/en/dataprot /directiv/directiv.html. ***6.*** *Директива 97/66/ЄС Європейського парламенту та Ради "Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі" від 15. 12. 1997 р. //www.evropa.eu. int/ISPO/legal/en/ dataprot/protection.html.* ***7.*** *Директива 96/9/ЄС Європейського парламенту та Ради "Про правовий захист баз даних" від 11. 03. 1996 р. //www.evropa.eu.int/ISPO.* ***8.*** *Решение Конституційного Суду № 15-АВ от 13 квітня 1991 року //*www.privacy.*org/ pi/coun tries/hungary/hungarian_id_decision_1991.html.* ***9.*** *Стаття 35 (5) Конституції Республіки Португалія 1976 року //www.parlamento.pt/ leis/constituicao_ingles/crp_uk.htm#article_35.* ***10.*** *Національні ідентифікаційні картки (посвідчення особи). Заява Privacy internetional для Комітету Парламенту Канади з питань громадянства та імміграції від 04.10.2003 р. // "Свобода висловлювань та приватність". – 2003. – № 1.* ***11.*** *Введення біометричних показників в паспортb в країнах ЄС //www.evropa.eu.int/eur-lex/en/com/pdf/2004/com2004_0116en01.pdf.*

УДК 340.5:351.86

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ НАТО

Володимир Сідак, Володимир Артемов

Інститут захисту інформації з обмеженим доступом Національної академії Служби безпеки України

Анотація: **Досліджена структура INFOSEC, основні напрями й тенденції щодо організаційно-правових засад регулювання обігу інформації з обмеженим доступом у інформаційно-комунікаційних мережах НАТО, головні завдання стандартизації у цій сфері.**

Summary: **INFOSEC Structure end Main Tendency of NATO Network Security Legal Regulation have been analyzed. The primary problems of standardizing in this sphere are reviewed.**

Ключові слова: **Захист інформації з обмеженим доступом, інформаційно-комунікаційні мережі, НАТО, INFOSEC.**

Вступ

Розходження в нормах національних правових систем суттєво перешкоджають розвитку та поглибленню широкого міжнародного співробітництва з багатьох суттєвих питань. Зокрема, країни Північноатлантичного договору вимагають від своїх партнерів, і передусім абітурієнтів, ретельного дотримання стандартів та вимог Альянсу щодо захисту інформації. Безумовно, це неможливо без врахування країнами-кандидатами основних принципів політики НАТО.

Політика інформаційної безпеки НАТО потребує, щоб уся інформація, як класифікована, так і не класифікована, що належить НАТО, незалежно від формату та виду носія, на якому вона розміщена, захищалася так, щоб протягом всього її життєвого циклу забезпечувалася її конфіденційність, цілісність та доступність [1].

Крім того, в Альянсі має забезпечуватись цілісність та доступність джерел інформації та систем підтримки.

Политика безпеки НАТО потребує таких заходів, які б, у будь-якому разі, забезпечували наступне:

- ідентифікацію та аутентифікацію інформації;
- конфіденційність механізмів захисту інформації;
- механізми попередження та виявлення порушень та відновлення інформації;
- реалізацію принципу «необхідно знати» (Need-to-Know).

Важливим є і те, що політика НАТО в галузі інформаційно-комунікативних технологій рекомендує широке використання (наскільки це можливо) комерційних продуктів і технологій. Це не поширюється на криптографічні вироби та технології, де приймати рішення та робити вибір повинні національні уряди.

Основна частина

У зв'язку з вищевикладеним доцільно розглянути політику НАТО стосовно використання інформаційно-комунікаційних технологій та мереж.

Процедури захисту конфедіційності, цілісності, готовності та звітності щодо інформації, яка передається і обробляються за допомогою інформаційно-комунікаційних технологій, регулюються документом "Попередня директива з INFOSEC", який був оприлюднений Комітетом безпеки НАТО та

Комітетом політики з питань консультації, командування і контролю (далі – С3). Основне завдання INFOSEC – організаційне та нормативне-правове регулювання захисту інформації НАТО, яка циркулює у інформаційно-комунікаційних мережах. [2]

Органами INFOSEC в структурі НАТО є:

- управління С3;
- робоча група INFOSEC у складі NCS;
- підкомітет INFOSEC;
- командування NACOSA/INFOSEC (яке відповідає за криптографічний захист та захист від витоків інформації через випромінювання або іманацію – TEMPEST);
- установа INFOSEC з акредитації комунікаційного обладнання НАТО – SAA (Security Accreditation Authority).
- Національним органом INFOSEC у кожній країні НАТО мають бути:
- національне управління з інформаційно-комунікаційних систем;
- національне представництво з безпеки комунікаційних мереж – NCSA (National Communication Security Authority);
- національне представництво з дистрибюції – NDA (National Distribution Authority);
- національне управління з акредитації комунікаційного обладнання (SAA), визнане НАТО.

