Дика О. В., магістр групи ФЕБ-11
Науковий керівник:
Карковська В. Я., ст. викладач
Національний університет
«Львівська політехніка»

Застосування міжнародних стандартів у вирішенні проблем управління інформаційною безпекою банку

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 [1].

На даний час в сфері інформаційної безпеки банків існує ряд проблем, а саме: ставлення керівників банків до інформаційних технологій неоднозначне: одні підтримують упровадження сучасних інформаційних технологій, розуміючи, що це дасть конкурентні переваги банку, сприятиме популярності серед клієнтів; інших стримує та обставина, що сучасні інформаційні технології потребують значних фінансових ресурсів, особливо під час впровадження [2].

Керівництво банку часто вважає, що витрати на систему захисту інформації занадто великі, та не приносять прибутку, тому без них можна обійтись. Однак, якщо банк не приділятиме достатньої уваги інформаційній безпеці в майбутньому він може зазнати значних ризиків: фінансові втрати, погіршення репутації, часті хакерські атаки, помилки та недостатня обізнаність персоналу, відсутність належної системи захисту, неправильна робота програмно-технічних комплексів, використання небезпечних інформаційних технологій, неправильне використання послуг третіх сторін та ін.

Всі ці ризики призводять до втрати конфіденційності, цілісності й доступності інформації, тобто — до порушення інформаційної безпеки. Щоб зменшити (усунути) ці ризики банк повинен розробити і впровадити систему захисту інформації та політику інформаційної безпеки.

Для покращення реалізації цих заходів варто звернути увагу на міжнародні стандарти з управління інформаційною безпекою (рис. 1), які дозволяють: оптимізувати вартість побудови та підтримання системи інформаційної безпеки; постійно відслідковувати та оцінювати ризики з урахуванням цілій бізнесу; ефективно виявляти найбільш критичні ризики та знижувати ймовірність їх реалізації; розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання; ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу; забезпечити розуміння питань інформаційної безпеки керівництвом та всіма працівниками банку; забезпечити підвищення репутації та ринкової привабливості банків; знизити ризики рейдерських та інших шкідливих для банку атак тощо.

Однак, наведені вище переваги не будуть досягнуті шляхом лише "формального" підходу до розроблення, впровадження та функціонування системи управління інформаційною безпекою, необхідно, щоб керівництво і працівники банку були теж зацікавлені в підвищенні рівня інформаційної безпеки.

Отже, застосування міжнародних стандартів у вирішенні проблем управління інформаційною безпекою сприятиме стабільній роботі банківських установ.

Стандарт	Опис
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»	
ISO 13335-1:2004	Інформаційні технології — Керівництво по управлінню IT безпекою — Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій
ISO 13335-3:1998	Інформаційні технології — Керівництво по управлінню IT безпекою — Методи управління IT безпекою
ISO 13335-4:2000	Інформаційні технології — Керівництво по управлінню IT безпекою — Вибір механізмів захисту
ISO 13335-5:2001	Інформаційні технології — Керівництво по управлінню IT безпекою — Керівництво по управлінню мережевою безпекою

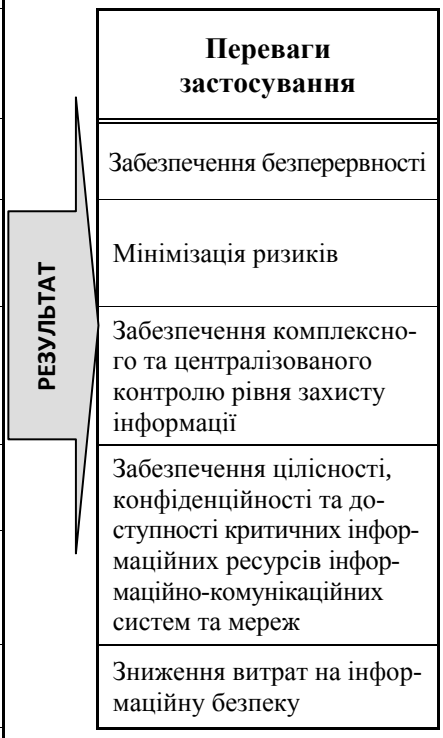

Рис.1. Переваги застосування системи управління інформаційної безпеки на базі міжнародних стандартів серії ISO

1. Енциклопедія банківської справи України / Ред. кол.: В. С. Стельмах (голова) та ін. — К.: Молодь, Ін Юре, 2001. — 680 с.
2. Савченко А., Івченко І. Інформаційна безпека банків: шляхи розв'язання проблеми [Текст] / А. Савченко, І. Івченко // Вісник Національного банку України. — 2010. — № 05 (171). — С. 3–5.