***Бєлоусова Н.Б.,*[*] *Афанасьєва П.А.*[**]**

ОСНОВНІ ВИМОГИ НАТО ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

This article deals with recommendations of NATO according providing security of information within the organization. The problem is to cope with cyber terrorism and to prevent harmful influence of cyber attacks for the States concerned. The task is to describe the measures of NATO for defense of cyber space of a government.

Key Words: NATO, information space, information security, cyber attacks, defense.

Ця стаття розглядає стандарти НАТО щодо забезпечення інформаційної безпеки в межах організації. Головною проблемою є боротьба з тероризмом та передбачення шкідливого впливу кібер атак на державний інформаційний простір. Метою є описання заходів НАТО для захисту кібернетичного простору.

Ключові слова: НАТО,інформаційний простір, інформаційна безпека, кібер атаки, захист.

Эта статья рассматривает стандарты НАТО для обеспечения информационной безопасности в границах организации. Главной проблемой является борьба с терроризмом и предупреждение вредоносного влияния кибер атак на государственное информационное пространство. Цель – описание принятых мер НАТО для защиты кибернетического пространства.

Ключевые слова: НАТО, информационное пространство, информационная безопасность, кибер атаки, защита.

Сьогодні інформаційна безпека нерозривно поєднує в собі аспекти національного та інтернаціонального характеру. Це підносить сутність проблеми захисту інформації на обидва рівня – внутрішній (самозбереження нації) та зовнішній (захист інформаційних потоків у глобальному довкіллі). Поширення інформації та зміщення кордонів приводить до того, що з кожним днем світ стає дедалі вразливішим. Світова спільнота стає все більш залежною від інформаційних систем та мереж передачі інформації. Терористичні атаки, спрямовані на інформаційну нішу, технічні негаразди або саботаж можуть викликати серйозні порушення функціонування систем, а також значні грошові втрати. Проблема стандартизування захисту інформації є важливим аспектом розвитку інформаційної безпеки, адже це забезпечить цілісність та непорушність кордонів інформаційного простору будь–якої держави. Метою цього дослідження є вивчення запропонованих НАТО стандартів щодо захисту інформації, визначення їх дієвості та актуальності в сучасному світі.

[*] кандидат політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

[**] студентка 4 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Глобалізація та стрімкий розвиток інформаційних систем дали істотне підґрунтя для розвитку тероризму. Міжнародний тероризм є потенційно дуже ефективним засобом ослаблення держави та підривання її стабільності. Він може мати два напрями – прямий і непрямий, де другий має більш істотний вплив на подальший розвиток ситуації. Вбити одного, але залякати тисячу – це матиме більший зміст, ніж проведення самого силового заходу. Засоби масової інформації створюють «віртуальний простір» для міжнародного тероризму, що також підсилює його непрямий вплив на світовий перебіг подій.

Цю проблематику активно розглядали багато науковців, серед яких треба виділити Таійе Ламбо, який видав низку статей з інформаційної безпеки, зокрема «Майбутнє інформаційної сертифікації» у 2006 році [1]. В роботі, яка має назву «Парадигми інформаційної безпеки», іспанський науковець Вісенте Ацеітуно Каналь розглядає проблему визначення поняття «Інформаційна безпека» та виділення основних правил задля її забезпечення [2]. Кент Андерсон, керівник відділу безпеки Network Risk LLC та член ISACA's CISM Certification Board, у своїй статті для журналу SC Magazine прогнозував майбутнє, яке чекає на сферу інформаційної безпеки [3]. Ще один науковець зі Сполучених Штатів Америки Гурпіт Диллон у 2007 році видав книгу «Принципи Безпеки Інформаційних Систем : теорія та випадки». У цій роботі розглядаються питання забезпечення інформаційної безпеки в межах світових кордонів [4]. Треба відмітити досягнення Російської Федерації в рамках вивчення інформаційного простору, та інформаційної безпеки зокрема. На теренах цієї держави виходить спеціалізований журнал «Information Security», який торкається всіх аспектів проблематики захисту проблематики інформаційного простору. Щодо вітчизняних науковців, то в цьому аспекті треба виділити Ігора Жданова та його «Можливі підходи до визначення основ державної політики забезпечення інформаційної безпеки України», де він акцентує увагу на інформаційний простір України [5].

