тереси бізнесу, ніж Податковий кодекс. Так, в даному документі враховано 70 % пропозицій Європейської бізнес-асоціації с Митним кодексом з 1 січня 2012 року буде запроваджено електронну систему декларування, визначено чіткий перелік документів, необхідних для оформлення товару на митниці; підприємець зможе самостійно обирати митницю, на якій проходитиме митну процедуру; час оформлення імпортно-експортної операції буде скорочено з 24 до 4 годин, митник нестиме персональну відповідальність за неправомірні затримки. Також новим Митним кодексом встановлено перелік особистих речей, які людина може перевозити через кордон без декларування, лібералізовані норми вивезення товару. Громадяни отримають право ввозити через кордон в Україну товари на 1000 євро вагою 50 кілограмів у ручній поклажі (сьогодні дозволено на 200 євро); товари на суму від 1 до 10 тисяч євро оподатковуватимуться за загальною ставкою мита у розмірі 10 відсотків [3].

Нові митні правила сприятимуть збільшенню товарообігу, контрабандні товари одразу вилучатимуться та продаватимуться, бюджет отримуватиме кошти, не чекаючи кілька років на завершення кримінальної справи; зменшення числа контролюючих органів сприятиме зниженню рівня корупції.

Прийнятий Податковий кодекс та діючі процедури адміністрування податків в Україні потребують значних доопрацювань з метою вдосконалення правового поля справляння податкових платежів. Для підвищення економічної безпеки підприємництва потрібно впровадити дієву систему моніторингу ефективності функціонування податкової системи. Доопрацювання ж нового Митного кодексу повинно здійснюватись в рамках максимального наближення українського митного законодавства до міжнародних конвенцій і стандартів, спрощення бюрократичної митної процедури, а також врахування тих труднощів, з якими зіштовхнулись вітчизняні податкові органи та бізнес на шляху впровадження в дію Податкового кодексу.

Література

1. http://dt.ua/ECONOMICS/male_pidpriemnitstvo_sezon_polyuvannya_vidkrito-90951.html
2. http://news.finance.ua/ua/~/2/110/all/2011/11/09/258325
3. http://news.finance.ua/ua/~/2/110/all/2011/11/13/258810

Ролдугіна Ю.В., Ковальова І.В.

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВ

Сьогодні спостерігається бурхливий розвиток інформаційних технологій. Говорячи про інформаційну безпеку, досить рідко згадують про блокування зовнішніх носіїв на робочих місцях. Інформація, яка знаходиться на електронних носіях, займає вагоме місце в житті суспільства. Доступність такої інформації обумовлена цілим рядом факторів, зокрема, великі об’єми, можлива анонімність доступу, можливість «інформаційних диверсій» і т.д. Все це робить завдання забезпечення захищеності інформації, що розміщується у комп’ютерному середо-

вищі, значно складнішою проблемою, ніж, наприклад, збереження таємниці традиційної поштової переписки.[3]

Актуальність обраної теми обумовлена тим, що стратегія інформаційної безпеки банків дуже сильно відрізняється від аналогічних стратегій інших компаній та організацій. Це зумовлено специфічним характером загроз, а також публічною діяльністю банків, які змушені робити доступ до рахунків досить легким з метою зручності для клієнтів.

В економічній літературі багато уваги приділяється дослідженню даної проблеми, зокрема важливе місце займають праці вчених: С.П.Расторгуєв, О.Г.Білорус, Д.Г.Лук'яненко, Є.А.Макаренко, А.М.Гуз та інші.

Мета дослідження полягає у вивченні теоретичних засад інформаційної безпеки, а також виявленні основних факторів, якими керується сучасна інформаційна безпека банку.

Інформація стає унікальним і вічним ресурсом для людини. Її унікальність тільки підсилюється у сучасних умовах. В Україні простежується тенденція зростаючої залежності окремих секторів національної економіки від значного обсягу інформаційних потоків. [6]

Існує багато понять інформаційної безпеки, одне з яких визначає її як захищеність інформації і підтримуючої інфраструктури від випадкових або спеціальних впливів природного чи штучного характеру, що може принести шкоду власникам чи користувачам інформації чи підтримуючої інфраструктури. [3] Сьогодні неможливо уявити функціонування банківських установ без використання сучасних інформаційних технологій та глобальних комп'ютерних мереж, у тому числі й Internet. Це пояснюється тим, що он-лайнові банківські послуги дозволяють проводити фінансові операції без посередників, що призводить до зниження комісійних і прискорення обігу фінансових активів. На користь використання сучасних інформаційних технологій для проведення банківських операцій, що здійснюються як з юридичними, так і з фізичними особами, свідчить дослідження, проведене консультаційною фірмою Booz, Allen and Hamilton. За його результатами оплата послуг через Internet обходиться клієнту в $ 0,01, з використанням автоматів — у $ 0,27, надання послуг по телефону — $ 0,54, а у касового вікна — у $ 1,07. [4]

