УДК 327

А. Ю. Вітенко
В. О. Корнієнко

НАТО ЯК ГАРАНТ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Вінницький національний технічний університет

Анотація
Стаття присвячена дослідженню про основні вимоги НАТО щодо забезпечення безпеки інформаційного простору.
Ключові слова: НАТО, безпека, інформація, інформаційний простір.

Abstract
The article is devoted to a study of NATO's basic requirements for ensuring the security of the information space.
Keywords: NATO, security, information, information space.

Вступ

З стрімким розвитком ІТ важливість інформаційного простору зростає з кожним днем. Проте, даний прогрес створює нові загрози безпеці, особливо у зв'язку з кібервійною, потенційним використанням терористами та кіберзлочинцями. Наразі, НАТО відіграє важливу роль у забезпеченні безпеки інформаційного простору та захисту від кібератак. Тому, у даній роботі розглядаються основні принципи захисту інформаційного простору НАТО.

Основна частина

Інформаційний простір є сукупністю інформаційних ресурсів та технічних засобів, які забезпечують обіг та обробку інформації в системі соціально-економічних та політичних відносин.

Засоби масової інформації створюють «віртуальний простір» для міжнародного тероризму, що також підсилює його непрямий вплив на світовий перебіг подій. Міжнародний тероризм є потенційно дуже ефективним засобом ослаблення держави та підривання її стабільності. Він може мати два напрями – прямий і непрямий.

Якщо держава не буде використовувати власний інформаційний простір в своїх інтересах, то його використання терористами може стати більш систематичним, що призведе до негативних наслідків для всього світу [1].

Не допустити такого розвитку подій і є важливим завданням для Альянсу. Основним принципом безпеки інформації НАТО є те, що інформація повинна зберігати свій ступінь захисту при всіх її передачах та необхідно забезпечувати відсутність її витоку, а також і те, що правила доступу до інформації повинні надаватись лише особам, яким вона потрібна.

У 2010 році на Лісабонському саміті НАТО було вирішено розробити нову політику НАТО з кіберзахисту, й розробити конкретний план дій, який набув чинності з червня 2011 року [2].

Були сформовані стандарти НАТО щодо захисту інформації. Ключовим терміном в цьому аспекті є «керування ризиком», тобто незалежна оцінка уразливості інформації, а також проведення контрзаходів з цього приводу.

Захист від кібернетичних атак є важливою ланкою розробок НАТО. Основні положення політики безпеки НАТО, в т.ч. щодо класифікованої інформації, викладені у документі СМ(2002)49 «Безпека в межах організації Північноатлантичного договору».

Класифікована інформація — термін, який використовується у законодавстві країн−членів НАТО відносно частини вразливої інформації. З позицій інформаційної безпеки вся інформація у світі

поділяється на загальнодоступну і з обмеженим доступом. Саме таке визначення прийнято в НАТО і країнах − членах Альянсу.

НАТО має п'ять рівнів захисту інформації з обмеженим доступом (Cocmic TOP Secret (CTS), NATO Secret (NS), NATO Confidential (NC), NATO Restricted (NR), Unclassified but Sensitive) [3].

Аналіз законодавчих актів країн − членів НАТО свідчить, що у власному внутрішньодержавному законодавстві використовують не більш як три рівні класифікації для інформації, що становить державну таємницю, зараховуючи інформацію з грифом, що відповідає рівню RESTRICTED до розряду офіційної, службової та громадської (public) таємниці.

У зв'язку з цим НАТО виокремлює наступні цілі і вимоги для всіх країн, зацікавлених у збереженні цілісності, непорушності і конфіденційності їхнього державного інформаційного простору. Інформаційна структура повинна постійно удосконалюватися, темпи розвитку нових інформаційних технологій та їх поширення повинні прискорюватися.

Важливим є розвиток систем електронної сертифікації та криптографії, належна підготовка персоналу. Формування і реалізація єдиної державної політики в контексті забезпечення безпеки національних інтересів від загроз в інформаційній сфері має стати одним з пріоритетних напрямків розвитку держави. Розвиток індустрії інформаційних та телекомунікаційних засобів, поширення їх на внутрішньому медіа–ринку держави, модернізація систем телемовлення та радіомовлення. Ефектна протидія інформаційній експансії та спробам використання національного інформаційного простору.

Ефективний кіберзахист вимагає засобів запобігання, виявлення, реагування і відновлення після атак. НАТО здійснює кроки з розвитку таких засобів через створення Відомства з управління кіберзахистом, Спільного Центру передового досвіду з кіберзахисту і Сил реагування на комп'ютерні інциденти.

Наразі НАТО виокремлює необхідність здійснення зусиль задля посилення моніторингу критично важливих мереж в межах Альянсу та оцінки і зміцнення виявлених слабких місць.

Висновки

Сьогодні важко переоцінити роль НАТО у захисті інформаційного простору. Хоча Альянс не єдиний, хто прагне повної безпеки в даній сфері, його поєднання військової єдності та основи політичної згуртованості робить його важливим учасником забезпечення захисту від кіберзлочинності. Тенденція зрозуміла, без майбутньої участі НАТО перспективи міжнародної стабільності та миру були б набагато нижчими, ніж сьогодні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. John E Dunn. NATO clause V could deter cyberattack, says defence minister. Techworld. 10 November 2010.

2.North Atlantic Treaty Organization. Defending against cyber attacks. *Довідка*. URL: http://www.nato.int/cps/en/natolive/topics_49193.htm (дата звернення: 10.05.2023).

3.William D. Gerhard, Henry W. Millington Attack on a Sigint Collector. *National Security Agency/ Central Security Service*. 1981.

Вітенко Артем Юрійович – студент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: vitenkoartem7@gmail.com

Корнієнко Валерій Олександрович – доктор політичних наук, професор, завідувач кафедри соціально-політичних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: valkorney1958@gmail.com

Artem Vitenko – student of the Department of Information Security, Vinnytsia National Technical University, Vinnitsa, e-mail: vitenkoartem7@gmail.com

Kornienko Valerii – Dr. of Political Sciences, Professor, Head of the Department of Social and Political Sciences, Vinnytsia National Technical University, Vinnitsa, e-mail: valkorney1958@gmail.com