Розділ І. ГРОШІ, ФІНАНСИ І КРЕДИТ

УДК 336.71

В. С. Білошапка
канд. екон. наук, доцент,
доцент кафедри банківської справи
ДВНЗ «КНЕУ імені Вадима Гетьмана»

ПРАКТИЧНІ АСПЕКТИ БЕЗПЕКИ БАНКІВСЬКИХ ЕЛЕКТРОННИХ СИСТЕМ

Работа посвящена исследованию практических вопросов и проблем работы банковских электронных систем. Дается определение безопасности банковских электронных систем в контексте современной банковской деятельности. Раскрыты некоторые аспекты данного процесса, на которые следует обратить особое внимание уже сейчас.

The work deals with investigation of practical questions and problems in the electronic systems of banks. Determination of the safety of electronic systems in modern banking is given. Some aspects to which it is necessary to pay special attention already now are opened.

Роботу присвячено дослідженню практичних питань і проблем роботи банківських електронних систем. Дано визначення безпеки банківських електронних систем у контексті сучасної банківської діяльності. Розкрито деякі аспекти даного процесу, на які слід звернути увагу вже зараз.

Ключевые слова: *электронна система, несанкционированный доступ, конфиденційність даних, антивирусные засоби, аутентыфикация.*

Keywords: *electronic systems, unauthorized division,confidentiality of information, antivirus facilities,authentification.*

Ключові слова: *електронна система, несанкціонований доступ, конфіденційність даних, антивірусні засоби, аутентифікація.*

Банківська діяльність досить насичена не тільки діловими відносинами, їй значною мірою притаманні тісні інформаційні відносини з партнерами. З іншого боку, будь-яке управлінське рішення банку базується на основі прийнятої інформації, і коштує тієї ж інформації. Витік інформації може завдати серйозної шкоди банку, його економічному становищу та іміджу, часто дозволяючи конкурентам зайняти провідні позиції на ринку, а іноді провокує і банкрутство банку.

Але безпека банківської електронної системи – це не тільки захист від крадіжок. Наприклад, відмова від обслуговування клієнта або несвоєчасне надання клієнту важливої інформації, що зберігається в системі, з причини непрацездатності цієї системи — за своїми наслідками рівноцінні втраті інформації. Таким чи-

ном, під час створення власних електронних систем безпеки банку треба приділяти велику увагу безпеці їх функціонування.

Значний внесок у дослідженні питань безпеки електронних систем банку внесли вчені СНД М. Вертузаєв, В. Шеломенцев, Ю. Батурін, В. Крилов, Ю. Ляпунов. Наукова розробка проблематики безпеки банківського бізнесу вітчизняними науковцями почалася зі здобуттям незалежності України. Зокрема, виділимо фундаментальні дослідження В. Задіраки, О. Олексюка, М. Недашковського [1], а також практичні розробки В. Міщенка та А. Шаповалова [2]. У той же час, загального розуміння проблеми безпеки банківських електронних систем у масштабах усієї банківської системи України вони не дають. У вітчизняній науковій літературі відсутні також дослідження підходів до побудови захисту банківських електронних систем, а класифікація погроз банківським електронним системам доволі схематична. Тому дослідження практичних аспектів безпеки банківських електронних систем є актуальними. Мета даної статті — обґрунтування необхідності захисту банківської інформації сучасними методами та інструментами, а також надання практичних рекомендацій щодо виконання задач підтримання конфіденційності та цілісності банківських електронних систем.

Банківська інформація може мати такий вигляд:

Рис. 1. Структура банківської інформації

Банківська інформація завжди була об’єктом уваги для різного роду злочинців, тому у наш час банки обладнані за останнім словом техніки. Але прогрес у техніці злочинів йшов не менш швидкими темпами, ніж розвиток банківських технологій. Особливо небезпечними для банків є так звані комп’ютерні злочини. Від-

критий характер комп'ютерних систем, що обслуговують велике число користувачів за допомогою засобів зв'язку в автоматичному режимі, поруч з високим ступенем концентрації та мобільності грошових коштів, сприяли появі комп'ютерної форми злочинності.

