УДК 347.73

А. В. Бригінець
здобувач
Науково-дослідного інституту публічного права

АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ ПРАВОВОГО РЕГУЛЮВАННЯ КОНФІДЕНЦІЙНОСТІ У ФІНАНСОВО-ПРАВОВИХ ВІДНОСИНАХ

У сучасній українській науці актуальні питання правового регулювання конфіденційності у фінансово-правових відносинах досліджені частково. Зокрема, це пояснюється тим, що система захисту інформації з обмеженим доступом у нашій державі перебуває на етапі становлення, а її дослідники – у стані постійного активного наукового пошуку. Проте дане явище не носить конструктивного та позитивного характеру, оскільки серед провідних науковців та вчених не вироблений єдиний підхід до вирішення нагальних питань у даній сфері. Варто погодитись, що особливу актуальність та ключове значення для нас становлять питання правового захисту і належного правового регулювання даного, вкрай важливого напряму, який, на жаль, законодавець залишає поза своєю увагою. Для ефективного подолання наявних правових прогалин необхідно насамперед розглянути й проаналізувати правове забезпечення конфіденційності у фінансово-правових відносинах провідних держав.

Потрібно відзначити, що у вітчизняній науковій літературі досить багато наукових публікацій, які присвячені аналізу зарубіжного досвіду правового регулювання конфіденційності. Але вони лише фрагментарно розглядали правове забезпечення комерційної таємниці у фінансово-правових відносинах.

Метою статті є визначення сутності проблем зарубіжного досвіду правового регулювання конфіденційності у фінансово-правових відносинах.

Розроблення та прийняття відповідних нормативно-правових актів у сфері регулювання конфіденційності у фінансово-правових відносинах у розвинених державах світу визначається як важлива і відповідальна діяльність. З історичних фактів відомо, що основоположними правовими актами в інформаційній сфері були закони про охорону державної таємниці, тобто законодавчі документи в галузі захисту інформації. У ФРН для належного захисту вітчизняних секретів були спеціально визначені кримінально-правові наслідки за протиправні діяння, пов'язані з розголошенням, передачею або втратою важливих державних документів та секретів, шпигунство, а також інші дії, які наносили шкоду державі. Німецьке Уложення 1871 року передбачало позбавлення волі за розголошення відомостей, які необхідно було зберігати у таємниці від інших держав [1, с. 45].

Крім розробки й прийняття законодавчих актів в інформаційній сфері, до заходів охорони конфіденційності у фінансово-правових відносинах належать: видання директив, положень, інструкцій, методичних рекомендацій, які безпосередньо регламентують режим використання інформації на підприємствах, установах, організаціях; проведення спеціальної перевірки осіб на компетентність у роботі з документами, матеріалами й виробами, що містять інформацію конфіденційного характеру; впровадження посиленої фізичної та технічної охорони об'єктів, на яких зберігаються матеріали, що потребують захисту; періодичне проведення різнопланових профілактичних заходів тощо.

У кримінальному законодавстві держав континентальної системи права існують свої відповідні норми, що охороняють конфіденційність у фінансово-правових відносинах. Наприклад, Кримінальний кодекс Королівства Іспанії (далі – Іспанія) містить детальну регламентацію кримінально-правової охорони комерційної таємниці. У діючому правовому акті зазначається, що той, хто з метою розкрити комерційну таємницю заволодіє яким-небудь способом відомостями, письмовими або електронними документами, інформаційними пристроями чи іншими об'єктами, які відносяться до комерційної таємниці, карається відповідно до норм чинного законодавства [2]. Передбачене законодавством покарання значно збільшується, якщо розкрита таємниця буде поширюватися, видана або передана третім особам. Ряд норм Кримінального кодексу Іспанії передбачає відповідальність за наслідки, що настали через розголошення конфіденційної інформації економічного характеру.

У Кримінальному кодексі Французької Республіки (далі – Франція) правова регламентація охорони конфіденційності у фінансово-правових відносинах регламентована досить детально. Наприклад, розділ «Про зазіхання на таємницю» містить перелік злочинів, що можливі у відповідній сфері [3].

