки є високим і це дозволяє іншим країнам отримати доступ до баз даних, проводити обмін розвідувальною інформацією в альянсі «Five Eyes» та запобігати кіберзлочинам на територіях своїх держав[14]. Слід наголосити, що на міжнародному рівні США і Канада мають доволі тісну історію співпраці в рамках альянсу «П'ять очей». Існує розрив у потенціалі між Сполученими Штатами – основним, технологічно розвиненим, добре забезпеченим партнером – та іншими партнерами альянсу «П'ять очей»[15]. Оскільки Канада має більш обмежені можливості для розробки складних технологій, вона більше використовує можливості Агенства національної безпеки (NSA) та Центральної служби безпеки (Central Security Service), щоб допомогти керувати своєю частиною місії партнерства. Для виконання своєї місії в альянсі «П'ять очей» – захисту урядових систем в кіберпросторі і надання розвідданих для підтримки прийняття урядових рішень, Канада частково покладається на американські можливості і, зокрема, на американську розвідку. Це означає, що Сполучені Штати, у свою чергу, можуть впливати на пріоритети канадської розвідки. В цьому відношенні Канада, звичайно, знаходиться в більш залежному становищі. Таким чином, уряд Канади має постійно стежити як за ефективністю спільної мережі кібербезпеки зі Сполученими Штатами, так і за суверенними канадськими параметрами безпеки та конфіденційності. Партнерство Канади із Сполученими Штатами Америки є надзвичайно важливим також завдяки можливості використовувати Національне управління з аеронавтики і дослідження космічного простору (NASA), а саме новітні технології і персонал, програмне та системне забезпечення. Географічна близькість двох країн та сучасні виклики посилюють тісну співпрацю у посиленні захисту кіберпростору, що дає можливість ефективніше управляти інформацією як ключовою цінністю у підтриманні безпеки як американської, так і канадської громадськості.

Також, варто нагадати, що в 1948 р. Канада приєдналася до договору UKUS SIGINT, який передбачає співробітництво в сфері радіоелектронної розвідки. Співробітництво виникло на базі двосторонньої угоди після Другої світової війни і сьогодні включає, поряд з Великою Британією і США, також Австралію, Канаду і Нову Зеландію. В роботі альянсу беруть участь Німеччина, Японія, Республіка Корея, Туреччина і Норвегія, а в останні роки і країни-учасники НАТО[16]. Одним з найбільш відомих проектів, який реалізовувався під егідою UKUSA є створення і експлуатація глобального комплексу радіоелектронної розвідки «Ешелон». Можливості цієї системи включають в себе контроль світових електронних комунікацій (телефон, факс та Інтернет-трафік). Кожен із учасників UKUSA несе відповідальність за збір та аналіз інформації у різних регіонах світу. Так, зоною відповідальності Австралії є регіон Індокитаю, Індонезія, південні та центральні регіони Китаю, зона роботи Канади – Південна та Центральна Америка та північне узбережжя Росії, Нова Зеландія несе відповідальність за Західну та Південну частини Тихоокеанського регіону, Велика Британія – за країни Європи (включаючи європейську частина Росії) та країни Африки, США – за країни Латинської Америки, азіатську частину Росії та північ Китаю.

---

[13] Five Eyes Intelligence Oversight and Review Council (FIORC) URL: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc (accessed: 16.02.2022).

[14] Артемчук, Д. (2020). Співробітництво США та Канади в сфері безпеки і оборони на сучасному етапі. *Наукові записки студентів та аспірантів,* С. 278-287. URL: https://eprints.oa.edu.ua/8291/1/32.pdf (дата перегляду: 1.03.2022)

[15] Макух-Федоркова, І. (2020). Сучасні інформаційні виклики та формування кібернетичної стратегії Канади . *Історико-політичні проблеми сучасного світу*, (41), с. 29-45. https://doi.org/10.31861/mhpi2020.41.

[16] National Security Agency/Central Security Service URL: https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/ (accessed: 16.02.2022).

Безпечний і захищений кіберпростір надзвичайно важливий для безпеки, стабільності та процвітання Канади, а надійна система кібербезпеки має вирішальне значення для конкурентоспроможності, економічної стабільності та довгострокового процвітання Канади. В даному контексті варто наголосити, що значну роботу в цьому напрямі здійснює канадський кіберцентр CCCS (Canadian Centre Cyber Security, 2005)[17], який є частиною Центру безпеки спецслужби Канади і відповідає за зовнішню радіоелектронну розвідку, захист урядових мереж і криптографію. Кіберцентр є єдиним уніфікованим джерелом експертних порад, рекомендацій, послуг та підтримки з питань кібербезпеки для уряду, власників та операцій критичної інфраструктури, приватного сектора та канадської громадськості. Завдяки Кібер-центру канадці мають чітке та надійне місце, куди можна звернутися з питань кібербезпеки. Діяльність центру є відкритою і спрямована на підтримку уряду та приватного сектору. Захист кіберсистем уряду Канади та реакція на значні загрози та інциденти є важливою в сучасних умовах. Дана установа виступає в якості національного координаційного центру по кібербезпеці сім днів на тиждень: координує і підтримує зусилля по реагуванню на інциденти; займається моніторингом та аналізом кібер загроз навколишнього середовища; надає технічні консультації по IT- безпеці; створює національний потенціал (стандартів, практик, інформування, співпраця з закладами освіти та науковими школами)

