оптимального рівня інфляції для України // Вісник НБУ. − 2007. − № 6. – С. 10-22.

8. Щербак О. Валютна політика НБУ // Вісник НБУ. − 2007. − № 6. – С. 6-9.

9. Рибак С., Лазерник Л. Фінансові аспекти економічного зростання в Україні // Економіка України.− 2007.− № 3.– С. 22-32.

10. Вахненко Т. Концептуальні засади управління зовнішнім національним боргом України // Економіка України. − 2007. − № 1 – С. 14-24.

Статья поступила в редакцию 17.12.2007

Л.М. ПЕРЕХРЕСТ,
Національний університет державної податкової служби України

ЗАХИСТ ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ БАНКІВ ВІД ВНУТРІШНІХ ЗАГРОЗ

В умовах реформування української економіки значення та роль банківського сектору в забезпеченні економічної стабілізації та безпеки країни невпинно зростає.

Необхідною умовою побудови та функціонування банківської системи є всебічне забезпечення безпеки у всіх сферах банківської діяльності, важливою складовою якої є безпека економічної інформації [1].

Сьогодні банківська система переживає значні зміни, обумовлені глобалізацією фінансових ринків, розвитком інформаційних технологій, розширенням асортименту банківських послуг, впровадженням інноваційних технологій в управлінні банками. Це, у свою чергу, ще більше загострило ситуацію із забезпеченням надійного захисту інформації.

Питання, пов'язані із захистом економічної інформації банків, останнім часом набувають особливої актуальності, оскільки банки є найбільш вразливими до такого виду загроз, як наявність каналів витоку інформації. Усе це викликає необхідність перегляду підходів до забезпечення безпеки інформації банку та передбачає необхідність створення відповідних систем її захисту.

Проблеми безпечного розвитку держави та її банківського сектора зокрема є предметом наукових досліджень як вітчизняних, так і зарубіжних вчених та практиків. Серед них: Ареф'єва О.В.[9], Барановський О.І. [8], Єрмошенко М.М. [6; 7], Клименко В.В. [10], Побережний С.Н. [13], Покотиленко Р.В. [11], Чорнодід І.С. [12] та інші.

Разом з тим, кількість робіт, присвячених захисту економічної інформації є вкрай недостатньою. Дані проблеми не дістали фундаментального та комплексного відображення в економічній літературі.

Висока значимість проблем захисту економічної інформації від загроз, недостатній рівень її теоретичної розробки, перед усім, з точки зору комплексного підходу обумовили вибір теми.

дослідження концептуальних положень щодо захисту економічної інформації банків від внутрішніх загроз та на цій основі розробка напрямів безпечного розвитку комерційних банків.

Інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми та внутрішніми. В даний час індустрія інформаційної безпеки розвивається, в основному, на протидії зовнішнім загрозам, пов'язаних з проривом в області високих технологій, Інтернет та електронної комерції. Водночас, чим більших успіхів досягає людство в боротьбі з зовнішніми загрозами, тим рішучіше на перший план виходять загрози внутрішні, з якими, згідно статистики, пов'язано близько 70% всіх інцидентів безпеки.

Слід зазначити, що серед внутрішніх загроз найбільш небезпечною є загроза наявності каналів витоку інформації. Засоби захисту від несанкціонованого доступу тут є практично безкорисними, оскільки в якості основного джерела загрози виступає

«інсайдер» – користувач інформаційної системи, що має цілком легальний доступ до конфіденційної інформації і який застосовує весь арсенал доступних йому засобів для того, щоб використовувати інформацію у своїх цілях [2].

Отож, останнім часом все більшої актуальності набуває проблема захисту економічної інформації від інсайдерів, оскільки дуже часто доступ до любих інформаційних активів мають чи не всі співробітники банку, в тому числі і ті, кому за родом своєї діяльності вони не потрібні.

Для того, щоб організувати ефективну систему захисту, необхідно розглянути загрози, які несуть інсайдери, і засоби, якими вони оперують.

