ГЛУХОВЕРЯ В. А.,
викладач кафедри
загальноправових дисциплін
(Дніпропетровський гуманітарний університет)

УДК 340+35.083

ІНОЗЕМНИЙ ДОСВІД АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У статті характеризуються основні принципи міжнародного законодавства щодо правового захисту інформації з обмеженим доступом та іноземний досвід їх реалізації.
Ключові слова: *інформація з обмеженим доступом, принципи, законодавство.*

В статье характеризуются основные принципы международного законодательства по правовой защите информации с ограниченным доступом и иностранный опыт их реализации.
Ключевые слова: *информация с ограниченным доступом, принципы, законодательство.*

The article characterized by the basic principles of international law on the legal protection of information with restricted access, and foreign experience of their implementation.
Key words: *information with restricted access, principles, legislation.*

Вступ. На початку 80-х років XX ст. професор Гарвардського університету А. Еттінгер зазначав: «Наступає час, коли інформація стає таким же основним ресурсом, як матеріали та енергія, отже, відносно цього ресурсу повинні бути сформульовані ті ж критичні запитання: хто ними володіє, хто в цьому зацікавлений, наскільки він доступний, можливість його ефективного використання» [4, с. 11]. У багатьох промислово розвинутих країнах приділяється значна увага здійсненню комплексу заходів, спрямованих на виключення або утруднення витоку інформації, яка захищається. С. Князєв відзначає, що до такого комплексу належить насамперед розробка й прийняття законодавчих актів в інформаційній сфері, що стосуються охорони державної таємниці та комерційних секретів фірм [6]. Основні засади, система та особливості розвитку законодавства, що врегульовує суспільні відносини у сфері обігу інформації з обмеженим доступом приватного та публічного характеру, у різних країнах різняться. На цю сферу правового регулювання значний вплив здійснюють обрані конкретною країною напрями міжнародної політики, приєднання чи підтримка окремих міждержавних або міжурядових утворень. Україна стоїть на шляху інтеграції в міжнародні інформаційні процеси. Національна інформаційна сфера України перебуває в стані активного становлення, гармонійного включення в глобальний світовий інформаційний простір [17]. Вплив на формування національного інформаційного законодавства, у тому числі й адміністративного деліктного законодавства у сфері обігу інформації з обмеженим доступом, будуть здійснювати існуючі у світі тенденції та традиції. Пріоритетними для дослідження іноземного досвіду правового захисту інформації з обмеженим доступом є досвід країн-партнерів України.

Постановка завдання. Мета статті – з'ясування зміст принципів міжнародного законодавства щодо правового захисту інформації з обмеженим доступом та іноземний досвід

їх реалізації. Предмет розгляду цього наукового дослідження – правові норми та наукові теорії, що визначають зміст правових засад регулювання суспільних відносин у сфері обігу інформації з обмеженим доступом.

Результати дослідження. Україна як європейська держава здійснює відкриту зовнішню політику та прагне рівноправного взаємовигідного співробітництва з усіма заінтересованими партнерами, виходячи насамперед з необхідності гарантування безпеки. Одними з основних засад зовнішньої політики є забезпечення інтеграції України в європейський політичний, економічний, правовий простір із метою набуття членства в Європейському Союзі (далі – ЄС) [11]. У цьому контексті існує постійна потреба в обміні інформацією з обмеженим доступом між Україною та ЄС та застосування відповідних заходів безпеки, що передбачені відповідною угодою між Україною та Європейським Союзом [20]. Водночас Україна ставить завдання в зовнішній політиці також щодо зближення з НАТО.

Питання міжнародних правових засад регулювання захисту інформації з обмеженим доступом розглядали такі правознавці, як В. Артемов, Д. Василенко, Г. Громов, С. Князев, В. Маслак, М. Павлова, А. Тунік.

