УДК 336.719.2(477)

Інна Колодій,
викладач кафедри цивільно-правових дисциплін
Чернігівського державного технологічного університету

ДО ПИТАННЯ ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ СТРУКТУР*

У статті розглядаються основні питання організації функціонування системи інформаційної безпеки банківських структур. Визначені загальноправові та специфічні для банківської діяльності принципи захисту банківської інформації з урахуванням методологічних підходів до їх визначення та систематизації.
***Ключові слова**: інформаційна безпека банку, система захисту банківської інформації, засоби захисту банківської інформації.*

Сучасний розвиток суспільства характеризується все більшою його залежністю від інформаційних процесів. Зі вступом України в світовий інформаційний простір, за сучасних темпів розвитку інформаційних технологій проблема формування цілісної та науково обґрунтованої системи забезпечення інформаційної безпеки стає все більш актуальною як на загальнодержавному, так і на галузевому рівні.

За останні роки в Україні реалізовано комплекс заходів, спрямованих на удосконалення інформаційної безпеки банківських структур. Сформовані правові та організаційні механізми захисту банківської інформації і протидії загрозам інформаційної безпеки банківських структур. Разом з тим, аналіз стану інформаційної безпеки банківських структур свідчить про те, що, незважаючи на заходи, які застосовуються, її рівень не повністю відповідає потребам особи, суспільства та держави.

Метою цієї статті є аналіз загальноправових та специфічних для банківської діяльності принципів захисту інформації з урахуванням методологічних підходів до їх визначення та систематизації. Реалізація відповідної мети передбачає виконання таких завдань: дослідження комплексу заходів, спрямованих на збереження банківської таємниці; виявлення взаємозв'язку між принципами захисту інформації характерними для підприємницької діяльності в цілому та специфічними для банківської діяльності.

При дослідженні та аналізі основних аспектів організації функціонування системи інформаційної безпеки банківських структур в Україні були використані праці І. А. Безклубого, М. І. Зубок, В. П. Паліюка, О. Е. Радутного, Г. О. Світличної, М. П. Стрельбицького, Л. М. Стрельбицької та ін.

Наявність досить великої кількості законодавчих актів, які так чи інакше регулюють інформаційні відносини суб'єктів підприємництва, ще не означає, що в Україні діє досконала система інформаційної безпеки, оскільки загальнообов'язкові положення галузевих законодавчих актів визначають права державних органів влади, управління та нагляду за доступом до банківської інформації [1].

Л. В. Щукін стверджує, що основою забезпечення інформаційної безпеки є вирішення трьох взаємозалежних проблеми: проблеми захисту інформації, що перебуває в системі, від впливу внутрішніх і зовнішніх загроз; проблеми захисту інформації від інформаційних загроз; проблеми захисту зовнішнього середовища від загроз із боку інформації, що перебуває в системі [2].

Безпека інформації в сучасних умовах комп'ютеризації інформаційних процесів має принципове значення для попе-

* Рекомендовано до друку кафедрою цивільно-правових дисциплін Чернігівського державного технологічного університету.

редження незаконного і часто злочинного використання цінних відомостей. Завдання забезпечення безпеки банківської інформації реалізується комплексною системою захисту інформації, яка здатна вирішити безліч проблем, що виникають у процесі роботи з такою інформацією.

Визначальним у проблематиці теорії організації інформаційної безпеки є з'ясування її напрямів на засадах комплексного підходу щодо методів захисту. Умовно можна визначити такі напрями організації захисту: правові, управлінські, інженерно-технологічні. У складі останніх як автономні визначаються програмно-математичні (комп'ютерні програмні продукти захисту) [3].

Важливим елементом в комплексній системі захисту банківської інформації є управлінсько-аналітична робота, спрямована на аналіз і оцінку ефективності системи захисту та розробку напрямів її удосконалення відповідно до виникаючих ситуативних проблем.

Необхідність управління в суспільстві є закономірним наслідком об'єктивної потреби організувати та узгодити спільну діяльність людей, їх відносини між собою [4]. Звідси стає зрозумілим значення організаційного фактора для проведення державної політики в різних сферах, для правильного формування структури державного-управлінського механізму, вибору засобів, які будуть застосовуватись у процесі управляючого впливу, а також характеру зв'язків між управляючими та тими, ким управляють [5].

