УДК 340.5:351.86

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В КРАЇНАХ НАТО (НА ПРИКЛАДІ ЧЕХІЇ І СЛОВАЧЧИНИ)

Володимир Артемов
Інститут захисту інформації з обмеженим доступом Національної академії Служби безпеки України

Анотація: **На прикладі законів Чехії і Словаччини проводиться порівняльне дослідження проблем реалізації міжнародно-правових норм захисту інформації з обмеженим доступом у внутрішньодержавному праві країн – членів НАТО.**
Summary: **The Security of Information Act Transformation into the NATO Countries Internal Justice Comparative Research will be carried out on Czech's and Slovak's Laws Examples.**
Ключові слова: **Захист інформації з обмеженим доступом, міжнародно-правові норми, НАТО, Чехія, Словаччина.**

I Вступ

Кожна країна, яка вступає в НАТО, бере на себе певні зобов'язання, у тому числі пов'язані із захистом інформації з обмеженим доступом, або у термінології НАТО – класифікованої інформації∗.

Метою даної статті є дослідження способів реалізації норм захисту інформації з обмеженим доступом у внутрішнім праві країн – членів НАТО, яке стає особливо актуальним в зв'язку із активізаією євроатлантичних спрямувань незалежної України.

У міжнародній практиці зазначена проблема вирішується за допомогою так званої "теорії трансформації" [1 – 5]. Трансформація міжнародно-правової норми означає її перетворення у норму внутрішньодержавного права. Існують два способи трансформації: шляхом посилання та шляхом інкорпорації. Якщо міжнародні договори встановлюють лише рамки, у межах яких країни визначають свої зобов'язання, то їхні норми приводяться в дію шляхом інкорпорації. Якщо ж міжнародні договори встановлюють норми, уже готові до застосування в сфері дії національного права і які не потребують подальшої конкретизації, то вони приводяться в дію шляхом прямого посилання. У цьому випадку виникає питання: чи можна вважати трансформаційним актом ратифікацію міжнародної угоди вищим органом влади держави. Це питання в різних країнах вирішується по різному, як того вимагають національні конституційні норми.

Трансформація не охоплює всіх способів реалізації міжнародно-правових норм. У міжнародному праві існує ідея уніфікації норм національних правових систем на основі прийняття модельних чи типових законодавчих актів. Існує, нарешті, і принцип гармонізації як один з методів уніфікації, особливість якого в тому, що уніфікації підлягають не законодавчі акти як такі, а, головним чином, правові категорії, зокрема мета, основні засади і принципи правового регулювання, понятійний апарат, нормативна термінологія тощо.

II Основна частина

Принципи нормативно-правового регулювання захисту інформації з обмеженим доступом, або – у термінології НАТО – політика інформаційної безпеки (Security Of Information policy - далі SOI) регулюються документом C-M(2002)49. Історично SOI вперше в повному обсязі була викладена в документі, відомому як C-M(55)15(Final)∗∗. Наприкінці 90-х років НАТО розпочало перегляд документа C-M(55)15(Final), у результаті чого в 2002 році з'явився документ, який тепер відомий як C-M(2002)49.

Документ C-M(2002)49 проголошує п'ять основних принципів політики безпеки НАТО: "Breadth", "Depth", "Centralization", "Controlled Distribution", "Personnel Controls" [6].

«Принцип широти» (Breadth) вбачає, що держави – члени НАТО беруть зобов'язання регулювати доступ до усіх видів чутливої інформації однаковим способом, незалежно від того, чи належить вона НАТО, чи ні. Така вимога діє на тій підставі, що НАТО має бути впевнено, що кожна країна – член НАТО

∗ НАТО розрізняє чутливу інформацію (sensitive), тобто таку, від якої залежить або може залежати безпека НАТО, і класифіковану інформацію (classified), яка офіційно визнана такою, від якої залежить безпека НАТО і для якої визначено відповідний гриф.

∗∗ Ці два документи доступні на сайті Ал. С. Робертса, професора Maxwell School of Citizenship and Public Affairs at Syracuse University (New York) – http://faculty.maxwell.syr.edu/asroberts/foi/

– забезпечує встановлені високі стандарти захисту інформації.