Кримінальне законодавство центральних держав Європи містить свої характерні особливості регламентації кримінально-правової охорони конфіденційності у фінансово-правових відносинах. Наприклад, Кримінальний кодекс ФРН основу класифікації таємниці зосереджує на злочи-

нах проти публічних інтересів та злочинах проти приватних інтересів [4, с. 43–44]. Законодавчо визначається відповідальність за незаконне розголошення таємниць довіреною особою, яка стала їй відомою під час здійснення власної діяльності. Встановлюється кримінальна відповідальність за використання відомостей, що становлять комерційну таємницю, яку особа зобов'язана була зберігати. Винятковий обов'язок щодо стосовно збереження комерційної таємниці покладено на посадових осіб фіскальних органів. Наприклад, відповідальності підлягає особа, яка безпідставно розголошує або використовує виробничу чи комерційну таємницю, яка їй не належить, але стала відома їй як посадовій особі під час такої діяльності. Питання стосовно боротьби з розкраданням секретів виробництва у сфері промисловості й торгівлі сформульовані досить детально в діючому законодавстві. До них відносяться: «Федеральний закон про охорону даних», «Закон про боротьбу з несумлінною конкуренцією», «Постанова про боротьбу з підкупом непосадових осіб» тощо. Для вдосконалення існуючого захисту конфіденційності у фінансово-правових відносинах у ФРН реалізовуються такі напрямки: деталізація та оновлення законодавства у сфері захисту державної таємниці; посилення органів безпеки та надання їм більших повноважень; створення організацій «самодопомоги» в промисловості й розгортання їхньої діяльності. Вважаємо, що у ФРН, як і загалом у державах-членах Європейського Союзу (далі – ЄС), недостатність засобів покарання, передбачених чинним законодавством, не сприяє підвищенню ефективності боротьби з промисловим шпигунством. Іншу причину німецькі вчені вбачають у протидії, яку промислові кола роблять спробам посилення заходів щодо охорони секретів виробництва, оскільки за нормами «Закону про несумлінну конкуренцію» постраждалі фірми часто уникають звертатися в судові органи з ряду причин, у тому числі побоюючись підриву своєї комерційної репутації.

Огляд сучасного законодавства розвинених держав як загального, так і континентального права дає можливість вести мову про наявну спільність кримінально-правової охорони конфіденційності у фінансово-правових відносинах [5, с. 37–38]. Крім того, у багатьох провідних державах використовується позитивна практика стосовно збереження конфіденційності працівниками підприємств за відповідною угодою. Особа не допускається до такої інформації або ж взагалі не приймається на роботу без укладання такої угоди. Відповідно, на службовців, так само як і на працівників приватного сектора, досить часто покладається відповідне зобов'язання не розголошувати інформацію з обмеженим доступом. Зобов'язання зберігати інформацію можуть поширюватись на відомості, що стосуються політики, виробничої, наукової та комерційної діяльності, а також на особисті дані працівників. Також службовці можуть бути зобов'язані зберігати інформацію особистого характеру їхніх стосунків із громадянами. Зауважимо, що конфіденційність в окремих випадках вступає в конфлікт із тим, що відноситься до інтересів суспільства. Наприклад, у Великобританії інтерес суспільства визнається важливішим від питань збереження конфіденційності. У розвинених європейських державах під час прийому на роботу, пов'язану з використанням інформації з обмеженим доступом, досить часто використовується спеціальний прилад – поліграф. Також його використовують під час проведення розслідувань, пов'язаних з витоком інформації, обмеженої в доступі. У США досить багато осіб без попереднього попередження проходять перевірку на поліграфі, що є умовою продовження з ними контракту. Дана умова обумовлюється у вищезазначеній угоді [6, с. 158–164]. Сучасні детектори є доволі складними приладами, які одночасно охоплюють кілька фізіологічних процесів людини. Але відношення до поліграфу, особливо в державах-членах ЄС, є неоднозначним. Наприклад, у ФРН поліграф не може використовуватися під час прийому на роботу. Вважається, що дана перевірка багато в чому залежить від підготовленості оператора, який скеровує даний пристрій.

Необхідно звернути увагу на те, що Великобританія законодавчо не закріплювала захист конфіденційності в цілому, а також у фінансово-правових відносинах зокрема. І тільки 1981 року був прийнятий Закон «Про порушення конфіденційності». Вказаний нормативний акт і до сьогодні регулює всі питання, пов'язані з конфіденційністю, встановлює відповідальність за порушення конфіденційності, а також засоби судового захисту, що застосовуються під час таких процедур. Дещо пізніше з введенням у дію Закону «Про свободу інформації» було запроваджено певну процедуру розголошення інформації з обмеженим доступом, якою володіють органи державної влади або особи, які надають послуги громадянам. Під час розголошення такої інформації аналізується можливість заподіяної шкоди певним інтересам. Проте положення даного нормативно-правового акту чітко не визначили випадки, в яких органи влади повинні так діяти. Обмеження доступу до інформації залежить від даних, що містяться в документі: інформація, пов'язана з питаннями національної безпеки; інформація, з якою працюють судові органи; записи судових органів; інформація стосовно державної політики; інша конфіденційна інформація.

