УДК 342.9

С. О. ЛИСЕНКО
Міжрегіональна Академія управління персоналом, м. Київ

ЗАРУБІЖНИЙ ДОСВІД АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ З ТОЧКИ ЗОРУ КОМПАРАТИВІСТИКИ

Наукові праці МАУП, 2016, вип. 51(4), с. 35–44

Аналізується зарубіжний досвід адміністративно-правового регулювання інформаційної безпеки підприємств з точки зору компаративістики, досліджується зміст поняття "компаративістика" у цьому контексті, визначаються основні положення проекту Доктрини інформаційної безпеки України.

Українська сучасність характеризується стрімкими темпами розвитку комунікативних технологій та прискоренням глобалізаційних процесів. За наявності останніх гостро постає питання гнучкого адаптування до них з боку держави та підприємств різних форм власності, що виявляються в інформаційній політиці, яка має охоплювати всі сфери комунікативних зв'язків у країні. Саме ефективне забезпечення інформаційної безпеки підприємств здатне якнайшвидше налагодити формування інформаційного суспільства, зменшивши й трансформувавши внутрішні та зовнішні загрози в інформаційній сфері, що мають у сучасному суспільстві часто визначальний характер.

Виокремимо науковців, які займаються цією проблематикою: Г. В. Виноградова, Б. А. Корміч, В. О. Заросило, Є. Д. Скулиш, А. І. Марущак, Р. А. Калюжний, В. А. Ліпкан, В. С. Цимбалюк, А. М. Подоляка, Н. В. Банчук, А. І. Мовчан, І. В. Арістова та ін.

Поряд з цим деякі питання досліджень інформаційної безпеки підприємств у праві залишаються нерозкритими.

Встановимо позитивний закордонний досвід з організації моделей інформаційної безпеки підприємств. Визначимо основні критерії ефективного його впровадження в сучасному українському суспільстві шляхом порівняння з власним досвідом. Задля досягнення такої мети доцільно залучити кілька методологічних засобів, головними серед яких визначено: аналіз (щодо окремих аспектів законодавства стосовно створення конкретних моделей інформаційної безпеки підприємств) та компаративістський метод (для визначення ступеня відповідності критеріям оптимальної інформаційної безпеки різних існуючих моделей).

За наявності у своїй основі порівняльних досліджень масиву законодавства, певної інфраструктури інформаційної безпеки підприємств та установ, засобів юридичної техніки та правового стилю юристів різних країн світу на основі їх співставлення та оцінки порівняння дає можливість прослідкувати альтернативні шляхи майбутнього розвитку національної системи інформаційної безпеки. У науковому суспільстві існує поняття "компаративістика", що є теоретичною дисципліною, яка тісно пов'язана із загальною теорією права. Компаративістика має власний об'єкт дослідження, вона глибше проникає у правові явища у порівняльному плані, ніж загальна теорія права. Порівняльні дослідження правових систем дають змогу визначити особливості структури національних правових систем, закономірності розвитку певних галузей законодавства [1].

З іншого боку, компаративістика дає можливість глибше досліджувати певні закономірності виникнення та розвитку теорії інформаційної безпеки і є порівняльним методом дослідження без власного предмета. Предмет компаративістики не можна поєднувати з іншими предметами національних галузей права. Компаративістика є дисципліною, яка містить методологію порівняльно-аналітичного дослідження окремих аспектів правових систем за певними інститутами кількох країн світу, особливостей застосування міжнародних правових норм у національній правовій системі з метою виявлення їх спільних або відмінних рис, для прогнозування подальшого розвитку чи оптимізації їх, а також для вирішення прикладних завдань правозастосування [17].