Інформаційний простір (Information space) – це інтегральний електронний інформаційний простір, що створюється при використанні електронних мереж[6]. Поняття «інформаційний простір» не космічне (хоча повітряний і космічний простір можуть входити і входять до складу інформаційного поля), не географічне (хоча територія є його невід'ємною частиною), це поняття – соціально–політичне і вбирає в себе як територіальний, так і космічний фактори, а надто – людський, оскільки суспільна інформація призначається для людини, людина – її споживач, і без людини вона втрачає свій сенс. Коли йдеться про інформаційний простір держави, то його межі ототожнюються з державними кордонами, охоплюючи національні територію, акваторію і повітряний простір. Саме у цих сферах діють засоби інформації, які й інформують, тобто повідомляють, зображають, складають про що–небудь уявлення [7].

Державний інформаційний простір – надзвичайно важливе політичне поняття, яке у вартісній шкалі соціальних цінностей можна поставити на друге місце після державної незалежності. Держава зобов'язана забезпечити використання свого інформаційного поля в інтересах саме держави та її громадян. Якщо вона цього не зробить, то цей інформаційний простір буде використаний проти неї самої.

Основним принципом безпеки інформації НАТО є те, що інформація повинна зберігати свій ступінь захисту при всіх її передачах, починаючи з джерела, а контроль за розподілом і поширенням інформації повинний забезпечити відсутність її витоку, а також і те, що правила доступу до інформації повинні дозволяти використання інформації лише особам, яким вона потрібна для виконання службових обов’язків. Присвоєння інформації НАТО того або іншого грифа таємності виробляється відповідно до правил систем безпеки країн–учасниць.

Інформаційний вплив у XXI сторіччі спричинив достатньо велику кількість змін в інститутах національної безпеки, а також у підходах до питань оборони. І хоча вважається, що перші інформаційні війни мали місце ще у Стародавньому Єгипті, після Холодної Війни це поняття нерозривно поєднане з питаннями національної оборони [8].

Дмитро Шимків, Генеральний директор Microsoft Україна, зазначив: «Посилення залежності суспільства від інформаційних технологій приводить до того, що неавторизований доступ до інформації або навпаки, неможливість доступу до неї, є серйозними сучасними загрозами. Допомогти зрозуміти ці загрози та ефективно протидіяти їм на будь–якому рівні – державному, особистому або у бізнесі – це те є головним завданням для суспільства. Озброїти знаннями, щоб захистити – ось мета дій в області інформаційної безпеки» [9].

На заміну залізній зброї приходить зброя інформаційна. По своїй суті інформаційна війна є поєднанням дій, спрямованих на конфліктну ситуацію, коли інформація одночасно є зброєю, ресурсом та ціллю.

За Дмитром Тарасовим, науковцем, що спеціалізується на питанні інформаційних війн, інформаційна війна – це дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах [10].

Всі технічні дії, методи та технології, що використовуються для встановлення контролю над інформаційними структурами потенційного противника, втручання в роботу його систем управління та інформаційних мереж з метою знищення або модифікації даних, дезінформації або поширення інформації спеціального призначення у системах формування громадської думки і прийняття рішень, а також сукупність засобів впливу на свідомість і психологічний стан політичних і військових структур, спецслужб та населення для протидії можливим інформаційним впливам іншої сторони отримали загальну назву інформаційна зброя [11].

Глобалізація та стрімкий розвиток інформаційних систем дали істотне підґрунтя для розвитку тероризму. Міжнародний тероризм є потенційно дуже ефективним засобом ослаблення держави та підривання її стабільності. Він може мати два напрями – прямий і непрямий, де другий має більш істотний вплив на подальший розвиток ситуації. Вбити одного, але залякати тисячу – це матиме більший зміст, ніж проведення самого силового заходу. Засоби масової інформації створюють «віртуальний простір» для міжнародного тероризму, що також підсилює його непрямий вплив на світовий перебіг подій.

У зв'язку з появою таких ризиків в сфері оборони та безпеки відбувається поєднання прямих і непрямих методів протидії, які відмінні від оригінальних військово–політичних концепцій, з метою досягнення політичних цілей.

Як було зазначено у стратегічному дослідженні групи експертів НАТО (на чолі з Мадлен К. Олбрайт (США)), НАТО повинна прискорити свою діяльність з реагування на небезпеку кібернападів, захищаючи власні системи зв'язку і управління, допомагаючи союзникам по Альянсу удосконалити свою здатність запобігати нападам і відновлюватися після них, і розвивати сили і засоби кіберзахисту з метою ефективного виявлення і стримування кібернетичних атак [12].