Особливу увагу уряд приділяє захисту секретних відомостей державного апарату. Розроблені спеціальні рекомендації стосовно правил поводження та дотримання таємниці під час виконан-

ня службових обов'язків. Відповідно до вказаних рекомендацій члени кабінету міністрів зобов'язані підтримувати імідж і єдність англійського уряду та зберігати в таємниці все, що стосується їхньої діяльності. У разі призначення на посаду необхідною умовою є проходження інструктажу з питань забезпечення державної безпеки. Інструктаж проводять працівники служби безпеки та контррозвідки. Кожний новопризначений на посаду член уряду підписує декларацію, яка засвідчує його ознайомлення з основними постулатами Закону «Про державну таємницю». Керуючись положеннями закону про державну таємницю, а також закону про конфіденційність, пріоритетним завданням уряду стає вжиття активних заходів щодо попередження та запобігання витоку секретних відомостей через засоби масової інформації. Відповідно до положень указаних нормативних актів уряд має право вимагати через суд першої інстанції заборонити публікацію матеріалів, які містять секретні відомості. Разом із тим автору можуть заборонити публікування матеріалів і за кордоном. Водночас суд має право зобов'язати автора забрати рукопис із будь-якого іншого видавництва. Якщо автор бажає, щоб заборона була знята, йому необхідно подати на розгляд уряду зміст публікації, а також перелік використаних джерел. 1995 року розроблено нову процедуру перевірки державних службовців, які мають доступ до секретної інформації. Пришвидшили реалізацію даного заходу часті випадки підкупу посадових осіб, у тому числі й спецслужбами іноземних держав. Перевірки банківських рахунків та кредитних платежів здійснюються стосовно службовців, які мають тривалий та неконтрольований доступ до секретних документів. Про всі випадки виявлення внесків підозрілого походження відразу інформується служба безпеки. Особи, які мають доступ до цілком таємних матеріалів, перевіряються найбільш детально. Передусім це стосується працівників спецслужб, котрі працюють під прикриттям за кордоном або виконують обов'язки офіцерів зв'язку при штаб-квартирах іноземних спецслужб.

Дослідження основних положень законодавства дозволяє говорити про те, що в його основі закладена ідея систематизації інформації з обмеженим доступом. Таким чином, прослідковується відмова від поділу інформації з обмеженим доступом на державну таємницю та конфіденційну інформацію. З цієї позиції основну роль відіграють різновиди обмеження доступу до інформації, які встановлюються законодавством. Виходячи з вищезазначеного, «конфіденційність» слід розглядати як ознаку інформації з обмеженим доступом, а також як ключову характеристику її правового режиму. На жаль, у законі не наведено повний перелік інформації з обмеженим доступом, а лише зазначені найбільш типові її різновиди. Вказана спроба систематизації інформації з обмеженим доступом отримала неоднозначні відгуки наукової спільноти. В основному причинами цього являється різне тлумачення та розуміння значення термінів «конфіденційна інформація», «конфіденційність», «таємність». Значна частина науковців вважає рівнозначними між собою ці поняття.