Під час передачі засобами інформаційно-комунікаційних технологій інформація з грифом:

- “НАТО/Цілком таємно” і вище захищається за допомогою криптографічних методів або продуктів, затверджених Військовим комітетом НАТО (NAMILCOM);

- “НАТО/Таємно” і “НАТО/Для службового користування” захищається за допомогою криптографічних методів або продуктів, затверджених Військовим комітетом НАТО (NAMILCOM) або державою-членом НАТО, за винятком випадків, коли такий метод або продукт є спільно консолідований (він затверджується NAMILCOM).

Під час передачі в межах систем держав, які не є членами НАТО/міжнародних організацій (NNN/IO), конфіденційність засекреченої інформації з грифом “НАТО/Цілком таємно” і вище захищається за допомогою затверджених Військовим комітетом НАТО криптографічних методів або продуктів. Протягом передачі в мережах країн-не членів конфіденційність засекреченої інформації з грифами “НАТО/Таємно” і “НАТО/Для службового користування” захищається за допомогою оцінених і затверджених відповідним органом криптографічних методів або продуктів. Таким відповідним органом може бути Військовий комітет НАТО, Орган безпеки національних комунікаційних систем держави-члена НАТО або рівнозначний орган NNN/IO, який обумовлює, що країна-не член володіє структурами, правилами, процедурами, доречними для оцінки, відбору, затвердження і контролю таких методів або продуктів. Такі структури, правила і процедури узгоджуються між країнами членами і не членами НАТО [3].

Для захисту проти компрометації інформації з грифом “НАТО/Таємно” і вище внаслідок ненавмисного електромагнітного випромінювання передбачається використання заходів безпеки. Такі заходи співрозмірні з ризиком використання і точним характером інформації.

Як вищий Комітет політики з питань консультації, командування і контролю в межах Альянсу, NC3B підтримує Військовий комітет НАТО та політичні організації НАТО в процесі ратифікації шляхів розвитку і планування С3 через перегляд діючих вимог С3. NC3B відповідальний за постачання безпечних і взаємодіючих в НАТО систем.

Кожна держава-член НАТО встановлює Національний орган безпеки комунікаційних систем (NCSA). Першочергова роль NCSA полягає в наступному:

- контроль за криптографічною технічною інформацією, яка стосується захисту інформації НАТО в межах власної держави;
- забезпечення гарантії, що криптографічні системи, продукти та механізми для захисту інформації НАТО ефективно і раціонально відібрані, керовані і підтримувані;
- повідомлення про безпеку комунікаційних систем НАТО та споріднені технічні справи INFOSEC, як цивільні, так і військові, відповідному органу НАТО або державному органу.

Схема типової ланки інформаційно-комунікаційної системи НАТО складається із домену користувача, мережного домену та мережної інфраструктури забезпечення безпеки. При цьому INFOSEC виділяє стаціонарних, дистантних (віддалених), розподілених та мобільних користувачів та партнерів, які беруть участь в обміні. У мережевому домені НАТО зазвичай використовуються декілька типів мереж для того, щоб забезпечити необхідний трафік та доступність. Ці мережі включають Інтернет, мережі національних

оборонних відомств, NGCS[2] або PSTN[3]. Жодна з цих мереж, окрім NGCS, не контролюється НАТО та, відповідно, їм не може бути наданий такий же захист, який надається мережам, що знаходяться у повному розпорядженні НАТО.

При цьому конфіденційність інформації НАТО досягається за рахунок її шифрування ще до передачі мережею. Те ж саме стосується цілісності і доступності, які досягаються на прикладному рівні.

