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

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ СТРУКТУР

Система інформаційної безпеки банку має складатися з таких сегментів: нормативно-правового; організаційно-технічного; морально-етичного. Саме таке поєднання має на меті довгострокове забезпечення інформаційної безпеки банківських структур.

Зростання рівня та кількості джерел, що загрожують інформаційним системам банків, обумовлює необхідність удосконалення вже наявної нормативної бази та розробки проектів нових нормативно-правових актів. Для забезпечення ефективного правового захисту банківської інформації необхідно чітко розмежувати інформаційні об'єкти для того, щоб на законодавчому рівні визначити правовий режим кожного виду таких об'єктів.

Режим банківської таємниці та комерційної таємниці банку передбачає визначення: порядку віднесення інформації до банківської таємниці і комерційної таємниці банку та строків її дії; системи доступу співробітників, приватних осіб до інформації,яка містить банківську таємницю та комерційну таємницю банку; порядку роботи з документами під грифом „банківської таємницГта „комерційноїтаємниці банку"; гарантій збереження документів, справ та видань з грифом „банківська таємниця"та „комерційна таємниця банку"; обов'язків осіб, які мають доступ до інформації, яка містить банківську таємницю та комерційну таємницю банку; принципів організації та проведення контролю за збереженням режиму при роботі з інформацією, яка містить банківську таємницю та комерційну таємницю банку; відповідальність за розголошення інформації, втрату документі в, які містять банківську таємницю та комерційну таємницю банку.

Діюче законодавство не визначає моменту виникнення правового режиму банківської таємниці по відношенню до конкретних відомостей. Що, *на* наш погляде суттєвим недоліком механізму захисту банківської таємниці, оскільки від визначення даного моменту в прямій залежності знаходиться питання щодо відповідальності банку за збереження отриманих даних.

Не менш важливе значення має питання способу виникнення правового режиму банківської таємниці по відношенню до конкретних відомостей, який також залишено поза увагою законодавця. Ми пропонуємо визначати момент виникнення правового режиму банківської таємниці по відношенню до конкретних відомостей моментом фактичного отримання таких даних співробітником чи іншим уповноваженим представником кредитної організації та Національного банку України. При цьому форма, час, місце та інші характеристики способу виникнення такого правового режиму не повинні мати жодного значення.

Інформаційні бази в державному управлінні банківською діяльністю мають бути організовані за такими принципами: об'єкти інформаційних баз можуть зберігатися централізовано або знаходитися на різних рівнях інформаційної системи банку (центральний, регіональний), тобто бути рознесеними регіонально (територіально); всі бази даних повинні надавати можливість одержання інформації в будь-який момент часу, за станом на будь-яку дату з урахуванням факту реального розміщення даних; має бути підтриманий наскрізний пошук інформації; доступ до інформації має здійснюватися за допомогою системи, яка дає змогу будувати запити

на природній мові і на підставі існуючих у системі класифікаторів; доступ до інформації має здійснюватися винятково на основі дозволу власника інформації. Структура внутрішньої інформаційної бази має визначався способами організації файлів, баз даних, взаємозв'язками між ними тощо.

Основним напрямом подальшого вдосконалення інформаційного забезпечення Національного банку України є створення корпоративного сховища даних. Головною метою створення сховища даних в НБУ є інтеграція різноманітної інформації, що існує і постійно надходить до НБУ, а також надання фахівцям НБУ потужного інструментарію її аналізу для прийняття обґрунтованих управлінських рішень. Система сховищ даних НБУ стане складовою його дворівневої інформаційної системи та охоплюватиме всю ієрархію локальних обчислювальних мереж, що є на кожному з цих рівнів.

Об'єднання можливостей програмних продуктів з підтримки сховищ даних і аналітичних систем, на думку МА Сендзюка [1,174], дасть змогу вирішувати практично будь-які завдання аналізута підтримки управлінських рішень в інформаційній системі НБУ. Ця система включає: засоби формування складних звітів та їх аналізу; засоби створення запитів довільного змісту у фахових банківських термінах; подання інформації у вигляді діаграм і графіків тощо.

До системи нормативно-правових документів, які регламентують організацію, порядок і правила захисту банківської таємниці та комерційної таємниці банку можна віднести: статут банку, в якому вказуються мета його діяльності, права, в тому числі право мати банківську таємницю і комерційнутаємницю банку та здійснювати її захист; колективний договір, в якому визначаються права та обов'язки сторін, які його уклали, в тому числі по захисту конфіденційної інформації, забезпеченню необхідних умов та засобів її захисту; правила внутрішнього трудового розпорядку, в які також можуть бути включені статті, що зобов'язують усіх працівників захищати інтереси банку, в тому числі банківську таємницю та комерційну таємницю банку; інструкції, які визначають організацію, порядок і правила захисту банківської таємниці та комерційної таємниці банку; положення, що регламентують права та діяльність різноманітних підрозділів, наприклад, служби безпеки відповідного банку; перелік, реєстр і т.п. - документи, які визначають категорії даних, що віднесені до банківської таємниці та комерційної таємниці банку.