Деякі українські дослідники займалися питаннями компаративістики і зазначали, що "порівняльне дослідження може носити широкий і вузький характери. На основі порівнянь окремих властивостей правових систем, понять і загальних процедур, що випливають із загальних їх характеристик, виділяють компаративістику на макрорівні (базисне порівняння). У даному випадку роблять загальний аналіз історії, класифікації, інфраструктури, методології та правової культури правових систем. Можна порівнювати законодавчу техніку та методи інтерпретації законодавчих актів, визначати роль судових прецедентів і техніку винесення судових рішень у різних країнах" [2]. Можливе порівняння організації моделей інформаційної безпеки у різних правових системах: яким чином розподіляються обов'язки між суб'єктами та державними органами; яка роль зібраних матеріалів у кримінальному та цивільному процесі. Порівняльний аналіз на загальних системах права складає сам предмет, куди входять поняття і зміст, структура і методологія компаративістики, класифікація правових сімей та значення компаративістики.

На рівні окремих інститутів, таких як організація інформаційної безпеки підприємств, аналізуються специфічні положення матеріального і процесуального права. Можуть порівнюватися норми, що регулюють питання укладання трудових договорів; процедура ознайомлення з переліком тем, віднесених до комерційної таємниці; якими правами володіє суб'єкт інформаційної безпеки тощо. До предмета компаративістики відносять порівняльний аналіз

на рівні окремих інститутів публічного, приватного, змішаних галузей права та процесуального права [6].

За своїми цілями компаративістику можна класифікувати на теоретичну та функціональну. Інші класифікації відбуваються за рівнями порівняння — внутрішньонаціональне (у федеративних державах), історичне (за типами права або за історичними закономірностями його розвитку), міжгалузеве (порівняння галузей та інститутів права однієї країни), міжсистемне (порівняння правових систем різних правових сімей), внутрішньосистемне (порівняння правових систем однієї правової сім'ї) [7]. У зв'язку з цим у нормативному середовищі існують особливості. Зрозуміло, що не може бути німецької, голландської, білоруської чи української математики, але у праві існує різноманітність. Ця особливість може бути обґрунтована певними рисами становлення і розвитку національної правової системи, а також рівнем міжнародного обміну в національному правотворенні і правозастосуванні залежно від його інтенсивності.

Історично транснаціональний обмін права спостерігався не завжди. У період домінування у Європі римського права існував єдиний правовий простір, але, починаючи з XIX ст., спостерігалися "націоналізація" права, прийняття окремими державами власних кодексів. Завдяки цій тенденції розвитку національного права юристи надавали перевагу тільки тлумаченню національних норм і перестали цікавитися розвитком права в сусідніх країнах. З посиленням ідей державного суверенітету у юристів "на ґрунті невимогливості правового самолюбування зростає гордість за власне право" [18].

Одним із найважливіших завдань компаративістики у сфері інформаційної безпеки підприємств залишається формування комплексу цілей по вирішенню теоретичних, адміністративних і практичних проблем права. Вирішення колізій, порівняно з міжнародними аналогами приватного права, можна досягти за допомогою знань суб'єктом та учасниками процесу іноземних норм і вироблення єдиних критеріїв формулювання правил застосування правових норм. Вирішення законних спорів за участю іноземного суб'єкта з використання конфіденційної інформації потребує знання колізійного права і застосування відповідних правових прив'язок та загальних правових понять. Публічне право бере участь у порівняльному аналізі національних засобів інформаційної безпеки, інститутів організації адміністративно-правового регулювання відносин, засад діяльності органів держави, адміністративних процедур та ін. Тому метою компаративістики не має бути порівняльне дослідження як самоціль.

Іншими функціями компаративістики можна визначити: взаємопроникнення певних елементів правових інститутів, процедур чи рішень з однієї до іншої правової системи та зміцнення міжнародного правопорядку; сприяння у реформуванні інститутів національного права на основі позитивного зарубіжного досвіду при коректному застосуванні методів компаративістики; виявлення і стимулювання досліджень у суміжних сферах правової діяльності, яка пов'язана з іноземних елементом, з метою досягнення оптимальних процедур та рішень, що сприятимуть їх адаптації у певній країні [10].

