УДК 351

Грабар Н.С., кандидат наук з державного управління, науковий співробітник наукового відділу проблем державної безпеки навчально-науково-виробничого центру Національного університету цивільного захисту України

Hrabar N.S., PhD in Public Administration, Researcher of State Security Research Department of Educational-scientific-production center, National University of Civil Protection of Ukraine, Kharkiv

ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ В СУСПІЛЬСТВІ - АКТУАЛЬНЕ ЗАВДАННЯ СУЧАСНОСТІ
FORMING A CULTURE OF CYBERSECURITY IN SOCIETY – AS A MODERN CHALLENGE

У статті розглянуто особливості та методи забезпечення інформаційної безпеки на прикладі Канади. Успіхи Канади в кіберпросторі вважаються одним з найбільших національних активів, а їх захист означає огорожу канадської кибersистеми від шкідливих зловживань та інших деструктивних дій. Кібербезпека Канади полягає в Стратегії створення більш безпечного кіберпростору для всіх канадців і передбачає заходи з виявлення, упізнання і захисту від нападів, що реалізуються кіберзлочинцями таємно, коли не залишається ніяких речових доказів про протизаконні дії, приховуваних через складну мережу заражених комп'ютерів.

Ключові слова: *інформаційна безпека, кібербезпека, формування культури кібербезпеки.*

The paper considers main features and methods of ensuring information security in Canada. In Canada protection of cyberspace is considered to be one of the greatest national assets and is manifested in protection of the Canadian cyber system from abuse and other destructive actions. The cyber security of Canada is based on the strategy for creating a more secure cyberspace for all Canadians and provides measures for detection, identification and protection from attacks by cybercriminals who leave no physical evidence of their illegal actions and conceal them through a complex network of infected computers.

***Keywords**: information security, cybersecurity, formation of a culture of cybersecurity.*

Постановка проблеми. Проблема інформаційної безпеки стає в сучасному світі однією з найактуальніших. Представляється можливим досить повно розкрити особливості захисту цієї області на прикладі створення і реалізації урядової стратегії забезпечення безпеки кіберсистем в Канаді.

Аналіз останніх досліджень і публікацій. Проблематику забезпечення державного управління у сфері запобігання і протидії кіберзлочинності в Україні в умовах світової глобалізації не систематизовано, щобільше, подекуди не визначено й найбільш суттєвих загроз. А це, у свою чергу, призводить до нехтування досвідом передових країн світу. На таке вказують більшість дослідників у своїх публікаціях як у друкованих виданнях, так і в мережі Інтернет: П. Андрушко, С. Бабанін, В. Бутузов, А. Волеводз, В. Голубєв, М. Дашян, В. Дзюндзюк, Д. Дубова, В. Марков, М. Литвинов, А. Семенченко, Ю. Сиротюк, О. Стеблинська, Т. Тропіна, В. Хахановський, В. Цимбалюк, Б. Цюпін та ін. Різноманітні питання теорії та практики запобігання кіберзлочинності, боротьби з її проявами та протидії злочинам у сфері високих технологій розглянуто в роботах Н. Ахтирської, П. Біленчука, В. Гавловського, В. Іщенка, М. Карчевського, О. Манжая, В. Номоконова, О. Орлова, О. Осипенко, Н. Савчука, І. Хараберюша та ін.

Постановка завдання. Метою статті є дослідження особливостей формування культури кібербезпеки в суспільстві.

Виклад основного матеріалу. Кіберзлочинність є однією з найактуальніших проблем сучасності, оскільки негативно впливає на діяльність органів державної влади та органів місцевого самоврядування, а завдана нею шкода стосується різних сфер суспільної життєдіяльності, зменшує рівень довіри до державного апарату в цілому. Ефективність запобігання і протидії кіберзлочинності засобами державного управління безпосередньо залежить від узгодженості дій та заходів усіх суб'єктів, наявна система яких, їх функціональна та організаційно-штатна структура є недосконалими.

У зв'язку з усе більшим використанням комп'ютерних технологій в різних сферах діяльності зростає й кількість злочинів, і розмір заподіюваного в результаті їх здійснення збитку. Отже, кіберзлочинність є одним із закономірних негативних наслідків розвитку інформаційних технологій.