Інформуванням громадськості займається національна інформаційна кампанію Get Cyber Safe, яка покликана допомогти канадцям краще зрозуміти кібербезпеку та допомагає захистити їх права в Інтернеті. Забезпечення безпеки в кіберпросторі залежить не тільки від державного регулювання і контролю, а в багатьох випадках залежить від поведінки учасників правовідносин, адже повсякчасна взаємодія державного регулятора з пересічними користувачами, підприємцями, організаціями, миттєвий відгук на їх проблеми чи підозри, складає основу безпеки канадського кіберпростору. Вагомий вклад в сферу безпеки внесла медіа-освіта громадян. Канада – найперша в світі країна, що визнала необхідність медіаграмотності (ще в 60-х рр. XX ст.). У 1978 році, з появою Асоціації медіаграмотності (AML), медіаосвіта почала бурхливо розвиватися. Якщо наприкінці XX століття громадянам достатньо було знаходити, аналізувати та систематизувати інформацію, то на початку XXI ст. цих навичок стало замало. З розвитком ІКТ медіаосвіта в Канаді стає обов'язковою. Це надзвичайно потужна галузь, яка охоплює не тільки школярів, а й готує спеціалістів в цій галузі, допомагає всім бажаючим навчитися не тільки аналізувати інформацію чи відкидати фейки, а й протидіяти прямим і непрямим впливам чи інформаційним операціям. Медіаосвіта, застосована з раннього віку, разом з заохоченням креативної діяльності дитини, розвиток критичного мислення, а також кібер-грамотність і вміння комунікувати, прищеплені з юності, зробили канадське суспільство досить стійким до сучасних кіберзагроз. Це підтверджує, що Канада обрала правильний шлях: використовувати ресурси задля освіти і грамотності громадян, замість витрачати ті ж ресурси на спростування дезінформації[18].

У зв'язку з поширенням коронавірусу Канада стала жертвою кібернетичних та інформаційних атак. Починаючи від звичайної дезінформації щодо COVID-19 закінчуючи витоком даних. Згідно з новим опитуванням, більше чверті Канадських IT-працівників заявили, що їх організація зазнала кібератаки на тему COVID-19. У «Звіті про кібербезпеку 2020 року», опублікованому Канадським органом реєстрації Інтернету («CIRA»), було опитано понад 500 канадців, які приймають рішення в сфері IT-безпеки. Вони наголосили, що серед кіберзагроз, зафіксованих в ході опитування, були підроблені програми для відстеження контактів і фішингові атаки, які використовували результати тестів на COVID-19. Приблизно три з десяти організацій повідомили про різке зростання числа нападів, яким вони піддалися з початку пандемії. Трохи більше половини заявили, що вони впровадили нові заходи захисту кібербезпеки у відповідь на зміни, викликані спалахом нового коронавірусу[19]. Для того, щоб вберегти громадян від неправдивої інформації, Канадська дослідницька кафедра в галузі медичного права та страхування запусти-

[17] Canadian Centre for Cyber Security. URL: https://cyber.gc.ca/en/about-cyber-centre (accessed: 16.02.2022).

[18] Макух-Федоркова, І.І. (2011) Канадська модель впровадження медіаосвіти в контексті сучасної освітньої політики *Аналітика. Прогнози. Інформаційний менеджмент.* Чернівецький національний університет, Чернівці Вип. 1. С. 113-133. Режим доступу: http://nbuv.gov.ua/UJRN/mfapim_2011_1_9.

[19] Coble, S. (2020) Canada bombarded with COVID-19-themed Cyber attacks *Infosecurity group* URL: https://www.infosecurity-magazine.com/news/canada-bombarded-with-covid19/ (accessed: 16.02.2022).

