УДК 336.717.3(477)

Островська Н. С.
Якуб'як І. М.

ОСНОВНІ АСПЕКТИ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ БЕЗПЕКИ КОМЕРЦІЙНИХ БАНКІВ УКРАЇНИ ТА ЇХ ВПЛИВ НА СПРОМОЖНІСТЬ ВИКОНУВАТИ НИМИ СВОЮ МІСІЮ

Анотація. Банківська безпека – один із основних елементів банківського менеджменту. Інформаційна та організаційно-технічна безпека комерційних банків на сучасному етапі займає центральне місце в загальній безпеці комерційних банків. Питання актуальності цієї теми наукової статті полягає в тенденційному розвитку новітніх інформаційних технологій та їхнє двозначне використання як для здійснення комерційними банками своєї діяльності, так і порушення такої діяльності третіми особами. Для забезпечення інформаційної безпеки діяльності банки використовують усі законні методи у сфері інформаційних технологій.

Ключові слова: інформаційний канал, інформаційна загроза, несанкціонований доступ.

Вступ. Сучасний світ неможливо уявити без інформаційних технологій, а саме технологій зв'язку та передачі даних. Новинки науково-технічного прогресу поглинули всі сфери діяльності людини, що дає змогу спрощувати роботу людини при вирішенні певних завдань та при виконанні певних видів робіт.

До одних із таких сфер відноситься і банківська діяльність. Саме в банківській діяльності на сучасному етапі розвитку інформаційні технології становлять основу функціонування будь-якого комерційного банку. Звідси питання безпеки таких інформаційних каналів передачі даних стоїть на одному з перших місць забезпечення загальної безпеки комерційного банку як фінансово-кредитного інституту.

Сьогодні банки вживають низку заходів, що дають змогу їм протистояти несанкціонованим доступам, розголошенню комерційної інформації і притягати правопорушників до відповідальності.

Питання досить актуальне з огляду на зростаючу динаміку злочинів щодо посягань та використання з корисливою метою третіми особами банківської інформації.

Україна як споживач новітніх розробок програмного забезпечення для банків тісно співпрацює в цій сфері з Російською Федерацією, оскільки функціональність російських банків майже ідентична українським банкам.

Цю проблематику досліджують такі вчені, як М. І. Зубок, І. П. Козаченко, В. О. Голубєв, Д. Й. Никифорак, О. І. Шостенко та ін.

Постановка завдання. Мета написання цієї роботи – дослідження інформаційно-технічної безпеки банків і висвітлення основних тенденційних змін у системах інформаційного убезпечення банківської інформації, а також необхідності їхнього вдосконалення в сучасних умовах розвитку інформаційних технологій. Вирішення обраного науково-практичного завдання базується на загальнонаукових принципах проведення комплексних наукових досліджень. У процесі роботи, залежно від конкретних цілей і завдань, використовувались різні методи, серед яких метод логічного синтезу щодо можливості практичного виникнення недоліків захисту інформаційних систем банків. Під час дослідження стану інформаційної

захищеності комерційних банків використані формалізовані методи порівняння та поелементного аналізу, а також метод ситуаційного моделювання.

Результати. Банківська безпека – один з основних елементів банківського менеджменту, має багатофункціональний і комплексний характер. Інформаційна та організаційно-технічна безпека – це одна зі складових загальної банківської безпеки.

Найнебезпечніша для банків інформаційна незахищеність, тому при розв'язанні цієї проблеми банку необхідно враховувати те, що одна з головних умов стабільного функціонування кожного банку – обмін інформацією.

Тобто в основу інформаційної безпеки має бути покладено заходи щодо захисту інформації в засобах і мережах її передавання й обробки, а також створення відповідної нормативної бази, яка б регулювала порядок доступу, зберігання і використання інформації фірми, банку, підприємства.

В основу організації режиму захисту банківської інформації покладено положення таких законодавчих актів:

1. Закону України «Про банки і банківську діяльність» (ст. 52 «Банківська таємниця») [1].
2. Закону України «Про інформацію» (ст. 30 «Інформація з обмеженим доступом»).
3. Закон України «Про захист інформації в автоматизованих системах» та ін.