Німецькі науковці Цвайґерт і Кьотц визначають чотири функції компаративістики, що мають прикладне значення, — результати порівняльно-правових досліджень як матеріал для законодавця; інструмент для тлумачення законодавства; значення висновків компаративістики для юридичної освіти і її роль в уніфікації права [18].

У межах забезпечення інформаційної безпеки матеріали, отримані в результаті компаративістських досліджень досвіду іноземних, більш розвинених країн, мають неоціненне значення для обміну досвідом у сфері законодавчої техніки, формування якісно нових масивів адміністративно-правових процедур. Як приклад, ми спостерігаємо, що в структурі прийнятих нових законів з'явились положення, що розпочинаються з основних дефініцій тощо. Якісне пристосування правових інститутів сприяє об'єктивному зближенню правових систем, стандартизації правових процедур, формуванню єдиного правового поля в межах наднаціональних структур, особливо стосовно такого транснаціонального питання, як інформаційна безпека. Особливо в наш інформаційний вік, коли кожна країна робить свій внесок у загальну систему інформаційної безпеки планети Земля.

У сфері адміністративно-правової організації інформаційної безпеки підприємств очікує свого вирішення лише техніка тлумачення актів законодавства, тому завданням компаративістики залишається отримання висновків для запровадження певних елементів іноземного досвіду в Україні. Слід звертатися до досвіду найрозвиненіших країн світу — Німеччини, Франції та США.

Тому для подальшого розуміння припускаємо, що основними функціями компаративістики є: 1) зближення національних законодавств шляхом прийняття або рецепції прийнятних законодавчих процедур та їх оптимізації; 2) вироблення єдиних концепцій, доктрин, юридичних конструкцій та одноманітних правових норм, стандартизація юридичних процедур; 3) вироблення єдиних критеріїв інтерпретації правових норм, забезпечення одноманітного режиму їх реалізації [12].

Аналізуючи критерії організації інформаційної безпеки, можемо дійти висновку, що інформаційна політика підприємства має бути спрямована на оновлення технологічних фондів (оснащення, підготовка фахівців) за рахунок корпоративних коштів, або шляхом економічних преференцій суб'єктам (система кредитів); забезпечення гарантій (умов) реалізації комунікативних прав усіх суб'єктів; стимулювання розвитку інформаційної безпеки одночасно з неухильним збільшенням прибутків. Таким чином, ідеальна інформаційна безпека підприємства має максимально ефективно діяти у кожному з напрямів зазначених критеріїв [9; 11; 13–15]. У свою чергу Г. Г. Почепцов, проаналізувавши сучасну зарубіжну практику організації інформаційної безпеки, виокремлює такі напрями ефективної інформаційної політики [2]:

- заохочення конкуренції, боротьба з монополізмом (передусім державний контроль за концентрацією засобів масової інформації);
- забезпечення права і технічних можливостей для доступу до інформації та інформаційних ресурсів для всього населення;

- дотримання свободи слова;
- захист інтересів національних меншин, підростаючого покоління в інформаційній сфері;
- захист національної культурної спадщини, мови, протистояння культурної експансії інших країн;
- охорона інтелектуальної власності, боротьба з піратством;
- боротьба з комп'ютерними і злочинами, пов'язаними з високими технологіями;
- впровадження електронного уряду;
- правове регулювання мережі Інтернет.

Тому, виходячи з того, якою має бути оптимальна модель інформаційної безпеки, можемо проаналізувати політичні і правові тенденції у цій сфері як на міжнародному (глобальному, регіональному), так і на національному рівні.

