УДК 004.021, 004.27

СТАНДАРТИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКУ

MANAGEMENT STANDARDS OF BANK INFORMATION SECURITY

Христина Омелянівна ЗАСАДНА

к.ф.-м.н., доцент кафедри комп'ютерних технологій Львівського інституту банківської справи УБС НБУ (м. Київ)
E-mail: zasadna@lbi.wubn.net

Khrystyna O. ZASADNA
PhD in Physical and Mathematical Sciences, Associate Professor of Computer Technologies Department Lviv Institute of Banking of the University of Banking of the National Bank of Ukraine (Kyiv)

Анотація. Розглянуто трактування терміну «інформаційна безпека банку». Обґрунтовано важливість створення системи стандартизації в сфері інформаційної безпеки в банках України з урахуванням міжнародних стандартів захисту інформації.

Summary. This article discusses interpretations of the term «bank information security». It also emphasizes the importance of standardizing the sphere of information security in Ukrainian banks based on international information security standards.

Ключові слова: *інформаційна безпека банку, стандарти інформаційної безпеки, інформаційні технології.*

Key words: *bank information security, information security standards, information technology.*

Постановка проблеми. Останнє десятиліття характеризується швидким розвитком системи дистанційних банківських послуг та розташованих поза банком систем електронних платежів. Оскільки відмовитися від їх використання неможливо, треба передбачити, оцінити та застрахувати всі види небезпек, які виникають при наданні фінансових послуг, пов'язаних з використанням комп'ютерних та телекомунікаційних мереж. Розроблені методи та засоби захисту інформації в каналах зв'язку є складовою частиною інформаційної безпеки банку.

Складові інформаційної безпеки банку мають перш за все властивості, притаманні інформаційній безпеці інформаційних систем загалом: конфіденційність, цілісність, доступність – тріада CIA [1]. Як об'єкт захисту інформаційні системи (також банківські) можна розділити на три частини – апаратне забезпечення, програмне забезпечення та комунікації і для захисту кожної з цих частин використовують різні стандарти інформаційної безпеки [1].

Аналіз останніх досліджень і публікацій. До недавнього часу серед науковців не існувало однозначного тлумачення терміну «інформаційна безпека банку», пояснювали цей термін як юристи, так і працівники банківських установ. Наведемо кілька його трактувань.

М. Зубок розрізняє інформаційну безпеку банку як один із видів безпеки банківської діяльності – це забезпечення гарантованого захисту інформаційних ресурсів банку від внутрішніх і зовнішніх посягань [2].

Доктор юридичних наук Марущак А. І. розглядає інформаційну безпеку банківських установ у

контексті трьох складових: безпеки інформаційних ресурсів (збереження від несанкціонованого розповсюдження, використання і порушення конфіденційності взаємозв'язаної, упорядкованої, систематизованої і закріпленої на матеріальних носіях інформації, яка належить банківській установі); безпеки інформаційної інфраструктури (стан захищеності електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку банківської установи, яка забезпечує цілісність і доступність інформації, що в них обробляється), та безпеки «інформаційного поля» (несистематизовані потоки інформації, що оприлюднюються різноманітними учасниками інформаційних відносин) [3]. Тут же описані найбільш суттєві загрози інформаційній безпеці банківських установ та заходи ліквідації цих загроз.

Кандидат юридичних наук Бодюл Є. М. під інформаційною безпекою банку розуміє стан захищеності інформації щодо власників, керівництва, клієнтів банку, технологій та інформаційних ресурсів банку від внутрішніх і зовнішніх загроз. А під політикою інформаційної безпеки банківської установи – науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного рішення задач інформаційного захисту банківської справи від протиправних дій. Автор також зазначає, що забезпечення інформаційної безпеки є невід'ємною складовою частиною діяльності комерційного банку та визначає мету і завдання системи інформаційної безпеки [3].