ла проект #ScienceUpFirst в якому закликає науковців, експертів в галузі охорони здоров'я та звичайних громадян об'єднатися проти дезінформації щодо COVID-19. Основною метою цього проекту є позначення фейкової інформації про вірус та заперечення неправдивих міфів про розповсюдження коронавірусу. Хештег #ScienceUpFirst або франкомовний #LaScienceD'abord запускається в усіх популярних соцмережах: Instagram, Facebook, Twitter та, навіть, TikTok[20]. Під час глобальної пандемії COVID-19 в Інтернеті зросла кількість дезінформації, переважна більшість якої надходила із Росії та Китаю. Близько половини усіх повідомлень у мережі Twitter стосовно скасування карантинних обмежень поширювалися ботами та дублювалася російськими та китайськими меседжами[21].

У зв'язку із загрозами з боку РФ, у січні 2022 р. Канадський центр кібербезпеки (CCCS) звернувся до операторів комп'ютерних мереж, які підтримують функціонування критично важливої інфраструктури із закликом посилити захист проти можливих кіберзагроз. Саме це попередження було оприлюднено на тлі напруження, що наростало між Заходом і РФ навколо України. Адже у ніч на 14 січня 2022 р. на Україну була здійснена серйозна кібератака, внаслідок якої з ладу вийшли близько 70 урядових та регіональних сайтів[22]. Як зазначалося вище, Кіберцентр (CCCS) активно контролює і реагує на усі кібератаки, ефективно координує національні заходи у відповідь на загрози кібербезпеці, тому значення цієї структури має неабияке значення як національного координаційного центру по кібербезпеці в Канаді.

Слід зазначити, що в багатьох провідних країнах світу вже сформовані і діють загальнодержавні системи кібернетичної безпеки критичної інфраструктури, такі оптимальні організаційні структури, які здатні в короткий проміжок часу швидко акумулювати сили та засоби різних державних і правоохоронних органів, установ приватного сектора для протидії кіберзагрозам, кібератакам, кіберзлочинам, кібершпигунству, кібертероризму. В США, Великій Британії, Канаді довгий час діють потужні кіберполіцейські структури (NIPS, FBI, FATF і тощо). Сьогодні в Сполучених Штатах Америки, Польщі та інших країнах світу створюються навіть кібервійська.

Характеризуючи специфіку нормативно-правових основ канадського кібернетичного законодавства, варто звергнути увагу на те, що влада докладає великих зусиль до зміни законодавства, модернізації повноважень правоохоронних органів та забезпечення такого порядку, який унеможливлює ухиляння від законодавчого контролю над злочинними діями у мережі.

Нормативний документ, який становить правову основу забезпечення кібербезпеки Канади є Закон «Про електронні документи та захист персональних даних» (Personal Information Protection and Electronic Documents Act, 2000 PIPEDA)[23]. Цей Федеральний закон застосовується до захисту конфіденційної інформації, встановлює, як організації приватного сектору економіки збирають, використовують і розкривають особисту інформацію в ході комерційних операцій. Крім того, він містить різні положення, які регламентують використання електронних документів. Метою документу було підвищити довіру споживачів до електронної комерції, а також переконати Європейський Союз в тому, що канадське законодавство є прийнятним для захисту особистої інформації громадян Європейського союзу. У відповідності з розділом 29 Закону, частина 1 («Захист особистої інформації в приватному секторі») повинна переглядатися Парламентом кожних п'ять років. Перший парламентський перегляд відбувся у 2007 р. Існують певні виключення при яких інформація може збиратися, використовуватися і розкриватися без згоди її власника. Наприклад, загроза національної безпеки, міжнародні справи або надзвичайні ситуації. Варто зазначити, що Закон виконувався в три етапи: з 2001 року був застосований до галузей економіки, що контролювалися федеральним управлінням (наприклад, авіакомпанії, банки, телерадіомовлення). У 2002 році Закон був розширений і охопив систему охорони здоров'я, а

[20] Stea, J. (2021) How canadians can use social media to help debunk COVID-19 misinformation. *The Conversation,* URL: https://theconversation.com/how-canadians-can-use-social-media-to-help-debunk-covid-19-misinformation-155653 (accessed: 16.02.2022).

[21] Burt, T. Cyberattacks targeting health care must stop URL: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/.

[22] Центр кібербезпеки Канади попередив про кібератаки підконтрольних РФ хакерів (2022). URL: https://aspi.com.ua/news/tekhnologii/centr-kiberbezpeki-kanadi-popered iv-pro-kiberataki-pidkontrolnikh-rf-khakeriv#gsc.tab=0 (дата перегляду: 1.03.2022).

[23] Personal Information Protection and Electronic Documents Act (S.C.2000, c. 5) URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html (accessed: 16.02.2022).

вже з 2004 р. будь-яка організація, яка збирала особисту інформацію в процесі комерційної діяльності підпадала під дію згаданого нормативного документа. Щоправда,з жовтня 2018 р. сім канадських провінцій користується подібними законами захисту даних, адже відомо, що канадське законодавство регулюється на провінційному рівні. Більше того, згідно з принципом децентралізації, кожна провінція Канади приймає та виконує власний закон, що відрізняється від стратегії тим, що враховує місцеві особливості регулювання та організації кібербезпеки, також вже чинні на цій території правові норми. Це дозволяє уникати дублювання функцій та надмірної бюрократизації в інфосфері.