Останні зміни в законодавстві щодо відмови України від здійснення політики позаблоковості свідчать про поглиблення співпраці України з Організацією Північноатлантичного договору з метою досягнення критеріїв, необхідних для набуття членства в цій організації [14]. За таких умов набуває все більшого значення координації діяльності органів виконавчої влади, державних засобів масової інформації з питань співробітництва з НАТО в інформаційній сфері [14]. Цей вектор розвитку зовнішньо політики України впливатиме й на правове регулювання системи безпеки інформації як складової частини євроатлантичного безпекового простору [12]. Таким чином, основоположними документами, що визначають зміст, характер і створюють договірно-правову основу відносин України з НАТО, є Рамковий документ Програми НАТО «Партнерство заради миру» (започатковано 10 січня 1994 року, Україна приєдналася 8 лютого 1994 року) [8], Хартія про особливе партнерство між Україною та НАТО від 9 липня 1997 року [21], Декларація про її доповнення від 21 серпня 2009 року та Закон України «Про засади внутрішньої і зовнішньої політики» від 1 липня 2010 року [11]. Відповідно до Декларації про доповнення Хартії під егідою КУН також розробляються Річні національні програми співробітництва Україна-НАТО.

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

Документ С-М(2002)49 проголошує п'ять основних принципів політики безпеки НАТО: «Breadth», «Depth», «Centralization», «Controlled Distribution», «Personnel Controls» [1].

«Принцип широти» (Breadth) вбачає, що держави-члени НАТО беруть зобов'язання регулювати доступ до всіх 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 забезпечує встановлені високі стандарти захисту інформації.

На «принципі глибини» (Depth) базується система поділу інформації з обмеженим доступом на рівні й 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 та підбір персоналу, за збір і реєстрацію повідомлень щодо шпигунства та 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

та 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 із метою гарантування ефективного захисту інформації з обмеженим доступом.

Принцип управління доступом (Controlled Distribution) ґрунтується на двох правилах. Перше правило «need-to-know» (потреба знати) полягає в тому, що особи повинні мати доступ до класифікованої інформації тільки за 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 у НАТО вважається фундаментальним. Друге правило є найважливішим в угоді, підписаній членами альянсу ще в січні 1950 року. Воно полягає в тому, що інформація не може бути занижена в 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 й способу життя кандидатів.

Попередній аналіз демонструє, що країни Центральної і Східної Європи, які є членами НАТО, пішли шляхом інкорпорації основних принципів політики інформаційної безпеки в національне законодавство. В. Артемов зазначає, що 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 [2, с. 60–61]. Це особливо добре видно на прикладі законодавства Чехії та Словаччини, дуже близьких у культурно-історичному й одночасно дещо віддалених за економічним рівнем країнах. Детальний аналіз законів щодо захисту інформації цих країн, проведений В. Артемовим, особливо актуальний з огляду на давні традиції культурних й економічних зв'язків між Україною та цими країнами, продемонстрував більший ступінь розробленості законодавства про інформацію з обмеженим доступом Республіки Словаччина [2, с. 61]. Інші країни-члени ЄС також мають закони, що регулюють використання та захист режиму інформації з обмеженим доступом: Чехія – «Порядок доступу до інформації» та «Акт про класифікацію інформації»; Естонія – «Акт про суспільну інформацію» та «Акт про державні таємниці»; Литва – «Закон про умови передання інформації громадськості» та «Закон про державну таємницю»; Латвія – «Закон про свободу інформації» та «Закон про державну таємницю»; Польща – «Про доступ до інформації» та «Акт про захист інформації, яка класифікується» [3, с. 130].

В. Артемовим прийшов до висновків, цікавих для розвитку українського законодавства про інформацію з обмеженим доступом за умов без блокового статусу України: 1) запровадження міжнародно-правових норм захисту інформації у внутрішньодержавному праві країн-членів НАТО відбувається шляхом інкорпорації основних принципів політики безпеки НАТО в правове поле цих держав; 2) політика безпеки НАТО в частині інформації з обмеженим доступом залишає досить широкі рамки, усередині яких можуть варіюватися конкретні норми національного права; 3) політика безпеки НАТО в частині інформації з обмеженим доступом не залишається постійною та піддається змінам під впливом викликів сьогодення [20, с. 63]. Принципи забезпечення інформації з обмеженим доступом у країнах НАТО повинні бути запроваджені й у вітчизняному законодавстві та відображені в Законі України «Про інформацію». Велика кількість правових питань, що потребують врегулювання у сфері обігу інформації з обмеженим доступом, створюють передумови для розробки та прийняття Закону України «Про інформацію з обмеженим доступом» чи відповідного розділу в Кодексі України про інформацію з обмеженим доступом.