Фізична безпека комунікаційних та інформаційних систем (COMMUNICATION AND INFORMATION SYSTEMS – CIS) забезпечується шляхом захисту територій. Території, на яких класифікована інформація НАТО циркулює з використанням інформаційних технологій, або там, де доступ до такої інформації потенційно можливий, облаштовуються таким чином, щоб відповідати сукупності вимог конфіденційності, цілісності і придатності. Території, на яких комунікаційні та інформаційні системи використовуються для збереження, відображення, обробки та передачі класифікованої інформації з грифом "CONFIDENTIAL" і вище, або там, де потенційний доступ до такої інформації можливий, створюються як зони безпеки НАТО класу I або класу II. Території, на яких комунікаційні та інформаційні системи використовуються для збереження, відображення, обробки та передачі класифікованої інформації з грифом "RESTRICTED", або там, де потенційний доступ до такої інформації можливий, створюються як адміністративні зони.

Реалізація безпечної мережної архітектури потребує виконання деяких правил.

Перше з них полягає у виконанні загальних критеріїв безпеки.

Друге пов'язане із запровадженням системи захисту від комп'ютерних інцидентів (збоїв). В результаті збільшення обсягів зв'язку з військовими та цивільними організаціями НАТО стикається з необхідністю захищати інформацію, джерела та системи підтримки від комп'ютерних інцидентів. Захист критичних ресурсів інформаційно-комунікаційних систем потребує не лише здійснення захисних заходів безпосередньо під час передачі або обробки інформації, але й спроможності попереджувати, виявляти, реагувати та виправляти наслідки комп'ютерних інцидентів.

Третє полягає у забезпеченні безпечного та ефективного управління інформацією. Це означає, зокрема, що будь-яка особа у межах НАТО повинна мати вільний доступ до інформації (з урахуванням принципу «Need-to-Know") та можливість безпечного обміну інформацією без істотних затримок, без порушення цілісності та конфіденційності. Ці можливості забезпечуються за рахунок досягнень сучасної криптографії.

Реалізація загальних критеріїв безпеки інформаційно-комунікаційних мереж НАТО починається із встановлення експлуатаційних вимог SOR (Statement of Operational Requirement). Ці вимоги з урахуванням директив та керівних принципів політики безпеки відображаються у архітектурі С3 систем покриття (NC3S Overarching Architecture). Опис архітектури NC3S задокументований у документі NC3S Reference Architecture. Вимоги з безпеки наводяться у спеціальному додатку до загальних технічних вимог. Положення, викладені в документі NC3S Reference Architecture, відбиваються в архітектурі конкретного проекту (NC3S Target Architecture).

Відповідність проекту ділянки інформаційно-комунікаційної мережі НАТО (NC3S Target Architecture) вимогам INFOSEC є основою для акредитації цієї ділянки в загальній системі комунікацій НАТО. Існує також концепція загальних критеріїв CC (Common Criteria). Їй відповідає таке поняття як профіль захисту (Protection Profile), тобто пакет функціональних характеристик, які гарантують якість захисту. Наявність таких профілів дозволяє:

- знаходити у репозитарії готових програмно-технічних рішень, які можуть відповідати вимогам конкретного проекту;
- формулювати замовлення на проведення тендеру на розробку проекту, якщо у репозитарії не знайшлося відповідного рішення;
- після завершення проекту включити його у репозитарій готових проектів.

З викладеного випливає, що НАТО не потребує розробки кожного разу нового проекту. Проект може бути виконаний на основі профілів та пакетів, що існують у комерційному секторі та доступні як членам НАТО, так і іншим країнам. Однак, частіше НАТО пред'являє більш високі вимоги. Крім того, НАТО зазвичай потребує використання криптографічних виробів у доповнення до звичайних комерційних профілів.

Загальні критерії інформаційної безпеки НАТО засновані на довірчих критеріях оцінки комп'ютерної безпеки TCSEC (Trusted Computer Security Evaluation Criteria). Існує порядок використання загальних критеріїв інформаційної безпеки НАТО. Порядок ідентифікує документацію, яка потрібна для прийняття

[2] NGCS (Next Generation Computer Solution) – компьютерные решения нового поколения

[3] PSTN (Public Switch Telephone Network) – общественные телефонные коммутируемые линии связи

рішень, процеси створення, перевірки, оцінки та сертифікації профілів та пакетів захисту, а також процедури використання та наповнення архіву (репозитарія) профілів та пакетів захисту.

