окупованій території. Для досягнення найбільшого впливу проукраїнськи налаштованих громадян, вони мають бути розташовані у спосіб, який найбільше нагадує розподілену мережу.

Література

1. Плотинський Ю. М. Моделі соціальних процесів: 2-е вид., перероб. та доп. / Ю. М. Плотинський. – М.: Логос, 2001. – 296 с.

2. Шиян А. А. Теорія ігор: основи та застосування в економіці та менеджменті : навч. посіб. / А. А. Шиян. – Вінниця: ВНТУ, 2009. – Режим доступу: http://inrtzp.vntu.edu.ua/pmba/stf/teach/books/Theory.pdf

Макух-Федоркова І.І.

кандидат політичних наук, доцент кафедри міжнародної інформації факультету історії, політології та міжнародних відносин Чернівецький національний університет імені Юрія Федьковича

КРИТЕРІЇ КАНАДСЬКОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні одними із визначальних факторів сучасної історії є процеси глобалізації та інформатизації. Під впливом цих процесів змінюються концепції національних кордонів, посилюється інтеграція соціально-економічного життя, а також зростає взаємовплив партій і всіх країн на світовій арені. Технологічний прогрес кінця минулого століття докорінним чином змінив ситуацію на світовому інформаційному ринку, адже потоки інформації виходять за рамки національного суверенітету та інтегруються в світовий інформаційний простір. Виникає загроза збереження інформаційних ресурсів держави та захищеності законних прав особистості і суспільства в інформаційній сфері. Не є виключення і Канада, яка на початку XXI ст. здійснила серйозний поворот у напрямку побудови інноваційного суспільства. В даному випадку мова йде про зміну ціннісних орієнтирів канадського суспільства, потенційних шляхах розвитку, створення «економіки, що ґрунтується на знаннях», а також підтримку його національної культурної самобутності. Уряд канадської держави одним з перших в рамках державної політики проголосив курс на побудову інформаційного суспільства і на проведення інформаційної політики. Серйозним чином приділяється увага політиці щодо забезпечення інформаційної безпеки як на національному, так і на міжнародному рівнях.

Одним з основних завдань в сфері інформаційної безпеки є розробка критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки. Тому в 1993 році спеціалістами Центру безпеки, що

входили в структуру відомства Канади були розроблені «Канадські критерії безпеки комп'ютерних систем», які на сьогоднішній день взяті за основу в багатьох інших країнах [1]. В даному контексті варто нагадати, що в 1990 році під егідою Міжнародної організації по стандартизації було розпочато роботу по створенню стандарту в сфері оцінки безпеки інформаційних технологій. Розробка цього стандарту мала наступні цілі: уніфікація національних стандартів в сфері оцінки безпеки 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» [4].

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 1983 р. в документі, що отримав назву «Оранжева книга» (по кольору видання) [5]. 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 [3].

Повертаючись до характеристики канадської системи інформаційної безпеки, варто наголосити, що вона була націлена на широкий діапазон комп'ютерних систем. Основними цілями документа були: розробка єдиної шкали критеріїв для можливості порівняння різних систем обробки інформації по ступені безпеки; створення основи для розробки специфікацій безпечних комп'ютерних систем; розробка уніфікованого підходу і стандартних засобів для опису характеристик безпеки комп'ютерних систем [1].

Крім того, важливим кроком Канади в забезпеченні інформаційної безпеки була активна діяльність міністерства промисловості, адже в 1994 році було прийняте рішення до переходу до інформаційного суспільства і економіки знань. У доповіді під назвою «Побудова інноваційної економіки» чітко зазначалось якими способами держава використовуючи інформаційні технології може досягнути високих економічних і соціальних результатів. Робота зі сторони держави почалась коли була утворена Консультативна рада по інформаційній магістралі з метою підготовки пропозицій уряду. Основна мета ради була спрямована на реалізацію трьох завдань: створення робочих місць за допомогою інновацій та інвестицій, посилення суверенітету Канади і культурної ідентичності, захист приватного життя і безпека мережі, конкуренція у виробництві обладнання, продуктів і послуг, а також забезпечення універсального доступу за прийнятними цінами. У вересні 1995 р. Рада випустила остаточну доповідь «Виклики інформаційної магістралі», в якій містилося близько 300 конкретних пропозицій для дій уряду. Згідно тверджень авторів цієї програми держава повинна максимально створювати конкурентне середовище, в якому канадські фірми могли створювати національну економіку [2, с. 2]. В рамках інформаційної магістралі пропонувалась активна робота з електронним урядом, а саме надання повної інформації і послуг уряду через мережу до 2004 р. На сьогоднішній день взаємодія між урядом і громадянами Канади здійснюється за допомогою офіційного сайту Канади і уряду. Стратегію доступу до послуг і змісту вибудовували на основі 4-х принципів: універсальний, доступний і рівний доступ, орієнтація на споживача і різноманітність інформації, компетентність та участь громадян, відкриті та інтерактивні системи. Ще одним етапом було тестування системи автентичності цифрового підпису для різноманітних урядових послуг.

