І. М. Колодій
викладач кафедри цивільно-правових дисциплін
Чернігівського державного інституту права,
соціальних технологій та праці

УДК 336.719.2 (477)

ПРИНЦИПИ ТА МЕТОДИ ЗАХИСТУ БАНКІВСЬКОЇ ІНФОРМАЦІЇ

В статті розглядаються особливості захисту банківської інформації. Визначені загальноправові та специфічні для банківської діяльності принципи захисту банківської інформації з врахуванням методологічних підходів до їх визначення та систематизації.
Ключові слова: інформаційна безпека банку, принципи захисту інформації, методи захисту інформації.

В статье рассматриваются особенности защиты банковской информации. Определены общеправовые и специфические для банковской деятельности принципы защиты банковской информации с учетом методологических подходов к их определению и систематизации.

The peculiarities of the bank information protection are considered in this article. The general legal and bank-specific principles of the bank information protection are determined, taking into account the methodological approaches when determining and systematization them.

Загальні засади банківського права, закріплені в його нормах, забезпечують цілеспрямоване регулювання банківської діяльності. Наявність об'єктивних взаємозв'язків та взаємозалежностей між фінансовою системою держави і банківською системою, фінансовою діяльністю держави і діяльністю банків, формування стійкої тенденції їх розширення і розвитку в умовах світової фінансової кризи обумовлює необхідність оптимізації фінансово-правового регулювання банківської діяльності і закріплення законодавцем її основоположних засад у вигляді спеціальних правових принципів.

Для банківської діяльності як особливого виду фінансово-економічної діяльності наявність закріплених в законодавстві спеціальних принципів також посилює притаманну їй якість системності. Оскільки діяльність банків пронизує всю соціально-економічну систему, принципові начала її організації важливі в рівних частинах як для держави і суспільства, так і для його громадян [1, с. 85].

Метою цієї статті є аналіз загальноправових та специфічних для банківської діяльності принципів захисту інформації з врахуванням методологічних підходів до їх визначення та систематизації. Реалізація відповідної мети передбачає виконання таких завдань: дослідження особливостей загальноправових принципів, що визначають напрямки розвитку відповідної галузі; виявлення взаємозв'язку між принципами характерними для підприємницької діяльності в цілому та специфічними для банківської діяльності; визначення можливих шляхів удосконалення нормативно-правової бази.

До проблем захисту банківської інформації в Україні зверталось багато авторів, зокрема, значний внесок зробили дослідники: І. А. Безклубий, М. І. Зубок, А. І. Марущак, Л. В. Ніколаєва, В. П. Паліюк, О. Е. Радутний, Г. О. Світлична, М. П. Стрельбицький, Л. М. Стрельбицька та ін.

www.univer.km.ua Університетські наукові записки, 2010, № 2 (34), с. 186-191.

В останні роки в Україні реалізовано ряд практичних заходів стосовно підвищення рівня банківської безпеки. Як результат сформована система нормативно-правового та організаційного забезпечення інформаційної безпеки банків, реалізовано практичні заходи по удосконаленню засобів інформаційної безпеки в самих банках. Разом із тим, рівень інформаційної безпеки банків на сьогоднішній день не відповідає об'єктивним вимогам, і стан захисту банків від злочинних посягань залишає бажати кращого.

Під захистом інформації розуміється комплекс заходів, які здійснюються власником інформації стосовно виокремлення своїх прав на володіння та розпорядження інформацією, створення умов, які обмежують її поширення і виключають чи суттєво ускладнюють несанкціонований, незаконний доступ до таємної інформації та її носіїв. Інформація що захищається, може містити дані, які належать до різних охоронюваних законом таємниць. Цілком природно, що кожний вид інформації, яка охороняється, може мати свої особливості в сфері регулювання, організації та здійснення захисту [2, с. 173].

Метою захисту інформації з обмеженим доступом є: попередження витоку, викрадення, втрати, викривлення, підробки такої інформації; попередження несанкціонованих дій щодо знищення, модифікації, викривлення, копіювання, блокування інформації; реалізація прав та законних інтересів на таку інформацію її власників [3, с. 86].