На «принципі глибини» (Depth) базується система поділу інформації з обмеженим доступом на рівні і визначення грифів таємності.

«Принцип централізації» (Centralization) має національний і міжурядовий аспекти. На національному рівні принцип базується на вимозі мати в кожній державі – члені НАТО – національний уповноважений орган або урядове бюро національної безпеки (national security organization – далі NSO), відповідальне за інформаційну безпеку і підбір персоналу, за збір і реєстрацію повідомлень щодо шпигунства і підривної діяльності. Бюро також має бути наділено повноваженнями контролю стану захисту інформації з обмеженим доступом в інших державних і недержавних режимно-секретних органах, організовувати методичну і дослідницьку роботу, сертифікацію засобів захисту інформації. На міжурядовому рівні існує центральний координуючий орган. У 1955 році в НАТО було створено Бюро безпеки, перетворене нині в Офіс безпеки НАТО (далі NOS), що несе відповідальність за повну координацію з питань інформаційної безпеки в НАТО. NOS повідомляє національні уряди щодо застосування принципів і стандартів та виконує моніторинг національних систем з метою гарантувати ефективний захист інформації з обмеженим доступом.

«Принцип управління доступом» (Controlled Distribution) ґрунтується на двох правилах. Перший з них – «need-to-know» (потреба знати) полягає в тому, що особи повинні мати доступ до класифікованої інформації тільки при наявності потреби в такій інформації для виконання своїх прямих службових обов'язків, і доступ не повинен надаватися лише тому, що людина посідає певне службове становище, є керівником. Цей принцип в НАТО вважається фундаментальним. Друге правило є найважливішим в угоді, підписаній членами альянсу ще в січні 1950. Воно полягає в тому, що інформація не може бути занижена у рівні таємності або розсекречена без згоди сторони, від якої вона отримана.

«Принцип персонального контролю» (Personnel Controls) передбачає правила вибору кандидатів на надання права доступу до класифікованої інформації. Контроль заснований на перевірці благонадійності, оцінках характеру і способу життя кандидатів.

Попередній аналіз демонструє, що країни Центральної і Східної Європи – члени НАТО – пішли шляхом інкорпорації основних принципів політики інформаційної безпеки в національне законодавство∗. При цьому стало очевидним, що розходження в способах здійснення міжнародно-правових норм захисту інформації у внутрішньодержавному праві цих країн залежать не лише від системи їх державного устрою, але й має генетичні корені, обумовлені динамікою світових процесів.

Це особливо добре видно на прикладі законодавства Чехії і Словаччини, дуже близьких у культурно-історичному і одночасно дещо віддалених по економічному рівню країн. Детальний аналіз законів щодо захисту інформації цих країн особливо актуальний з погляду давніх традицій культурних і економічних зв'язків між Україною і цими країнами.

Як першоджерела для порівняння були взяті «The Protection of Classified Information Act and Amendments to Relevant Legislation», прийнятий Палатою Депутатів Чеської Республіки 20 травня 1998 року, і «Act on Protection of Classified Materials and on Amendment of Certain Laws», прийнятий Національною Радою Словацької Республіки 30 травня 2001 року. Обидва закони доступні на сайті FOI (http://faculty.maxwell.syr.edu/ asroberts/foi).

Для цього на підставі рекомендацій, що містяться в доступній юридичній літературі [7 – 9], нами були розроблені методичні рекомендації щодо порівняльного аналізу законодавства країн – членів НАТО – у галузі захисту інформації з обмеженим доступом. При цьому особлива увага приділялася **діахроному аналізу**, тобто такому, який зорієнтований на дослідження генетичних основ правових норм в законодавстві різних країн, в нашому випадку – розходжень, що обумовлені динамікою розвитку правових процесів і явищ.

Як метод наукового дослідження порівняльне правознавство дозволяє глибше осягнути процеси і явища у сфері правового регулювання захисту інформації з обмеженим доступом, краще зрозуміти обсяг і характер правового впливу законодавства НАТО при вступі України до міжнародних організацій та угод, більш повно використовувати масштаби і форми закордонного досвіду.