Також, у лютому 2005 року вступив в дію Закон «Про безпеку електронних підписів» (Secure Electronic Signature Regulations)[24]. В його основі закладені наступні гарантії: унікальність для кожної людини і особистий контроль; використовується для ідентифікації особи; пов'язаний з електронними документами особи таким чином, щоб з їх допомогою можна було визначити чи були вони змінені з того часу, як був поставлений підпис. 7 березня 2012 року набув чинності Закон «Про захист електронної комерції»[25]. Його метою є «сприяння ефективності та адаптивності канадської економіки шляхом регулювання комерційної поведінки, яка перешкоджає використанню електронних засобів для здійснення комерційної діяльності», оскільки така поведінка: погіршує доступність, надійність, ефективність і оптимальне використання електронних засобів для здійснення комерційної діяльності; накладає додаткові витрати на підприємства і споживачів; ставить під загрозу конфіденційність та безпеку конфіденційної інформації; підриває довіру канадців до використання електронних засобів зв'язку для здійснення своєї комерційної діяльності в Канаді та за кордоном[26].

Варто звернути увагу також на розроблені стандарти з безпеки, в так званому Аудиті кібербезпеки Канади (ISO 27032 і ISO 27701)[27], який містить рекомендації щодо подолання поширених ризиків кібербезпеки, включаючи безпеку кінцевої точки користувача, безпеку мережі та захист критичної інфраструктури. Справді, ISO 27032 і ISO 27701 використовується всіма підприємцями, бо ризик загроз безпеці зростає щодня, а цей документ гарантує захист та довгострокову стійкість бізнес-процесів. Переваги ISO 27032 полягають у наступному: захищає дані та конфіденційність організацій від кіберзагроз; посилює створення та підтримку програм кібербезпеки; розробляє найкращі методи керування політикою кібербезпеки; покращує систему безпеки організацій та її безперервність; формує довіру зацікавлених сторін щодо необхідності заходів безпеки; реагує та швидко відновлюється в разі інциденту. У свою чергу, ISO 27701 визначає вимоги до PIMS (системи управління конфіденційною інформацією) на основі вимог ISO 27001 (ISMS), володіє розширеним набором вимог щодо конфіденційності, цілей та засобів контролю, а також застосовується до всіх типів і розмірів організацій, включаючи державні та приватні компанії, державні установи та неприбуткові організації. Більше того, саме ці розроблені канадські стандарти застосовується багатьма приватними організаціями по всьому світі.

З метою створення безпечного онлайн ринку та забезпечення гарантій споживачам і підприємствам від неправомірного використання цифрових технологій, включаючи спам та інші електронні загрози, 1 липня 2014 р. Канада прийняла Закон «Про боротьбу зі спамом» (Anti-Spam Act, CASL)[28]. Цей нормативний документ також спрямований не те, щоб допомогти бізнесу залишатися конкурентоспроможним на глобальному інформаційному ринку.

Правила CASL застосовуються до будь-якого «комерційного електронного повідомлення» («СЕМ»), надісланого або з канадського комп'ютера, або з будь-якого пристрою зареєстрованого в Канаді. Якщо особа перебуває в Канаді або надсилає комерційне електронне повідомлення (СЕМ) жителям Канади, то вона повинна дотримуватися правил CASL. Повідомлення, що передаються через канадські комп'ютерні системи не підлягають під дію цього Закону. Згідно

[24] Secure Electronic Signature Regulations SOR/2005-30 URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html (accessed: 16.02.2022).
[25] Electronic Commerce Protection Regulations (SOR/2013-221) URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-221/ (accessed: 16.02.2022).
[26] Там само.
[27] Cybersecurity Audit in Canada. URL: https://smg-aw.com/cybersecurity-audit-in-canada/ (accessed: 15.02.2022).
[28] Canada's anti-spam legislation. URL: https://fightspam.gc.ca/eic/site/030.nsf/eng/home/ (accessed: 15.02.2022).