О. В. Олійник стверджує, що принципи віднесення відомостей до категорії з обмеженим доступом та встановлення обмежень доступу до цієї інформації мають регулювати суспільні відносини, які включають: прийняття рішень щодо необхідності віднесення цих відомостей до державної таємниці, до інших передбачених законодавством таємниць та до конфіденційної інформації; правила встановлення ступенів секретності (конфіденційності) вказаної інформації шляхом обґрунтування шкоди державним, суспільним, особистим інтересам у разі розголошення цих відомостей; норми і порядок встановлення обмежень на доступ до конкретної інформації з обмеженим доступом шляхом надання відповідного грифа секретності (конфіденційності) документам, виробам або іншим матеріальним носіям цієї інформації. У світовій практиці до цієї сфери захисту інформації належать наступні принципи: законність, обґрунтованість, своєчасність [4, с. 74].

Принцип законності передбачає розробку системи безпеки на основі законодавства в сфері підприємницької діяльності, інформатизації і захисту інформації, приватної охоронної діяльності та інших нормативних актів з безпеки, затверджених органами державного управління в межах їх компетенції з застосуванням всіх не заборонених методів виявлення і попередження правопорушень [5, с. 161]. Система законодавчих актів та розроблених на їх основі нормативних і організаційно-розпорядчих документів повинна забезпечувати організацію ефективного нагляду за їх виконанням з боку правоохоронних органів та реалізацію заходів судового захисту і відповідальності суб'єктів відповідних відносин [6, с. 16].

Принцип обґрунтованості полягає в тому, що можливості і засоби захисту, які використовуються на сучасному рівні розвитку науки та техніки, обґрунтовані з точки зору заданого рівня безпеки і мають відповідати встановленим вимогам і нормам [5, с. 161].

Принцип своєчасності передбачає постановку задач з комплексної безпеки на ранніх стадіях розробки системи інформаційної безпеки на основі аналізу і прогнозування обставин, загроз, а також розробку ефективних заходів попередження посягань на законні інтереси [5, с. 160]. Це зумовлено тим, що методи і засоби реалізації загроз інформаційній безпеці розвиваються випереджувальними темпами, порівняно з методами і засобами захисту інформації. У цілому знаходить своє відображення діалектика розвитку нападу і захисту. Крім цього, відомо, що розробка технічних засобів, які реалізують достатньо велику кількість загроз, базуються, як правило, на найостанніших досягненнях науки, техніки і технології, тому засоби протидії, тобто технічні засоби інформаційної безпеки (засоби технічного захисту інформації), повинні створюватись виходячи з цих умов [7,

Університетські наукові записки, 2010, № 2 (34), с. 186-191. www.univer.km.ua

с. 10].

В зв'язку з тим, що банківська діяльність є одним із видів підприємницької діяльності, право, яким вона регулюється, детермінується принципами двох типів: по-перше, — загальними для підприємницької діяльності в цілому; по-друге, — специфічними для банківської діяльності. Перші принципи являють собою елементи конституційного статусу суб'єктів підприємницької, а відповідно і банківської, діяльності, другі — визначають порядок побудови, функціонування і розвитку банківської системи [8, с. 48].

В свою чергу, принципи другої групи підрозділяються на: принципи організаційно-правової побудови і розвитку банківської системи України та принципи, які визначають порядок здійснення банківської діяльності. Ми підтримуємо позицію науковців [9, с. 90; 8, с. 57], які вважають, що саме до останньої групи необхідно віднести принцип банківської таємниці.

На сьогодні ситуація щодо правового регулювання банківської таємниці суттєво змінилася. По-перше, у процесі фінансової діяльності банки також оперують "інформацією з відкритим доступом" (наприклад, статутні документи, звітність банку, види та форми банківського обслуговування, своєчасність і повнота виконання банком своїх обов'язків як кредитора). В правовому полі банків існує "інформація з обмеженим доступом", яка поділяється на конфіденційну і таємну, а остання — на банківську таємницю і комерційну. По-друге, банківська таємниця є об'єктом цивільного права. Особливістю цього об'єкта цивільних правовідносин є те, що власником інформації, як правило, виступає клієнт банку, а банк є утримувачем такої інформації та зобов'язаним суб'єктом її збереження [10, с. 292]. По-третє, на банки покладений обов'язок щодо збереження банківської таємниці та відповідальність за незаконне її розкриття [11, с. 40].