Відповідно до статей цих законів склад банківської інформації можна розглядати так, як указано на рис. 1 [2].

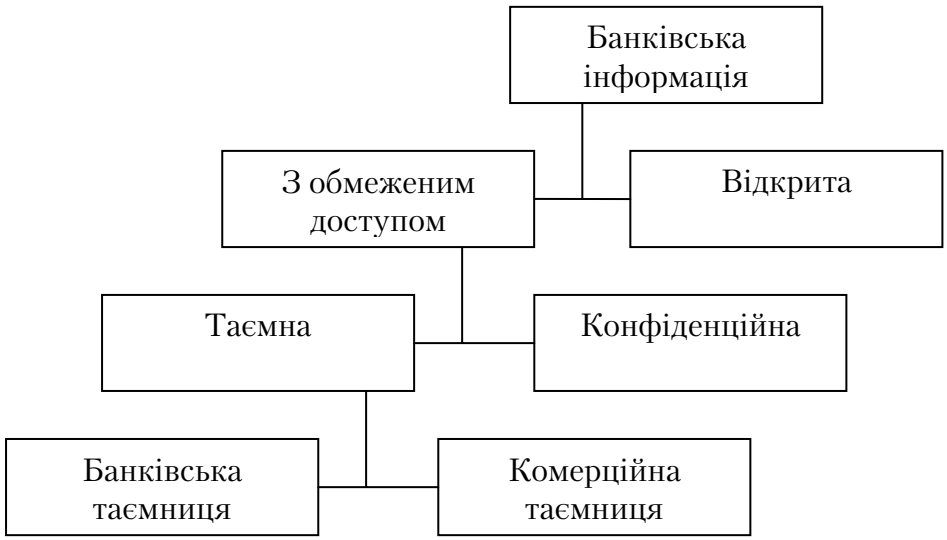

Рис. 1. Режим захисту банківської інформації

Погіршення стану інформаційної безпеки комерційного банку може бути спричинене дією таких чинників:

1) збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерів;

2) зосередження в базах даних інформації різного призначення і різної приналежності;

3) розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та масивів даних;

4) ускладнення режимів роботи технічних засобів обчислювальних систем;

5) обмін інформацією в локальних та глобальних мережах, у тому числі на великих відстанях.

У всіх аспектах забезпечення захисту інформації основний елемент – аналіз можливих дій щодо порушення роботи банківських автоматизованих систем.

Під цими діями розумітимемо такі, що підвищують уразливість інформації, яка обробляється в автоматизованій системі, приводять до її просочення, випадкової або навмисної зміни чи знищення.

Випадкові загрози включають у себе помилки, пропуски тощо, а також події, що не залежать від людини, наприклад природні або спричинені діяльністю людини катаклізми. Заходи захисту від них в основному організаційні.

До помилок апаратних і програмних засобів відносяться пошкодження комп'ютерів і периферійних пристроїв (магнітних носіїв тощо), помилки в прикладних програмах. До помилок через неуважність, які досить часто виникають під час технологічного циклу обробки, передачі або зберігання даних, відносяться помилки користувача, оператора або програміста, втручання під час виконання програм, пошкодження носіїв інформації та ін. Навмисні загрози можуть реалізовуватися учасниками процесу обробки інформації (внутрішні) і «хакерами» (зовнішні).

Дослідження показують, що безпосередній несанкціонований доступ до ЕОМ, систем та комп'ютерних мереж мають співробітники банків: програмісти, інженери, оператори, які є користувачами або обслуговуючим персоналом ЕОМ (41,9 %). Майже вдвічі менший такий доступ мають інші співробітники банку (20,2 %), а у 8,6 % випадків злочин було вчинено співробітниками, що були звільнені, 25,5 % – несанкціонований доступ учинений сторонньою особою [6].

