УДК 340.5:351.86 **Артемов В.Ю.**

КЛАСИФІКАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ НАТО

Аналіз доступних джерел свідчить про відсутність чіткої класифікації правових норм НАТО з питань захисту інформації з обмеженим доступом.

Побудова такої класифікації актуальна не лише тому, що класифікація є необхідною умовою існування та доцільного розвитку будь-яких знань, але ще й тому, що наявність чіткої класифікації правових норм НАТО з питань захисту інформації з обмеженим доступом сприятиме реалізації євроатлантичних спрямувань України у сучасному світі. Це дозволить коректно провести порівняльний правовий аналіз законодавчих норм захисту інформації з обмеженим доступом в країнах Центральної та Східної Європи з тим, щоб у майбутньому обирати оптимальні шляхи трансформації стандартів НАТО у внутрішньодержавне право України.

Головною проблемою, яка виникає при цьому, є виділення суттєвих ознак та природних підстав для розділення всього розмаїття правових норм та правил захисту інформації, які діють в цих країнах.

Рішенню цієї проблеми сприяє загальна теорія класифікації [1-2]. Головною філософською проблемою, яку вирішує ця теорія, є обгрунтування вибору природних підстав та виділення суттєвих ознак явищ та об'єктів, що класифікуються. Існують три основних методи у загальній теорії класифікації: дискримінантний аналіз, кластерний аналіз та метод групування.

У дискримінантному аналізі класи вбачаються заданими, а завдання полягає в тому, щоб віднести об'єкти, що класифікуються до одного з цих класів. При кластеризації та групуванні метою є виявлення та виділення класів об'єктів, що класифікуються. Якщо завданням є виділення класів, що суттєво різняться один від одного, то застосовують кластер-аналіз. Якщо природні підстави не вимагають чіткого відокремлювання класів, то використовуються методи групування

Цілком очевидно, що природною основою для класифікації правових норм НАТО з питань захисту інформації з обмеженим доступом у нашому випадку мають стати види захисту інформації та способи їх реалізації.

На жаль, офіційно прийнята класифікація видів та способів захисту інформації в НАТО також відсутня. Але суттєвим є те, що НАТО відрізняє чутливу (sensitive) інформацію, тобто таку, від якої залежить або може залежати безпека НАТО, і інформацію, від якої безпека НАТО не залежить (unsensitive).

У свою чергу чутлива інформація може бути класифікованою (classified), тобто такою, на яку накладено гриф і яка внесена до реєстру, і таку, на яку відповідний гриф не накладено, але вона є чутливою (unclassified but sensitive). Норми щодо захисту класифікованої інформації в НАТО викладені у документі C-M(2002)49 , а норми захисту некласифікованої але чутливої інформації - у документі C-M(2002)60 [3].

Цим законодавство НАТО суттєво відрізняється від України, де відсутня категорія чутливої інформації, поруч з терміном "інформація з обмеженим доступом" використовується термін "засекречена інформація", а з усього розмаїття способів захисту інформації окремо виділяються лише технічні.

Деяке уявлення про види та способи захисту інформації в НАТО подає структура документу C-M(2002)49, яка включає такі розділи:

- **Фізична безпека**
- Безпека персоналу
- Безпека інформації
- Промислова безпека

- INFOSEC (безпека автоматизованих інформаційних систем та мереж)

Аналіз структури законів про захист інформації з обмеженим доступом країн Центральної та Східної Європи – членів НАТО дозволяє дещо розширити уявлення про те, у який спосіб розподіляється увага до різних способів захисту інформації з обмеженим доступом в цих країнах. Відповідні відомості наведені у таблиці. Розгляд цієї таблиці дозволяє зробити декілька висновків. По-перше, країни-члени НАТО самостійно визначають структуру правових норм захисту інформації, виділяючи на свій розсуд ті або інші з них в окремі глави та параграфи правових актів. Наприклад, в законі Польщі окремо виділено навчання персоналу класифікації інформації як спосіб забезпечення безпеки. В законі Словакии такої норми немає, але окремо виділяються способи захисту фотографічної та аерофотографічної інформації.

По-друге, політика безпеки НАТО не перешкоджає такий варіативності. НАТО визнає [3], що існує безліч шляхів трансформації стандартів НАТО у внутрішньодержавне законодавство країн-членів, і що для альянсу краще не намагатися в цьому випадку нав'язувати готові рішення, а навпаки – надавати вільної можливості цим країнам обирати власний шлях, виходячи з політичної доцільності, економічних можливостей, культурних та історичних традицій, що відбиваються національні реалії.

В той же час слід визначити, що дані, наведені в таблиці, не можуть складати повного переліку класифікаційних параметрів щодо правових норм захисту інформації з обмеженим доступом в НАТО. Відповідно до положень загальної теорії класифікації до уваги слід брати повний набір суттєвих ознак об'єктів, що класифікуються. У цей набір першочергово має увійти розподіл інформації на чутливу, тобто ту, від якої залежить або може залежати безпека НАТО і яку, відповідно, необхідно захищати, та всяку іншу.