Кандидат юридичних наук Сліпченко В. І. визначає інформаційну безпеку банку як організацію гарантованого захисту його інформаційних ресурсів, відповідну професійну підготовку працівників у галузі інформаційних технологій, що забезпечує захист інформаційних ресурсів та інформаційних потоків від несанкціонованого доступу до них. Він також вважає, що політика інформаційної безпеки банку повинна відображати принципи та методи захисту інформації з обмеженим доступом [3].

Мета статті полягає у дослідженні створення системи стандартизації в сфері інформаційної безпеки в банках України з урахуванням міжнародних стандартів захисту інформації.

Обґрунтування отриманих наукових результатів. Інформаційна безпека передбачає забезпечення захисту інформації та інфраструктури, що здійснює її підтримку, від будь-якого випадкового або ж зловмисного втручання, в результаті якого інформація може бути втрачена, нанесені збитки її безпосереднім власникам та інфраструктурі, що підтримує її зберігання й існування. Інформаційна безпека виконує завдання, пов'язані з прогнозуванням і запобіганням можливим подібним діям, а також зводить до мінімуму можливий збиток [4].

Інформаційна безпека банку – система організаційних і технічних засобів, які забезпечують конфіденційність, збереження інформації, її захищеність від несанкціонованого доступу, псування, вилучення, порушення повноти й цілісності – з одного боку, і ефективне функціонування механізмів поповнення, оновлення, аналізу необхідних для діяльності банку відомостей, доступність цієї інформації для авторизованих (таких, що мають право доступу) користувачів – з іншого. Інформаційна безпека банку тісно пов'язана із загальною безпекою банку, дотриманням банківської та службової таємниці. Особливим напрямом інформаційної безпеки банку є забезпечення захисту банківських інформаційно-обчислювальних мереж, систем електронних платежів, комп'ютерних баз даних від несанкціонованого проникнення, а також від технічних перебоїв і неполадок [5].

Узагальнюючи наведені вище трактування терміну «інформаційна безпека банку», можна зробити такі висновки. Інформаційна безпека банку – це особлива складова частина його загальної безпеки. Захист паперового та електронного документообігу в банку має свої особливості, зокрема, паперовий документообіг проконтролювати складніше, ніж електронний, але методи захисту паперового документообігу вже усталені. Одночасно з швидким впровадженням у банківській сфері систем електронного документообігу та послуг дистанційного обслуговування клієнтів виникло питання захисту цих послуг, а акценти інформаційної безпеки банку змістилися у напрямі

захисту електронних послуг банків. Тому служби інформаційної безпеки банків активно зайнялися питаннями дотримання правил опрацювання інформації засобами інформаційних технологій (програмні засоби адміністрування прав користувачів, їх ідентифікацію, автентифікацію та авторизацію, засоби технічного, апаратно-програмного та криптографічного захисту, захист інформації, що поступає з мережі Інтернет), хоча вони передбачають також дотримання організаційних заходів адміністративного характеру. Термін «інформаційна безпека» використовується у нормативно-правових актах НБУ, які стосуються захисту систем електронного документообігу та електронних платежів. Так, у Постановах Правління НБУ вживаються терміни «інформаційна безпека під час роботи з електронними банківськими документами», «виконання вимог щодо правил інформаційної безпеки в банках України, їх філіях, органах державної влади, небанківських установах», «конфіденційність та цілісність електронної інформації, автентифікація учасників СЕП та учасників інформаційних задач», «організаційні заходи інформаційної безпеки» [6, 7].

Зміст терміну «інформаційна безпека банку» розкрито в стандарті НБУ [8]. Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації; крім того можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність. Для банків України відстежуваність, неспростовність, надійність та автентифікація користувачів та інформаційних ресурсів є обов'язковими вимогами інформаційної безпеки [8].

Безумовно, основна увага в питаннях інформаційної безпеки банку повинна приділятися дотриманню нормативно-правових актів НБУ з питань організації та управління інформаційною безпекою. А це як правові заходи – закони, укази, положення, постанови, правила, стандарти, інші нормативні документи; так і організаційні заходи – розробка правил обробки інформації, підбір персоналу, організація режиму доступу до приміщень, де розміщена автоматизована система, заходи щодо захисту системи та інформації, що обробляється та ін. [5].