На думку А. І. Марущака, режим захисту банківської таємниці, насамперед, можна визначати через можливість розкриття відомостей, що становлять банківську таємницю, перед сторонніми суб'єктами — не власниками такої інформації. Законодавство переважної більшості країн світу декларує певну гарантію захисту інформації, що містить банківську таємницю. Однак велике значення мають не декларативні гарантії, а конкретні правові механізми їх застосування [12, с. 76].

Правовий режим банківської таємниці встановлено Цивільним кодексом України та Законом від 7 грудня 2000 року № 2121–III "Про банки і банківську діяльність". Відповідно до ст. 1076 Цивільного кодексу України банк гарантує таємницю банківського рахунку, операцій за рахунком і відомостей про клієнта. Відомості про операції та рахунки можуть бути надані тільки самим клієнтам або їхнім представникам. Іншим особам, у тому числі органам державної влади, їхнім посадовим і службовим особам, такі відомості можуть бути надані виключно у випадках та в порядку, встановлених законом про банки і банківську діяльність [13, с. 25].

Оскільки будь-яке правове регулювання являє собою визначений вплив на суспільні відносини, здійснюється на основі деяких принципів, то, називаючи принципи правового регулювання використання і розвитку інформаційно-електронних технологій, необхідно зазначити, що під такими, перш за все, розуміються узагальненні ідеї, на основі яких повинні прийматися нормативні акти. До них можуть бути віднесені:

— принцип рівної безпеки особи, суспільства та держави, реалізація якого передбачає забезпечення безпеки електронних банків конфіденційної інформації за умови максимально допустимого обліку і задоволення інтересів особи, а також максимальний захист від загрози використання (створення) особою загрозливих для існування соціуму біоелектронних систем;

— принцип свободи вибору особою поведінки стосовно своєї конфіденційної інформації в електронних базах даних; він реалізовується в оцінці особою балансу затрат та прибутків при здійсненні тих чи інших дій, пов'язаних з доступом та зміною такої інформації;

— програмний принцип, який передбачає на міжнародному та національному рівнях здійснення політики, спрямованої на підвищення освітнього рівня в області розвитку інформаційно-електронних технологій шляхом створення нормативно-

www.univer.km.ua Університетські наукові записки, 2010, № 2 (34), с. 186-191.

правових умов, які визначають правила поведінки людей і процедури, пов'язані з використанням інформаційно-електронних технологій;

— принцип єдності правового простору, який породжує обов'язок держави не допускати перешкод для вільного переміщення інформаційно-електронних послуг та фінансів, якщо це негативно не впливає на забезпечення його безпеки, захист життя та здоров'я людей, охорону моральних цінностей суспільства [14, с. 70].

Отже, безпека інформації в сучасних умовах комп'ютеризації інформаційних процесів має принципове значення для запобігання незаконному і часто злочинному використанню цінних відомостей. Задачі забезпечення безпеки інформації реалізуються комплексною системою її захисту, що за своїм призначенням здатна вирішити безліч проблем, які виникають у процесі роботи з конфіденційною інформацією і документами [15, с. 38].

Наступною, не менш важливою, є проблема розробки методів визначення стійкості систем інформаційної безпеки банку й визначення відповідних технічних критеріїв, прийнятних для інженерної практики.

Сучасний ринок, у тому числі і банківських послуг, не може бути без ризику. Ризикованими є всі операції банку, а оскільки вся діяльність банку може бути відображена у вигляді конкретних відомостей, то цілком зрозуміло, що має існувати й інформаційний ризик. Досвід роботи банків із забезпечення їх інформаційної безпеки показує, що є чотири види інформаційного ризику банку: ризик витоку і руйнування необхідної для функціонування банку інформації, особливо такої, яка містить відомості таємного або конфіденційного характеру; ризик використання в діяльності банку необ'єктивної інформації; ризик відсутності у керівництва банку об'єктивної інформації; ризик розповсюдження ким-небудь у зовнішньому середовищі невідповідної або небезпечної для банку інформації.