Чутливу інформацію можна розділити на ту, яка має матеріальне втілення, і ту, яка матеріального втілення не має.

В свою чергу інформацію, яка має матеріальне втілення, можна поділити на документовану та недокументовану.

Документованою є будь-яка інформація, яка нанесена на матеріальні носії – паперові, магнітні (аудіо-, відеоплівка, флопі-диски, стримери тощо), магнітооптичні (CD, DVD - диски), фото, кіноплівки тощо. Документована інформація може бути класифікованою або ні.

Але захисту потребує не лише документована інформація. Зовнішній вигляд літака-винищувача, танка, концептуального автомобіля, геометрія антен та топологія антенних комплексів являє собою важливішу інформацію, розголошення якої може призвести до великих втрат для НАТО в цілому, держав - її членів, а також їх окремих агенцій та відомств.

Захист такої інформації забезпечується охороною територій, споруд, приміщень, заходами по маскуванню, залученням персоналу охорони тощо.

Значна частина важливої інформації НАТО знаходиться в комп'ютерних мережах, періодично розповсюджується у проводовому та радіо ефірі. Ця форма існування інформації є невід'ємною від матеріальних об'єктів – комп'ютерів, випромінювачів, провідних систем тощо. Захистом цієї інформації НАТО займається одна з важливіших структур альянсу, котра носить назву INFOSEC. Ця структура змушена займатися захистом інформації НАТО не лише від несанкціонованого проникнення або використання, але й від природних збоїв комп'ютерних систем. Особливістю функціонування INFOSEC є те, що НАТО широко використовує для своїх військових та невійськових цілей комерційні інформаційно-комунікаційні мережі.

Болгарія	**Чехія**	**Словаччина**	**Польща**
Фізична безпека	Фізична безпека та безпека засобів обслуговування	Фізичні засоби захисту класифікованої інформації	
	Технічна безпека	Безпека технічних пристроїв	
	Безпека приміщень		
Персональна безпека	Персональна безпека	Перевірка персоналу	Безпека персоналу
			Навчання класифікації інформації з метою забезпечення безпеки
	Адміністративна безпека		
Безпека документообігу			
Криптографічна безпека	Криптографічна безпека	Захист даних шифруванням Захист фотографічної та аерофотографічної інформації Захист іноземної інформації	
Індустріальна безпека	Промислова безпека		Індустріальна безпека
Безпека автоматизованих інформаційних систем та мереж	Безпека інформаційних систем		Безпека електронних інформаційних систем і мереж

Наявна ще одна форма існування інформації. Це інформація, якою володіють люди, персонал. Суттєво те, що ця інформація принципово невідчужувана від її носіїв. Способи захисту її пов'язані з підбором, перевіркою, підготовкою та контролем персоналу.

Таблиця . Структура законодавчих актів країн-членів НАТО щодо видів та способів захисту інформації з обмеженим доступом Подальший аналіз структури правових актів країн Центральної та Східної Європи – членів НАТО, свідчить, що НАТО окремо виділяє ті з них, які пов'язані з передачею інформації зарубіжним країнам та промисловості (Industrial Security).

