РОЗВІДКИ МОЛОДИХ НАУКОВЦІВ

УДК: [351.746:004.738.5.056](480)
© Вікторія Акульшина
Науковий керівник: доц. О.Я. Звоздецька

КІБЕРБЕЗПЕКА ФІНЛЯНДІЇ: ПРАВОВИЙ ТА ІНСТИТУЦІЙНИЙ МЕХАНІЗМИ[1]

В дослідженні проаналізовано кібербезпекову стратегію Фінляндії, а також охарактеризовано діяльність урядових і неурядових організацій, до компетенції яких входить вирішення питань щодо забезпечення функціонування інформаційного простору.

Ключові слова: *кіберпростір, кібератаки, кібербезпека, Фінляндія.*

Кибербезопасность Финляндии: правовой и институциональный механизмы

В исследовании проанализировано стратегию кибербезопасности Финляндии, а также описана деятельность правительственных и неправительственных организаций, в компетенцию которых входит решение вопросов обеспечения функционирования информационного пространства.

Ключевые слова: *киберпространство, кибератаки, кибербезопасность, Финляндия.*

Cyber Security of Finland: Legal and Institutional Mechanisms

The research contains the analysis of the Finland´s cyber security strategy and describes the work of government and nongovernment organizations which are aimed at inosphere functioning facilitation.

Keywords: *ccyberdomain, cyberattacks, cybersecurity, Finland.*

Актуальність теми. На сучасному етапі Фінляндія займає провідну сходинку серед країн Європи за індексом розвитку людського потенціалу, оскільки інформатизація торкнулася всіх сфер життєдіяльності суспільства.

Зокрема, у 2015 р. за оцінкою глобального звіту про стан світової

[1] ***Для цитування:*** Акульшина В. Кібербезпека Фінляндії: правовий та інституційний механізми // Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 158-165.

кібербезпеки Фінляндія увійшла у десятку країн з найвищим показником розвитку ІКТ [6, с. 19]. Вже наприкінці 2016 р. у країні було відкрито новий Європейський центр передового досвіду з протидії гібридним загрозам. Мета центру – збір та обмін інформацією щодо протидії гібридним загрозам (кібератакам, пропаганді та дезінформації), допомога у формуванні учасникам ініціативи програм або стратегій боротьби з гібридними загрозами [3]. Тому досвід інформаційного захисту Фінляндії, дослідження сучасного стану її розвитку та аналіз законодавчої бази держави з даного питання є надзвичайно важливим для України в умовах ведення гібридної війни з РФ.

Аналіз останніх досліджень і публікацій. Серед вітчизняних науковців, які вивчали окремі аспекти розвитку інформаційного суспільства в Фінляндії, варто відзначити О.М. Андрєєву та О.Ю. Запорожець – співробітників кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

Доктор політичних наук О.М. Андрєєва у своїй статті «Електронне урядування країн Скандинавії: становлення та розвиток» акцентує увагу на важливій ролі інформаційно-комунікаційних технологій в житті фінського суспільства та важливості захисту інформаційного простору держави. Зокрема, авторка висвітлює проблему розвитку електронної комерції, що, безумовно, пов'язана з питанням захисту інформації і передачі даних [2].

В науковій роботі О.Ю. Запорожець «Політика Європейського Союзу в сфері інформаційної безпеки», розглядається діяльність урядових і неурядових організацій Фінляндії, які відповідають за забезпечення кіберзахисту держави. Крім того, дослідниця визначає загальні положення Національної стратегії інформаційної безпеки на 2009-2015 рр., яку було прийнято урядом Фінляндії у 2008 р. [5].

Мета дослідження полягає у вивченні досвіду Фінляндії у сфері захисту інформаційного простору від кібернетичних атак.