Питанням забезпечення безпеки в інформаційному просторі задаються майже всі держави та високо посадовці. Так, Міністр Оборони Великобританії Нік Харві посилається на статтю V Пакту НАТО про Взаємну оборону, що саме стосується актів агресії кіберпросторі. Використання інформаційного простору терористами може стати більш систе-

матичним, що призведе до негативних наслідків для всього світу. Не допустити такого розвитку подій і є важливим завданням для Альянсу [13].

У 2010 році на Лісабонському саміті НАТО було вирішено розробити нову політику НАТО з кіберзахисту, а також розробити конкретний план дій, який набуде чинності з червня 2011 року. НАТО планує використовувати процеси оборонного планування з метою сприяння розвитку захисту від кіберзлочинності для союзників, а також для оптимізації взаємодії, співпраці та обміну інформацією. НАТО тісно співпрацює за країнами ЄС та з ООН для вирішення питань небезпеки, що виникає у кіберпросторі [14].

Кібер–атаки стають все більш частими, більш організованими і більш збитковими для державних установ, підприємств, економіки і, можливо, також транспортній та електричній мережам та інших об'єктів критичної інфраструктури; вони можуть досягти критичного рівня, який загрожує національному та Євроатлантичному процвітанню, безпеці і стабільності. Джерелом таких атак можуть бути іноземні військові та розвідувальні служби, організовані злочинні угруповання, терористичні та/або екстремістські групи [15].

Захист від кібернетичних атак є важливою ланкою розробок НАТО. Були сформовані стандарти НАТО щодо захисту інформації , мінімальні з яких містять вимоги зі збереження, передачі та обробки інформації. Ключовим терміном в цьому аспекті є «керування ризиком», тобто незалежна оцінка уразливості інформації, а також проведення контрзаходів з цього приводу. Для розуміння важливості захисту інформації, потрібно чітко уявляти розміри вартості можливих збитків при витоку інформації, і враховувати відповідність затрат необхідних ресурсів для захисту інформації.

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 ту, доступ до якої з тих чи інших причин обмежується. В англомовній традиції їй відповідає поняття «вразлива інформація» (sensitive), тобто інформація, яка вразлива до загроз, що виникають у зв'язку з несанкціонованим доступом до неї, і тому потребує захисту або хоча б обмеження доступу до неї. 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) [16]. 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.

Питання забезпечення захисту інформації входять до юрисдикції Комітету внутрішньої безпеки НАТО (NSC), який є дорадчим органом при Північноатлантичній Раді, з питань, що стосуються безпеки НАТО. Головою Комітету є директор Служби безпеки НАТО (NOS), яка надає підтримку Комітету з боку Міжнародного секретаріату НАТО. Комітету внутрішньої безпеки також підпорядкована Робоча група з питань гарантування безпеки автоматичної обробки даних [17].

НАТО вимагає від країни–члена створити національний уповноважений орган, відповідальний за безпеку таємної інформації, через який Служба безпеки НАТО здійснює контакти з країною. Усередині НАТО національний уповноважений орган по безпеці ін-

формації виконує функції керівництва створенням органа правління та режимних відділів, забезпечення безпеки таємної інформації НАТО у всіх установах, що знаходяться під її юрисдикцією, як всередині країни, так і за її межами, забезпечення розробки планів захисту інформації в разі виникнення надзвичайних обставин, з метою запобігання втрати конфіденційності таємної інформації НАТО.

Представники національного уповноваженого органа по безпеці інформації беруть участь у нарадах Комітету безпеки НАТО, на яких виробляються політика й інструкції в області безпеки. Є країни НАТО, в яких уповноважений орган по безпеці інформації знаходиться в міністерстві закордонних справ, оборони і юстиції. В інших країнах керівником уповноваженого органа по безпеці є прем'єр–міністр, міністр оборони або міністр внутрішніх справ. На обсяг функцій відповідального уповноваженого впливають розмір країни і кількість населення, географічне розташування місць обробки таємної інформації і не в останню чергу, розподіл повноважень між органами в області національної безпеки. Часто значна частина функцій відповідального уповноваженого делегується в міністерство оборони.