Окрему увагу приділяють конфіденційній інформації, вказуючи, що це основний термін для позначення всієї інформації з обмеженим доступом [7, с. 154–159; 8, с. 5–7]. Водночас, як справедливо вказує Л.К. Терещенко, поняття «конфіденційна інформація» має свої певні особливості. Наслідком цього є те, що не вся інформація з обмеженим доступом може розглядатися як така [9, с. 72]. Термін «конфіденційний» можна дослівно перекласти як «довірчий» по відношенню безпосередньо до інформації, у випадках передачі її власником іншим суб'єктам, тобто забезпечити її конфіденційність. Необхідність останнього викликана її наявністю у власника, який може опинитися під загрозою в результаті поширення інформації або передачі без згоди останнього третім особам. У даному випадку «конфіденційність» як вимога стосується виключно особи, яка відповідно до норм закону, а також за бажанням власника отримала доступ до інформації чи інших відомостей. Що стосується останнього, то власник, як правило, має право розпоряджатися та контролювати обіг інформації, що становить таємницю. Наприклад, усі існуючі різновиди таємниць фактично віднести до переліку «конфіденційної інформації» неможливо. У переважній більшості власник, тобто суб'єкт таємниці, здійснює її охорону самостійно та не передає інформацію іншим особам. У випадках передачі відомостей іншим особам вони набувають статусу держателя інформації, проте режим таємниці або інформації при цьому змінюється. У разі передачі відомостей державним органам така інформація вже охороняється в режимі службової таємниці. Таким чином, конфіденційною інформація стає у разі передачі її особі, вимушеній на підставі закону забезпечувати її конфіденційність, передусім в інтересах власника. Як бачимо, термін «конфіденційність» може бути застосовано виключно до держателів інформації, тоді як власник здійснює безпосередній захист інформації, як правило, добровільно, у своїх власних інтересах, так само як і відмовляється від неї. Зазначимо, що термін «конфіденційність» широко використовується у відносинах, що виникають між роботодавцем до працівником, тобто у трудових відносинах. У даному випадку найманих працівників тимчасово допускають до такого виду інформації для виконання ними власних посадових обов'язків. Загалом, законодавством РФ визначено умови

віднесення інформації до категорії конфіденційної, а також необхідність дотримання такої конфіденційності, але водночас не визначено правил та вимог стосовно її забезпечення. Наприклад, у Податковому кодексі зазначається, що відомості, які були отримані податковими органами і становлять податкову таємницю, мають спеціальний режим зберігання та доступу [10].

Також, у сфері аудиту підприємство, що отримало у процесі власної професійної діяльності доступ до конфіденційної інформації особи, зобов'язано забезпечити її збереження [11]. Існуючий Закон «Про інформацію, інформаційні технології і захист інформації» лише визнає термін «конфіденційність» як обов'язкову для виконання особою, яка одержала доступ до певної інформації, вимогу не передавати таку інформацію третім особам без згоди її власника. З іншого боку, Указом Президента РФ «Про затвердження переліку відомостей конфіденційного характеру» до відомостей конфіденційного характеру віднесено: службову таємницю; персональні дані; відомості, пов'язані з професійною діяльністю; комерційну таємницю та інші [12]. Відповідний перелік даних, що міститься в Указі Президента РФ, не варто вважати повним, оскільки Закон «Про інформацію, інформаційні технології і про захист інформації» дозволяє власникові інформації особисто наділяти її статусом конфіденційності.

Зауважимо, що конфіденційність інформації виступає досить часто основою роботи з аудиторськими організаціями. З огляду на те, що аудиторські організації отримують доступ до повної та достовірної інформації про осіб, то саме на них спрямовується підвищена увага з боку правоохоронних органів та інших установ, що виявляють інтерес до цієї інформації. Важливою проблемою забезпечення конфіденційності інформації аудиторських організацій є питання про державне регулювання даної діяльності. Закон «Про аудиторську діяльність» зобов'язує аудиторів дотримуватись аудиторської таємниці та передбачає її надання державним органам лише в окремих виняткових випадках. Саме тому аудиторські організації повинні забезпечити максимальне виконання таких заходів забезпечення конфіденційності інформації, як, наприклад, розроблення і впровадження політики інформаційної безпеки, що являє собою документ, який містить перелік організаційних заходів забезпечення безпеки інформації та її цілісності. Враховуючи думку експертів, ключовим аспектом розробки політики інформаційної безпеки виступає аналіз ризиків інформаційної сфери, який полягає в аналізі ймовірних загроз, а також перелік заходів, необхідних для запобігання реалізації загроз щодо ресурсів організації [13, с. 69–73]. Зазвичай застосовуються кілька підходів до аналізу ризиків, зокрема: базовий, що включає в себе перевірку стандартного захисту від поширених загроз і виконання вимог сертифіката безпеки, та цілісний, що передбачає більш прискіпливу оцінку ресурсів підприємства. Більш доцільним вважаємо використання цілісного підходу до аналізу ризиків власної інформаційної системи.