Враховуючи викладене, проведено порівняння двох приведених вище законів. Навіть поверхневий аналіз результатів порівняння визначень і норм вказує на наявність істотних розходжень. Внаслідок браку місця нижче для прикладу розглянемо результати порівняння лише деяких основних формулювань.

Позначення об'єкта регулювання і збитку, пов'язаного із втратою або розголошенням класифікованої інформації, відрізняються. Об'єкт регулювання визначено у законі Словаччини ширше (табл. 1).

∗ Законодавчі акти цих країн доступні на сайті http://faculty.maxwell.syr.edu/asroberts/foi/

Таблиця 1

Визначення та норми	Чеська Республіка	Республіка Словаччина
Об'єкт регулювання	Класифікована інформація (частина 1, глава 1, секція 1)	**Класифіковані матеріали** - інформація та матеріальні об'єкти **Інформацією вважається:** - зміст документів, схем, ескізів, карт, фотографій, графічних та інших записів; - зміст усних заяв (висловлень); - зміст електричних, електромагнітних, електронних та інших фізичних носіїв. **Об'єктами вважаються:** - матеріальні носії з інформаційними записами; - вироби; - обладнання; - споруди. (стаття 2, пп. a, b, c)

Принциповим є те, що Чехія під збитком розуміє нанесення шкоди або створення загрози власним інтересам чи інтересам, які Чеська республіка зобов'язалася захищати. Це може означати, що для захисту інформації, що належить третім країнам, потрібна наявність деяких офіційних зобов'язань з боку Чехії. У законі Словаччини така норма відсутня (табл. 2).

Наявні розбіжності в частині нормування принципу глибини (Depth). Тут суттєвим є те, що Республіка Словаччина бере під захист не лише інтереси державних органів але й громадян Словаччини (табл. 3).

Всього ж порівняння проводилося по всіх 90 секціям закону Чеської Республіки і 70 статтям закону Республіки Словаччини. Втім, і це порівняння дозволяє зробити певні висновки і простежити деякі тенденції. Більш повну картину, цікаву в зв'язку зі стратегічними устремліннями незалежної України, можна отримати, якщо виконати попарне порівняння всіх законодавчих актів нових країн – членів НАТО в частині захисту інформації з обмеженим доступом з наступним обчисленням їх близькості у певних багатомірних шкалах з екстраполяцією напрямків розвитку міжнародного законодавства в цій сфері. Ця задача буде предметом подальших досліджень автора.

Таблиця 2

Визначення та норми	Чеська Республіка	Республіка Словаччина
Збиток, пов'язаний із втратою або розголошенням класифікованої інформації	Збиток або створення небезпечних умов для інтересів Чеської Республіки або інтересів, які Чеська Республіка зобов'язалася захищати, наслідки яких не можуть бути усунуті або можуть бути пом'якшені тільки певними заходами (частина 1, глава 1, секція 1 – 2)	Завдання збитків або загроза завдання збитків інтересам Словацької Республіки або інтересам, з якими пов'язаний захист Республіки Словаччина, при цьому ефект від нанесеного збитку або не може бути усунутий, або зменшення його пов'язане з необхідністю прийняття серйозних заходів (стаття 2, п. f)

Таблиця 3

Визначення та норми	Чеська Республіка	Республіка Словаччина
"Цілком таємно" TOP SECRET	у випадках, коли несанкціоноване розкриття інформації призвело б до винятково серйозного збитку інтересам Чеської Республіки, цей ступінь класифікації позначається словами PŘÍSNĚ TAJNÉ або скорочено PT.	Цим ступенем захисту визначаються секретні матеріали, якщо у разі їх неправомочного розкриття і маніпуляції конституційність, суверенітет і територіальна цілісність держави може бути піддана небезпеці, або буде нанесена непоправна і серйозна шкода безпеці,

