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

ЩОДО ПРОБЛЕМИ ВИЗНАЧЕННЯ ВНУТРІШНІХ ТА ЗОВНІШНІХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКІВСЬКИХ СТРУКТУР

Банківська система як складова частина фінансової системи будь-якої держави відіграє важливу роль в її економічному розвитку, що в свою чергу визначає зацікавленість держави в жорсткому регулюванні банківської діяльності. Зміни, які мають місце в банківській діяльності нашої держави, потребують розгляду проблеми регулювання банківської діяльності в їх зв'язку і взаємодії з питаннями інституційної побудови фінансово-кредитної системи в рамках загальної концепції зміцнення фундаменту правової держави та інститутів громадянського суспільства. Безперечно, що стан і перспективи функціонування фінансово-правових інститутів мають життєво важливе значення для національної економіки. В той же час, у банківському бізнесі, за умови економічної, соціальної та фінансової кризи, яка охопила всі сторони життя нашого суспільства, існує високий ступінь різноманітних загроз, у тому числі і загроза витоку банківської інформації.

За останні роки дослідженню поняття загроз інформаційній безпеці банківських структур та напрямам її забезпечення присвячені праці М.1. Зубок, Л.В. Ніколаєвої, Л.М. Стрельбицької, М.П. Стрельбицькогота ін.

При проведенні даного наукового дослідження автор поставила за мету проаналізувати внутрішні та зовнішні загрози інформаційній безпеці банківських структур та виділити групи протиріч, які призводять до витоку відповідної інформації за межі банку.

Для розуміння змісту захисту інформації від загроз та інформаційної безпеки необхідно звернутися до самих визначень цих понять. СІ. Ожегов зазначає, що безпека - це стан, при якому не загрожує небезпека, є захист від небезпеки [1,41].

Як загальнонаукову категорію, „безпеку" можна визначити як такий стан розглянутої системи, коли вона здатна протистояти впливу зовнішніх і внутрішніх загроз, а також функціонування цієї системи не створює загрози для складової цієї ж системи й зовнішнього середовища [2,42].

А.Ю. Моздаков зазначає, що в житті людини поняття небезпеки та безпеки відіграють роль ключових орієнтирів, навколо яких групуються фундаментальні цінності людського існування [3,102].

О Колодій І.М.

Поняття безпеки передбачає визначені заходи, направлені на усунення тієї чи іншої загрози. Теоретична розробка загального поняття безпеки залишається слабкою, в зв'язку з чим різні розробники вкладають свій особливий змісту конкретні види безпеки.

Д.Б. Халяшин та В.І. Ярочкин розкривають безпеку інформації як забезпечення захисту інформації від випадкового або навмисного доступу осіб, що не мають права на її отримання, розкриття, модифікацію або руйнування [4, 6].

Види безпеки розмежовуються залежно від об'єкта, предмета та джерел загроз. О.В. Кохановська розкриває загрози безпеці як сукупність умов і факторів, які створюють загрозу цим життєво важливим інтересам [5,424]. Відповідно диференціюється й інформаційна безпекада в умовах всебічного впровадження інформаційних технологій вирішити проблеми інформаційної безпеки важко з таких причин:

- інформація як матеріальна цінність, порівняно з іншими матеріальними цінностями, відносно просто копіюється шляхом дублювання раніше створених інформаційних продуктів;
- розвиток обчислювальної техніки і техніки зв'язку поряд з підвищенням ефективності її використання призвели до ускладнення можливостей контролю й запобігання несанкціонованого отримання і використання інформації з обмеженим доступом;
- різноманітність апаратних і програмних засобів формування, передачі, перетворення, відображення і зберігання інформації при впровадженні інформаційнихтехнологій з урахуванням орієнтування на засоби закордонного виробництва в умовах відсутності в Україні матеріально-технічної й методологічної бази їх обслуговування й атестації збільшує потенційні можливості формування нових каналів її витоку і порушення цілісності [5,463].

Аналіз та виявлення загроз інформаційній безпеці є другою важливою функцією адміністративного рівня забезпечення інформаційної безпеки. Багато в чому змістсистеми захисту і склад механізмів її реалізації визначається потенційними загрозами, виявленими на певному етапі [6,49].