Відзначимо, що історія міжнародної співпраці у питанні розвитку інформаційної безпеки бере свій початок із промови віце-президента США А. Гора на Конгресі фахівців Міжнародного союзу електрозв'язку в Буенос-Айресі в 1994 р. У цій промові А. Гор визначив п'ять головних принципів побудови сучасного інформаційного суспільства, що були покладені в основу напрямів розвитку інформаційної безпеки: 1) заохочення приватних інвестицій; 2) сприяння розвитку конкуренції; 3) створення рухомої регулюючої структури для підтримки темпів технологічного і ринкового розвитку; 4) забезпечення відкритого доступу до мережі усіх провайдерів; 5) створення універсальної служби та організація універсального обслуговування [6].

Найбільш впливова і розвинена міжнародна організація ООН також визначає головні напрями розвитку інформаційної безпеки у документі "ЮНЕСКО та інформаційне суспільство для всіх" у 1996 р. [3]:

- інфраструктура: її фінансування, розвиток і стійкість;
- визначення і подолання бар'єрів, що перешкоджають створенню інформаційного суспільства;
- освіта, розвиток людських ресурсів і професійна підготовка;
- доступ до інформаційних і комунікативних технологій;
- безпека інформації в мережевому середовищі;
- розробка політики і регламентних меж;
- види застосування ІКТ (освіта, охорона здоров'я, культура, державне управління, працевлаштування, бізнес).

ООН зобов'язує себе сприяти організації інформаційної безпеки таким чином, щоб це позитивно позначилося на розвитку суспільства, покладаючи певний перелік обов'язків на органи своїх країн-учасниць. Тому українському законодавцю та адміністратору на підприємстві не можна нехтувати цими положеннями під час створення адміністративно-правових норм власної інформаційної безпеки.

Аналізуючи доповідь уряду США, яка відбулася ще у 1993 р., що була присвячена планам розвитку інформаційної інфраструктури, знаходимо, що інформаційна безпека США має забезпечуватись за такими принципами:

- згідно з визначеними заздалегідь цілями та завданнями, які мають регулюватися законодавчо, включаючи забезпечення конкуренції;
- бути досить гнучкими, щоб дати змогу впроваджувати нові послуги і технології без внесення додаткових виправлень у законодавство;
- делегувати широкі повноваження суб'єктам забезпечення інформаційної безпеки підприємств, незалежним від національних органів;
- встановити відкритий процес участі підприємств у написанні норм адміністративного регулювання цього процесу [3; 4].

Необхідно зауважити, що вихідним в інформаційній безпеці США є принцип підтримання та розвитку конкуренції між державними і приватними суб'єктами забезпечення інформаційної безпеки. В той час в Україні існує певна монополія держави на впровадження заходів забезпечення інформаційної безпеки підприємств та організацій, ні про яку здорову конкуренцію йтися не може. Держава не делегує частину своїх прав і не підтримує інформаційну безпеку на потрібному рівні. Рівень підготовки кадрів бажає бути кращим, але не розвивається через відсутність певного попиту на спеціалістів цієї кваліфікації.

Досвід США для нас найбільш корисний з боку компаративістики та подальшого впровадження. Окремі моменти теорії інформаційної безпеки розроблювались Т. Шелінгом, Г. Каном, Р. Лиска, Г. Снайдером, К. Норром, З. Бжезінським, Е. Люттваком, М. Портером, Г. Кісінджером та ін.

Основним напрямом розвитку інформаційної безпеки в США є забезпечення саме безпеки інформаційних систем відомств та підприємств — від державних до приватних. З 1992 року значні зусилля з організації заходів у сфері інформаційної безпеки здійснювались Міністерством оборони США в межах концепції "Інформаційного протиборства", що спрямована на вирішення завдань боротьби з ворожими системами управління на усіх рівнях і збереження безпеки та ефективності власних інформаційних систем [5].

Відповідно до стратегії інформаційної безпеки основними пріоритетними напрямами мають бути [4]:

1. Становлення та розвиток національної системи реагування на події у сфері інформаційної безпеки.

2. Реалізація комплексної системи заходів зі зменшення загроз інформаційної безпеки.

3. Забезпечення підготовки спеціалістів у сфері комп'ютерної безпеки та відповідального відношення всього населення до питань захисту інформації.