Інформаційна система Канади постійно тестується на стан безпеки та проводиться контроль по захисту інформації від зовнішнього впливу. З метою посилення ефективності діяльності підрозділів Міністерства оборони проводиться робота з групою інформаційних операцій Канадських збройних сил. Свідченням успішного розвитку канадської інформаційної інфраструктури було створення в 2005 році Центру по кібер – інцидентам (CCIRC). Даний центр має мандат для боротьби із загрозами і нападами на критичну інфраструктуру цілодобово сім днів на тиждень. Важливим рішенням було прийняття в 2010 році канадської стратегії кібербезпеки, яка включає в себе такі аспекти: захист урядових систем; забезпечення безпеки канадських громадян в онлайн середовищі; контроль кібернетичної системи країни за межами федерального уряду [1].

Підсумовуючи варто наголосити, що останніми роками в Канаді створюються усі передумови для переходу до якісно нової моделі розвитку, яка базується на освіті, інноваціях та надійній політиці в сфері безпеки. Ці зміни обумовлені необхідністю пріоритетного розвитку наукоємких галузей

виробництва країни, а також завдяки постійному удосконаленню інформаційної політики, яка включає в себе єдиний інформаційний простір, систему електронного урядування, вільний доступ до інформації, державне регулювання ЗМІ, розвиток Інтернету, нормативне регулювання всіх інформаційних відносин і процесів, переведення більшості державних послуг в електронний варіант. Якість інформаційної безпеки Канади визнана усім міжнародним співтовариством і відзначається, що канадські критерії безпеки комп'ютерних систем є надійними і досконалими національними стандартами інформаційної безпеки. Варто відзначити, що важливу роль в цьому процесі відіграла активність канадського уряду в напрямку фінансування інноваційній діяльності країни, адже за останні роки створена комплексна система фондів інноваційного розвитку, таких як Канадський фонд інновацій, Фонд нових ініціатив, Фонд передових технологій, Фонд лідерських можливостей та ін. І найголовнішим є те, що приймаючи програму створення інноваційного суспільства канадський уряд, виходив з того, що в інноваційний процес мають бути залучені усі прошарки канадського суспільства, які в тісному взаємозв'язку і при фінансовій підтримці держави можуть забезпечити входження Канади в п'ятірку найбільш розвинутих в науково-технічному плані країн.

Література

1. Гунина А.А. Политика Канады в сфере обеспечения информационной безопасности. [Електронний ресурс] – Режим доступу: http://www.scienceforum.ru/2014/676/5473
2. Информационное общество и государство [Електронний ресурс] – Режим доступу: www.relcom.ru/Archive/1997/ComputerLaw/State.htm;
3. Профили защиты на основе «Общих критериев» Аналитический обзор / Под ред. В.Б. Бетелин, В.А. Галатенко, М.Т. Кобзарь, А.А. Сидак, И.А. Трифаленков. – Информационный бюллетень – № 3 (118) / 2003 [Електронний ресурс] – Режим доступу: file:///D:/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/2003_3.319A4A356B684F33A06E15C657633935.pdf
4. Никифорова Н.М. Аналитический обзор критериев информационной безопасности ведущих зарубежных стран (США, Канада, Европейский союз) [Електронний ресурс] – Режим доступу: http://kaf42.mephi.ru/wp-content/uploads/2015/12/part_12-2.pdf
5. Department of defense trusted computer system evaluation criteria / December. 1985. [Електронний ресурс] – Режим доступу: http://csrc.nist.gov/publications/history/dod85.pdf