Найпоширенішими видами навмисних загроз сьогодення виступають такі за частотою прояву:

– копіювання і крадіжка програмного забезпечення;
– несанкціоноване введення даних;
– зміна або знищення даних на магнітних носіях;
– саботаж;
– крадіжка інформації;
– несанкціоноване використання ресурсів комп'ютерів;
– несанкціоноване використання банківських автоматизованих систем;
– несанкціонований доступ до інформації високого рівня секретності [4].

Основне завдання банківської інформаційної безпеки – забезпечення умов унеможливлення незаконного або недобросовісного витоку комерційної інформації та її використання в злочинних чи протиправних діях [3].

Розголошення інформації виявляється в умисному або необережному її повідомленні, опублікуванні, оголошенні, переданні, наданні для ознайомлення, пересиланні, втраті особами, яким така інформація була відома у зв'язку з їхньою професійною діяльністю і коли в цьому не було службової необхідності.

Несанкціонований доступ до інформації тут розуміється як доступ до інформації, який здійснюється з порушенням установлених правил розмежування доступу.

Усі зазначені вище шляхи отримання інформації можуть використовуватись конкурентами, промисловими шпигунами, спецслужбами за допомогою створення так званих каналів витоку й передавання інформації. У свою чергу, ці канали передбачають створення відповідних умов для переходу інформації від її носія до споживача. Відомо, що взагалі інформація переноситься або передається енергією чи матеріальними носіями. У фізичній природі можливі такі шляхи перенесення інформації: світлові промені, звукові хвилі, електромагнітні хвилі, матеріали і ре-

човини. Використовуючи ті чи інші фізичні поля, створюють відповідні системи передавання інформації, які складаються з джерел інформації, передавачів, каналу передавання, приймачів та отримувачів інформації. Подібне існує в разі передання інформації та у взаєминах людей. Носії інформації (джерела) через «передавачі», а в деяких випадках і «приймачі» передають її отримувачам. Джерелами інформації можуть бути люди, документи, публікації, технічні засоби забезпечення виробничої діяльності, продукція, промислові та виробничі відходи [5].

Як у разі мимовільного витоку інформації, так і за несанкціонованого доступу використовуються відповідні канали отримання інформації: візуально-оптичні (спостереження, відео-, фотозйомка), акустичні та акустоперероблювальні, електромагнітні (у тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії і т. д.).

Поряд із неправомірним отриманням інформації існують і інші загрози, які не передбачають отримання інформації, але, у свою чергу, не менш небезпечні. Серед них знищення і модифікація (зміна змісту) інформації. Слід зазначити, що до факторів, які створюють умови витоку (передавання) інформації, за дослідженнями спецслужб, відносять відображені в табл. 1 [5].

Таблиця 1

Фактори	%
Надмірна балакучість співробітників підприємств, фірм, банків	32
Прагнення працівників підприємств, фірм, банків заробити гроші будь-яким способом і будь-якою ціною	24
Відсутність на підприємстві, фірмі, у банку системи заходів, спрямованих на захист інформації	14
Звичка співробітників підприємств, фірм, банків ділитись один з одним почутими новинами, чутками, інформацією	12
Безконтрольне використання інформаційних систем	10
Наявність передумов для виникнення серед співробітників конфліктних ситуацій	8

На підставі викладеного можна зробити висновок, що отримання інформації спецслужбами, конкурентами та зловмисниками здебільшого здійснюється через технічні засоби, які використовуються на фірмах, підприємствах, у банках та через їхніх співробітників.

Для оцінки захищеності банківських інформаційних мереж проводиться обстеження, яке можна умовно розділити на такі етапи:

– збір інформації про мережу (наприклад, визначення типу операційної системи атакуючих хостів);

– визначення загроз інформації й уразливих місць;

– проникнення в мережу;

– оцінка ризику, зв'язаного зі знайденими уразливими місцями і можливістю їхнього використання для одержання несанкціонованого доступу до мережі;

– розробка рекомендацій із формування системи захисту інформації і відповідної політики безпеки;

– за узгодженням із керівництвом банку пропонується таке впровадження, настроювання і гарантійний супровід комплексної системи захисту інформації (мережних і обчислювальних ресурсів).