У теорії управління існує декілька способів визначення й зміни компетенції органів, тобто нормативного закріплення предметів ведення, прав та обов'язків. Зокрема централізація — здійснення функцій тільки центральними органами; децентралізація — передача частини функцій нижчестоящим та місцевим органам; деконцентрація — розосередження функцій управління за «горизонталлю» і за «вертикаллю» (включаючи функціональні аспекти); делегування — взаємоузгоджене переадресування повноважень органам різних рівнів; субсидіарність — взаємодоповнена діяльність різних ланок влади та управління [6].

В основу організації банківського регулювання та нагляду покладена комбінована модель, що базується на поєднанні певних елементів трьох відомих у світовій практиці підходів: неформальний базується, головним чином, на консультаціях, переговорах та попередженнях; формалізований вимагає активної перевірки шляхом експериментування на місцях з боку органу банківського контролю; легалістичний підхід базується на обговоренні сукупності показників, яких повинен дотримуватися банк, і на делегуванні повноважень з перевірки та контролю банківської документації на місцях незалежними аудиторами [7]. Вибір моделі, яка включає елементи всіх трьох підходів, на практиці означає встановлення сфери діяльності та функції органу банківського регулювання і нагляду. В Україні це Національний банк України.

У ст. 22 Закону України «Про Національний банк України» [8] зазначено, що структура Національного банку будується за принципом централізації з вертикальним підпорядкуванням. Національний банк наділений правом самостійно вирішувати питання організації, створення, ліквідації та реорганізації структурних підрозділів та установ Національного банку України, його підприємств, затверджувати їх статути та положення. Зрозуміло, що філія центрального банку не може мати статусу юридичної особи і не може видавати нормативні акти, а уповноважена діяти від імені Національного банку України в межах отриманої від нього компетенції на підставі затвердженого положення [9].

Вагоме значення Національного банку України в управлінні банківською системою проявляється в тому, що він, насамперед, бере активну участь у відносинах управління грошовими коштами фінансово-економічної діяльності держави та здійснює фінансовий контроль (валютний, банківський тощо).

Організація інформаційного забезпечення Національного банку України визначається складом керованих об'єктів предметної області, задач, даних і сукупністю інформаційних потреб користувачів НБУ. Згідно із визначенням інформаційне забезпечення включає повний набір показників, документів, класифікаторів, файлів, баз даних, методів їх використання в роботі Національного банку України, а також способів подання, нагромаджування, зберігання, перетворення, передавання інформації для всіх категорій користувачів у необхідній формі та за вимогами часу.

До організації інформаційного забезпечення органів Національного банку України висувається низка вимог. Найважливішими з них є такі: забезпечення для широкого кола користувачів можливостей роботи в реальному режимі; формування для управління оперативних баз даних, які реально знаходяться в базах даних низових структур інформаційної системи Національного банку України (по суті, це є створення і використання сховищ даних); автоматичне формування зведень на кожному рівні ієрархії структури Національного банку України на основі звітних файлів; гарантування безпеки електронних документів і збереження банківської інформації; забезпечення цілісності інформації у разі відмови апаратури [10].

На думку російського вченого О. А. Степанова, в рамках правового регулювання використання та розвитку інформаційно-електронних технологій можуть бути виділені два головних напрями, пов'язані: із забезпеченням інформаційно-електронної безпеки, тобто зі створенням і реалізацією норм, що визначають порядок доступу та використання електронних банків даних конфіденційної інформації, а також даних, що стосуються розвитку біоелектронних та психоінформаційних технологій; з процедурою подання позовів при порушенні балансу суспільних та особистих інтересів, що передбачає розробку норм для вирішення конфліктних ситуацій, що виникають в зв'язку з застосуванням і розвитком комп'ютерних технологій в сфері зберігання конфіденційної інформації в електронному вигляді, а також у сфері біоінженерії та психокомп'ютерної регуляції [11].

На банк покладається обов'язок реалізувати комплекс заходів для забезпечення збереження банківської таємниці. Для цього банком можуть бути розроблені відповідні внутрішні нормативно-правові акти, які б визначали конкретні умови реалізації відповідних заходів щодо охорони інформації, яка становить банківську таємницю, в межах відповідного банку [12].

Одним із важливих нормативних документів банку з безпеки є Положення про комерційну таємницю і конфіденційну інформацію, яке оголошується наказом по банку. Положення передбачає перелік відомостей, що становлять комерційну таємницю і конфіденційну інформацію банку. В ньому зазначають, яким посадовим особам така інформація може доводитись в повному обсязі, порядок її захисту в установах банку, хто відповідає за організацію заходів захисту, відповідальність за розголошення відомостей, що становлять комерційну таємницю. В наказі може визначатися склад комісії, яка буде розглядати і визначати цінність банківської інформації, подавати пропозиції керівникові банку про прийняття рішення щодо надання відповідній інформації статусу комерційної таємниці чи конфіденційної інформації.