Досвід роботи українських банків із захисту таємниць від протиправних посягань показує, що залежно від суб'єкта посягання вони можуть бути зовнішніми та внутрішніми. Зовнішні посягання здійснюються конкуруючими банками, кримінальними елементами та іншими зацікавленими в цьому особами, внутрішні - працівниками банку, його акціонерами та клієнтами [7,398].

Аналізуючи характер посягань, слід зазначити, що факти нелегальних дій з отримання відомостей, що становлять таємниці банків, у загальному обсязі витоку інформації становлять менше *1%.* Дається взнаки складність доступу до таких відомостей, створена системою заходів їх захисту, досить жорстка відповідальність за посягання на них і, як правило, наявність можливості легального доступу з боку третіх осіб [8, 35].

Особливістю протиправних посягань на таємниці банків з боку конкурентів і кримінальних елементів є й те, що практично всі їх дії здійснюються через або за сприяння працівників банків. Тобто внутрішні посягання, як правило, бувають не з ініціативи самих працівників банку [8, 36].

Відповідно, не зменшуючи значимість внутрішніх загроз інформаційної безпеки банку, на нашу думку, необхідно все-таки визнати домінуючими зовнішні загрози, які до того жтак чи інакше провокують загрози внутрішні.

Інформаційні ризики становлять загрозу зовнішніх і внутрішніх атак на інформаційну систему, внаслідок чого відбувається крадіжка, псування або підміна функціонуючої в системі інформації, насамперед, конфіденційної. На думку Л.В. Щукіна, більш точним є наступне визначення. Інформаційний ризик - це ймовірність одержання збитків або збитку в результаті застосування компанією інформаційних технологій. Таким чином, інформаційні ризики пов'язані зі створенням, передачею, зберіганням і використанням будь-якої інформації за допомогою електронних носіїв й інших засобів зв'язку [9, 32].

Для того, щоб отримати уявлення стосовно характеристики загроз, які виникають в інформаційній сфері, необхідно проаналізувати суть інформаційної діяльності в банківських структурах. Інформаційна діяльність - вид соціальної діяльності з характерними для неї ознаками системності, цілісності, вартості, співставлення об'єктивного та суб'єктивного факторів, комунікативності, процедурності. Необхідно звернути увагу лише на три з них, найбільш важливі для розуміння загроз, які виникають у банківській сфері.

Об'єктивно-суб'єктивний характер. При всіх об'єктивних даних інформаційної діяльності вона здійснюється суб'єктами, що надає їй об'єктивно-суб'єктивний характер. Суб'єктивний фактор значною мірою обумовлює відхилення від належного результату діяльності, які утворюють базу для загроз безпеці та передбачають випадкову форму її результатів.

Комунікативність. Ця ознака інформаційної діяльності зобов'язує відмовитись від уявлення про дану діяльність як сугубо управлінську. Комунікація - це завжди відносини,засновані на партнерській взаємодії сторін, направленій на спільний пошук істини, коли „людина, вступаючи в контакт з іншою людиною, бачить у ній собі подібну і тому розраховує на активний зворотній зв'язок, на обмін інформацією, а не на одностороннє її спрямування чи зняття її з об'єкта".

Процедурність. інформаційна діяльність має свою процесуальну і результативну сторони. Для проблеми інформаційної безпеки принципове значення має ця формальна, юридична сторона, саме в цій частині діяльності найчастіше виникають та реалізуються загрози.

Відповідно, інформаційна діяльність - це діяльність визначеного органу, що має певну структуру, вертикальні та горизонтальні зв'язки та відносини, які також мають на меті забезпечення очікуваного результату і тому підлягають правовому реп/люванню, утворюють самостійний вид правовідносин.

Аналіз і дослідження потенційних загроз несанкціонованого доступу до інформації в інформаційних системах доцільно поділити на цілеспрямовані (умисні) і випадкові.Умисні загрози можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкціонованими запитами або комп'ютерними вірусами та ін. [10,16].