Враховуючи особливість підприємницької діяльності банків, слід зазначити, що найбільший ризик банк має при втраті відомостей, що становлять банківську або комерційну таємницю [16, с. 31].

Якість управління банківськими ризиками є одним із ключових елементів укріплення фінансової стабільності банківської системи, підвищення довіри до неї з боку клієнтів, кредиторів та вкладників.

За посягання на комерційну та банківську таємниці може настати кримінальна, цивільна, адміністративна або дисциплінарна відповідальність, згідно з чинним законодавством. А це означає, що заходи захисту інформації повинні бути направлені на мінімізацію саме зазначених видів ризику [17, с. 399].

Всі методи оцінки ризиків умовно можна розділити на прямі і побічні. Прямі методи дозволяють оцінити вірогідність та величину негативного відхилення цільової функції від очікуваних значень. В основному застосовуються для оцінки ринкових ризиків за наявності необхідної статичної інформації. Побічні методи мають більш індикативний характер — з їх допомогою визначаються кількісні характеристики ризиків [18, с. 87].

Рівень ризику зростає переважно за наявності таких умов: проблеми виникають раптом та несподівано; визначені нові завдання банку, що не відповідають минулому досвіду; керівництво не в змозі вживати потрібні та термінові заходи, що може призвести до фінансових збитків; наявний порядок діяльності банку чи недосконалість законодавства заважає вжиттю деяких оптимальних для конкретної ситуації заходів [19, с. 273]. Відповідно, лише від обставин конкретної ситуації залежить, якими способами банки будуть визначати рівень інформаційного ризику банку та за використання яких принципів і методів здійснюватиметься захист банківської інформації.

Як підсумок необхідно зазначити, що на сучасному етапі розвитку банківської діяльності правове регулювання здійснюється в рамках банківського законодавства як в сфері фінансової діяльності держави, так і руху грошових коштів, пов'язаного з цивільним обігом. Через банківську систему здійснюється рух грошових коштів держави та суб'єктів підприємницької діяльності. Вищеназвані учасники банківської діяльності

Університетські наукові записки, 2010, № 2 (34), с. 186-191. www.univer.km.ua

формують публічний інтерес до стабільного функціонування банківської системи з позицій суспільства та держави, що зумовлює публічний аспект її діяльності. Дана специфіка банківської діяльності передбачає постійний підвищений інтерес до інституту банківської таємниці та порядку її розкриття [11; 13; 20], що передбачає необхідність її спеціального правового регулювання, яке має забезпечити на законодавчому рівні інтереси держави, суспільства і громадянина.

В основу банківської системи покладено принципи, притаманні адміністративному та цивільному праву, специфічний метод правового регулювання, а також спеціальні правові норми, встановлені банківським законодавством та нормативно-правовими актами Національного банку України, які свідчать про появу в системі права нашої держави якісно нового явища — банківського права. Відповідно, основні принципи банківської діяльності як основи комплексного регулювання банківських відносин могли б бути закріплені в Банківському кодексі України.

Викладені в даній роботі проблеми безумовно потребують подальшого обговорення, уточнення і не вичерпують всіх особливостей організації та функціонування вітчизняної банківської системи. Але завдання юридичної науки полягає в тому, щоб уже сьогодні на теоретичному рівні розпочати відповідні дослідження для визначення правових основ найбільш досконалої банківської системи.