Проблема інформаційної безпеки стає в сучасному світі однією з найактуальніших. Представляється можливим досить повно розкрити особливості захисту цієї області на прикладі створення і реалізації урядової стратегії забезпечення безпеки киберсистем в Канаді. Канадська економіка в значній мірі спирається на Інтернет: в 2007 році обсяг продажів через мережу склав 62,7 млрд дол., 87% канадських підприємств використовували Інтернет для забезпечення комерційної діяльності. Канадський бізнес швидко взяв на озброєння сучасні цифрові технології, в тому числі і нове покоління мобільних пристроїв. Уряд Канади також стає більш залежним від Інтернету і в даний час пропонує громадянам понад 130 послуг в електронному вигляді, в тому числі заповнення податкових декларацій, страхових форм зайнятості, кредитних заявок і т.п. Успіх країни в кіберпросторі вважається одним з найбільших національних активів, а його захист означає огорожу канадської киберсистеми від шкідливих зловживань та інших деструктивних дій, що являється досить складним завданням

[3].

Стратегія кібербезпеки Канади є лише одним з елементів в серії ініціатив, спрямованих на захист національних інтересів. Уряд створив канадський КІБЕРЦЕНТР реагування на інциденти, який здатний контролювати і забезпечувати пом'якшення кіберзагроз, надавати консультації та координувати національні заходи у відповідь на будь-які загрози кібербезпеки. Влада Канади вносять зміни в законодавство, модернізують повноваження правоохоронних органів і забезпечують порядок, при якому технологічні інновації не зможуть застосовуватися з метою ухилення від законодавчого контролю над діями злочинної спрямованості в мережі.

Кібербезпека Канади полягає в Стратегії створення більш безпечного кіберпростору для всіх канадців і передбачає заходи з виявлення, упізнання і захисту від нападів, що реалізуються кіберзлочинцями таємно, через складну мережу заражених комп'ютерів. Кібербезпека зачіпає все суспільство, тому нападники, що володіють навичками, технічним потенціалом, здатні заподіяти своїми діями реальну шкоду.

Зловмисники можуть порушити систему електронного управління електричними і телекомунікаційними мережами, гідротехнічними спорудами, здійснити збій в виробництві і постачаннях основних товарів і послуг. Крім того, вони здатні втограться в приватне життя, викрадаючи особисту інформацію про громадян.

Існують різні способи отримання незаконного доступу до інформації в кіберпросторі. Зловмисники можуть використовувати уразливості в програмному забезпеченні і апаратних засобах, експлуатувати прогалини в інформаційній безпеці, обманювати людей шляхом направлення заражених листів.

Вони можуть скористатися тим, що більшість людей не дотримуються основних вимоги кібербезпеки, такі як часта зміна паролів, регулярне оновлення антивірусного захисту і використання тільки захищеної бездротової мережі.

Підключившись до комп'ютера, злочинці можуть вкрасти або пошкодити / змінити інформацію, що зберігається на ньому, модифікувати програмне забезпечення для атак на інші комп'ютери і системи, до яких він підключений. Найчастіше всього жертви страждають через крадіжку ідентифікаційних даних і посягань на особисте майно. Дослідження, проведене університетом Мак-Мастера, показало, що тільки в 2008 р 1700 тис. канадців стали жертвами крадіжки особистих даних. З цієї причини щорічні витрати в Канаді складають, за деякими оцінками, близько 1,9 млрд дол. Тому уряд внес поправки в Кримінальний кодекс, щоб краще захистити канадців від кібератак.

Уряд Канади вважає, що рішення задач щодо усунення подібних ризиків вимагає модернізації військової доктрини країни. У зв'язку з цим НАТО прийняла ряд документів, що стосуються політики кіберзахисту, а Департамент національної оборони і канадських збройних сил вивчають пропозиції про те, як попередити майбутні кібератаки.

Незважаючи на деяку схожість цілей, методів кібератак і характеру загрози, яку представляє кожна з них, існують певні відмінності в їх мотиви і наміри.

Виділяють три типи загроз.