Саме тому необхідно звернути увагу на той факт, що витік охоронюваної інформації - це наслідок певних подій. Витоку завжди передують факти об'єктивного і суб'єктивного характеру, які прийнято називати причинами. Для того, щоб виявити витік охоронюваної інформації, необхідно мати уявлення про систему причинності явищ і процесів, які мають місце в банку.

Знищення та попередження внутрішніх і зовнішніх загроз інформаційній безпеці банківських структур базується на розробці та реалізації комплексу засобів і механізмів захисту. Це можуть бути організаційні (адміністративні), технічні, програмні, соціальні, правові та інші механізми, які можуть забезпечити локалізацію та попередження таких загроз [11,53].

Адміністративні заходи захисту - це заходи організаційного характеру, що регламентують процеси функціонування системи обробки інформації, використання її ресурсів,діяльність персоналка також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити чи унеможливити реалізацію загроз безпеці. Вони включають: розробку правил обробки інформації в автоматизованих системах обробки інформації банку; заходи, вживані при проектуванні, будівництві й устаткуванні обчислювальних центрівта інших об'єктів АСОІБ (урахування впливу стихії, пожеж, охорона приміщень, організація захисту від установки апаратури, що прослуховує і т.ін.); заходи, вживані при підборі й підготовці персоналу (перевірка нових співробітників; ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки; створення умов, за яких персоналу було б невигідно припускатися зловживань і т.ін.); організацію обліку, збереження, використання та знищення документів і носіїв з конфіденційною інформацією.

Технічними засобами захисту є різні електронні пристрої і спеціальні програми, що виконують (самостійно чи в комплексі з іншими засобами) функції захисту (ідентифікацію й аутентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічний захист інформації тощо) [7, 346].

Вагоме значення для розкриття характеристики правопорушень режиму охоронюваної інформації має також виявлення можливих каналів витоку інформації.

Згідно з п. 4.1.3. ДСТУ 3396.0-96 загрози порушників технічного захисту інформації можуть здійснюватись:

- технічними каналами, що включають канали витоку по ПЕМВН, акустичні, оптичні, радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом шляхом під'єднання до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання засобів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Що стосується програмних засобів захисту,то у західних банках програмне забезпечення розробляється конкретно під кожен банк і пристрій АСОІБ і є комерційною таємницею. В Україні поширені „стандартні" банківські пакети, інформація про які широко відома, що полегшує несанкціонований доступ у банківські комп'ютерні системи.

Цілісну систему захисту створити досить складно, оскільки досі немає єдиної теорії захисту комп'ютерних систем. Існує багато підходів і точок зору на методологію її побудови.У цьому напрямку докладаються серйозні зусилля як у практичному, так і в теоретичному плані, використовуються самі останні досягнення науки, залучаються передові технології. Цією проблемою займаються правові фірми з виробництва комп'ютерів і програмного забезпечення, інститути, а також великі банки та міжнародні корпорації [7,362].

Правові механізми захисту повинні розроблятися та запроваджуватися в конкретній предметній області банківської сфери.Так, у предметній області пошуку, отримання та використання банківської інформації, перш за все, повинні бути захищені: право на отримання і використання інформації.

У главі 2 Правил зберігання, захисту, використання та розкриття банківської таємниці, затверджених постановою Правління Національного банку України від 14 липня 2006 року № 276, від банку вимагається вчинення наступних організаційно-правових заходів.

Банки зобов'язані у внутрішніх положеннях, з метою забезпечення зберігання та захисту банківської таємниці, встановити спеціальний порядок ведення діловодства з документами, що містять банківську таємницю, а саме: визначити порядок реєстрації вихідних документів, роботи з документами, що охоплюють банківськутаємницю, відправлення та зберігання документів, що містять банківськутаємницю, а також особливості роботи з електронними документами, які містять банківську таємницю.