4. Забезпечення захисту інформаційних систем, підприємств та державних органів.

5. Розвиток різних форм кооперації (у тому числі й міжнародних) у сфері забезпечення інформаційної безпеки.

Іншими пріоритетами національної інформаційної політики США було визначено: "підтримка наукових розробок у галузі інформації і комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудову та вдоско-

налення інформаційної інфраструктури, контроль за її діяльністю, побудову глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформацію як суспільне благо, інформацію як товар, інформацію як невіддільний компонент існування держави (необхідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин); недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; творення державної політики в галузі інформації і комунікації" [6]. Як бачимо, перед нами відкривається досить глобальна картина з боку компаративістики, виходячи з аналізу досвіду США.

Однією з головних рис політики США у сфері інформаційної безпеки є поєднання ринкових інструментів регулювання інформаційної безпеки і прямого державного контролю над інформаційними ресурсами в національних і міжнародних масштабах. Може здаватись, що ці напрями суперечать один одному. США намагалися створювати сприятливі умови для розвитку інформаційного сектору економіки, передавши велику частку державних військових технологій у приватний сектор. Одночасно використовувались механізми державного політичного контролю, шляхом створення стандартів у інформаційній сфері, через застосування комерційних технологій в органах державної влади, а також залученням приватних компаній для ведення розвідувальної та контррозвідувальної діяльності. Такий досвід, з готовою моделлю забезпечення інформаційної безпеки в державі та на підприємствах, просто неоціненний для України з боку компаративістики та впровадження в національну правову систему. Особливо заслуговує на увагу відношення до популяризації наукових розробок та підготовки кваліфікованих спеціалістів цієї сфери [12].

Головним аспектом у політиці адміністрації Президента Б. Обами у питаннях забезпечення інформаційної безпеки стало більш тісне співробітництво держави і бізнесу, спрямоване на захист державних інформаційних ресурсів, а також всього інформаційного простору США. Розроблено важелі втручання та засоби контролю американської держави стосовно інформаційної сфери, не виключаючи інформаційний сектор економіки.

Досвід США у сфері інформаційної безпеки підприємств та державних органів може бути актуальним об'єктом компаративістики для багатьох питань українських законодавців. Насамперед необхідно звернути увагу на ефективний підхід до регулювання ринку інформаційних технологій. Україна має необхідний потенціал для того, щоб бути повноправним учасником світового інформаційного суспільства. Зауважимо, що ефективність державної політики у цій сфері має не менш важливу роль поряд з рівнем технологічного розвитку [5]. Інформаційна безпека підприємств може стати одним із основних напрямів взаємовигідного співробітництва між Україною та США.

Створенням національної системи інформаційної безпеки ретельно займалася також Франція, реалізовуючи відповідну державну програму "Мі-

нітель" [7]. Одночасно велика та комплексна частки розробки питання щодо забезпечення інформаційної безпеки, у контексті розбудови інформаційного суспільства, здійснювалися Європейським Союзом. З 1994 року ці питання розв'язалися на теренах ЄС в межах четвертої рамкової програми протягом наступних чотирьох років. Потім приймались п'ята та шоста програми, а також низка інших тематичних актів, що задають зміст інформаційній безпеці Співтовариства. Конкретніше це виявлялося у спільному підході Співтовариства до побуди загальної системи інформаційної безпеки; міждержавного регулювання інформаційної сфери; впровадження програми та плану дій "е-Європа"; захисту даних; захисту авторських і суміжних прав; електронної торгівлі; безпеки цифрових мереж від негативного втручання; супутникового зв'язку; радіочастоти; телезв'язку і ринку інформаційних послуг; ліцензії; стандартизації; європейських угод щодо мереж; системи платежів; телефонії; регламенту взаємодії органів та суб'єктів забезпечення інформаційної безпеки організацій різних форм власності [16].