Особливості злочинів у банківській сфері такі:

1) більшість комп'ютерних злочинів є дрібними. Збитки від них становлять 10 000 — 50 000 дол. [2, с. 144];

2) комп'ютерні злочини, як правило, потребують великої кількості банківських операцій (до кількох сотень), але не завжди високотехнологічні;

3) багато шахраїв пояснюють свої дії тим, що вони начебто беруть позику в банку з наступним поверненням.

Оцінки збитків від злочинів, що пов'язані з втручанням у діяльність банківських електронних систем, дуже сильно розрізняються — від 150 млн дол. до 40 млрд дол. кожного року, причому зберігається стійка тенденція до зростання таких збитків.

Хоча процес автоматизації вітчизняних банків почався нещодавно, сумний досвід подібних злочинів вже є. Дії злочинців часто досягають мети у зв'язку з тим, що в переважній більшості банків України експлуатуються однотипні стандартні обчислювальні засоби (IBM-узгоджені персональні комп'ютери, локальні мережі з програмним забезпеченням фірми Novell), котрі добре відомі професіоналам. Проблеми створює і постійно зростаюча комп'ютерна грамотність клієнтів.

У плані захисту особливу увагу банки приділяють захисту великих ЕОМ, відновленню інформації після аварій і катастроф, захисту від комп'ютерних вірусів, захисту персональних ЕОМ.

До особливостей організації захисту мереж ЕОМ у банках можна віднести широке використання комерційного програмного забезпечення для управління доступом до мережі, захист точок підключення до систем через комутовані лінії зв'язку, використання антивірусних засобів, шифрування даних, що передаються. Велика увага приділяється захисту приміщень, у яких розміщені комп'ютери.

Ми поділяємо позицію [3], що система обробки інформації повинна враховувати такі особливості:

організаційну структуру банку;

обсяг і характер інформаційних потоків банку;

кількість і характер банківських операцій: аналітичних і щоденних;

кількість і функціональні обов'язки персоналу;
кількість клієнтів.

Наслідки недооцінки питань безпеки можуть виявитись катастрофічними для банків. Більшість коштів, якими користуються банки — це переважно гроші вкладників, якими банки користуються тільки тоді, коли їм довіряють. Таким чином, так важливо не підірвати довіру до банку.

Під безпекою банківської електронної системи слід розуміти її властивість, що виражається в здатності протидіяти спробам нанесення збитків власникам та користувачам системи при різних впливах (випадковим та спланованим) на неї. Природа впливу може бути різною: спроби проникнення злочинця, помилки персоналу, стихійні події (пожежа, буран), вихід із ладу окремих ресурсів.

У даний час склались два підходи до побудови захисту банківських електронних систем: фрагментарний — протидія суворо визначеним загрозам під час деяких умов (наприклад, спеціалізовані антивірусні засоби, автономні засоби шифрування та т. ін.) та комплексний підхід — створення захищеного середовища обробки інформації, що об'єднує різнорідні заходи протидії загрозам (правові, організаційні, програмно-технічні). Комплексний підхід застосовують для захисту великих систем (наприклад, СВІФТ) або локальних систем, що обробляють особливо цінну банківську інформацію.

Несанкціонований доступ (НСД) — найрозповсюдженіший вид комп'ютерних порушень. Він полягає в отриманні користувачем доступу до об'єкту, до якого у нього нема офіційного доступу згідно політики безпеки.

Загальна класифікація погроз банківським електронним системам має наступний вигляд:

1. Погрози конфіденційності даних та програм. Реалізуються під час несанкціонованого доступу до даних, програм або каналів зв'язку.

2. Погрози цілісності даних, програм, апаратури. Цілісність даних та програм порушується при несанкціонованій ліквідації, додатку зайвих елементів та модифікації даних, зміни порядку розташування даних, формуванні фальсифікованих платіжних документів у відповідь на законні запити, активної ретрансляції повідомлень з їх затримкою. Цілісність апаратури порушується під час її пошкодження, крадіжки або незаконному зміненні алгоритмів роботи.