Аудиторські організації повинні керуватися стандартами аудиторської діяльності, які базуються на принципах проведення аудиторської діяльності, а саме: конфіденційності, незалежності, професійної етики. Будь-яка аудиторська організація зобов'язана виробляти власні стандарти з метою практичної реалізації зазначених принципів. Працівники аудиторських організацій повинні знати внутрішні стандарти та виконувати їх. Як бачимо, будь-яка діяльність аудиторських організацій безпосередньо пов'язана з конфіденційністю у фінансово-правових відносинах, а саме з фінансовою інформацією, що є предметом власності інших юридичних осіб. У цьому полягає специфіка аудиторської діяльності, адже аудиторські організації зобов'язані не лише захищати дану інформацію, але й забезпечувати її конфіденційність. Особливістю вказаної діяльності є і те, що терміни дії аудиторської таємниці не встановлені законодавством, тобто передбачено обов'язок зберігати в таємниці конфіденційну інформацію про операції клієнтів, отриману під час надання професійних послуг, без обмеження термінів та незалежно від продовження або припинення безпосередніх відносин із ним. Виходячи з норм чинного законодавства, невірне використання інформаційних ресурсів, що перебувають у володінні аудиторських організацій, може спричинити серйозні наслідки. Максимальним із них визнається позбавлення волі на строк до трьох років із позбавленням права обіймати певні посади чи займатися певною діяльністю. Саме тому аудиторські організації повинні дотримуватися принципу конфіденційності та впроваджувати елементи політики інформаційної безпеки, яка здатна не тільки забезпечити конфіденційність інформації, що захищається, але й її доступність і цілісність. На жаль, через відсутність загальних вимог щодо забезпечення безпеки конфіденційної інформації відповідні суб'єкти повинні розробляти та застосовувати комплекс заходів на власний розсуд.

Як бачимо, досліджувана проблема забезпечення і дотримання конфіденційності інформації дослідниками розглядається досить по-різному. Доволі поширеним у науці є уявлення про те, що в разі отримання конфіденційної інформації відповідний режим таємниці перетворюється з одного режиму в інший. Наприклад, відомості про діяльність юридичних осіб являються предметом

комерційної таємниці, але вказана діяльність із банківськими рахунками захищається режимом банківської таємниці. Під час надання таких відомостей до фіскальних органів виникають відносини з приводу податкової таємниці, наприклад, режим податкової таємниці або службової таємниці. Тобто банківська, комерційна, професійна таємниці, персональні дані після подання їх до контролюючих органів не припиняють своє функціонування, оскільки до органів виконавчої влади передається не режим, а сама інформація. Конфіденційна інформація стає не тільки об'єктом обміну між особами та органами державної влади; всередині однієї організації можуть функціонувати відомості, що становлять комерційну таємницю, персональні дані, різновиди професійної таємниці, щодо яких власник повинен забезпечити конфіденційність.

Вищезгадані приклади свідчать, що для забезпечення конфіденційності однієї і тієї ж інформації доводиться встановлювати різні режими, які можуть призвести до виникнення конфліктів інтересів суб'єктів таємниць, тобто для виключення конфліктів під час здійснення інформаційного обміну доцільно закріпити в нормативних актах поняття «режим конфіденційності інформації», який дозволив би встановити єдині правила і вимоги до забезпечення безпеки інформації як в органах державної влади, так і юридичних осіб та ґрунтувався б на основі оцінки ризиків суб'єкта таємниці у фінансово-правових відносинах. Використовуючи оцінку ризиків у фінансово-правовій сфері, здійснюється виявлення загроз активів, оцінка уразливості відповідних активів та ймовірності виникнення загроз. Також важливим визнається використання законодавчих вимог для забезпечення узгодженості, цілеспрямованості, планомірності діяльності із забезпечення інформаційної безпеки; оцінка можливих наслідків; визначення адекватності заходів захисту з урахуванням принципу оптимальності витрат на захист конфіденційності у фінансово-правових відносинах.

Варто зазначити, що дослідження позитивного зарубіжного досвіду розвинених держав з метою поширення базових та основоположних підвалин даної сфери у вітчизняне законодавство є, безумовно, актуальним, як з наукового, так і з практичного погляду. Слід вказати, що режим конфіденційності у фінансово-правових відносинах визначається як предмет правового регулювання, який являє собою особливий правовий порядок, установлений державою за допомогою правових норм і забезпечений нею шляхом роботи з інформацією конфіденційного характеру, що включає в себе: збір, накопичення, зберігання, уточнення, систематизацію, використання, поширення, знищення. У зв'язку з цим розвинені держави для захисту власних інформаційних систем використовують відповідні механізми для їх охорони. Ефективність запровадження таких механізмів вимагає врахування передового досвіду в інформаційній сфері та у вітчизняній практиці стосовно належного захисту конфіденційності у фінансово-правових відносинах.