Оцінка та сертифікація профілів та пакетів має бути виконана або органом країни-члена НАТО, спеціально аккредитованим для цих цілей, або одною з організацій НАТО (наприклад, SECAN та EUSEC). Репозитарий НАТО базується на вимогах стандарту ISO/IEC 15292 "Процедури реєстрації профілів захисту". При цьому повинні існувати два репозитария: один для класифікованої інформації (з урахуванням принципу «Need-to-Knew"), інший – для загального використання [4].

План використання загальних критеріїв передбачає наступні процедури:

- НАТО реєструє вироби, що забезпечують безпеку, у списку продуктів НАТО;
- якщо необхідний виріб створений або вже існує, його використання для конкретного проекту має бути підтверджено уповноваженим органом та зареєстровано у списку продуктів НАТО;
- якщо продукт існує, але його сертифікація відсутня або знаходиться у процесі виробництва, НАТО потребує його сертифікації акредитованим органом країни-члена НАТО або однієї з організацій НАТО (наприклад SECAN та EUSEC), що володіє відповідними технічними засобами та технологіями; як тільки оцінка та сертифікація виконані, продукт повинен бути схвалений SAA та зареєстрований.

На тепер НАТО знаходиться у стадії переходу від критеріїв довірчої оцінки комп'ютерної безпеки (NTCSEC) до загальних критеріїв (CC) для нових проектів та надбань. Остаточні рішення містяться у документі CC2 Q. Він встановлює процеси та процедури стосовно всього життєвого циклу інформаційно-комунікаційних систем, включаючи твердження технічних вимог, замовної документації та документації з оцінці та сертифікації.

Стандарти НАТО покликані забезпечувати лише найбільш доцільні та обов'язкові вимоги безпеки. Існує багато шляхів забезпечення інформаційної безпеки, та альянс не припускає в таких питаннях диктат, бо вважає, що для нього краще, якщо кожна суверенна нація обере свій шлях. Важливо, щоб у результаті була досягнута обумовлена мета у питаннях оборони та безпеки.

Подальший розвиток стандартизації ще нещодавно не був проблемою. Але бажання відкрити доступ до НАТО новим членам з Центральної та Східної Європи, допомогти їм перетворити їх суспільну та воєнно-політичну структуру змушують НАТО знову повертатися до питань стандартизації. Процеси планування стають все більш важливими та кількість угод із стандартизації між партнерами постійно збільшується. Виникає питання – чи можливо прискорити процес інтеграції та розширення НАТО або зробити його більш ефективним за рахунок стандартизації? Чи є доцільним використання набору жорстких принципів та критеріїв стандартизації, співрозмірних з умовами НАТО?

Але, як мінімум, НАТО потребує забезпечення ефективного механізму ідентифікації, контролю та відкритого визначення того, як виконуються вимоги НАТО стосовно інформаційної безпеки у інформаційно-комунікаційних мережах [5].

Висновок

Чим більша кількість країн-членів НАТО перетворює свої армії на сучасні боєспроможні та життєспроможні збройні сили, тим далі вони повинні просуватися шляхом спеціалізації своїх збройних сил. Чим далі країни-члени НАТО просуваються цим шляхом, тим важливішою стає вимога, щоб всі вони притримувалися стандартів та критеріїв, на які погодилися.

Оскільки критерії та стандарти цілком безсумнівні, то дослідження з проблем стандартизації в галузі інформаційної безпеки НАТО повинні проводитися обережно і з урахуванням розуміння всього комплексу факторів.

Однак прийняття стандартів та критеріїв не повинно протирічити сутності НАТО. Це особливо важливо в чутливій сфері демократичного контролю збройних сил. Націям необхідно дозволити використовувати якнайбільше шляхів, що задовольняють індивідуальні культурні та політичні обставини. Важно визначити нові параметри для оцінки результатів, що забезпечують реалізацію реалістичних та корисних цілей, на які націлюються претенденти. Стандарти повинні бути суворими, але не жорсткими. Обов'язок тих, хто відповідає за вибір способів захисту інформаційної безпеки, забезпечити контроль не лише збройних сил, але також і надзвичайно широкого діапазону діяльності різних міністерств – економіки, фінансів, внутрішніх справ, юстиції, транспорту, належне функціонування яких необхідно для безпеки нації.