3. Погрози доступності даних. Виникають у тому випадку, коли об'єкт (користувач або процес) не отримує доступу до законно

виділеним йому службам або ресурсам. Ця погроза реалізується захопленням всіх ресурсів, блокуванням ліній зв'язку несанкціонованим об'єктом, виключенням необхідної системної інформації. Ця погроза може призвести до ненадійності або поганої якості обслуговування в системі та, відповідно, потенційно буде впливати на достовірність та своєчасність доставки платіжних документів.

4. Погрози відмови від виконання транзакцій. Виникають, коли легальний користувач передає або приймає платіжні документи в системі, а потім відмовляється від своєї участі в них, щоби зняти з себе відповідальність.

За характером виконання зловмисних дій необхідно розділити на три види:

1) дії, не пов'язані з проникнення виконавців у приміщення, де розташовані комп'ютерні системи;

2) дії з одиничним проникненням виконавців у приміщення:

- відкриті — під виглядом відвідувачів, співробітників комунальних служб;
- негласні — у вихідні дні або вночі;

3) дії, що передбачають наявність виконавців серед співробітників банку, його клієнтів або постачальників обладнання.

Виходячи зі списку існуючих погроз можна виділити наступні основні напрямки захисту.

1. Захист апаратури та носіїв інформації від крадіжки, пошкодження та ліквідації. Для боротьби з погрозами цього виду використовується традиційний комплекс організаційно-технічних заходів: фізична охорона та обмеження доступу до апаратури, обладнання сигналізацією, а також пристроями, що перешкоджають крадіжкам комп'ютерної апаратури та її компонентів.

2. Захист інформаційних ресурсів від несанкціонованого використання. Для цього застосовуються засоби контролю включення живлення та завантаження програмного забезпечення, а також парольний захисту під час входу в систему.

3. Захист інформаційних ресурсів від несанкціонованого доступу. Забезпечує захист конфіденційності, цілісності і готовності (доступності) інформації та автоматизованих служб системи.

4. Захист інформації у каналах зв'язку та вузлах комутації. Блокує погрози, що пов'язані з пасивним підключенням до каналу («підслуховування»), попереджає активне підключення з фальсифікацією повідомлень або ретрансляцією справжніх повідом-

лень, а також перешкоджає блокуванню каналів зв'язку. Для захисту використовуються процедури аутентифікації абонентів та повідомлень, шифрування та спеціальні протоколи зв'язку.

5. Захист юридичної значимості електронних документів. Для захисту від таких погроз у практиці обміну фінансовими документами використовуються методи аутентифікації повідомлень при відсутності у сторін довіри одна до одної. Документ (повідомлення) доповнюється так званим цифровим підписом — спеціальною поміткою, що нерозривно логічно пов'язана з текстом.

6. Захист автоматизованих систем від вірусів та незаконної модифікації.

Розрізняють наступні класи технічних засобів захисту:

1) засоби фізичного захисту територій, будівель та приміщень інформаційних центрів;

2) пристрої, що попереджають крадіжку комп'ютерів, периферійного обладнання, їх вузлів та компонентів;

3) засоби захисту від виходу з ладу мережі електроживлення;

4) засоби зберігання магнітних носіїв;

5) апаратні та апаратно-програмні засоби управління доступом до персональних комп'ютерів, робочих станцій та пристроїв зв'язку;

6) засоби криптографічного захисту;

7) комбіновані пристрої та системи.

До програмних засобам захисту відносяться програми аутентифікації користувачів та розмежування їх прав на доступ до ресурсів системи, програми криптографічного перетворення, засоби контролю цілісності інформації, програми відновлення та резервного зберігання даних, а також програми сигналізації та спостереження за роботою механізмів захисту.

Програми захисту при значно меншій у порівнянні з апаратними засобами вартості часто забезпечують достатній рівень безпеки комерційних систем. Важлива перевага програмного підходу полягає у тому, що він дозволяє легко модифікувати систему захисту, змінюючи саму програму або її параметри. Вартість обслуговування програмних систем у порівнянні з апаратними надто незначна. Під час програмної реалізації захисту є можливість її поступового нарощування та ускладнення залежно від умов, що змінюються.

Для захисту від специфічних погроз, виникаючих під час передачі фінансових документів по зовнішніх (неконтрольованих) каналах зв'язку, використовуються криптографічні методи та спеціальні протоколи.