Виклад основного матеріалу. Система інформаційного забезпечення Фінляндії є самостійною галуззю, що продовжує динамічне зростання та має величезний вплив на економіку всієї держави. Велика кількість різноманітних організацій і компаній Фінляндії має доступ до інформаційних мереж, за допомогою яких здійснюється пошук необхідної інформації у режимі on-line. Завдяки новітнім інформаційним технологіям підприємствами країни реалізується, зо-

крема, продаж власної і купівля необхідної продукції та послуг за допомогою використання сучасних інформаційних мереж; відбувається безперервний обмін необхідної інформації каналами електронного зв'язку зі своїми філіалами, партнерами; проводиться дослідження нових ринків збуту товарів і послуг, а також здійснюється моніторинг виробництва, транспортування товару тощо.

Разом із тим, безперервний розвиток інформаційно-комунікаційних технологій і інформатизація суспільства створюють все більше можливостей для заподіяння шкоди національному кіберпростору Фінляндії. Кіберзлочинці здійснюють атаки задля отримання доступу до стратегічних напрямів, що є привабливими з погляду економічних і політичних інтересів.

Так, 2008 р. на електронну пошту тодішнього прем'єр-міністра Матті Ванханена була здійснена хакерська атака – на його пошту надійшло понад 50 тисяч різних повідомлень. Пізніше, у 2010 р., об'єктами злому в скандинавських країнах стали сайти політиків і політичних організацій. Великого розголосу також набув злам приблизно 500 тисяч користувацьких поштових аккаунтів хакерської групи під назвою Anonymous Finland у 2011 р. [8].

Як наслідок, задля забезпечення належного функціонування свого кіберпростору, Урядом Фінляндії було сформовано нормативно-правову базу в даній сфері. Вона містить у собі ряд програмних документів, що спрямовані на зміцнення кіберзахисту держави. Основними серед них є Національна стратегія інформаційної безпеки на 2009-2015 рр. [5, с. 40], Програма інформаційного суспільства Фінляндії тощо [12].

У документах визначено основні положення щодо кіберзахисту, зокрема, розкрито визначення поняття «кібербезпека», затверджено загальні принципи національного підходу до її управління, вказано основні обов'язки, що покладені на Уряд Фінляндії у даній сфері, визначено базові засади щодо недоторканості приватного життя громадян в сфері електронних комунікацій тощо.

Провідну роль у системі інформаційного захисту Фінляндії відіграє Стратегія кібербезпеки 2013 р., що стала першим самостійним документом у даній сфері. Вона являє собою бачення та стратегічні орієнтири стосовно кібербезпеки, а також в ній зазначено реальні для виконання положення щодо досягнення бажаного кінцевого стану у захисті інформаційного простору.

Структуру Стратегії становлять чотири основні розділи, додаток, що представлено у вигляді основних визначень та дефініцій, а також окремий допоміжний документ, який дає можливість краще зрозуміти поняття кібербезпеки та процес її реалізації.

За даними Європейського інформаційно-дослідницького центру, у Стратегії визначено основні цілі та способи реагування на загрози, що спрямовані проти кібербезпеки Фінляндії. Уряд самої країни зазначив, що основною метою документа було створення загального розуміння кібербезпеки та визначення її ролі в забезпеченні спільної безпеки [4, с. 17].

За визначенням Стратегії, кібербезпека – це такий сприятливий стан, при якому надійно захищено кіберпростір і забезпечено належне його функціонування. Крім того в документі наголошено на тому, що кібербезпека є частиною спільної стратегії суспільства [1, с. 13].

Урядом Фінляндії визначені наступні завдання захисту кіберпростору:

- держава спроможна забезпечити належний захист своїх життєво необхідних функцій від будь-якого роду кібернетичних загроз у різних ситуаціях;
- громадяни держави, владні органи та підприємства можуть ефективно використовувати безпечний кібер-домен, що є результатом заходів з кібербезпеки на національному та міжнародному рівнях;
- Фінляндія поставила собі за мету до 2016 року стати беззаперечним лідером серед інших країн у готовності відбити будь-які кібернетичні загрози [1, с. 3].