Не тільки документи, що регулюють співпрацю з ООН, містять основні засади правового регулювання обігу інформації з обмеженим доступом. Угода між Україною та Європейським Союзом про процедури безпеки, які стосуються обміну інформацією з об-

меженим доступом, визначає такі засади використання відповідної інформації: принцип контролю з боку власника інформації та принцип потреби в доступі за умовами службової діяльності [19].

Важлива роль у міжнародних документах відводиться для узгодження вітчизняного законодавства із законодавством ЄС щодо процедур обміну таємною інформацією та забезпечення конфіденційності персональних даних [9]. Підґрунтям для розробки та прийняття національного законодавства про захист персональних даних стали такі міжнародні документи, як Модельний закон про інформатизацію, інформацію та захист інформації, прийнятий на двадцять шостому пленарному засіданні Міжпарламентської Асамблеї держав-учасниць Співдружності Незалежних Держав (далі – СНД) у 2005 році [7], та ратифікована в 2010 році Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [13]. Принципи, що містяться в Конвенції, уточнюються та розширюються в Директиві 95/46/ЕС Європейського парламенту та Ради від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [5] та Директиві 97/66/ЕС Європейського парламенту та Ради від 15 грудня 1997 року «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» [16], які покищо не ратифіковані Україною, проте можуть бути використані для удосконалення вітчизняного законодавства. Відповідно до зазначених документів більшість країн ЄС та СНД видала свої національні закони: щодо діяльності з персональними даними в медичній, статистичній, державній, журналістській, поліцейській та інших сферах.

Закріплення на міжнародному рівні норм, що визначають необхідність правового захисту персональних відомостей, відображають сталу тенденцію в розвитку інформаційних відносин, що виникають у процесі функціонування суб'єктів владних повноважень, зокрема збільшення обсягів використання персональних даних громадян.

У європейських країнах правовий захист персональних даних здійснюється на рівні двох законів, що взаємодоповнюються: закон *Data Protection Act і закон Information Freedom Act* (закон про свободу інформації). Такі типи законів, як правило, розробляються та приймаються одночасно. В окремих країнах принцип свободи доступу до інформації безпосередньо закладається в положеннях закону *Data Protection Act.* А Тунік зазначає: «Закони про захист персональних даних різних країн намагаються охопити всі послідовні етапи циклу, починаючи зі збору даних і закінчуючи їх знищенням, інформуванням, участю та контролем зі сторони індивідуума. Розбіжності в національних підходах, що спостерігаються в даний час у законах, законопроектах і законодавчих пропозиціях, стосуються таких аспектів, як масштаб дії законодавчого акта, акцентування в ньому різних елементів системи захисту, дотримання вищезазначених принципів, система контролю за виконанням законодавства» [18, с. 12]. Крім того, можна вказати на розбіжності в категоріях даних, що не підлягають розголошенню, у методах забезпечення відкритості та індивідуальної участі. Акцентовано, що механізми захисту даних, які відносяться до приватних осіб, не можуть бути аналогічні тим, що необхідні для захисту даних ділових підприємств, асоціацій і груп, що мають статус юридичної особи. Водночас, дослід багатьох країн свідчить про те, що чітко розмежовувати персональні й неперсональні дані досить складно. А. Тунік проаналізував правові засади захисту персональних даних у СНД та прийшов до висновку, що в країнах СНД системою захисту персональних даних обрано закон типу *Data Protection Act* (Закон про захист даних), де обов'язково закріплюються ознаки персональних даних; права суб'єкта даних у зв'язку з обробкою та використанням даних; правила доступу до чужих персональних даних, їх розкриття й передача; вилучення з правового регулювання даних в інтересах державної та суспільної безпеки, у зв'язку з розслідуванням злочинів; заходи правового регулювання збору, збереження, обробки, передачі й використання персональних даних; вимоги до організаційно-технічних заходів із забезпечення безпеки під час їх обробки, використанні, передачі та збереженні; норми, що встановлюють відповідальність за порушення принципів захисту даних тощо [18, с. 11]. На наш погляд, цей закон має багато переваг: він чітко визначає принципи регулювання обробки персональних даних, права та обов'язки суб'єктів персональних

даних та їх користувачів. Вважаємо за необхідне ці положення відобразити й у вітчизняному Законі України «Про захист персональних даних».