Література: ***1.*** *Директива з управління безпекою електронної інформації для комунікаційно-інформаційних систем // Cornell International Law Journal 26, No. 2 (May 2003);* ***2.*** *Al. S.Roberts Nato's security of information policy and the entrenchment of State Secrecy. // Reports Basic Newsletter on Internal International Security October 2003 №. 76;* ***3.*** *Асландер Робертс. Нато, секретность и право на информацию. // Reports*

Basic Newsletter on Internal International Security October 2005 №. 6; ***4.*** *Україна на шляху до НАТО: через радикальні реформи до набуття членства: кол. авторів // Під ред. Г. М. Перепелиці. – К. 2004. – С. 300 – 385;* ***5.*** *Будаков М .О. Організаційно-правові засади діяльності спеціальних служб держав НАТО. // Вид. НА СБ України. – К. 2004; Бахин В. С. Интегральные конвенции как способ унификации национального законодательства // Господарство, підприємство і право. – 2003. – № 7. – С. 73 – 79; Харитонова О. І., Харитонов Е. О. Порівняльне право Європи: Основи порівняльного правознавства. європейські традиції. – Х., 2002.*

УДК 35.078:342.738

СИСТЕМА ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ. ІСТОРИЧНИЙ АСПЕКТ

Олександр Ботвінкін
Інститут захисту інформації з обмеженим доступом Національної академії СБ України

Анотація: *Розглядаються питання, пов'язані з формуванням системи охорони державної таємниці на території України.*
Summary: *Questions related to formation of system of the state secrets protection in Ukraine's territory are considered.*
Ключові слова: *Охорона державної таємниці, система охорони державної таємниці.*

Вступ

Національна система охорони державної таємниці створювалась з урахуванням досвіду розвинених демократичних країн та випробуваних на практиці традиційних засобів і методів. Значною мірою сучасна Україна є спадкоємцем системи захисту секретної інформації, яка існувала за часів Радянського Союзу. Більшість елементів цієї структури було збережено, а згодом розвинуто і вдосконалено.

Заходи, які вживає держава, охороняючи свої секрети, мають бути адекватними загрозам (як зовнішнім, так і внутрішнім), що існують на даний момент. Ефективне вирішення цього питання можливе лише за умови комплексного підходу. Зрозуміло, що комплексний підхід включає дослідження виникнення потреби в охороні державної таємниці взагалі та особливостей формування цієї системи на території України зокрема, пізнання сутності, змісту та закономірностей розвитку системи охорони державної таємниці на різних етапах державного розвитку України. Крім того, для сучасної юридичної практики є важливим вивчення досвіду правового забезпечення функціонування системи охорони державної таємниці на території України протягом історичного періоду його впровадження.

Отже, з метою з'ясування певних закономірностей та тенденцій розвитку системи збереження секретів та використання досвіду історичних аналогій на сучасному етапі розбудови цієї системи актуальним і, безперечно, доцільним є використання історичного аналізу цієї проблеми.

Формування системи охорони державної таємниці передбачає запровадження системи взаємодіючих адміністративно-правових режимів, функції яких, в тій чи іншій мірі, направлені на охорону державної таємниці. Запровадження ж відповідних режимів передбачає нормативно-правове регулювання відносин у цій сфері та створення державних органів, діяльність яких направлена на вирішення конкретних завдань з забезпечення вказаних режимів.

На сьогодні наукових робіт, присвячених історії збереження секретної інформації в Україні, немає. За часів СРСР про діяльність зі збереження державної таємниці йшлося в дослідженнях, присвячених історії органів держбезпеки, окремих аспектів цієї проблеми торкались науковці і в наші дні, серед них В. Козенюк [1, 2], В. Окіпнюк [3], В. Пилипчук [4, 5], С. Пупко [6], О. Шамсутдінов [7] та ін.

Вивченням історії створення системи захисту державної таємниці в СРСР переймається російський дослідник С. Чертопруд [8, 9], відомі дослідження історії органів цензури колишнього СРСР Т. Горяєвої [10] та ін. Загалом матеріал за цією тематикою в науковій літературі подано з позиції існуючого тоді СРСР. В сучасних умовах він має бути проаналізований з акцентом на особливості діяльності державних органів саме в Україні.

Прослідкуємо, як відбувалось становлення органів захисту секретної інформації в Україні.

Основна частина

Незважаючи на окремі організаційно-правові заходи охорони державної таємниці ефективної цілісної