Для встановлення режиму банківської таємниці та комерційної таємниці банку може бути створена власна служба безпеки банку, яка буде здійснювати контроль за обліком, розмноженням, збереженням та використанням документів, справ та видань з грифом „банківська таємниця"та „комерційна таємниця банку", а також контроль за нерозголошенням інформації, яка

міститься в документах, справах і виданнях з грифом „банківська таємниця" та „комерційна таємниця банку" й інші повноваження.

Такий спосіб забезпечення збереження інформації, що містить банківську таємницю та комерційну таємницю банку, має свої переваги: знаючи об'єкт, співробітників, можливі загрози,тобто володіючи обставинами, служба безпеки, постійно знаходячись (перебуваючи) на території банку, здатна оперативно знешкодити можливі внутрішні та зовнішні загрози.

Однак основним негативним моментом такого способу є те, що на створення та підтримку належного рівня (підбірта навчання співробітників, закупка техніки) необхідно витратити багато часу та виділити чималі кошти.

Альтернативним способом встановлення режиму банківської таємниці та комерційної таємниці банку і забезпечення безпеки відповідної інформації є запрошення спеціалізованої організації (що має ліцензію на відповідні види діяльності), яка на високому професійному рівні здійснить повний комплекс робіт, пов'язаних з організацією захисту банківської таємниці та комерційноїтаємниці банку та підтриманням стану й захищеності на належному рівні.

Однак цей спосіб має два суттєвих недоліки: по-перше, такі послуги досить дорого коштують, а по-друге, спеціалісти не зможуть бути присутніми в банку постійно, а за разового відвідування є досить вірогідним пропуск факту вторгнення.

Тому, найбільш діючим уявляється комбінований варіант,тобто спільна робота спеціалізованої організації та служби безпеки банку. В такому випадку спільними зусиллями розробляється план, який має містити:

- визначення мети плану по захисту інформації, що містить банківську таємницю та комерційну таємницю банку (такою метою може бути попередження витоку банківської таємниці та комерційноїтаємниці банку);
- аналіз інформації,яка складає банківськутаємницюта комерційну таємницю банку (для цього необхідно визначити, яка інформація буде віднесена до банківської таємниці та комерційноїтаємниці банку; встановити місця їх накопичення та збереження; оцінити можливості перекриття каналів витоку; призначити співробітників, персонально відповідальних за кожну ділянку системи забезпечення безпеки);
- забезпечення реалізації діяльності створеної системи охорони за наступними напрямками: контроль за побудовою та оснащенням банку; робота з персоналом (бесіди при прийомі на роботу, з особами, які звільняються; навчання співробітників правилам роботи з банківськими документами тощо); організація роботи з конфіденційними документами (встановлення порядку та правил ведення діловодства, знищення конфіденційних документів, охорона чужої конфіденційної інформації); робота з конфіденційною інформацією, яка циркулює в технічних засобах та системах, що забезпечують трудову діяльність; робота з конфіденційною

інформацією, накопиченою в комп'ютерних системах; захист банківської таємниці та комерційної таємниці банку в організаційно-правових документах, у процесі укладання договорів із співробітниками тощо.

Після складення такого плану мають бути визначені ті заходи, які виконуються (реалізуються) спеціалізованою організацією, і ті з них, які реалізуються силами та засобами власної служби безпеки.

Уявляється, що заходи по охороні інформації, яка містить банківську таємницю та комерційну таємницю банку, визнаються розумно достатніми, якщо: виключається доступ до інформації, яка містить банківську таємницю чи комерційнутаємницю банку, будь-яких осіб без згоди її власника; забезпечується можливість використання інформації, яка містить банківську таємницю та комерційнутаємницю банку, працівниками і передачі її контрагентам без порушення режиму банківської таємниці та комерційної таємниці банку.

Технічні засоби захисту банківської інформації можуть включати в себе електромеханічні, електронні та інші засоби і системи, які в сукупності з іншими засобами сприяють збереженню інформації. До них можна віднести: автоматизацію охорони приміщень, в яких знаходиться техніка, захист носіїв інформаціїта апаратури від викрадення; застосування спеціальних технічних засобів, які виключають прослуховування та перехват інформації. Для захисту інформації, яка зберігається в комп'ютері, використовуються програмні та апаратні засоби захисту, в тому числі засоби захисту диску від несанкціонованого запису чи копіювання, різноманітні шифратори, застосовується парольна ідентифікація і т.п.