За даними Харківської правозахисної групи майже всі країни світу визнають право на приватність безпосередньо у своїх конституціях. Наприклад, основні закони Південної Африки та Угорщини містять у собі спеціальні норми щодо доступу та контролю за інформацією особистого характеру. У багатьох країнах, де приватність не визнано безпосередньо в конституції (наприклад, Сполучених Штатах, Ірландії та Індії), для реалізації цього права суди застосовують інші норми, зокрема міжнародні договори, де визнається право на приватність, такі як Міжнародний пакт про громадянські й політичні права або Європейська Конвенція про права людини, що є частиною законодавства багатьох країн.

Нині міжнародне законодавство включає приблизно 20 загальноєвропейських конвенцій, директив та рекомендацій із питань захисту персональних даних. 6 липня 2010 року Україна ратифікувала базові європейські стандарти у сфері захисту персональних даних, зокрема Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, а також додатковий протокол до неї стосовно органів нагляду та транскордонних потоків даних, таким чином беручи на себе зобов'язання імплементувати їх положення в українське законодавство.

Спеціалісти Харківської правозахисної групи, дослідивши моделі захисту приватності в різних країнах, констатують факт існування декількох загальних моделей захисту приватності. У деяких країнах одночасно використовується кілька моделей. Модель регулювання, що застосовується в Європі, Австралії, Гонгконзі, Новій Зеландії, Центральній і Східній Європі та Канаді, полягає в тому, що існує посадова особа (наприклад, уповноважений, омбудсмен, реєстратор), яка забезпечує виконання положень детально розробленого закону про приватність. Ця посадова особа здійснює нагляд за дотриманням законності та проводить розслідування щодо виявлених порушень, а також відповідає за громадянську освіту та міжнародні стосунки щодо захисту даних та їх передачі. Такої моделі дотримуються більшість країн, де існують закони про захист даних. Цю модель також обрано Європою для створення нового режиму захисту даних. Однак коло повноважень таких органів дуже різниться, часто надходять повідомлення про серйозну нестачу засобів, що призводить до невиконання положень чинного законодавства.

Дотримання конфіденційності персональних даних є одним з аспектів приватності, визнаного фундаментальним правом людини в Загальній декларації прав людини ООН, Міжнародному пакті про громадянські й політичні права та в багатьох інших міжнародних і регіональних угодах. Інформаційна приватність включає в себе встановлення таких правил збору та обігу персональних даних, як інформація кредитних установ та медичні записи [10, с. 12]. З огляду на зміст відомостей, що складають зазначену інформацію, перелік її користувачів та джерел отримання стає майже невичерпним, що обумовлює включення до інформаційних відносин, що виникають із приводу використання персональних даних усіх суб'єктів права.

М. Павлова зазначає, що протягом багатьох років США та Європа по-різному підходять до захисту особистої інформації. Зараз обидві сторони намагаються подолати цей розрив. Так, щодо загального населення, без прив'язки до займаної посади, у США Конгрес прийняв законодавчі акти, які в окремих випадках обмежують використання персональних даних американців, що містяться в медичних документах, кредитних звітах, відеозаписах тощо. З іншого боку, Європейський Союз прийняв більш повну систему правових документів і має загальну директиву, яка надає громадянам ЄС певні основоположні права, такі як право на отримання копій документів, що містять персональні дані про них із боку компаній та організацій, що, на думку М. Павлової, не має аналога в законодавстві США [15]. Підтримують цю позицію й дослідники Харківської правозахисної групи, зазначаючи, що Сполучені Штати Америки уникають схвалення загальних принципів захисту даних, надаючи перевагу таким спеціальним секторальним законодавчим актам, як відеозаписи під час укладення договорів оренди та збереження приватності у фінансових питаннях.