Під час роботи з документами, що містять банківськутаємницю, на електронних носіях банки мають забезпечити дотримання таких вимог:

1) позначка грифа „Банківська таємниця" до інформації та даних в електронному вигляді, що мають визначений формат і обробляються автоматизованими системами, а також до лістингів програмних модулів не додається. Для текстових повідомлень, які створюються, обробляються, передаються та зберігаються в електронному вигляді, наявність позначки грифа „Банківська таємниця" є обов'язковою;

2) автоматизовані системи, які обробляють інформацію, що містить банківську таємницю, мають створюватися банками таким чином, щоб обмежити доступ користувачів лише в межах, що необхідні для виконання їх службових обов'язків.

Автоматизованим системам оброблення інформації слід мати вбудовану систему захисту інформації, яку неможливо відключити або здійснити оброблення інформації, минаючи її.

Автоматизовані системи оброблення інформації, що містить банківську таємницю, які працюють у режимі реального часу (on-line), повинні мати таку архітектуру, за якої користувачі не мають прямого доступу до конфіденційних даних у базі даних і можуть отримувати доступ лише через сервер застосувань, що здійснює сувору автентифікацію запитів.

3) приймання та реєстрація інформації визначеного формату, що містить банківську таємницю, в електронному вигляді технологічними АРМ автоматизованих систем здійснюється згідно з технологічними схемами проходження інформації безпосередньо на відповідних робочих місцях з використанням вбудованої в ці технологічні АРМ системи захисту інформації;

4) передавання інформації, яка містить банківську таємницю, електронною поштою або в режимі on-line здійснюється лише в захищеному (зашифрованому) вигляді з контролем цілісності та з обов'язковим наданням підтвердження про її надходження з електронним підписом отримувача з використанням засобів захисту;

5) роздрукування документів з грифом „Банківська таємниця"утехнологічнихАРМ здійснюється згідно з технологічними схемами роботи відповідних АРМ банку. На роздрукованих документах проставляється гриф „Банківська таємниця" і вони обліковуються згідно з вимогами щодо обліку паперових документів.

Лістинги програм захисту інформації, що містять банківську таємницю, повинні зберігатися банком на захищених серверах або електронних носіях.

Формування архівів в електронному вигляді здійснюється згідно з технологічними схемами оброблення документів, а також вимогами нормативно-правових актів Національного банку України. Архіви зберігаються на серверах або зовнішніх носіях у захищеному вигляді із забезпеченням контролю цілісності інформації під час роботи з архівними документами.

На основі аналізу факторів, які впливають на вчинення порушень режиму банківської інформації, що охороняється, можна виділити наступні групи протиріч, які призводять до витоку відповідної інформації за межі банку:

1. Складності, які спостерігаються при вирішенні завдань по захисту банківської інформації, яка не підлягає розголошенню, і вимагають оперативного реагування з боку адміністрації та служб безпеки на зміни в законодавстві і практиці роботи банків. Відповідні завдання можуть змінюватися в результаті прийняття нових законодавчих актів, що змінюють

попередньо закріплені умови діяльності. Відповідним чином змінюється і оперативна обстановка в банку, яку необхідно враховувати при організації та реалізації захисних заходів. Однак керівництво банку не завжди відстежує зміни, що призводить до відсутності належного контролю на окремих дільницях, де циркулює охоронювана інформація, та її витоку.

2. Протиріччя між вимогами, які висуваються до підбору кадрів, і станом сучасної практики їх виконання. Мова йде про призначення на посади осіб, не підготовлених до виконання функціональних обов'язків, тих, які не використовують сучасні форми і методи роботи по попередженню витоку охоронюваної інформації.

3. Протиріччя, які відносяться до системи реалізації відповідальності за неналежне виконання службових обов'язків працівниками банку, пов'язаних із захистом охоронюваної інформації. Вони проявляються у недотриманні принципу невідворотності відповідальності за вчинення порушень режиму охоронюваної інформації. Практика показує, що на фоні збільшення загального числа злочинів у державі керівники банків звиклись з багатьма правопорушеннями і не звертають на них увагу, крім тих, які явно призводять до значних економічних втрат. Однак причини втрат від розголошення (витоку) банківської інформації не завжди виявляються, а винні особи не несуть відповідальності в силу складності процесуального доказування матеріальної шкоди та розміру завданих збитків у суді.

