В.С. Остапчук, *Луцький національний технічний університет*

КОМП'ЮТЕРНІ СКЛАДОВІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ БАНКУ

Останнім часом усе частіше в офіційних джерелах та чисельних періодичних виданнях різного рівня з'являються такі терміни, як "інформаційна безпека", "комп'ютерна безпека", "безпека інформації" тощо. У зв'язку з впровадженням у банках та в інших фінансово-кредитних установах нових інформаційних (комп'ютерних) технологій інколи поняття "інформаційна безпека" зводитися до поняття "комп'ютерна безпека". Сьогодні не існує чіткого визначення сутності цих понять, має місце некоректність вживання деяких термінів. *Інформаційна безпека* не зводиться до суто *комп'ютерної безпеки*, як і поняття інформатизації не зводиться до поняття комп'ютеризації.

Інформаційна безпека, включаючи в себе *комп'ютерну безпеку* як необхідну складову, має ще й організаційну, правову, морально-етичну та інші складові та поширюється на усі соціальні процеси, в яких функціонує банк. При класичній структурі управління з функціональним підходом (по горизонталі) *комп'ютерна безпека* стосується лише охорони устаткування та інформації в ЕОМ від порушення правил технічної експлуатації, присвоєння майна, стихійних лих, нанесення навмисного чи випадкового збитку.

Як і для інших цінностей, наприклад, грошей, найбільша загроза інформацію підстерігає у місцях її зберігання, оброблення та переміщення, зокрема базах даних, робочих станціях і комп'ютерних мережах. Звідси і виникає проблема забезпечення захищеності даних *від утрати чи псування*, від *несанкціонованого доступу*, а також захист ІС від *катастроф чи аварій* при експлуатації. ІС вразлива в плані можливості порушення її роботи. Ці порушення можуть мати як випадковий, так і умисний характер. Отже, ІС ще мають бути захищені від *технічних відмовлень* і від *технологічних порушень* при експлуатації.

Усі загрози інформації можуть обумовлюватися як зовнішніми, так і внутрішніми причинами. Відповідно до цього на всіх етапах життя системи необхідно вживати спеціальні заходи щодо забезпечення її надійного функціонування й захищеності.

Нині відомий перелік загроз, внаслідок яких може наступити утрата чи псування інформації: крадіжки комп'ютера чи пристрою для збереження інформації в комп'ютері; аварії у комп'ютерній системі, що призводять до псування пристрою для збереження інформації; технічний вихід з ладу пристрою для збереження інформації; навмисне або випадкове затирання чи зміна сутності інформації особами, які мають доступ до інформації; навмисне затирання чи зміна сутності інформації комп'ютерними вірусами; навмисне затирання чи зміна сутності інформації особами, що несанкціоновано фізично або програмно проникають до місця збереження інформації.

На противагу інформаційним загрозам розроблено заходи безпечного збереження інформації. До них належать такі: аутентифікація користувача і встановлення його ідентичності; управління доступом до баз даних; підтримання цілісності даних; протоколювання й аудит; захист комунікацій між клієнтом і сервером; шифрування даних; сервіси безпеки ІС та ін. При впровадженні кожного із заходів дотримуються певних принципів. Розробляються нові заходи.

Ефективність заходів безпеки оцінити важко, бо вітчизняні комерційні банки з метою забезпечення конкурентоспроможності не розкривають фактів порушення безпеки. Однак деякі висновки щодо комп'ютерної безпеки уже зроблені. Наприклад, відомо, що кожну систему обробки інформації варто розробляти індивідуально.

Остапчук, В.С. Комп'ютерні складові безпеки інформаційних технологій банку [Текст] / В.С. Остапчук // Проблеми і перспективи розвитку банківської системи України : збірник тез доповідей XI Всеукраїнської науково-практичної конференції (30-31 жовтня 2008 р.) : у 2-х т. – Суми : УАБС НБУ, 2008. – Т. 1. – С. 93-94.