Сьогодні пріоритетним є впровадження найсучасніших систем спостереження і засобів обробки інформації і зв'язку. Тематичні публікації останніх років зазначають також, що у перспективі НАТО треба зосереджувати свою увагу на визначення довгострокових перспектив як впливової міжнародної організації. Витрати на утримання інформаційно–комунікаційних систем в межах НАТО покриваються коштами з бюджету Програми інвестицій у безпеку НАТО. В останні роки було відмічено, що змістився наголос у проведенні кібернетичних атак. Сьогодні це більше порушення конфіденційності інформації, ніж порушення цілісного викладу інформації в мережі. В основному це відбувається шляхом збору інформації лише для службового користування, читання пошти тощо. Збитки від проведення таких кібернетичних атак складають майже мільярд доларів США, що є надзвичайно великою сумою в цьому контексті.

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, оновлення технічної бази для забезпечення захисту інформації в цій сфері є також важливими заходами на шляху до формування державної інформаційної безпеки. Якщо до цього буде приєднана також ефектна протидія інформаційній експансії та спробам використання національного інформаційного простору, можна буде сказати, що держава обрала вірний шлях боротьби з кіберзлочинністю.

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.

НАТО виокремлює необхідність визначення спільних підходів з країнами до використання сучасних систем захисту інформації з урахуванням вимог інформаційної безпеки

країни. Забезпечення режиму захисту інформації в разі створення спільних інформаційних та телекомунікаційних систем, в яких циркулюватиме інформація з обмеженим доступом, відбувається шляхом розроблення пропозицій щодо захисту конфіденційного зв'язку з використанням обладнання НАТО, необхідного для створення сумісних з НАТО відокремлених інформаційно–комунікаційних систем в органах виконавчої влади, а також підвищенням кваліфікації фахівців органів виконавчої влади з питань захисту інформації у рамках заходів Програми «Партнерство заради миру» [18].

НАТО виокремлює необхідність здійснення зусиль задля посилення моніторингу критично важливих мереж в межах Альянсу та оцінки і зміцнення виявлених слабких місць. Центр передового досвіду має робити більше за допомогою навчання, допомоги країнам–членам поліпшувати свої програми для захисту від кібернетичних атак, а союзники мають розширювати свої засоби раннього попередження у формі загальної мережі моніторингових вузлів і сенсорів [19].

Альянс не виключає необхідності швидкого реагування на кібернетичні атаки шляхом надсилання групи експертів до будь–якої країни–члена, що постраждала від кібернападу, або до країни, яка відчуває загрозу вторгнення у її інформаційний простір. З часом, НАТО планує забезпечити себе повністю відповідним набором засобів кіберзахисту, включно з пасивними та активними елементами.

Інформаційно–психологічна боротьба велася протягом всього існування людства. Зміст її в основному полягав у поширенні дезінформації однією чи двома сторонами конфлікту, тенденційної інформації для впливу на оцінки, наміри та орієнтацію населення, особового складу військових сил та осіб, які приймають рішення, з метою формування громадської думки на користь діючої сторони. Аналіз впливу інформаційного протистояння на сучасні міжнародні відносини, дозволяє зробити висновки щодо покращення інформаційної безпеки в державах світу в XXI столітті. Розвиток інформаційних технологій веде до глобальних змін у політичній, економічній, військовій та культурній сферах. На думку західних і вітчизняних політологів, це саме і призводить в першій чверті XXI століття до кардинальних змін самого способу протиборства в міжнародних відносинах. Інформаційне протиборство було й залишається супутником міждержавного спілкування.

В контексті захисту інформації неможливо не говорити про роль НАТО в цій боротьбі. Альянс не поодинокий в прагненні досягти цілковитої безпеки інформаційного простору, але його поєднання військового загалу та і засад політичної солідарності однозначно робить його незамінним учасником на шляху до забезпечення захисту від кіберзлочинності. Без участі НАТО у майбутньому перспективи міжнародної стабільності та миру були б набагато менш вірогідними, ніж вони є на сьогоднішній день.

НАТО існує як джерело надії ще і тому, що з самого початку його члени виокремили для себе наступні питання, що є головними у діяльності кожної держави: зміцнити міжнародну безпеку; захистити свободу; сприяти верховенству права. Ці цілі не прив'язані до жодного календаря і не применшуються внаслідок технічного прогресу. Вони не стосуються жодного конкретного супротивника. Це постійні потреби і будуть існувати стільки, скільки НАТО матиме хоробрості захищати їх за допомогою єдності своїх членів, хоробрості своїх громадян і вільного виразу своєї колективної волі.