Список використаних джерел

1. *Черникова, Е. В.* Публичность в правовом регулировании банковской деятельности [Текст] / Е. В. Черникова // Государство и право. — 2009. — № 6. — С. 85–87.
2. Государственная тайна и ее защита в Российской Федерации [Текст] : [учеб. пособ.] / под общ. ред. М. А. Вуса и А. В. Федорова. 3–е изд., испр. и доп. ; предисловие Р. М. Юсупова ; предисловие ко 2-му изданию Н. М. Кропачева, Н. А. Сидоровой. — СПб. : Юридический центр Пресс, 2007. — 752 с.
3. *Лопатин, В. Н.* Правовая охрана и защита служебной тайны [Текст] / В. Н. Лопатин // Государство и право. — 2000. — № 6. — С. 85–91.
4. *Олійник, О. В.* Організаційно-правові засади захисту інформаційних ресурсів України [Текст] : дис. ... канд. юрид. наук : 12.00.07 / Олійник Олег Вікторович ; Інститут законодавства Верховної Ради України. — К., 2006. — 198 с.
5. *Филин, С. А.* Информационная безопасность [Текст] : [учеб. пособ.] / С. А. Филин. — М. : Альфа-Пресс, 2006. — 412 с.
6. *Башлы, П. Н.* Информационная безопасность [Текст] / П. Б. Башлы. — Ростов н/Д : Феникс, 2006. — 253 с.
7. *Василюк, В. Я.* Інформаційна безпека держави [Текст] : [курс лекц.] / В. Я. Василюк, С. О. Климчук. — К. : КНТ ; Скіф, 2008. — 136 с.
8. *Тосунян, Г. А.* Принципы банковского права [Текст] / Г. А. Тосунян, А. Ю. Викулин // Государство и право. — 1998. — № 11. — С. 47–57.
9. *Гейвандов, Я. А.* Основы правового регулирования банковской системы в Российской Федерации [Текст] / Я. А. Гейвандов // Государство и право. — 1997. — № 6. — С. 84–91.
10. Закон України "Про банки і банківську діяльність": Науково-практичний коментар [Текст] / за заг. ред. В. С. Стельмаха. — К. : Видавничий Дім "Ін Юре", 2006. — 520 с.
11. *Паліюк, В. П.* Особливості розкриття банківської таємниці судами (вид. друге, виправлене та доповнене) [Текст] / В. П. Паліюк. — К. : Юстиніан., 2009. — 384 с.
12. *Марущак, А. І.* Правові основи захисту інформації з обмеженим доступом [Текст] : [курс лекц.] / А. І. Марущак. — К. : КНТ, 2007. — 208 с.
13. *Світлична, Г. О.* Правові аспекти розкриття інформації, яка містить банківську таємницю, щодо юридичних та фізичних осіб [Текст] / Г. О. Світлична // Вісник Верховного Суду України. — 2007. — № 11 (87). — С. 25–31.
14. *Степанов, О. А.* Ключевые аспекты правового регулирования использования и развития информационно-электронных технологий [Текст] / О. А. Степанов // Государство и право. — 2004. — № 4. — С. 70–72.
15. *Гуцалюк, М. В.* Організація захисту інформації [Текст] : [навч. посіб.] / М. В. Гуцалюк, Н. А. Гайсенюк. — К. : Альтпрес, 2005. — 244 с.
16. *Зубок, М. І.* Організаційно-правові основи безпеки банківської діяльності в Україні [Текст] : [навч. посіб.] для студ. вищ. нав. закл. / М. І. Зубок, Л. В. Ніколаєва. — 2–е вид., допов. — К. : Істина, 2000. — 88 с.
17. *Стрельбицька, Л. М.* Банківське безпекознавство [Текст] : [навч. посіб.] / Л. М. Стрельбицька, М. П. Стрельбицький, В. К. Гіжевський ; за ред. М. П. Стрельбицького. — К. : Кондор, 2007. — 602 с.
18. *Бухта, М. А.* Методы анализа и оценки рисков банковских операций [Текст] / М. А. Бухта // Закон и право. — 2005. — № 12. — С. 87–89.

www.univer.km.ua Університетські наукові записки, 2010, № 2 (34), с. 186-191.

19. *Стрельбицька, Л. М.* Основи безпеки банківської системи України та банківської діяльності [Текст] : [монограф.] / Л. М. Стрельбицька, М. П. Стрельбицький ; За ред. М. П. Стрельбицького. — К. : Кондор, 2004. — 600 с.
20. *Присяжнюк, Т. І.* Розкриття банківської таємниці: кримінально-процесуальні питання [Текст] / Т. І. Присяжнюк // Вісник Верховного Суду України. — 2008. — № 1 (89). — С. 40–43.

Рекомендовано до друку кафедрою цивільно-правових дисциплін Чернігівського державного інституту права, соціальних технологій та праці (протокол № 6 від 29 січня 2010 року)

Надійшла до редакції 01.03.2010