Тетяна Стубайло, Інна Грод

Інформаційний захист банківських систем

В сучасному світі актуальною стала інформаційна безпека певної системи діяльності. Під інформаційною безпекою розуміють стан захищеності іформаційного середовища суспільства, який забезпечує формування цього середовища і розвиток в інтересах громадян, організацій і держави. Важливість цього питання зумовлена такими причинами, як новизна проблеми інформаційної безпеки; недостатній розвиток галузі сучасних інформаційних технологій в Україні; нечітке уявлення про роль та місце інформації в сучасному суспільстві. Відомо, що той хто володіє інформацією, володіє світом. Експерти вважають, що витік 20% комерційної інформації в шістдесяти випадках із ста приводить до банкрутства фірми.

Аналізуючи сучасний стан проблеми захисту діяльності комерційних підприємств, зручно вибирати такий об`єкт, в якому зосереджені всі основні проблеми в цій області. Зараз таким об`єктом є банківська система. Банк – найбільш розгалужене підприємство, яке акумулює значні фінансові засоби і тому притягає до себе увагу зловмисників.

При використанні обчислювальних сіток відносно нескладно ввійти в бази даних банків, зчитувати або змінювати їх зміст, підробляти перекази коштів тощо. Але найгіршим є порушення адекватного функціонування обчислювальної системи, тобто повне або часткове знищення інформації. Тут виникає багато проблемних питань. А саме: як відновити таку інформацію, за який час і яким методом, як проконтролювати повноту відновлення? Стан боротьби з комп'терною злочинністю на теперішній час потребує вдосконалення. Він зумовлений:

- недосконалістю законодавства, яке передбачає адміністративну, громадську, матеріальну і кримінальну відповідальність за комп`ютерні порушення ;
- відсутністю в системі правоохоронних органів, органів суду і прокуратури спеціально підготовленого штату фахівців, здатних виявляти, попереджувати і знешкоджувати комп`ютерну злочинність;
- відсутністю обліку правопорушень, які здійснюються з використанням засобів інформатизації;
- відсутністю необхідного технічного і методичного інструментарію і досвіду виявлення і попередження даного роду правопорушень;
- низьким рівнем інформаційної і правової культури суспільства .

За міжнародною практикою стосовно безпеки об'єктами захисту з урахуванням їх пріоритету є: людина, інформація, матеріальні цінності. Якщо пріоритет збереження безпеки людей можна вважати звичайним, то пріоритет банківської інформації про матеріальні цінності вимагає уточнення. Це стосується не тільки інформації, яка складає державну або комерційну таємницю, але й відкритої інформації і зумовлена тим, що вона стає доступною протягом її обробки засобами обчислювальної техніки. В крайньому випадку її знищення може привести до банкрутства банку.

Комерційна безпека діяльності банків включає в себе: фізичну безпеку, під якою розуміється забезпечення захисту від посягання на життя персоналу і клієнтів банку; економічну безпеку банку; інформаційну безпеку банку; матеріальну безпеку банку, тобто збереження матеріальних цінностей від непередбачених випадків-пожеж, крадіжок.

Стан в українській банківській сфері ускладнюється тим, що здійснюється поступове об'єднання українського і зарубіжного злочинного світу. Прогнози на найближче майбутнє передбачають появу нових і посилення суспільно небезпечних форм злочинної діяльності в сфері кредитно-грошових відносин (махінації з векселями, кредитними картками, незаконна емісія цінних паперів тощо). Можна виділити основні чинники, що впливають на економічну безпеку банку:

- погана адаптованість існуючої банківської системи в умовах ринку;
- недостатня платіжна спроможність;
- неповернення позик;
- втрата засобів за операціями з фальшивими документами;
- псевдопідприємництво;
- шахрайство.

Наявність вказаних чинників зумовлена такими видами ризику:

- ризик витоку, знищення або модифікації банківської інформації;
- ризик відсутності у керівництва банку об'єктивної інформації;
- ризик розповсюдження конкурентами необ'єктивної або небезпечної для банку інформації.

Арсенал прийому банківського шпигунства включає і несанкціоноване використання засобів обчислювальної техніки. Сотні фірм спеціалізуються на виготовленні засобів технічної розвідки і проведення заходів із промислового шпигунства. Засоби і методи промислового шпигунства використовують або недобросовісні конкуренти або мафіозні структури. Протидіяти викраденню інформації за допомогою технічних засобів розвідки досить складно і під силу лише досвідченим спеціалістам.