CASL, CEM – це будь-яке повідомлення, яке: знаходиться в електронному форматі, включаючи електронну пошту, екстрені повідомлення, текстові повідомлення і деякі повідомлення в соціальних мережах; надсилається на електронну адресу, включаючи адреси електронної пошти, акаунти екстрених повідомлень, акаунти телефонні і в соціальних мережах; містить повідомлення, що закликає одержувачів взяти участь у будь-якому виді комерційної діяльності, включаючи просування товарів, послуг, людей/персонажів, компаній або організацій. Загалом, варто зазначити, що CASL забороняє компаніям: надсилати комерційні електронні повідомлення без особистої згоди, включаючи електронну пошту, соціальні мережі та текстові повідомлення; зміну даних передачі в електронному повідомленні таким чином, щоб повідомлення було відправлено в інше місце призначення без вашої згоди; установку програмного забезпечення на ваші електронні пристрої без вашої згоди; використання оманливих методів для просування товарів або послуг в Інтернеті; збір особистої інформації шляхом несанкціонованого доступу до комп'ютерної системи або електронного пристрою; збір даних електронної пошти або її використання без дозволу. Варто наголосити, що згідно CASL наслідки для спамерів включають штрафи у розмірі 1 млн. доларів за порушення прав фізичних осіб та 10 млн. доларів за порушення прав компаній[29].

Канадський федеральний уряд підвищує стійкість державних систем, розвиває державно-приватне партнерство для забезпечення безпеки критичної інфраструктури, ділиться інформацією про кібербезпеку з громадськістю та розширює повноваження поліції. Королівська канадська кінна поліція (*RCMP*) виконує провідну правоохоронну функції держави, а саме: забезпечує боротьбу зі злочинністю, сприяє запобіганню та припиненню правопорушень[30]. Також завданнями Канадської королівської кінної поліції є: зміцнення потенціалу по боротьбі зі злочинною діяльністю, пов'язаною з кіберзлочинністю; посилення спеціалізованого кібернетичного потенціалу федеральних слідчих груп і розширення можливостей реагування на спільні розслідування з міжнародними партнерами по правоохоронних органах; виявлення, запобігання та реагування на загрози безпеці канадських громадян[31].

Розслідування кіберзлочинів є складним і технічним завданням, тому функцією канадської поліції є боротьба з такими інцидентами. Окрім, що в Канаді прийнято дві Стратегії кібербезпеки Канади, королівською канадською кінною поліцією запроваджено свою *Стратегію RCMP щодо кіберзлочинності, яка спрямована на* зменшення загрози, вплив кіберзлочинності в Канаді через дії правоохоронних органів. У стратегії визначено такі три напрями, які керують зусиллями RCMP у боротьбі з кіберзлочинністю: виявлення та визначення пріоритетності загроз кіберзлочинності шляхом збору та аналізу розвідувальних даних; переслідувати кіберзлочинність шляхом цілеспрямованих правоохоронних та слідчих дій; підтримувати розслідування кіберзлочинів за допомогою спеціальних навичок, інструментів та навчання[32]. Більше того, королівською канадською кінною поліцією було створено Національну групу кіберзлочинності (NC3), до якої входять офіцери RCMP та цивільні особи різного походження. Вони активно співпрацюють з правоохоронними органами та іншими партнерами задля зменшення загроз та впливу кіберзлочинності в Канаді. Основними завданнями NC3 є: координування канадських операцій по боротьбі з кіберзлочинністю та співпраця з міжнародними партнерами; надання консультацій та рекомендацій щодо цифрових розслідувань канадській поліції; підготовка дієвої інформації про кіберзлочинність для канадської поліції; співпраця з Канадським центром кібербезпеки; створення національного механізму публічної звітності для канадців і підприємств щодо кіберзлочинів і шахрайства.

[29] About the Canada Anti-Spam Law (CASL) URL: https://mailchimp.com/help/about-the-canada-anti-spam-law-casl/ (accessed 15.02.2020).

[30] 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: 05.02.2022).

[31] National Cyber Security Action Plan 2019-2024– URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx (accessed: 13.02.2022).

[32] Royal Canadian Mounted Police Cybercrime Strategy (2015) URL: https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496 pdf (accessed 16.02.2022).

Канада має добре розроблену нормативно-правову базу у забезпеченні кібернетичної безпеки та визначені стратегічні напрями розвитку кіберпростору, адже пріоритетом країни є безпека громадян та захист демократичних інституцій. Канадський уряд докладає максимальних зусиль для підтримки високого рівня безпеки у всіх інстанціях. Ще 3 жовтня 2010 року було прийнято Стратегію кібербезпеки Канади (2010-2015)[33], яка ґрунтувалася на трьох основних принципах: захист урядових систем; співробітництво з метою захисту ключових інформаційних та телекомунікаційних систем, що знаходяться поза веденням федерального уряду. Уряд сприяє формуванню довіри канадців до державних інформаційних систем при роботі з особистою інформацією чи наданні електронних послуг громадянам, гарантування безпеки канадських громадян в онлайн-середовищі. Перший принцип передбачає встановлення чітких ролей та відповідальності, посилення безпеки інформаційних та телекомунікаційних систем федерального рівня та підвищення поінформованості уряду в галузі кібербезпеки. Захист канадського суверенітету, забезпечення кіберзахисту національної безпеки і економічних інтересів, а також виділення коштів і необхідного персоналу для виконання усіх необхідних зобов'язань з кібербезпеки[34].