Стандарт – це зразок, модель, еталон, який використовується для порівняння. В багатьох країнах стандарт – це нормативний документ, який встановлює комплекс норм, правил, вимог до об'єкта стандартизації, прийняті стандарти мають статус законів. Необхідність застосування тих чи інших стандартів залежить від сфери діяльності та конкретних потреб підприємства. За категоріями стандарти поділяють на Міжнародні, Регіональні, Національні (Державні, Галузеві), організацій, підприємств, товариств. Стандарти управління інформаційною безпекою давно впроваджені в банківських системах економічно розвинутих країн світу, Європи, в Росії та Білорусії. В Росії та Білорусії принято стандарти ISO/IEC 27002:2005 – ГОСТ Р ИСО\МЭК 17799-2005, ГОСТ 27001:2006, ГОСТ 13335-1:2006, ГОСТ 13335-3:2007, СТО БР ИББС-1.0-2010, РС БР ИББС-2.0-2007, СТО БР ИББС-1.1-2007, СТО БР ИББС-1.2-2010. РС БР ИББС-2.1-2007 та ін. Розробниками міжнародних стандартів є Міжнародна Організація із Стандартизації ISO, Міжнародна Електротехнічна Комісія IEC та Британський інститут стандартів BSI, вони формують спеціалізовану систему всесвітньої стандартизації [1].

На сьогодні в питаннях інформаційної безпеки прийняті, зокрема, такі міжнародні стандарти.

1. Серія ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»:

– ISO/IEC 27000:2009. Визначення і основні принципи;

– ISO/IEC 27001:2005. Інформаційні технології – Методики безпеки – Системи менеджменту інформаційної безпеки – Вимоги (BS 7799-2:2005);

– ISO/IEC 27002:2005. Інформаційні технології – Методики безпеки – Практичні правила управління інформаційною безпекою (попередній код ISO/IEC 17799:2005;

– ISO/IEC 27003:2010. Настанова з впровадження системи управління інформаційною безпекою;

– ISO/IEC 27005:2008. Інформаційні технології – Методики безпеки – Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006);

– ISO/IEC 27006:2007. Інформаційні технології – Методики безпеки – Вимоги до організацій, що провадять аудит і сертифікацію систем менеджменту інформаційної безпеки;

– ISO/IEC 27011:2008. Керівництво з менеджменту інформаційної безпеки для телекомунікацій;

– ISO/IEC 15408. Загальні критерії оцінки безпеки інформаційних технологій.

2. Серія ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»:

– ISO13335-1:2004. Інформаційні технології – Керівництво по управлінню IT безпекою – Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій;

– ISO13335-3:1998. Інформаційні технології – Керівництво по управлінню IT безпекою – Методи управління IT безпекою;

– ISO13335-4:2000. Інформаційні технології – Керівництво по управлінню IT безпекою – Вибір механізмів захисту;

– ISO13335-5:2001. Інформаційні технології – Керівництво по управлінню IT безпекою – Керівництво по управлінню мережевою безпекою.

НБУ послідовно впроваджує міжнародну політику в сфері забезпечення інформаційної безпеки банків. Постанова Правління НБУ № 474 [9] зобов'язує всі українські банки до 1 жовтня 2011 року привести у відповідність свої системи менеджменту інформаційної безпеки до вимог стандарту ISO/IEC 27001. Згідно з цією постановою з дня її опублікування набирають чинності два галузеві стандарти: Стандарт організації України. Настанова «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та Стандарт організації України. Настанова «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою». Перший стандарт є прийнятий зі змінами стандарт ISO/IEC 27001:2005. Другий стандарт є прийнятий зі змінами міжнародний стандарт ISO/IEC 27002:2005 [8, 10].