Засоби промислового шпигунства дозволяють не тільки підслуховувати або підглядати за діями конкурентів, але і отримувати інформацію, яка опрацьовується засобами обчислювальної техніки. Щоденним явищем стало, наприклад, зняття інформації з дисплеїв або з ліній сіток зв'язку ЕОМ.

Комерційні обчислювальні сітки, які широко використовуються, не зовсім забезпечують надійний захист інформації. При цьому злочинці можуть отримати доступ до відкритої інформації, до інформації, яка містить комерційну таємницю. В результаті банк або фірма терплять збитки або фінансовий крах.

Протидіяти комп'ютерній злочинності важко, що, головним чином пояснюється:

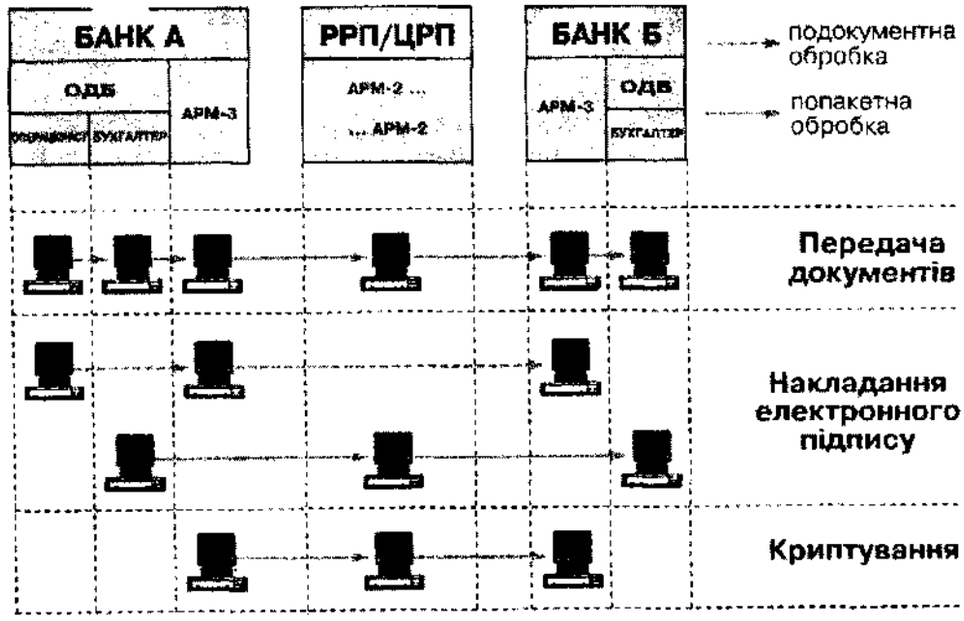
- новизною і складністю проблеми;
- складністю своєчасного виявлення комп'ютерної злочинності і ідентифікації зловмисників;
- можливістю вдосконалення злочинів із використанням засобів віддаленого доступу (коли злочинців немає на місці злочину);
- труднощами збору і юридичним оформленням доказів комп'ютерного злочину.

Політична орієнтація України на формування вільної ринкової економіки призвела на початку 90-х років до істотних змін у банківській сфері країни. Комерціалізація державних банків, поява мережі комерційних банків, збільшення кількості суб'єктів підприємницької діяльності сприяли зростанню суспільної зацікавленості в автоматизованій системі, яка прискорила б міжбанківські розрахунки та підвищила б їхню надійність і безпеку. Кожний день зволікання створення системи призводив до значних збитків держави та підприємців внаслідок прискорення темпів інфляції та фінансових втрат від використання підроблених платіжних документів. Адже розлад платіжної системи тієї чи іншої країни часто є одним із найперших і безпосередніх проявів зародження фінансової кризи.

Розуміючи важливість цієї проблеми, Національний банк України у1992 році розробив концепцію грошового обігу в Україні, яка була розглянута банками України і затверджена правлінням НБУ.