Наказом також можуть передбачатися заходи щодо роботи персоналу стосовно збереження ним у таємниці службової інформації.

Досліджуючи питання збереження в таємниці відомостей, що становлять комерційну таємницю банку, О. О. Качан зазначає, що при визначенні складу комерційної таємниці необхідно виходити з економічної вигоди і безпеки банку. Занадто таємна діяльність банку може призвести до втрати прибутку, бо умови ринку вимагають широкої реклами. Зневажливе ставлення до комерційної таємниці також може призвести до негативних результатів [13].

В. Б. Харченко акцентує увагу на тому, що віднесення інформації до переліку відомостей, що не становлять комерційної таємниці, не накладає на її володільця обов'язку відкрити до неї вільний доступ усіх бажаючих. Більше того, володілець такої інформації правомочний застосувати організаційні та інші заходи щодо обмеження доступу до такої інформації фізичних та юридичних осіб, які не мають визначеного законом права ознайомлюватися з нею. Разом з тим, у випадку розголошення або іншого використання такої інформації володілець останньої неправомочний вимагати заборони на її поширення та відшкодування спричиненої шкоди [14].

На думку В. С. Цимбалюка, при формуванні системи інформаційної безпеки виникає необхідність застосування методів інтеграції та агрегації складових системи як її підсистем, що можливо при адаптації до предметної сфери теорії алгоритмізації, моделювання, теорії систем тощо. Підтримку інформаційної системи він визначає як комплекс організаційних, правових та інженерно-тех-

нологічних заходів щодо збереження, охорони та захисту життєво важливих інтересів суб'єктів інформаційної діяльності [15].

Відповідно, виявлення чинного або ймовірного каналу несанкціонованого доступу до інформації, а також запобігання його появі можливе лише за наявності постійного контролю й аналізу об'єкта захисту, рівня безпеки інформаційних ресурсів у джерелі і каналі поширення інформації. Уразливим є будь-який елемент інформаційних ресурсів та інформаційних систем [16].

Таким чином, система технічного захисту інформації є утворенням, призначеним для досягнення мети захисту інформації, а відтак — однією з центральних категорій у сфері технічного захисту інформації. Але на сьогодні зміст самого поняття системи технічного захисту інформації має досить широку інтерпретацію, що свідчить про його недостатню дослідженість. Так, закріплене на нормативному рівні визначення терміна «система захисту інформації» охоплює організовану сукупність методів і засобів технічного захисту інформації [17].

Чинне законодавство не містить ані визначення терміна «методи технічного захисту інформації», ані переліку таких методів, що суттєво ускладнює ситуацію.

Що стосується засобів технічного захисту інформації, то до їх складу віднесено засоби контролю та спеціальні інженерно-технічні споруди, засоби і системи [18]. Знову ж таки, місце і роль засобів технічного захисту інформації, до яких віднесено захищені програми і технічні засоби забезпечення інформаційної діяльності, програмні і технічні засоби захисту інформації, залишаються невизначеними.

Організаційні засоби захисту інформації (на практиці їх також називають адміністративними) регламентують процеси функціонування автоматизованої банківської системи через управління персоналом, тобто запровадження відповідних інструктивних матеріалів про конфіденційність інформації, захист від встановлення прослуховуючої апаратури в службових приміщеннях, обмеження доступу, навіть у приміщеннях, де знаходяться АРМ НБУ, АРМ-2, АРМ-1, АРМ адміністратора БД тощо.

Апаратні засоби захисту здійснюються за допомогою спеціальних пристроїв як функціонуючих автономно, так і вмонтованих у конфігурацію ЕОМ. Вони забезпечують передусім надійну роботу апаратури, захист цілісності програмного забезпечення, забороняють несанкціонований доступ до баз даних. Велике значення мають апаратні засоби захисту інформації в комунікаціях передавання інформації в локальних і глобальних банківських мережах, особливо для підтримки закритості системи електронних платежів [19].