Уявляється, що досвід групи протиріч, які сприяють витоку охоронюваної банківської інформації, необхідно враховувати в законотворчій роботі, так як вищезазначені протиріччя, на нашу думку, є результатом конкретних причин, які, в свою чергу, обумовлені іншими обставинами організаційно-управлінського, економічного, правового характеру тощо. Мова йде про конкретні недоліки організації та управління в забезпеченні режиму охоронюваної інформації, викликані відсутністю належного порядку і дисципліни в справі збереження банківської інформації обмеженого доступу; про недосконалість правового регулювання, коли при виконанні одних нормативно-правових актів порушуються інші; про недоліки в практиці застосування санкцій за порушення вимог режиму збереження інформації, що виражені в недостатньо якісному проведені контрольно-наглядової та аналітичної роботи по виявленнюта процесуальному оформленню порушеньта у неадекватному реагуванні керівництва банку на порушення норм (правил) захисту банківської інформації.

Література: 1. Ожегов С. И. Толковый словарь русского языка: 80 000 слов и фразеологических выраженный / С. И. Ожегов, Н. Ю, Шведова (Российская академия наук. Институт русского языка им. В.В. Виноградова). - М.: Азбуковник, 1999. ~ 944 с. 2. Боровський О. О. Безпека національна/Боровський О. О.//Соціологічна енцикл. /укл.В. Г.Городяненко.-К.:Академвидав,2008.-456 с.3.Моздаков А. Ю. Социальная безопасность и безопасность личности /А. Ю. Моздаков // Государство и пра-

во. - 2008. - №6. - С. 102-105.4. Халяшин Д. Б. Основы промышленной и коммерческой информации, термины и определения / Д. Б. Халяшин, В. И. Ярочкин. ~ М., 1992. - 39 с. 5. Кохановська О. В. Теоретичні проблеми інформаційних відносин у цивільному праві: монографія/ Кохановська О. В. - К.: Видавничо-поліграфічний центр „Київський університет" 2006. - 463 с 6. Башлы П. Н. Информационная безопасность/ П. Н. Башлы. - Ростов н/Д: Феникс, 2006. - 253 с. 7. Стрельбицька Л. М. Банківське безпекознавство: навчальний посібник/Стрельбицька Л. М.,Стрельбицький М. П., Пжевський В. К.; за ред. М. П. Стрельбицького. - К.: Кондор, 2007. - 602 с. 8. Зубок М. І. Організаційно-правові основи безпеки банківської діяльності в Україні: навч. посіб.для студ. вищ. навч.закл./Зубок М. І., Ніколаєва Л. В. - 2-е вид.,допов. - К.: Істина, 2000. - 88 с 9. Щукін Л. В. Щодо обґрунтування поняття „інформаційна безпека7Л. В. Щукін// Інформаційна безпека людини, суспільства, держави.- 2009. - № 1(1).-С 31-33. Ю.Вертузаєв М. С Захист інформації в комп'ютерних системах від несанкціонованого доступу: навч. посібник/ Вертузаєв М. С, Юрченко О. М.; за ред. С Г.Лаптєва.-К.:Вид-воЄвроп.ун-ту,2001.-321 с. 11.Копылов В. А.Информационное право: учебное пособие/ Копылов В.А. - М.: Юристь, 1997. - 472 с.

УДК378.6(477.51)(066)

Рекомендовано до друку Вченою радою Чернігівського державного інституту права, соціальних технологій та праці 29.жовтня 2010р., протокол №3.*

ВІСНИК Чернігівського державного інституту права, соціальних технологій та праці (серія Право. Економіка. Соціальна робота. Гуманітарні науки) (Текст): щоквартальний науковий збірник. -2010, - Ж З. - Чернігів: Чернігівський державний інститут права, соціальних технологій та праці, 2010. - 336 **с**

У журналі висвітлюються актуальні питання трудового права, права соціального забезпечення, історії та теорії держави і права, конституційного та адміністративного права, цивільного права та процесу, економічної теорії, соціальної роботи, гуманітарних дисциплін та філології.

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

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