За розробку та реалізацію політики в сфері захисту національного інформаційного простору Фінляндії відповідальними є урядові та неурядові організації, що здійснюють постійний нагляд і контроль за поточним станом інформаційного захисту. До їх компетенції входить, зокрема, захист персональних даних громадян, конфіденційної і таємної інформації; реалізація національної політики в сфері інформаційного захисту; створення законодавства щодо комунікаційних мереж; забезпечення належного доступу громадян до комунікаційних послуг, сприяння покращенню рівня обізнаності населення в сфері інформаційних технологій і т. д.

Головним органом у галузі захисту національної безпеки Фінляндської Республіки є Міністерство оборони. Його першочерговою

метою є створення гідних умов для стабільного функціонування та життєдіяльності всього суспільства. Міністерство оборони є відповідальним за координацію загальної оборони держави, в тому числі й за захист кібернетичного простору [7].

Одним із комітетів у складі Міністерства оборони є Комісія захисту інформації і планування (Maanpuolustustiedotuksen Suunnittelukunta – MTS), до складу якої входять члени парламенту і члени різних експертних організацій. Дана комісія заснована у 1976 р. та діє в якості парламентського форуму, що влаштовує різноманітні обговорення й семінари з питань безпеки, національної оборони, а також з приводу надзвичайних ситуацій й готовності до них неурядових організацій, політиків, ЗМІ тощо. Комісія захисту інформації і планування здійснює наукову діяльність, з підготовки кадрів та активно співпрацює з такими країнами Скандинавії, як Швеція і Норвегія [14].

Ще однією з важливих державних установ, що відповідає за кібербезпеку країни, є Міністерство транспорту і зв'язку Фінляндії. Основне завдання, яке покладене на Міністерство – це розробка та реалізація національної політики в сфері інформаційної безпеки [13].

Одним із структурних підрозділів Міністерства транспорту і зв'язку є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA), створений у 1988 р., та покликаний здійснювати контроль, а також державне регулювання у сфері інформаційно-комунікаційних технологій.

Зокрема, до повноважень FICORA відноситься інформування про потенційні загрози інформаційній безпеці держави, ретельний нагляд за станом функціональності комунікаційних мереж, підвищення рівня обізнаності громадян з питань інформаційної безпеки, управління використанням радіочастот, мережевими адресами, а також контроль за змістом програм та реклами на телебаченні і радіо [10].

В структурі FICORA функціонує Фінська комп'ютерна група швидкого реагування (Computer Emergency Response Teamof Finnland– CERT-FI), що ставить собі на меті попередження, виявлення й реагування на певні проблеми у сфері інформаційної безпеки та поширення інформації про засоби попередження інцидентів, які пов'язані з кібербезпекою [9].

До компетенції CERT-FI відносять також такі питання, як: проведення моніторингу надзвичайних випадків на національному та

міжнародному рівнях; підвищення рівня громадської обізнаності з питань стосовно інформаційного захисту держави; поширення інформації серед громадян про засоби попередження інцидентів, що пов'язані з кібербезпекою; співробітництво з постачальниками обладнання й програмного забезпечення, а також з правоохоронними органами і т.д.

З 2014 р. здійснює свою діяльність Національний центр з кібербезпеки Фінляндії (NCSC-FI), до обов'язків якого входить певний перелік завдань CERT-FI і NCSA-FI. NCSC-FI покликаний забезпечити надійне користування мережами загального зв'язку, долаючи при цьому всі можливі кібернетичні загрози, а також створити сприятливі умови для підтримки існування найважливіших соціальних функцій. NCSC-FI прагне розширювати свої послуги щодо надання інформаційної безпеки за допомогою, наприклад, дослідно-конструкторських робіт та створюючи великі мережеві товариства [11].