Відповідно, недостатність правових заходів охорони і захисту прав на банківську таємницю та комерційнутаємницю банку всередині банку може компенсуватись за рахунок використання організаційно-технічних заходів.

Ще одним сегментом системи інформаційної безпеки банкує морал ьно-етичний.Томуоднимзнайважливішихдлябанкузавданьусфері організації надійного захисту охоронюваної інформації є робота з кадрами, що мають допуск і доступ до банківської таємниці та комерційної таємниці банку, їх виховання і навчання.

Зазначене положення реалізується в трудових відносинах наступним чином з врахуванням вимог діючого законодавства. В трудовому договорі (контракті), в межах додаткових (факультативних) умов законодавець надав сторонам можливість самим встановлювати необхідні критерії для вирішення питань, в яких сторони зацікавлені. Додаткові (факультативні) умови трудового договору (контракту) є тим юридично обумовленим колом обов'язків, у рамках якого і можуть бути закріплені питання охорони та захисту прав на інформацію,яка містить банківськутаємницю і комерційнутаємницю банку. В обов'язки працівника може бути включено умови про нерозголошення ним банківської таємниці та комерційної таємниці банку, до

якої він буде допущений у силу його посадових обов'язків. За своєю юридичною природою така умова в трудовому договорі (контракті) є логічним завершенням юридичного оформлення правового режиму банківської таємниці та комерційної таємниці банку.

Крім того, в трудовому договорі (контракті) або його невід'ємній частині (зобов'язані про нерозголошення інформації, яка містить банківську таємницю і комерційнутаємницю банку) необхідно передбачити порядок ознайомлення працівника з діючими в банку положеннями та інструкціями щодо збереження банківської таємниці та комерційної таємниці банку. Поряд з цим, працівнику може бути встановлена оплата праці з врахуванням компенсації за взятий ним на себе обов'язок щодо збереження банківської таємниці та комерційної таємниці банку.

Крім працівника, необхідно приділити увагу статусу керівника банку. В силу своїх посадових обов'язків та наданих йому власником повноважень, керівник банку може бути наділений виключними правами по організаційному захисту банківської інформації. В зв'язку з цим у контракт, який заключається (укладається) з керівником при його прийомі на роботу, призначені чи обрані, необхідно включити відповідні положення з зазначеного питання.

Дослідження сучасного стану процесу протидії інформаційним правопорушенням у банківській сфері - це забезпечення інформаційної безпеки банківських структур як складової національної безпеки. Саме тому, на нашу думку, постала нагальна потреба в розробленні єдиного комплексного системоутворюючого законодавчого акту, який би забезпечив: детальне регламентування правового статусу суб'єктів інформаційних відносин у банківській сфері; створення системи збирання й аналізу даних щодо джерел загроз інформаційній безпеці банківських структур; створення системи підготовки кадрів, орієнтованих на використання їх знаньта досвіду у сфері забезпечення інформаційної безпеки банківських структур; розробку організаційно-правових механізмів забезпечення інформаційної безпеки банківських структур.

Однак ефективність дії механізму інформаційної безпеки банку неможливо забезпечити лише шляхом встановлення на нормативному рівні необхідних юридичних засобів і механізмів, як би грамотно це не було зроблено. Необхідна також визначена активність, цілеспрямована діяльність суб'єктів реальних правовідносин, які, використовуючи правові інструменти, реалізують їх потенціал на практиці.

Література: 1. Сендзюк М. А. Інформаційні системи в державному управлінні: навч. посіб./Сендзюк М. А. - К.: КНЕУ, 2004. - 339с.

УДК 378.6(477.51)(066)

Рекомендовано до друку вченою радою Чернігівського державного інституту права, соціальних технологій та праці 24 грудня 2010р., протокол № 5.

ВІСНИК Чернігівського державного інституту права, соціальних технологій та праці (серія Право. Економіка. Соціальна робота. Гуманітарні науки) [Текст|: щоквартальний науковий збірник.-20 Ю.-№ 4.- Чернігів: Чернігівський державний інститут права, соціальних технологій та праці, 20 J 0. - 351 с.

У збірнику висвітлюються актуальні питання історії та теорії держави і права, конституційного та адміністративного права, цивільного права, права соціального забезпечення, економіки, фінансів, управління персоналом та економіки праці, інформаційних технологій та вищої математики, соціології та психології.

Видання розраховане на науковців, викладачів, аспірантів, студентів і всіх, хто прагне отримати знання з юридичних, економічних, соціологічних та гуманітарних наук.

Свідоцтво: Серія ЧГ №424-73Р від 16.09.2008 р.