Всіх носіїв внутрішніх загроз можна умовно розділити на декілька груп: несвідомі порушники та свідомі порушники. Дуже часто інсайдери наражають на ризик корпоративні секрети не навмисно. Так, скажімо, вони можуть випадково викласти секретні документи на веб-сайт, записати дані на ноутбук або кишеньковий комп'ютер, який згодом буде викрадений або втрачений, а також відіслати конфіденційні дані за не правильною адресою.

Для прикладу можна навести випадок, коли фірма Merrill Lunch відправила електронний лист в компанію Standart &Poor's, в якому просила оцінити активи банку Commerzbank. Лист став доступним гласності, що змусило банк виступити із заявою про свою фінансову спроможність [3].

Іншу категорію несвідомих порушників складають співробітники, які вважають, що здатні на більше, аніж приписано їхніми функціональними обов'язками. Так, скажімо, вони часто беруться за переустановку програмного забезпечення, яке, на їх думку, функціонує не зовсім правильно, в результаті чого воно взагалі перестає робити.

Разом з цим, необхідно зазначити, що в решті решт дані особи мають на меті виключно добрі наміри. Значно гірше складається справа з порушниками, які свідомо намагаються нанести шкоду банку. Як правило, це люди з ураженим самолюбством, завищеною самооцінкою, якості були «недооцінені» керівництвом. До такого типу найнебезпечніших внутрішніх порушників відносяться «ображені» та «саботажники». Головною відміною цих зловмисників є намагання нанести шкоду за особистими, як правило, безкорисливим мотивам. Це накладає свій відбиток на ті загрози, які несуть саботажники, і способи, якими вони можуть скористатися. Справа у тому, що для реалізації своєї мети ображені інсайдери готові піти буквально на все, часто навіть не турбуючись про самозбереження.

Так, скажімо, саботажник може скопіювати врай важливу для компанії інформацію на мобільний носій, а потім знищити її на всіх серверах фірми і навіть в резервних копіях на матеріальних носіях. Зрозуміло, що після таких дій в руках зловмисника виявляються важелі тиску на керівництво.

Однак в деяких випадках ображений службовець може видалити всі важливі дані, навіть не залишивши інформацію собі. В цьому випадку порушник хоче просто помститись і перетворюється у диверсанта.

Інша категорія порушників – співробітники, що звільняються із організації в результаті переходу на іншу роботу або конфлікту. Для прикладу можна навести інцидент, в якому керівник місцевого відділення Private Banking, що обслуговував самих багатих клієнтів, перейшов на роботу до банку-конкурента UBS. Разом із собою він забрав конфіденційні дані всіх заможних клієнтів. Зрозуміло, що через деякий час і клієнти перейшли до іншого банку [3].

На рисунку 1 дано авторське бачення класифікації внутрішніх загроз економічній інформації банку, джерелом яких виступає персонал банку.

Зрозуміло, що дана класифікація є умовною, оскільки на практиці реальні порушники можуть одночасно відноситись до декількох категорій одночасно, або їх мотиви можуть лежати між мотивами описаних категорій носіїв загроз.