У повному обсязі система електронного платежу (СЕП) почала діяти з 1 січня 1994 року. Практично всі банківські установи України були підключені до системи, що зробило її загальнодержавною електронною платіжною системою. Запровадження СЕП дало змогу наблизитись до світового рівня обробки інформації у сфері міжбанківських розрахунків, значно підвищити їхню надійність, виключити ризик виготовлення фальшивих авізо та скоротити термін проходження платежів від трьох-чотирьох тижнів до кількох годин. Скорочення терміну проходження платежу сприяло зменшенню готівки в обігу, дозволило банкам ефективніше використовувати свої ресурси, а клієнтам – свої кошти. НБУ отримав інструмент контролювання та регулювання грошового обігу, що має особливе значення у перехідний період, прискорилися надходження до державного бюджету.

Протягом всього часу функціонування СЕП ведеться робота стосовно підвищення безпеки міжбанківських розрахунків, програмних та бухгалтерських засобів контролю за виконанням розрахунків, удосконалення існуючих та впровадження апаратних засобів захисту. Так, з червня 1994 року розпочалося впровадження апаратних засобів криптозахисту інформації. Нині всі банки перейшли на роботу з криптограмами, при цьому програмний засіб захисту залишився лише як резерв на випадок виходу з ладу апаратного. З метою подальшого підвищення безпеки розрахунків з початку 1996 року запроваджено нові програмні засоби захисту, «електронний цифровий підпис», які запобігають викривленню та підробці електронних платіжних документів на всіх етапах їх обробки та транспортування як у самому банку, так і по всій мережі СЕП. Суть цієї технології полягає у тому, що ні в одному пункті проходження платежу немає повного набору ключів, який би дав можливість викривити інформацію СЕП. Таким чином забезпечується контроль платежів як у самому банку, так і у мережі розрахункових палат НБУ (див. мал.).



Сьогодні система має багаторівневий (до 10 рівнів) захист від несанкціонованого втручання. Система захисту банківської інформації включає:

- бухгалтерську балансову модель щоденних оборотів та контроль за станом кореспондентських рахунків;
- організаційні заходи із обмеження доступу до інформації в системі, виконання режимних умов у кожній банківській установі;
- багаторівневу систему програмного контролю руху платіжних документів на усіх ланках оброблення та транспортування платежів;
- комплекс заходів по криптографуванню та ключову систему до них;
- апаратні засоби захисту грошового обігу.

Таким чином, забезпечення комерційної діяльності банку охоплює не тільки захист інформації, але й збір, класифікацію, аналіз, оцінку і видачу прогнозів для успішної комерційної діяльності. Інформаційна і економічна безпека фірми або банку тісно пов`язані між собою.

Про необхідність удосконалення захисту банківської інформації і телекомунікаційних систем свідчить число факторів незаконного володіння фінансовою інформацією, яке зростає. Удо-

сконалення стало можливим завдяки використанню новітніх засобів захисту комп`ютерної і телекомунікаційної сітки.

Література

1. Справочник финансиста. Под редакцией Уткина Є.А. Москва,1998. Ассоциация «ТАНДЕМ». 2. Финансовое состояние предприятия. Крейнина М.Н. Москва, 1997. ИПС «ДИС». 3.Информатика и образование. № 4-№ 6. 1999. 4. Компьютеры и программы. №2. 2000.

Анотація

Комерціалізація державних банків, поява мережі комерційних банків, збільшення кількості суб`єктів підприємницької діяльності сприяли зростанню суспільної зацікавленості в автоматизованій системі, яка прискорила б міжбанківські розрахунки та підвищила б їх надійність і безпеку. Запроваджуються нові програмні засоби захисту, які запобігають викривленню та підробці електронних платіжних документів на всіх етапах їх обробки та транспортування.

Аннотация

Коммерциализация государственных банков, возникновение сети коммерческих банков, увеличение количества субьектов предпринимательской деятельности воздействовали увеличению общественной заинтересованности в автоматизированной системе, которая ускорила бы расчеты между банками и подняла бы их надежность и безопасность. Вводятся новые программные обеспечения защиты, которые не допускают искривления и подделки электронных платежных документов на всех этапах их обработки и транспортировки.

Annotation

Origin of a web of commercial banks, magnification of an amount of the subjects of enterprise activity effected to magnification of public interest in the automized system, which would speed up calculations between banks and would lift their reliability and safety. The new softwares of a guard are inlet which do not suppose warpages and fakes of the electronic payment documents at all stages of their handling and transportation.