Продовження Таблиці 3

	(частина 1, глава 1, секція 1 – 2)	економічним інтересам, зовнішній політиці або міжнародним відносинам Республіки Словаччини. (стаття 2, п. f)
"Для службового користування" RESTRICTED	... у випадках, коли несанкціоноване розкриття інформації призвело б до нанесення шкоди інтересам Чеської Республіки, цей ступінь класифікації позначається словами VYHRAZENÉ або скорочено V. (частина 1, глава 1, секція 1 – 2)	Цим ступенем захисту визначаються секретні матеріали, якщо у разі їх неправомочного розкриття і маніпуляції буде завдано шкоди інтересам державних органів або громадян Республіки Словаччини. (стаття 2, п. f)

III Висновки

Враховуючи викладене, аналізуючи реалізації норм політики безпеки у внутрішньому праві зазначених держав згідно з вимогами НАТО, можна, на наш погляд, зробити наступні висновки:

- здійснення міжнародно-правових норм захисту інформації у внутрішньодержавному праві країн-членів НАТО відбувається шляхом інкорпорації основних принципів політики безпеки НАТО в правове поле цих держав;
- політика безпеки НАТО в частині інформації з обмеженим доступом залишає досить широкі рамки, всередині яких можуть варіюватися конкретні норми національного права;
- політика безпеки НАТО в частині інформації з обмеженим доступом не залишається постійною і піддається змінам під впливом викликів сьогодення;
- виходячи із стратегічних інтересів та спрямувань незалежної України актуальним є поглиблене порівняльно-правове вивчення внутрішньодержавного права нових країн – членів НАТО, в частині захисту інформації з обмеженим доступом.

Література: ***1.*** *Черниченко С. В. Международное право: современные теоретические проблемы. М., 1993.* ***2.*** *Мюллерсон Р. А. Соотношение международного и национального права. М., 1982.* ***3.*** *Левин Д. Б. Актуальные проблемы теории международного права. М., 1974. С. 252.* ***4.*** *Інформатизація, право, управління (організаційно-правові питання). Монографія /Калюжний Р. А., Крупчан О .Д., Гавловський В. Д., Гуцалюк М. В., Цимбалюк В. С., Швець М. Я. /За заг.ред. Швеця М. Я., Крупчана О. Д. - Київ: НДЦ правової інформатики АПрНУ, 2002. 191 с.* ***5.*** *Правова інформатика: система інформатизація законотворчої, правозастосовсовчої, правоохоронної, судочинної та право освітньої діяльності в Україні. Монографія /Брижко В. М., Вознюк І. А., Гавловський В. Д, Глодківська О. В., Задорожня Л .М., Калюжний Р. А., Клімашевська Ю. А Савицький В. А., Севастьянов В. Ф. Смаглюк В. М., Хахановський В. Г., Цимбалюк В. С., Швець М. Я., Яременко О. І. /За ред. М. Я. Швеця, Р. А. Калюжного. – Ужгород: ІВА, 2003. 13,55 у.д.а. - 168 с.* ***6.*** *Al. S. Roberts Nato's security of information policy and the entrenchment of State Secrecy. Reports Basic Newsletter on Internal International Security October 2003 Nb. 76* ***7.*** *Тихомиров Ю. А. Курс сравнительного правоведения. М., 1996.* ***8.*** *Саидов А. Х. Введение в сравнительное правоведение. М., 1988* ***9.*** *Топорнин Б. Н. Европейское право. М., 1998.*

УДК 025:46

ОСНОВА ТЕХНІЧНИХ РЕГЛАМЕНТІВ УКРАЇНИ – ДИРЕКТИВИ ЄВРОПЕЙСЬКОГО СОЮЗУ НОВОГО ТА ГЛОБАЛЬНОГО ПІДХОДУ

Юлія Кожедуб
ДП „УкрНДНЦ"

Анотація: **Розглянуто законодавчу базу технічного регулювання в Україні. Висвітлено найголовніші аспекти європейської практики щодо гармонізації та стандартів. Ннаведено наявні Директиви ЄС Нового та Глобального підходу, затверджені технічні регламенти України, заплановані до розроблення міждержавні технічні регламенти.**