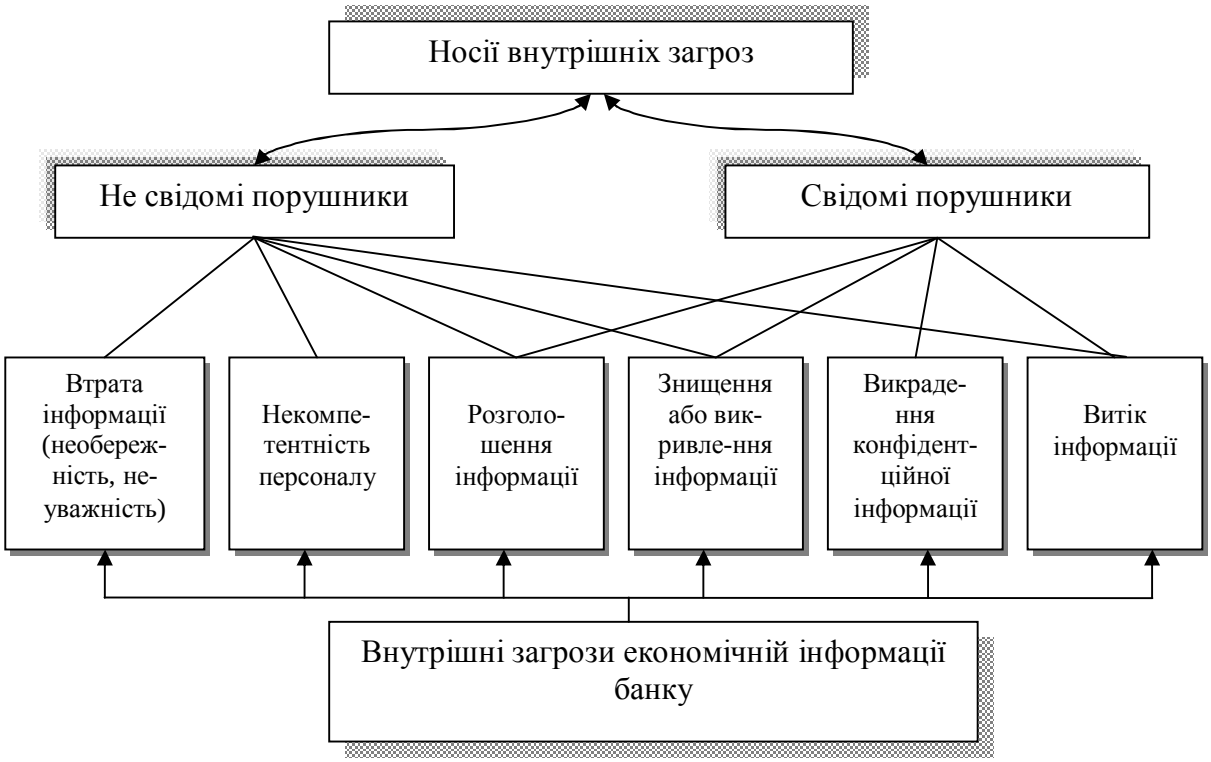

Рис.1. Класифікація внутрішніх загроз економічній інформації банку, джерелом яких виступає персонал банку

Загрози банку зі сторони персоналу можуть також проявлятися в недостатній кваліфікації, а також в нелояльності персоналу банку (рис.2)

Рис. 2. Ризики нелояльності персоналу [4]

На думку більшості банкірів, ризики нелояльності персоналу, під якими розуміють свідомі дії персоналу банку, метою яких є нанесення шкоди (збитку) банку із корисливих або інших мотивів, представляють найбільшу загрозу для банку [4].

Деякі висновки відносно лояльності людини можна зробити на основі регулярного моніторингу опосередкованих факторів: яким чином побудований робочий графік, які документи і в якій кількості копіює, чи чистить свій поштовий ящик або накопичує листи і тому подібне, і тут неоціниме співробітництво з психологами, в тому числі соціальними і фахівцями з управління персоналом.

Однією із основних причин, що стримує розвиток захисту економічної інформації від внутрішніх загроз є небажання банків виносити на широке обговорення випадків витоку інформації або збоїв у роботі інформаційної системи з вини власних співробітників, оскільки вони можуть негативно вплинути на імідж банку з усіма випливаючими фінансовими наслідками.

Стає очевидним, що корпоративна гординя заважає банкам обмінюватись досвідом із попередження або відшкодування втрат. Частіше всього банк вважає, що дешевше в глибокій конспірації списати збитки і спасти репутацію від клейма жертви, аніж починати публічне розслідування. Тому спритні «колеги» безкарно обкрадають банки на сотні тисяч доларів та мільйони гривень.