Інформація, яка зберігається та обробляється в банківських системах представляє собою реальні гроші. Цілком зрозуміло, що незаконне маніпулювання з такою інформацією може привести до серйозних збитків. Конкурентоспроможність банку залежить від того, наскільки клієнтові зручно працювати з банком, наскільки клієнт довіряє банку, а також наскільки широкий спектр його послуг, включаючи послуги, пов'язані з віддаленим доступом. Тому клієнт повинен мати можливість швидко розпоряджатися своїми грошима. Але така легкість доступу до грошей підвищує ймовірність злочинного проникнення в банківські системи.

Комп'ютерні злочини не завжди високотехнологічні. Досить підробки даних, зміни параметрів середовища автоматизованих систем обробки інформації банків (АСОІБ) і т.д., а ці дії доступні і обслуговуючому персоналу.

Специфіка захисту автоматизованих систем обробки інформації банків обумовлена особливостями розв'язуваних ними завдань. Як правило АСОІБ обробляють великий потік запитів, що постійно надходять в реальному масштабі часу, кожен з яких не вимагає для обробки численних ресурсів, але всі разом вони можуть бути оброблені тільки високопродуктивної системою. У АСОІБ зберігається і обробляється конфіденційна інформація, не призначена для широкої публіки. Її підробка або витік можуть призвести до серйозних наслідків. [2] Одна з систем, що забезпечує захист інформації - це DLP (Data Loss Prevention) – система та інші засоби, що захищають від витоків, перекривають або контролюють ті чи інші канали, по яким інформація може покинути інформаційну систему, такі як мережеві з'єднання по різних протоколах, відчужувані носії інформації, мобільні комп'ютери, принтери і т.д. [1] Не завжди у банків вистачає коштів і умінь перекрити всі можливі канали. Ті носії, які залишаються без належного контролю, є провідниками відповідної частки випадкових витоків. Щоб ефективно протидіяти як випадковим, так і умисним витокам, DLP-система, зрозуміло, повинна охоплювати всі без винятку канали (носії).

Проаналізувати глобальний виток інформації по всьому світу, можна за даними наведеними у таблиці . [1]

Таблиця 1

Основні канали витоку інформації за 2009-2010 роки

Канали витоку	2009		2010	
	Кількість	%	Кількість	%
Мобільний комп’ютер	49	11,9	40	10,5
Носії інформації (CD/DVD, флешносії)	23	5,6	32	8,4
Настільний комп'ютер, сервер, НЖМД	41	9,9	90	23,6
Інтернет (вкл. e-mail)	97	23,5	82	21,4
Паперовий документ	84	20,3	78	20,4
Архівний носій	48	11,6	6	1,6
Інший	36	8,7	25	6,5
Не встановлено	35	8,5	29	7,6
ВСЬОГО	413	100	382	100

Протягом проаналізованого періоду спостерігається зменшення загальної кількості витоку інформації – якщо у 2009 році цей показник складав 413 одиниць, то у 2010 він зменшився до 382. Найбільшу частку серед усіх зазначених каналів витоку у 2010 році займає настільний комп’ютер – 23,6 %, тоді як ще у попередньому році його частка була 9,9 %. Помітно зменшилася у 2010 році кількість витоків за допомогою архівних носіїв. Виток через мобільні комп'ютери (у 2010 році їх кількість зменшилася на 1,4%) і мобільні носії були надзвичайно популярні 2-3 роки тому і раніше. Зменшення числа витоків, пов'язаних з відчужуваними носіями, пояснюється впровадженням засобів шифрування. Зашифрований носій при втраті або крадіжці витоком не вважається. Що стосується рівня безпеки банківської системи України, то необхідно зазначити, що більшість керівників українських банків всерйоз задумалися над захистом корпора-

тивних даних лише після впровадження ISO27001/ISO27002 як галузевого стандарту НБУ, що заклав основу правильного розуміння ІБ. При цьому згідно з дослідженням, проведеним SearchInform в квітні 2007 року в Києві, основна частина (71,4%) комерційних і державних організацій столиці до цих пір не використовують комплексні системи запобігання витоків даних.

З метою підвищення рівня інформаційної безпеки банківських систем Правління НБУ видало постанову від 28.10.2010 N 474, де встановлено, що з дня опублікування даної постанови вступають в силу такі стандарти НБУ: 1) СОУ Н НБУ 65.1 СУІБ 1.0:2010 "Методи захисту в банківській діяльності Система управління інформаційною безпекою. Вимоги "(ISO / IES 27001:2005, MOD); 2) СОУ Н НБУ 65.1 СУІБ 2.0:2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO / IES 27002:2005, MOD).