На нашу думку, багатогранність і множинність думок провідних учених та науковців, які досить часто мають суперечливий характер, можна пояснити передусім недосконалістю чинного законодавства, наявністю колізій у правовому регулюванні конфіденційності взагалі й у фінансово-правових відносинах зокрема. Вважаємо, що для вирішення всіх існуючих питань щодо належного врегулювання та забезпечення інституту конфіденційності, ліквідації ряду прогалин у законодавстві необхідно прийняти закон про конфіденційність, що зможе узагальнити та систематизувати основоположні постулати даної галузі. Даний нормативно-правовий акт надасть змогу об'єднати цілий масив норм, що є чинними в даний час, але розпорошені між низкою правових документів різних галузей права.

Література

1. Князєв С.О. Генезис системи охорони державної таємниці на території України: Аналітичний огляд / С.О. Князєв, О.В. Ботвінкін, О.А. Колєснік ; Вид-во НА СБ України. – К., 2005. – 88 с.

2. Уголовный кодекс Испании / под редакцией и с предисловием доктора юридических наук, профессора Н.Ф. Кузнецовой и доктора юридических наук, профессора Ф.М. Решетникова. – М. : ЗЕРЦАЛО, 1998. – 218 с.

3. Уголовный кодекс Франции. – СПб. : Юрид. Центр Пресс. – 2010. – 560 с.

4. Кузнецова Н.Ф. Уголовное право ФРГ / Н.Ф. Кузнецова, Л. Вельцель. – М., 2000. – 320 с.

5. Кибальник А.Г. Уголовная ответственность за незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну / А.Г. Кибальник, А.В. Масленников, И.Г. Соломоненко. – Ставрополь. – 2001. – № 25. – 350 с.

6. Климчук С. Загальна характеристика законодавства про інформаційну безпеку ЄС, США та Канади / С. Климчук // Юстініан, 2006. – № 11. – С. 158–164.

7. Ефремов А. Понятие и виды конфиденциальной информации / А. Ефремов // Программные продукты и системы ; под ред. С.В Емельянова. – № 4 (88). – 2014. – № 18. – С. 154–159.

8. Алексенцев А.И. О составе защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – 2002. – № 2. – С. 5–7.

9. Терещенко Л.К. Правовой режим информации / Л.К. Терещенко // Безопасность информационных технологий. – 2008. – № 65. – С. 72.

10. Налоговый кодекс Российской Федерации № 146-ФЗ от 31.08.1998 г. // Информационно-правовой портал Гарант [Электронный ресурс]. – Режим доступа : http://base.garant.ru/10900200/.

11. Федеральный закон «Об аудиторской деятельности» от 30 декабря 2008 г. // Собрание законодательства РФ. – 2009. – № 1. – Ст. 15.

12. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

13. Чернова Е.В. Обеспечение безопасности системы информационно-аналитической поддержки научных исследований / [Е.В. Чернова, И.В. Попова, Е.В. Попова, И.В. Зленко] // Программные продукты и системы ; под ред. С.В. Емельянова. – 2009. – № 4 (88). – 192 с.

Анотація

Бригінець А. В. **Аналіз зарубіжного досвіду правового регулювання конфіденційності у фінансово-правових відносинах.** – Стаття.

Стаття присвячена проблемам аналізу зарубіжного досвіду правового регулювання конфіденційності у фінансово-правових відносинах. Обґрунтовано, що виникло дане поняття досить давно, але у правовому вимірі розпочало знаходити своє відображення лише нещодавно.

Ключові слова: комерційна таємниця, фінансово-правові відносини, правове забезпечення.

Аннотация

Бригинец А. В. **Анализ зарубежного опыта правового регулирования конфиденциальности в финансово-правовых отношениях.** – Статья.

Статья посвящена проблемам анализа зарубежного опыта правового регулирования конфиденциальности в финансово-правовых отношениях. Обосновано, что возникло данное понятие достаточно давно, но в правовом измерении начало находить свое отражение лишь недавно.

Ключевые слова: коммерческая тайна, финансово-правовые отношения, правовое обеспечение.

Summary

Bryhinets A. V. **Analysis of foreign experience of legal regulation of confidentiality in financial and legal relations.** – Article.

The article is devoted to the problems of the analysis of foreign experience of legal regulation of confidentiality in financial and legal relations.It is proved that this conception appeared quite a while, but in legal dimension it began to reflect only recently.

Key words: commercial secret, financial and legal relations, legal support.