Крім загальних для всіх комп'ютерних систем задач підтримання конфіденційності та цілісності даних, у системах зв'язку треба вирішувати окрему задачу аутентифікації або взаємного встановлення справжності видалених абонентів. Наприклад, знаючи телефонний номер модему комп'ютерної системи, можна спробувати підключитися до неї, видаваючи себе за легального користувача. Звичайна практика полягає в тому, що комп'ютери автоматично набирають підряд телефонні номера та очікують відгуку віддалених комп'ютерів. Після визначення номеру модему вгадується або підбирається пароль доступу. Часто такий пароль тривіальний та знаходиться автоматично з допомогою комп'ютера, котрий використовує великий словник найімовірніших паролів.

У якості висновку зазначимо, що розвиток банківських технологій та загальний стан платіжної системи України вимагає якісно іншого рівня розвитку систем безпеки. Збільшуються обсяги електронних платежів, у цю сферу включаються все більше користувачів. З кількісним ростом підвищується уразливість системи, підвищується ризик здійснення економічних злочинів з використанням систем електронних платежів. Цьому сприяють незадовільна економічна ситуація в країні та наявність великої кількості висококваліфікованих кадрів, які тимчасово без роботи.

В Україні є висококваліфіковані спеціалісти та досвід у створенні потужних криптографічних технологій, але в даний час технічних засобів захисту потрібної якості та в необхідних кількостях тут не виробляється. Єдиним виходом із ситуації залишається залучення іноземних технологій. У перспективі вітчізняні засоби захисту повинні бути уніфіковані з іноземними, а рівень захищеності повинен відповідати світовим вимогам. Підсумовуючи, важливо наголосити, що організація захисту банківської інформації є важливою умовою розвитку сучасних банківських технологій, а системи безпеки нового покоління повинні враховути кращий світовий досвід і можливі потреби банківської сфери України в майбутньому. З огляду на це, методичні аспекти побудови захисту банківських електронних систем потребують переосмислення і подальшого розвитку економічною наукою в Україні.

Література

1. Методи захисту банківської інформації: Навчальний посібник / В. К. Задірака, О. С. Олексюк, М. О. Недашковський. — К.: Вища шк., 1999. — 144 с.

2. *Міщенко В. І., Шаповалов А. В., Юрчук Г. В.* Електронний бізнес на ринку фінансових послуг: Практич. посіб. — К.: «Знання», КОО, 2003. — 278 с.

3. *Чижов Н. А.* Клиентские технологии. — Минск: Амалфея, 2003. — 839 с.

4. *Лакосник Е.* Управление взаимоотношениями с клиентами в отделениях // Банк. практика за рубежом. — 2004. — № 3 (63). — С. 22—23.

Стаття надійшла до редакції 15.12. 2009 р.

УДК 336.051

Є. І. Волковський
аспірант кафедри фінансові ринки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

ТЕОРЕТИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ СУТНОСТІ ТА СКЛАДУ ФІНАНСОВОГО ПОТЕНЦІАЛУ МІСТА

В статье рассмотрены взгляды учёных на понимание сущности финансового потенциала, сформулировано авторское определение сущности финансового потенциала города, аргументированы составляющие финансового потенциала города.

The article describes the attitudes of scientists to understand the nature of the financial potential, formulated by the author's definition of the nature of the financial potential of the city and argued the components of the financial potential of the city.

У статті розглянуто погляди вчених на розуміння сутності фінансового потенціалу, сформульовано авторське визначення сутності фінансового потенціалу міста, аргументовано складові фінансового потенціалу міста.

Ключевые слова: *город, предприятия, финансовая политика, финансовый потенциал, финансовые ресурсы.*

Keywords: *city, business, financial policy, financial potential, financial resources*

Ключові слова: *місто, підприємства, фінансова політика, фінансовий потенціал, фінансові ресурси.*

Фінансовий потенціал є складним і багатогранним явищем, яке має надзвичайне суспільне та економічне значення. В умовах кризового стану економіки значення фінансового потенціалу та вміння його використовувати у максимально ефективній формі