У випадку неможливості такого обстеження як альтернативу можна запропонувати скористатися спеціалізованим програмним забезпеченням, призначеним для пошуку відомих уразливих місць мережних сервісів і некоректних параметрів конфігурації операційної системи. У процесі аналізу захищеності розглядаються конкретні елементи інформаційної системи, що вимагають захисту й уходять у політику безпеки, прийняту в банку, відповідно до важливості (ранжирування) оброблюваної, збереженої і переданої інформації, а також безпосередньо інтегровані з глобальною мережею Internet.

Сьогодні банки використовують спеціальні програмні комплекси зі сканування рівня інформаційної захищеності комп'ютерних мереж. Серед таких комплексів виступають спеціалізована мова Vulnerability Description Language, Internet SafeSuit (Internet Security Systems) та ін.

Для контролю за виходом банківської інформації через «зломи» інформаційних мереж комп'ютерними злочинцями використовують відповідне програмне забезпечення.

Нині на ринку представлена достатня кількість програмного забезпечення, що відноситься до категорії засобів пошуку «злому» мереж. Це:

1. Internet Security Scanner (фірма Internet Security Systems).
2. NetRecon (фірма Axent).
3. NetProbe (фірма Qualix).
4. Ballista (фірма Secure Networks).
5. NetGuard (фірма Network Guardians).
6. NetSonar (фірма WheelGroup).

Комерційні банки України виступають переважно споживачами спеціального банківського програмного забезпечення іноземного виробництва, зокрема виробництва Росії:

– комплексну безпеку корпоративних мереж забезпечують програмні продукти VPN ЗАСТАВА 3.3, створені компанією «ЭЛВИС-ПЛЮС»;

– криптографічний захист «Крипто Про CSP», розроблена компанією «Крипто Про», допомагає ефективно перевіряти електронний цифровий підпис;

– фінансову безпеку кредиторів забезпечує система A2 AGRUS APPLICATION, створена компанією «Агрус MGS»;

– комплекс «Банк-Доступ» забезпечує централізоване керування, розподіляючи доступ до інформаційних ресурсів;

– комплекс «Банк – Активний Захист», розроблений фірмою «Андек», використовують для ліквідації наслідків атак хакерів, якщо їм усе-таки удалося прорвати інформаційний захист.

Висновки. Сукупність зазначених аспектів формування та підтримки інформаційної безпеки комерційних банків дасть змогу практично ідентифікувати можливі існуючі загрози та оперативно їх усунути без негативних наслідків для сучасних комерційних банків України. З погляду на обсяги завданих збитків комерційним банкам слід зазначити, що врахування вказаних способів убезпечення

інформаційних ресурсів – сьогодні найдоцільніший альтернативний варіант, що дасть змогу ефективно виявляти та відповідно карати порушників.

Література

1. Закон України «Про банки і банківську діяльність» від 17.01.2001 // Відомості Верховної Ради України. – 2001. – № 4.
2. Закон України «Про інформацію» // Ст. 30 «Інформація з обмеженим доступом».
3. Козаченко І. П. Загальні принципи захисту інформації в банківських автоматизованих системах / І. П. Козаченко, В. О. Голубєв // http://bezpeka.com/.
4. Никифорак Д. Й. Виявлення злочинів у банківській системі України / Д. Й. Никифорак, О. І. Костенко // www.naiau.kiev.ua
5. Зубок М. І. Безпека банківської діяльності: навч. посіб. / М. І. Зубок. — К. : КНЕУ, 2002. — 190 с.
6. Матеріали «Центру дослідження комп'ютерної злочинності», www.crime-research.org.

Summary. Bank safety is one of the basic elements of bank management. The one of compound of bank safety is information that organizational-technical safety. In bank activity wide applications of computer facilities and means of information interchange extend opportunities of its impregnation and not authorized access to it with the criminal purpose. Banks use all accessible methods of prevention to such phenomena.

Keywords: informative channel, informative threat unauthorized division.