Згідно даних аналітичних досліджень, в офіційних опитуваннях на питання про те, чи реалізовувались загрози в області інформаційної безпеки із-за дій персоналу, позитивно відповідають не більше 20% установ. В приватних бесідах або в процесі IT-аудиту систем інформаційної безпеки з'ясовується, що постраждалими виявляється близько 80% організацій. По цій же причині поки що немає достовірної статистики реалізації загроз, які виходять із кожної групи порушників.

Практика останніх років показала, що найбільший резонанс викликають випадки витоку конфіденційної інформації саме із фінансово-кредитних установ.

Зростаюче занепокоєння ризиком витоку інформації було викликане серією корпоративних скандалів, у зв'язку із розголосом конфіденційних даних. Більшість таких інцидентів показали, що прогалини у безпеці, як правило, не є результатами зловмисної діяльності. Напроти, найчастіше всього загрозу представляють співробітники, які із некомпетентності наражають компанію на ризик. Таке може трапитись, якщо службовець відправляє електронне повідомлення з додатком, про конфіденційний характер якого йому просто не відомо. У інших випадках співробітник відправляє важливі файли через загальнодоступний поштовий веб-сервер або копіює їх на мобільний телефон – таким чином, дані виявляються у незахищеному середовищі.

Однією із невирішених проблем на сьогодні є безпека процесів, винесених в треті компанії, а іноді і в треті країни. Взяти хоча б інцидент з публікацією в лондонському таблоїді «The Sun», де журналіст просто пообіцяв опублікувати конфіденційні дані про банківські рахунки більш як тисячі англійців. Як показало подальше розслідування, витік відбувся в одному із call-центрів Індії, куди декілька британських банків винесли частину своїх функцій. В результаті інциденту довіру до компаній Lloyds TSB, Barclays, Woolwich та HSBS було підірвано.

На кінець самою серйозною проблемою, як ми зазначали вище, залишається персонал банку, який свідомо готовий продавати інформацію про рахунки клієнтів. Наприклад, у 2005 році було зареєстровано найбільший банківський витік інформації приватних даних США. Жертвою цілої банди продажних клерків стали чотири найбільших банків США (Wachovia, Bank of America, Commerce Bancorp та PNC Bank) і майже 700 тисяч американських громадян [3].

Разом з тим, труднощі такого роду характерні не тільки для західних банків. На думку багатьох експертів, в Росії та Україні безпека call-центрів ще нижча, аніж в країнах Європи та Північної Америки, оскільки згідно нашого законодавства

компанії не зобов'язані повідомляти клієнтів, чиї дані були скомпрометовані. Іншими словами, створені такі умови, щоб якнайскоріше «зам'яти» інцидент і уникнути спілкування із пресою.

На превеликий жаль, в Україні відсутня статистика щодо фактів злочинної інсайдерської діяльності в банківській сфері, яка дозволяє розпізнати внутрішнього порушника. Однак за кордоном ці факти відслідковують та накопичують спеціалізовані служби.

Так можна навести дані дослідження компанії InfoWatchy [5], проведені в період з 20.12.2006 по 25.01.2007р., в процесі якого були опитані представники 312 російських банків з метою визначення ставлення респондентів до загроз внутрішньої інформаційної безпеки, узагальнення інформації про засоби захисту, виявлення специфіки забезпечення внутрішньої інформаційної безпеки у російському банківському секторі.

Підвищена увага до внутрішніх загроз інформаційної безпеки обумовлена тим, що інсайдерські ризики превалюють над зовнішніми загрозами (рис. 3).

Для побудови даної діаграми в категорію внутрішніх загроз було віднесено халатність співробітників, саботаж та фінансове шахрайство, а в категорію зовнішніх загроз – віруси, хакери, спами. Разом з тим, необхідно зазначити, що загрози викрадення інформації, різноманітні збої і викрадення обладнання спеціально не були віднесені ні до однієї із груп, так як вони можуть бути реалізовані як в самому банку, так і за його межами.