1. За найвитонченішими кіберзагрозами стоять військові та спеціальні служби іноземних держав. У більшості випадків ці нападники володіють величезними ресурсами і послідовні в діях. Їх метою є посилення політичного, економічного, комерційного або військового впливу Все технологічно передові урядові і бізнес-інформсистеми уразливі для шпигунства і кібератак. Розслідування інцидентів подібного роду в Канаді і по всьому світу підтверджують, що ці напади переслідували крадіжку державних і промислових секретів, особистих даних та іншої цінної інформації.

Деякі іноземні держави публічно заявили, що кібератаки є центральним елементом їх військової стратегії і призначені для диверсій і виведення з ладу інфраструктури і засобів зв'язку супротивника.

2. Деякі злочинні організації в даний час розробляють для нападів спеціальне програмне забезпечення, використовують шифрування для захисту своїх активів. У зв'язку з цим можливості деяких кіберзлочинців тепер часто перевершують можливості технологічно розвинених держав У 2007 р було виявлено, що з американської роздрібної мережі викрадено понад 45 млн записів клієнтів. Виявилося, що це була не разова акція: три роки злочинці вели моніторинг бездротових каналів передачі інформації про продажі за допомогою кредитних карт через термінали. Завдані збитки становлять понад 130 млн дол. У 2008 р 11 осіб, що знаходилися в п'яти різних країнах, були звинувачені у зломі бази даних дев'яти основних роздрібних мереж і крадіжці близько 40 млн записів з баз даних про кредитних і дебетових картах з метою продажу через Інтернет іншим злочинцям.

3. Еволюція кібератак, їх інструментів і методів помітно прискорилася. Статистичні дані, зібрані двома добре відомими компаніями по інтернет-безпеки (Akamai і Symantec), показують, що шкідливі програми зараз існують в більш ніж 190 країнах. Більше 60% виявленого шкідливого коду був виявлено в кіберпросторі в 2008 р [1].

Стратегія кібербезпеки Канади повинна зміцнити інформаційні системи країни, особливо в критично важливих секторах інфраструктури, забезпечити підтримку економічного зростання і захисту канадців Стратегія кібербезпеки Канади побудована на трьох основних принципах [2]:

1) забезпечення довіри канадців державним інформаційних систем при роботі уряду з їх особистим та діловим інформацією, а також при наданні електронних послуг громадянам. Уряд прагне захистити канадський суверенітет і забезпечити кіберзахист національної безпеки і економічних інтересів. Для цього створюються необхідні структури, виділяються кошти і персонал для виконання зобов'язань з кібербезпеки;

2) партнерство для забезпечення захисту життєво важливих кіберсистем

поза державою. З цією метою в співробітництво з урядами провінцій і територій, а також приватним сектором влади Канади надають підтримку кіберініціативам і вживають заходів по зміцненню найважливіших секторів інфраструктури. Канадські дослідники працюють над прогнозуванням, виявленням і оперативної ліквідацією кіберзагроз, вносять пропозиції щодо найбільш раціональному використанню кіберпростору в національних інтересах Канади;

3) міжнародне партнерство. Канада підтримує міжнародні зусилля з розробки і реалізації глобального режиму управління кібербезпекою, який підвищить безпеку країни в цілому. Канада бере участь у створенні потенціалу кібербезпеки в менш розвинених країнах спільно із зарубіжними партнерами, що допоможе запобігти появі супротивників, які експлуатують слабкі ланки в глобальній системі кіберзахисту.

Забезпечення інформаційної діяльності уряду є не просто питанням його операційної ефективності - це питання національної безпеки, суверенітету і захисту всього суспільства. Ще в 2009 р уряд Канади прийняв ряд важливих поправок щодо безпеки держави, встановивши гарантії надання державних електронних послуг для громадян. Міністерства і відомства зобов'язані здійснювати постійний моніторинг з метою виявлення загроз, а також забезпечення безпеки електронних операцій і усунення ризиків діяльності електронного уряду в країні [2].