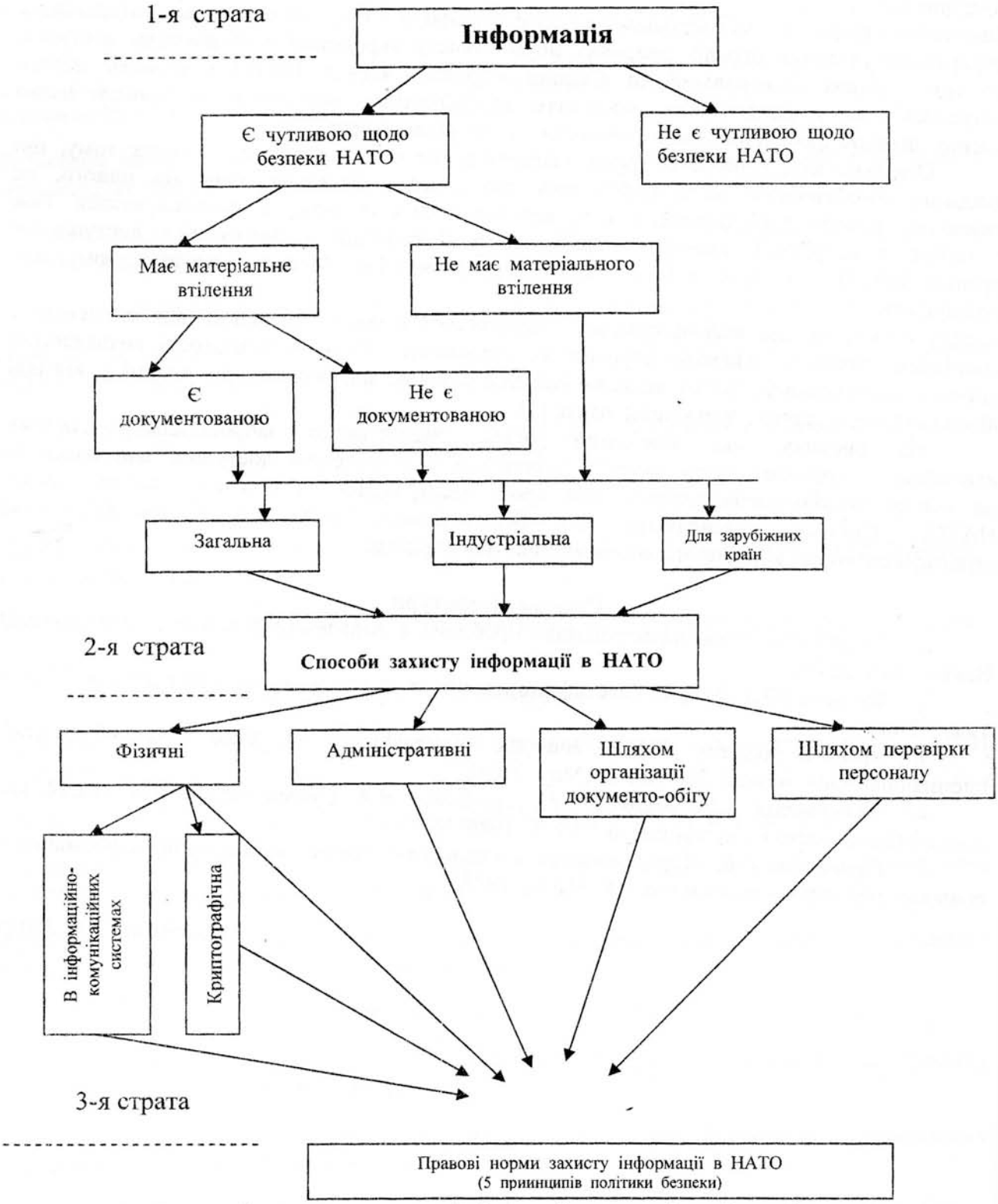

Рис 1. Стратифікована структура інформації, складові якої є об`єктом захисту в НАТО.

Якщо звернутися до правових норм захисту інформації, то можна побачити, що політика безпеки НАТО вимагає забезпечення реалізації п'яти основних принципів, які формулюються як широта (Breadth), глибина (Depth), централізація (Centralization), контрольований доступ (Controlled Distribution), персональний контроль (Personnel

Controls) [3]. Тож до складу класифікаційних параметрів мають бути внесені ще й ці показники.

Викладене вище є мінімальним описом природи тих об'єктів, які підлягають класифікації. Повний перелік правових норм захисту інформації з обмеженим доступом по всіх країнах Центральної та Східної Європи – членах НАТО становить досить потужний багатомірний масив. Завданням класифікації є зменшення розмірності цього масиву шляхом поєднання його елементів у споріднені групи.

Оскільки класифікаційні групи заздалегідь не є визначеними, а також тому, що завдання обов'язкового виділення класів, що суттєво різняться один від одного, не ставиться, методи дискримінантного та кластер-аналізу не можуть застосовуватися. Тож з метою класифікації правових норм захисту інформації з обмеженим доступом в країнах НАТО для було вибрано метод групування [4]. Метод полягає в тому, що розмірність

масиву елементів, що класифікуються, зменшується шляхом поєднання цих елементів у споріднені групи за ознакою ступеню їх близькості . Ступінь близькості визначається шляхом квантифікації, тобто шляхом надання якісним показникам, що задані у вигляді лінгвістичних змінних, кількісних ознак [5].

На рисунку, що наведений нижче, відображено запропоновану систему класифікації правових норм захисту інформації з обмеженим доступом, яка виведена на основі аналізу законодавчих актів країн Центральної та Східної Європи - членів НАТО. Система класифікації, що запропонована, подається у вигляді, який стратифіковано за ключовими ознаками на трьох рівнях.

Список літератури

1. *Розова С.С.* Классификационная проблема в современной науке . Новосибирск: Наука, 1996. 224 с.

2. *Воронин Ю.А.* Теория классифицирования и ее приложения. Новосибирск: Наука, 1995. 256с.

3. NATO's Security Policy and the Entrenchment of State Secrecy// Cornell International Law Journal 26, No. 2 (May 2003).

4. *Куперштох В.Л., Миркин Б.Г., Трофимов В.А.* Сумма внутренних связей как показатель качества классификации //А и Т. 1986. № 3.

5. *Раушенбах Г.В.* Меры близости и сходства // Анализ нечисловой информации в социологических исследованиях. М.: Наука, 1995.

Надійшла 25.12.2007р.