Висновки. Таким чином, запровадження у вітчизняне законодавства про інформацію з обмеженим доступом принципів ООН та ЄС щодо захисту інформації з обмеженим доступом, на наш погляд, потребує внесення змін до ст. 4 Закону України «Про доступ до публічної інформації» шляхом доповнення її частиною другою, де слід зазначити засади використання інформації з обмеженим доступом у роботі суб'єктів владних повноважень: 1) інформація з обмеженим доступом повинна бути отримана й оброблена законним чином на підставі чинного законодавства; 2) інформація з обмеженим доступом суб'єктів приватного права включаються до державних баз даних на підставі вільної згоди суб'єкта, вираженого в письмовій формі; 3) інформація з обмеженим доступом повинна накопичуватися для точно визначених і законних цілей, не використовуватися в суперечності із цими цілями та не бути надмірною щодо них; 4) інформація з обмеженим доступом в разі необхідності може оновлюватися та передаватись іншим суб'єктам владних повноважень на підставі вільної згоди суб'єкта (власника, законного користувача інформації), вираженого в письмовій формі; 5) інформація з обмеженим доступом повинна зберігатися не довше, ніж цього вимагає мета, для якої вона накопичуються, і підлягає знищенню після досягнення цієї мети або за умови зникнення потреби; 6) слід вживати заходів для охорони інформації з обмеженим доступом, що виключають випадкове або несанкціоноване руйнування, або випадкову її втрату, а також несанкціонований доступ до неї, зміну, блокування чи передачу даних; 7) забезпечення безперервного захисту інформації з обмеженим доступом; 8) відповідальність за порушення режиму інформації з обмеженим доступом та відшкодування завданої шкоди.

Список використаних джерел:

1. 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.

2. Артемов В.Ю. Захист інформації з обмеженим доступом в країнах НАТО (на прикладі Чехії і Словаччини) / В.Ю. Артемов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. – Вип. 11. – С. 60–63.

3. Василенко Д.П. Законодавство провідних країн світу у сфері захисту інформації / Д.П. Василенко, В.І. Маслак // Вісник КДУ імені Михайла Остроградського. – Вип. 2010. – № 2 (61). – Ч. 1. – С. 128–132.

4. Громов Г.Ю. Беспилотные информационные средства / Г.Ю. Громов // Знание сила. – № 7. – М., 1986. – С. 12 – 17; 3. Signal. – USA, 1983. – P. 10–14.

5. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_242/print1359106886760987.

6. Князев С. Деякі аспекти забезпечення охорони інформації з обмеженим доступом в провідних країнах світу / С. Князєв // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип. 2 (13). – С. 102–109.

7. Модельный закон об информатизации, информации и защите информации : Постановление № 26-7 от 18 ноября 2005 года, принятое двадцать шестом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/997_d09/print1329875570254855.

8. Партнерство заради миру : Рамковий документ, підписаний Україною 8 лютого 19994 року // Офіційний вісник України. – 2006. – № 48. –Ст. 3232.

9. План дій «Україна – Європейський Союз», схвалена Кабінетом Міністрів України 12 лютого 2005 року [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/994_693/print1390908416635159.

10. Право на приватність: conditio sine qua non. – Х. : Фоліо, 2003. – 216 с.

11. Про засади внутрішньої і зовнішньої політики : Закон України від 1 липня 2010 року № 2411-VI // Відомості Верховної Ради України. – 2010. – № 40. – Ст. 527.

12. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV // Офіційний вісник України. – № 29. – Ст. 1433.

13. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних // Відомості Верховної Ради України. – 2010. – № 46. – Ст. 542.

14. Про Рекомендації парламентських слухань про взаємовідносини та співробітництво України з НАТО : Постанова Верховної Ради України від 21 листопада 2002 року № 233-IV // Відомості Верховної Ради України. – 2002. – № 51. – Ст. 374.

15. Павлова М.О. Захист персональних даних суддів: прогалина чи примха? / М.О. Павлова [Електронний ресурс]. – Режим доступу : http://ukrjustice.com.ua/zahyst–personalnyh–danyh–suddiv–prohalyna–chy–prymha/.

16. Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі : Директива 97/66/ЄС Європейського Парламенту і Ради від 15 грудня 1997 року [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_243.

17. Стратегія розвитку інформаційного суспільства в Україні : Розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р // Урядовий кур'єр. – 2013. – № 105.

18. Тунік А.В. Правові основи захисту персональних даних : автореф дис. … канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / А.В. Тунік ; Національний авіаційний університет. – К., 2012. – 21 с.

19. Угода між Україною та Європейським Союзом про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом, ратифікована Законом України № 499-V від 20 грудня 2006 року // Офіційний вісник України. – 2007. – № 15. – Ст. 582.

20. Угода між Україною та Європейським Союзом про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом, ратифікована Законом України № 499-V від 20 грудня 2006 року // Офіційний вісник України. – 2007. – № 15. – Ст. 582.

21. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору, підписана 9 липня 1997 року // Офіційний вісник України. – 2006. – № 34. – Ст. 2453.