Інформаційна війна використовує переваги технологічного прогресу. З процесом глобалізації будуть вдосконалюватися засоби впливу на інформаційний простір держави, а також заходи, направлені на порушення цілісності інформаційного кордону. Інформаційна безпека має на увазі під собою забезпечення захисту інформації і інфраструктури, що здійснює її підтримку від будь–якого випадкового або ж зловмисного втручання, в результаті

якого може бути нанесений утрата інформації в цілому, її безпосереднім власникам і інфраструктурі, що підтримує її зберігання і існування. Інформаційна безпека виконує завдання, пов'язані з прогнозуванням і запобіганням можливим діям подібного роду, а також зводить до мінімуму можливий збиток.

Література

1. Taiye Lambo The Future of infosec certification. / Lambo Taiye – ISSA Journal – November, 2006.
2. Vicente Aceituno Canal On Information Security Paradigms. / Canal Vicente Aceituno – The Global Voice of Information Security – September 2005.
3. Kent Anderson IT security professionals must evolve for changing market. / Anderson Kent – SC Magazine – 12 October 2006.
4. Gurpeet Dhillon Principles of Information Systems Security: text and cases. / Dhillon, Gurpreet – NY: John Wiley & Sons – 2007.
5. Жданов І. Можливі підходи до визначення основ державної політики забезпечення інформаційної безпеки України / Матеріали до круглого столу «Безпека інформації в інформаційно–телекомунікаційних системах». – К., 2001. – 28 трав.
6. Институт по связям с общественностью РИСО [Електронний ресурс] / Гусаковский А. Иллюзия восприятия или «PR как фактор угрозы корпоративной безопасности» / А. Гусаковский – 2007. – Режим доступу: http://www.rpri.ru/materials/gusakovskii3.htm
7. Почепцов Г. Паблик рилейшнз, или как успешно управлять общественным мнением / Г. Почепцов. – М.: Центр, 1998. – 349 с.
8. Кормич Б.А. Інформаційна безпека: організаційно–правові основи: Навч. посібник. – К.: Кондор, 2004. – 384 с.
9. Асоціація підприємств інформаційних технологій України [Електронний ресурс] / Руденко Т. Американська торгівельна палата в Україні за підтримки Microsoft провела конференцію з інформаційної безпеки / Тетяна Руденко. – 11 грудня 2009. – Режим доступу: http://apitu.org.ua/node/1300
10. Тарасов Д.О. Моделювання інформаційної інфраструктури комп'ютерних мережі та інформаційна безпека / Інформаційні системи та мережі. Вісник НУ «Львівська політехніка» №464. – Львів 2002. – С. 302–311
11. Прокофьєва Д.М. Інформаційна війна та інформаційна злочинність [Електронний ресурс] / Д. М. Прокофьева – 2008. – Режим доступу: http://www.crime–research.iatp.org.ua/library/Prokop.htm
12. Аналіз і рекомендації групи експертів з розроблення нової стратегічної концепції для НАТО. НАТО 2020: упевненість у безпеці. Динамічні підходи – Група експертів – 17 травня 2010.
13. John E Dunn. NATO clause V could deter cyberattack, says defence minister./ Dunn John E – Techworld. – 10 November 2010
14. North Atlantic Treaty Organization. Defending against cyber attacks [Електронний ресурс]/ Довідка. – Режим доступу: http://www.nato.int/cps/en/natolive/topics_49193.htm
15. North Atlantic Treaty Organization. Active Engagement. [Електронний ресурс]/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. / Режим доступу: http://www.nato.int/lisbon2010/strategic–concept–2010–eng.pdf
16. William D. Gerhard, Henry W. Millington Attack on a Sigint Collector./ Gerhard William D., Millington Henry W. – National Security Agency/ Central Security Service. – 1981

17. Структура НАТО [Електронний ресурс]/ Довідка. – Режим доступу: http://nato.host–ua.org.ua/Stryktyra_NATO.html
18. Міністерство Інфраструктури України [Електронний ресурс]/Євроатлантична інтеграція. – 3 липня 2008. – Режим доступу: http://www.mintrans.gov.ua/uk/integration/ 65.html
19. The Associated Press (Bucharest, Romania). NATO Officials Want Romania to Exclude Some Former Communists from Intelligence Positions. – March 20, 2002.