Другий принцип передбачає захист важливих кіберсистем за межами держави. Для цього встановлюються партнерські проекти державного рівня із залученням приватного сектору, урядів провінцій і територій щодо зміцнення важливих секторів критичної інфраструктури. Канадські спеціалісти постійно працюють над виявленням і ліквідацією кіберзагроз, прогнозують та вносять пропозиції щодо раціонального використання кіберпростору в національних інтересах Канади. Взаємодія державного і приватного секторів в реалізації економічної і національної безпеки забезпечується за рахунок постійного обміну інформацією щодо можливих кіберзагроз.

І нарешті, третій – це боротьба з кіберзлочинністю та захист канадських громадян в онлайн-середовищі. В цьому аспекті також зачіпалася проблема захисту персональних даних. Більше того, задля втілення політики національної безпеки, Канада почала розробляти Національну стратегію кібербезпеки, яку оновлюється кожних п'ять років. Постійно підтримує міжнародне партнерство в реалізації глобального режиму управління кібербезпекою та сприяє посиленню потенціалу кібербезпеки спільно із зарубіжними партнерами у менш розвинених країнах.

Варто зазначити, що Національний план дій з кібербезпеки (2019-2024) передбачає спільну відповідальність та тісну співпрацю з різними рівнями влади, приватним сектором міжнародними партнерами та громадянами Канади. В документі зазначається, щоб збудувати безпечне цифрове середовище необхідно втілювати збалансовані заходи, постійно пристосовуватися до змін безпекової політики та формувати нові можливості для цифровізації усіх сфер суспільного життя[35]. Також міститься план дій щодо підтримки канадських власників та операторів критичної інфраструктури, подається комплексна оцінка загроз, а також зазначається про підготовку звітів уряду Канади у зв'язку з досягненням в сфері квантових технологій. Крім того, визначаються завдання Федеральній поліції та Національному координаційному підрозділу у боротьбі із кіберзлочинністю.

Стратегія кібербезпеки Канади не містить чіткого визначення, що таке кібербезпека, проте в самому документі зазначається, що основна шкода від кібератак несе збиток системі життєдіяльності всієї країни, бізнесу, окремому громадянину. Забезпечення ефективної діяльності уряду є питанням національної безпеки, суверенітету та захисту суспільства, а ключовим органом, на який покладена координація та контроль за реалізацією державної політики у протидії кіберзагрозам покладено на Міністерство громадської безпеки Канади (Public Safety Canada).

Висновки Кіберзагрози є серйозною проблемою на сучасному етапі, адже масштабність їх впливу негативно відображується на діяльності органів державного апарату та усіх сферах суспільного життя. Канадська законодавча та виконавча влада швидко реагує на виклики сучасності і створює гнучку нормативно-правову базу (кожна провінція подає свої пропозиції і вносить власні поправки), яка націлена на попередження загроз в майбутньому. Країна однією з найперших почала розробляти нормативно-правову базу для регулювання кіберпростору

[33] Action Plan 2010-2015 for Canada's Cyber Security Strategy. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf (accessed: 13.02.2022).

[34] Грабар Н. Формування культури кібербезпеки в суспільстві – актуальне завдання сучасності. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12389/1/stGrabar1.pdf (дата перегляду: 1.03.2022).

[35] National Cyber Security Action Plan (2019-2024) URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf (accessed: 13.02.2022).

(з 2000-их років). Її законодавча база постійно оновлюється, розширюється та доповнюється. Забезпечення кібербезпеки в Канаді ґрунтується на комплексному узгодженні дій усіх суб'єктів державно-приватної взаємодії у співпраці з громадянським суспільством у сфері кібербезпеки. Успішно реалізовуються науково-дослідні проєкти спрямовані на прогнозування і виявлення кіберзагроз та реалізовуються принципи міжнародного права щодо агресивних дій у кіберпросторі. Діяльність Кіберцентру спрямована на забезпечення надання консультативних послуг та постійна координація заходів у відповідь на будь-які загрози кібербезпеці Канади. Також уряд цілеспрямовано підтримує цілісну систему управління, яка включає програми захисту критичної інфраструктури, інформаційну безпеку, обмін інформацією між федеральними міністерствами та відомствами, угоди з міжнародними партнерами і захист приватного сектору інформації. Враховуючи сучасні інформаційні виклики та загрози, держава в Канаді – головний суб'єкт управління усіма інформаційними потоками, які використовують різні прийоми і механізми регулювання. Стратегії кібербезпеки Канади дозволяють захистити цілісність урядових систем та об'єктів критичних інфраструктур, ефективно контролюється кіберпростір та вживаються заходи боротьби з кіберзлочинцями.