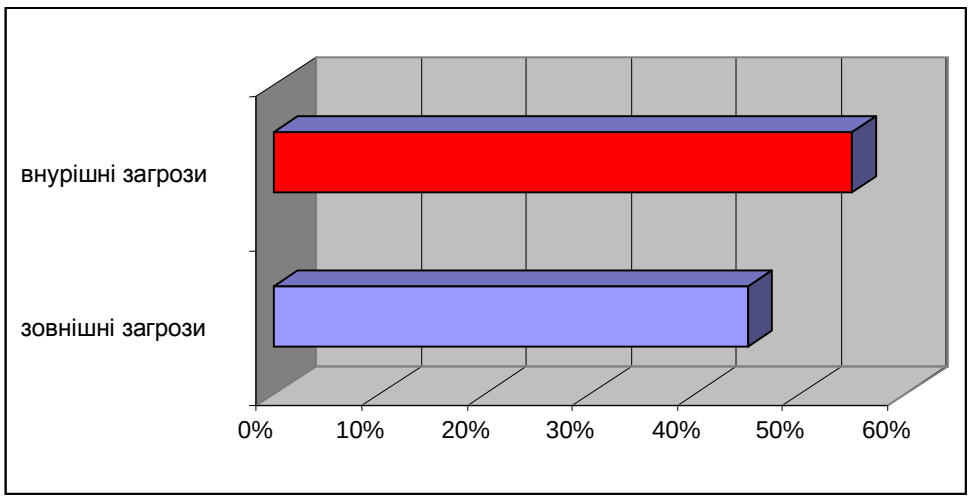

Рис. 3. Співвідношення внутрішніх та зовнішніх загроз безпеки інформації

Виходячи із отриманих результатів, респонденти значно більше занепокоєні внутрішньою інформаційною безпекою (55%), ніж захистом від зовнішніх загроз (45%). Крім того, необхідно враховувати, що такі некласифіковані ризики як, наприклад, викрадення інформації або обладнання, найчастіше відносять до внутрішніх загроз, а в даному випадку взагалі не були враховані для того, щоб не придавати загрозам зі сторони інсайдерів ще більш вагомого значення. Однак, як показали розрахунки, навіть у цьому випадку зовнішні ризики суттєво поступаються внутрішнім загрозам.

Отож, з'ясувавши, що найбільш небезпечні загрози виходять із середини організації, цілком логічно вивчити структуру інсайдерських ризиків.

В рамках дослідження респондентам запропонували вибрати три найбільш небезпечних загроз інформаційній безпеці.

Як показали результати дослідження, (рис.4) у списку самих небезпечних внутрішніх загроз головне місце посідає порушення конфіденційності інформації (78%). На другому і третьому місцях втрата інформації (61%) і збій в роботі інформаційних систем (52%).