Висновки. Отже, у кінцевому підсумку варто сказати, що Фінляндська Республіка є дійсно провідною державою у сфері системи захисту кіберпростору, про що свідчить рівень інформаційного розвитку її суспільства, готовність країни відбити можливі кібератаки, а також прагнення до створення надійної цілісної системи інформаційної безпеки задля належного існування та життєдіяльності всього суспільства. Наразі Урядом Фінляндії сформовано нормативно-правову базу у даній сфері, що покликана регулювати всі питання, пов'язані з інформаційним простором держави. Зокрема, у Фінляндії діє багато урядових і неурядових установ, які спрямовують свою діяльність на кібернетичний захист свого кіберпростору.

Проте не зважаючи на те, що сучасне інформаційне суспільство Фінляндії вже є сформованим, система інформаційного захисту держави досі залишається вразливою до кібератак, оскільки у той час, коли відбувається стрімкий розвиток інформаційно-комунікаційних технологій, з'являється також все більше різноманітних видів кібернетичних загроз.

Джерела та література:

1. Finland´s Cyber security Strategy: станом на 24 січ. 2013 р. [Електронний ресурс] / Міністерство оборони Фінляндії. – 40 с.– Режим доступу: http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

2. Андрєєва О. М. Електронне урядування країн Скандинавії: становлення та розвиток [Електронний ресурс] / О. М. Андрєєва. // Проблеми міжнародних відносин. – 2014. – №9. – С. 154 – 168. – Режим доступу: http://www.kymu.edu.ua/vmv/v/p09/11.pdf

3. В Финляндии появился новый центр по изучению гибридных угроз [Електронний ресурс] // FlashNord: информационное агентство – 2017. – Режим доступу: http://flashnord.com/news/v-finlyandii-poyavilsya-novyy-centr-po-izucheniyu-gibridnyh-ugroz

4. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших [Електронний ресурс] // Європейський інформаційно-дослідницький центр. – 2016. – 37 с.– Режим доступу: http://euinfocenter.rada.gov.ua/uploads/documents/28798.pdf

5. Запорожець О. Ю. Політика Європейського Союзу в сфері інформаційної безпеки [Електронний ресурс] / О. Ю. Запорожець. // Актуальні проблеми міжнародних відносин. – 2009. – №87. – С. 36 – 45. – Режим доступу: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/1195/1139

6. Измерение информационного общества – Отчет 2015 год [Електронний ресурс] // Международный союз электросвязи. – 2015. – 42 с.– Режим доступу: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-R.pdf

7. Міністерство оборони Фінляндії [Електронний ресурс]. – Режим доступу: http://www.defmin.fi/

8. Финляндию атакуют хакеры из Anonymous [Електронний ресурс] // Центр информационной безопасности – 2011. – Режим доступу: http://www.bezpeka.com/ru/news/2011/11/17/finland-under-anon-attack.html

9. CERT-FI [Електронний ресурс] // Finnish Communications Regulatory Authority. – 2017. – Режим доступу: https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi.html

10. FICORA [Електронний ресурс] // Finnish Communications Regulatory Authority. – Режим доступу: https://www.viestintavirasto.fi/en/ficora.html

11. Information security services of the NCSC-FI [Електронний ресурс]. – Finnish Communications Regulatory Authority. Режим доступу:

https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices.html

12. Kalja H. Measurements in support of policy decisions [Електронний ресурс] / Hovi Kalja // OECD World Forum on Key Indicators. – 2004. – Режим доступу: http://www.oecd-ilibrary.org/economics/statistics-knowledge-and-policy_9789264009011-e

13. Key duties of the Ministry [Електронний ресурс] // The Ministry of Transport and Communications. – Режим доступу: https://www.lvm.fi/en/information-en

14. The Advisory board for defence information (ABDI) – A Permanent Parliamentary Commmittee [Електронний ресурс]. – Ministry of Defence of Finland. Режим доступу: http://www.defmin.fi/en/tasks_and_activities/media_and_communications/the_advisory_board_for_defence_information_abdi