Важливим документом є також «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України від 01.03.2011» [11]. У цьому документі сказано, що система управління інформаційною безпекою є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках. Стандарти Національного банку України основані на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами, які вже висунуто в нормативних документах Національного банку України. Відповідність системи управління інформаційною безпекою стандартам Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 гарантує банку відповідність міжнародним стандартам ISO 27001 та ISO 27002. Необхідність впровадження в банках України стандартів з управління інформаційною безпекою продиктована вимогами Базельського комітету Basel II з управління та зменшення операційних ризиків банків. Ці Методичні рекомендації розроблені на основі міжнародного стандарту ISO/IEC 27003:2010 з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки. Система інформаційної безпеки повинна забезпечити безпечність та надійність функціонування бізнес-процесів / банківських продуктів банку [11].

Висновки. Інформаційна безпека є сьогодні однією з актуальних тем, особливо для банків та інших фінансово-кредитних установ. Впровадження нових стандартів НБУ з управління інформаційною безпекою дозволить підвищити рівень безпеки клієнтів банку, запровадити механізми управління операційними ризиками, виявляти критичні ризики та зменшити ймовірність їх реалізації, забезпечити розуміння питань інформаційної безпеки працівниками. Впровадження стандартів [8, 10] – це важливий крок у створенні системи стандартизації в сфері інформаційної безпеки в банках України з урахуванням міжнародних стандартів захисту інформації.

На думку фахівців ТОВ «Агентство активного аудиту» впровадження в банках України

стандартів з управління інформаційною безпекою дозволить:

– знизити та оптимізувати вартість побудови та підтримки системи інформаційної безпеки;

– постійно відстежувати та оцінювати ризики з урахуванням цілей бізнесу;

– ефективно виявляти найбільш критичні ризики та уникати їх реалізації;

– розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;

– забезпечити розуміння питань інформаційної безпеки керівництвом банку та всіма працівниками банку;

– забезпечити підвищення репутації та ринкової привабливості банків;

– забезпечити захист від рейдерських атак [12].

ТОВ «Агентство активного аудиту» розробило й опублікувало План дій щодо впровадження вимог галузевих стандартів інформаційної безпеки СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, його можна знайти в мережі інтернет за адресою [12].

Список використаних джерел

1. Електронний ресурс [сайт]. – Режим доступу: – http://uk.wikipedia.org.

2. Зубок М. І. Безпека банківської діяльності: навч. посіб. / М. І. Зубок. – К. : КНЕУ, 2002. – 190 с.

3. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж: тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1-2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи НБУ». – Суми: ДВНЗ «УАБС НБУ», 2010.

4. Електронний ресурс [сайт]. – Режим доступу: – http://kaspersky-antivirus.kiev.ua/reshenija/infosecur.html.

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

6. Постанова Правління НБУ від 02.04.2007 № 112 «Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України» [Електронний ресурс] // [сайт]. – Режим доступу: http://www.bank.gov.ua.

7. Постанова Правління НБУ від 16.08.2006 № 320 «Про затвердження Інструкції про міжбанківський переказ коштів в Україні в національній валюті». [Електронний ресурс] // [сайт]. – Режим доступу: http://www.bank.gov.ua.

8. 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). [Електронний ресурс] // [сайт]. – Режим доступу: http://www.zakon.rada.gov.ua.

9. Постанова Правління НБУ від 28 жовтня 2010 року N 474 «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України». [Електронний ресурс] // [сайт]. – Режим доступу: http://www.zakon.rada.gov.ua.

10. СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27001:2005, MOD). [Електронний ресурс] // [сайт]. – Режим доступу: http://www.zakon.rada.gov.ua.

11. Лист Департаменту інформатизації НБУ від 03.03.2011 № 24-112/365/ – [Електронний ресурс] // [сайт]. – Режим доступу: http://www.zakon.rada.gov.ua.

12. [Електронний ресурс] // [сайт]. – Режим доступу: – http://www.auditagency.com.ua.