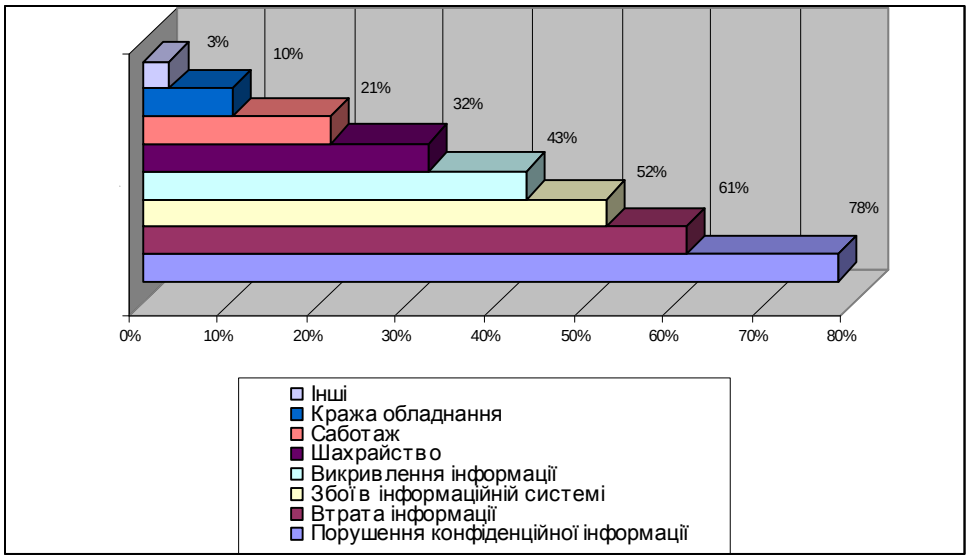

Рис. 4. Найбільш небезпечні загрози внутрішній інформаційній безпеці

Необхідно зазначити, що в принципі, переважна кількість внутрішніх загроз взаємопов'язані. Наприклад, під шахрайством розуміють викривлення інформації у фінансових звітах, а саботаж, в кінцевому рахунку, може реалізовуватися в порушенні конфіденційної інформації, викраденні обладнання, втраті даних. Однак той факт, що ризик витоку цінної інформації хвилює респондентів набагато більше аніж любої іншої інсайдерської загрози, говорить про те, що до цієї внутрішньої загрози необхідно підходити найбільш відповідально.

Поглиблене опитування респондентів показав, що російські банки побоюються витоку в основному за двома причинами. По-перше, кожний витік конфіденційної інформації та персональних даних підриває репутацію банку, так як в очах його партнерів, інвесторів і клієнтів банк набуває імідж організації, яка не в змозі навести порядок в своїх власних стінах. В результаті відбувається відтік інвестицій та міграція клієнтів до конкурентів. По-друге, інциденти такого роду можуть привести до втрати конкурентноздатності банку, якщо, наприклад, інтелектуальна власність або база клієнтів попадуть до конкурентів

Отже, наслідком витоку конфіденційної інформації є втрата клієнтів, погіршення іміджу, зниження конкурентноздатності та прямі фінансові збитки банків (рис.5).

Разом з тим, необхідно зазначити, що прямі фінансові збитки виявилися на четвертому місці. Це дійсно відповідає реальному стану справ, так як в Росії та інших країнах бувшого СНД ні одна організація не зобов'язана нести прямі втрати унаслідок витоку інформації. Цим наша країна та Росія відрізняється від США та Євросоюзу, де компанії можуть втратити ліцензії, заплатити багатомільйонний штраф, а в деяких випадках вище керівництво може навіть потрапити в тюрму. Із-за цієї ж причини мала доля респондентів вказала на юридичні витрати та переслідування зі сторони регуляторів ринку.

З проблемою витоку інформації можна боротись, але перемогти її повністю не можливо, оскільки ні апаратні, ні технічні засоби не можуть забезпечити необхідного захисту, бо техніка безсила проти витонченого розуму людини.

Таким чином, для боротьби з інсайдерством необхідно:

– проводити моніторинг дій інсайдерів з метою запобігання витоку конфіденційної інформації, завчасного виявлення шахрайства та захисту від саботажу або зловживань;здійснювати нагляд за діяльністю співробітників, з метою формування ланцюга підозрілих трансакцій;