Згідно із Законом України "Про інформацію" основними напрямами державної політики із забезпечення інформаційної безпеки в державі визнаються [8]:

- забезпечення доступу громадянам до інформації;
- створення національних систем і мереж інформації;
- зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;
- забезпечення ефективного використання інформації;
- сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- створення загальної системи охорони інформації;
- сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України.

Також слід враховувати те, що 29 грудня 2016 р. Рада національної безпеки та оборони України затвердила проект Доктрини інформаційної безпеки України. Тому можемо пишатися, що в нашому правовому полі відбуваються зміни на зміцнення системи інформаційної безпеки країни та її організацій. Проте, вивчивши проект Доктрини, помічаємо, що він стосується протидії інформаційному вторгненню Росії, як країни агресора, на нашу суверенну територію. Водночас Доктрина регламентує санкції стосовно посадовців органів, незаконно сформованих на окупованих територіях АР Крим, Донецькій та Луганській областей. Основними виконавцями та суб'єктами положень Доктрини визначено відповідні Міністерства та Службу безпеки України [19]. Проводячи компаративістський аналіз нової української Доктрини та вказаних положень передових держав, бачимо досить вузьке коло питань, висвітлених у Доктрині. Зрозуміло, що українська Доктрина виникла на тлі необхідності боротьби із агресором, але можна було б розширити тематику напрямів забезпечення інформаційної безпеки в Україні. Потрібно було б розширити коло виконавців, приділивши увагу недержавним суб'єктам інформаційної безпеки, особливо на підприємствах.

Таким чином, кожна із зазначених країн світу орієнтується на той ринок, менталітет та актуальні завдання правових систем, які цій країні (групі країн) властиві. Так, у США та країнах ЄС велику увагу приділяють захисту суміжних прав і правам інтелектуальної власності приватних підприємств, а також стимулюванню конкуренції у сфері інформаційної безпеки підприємств. В Україні акценти зміщені щодо державного забезпечення гарантій здійснення інформаційної безпеки підприємств, захисту прав окремої людини і громадянина.

Однак варто зазначити, що загальним для всіх світових підходів в організації інформаційної безпеки на підприємствах є усвідомлення необхідності активного залучення недержавних суб'єктів цієї сфери, зменшення державного регулювання та впливу під час розбудови національної системи інформаційної безпеки, яка повинна, великою мірою, складатися з різноманітних систем інформаційної безпеки окремих підприємств та організацій.

Джерела

1. *Скалацький В. М.* Інформаційне суспільство: сучасні теорії та моделі (соціально-філософський аналіз): дис.: 09.00.03 / В. М. Скалацький. — Київ : Київ. нац. ун-т ім. Тараса Шевченка, 2006. — 181 с.
2. *Почепцов Г. Г.* Інформаційна політика: навч. посіб. / Г. Г. Почепцов, С. А. Чукут. — Київ : Знання, 2006. — С. 130–211.
3. *Information* Superhighway: An Overview of Technology Challenges [Доповідь Конгресу США] / USA Congress. — Washington, 1995.
4. *Brown R.* The Global Information Infrastructure: Agenda of Cooperation [Електронний ресурс] / R. Brown, L. Irving, A. Prabhakar, S. Katzen. — 1995. — Режим доступу: http://www.ntia.doc.gov/report/1995/globalinformation-infrastructure-agenda-cooperation
5. *Building* the Information Society: Moving Canada into the 21st Century [Нормативний документ Міністерства Постачання та Послуг Канади] / Ministry of Supply and Services. — Ottawa, 1996.
6. *Шевчук О.* E-Ukraine — "Електронна Україна" [Електронний ресурс] / О. Шевчук, О. Голобуцький. — Режим доступу: http://www.e-ukraine.biz/ukraine5.html
7. *Проект* Плана действий, 2003–2005. — Женева-Тунис — (Всесвітня зустріч на вищому рівні з питань інформаційного суспільства) // Документ WSIS/PC-3/DT-2 (Rev. 1) -R.
8. *Закон* України "Про інформацію" від 02.10.1992 р. № 2657-XII [Електронний ресурс] // ВРУ. Офіційний веб-портал. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/2657-12
9. *Деньщиков А. Л.* Информационная стратегия США (анализ, современность, перспективы): автореф. дис. ... канд. юрид. наук [Электронный ресурс] / А. Л. Деньщиков. — Режим доступа: http:rudocs.exdat.com
10. *Логунов А. Б.* Региональная и национальная безопасность: учеб. пособие / А. Б. Логунов. — Москва : Вузовский учебник, 2009. — 432 с.
11. *Соснін О. В.* Державна політика в галузі управління інформаційним ресурсом України: дис. ... д-ра політ. наук: спец. 23.00.02. / О. В. Соснін; Одес. нац. юрид. акад. — Одеса, 2005. — 264 с.
12. *Общая* политика США в сфере информационной безопасности / [Электронный ресурс]. — Режим доступа: http:www.INTUIT.ru