Канадські критерії безпеки комп'ютерних систем є базовими стандартами інформаційної безпеки і на високому рівні визнаються міжнародним співтовариством. У міжнародному плані розвиток кібербезпеки Канади відбувається через альянс «П'ять очей» і тісно пов'язаний з пріоритетними напрямами політики США, Великої Британії Австралії та Нової Зеландії, що дає можливість забезпечувати доступ до розвідувальних даних з усього світу та забезпечує високий рівень захисту від кібернетичних атак. Канада володіє однією з найкращих у світі інституційних систем забезпечення інформаційної політики, включаючи створення єдиного інформаційного простору, функціонування електронного урядування, вільного доступу до інформації, державне регулювання діяльності ЗМІ, а головне чітке нормативне регулювання усіх інформаційних відносин і процесів.

Список джерел

1. Артемчук, Д. (2020). Співробітництво США та Канади в сфері безпеки і оборони на сучасному етапі. *Наукові записки студентів та аспірантів,* с. 278-287. URL: https://eprints.oa.edu.ua/8291/1/32.pdf (дата перегляду: 1.03.2022).
2. Варунц, Л. (2017) Роль Королівської канадської кінної поліції в реалізації правоохоронної функції держави URL: 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).
3. Грабар Н. Формування культури кібербезпеки в суспільстві – актуальне завдання сучасності. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12389/1/stGrabar1.pdf (дата перегляду: 1.03.2022).
4. Макух-Федоркова, І. (2011) Канадська модель впровадження медіаосвіти в контексті сучасної освітньої політики *Аналітика. Прогнози. Інформаційний менеджмент*. Чернівецький національний університет, Чернівці Вип. 1. С. 113-133. URL: http://nbuv.gov.ua/UJRN/mfapim_2011_1_9.
5. Макух-Федоркова, І. (2020). Сучасні інформаційні виклики та формування кібернетичної стратегії Канади. *Історико-політичні проблеми сучасного світу*, (41), с. 29-45. https://doi.org/10.31861/mhpi2020.41.
6. Проєкт Стратегії кібербезпеки України (2021-2025). Безпечний кіберпростір – запорука успішного розвитку країни. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата перегляду: 13.02.2022).
7. Центр кібербезпеки Канади попередив про кібератаки підконтрольних РФ хакерів (2022). URL: https://aspi.com.ua/news/tekhnologii/centr-kiberbezpeki-kanadi-poperediv-pro-kiberataki-pidkontrolnikh-rf-khakeriv#gsc.tab=0 (дата перегляду: 1.03.2022).
8. Action Plan 2010-2015 for Canada's Cyber Security Strategy. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf (accessed: 13.02.2022).
9. About the Canada Anti-Spam Law (CASL) URL: https://mailchimp.com/help/about-the-canada-anti-spam-law-casl/ (accessed: 15.02.2022).

10. Burt, T. Cyberattacks targeting health care must stop. URL: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (accessed: 16.02.2022).
11. Canada's anti-spam legislation. URL: https://fightspam.gc.ca/eic/site/030.nsf/eng/home/ (accessed: 15.02.2022).
12. Canadian Centre for Cyber Security. URL: https://cyber.gc.ca/en/about-cyber-centre (accessed: 16.02.2022).
13. Coble, S. (2020) Canada bombarded with COVID-19-themed Cyber attacks *Infosecurity group* URL: https://www.infosecurity-magazine.com/news/canada-bombarded-with-covid19/ (accessed: 16.02.2022).
14. Communications Security Establishment URL: https://www.cse-cst.gc.ca/en (accessed: 16.02.2022).
15. Cybersecurity Audit in Canada. URL: https://smg-aw.com/cybersecurity-audit-in-canada/ (accessed: 15.02.2022).
16. Electronic Commerce Protection Regulations (SOR/2013-221) URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-221/ (accessed: 16.02.2022).
17. Five Eyes Intelligence Oversight and Review Council (FIORC) URL: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc (accessed: 16.02. 2022).
18. Louie, C. (2017) U.S.-Canada Cybersecurity Cooperation. URL: https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/(accessed: 16.02.2022).
19. National Security Agency/Central Security Service URL: https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/ (accessed: 16.02.2022)
20. National Cyber Security Action Plan (2019-2024) URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf (accessed: 13.02.2022).
21. Personal Information Protection and Electronic Documents Act (S.C.2000, c. 5) URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html (accessed: 16.02.2022).
22. Royal Canadian Mounted Police Cybercrime Strategy (2015) URL: https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496 pdf (accessed: 16.02.2022).
23. Secure Electronic Signature Regulations SOR/2005-30 URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html (accessed: 16.02.2022).
24. Stea, J. (2021) How canadians can use social media to help debunk COVID-19 misinformation. *The Conversation,* URL: https://theconversation.com/how-canadians-can-use-social-media-to-help-debunk-covid-19-misinformation-155653 (accessed: 16.02.2022).