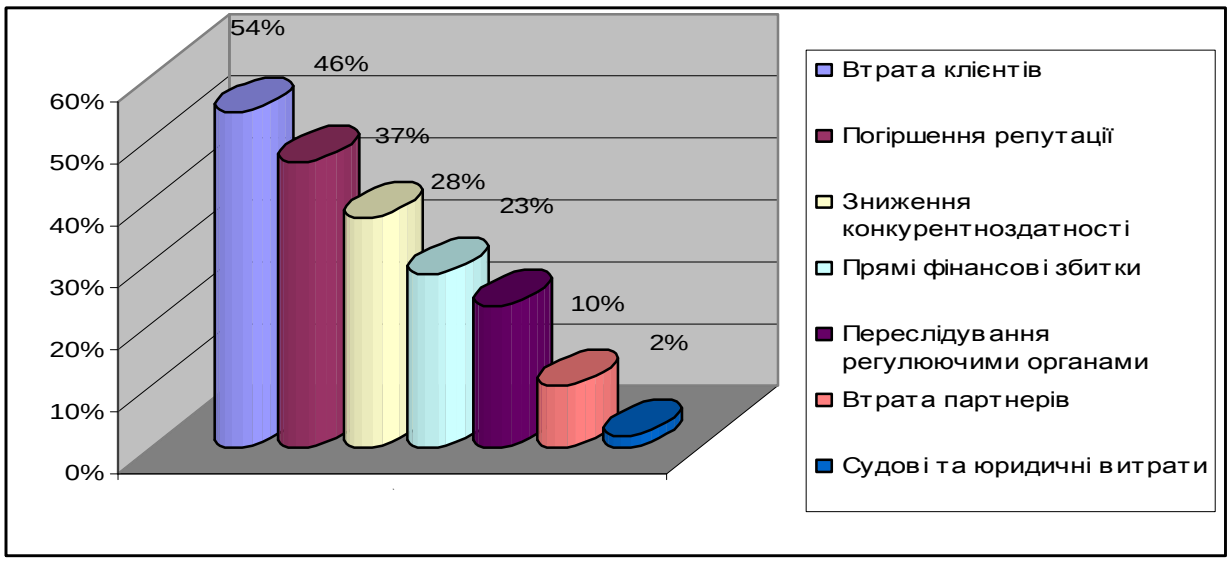

Рис.5. Негативні наслідки витоку інформації

– здійснювати апаратні обмеження можливостей роботи з інформаційною системою, при якому користувач не зможе скрити ні однієї своєї дії;

– надавати тільки авторизований доступ до баз даних, захищеним файловим архівам і порталам для можливості аудиту та профілактики правопорушень;

– вибраний продукт для захисту конфіденційної інформації, який зберігається в базах даних, повинен мати можливість віддаленого адміністрування і екстреного блокування доступу у випадку виникнення небезпеки;

– виконання принципів „знай свого клієнта" та „знай свого співробітника", які нашли своє відображення і в міжнародних, і в вітчизняних стандартах безпеки банківської діяльності;

– строга регламентація і контроль діяльності персоналу, а також закріплена у контрактах і трудових договорах відповідальність за можливі порушення.

Проведені дослідження показали, що не існує якогось одного способу, щоб повністю убезпечити себе від інсайдерів. Разом з тим, застосування комплексних методів захисту дозволяє мінімізувати ризики витоку та викривлення конфіденційної інформації.

Отже, основні проблеми захисту банків від внутрішніх загроз зумовлені їх недостатньою увагою до власної безпеки економічної інформації. Реалізація зазначених вище заходів дозволить мінімізувати ризики витоку конфіденційних даних, не втратити довіру клієнтів і не перетворитися на черговий об'єкт статистики інцидентів у сфері інформаційної безпеки.

Література

1. Перехрест Л.М. Забезпечення фінансової безпеки банків як умова стабільного функціонування банківської системи // Соціально-економічні дослідження в перехідний період. Методи оцінки рівня капіталізації інноваційних структур (Збірник наукових праць). Випуск 2(64)/ НАН України. Інститут регіональних досліджень. – Львів 2007. – С.334.

2. http;//www.ase/md/~osa/rus/index.html.

3. http;//www.securitylab.ru/news/278948/php.

4. Алавердов В.А. Риски нелояльности персонала в деятельности современного банка и противодействие им. // Оперативное управление и стратегический менеджмент в коммерческом банке. – 2003. – №3. – С. 117

5. http://www.infowatch.ru/threats?chapter=14151398&id=179263028

6. Єрмошенко М. М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. – К.: Київ, Нац. торг.-екон. ун-т, 2001. –309 с.