У даній статті ми спробували узагальнити існуючі підходи до класифікації засобів захисту інформації та на їх підставі розробити узагальнену класифікацію, яка б дозволила у процесі побудови системи захисту банківської інформації у кожному окремому випадку скласти повний перелік характерних ймовірних способів вчинення атак на банківську інформацію, що стало б вагомим на шляху формування концепції протидії злочинності.

Усе вищезазначене свідчить про необхідність прийняття відповідного спеціального законодавства щодо банківської таємниці та комерційної таємниці банку. Уявляється необхідним визначити єдині підходи до охорони інформації, віднесеної до комерційної таємниці банку, з відображенням їх у законодавстві України про працю. Крім того, проведений аналіз змісту права на банківську таємницю і комерційну таємницю банку свідчить про неоднозначність їх тлумачення та необхідність подальших досліджень у сфері банківського сектору.

ПРИМІТКИ

1. Зубок М. І. Організаційно-правові основи безпеки банківської діяльності в Україні : навч. посіб. для студ. вищ. навч. закл. — 2-ге вид., допов. / М. І. Зубок, Л. В. Ніколаєва. — К. : Істина, 2000. — С. 12.

2. Щукін Л. В. Щодо обґрунтування поняття «інформаційна безпека» / Л. В. Щукін // Інформаційна безпека людини, суспільства, держави. — 2009. — № 1(1). — С. 31—32.

3. Основи інформаційного права України : навч. посіб. / В. С. Цимбалюк, В. Д. Гавлов-

ський, В. В. Гриценко [та ін.] ; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. — К. : Знання, 2004. — С. 217.

4. Дюрягин И. Я. Право и управление / И. Я. Дюрягин. — М. : Юрид. лит., 1981. — С. 37.

5. Административное право : учебник / под ред. Ю. М. Козлова, Л. Л. Попова. — М. : Юристъ, 2000. — С. 483—484.

6. Тихомиров Ю. А. Курс административного права и процесса / Ю. А. Тихомиров. — М., 1998. — С. 216.

7. Костіна Н. І. Банки: сучасні інформаційні технології : навч. посіб. / Н. І. Костіна, В. М. Антонов, Н. І. Ганах. — Ірпінь : Нац. академія ДПС України, 2004. — С. 94.

8. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV // Відомості Верховної Ради України. — 1999. — № 29. — Ст. 238.

9. Орлюк О. П. Банківська система України. Правові засади організації / О. П. Орлюк. — К. : Юрінком Інтер, 2003. — С. 119.

10. Сендзюк М. А. Інформаційні системи в державному управлінні : навч. посіб. / М. А. Сендзюк. — К. : КНЕУ, 2004. — С. 169—170.

11. Степанов О. А. Ключевые аспекты правового регулирования использования и развития информационно-электронных технологий / О. А. Степанов // Государство и право. — 2004. — № 4. — С. 71.

12. Закон України «Про банки і банківську діяльність» : наук.-практ. ком. / за заг. ред. В. С. Стельмаха. — К. : Ін Юре, 2006. — С. 296.

13. Качан О. О. Банківське право : навч. посіб. / О. О. Качан. — К. : Школа, 2004. — С. 228—229.

14. Харченко В. Б. Комерційна таємниця як об'єкт права інтелектуальної власності та категорія кримінального права / В. Б. Харченко // Вісник господарського судочинства. — 2009. — № 1. — С. 85.

15. Цимбалюк В. С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) / В. С. Цимбалюк // Підприємництво, господарство і право. — 2004. — № 3. — С. 90—91.

16. Гуцалюк М. В. Організація захисту інформації : навч. посіб. / М. В. Гуцалюк, Н. А. Гайсенюк. — К. : Альтпрес, 2005. — С. 62.

17. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. — Введено вперше; Чинний від 01.01.1997. — К.: Держстандарт України, 1997. — С. 3.

18. Там само. — С. 5.

19. Сендзюк М. А. Зазнач. праця. — С. 173.

Колодий Инна. К вопросу организации функционирования системы информационной безопасности банковских структур.
В статье рассматриваются основные вопросы организации функционирования системы информационной безопасности банковских структур. Определены общеправовые и специфические для банковской деятельности принципы защиты банковской информации с учетом методологических подходов к их определению и систематизации.
Ключевые слова: *информационная безопасность банка, система защиты банковской информации, средства защиты банковской информации.*

Kolodiy Inna. To the question of organization of functioning of the system of informative safety of bank structures.
The basic questions of organization of functioning of the system of informative safety of bank structures are examined in the 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.
Key words: *bank information security, system of defence of bank information, facilities of defence of bank information.*