Шпирко І.Б.,
аспірант кафедри публічного управління та адміністрування,
Університет Григорія Сковороди в Переяславі

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ НАТО В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Ядром «проблемного поля» інформаційної безпеки є визначення того, яким є природа та деструктивний потенціал інформаційних загроз. П. Корніш із лондонського Королівського інституту закордонних справ (Chatam House) наводить таку класифікацію інформаційних загроз:

1) діяльність хакерів-одинаків;

2) організована злочинність, що діє у глобальних Інтернет-мережах;

3) ідеологічний та політичний екстремізм;

4) інформаційна агресія, що проводиться державою [1, p. 7-16].

На сьогодні лише перші два різновиди загроз із даної класифікації набули практичного втілення у світовому інформаційному суспільстві. Що стосується кібертероризму та кібервійни між державами, то вони є скоріше є майбутніми загрозами, які можуть бути реалізовані.

Експерти з Центру кіберзахисту НАТО розглядають мілітаризацію Інтернету як один із головних і найнебезпечніших трендів розвитку світового кіберпростору: «Сучасні військові структури готові використовувати інформаційний простір як «паралельне поле битви» у конфліктах майбутнього». При цьому висловлюється впевненість у тому, що проведення кібератаки у чистому вигляді малоймовірно [2].

Інші експерти в галузі інформаційної безпеки також переконані в тому, що «окремих кібервійн поза традиційними бути не може» [1]. Найімовірнішим є наступний сценарій: агресивні акції в кіберпросторі будуть використовуватися для посилення ефекту традиційних операцій із застосуванням традиційних наступальних озброєнь. Саме така формула – звичайне озброєння плюс кіберзброя – лежатиме в основі стандартних оперативних та стратегічних дій у майбутніх конфліктах. Що ми зараз спостерігаємо у війні росії на території України.

При цьому К. Гірз зазначає, що політичні лідери, відповідальні за ухвалення рішень, які можуть засновувати свої дії лише на теоретичних припущеннях [1, p. 12]. Причин тому кілька: на сьогоднішній день надто мало показових прикладів; переважний масив інформації засекречений і знаходиться поза простором публічної політики; більшість організацій не усвідомлюють справжній стан власної інформаційної безпеки та кібербезпеки. Тому для політичних еліт часто складно відповісти на запитання, чи справді інформаційні та кібератаки несуть серйозну загрозу національній безпеці.

Ключова роль в інформаційному забезпеченні політики НАТО відводиться головному органу організації – Північноатлантичній раді. Ця структура займається інформуванням широкого загалу про діяльність Альянсу за допомогою публікації в пресі своїх рішень та заяв.

Безпосередньою реалізацією публікацій матеріалів Атлантичної ради займається Комітет громадської дипломатії НАТО та його підрозділи. Крім цього, за допомогою організації різних громадських заходів та програм, Комітет проводить роботу з інформування суспільств країн-членів і країн-партнерів про цілі та завдання Альянсу на сьогоднішній день та на найближче майбутнє.

Для цього Комітет підтримує тісні зв'язки зі ЗМІ країн-членів, а також аналізує суспільні настрої інших країн, що входять у сферу інтересів організації [3].

Основи роботи в тій чи іншій сфері прописуються в офіційних документах НАТО. Так, наприклад, основні принципи забезпечення безпеки класифікованої інформації виділяються в документ С-М(2002)49 «Безпека в організації Північноатлантичного договору». За визначенням цього ж документу класифікована інформація є будь-якою інформацією (а саме, знання, які можуть бути передані у будь-якій формі) або матеріал, який вимагає захисту від несанкціонованого розкриття та включений до списку класифікації безпеки. Тут же вказано, що всю важливу внутрішню інформацію НАТО поділяє на п'ять рівнів по мірі зменшення: COSMIC TOP Secret (CTS – «Цілком таємно»), NATO Secret (NS – «Секретно»), NATO Confidential (NC – «Конфіденційно»), NATO Restricted (NR – «Обмежений доступ»), Unclassified but sensitive («Внутрішня інформація. Не класифікована»). Крім того, в цьому ж документ вказуються основні вимоги, необхідні для забезпечення безпеки інформації [4].

Таким чином, кожна держава-член дає оцінку тій чи іншій інформації та, спираючись на те, як інші члени дотримуються конфіденційності щодо даної інформації, приймає рішення, якої інформації слід надати доступ Альянсу. Тобто будь-яке порушення правил конфіденційності з боку того чи іншого члена НАТО може призвести до зменшення потоку інформації, що надається іншими країнами-членами. Основний принцип полягає в тому, що інформація повинна зберігати цей статус протягом усього процесу звернення.

Список використаних джерел:

1. Geers, K. Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p.
2. NATO CCD CoE Mission and Vision. NATO Cooperative Cyber Defence Centre of Excellence. URL: http: //www.ccdcoe.org/11.html.
3. NATO Information Management Policy (NIMP). URL: https://nisp.nw3.dk/ node/T-35ac841c-00ad-4b74-b116-8e1df21c702c-X.html
4. Document C-M(2002)49: Security withing the North Atlantic Treaty Organization. URL: https://www.nbf.hu/docs/C-M(2002)49-REV1.pdf