7. Єрмошенко М.М. Безпека фінансова. // Енциклопедія банківської справи України/ Редкол.: В.С. Стельмах (голова) та ін. – К.: Молодь, Ін Юре, 2001. – 680 с.

8. Барановський О.І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення): Монографія. – К.: Київ. нац. торг.-екон. ун-т, 2004. – 759 с.

9. Ареф'єва О.В., Кузенко Т.Б. Планування економічної безпеки підприємств. – К.: Вид-во Європ. ун-ту, 2004. – 170 с.

10. Клименко В.В. Фондовий ринок у контексті фінансової безпеки держави // Актуальні проблеми економіки. – 2002. – № 4. – С. 21-26.

11. Покотиленко Р.В. Механізм формування та забезпечення економічної безпеки: Автореф. дис. ... канд. екон. наук. – Донецьк: Ін-т економіки промисловості НАН України, 2003. – 20 с.

12. Чорнодід І.С. Економічна безпека як категорія економічної теорії // Актуальні проблеми економіки. – 2003. – №11. – С. 13-20.

13. Побережный С.Н. «Оценка финансово-экономической эффективности деятельности подразделений банковской безопасности»: Автореф. дисс. ... канд. экон. наук. – Суми: Украинская академия банковского дела Национального банка Украины, 2006. – 21с.

Статья поступила в редакцию 17.12.2007

О.І. БЛАГОДАРНИЙ, ***к.е.н., доцент,***
Інститут економіко-правових досліджень НАН України, м. Донецьк
С.В. РАК,
Головне управління статистики у Донецькій області
А.О. ФОМЕНКО,
Донецький національний технічний університет

НЕОБХІДНІСТЬ СІМЕЙНОЇ ПОЛІТИКИ ЯК ВІДПОВІДЬ НА ВИКЛИКИ ДЕМОГРАФІЧНОЇ СИТУАЦІЇ В ДЕРЖАВІ

Сьогодні в колі науковців ведеться активна дискусія щодо демографічної ситуації в країні, проте в суспільстві ще не відбулося усвідомлення важливості цієї проблеми і тих руйнівних наслідків, які несе в собі явище депопуляції населення.

Слід відзначити, що особливості демографічного розвитку держави, домінуючі тенденції становлення якісних та кількісних характеристик народонаселення відіграють важливу роль у забезпеченні повномасштабних перетворень. Тому дослідження кожного аспекту цієї проблеми завжди приваблювало дослідників і було досить актуальним.

Проблемі демографічного розвитку та назрівання демографічної кризи приділяли значну увагу В. Стешенко[1; 2], Е. Лібанова[3], С. Цапок [4]та інші спеціалісти не тільки України, а і других держав СНД та дальнього зарубіжжя. Але як правило, значна увага приділялася кількісним процесам в загальному вигляді і майже не досліджувалась згадана проблема в соціальному аспекті.

В зв'язку з цим метою цієї статті є аналіз процесів народжуваності в Україні, особливо поза офіційно зареєстрованим шлюбом і розробка пропозицій щодо вдосконалення сімейної політики в Україні.

Дуже часто суспільно-політичне обговорення даної проблематики „грішить" популізмом, спекулятивністю, має поверхневий характер. Безперечно важливо, що на рівні держави ведуться спроби виправити ситуацію в демографічній сфері. Проте виникають сумніви, чи в змозі цьому зарадити просте нарощування суми виплат на народження дитини. Як показала практика, чим вище виплати, тим дорожче все, що пов'язано з немовлям: медичне обслуговування вагітності і пологів, дитяче харчування, дитячі речі. Сьогодні дитячий візок коштує як невеликий меблевий гарнітур.

Зростає кількість жахливих фактів, коли матері народжують дітей тільки з метою отримати грошову допомогу, але немовлят не доглядають, не займаються їх