References

1. Artemchuk, D. (2020). Spivrobitnytstvo SShA ta Kanady v sferi bezpeky i oborony na suchasnomu etapi. Naukovi zapysky studentiv ta aspirantiv, s. 278-287. URL: https://eprints.oa.edu.ua/8291/1/32.pdf (data perehliadu: 1.03.2022)
2. Varunts, L. (2017) Rol Korolivskoi kanadskoi kinnoi politsii v realizatsii pravookhoronnoi funktsii derzhavy URL: 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).
3. Hrabar N. Formuvannia kultury kiberbezpeky v suspilstvi – aktualne zavdannia suchasnosti. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12389/1/stGrabar1.pdf (data perehliadu: 1.03.2022).
4. Makukh-Fedorkova, I. (2011) Kanadska model vprovadzhennia mediaosvity v konteksti suchasnoi osvitnoi polityky Analityka. Prohnozy. Informatsiinyi menedzhment. Chernivetskyi natsionalnyi universytet, Chernivtsi Vyp. 1. C. 113-133. URL: http://nbuv.gov.ua/UJRN/mfapim_2011_1_9.
5. Makukh-Fedorkova, I. (2020). Suchasni informatsiini vyklyky ta formuvannia kibernetychnoi stratehii Kanady. Istoryko-politychni problemy suchasnoho svitu, (41), s. 29-45. https://doi.org/10.31861/mhpi2020.41.

6. Proiekt Stratehii kiberbezpeky Ukrainy (2021-2025). Bezpechnyi kiberprostir – zaporuka uspishnoho rozvytku krainy URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (data perehliadu: 13.02.2022).

7. Tsentr kiberbezpeky Kanady poperedyv pro kiberataky pidkontrolnykh RF khakeriv (2022). URL: https://aspi.com.ua/news/tekhnologii/centr-kiberbezpeki-kanadi-poperediv-pro-kiberataki-pidkontrolnikh-rf-khakeriv#gsc.tab=0 (data perehliadu: 1.03.2022).

8. Action Plan 2010-2015 for Canada's Cyber Security Strategy. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf (accessed: 13.02.2022).

9. About the Canada Anti-Spam Law (CASL) URL: https://mailchimp.com/help/about-the-canada-anti-spam-law-casl/ (accessed: 15.02.2022).

10. Burt, T. Cyberattacks targeting health care must stop. URL: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (accessed: 16.02.2022).

11. Canada's anti-spam legislation. URL: https://fightspam.gc.ca/eic/site/030.nsf/eng/home/ (accessed: 15.02.2022).

12. Canadian Centre for Cyber Security. URL: https://cyber.gc.ca/en/about-cyber-centre (accessed: 16.02.2022).

13. Coble, S. (2020) Canada bombarded with COVID-19-themed Cyber attacks *Infosecurity group* URL: https://www.infosecurity-magazine.com/news/canada-bombarded-with-covid19/ (accessed: 16.02.2022).

14. Communications Security Establishment URL: https://www.cse-cst.gc.ca/en (accessed: 16.02.2022).

15. Cybersecurity Audit in Canada. URL: https://smg-aw.com/cybersecurity-audit-in-canada/ (accessed: 15.02.2022).

16. Electronic Commerce Protection Regulations (SOR/2013-221) URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-221/ (accessed: 16.02.2022).

17. Five Eyes Intelligence Oversight and Review Council (FIORC) URL: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc (accessed: 16.02.2022).

18. Louie, C. (2017). U.S.-Canada Cybersecurity Cooperation. URL: https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/(accessed: 16.02.2022).

19. National Security Agency/Central Security Service URL: https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/ (accessed: 16.02.2022).

20. National Cyber Security Action Plan (2019-2024) URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf (accessed: 13.02.2022).

21. Personal Information Protection and Electronic Documents Act (S.C.2000, c. 5) URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html (accessed: 16.02.2022).

22. Royal Canadian Mounted Police Cybercrime Strategy (2015) URL: https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496 pdf (accessed: 16.02.2022).

23. Secure Electronic Signature Regulations SOR/2005-30 URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html (accessed: 16.02.2022).

24. Stea, J. (2021) How canadians can use social media to help debunk COVID-19 misinformation. *The Conversation*, URL: https://theconversation.com/how-canadians-can-use-social-media-to-help-debunk-covid-19-misinformation-155653 (accessed: 16.02.2022).