В рамках забезпечення громадської безпеки Канадський центр реагування на кіберінциденти координує моніторинг і надання консультаційної допомоги в пом'якшенні кіберзагроз та працює над створенням національних заходів, спрямованих на вирішення будь-яких кіберінцідентов. служба Громадської безпеки Канади веде інформаційно-пропагандистську діяльність про потенційні ризики, з якими громадяни можуть зіткнутися, і про дії, які вони можуть зробити для захисту себе і своїх сімей в кіберпросторі Створення системи безпечного зв'язку Канади розширить можливості з виявлення та виявлення загроз,

забезпечить ефективність дій зовнішньої розвідки і служб кібербезпеки. Підтримка повсякденній діяльності по захисту від кіберзагроз попередить можливі провали, які матимуть негативні політичні та економічні наслідки і підривати довіру громадян до уряду.

Відзначимо, що Стратегією поставлена задача об'єднання зусиль уряду Канади, академічної спільноти, неурядових організацій та приватного сектора по забезпечення безпеки кіберсистеми держави. Кожен із суб'єктів цієї діяльності має унікальні технологічні та аналітичні можливості для вироблення пропозицій щодо забезпечення безпеки власних систем Ця співпраця має важливе значення для загального успіху, проте і канадці повинні брати безпосередню участь у вирішенні цієї проблеми: знати про можливість кіберзагроз, володіти інструментами для їх розпізнавання і захисту, використовувати ці кошти для захисту себе і своїх сімей. У 2008 р в результаті досліджень університету Мак-Мастера встановлено, що 20% споживачів самоусунулися від торгових угод в Інтернеті, 19% - відмовляються від он-лайн банківської діяльності в зв'язку з ризиками, можливими при веденні бізнесу в Інтернеті.

Глобалізація індустрії високих технологій ускладнює в провінціях оцінки надійності постачальників луг і техніки. Кіберзлочинці обізнані про можливості, що виникають за рахунок проломів в захисті і ланцюга поставок. Деякі організовані злочинні синдикати використовують ці вади шляхом поширення необхідних для вчинення злочинів технологій. Тому уряд активізує необхідні процеси для зменшення ризику, пов'язаного з погрозами з боку інформаційних технологій. Розширення можливостей уряду щодо виявлення, припинення та захисту від кібератак відбувається на тлі активного впровадження в країні кібертехнологій для розвитку країни, забезпечення економічної і національної безпеки. У системах обробки інформації уряду присутній суворо засекречена інформація, пов'язана з військовою і національною безпекою; уряду доручено надавати послуги громадянам в електронному вигляді, тому громадяни надають

важливу особисту та конфіденційну інформацію для заповнення електронних баз даних.

Відповідно, кіберзлочинці регулярно зондують ці системи, виявляючи наявність в них вразливостей.

Успіх уряду в забезпеченні безпеки своїх Інформсистему в значній мірі залежить від співробітників: численні інциденти показали, що навіть найсучасніші системи безпеки можуть постраждати від людської помилки. В уряді, як і всюди, люди не завжди дотримуються головним правилам кібербезпеки: не змінюють на регулярній основі свої паролі, не стежать за антивірусним захистом комп'ютерів, відвідують шкідливі сайти, помилково вважають, що незахищена система електронної пошти досить безпечна.

Необхідно впроваджувати програму навчання, тренінгів, для того щоб підвищити відповідальність персоналу в цих питаннях. За даними дослідницького центру університету Мак-Мастера, до 63% користувачів використовують Інтернет для передачі чутливої інформації. Дані про комерційні угоди на 57% містять чутливу інформацію в комп'ютерах і мережах. Тільки 35% канадців вважають, що їхній комп'ютер захищений від загроз [1].

Тому мета уряду Канади полягає в тому, щоб сформувати в суспільстві культуру кібербезпеки. Створення централізованого об'єднаного КІБЕРЦЕНТР по боротьбі зі злочинами збільшить ефективність виявлення злочинців, в тому числі на основі аналізу ризиків та запитів канадців.

Висновки. Таким чином, Стратегія кібербезпеки Канади дозволяє захистити цілісність урядових систем і національних критичних активів, ефективно боротися з кіберзлочинами і захищати канадців при щоденному використанні ними кіберпростору.

Стратегія спонукає громадян, промисловість і всі рівні уряду коригувати свої дії і застосовувати технології, необхідні для протистояння кіберзагрозам в умовах,

коли життя без Інтернету - складного і корисного методу комунікації - стає неможливим.

Список використаних джерел:

1. Стратегия кибербезопасности Канады. URL: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf (дата обращения: 14.06.2011).