Протягом 90 днів після вступу в силу цих стандартів банкам було надано методичні рекомендації щодо впровадження стандартів, рекомендації щодо переліку, змісту та правил заповнення документів, які повинні бути створені при впровадженні стандартів у банках України, а також рекомендації щодо методик оцінки ризиків, пов'язаних з інформаційними технологіями. Банки зобов'язані впровадити системи управління інформаційною безпекою відповідно до стандартів НБУ до 01.10.2011. [5]

Таким чином, інформаційна безпека – стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків. Сьогодні існує гостра необхідність побудови повноцінної системи інформаційної безпеки. Зокрема, гострим постає питання інформаційної безпеки банківських систем не лише для України, а й для світу в цілому. Для банків ця проблема є дуже важливою, оскільки щомісяця в світі звідти відбувається витік інформації, результатом чого є не лише втрата довіри клієнтів (отже і зниження конкурентоспроможності), а й значні збитки в десятки і навіть сотні мільйонів доларів. Існує багато сучасних методів захисту інформації у банках, використання яких помітно зменшило кількість основних каналів витоку інформації протягом останніх двох років.

В Україні з метою вирішення даного питання НБУ прийняв Постанову Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України, проте це лише крок до подолання проблеми, що склалася. Але для отримання помітних результатів не достатньо прийняття нормативних постанов, необхідна взаємодія нормативно-правового, організаційно-економічного та морально-етичного елементів інформаційної системи. Лише поєднання ефективної дії цих сегментів дозволить забезпечити довгостроковий прогнозований розвиток інформаційної безпеки не лише банківських установ, а й держави в цілому.

Література

1. Аналітичні дані інформаційної безпеки – www.infowatch.ru
2. Банковские системы // Информационная безопасность [Электронный ресурс] Информационная безопасность – Режим доступа: http://inf-bez.ru/?p=449
3. Безопасность режима банка // Информационные технологи [Электронный ресурс] Информационные технологии – Режим доступа: http://www.prostobankir.com.ua/it/stati/bezopasnyy_rezhim_banka
4. М. Гуцалюк Безпека банківських інформаційних систем // Центр исследования проблем компьютерной преступности [Електронний ресурс] Crime-research – Режим доступу: http://www.crime-research.ru/library/bezp_ba.htm
5. Повышение уровня информационной безопасности в банковской системе Украины // Центр бизнесс-знаний [Електронний ресурс] Центр бизнесс-знаний – Режим доступу:http://www.cbz.com.ua/contents/article/index/language/ru/ section/63/article/3182.
6. Л. Щукін Окремі питання інформаційної безпеки та її роль у вітчизняних умовах // Seemus Media [Електронний ресурс] Seemus Media – Режим доступу: http://www.seemus.com.ua/article/Tochka_zreniya/Okremi_pitannya_informatsiynoyi_bezpeki_ta_yiyi_rol_u_vitchiznyanih_umovah.html

Томашик Л. С.

ЗОЛОТОВАЛЮТНІ РЕЗЕРВИ ДЕРЖАВИ ЯК МЕТОД МОБІЛІЗАЦІЇ РЕСУРСІВ ДЛЯ СТАБІЛІЗАЦІЇ ЕКОНОМІКИ

Важливим методом валютного регулювання є управління офіційними валютними резервами. Валютні резерви – це запаси резервних активів, які перебувають на рахунках у центральному банку та в банках за кордоном і використовуються для сплати боргових зобов'язань, а також, уразі необхідності, для проведення валютних інтервенцій з метою регулювання курсу національної грошової одиниці.

Рівень офіційних валютних резервів залежить від низки факторів, зокрема:

1. Стану зовнішньої торгівлі. За сприятливої кон'юнктури на світових ринках, яка зумовлює зростання прибутків від експорту та падіння цін на імпорт, а відповідно і падіння імпортних витрат, спостерігається збільшення обсягу офіційних валютних резервів країни. Натомість коли знижуються ціни на експорт, відповідно дорожчає імпорт та з'являється негативне сальдо торговельного балансу, що призводить до скорочення валютних резервів через необхідність витрачати значні кошти в іноземній валюті для фінансування імпорту [3, с. 377].

2. Врівноваженості платіжного балансу. Погіршення платіжного балансу призводить до падіння курсу національної грошової одиниці, виникає потреба використовувати валютні резерви для регулювання курсу національної грошової одиниці.

3. Режиму валютних обмежень. В окремих країнах обмін національної