13. *Шариков П. А.* Политические проблемы международных отношений и глобального развития : автореф. дис. ... канд. полит. наук. / П. А. Шариков. — Москва, 2004. — 20 с.
14. *Туманова Л. В.* Обеспечение и защита права на информацию / Л. В. Туманова, А. А. Снытников. — Москва : Городец-издат, 2001. — 345 с.
15. *Волковский В. И.* Экономическая безопасность и информация / В. И. Волковский // Информационная безопасность России в условиях глобального информационного общества: Инфофорум-4: сб. материалов 4-й Всерос. конф. — Москва, 2002. — С. 70–71.
16. *Давид Р.* Основные правовые системы современности / Р. Давид, К. Жоффре-Спинози; пер. с фр. В. А. Туманова. — Москва: Междунар. отношения, 1999.
17. *Осакве К.* Сравнительное правоведение в схемах: общая и особенная часть / К. Осакве. — Москва: Дело, 2000.
18. *Цвайгерт К.* Введение в сравнительное правоведение в сфере частного права: в 2 т. / К. Цвайгерт, Х. Кетц; пер. с нем. — Москва: Междунар. отношения, 1995. — Т. 1. Основы.
19. *Проект* Доктрини інформаційної безпеки України від 29.12.2016 р. [Електронний ресурс]. — Режим доступу: http://www.rnbo.gov.ua/news/2678.html

Коректне ставлення до зарубіжного досвіду дає змогу в майбутньому зробити реальну оцінку певним правовим явищам та ситуаціям, визначити межі сприйняття окремих аспектів іноземного права. Залежно від ситуації масштаби використання результатів компаративістики можна застосовувати у формуванні юридичних кадрів, діяльності юридичного співтовариства, бізнесовій сфері, законодавчій, правозастосовчій та інтерпретаційній діяльності. Звичайно, цей процес передбачає зміни у структурі всієї системи національної інформаційної безпеки України.

The correct attitude to foreign experience allows, in the future, to make a realistic assessment of certain legal situations and phenomena, to define the boundaries of perception of certain aspects of foreign law. Depending on the situation, the extent of use of the results of comparative studies can be used in the formation of the legal frame of the legal community, business, legal, enforcement and interpretive activities. Of course, this process involves changes in the structure of the entire system of national information security of Ukraine.

Корректное отношение к зарубежному опыту позволяет в будущем сделать реальную оценку определенным правовым явлениям и ситуациям, определить границы восприятия отдельных аспектов иностранного права. В зависимости от ситуации масштабы использования результатов компаративистики можно применять в формировании юридических кадров, деятельности юридического сообщества, сфере бизнеса, законодательной, правоприменительной и интерпретационной деятельности. Конечно, этот процесс предполагает изменения в структуре всей системы национальной информационной безопасности Украины.

Надійшла 28 грудня 2016 р.