2. URL: http://www.tbs-sct.gc.ca/ pol/doc-eng.aspx?id=16578&section=text (дата обращения: 12.06.11).

3. URL: http://www:bs-stc.gc.ca/pol/doc-end.aspx/kin5B,ALKG9,15bzd,GUi7 (дата обращения: 12.06.11).

References:

1. Dzlyev M.I., Romanovych A.L., Ursul A.D. Security Issues: Theoretical and Methodological Aspects [Problemы bezopasnosty`: teorety`ko-metodology`chesky`e aspektы], M. 2001. p. 348.

2. Ynshakov O.V., Lebedeva N.N. Economic and institutional mechanisms: correlation and interaction in the conditions of social and market transformation of the Russian economy [Xozyajstvennыj y` y`nsty`tucy`onal`nыj mexany`zmы: sootnosheny`e y` vzay`modejstvy`e v uslovy`yax socy`al`no-rынochnoj transformacy`y` rossy`jskoj эkonomy`ky`] S.-Petersburg newspaper. state. Unta. Avg. 5. 1998. Issue. 4 (No. 16). - p. 54-58.

3. Kormych B.A. Organizational and legal bases of information security policy of Ukraine [Organizacijno-pravovi osnovy` polity`ky` informacijnoyi bezpeky` Ukrayiny`] diss. ... Dr. Jurd. Sciences: Special. 12.00.07. - Odessa, 2004. - p. 427.

4. Prysiazhniuk M.M., Bieloshevych Ya. I. Information security of Ukraine in modern conditions [Informacijna bezpeka Ukrayiny` v suchasny`x umovax] Bulletin of Taras Shevchenko National University of Kyiv. Military Special Sciences. - 2013. - Vip. 30. p. 42-46.

Extended abstract of the article Hrabar N.S. "INFORMATION SECURITY AS ONE OF THE COMPONENTS OF NATIONAL SECURITY OF UKRAINE"

Hrabar N.S., PhD in Public Administration, Researcher of State Security Research Department of Educational-scientific-production center, National University of Civil Protection of Ukraine, Kharkiv

Target setting. At this stage of world history, the role of the information sphere of the life of society is growing, which means the totality of information, information infrastructure, subjects of information legal relations, and the system of regulation of the social relations that arise in the process. In turn, the information sphere has a very significant impact on the state of political, economic, defense and other components of the security of Ukraine. From this it should be concluded that national security is significantly dependent on information security, and in the course of further advances in information technology, this interdependence will increase more and more.

Analysis of recent research and publications. The conducted doctrinal analysis of the problems of information security showed that, despite the great interest in this issue, its study is mainly of technical and applied nature and focused on solving specific scientific and technical problems.

The research of theoretical and practical aspects of information security, addressed to the role of information processes, is devoted to the work of domestic scientists O. Bodruk, A. Kachinsky, V. Krysachenko, S. Pyrozhkov, T. Starodub, O. Shevchenko, while information security as one of the components of national safety was not considered by scientists, which caused the scientific interest of the author.

Objectives setting. The purpose of the article is to investigate the features of information security as one of the components of national security.

Presenting main material. In modern literature, information security is understood to mean its protection against accidental or deliberate interference with its functioning,

from attempts to steal, modify, and destroy its components. The scientific doctrine of information security of Ukraine provides a comprehensive definition of information security. It should be understood as a state of protection of national interests in the information environment, which determines the set of balanced interests of the individual, society and state.

The main objects of legal relations that are developing in the field of information security are the rights and freedoms of the individual in the information sphere, such as the right to access to information, the right to education, the right to access to cultural property, and the right of intellectual property; moral and cultural values of society, constitutional order, democracy and territorial integrity of the state. Cybercrime in the domestic market is one of the problems of information security. Computer crimes targeting networks of banks and credit institutions are also heavily harmed.

Conclusions. Thus, the most important task of ensuring information security is to ensure the balance of interests of the individual, society and the state and their effective cooperation within the global information space. This balance must be consistent with public security policy in general. In the context of globalization, it becomes necessary to analyze changes in the foreign and domestic policies of other countries, as well as their legislation and enforcement practices. All of the above is a crucial prerequisite for the effective functioning of the information security and information security system.