**6. Інформаційна безпека банківських установ**

**Мета** – розглянути теоретичні засади та практичні аспекти органі­зації інформаційної безпеки банківських установ.

**Ключові поняття:**  банківська таємниця, інформаційна безпека, захист банківських таємниць, канали розповсюдження інформації.

**Основні питання:**

61. Сутність інформаційної безпеки банку.

6.2. Неправомірне розголошення інформації і захист від нього.

6.3. Правове регулювання захисту таємниць банків.

6.4. Нормативна база банку із забезпечення інформаційної безпеки.

***Література:*** [13; 17; 24; 28; 29].

**6.1. Сутність інформаційної безпеки банку**

*Інформаційна безпека банку* – стан захищеності та збережності інформаційних ресурсів банку, за якого забезпечується необхідний рівень інформованості керівництва, персоналу банку та контрагентів, а також недопущення неправомірного доступу до інформації.

Інформаційна безпека має виключати будь-який несанкціонований доступ до інформації. Згідно з СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» вона має забезпечувати збереження конфіденційності, цілісності і доступності інформації. Можуть врахо­вуватися інші властивості, а саме: автентичність, відстежуваність, неспростовність та надійність. Для банків України відстежуваність, неспростовність, надійність та автентифікація користувачів та інформаційних ресурсів є обов’язковими вимогами інформаційної безпеки [29].

Інформаційна безпека в практичному аспекті означає комплекс засобів, застосування яких дозволяє забезпечити належний доступ до інформації та її захист від витоку і неправомірного використання в шахрайських цілях шпигунами або недобросовісними конкурентами.

Об’єкти інформаційної безпеки – це ресурси, засоби чи програмне забезпечення, на яке спрямовані дії суб’єктів безпеки. Їх перелік показано на рис. 6.1.

Об’єкти інформаційної безпеки банку

Комп’ютерне обладнання

інформаційні бази, файли, документи

Програмне забезпечення

Обслуговуюча та підтримуюча комп’ютерне обладнання інфраструктура (енергопостачання, умови експлуатації)

Рис. 6.1. **Об’єкти інформаційної безпеки банку**

*Принципи інформаційної безпеки банківських установ*:

1) оперативність – cвоєчасність реагування банку на загрози інфор­маційній безпеці банку, на проблеми, що можуть спричинити несанк­ціонований доступ до інформації;

2) ефективність – розроблені заходи щодо забезпечення інфор­маційної безпеки повинні виконуватися з мінімальними витратами в мінімальний проміжок часу;

3) адекватність – означає розробку і впровадження заходів захисту, адекватних характеру виявлених загроз, з урахуванням витрат на їх реалізацію і сумісності цих заходів з діючим банківським технологічним процесом. Ці заходи не повинні вступати в протиріччя зі стратегічними цілями банку;

4) безперервність – постійний і всебічний аналіз інформаційної сис­те­ми з метою виявлення уразливості інформаційних активів банківської установи;

5) контрольованість – всі операції з доступом до банківської інформації повинні носити контрольований характер;

6) персоніфікація – означає розподіл ролей і відповідальності між користувачами інформаційної системи банку, виходячи з принципу персональної і одноосібної відповідальності за здійснені операції;

7) принцип багаторазової перевірки – критичні операції та дії здійснюються або підтверджуються мінімум двома уповноваженими особами;

8) обізнаність – означає знання банківським персоналом клієнтів своїх відділів та колег по роботі, що виключить доступ до інформації сторонніх осіб.

*Фактори ризику, що створюють загрози інформаційній безпеці банку:*

недотримання банківської таємниці банківським персоналом;

прагнення персоналу заробити додаткові гроші;

ненадійна система захисту банківської інформації;

незадоволеність персоналу роботою в банку;

звичка персоналу ділитися чутками, плітками, здогадками;

конфліктні ситуації;

безконтрольний доступ до банківської інформації.

*Загрози інформаційній безпеці банківської установи* включають:

саботаж;

крадіжку програмного забезпечення та інформаційних ресурсів;

шахрайські дії;

несанкціонований доступ до інформаційної системи банку;

розголошення комерційних таємниць банку;

знищення інформації;

підміну інформації, її викривлення;

знищення або викрадення носіїв банківської інформації;

організація збоїв у функціонуванні банківської інформаційної сис­теми.

**6.2. Неправомірне розголошення інформації і захист від нього**

Витік інформації (неправомірне отримання інформації) – це мимовільне або несанкціоноване розголошення або знищення інформації шляхом втручання в інформаційні системи, копіювання, перекручування інформації, знищення електронних та паперових носіїв.

Несанкціонований доступ до інформації – це доступ до інформації, який здійснюється з порушенням установлених правил розмежування доступу.

Способи витоку інформації наведено в табл. 6.1.

Ці способи мають різне походження, як із внутрішнього, так із зовнішнього середовищ.

Таблиця 6.1

**Способи витоку інформації в банківській системі**

|  |  |
| --- | --- |
| Способи витоку інформації | Характеристика |
| Мимовільне поширення інформації банку | Здійснюється за рахунок технічних або експлуатаційних особливостей певного обладнання |
| Втрати, пошко­дження, знищення документальних та програмних носіїв інформації банку | Відбувається в результаті дії стихійного лиха, несанкціонованого втручання конкурентів, промислових шпигунів, потрапляння в інформаційні мережі банку комп’ютерних вірусів |
| Розголошення інформації | Виявляється в умисному або необережному повідомленні інформації, опублікуванні, оголошенні, переданні, наданні для ознайомлення, пересиланні, втраті особами, яким така інформація була відома у зв’язку з їх професійною діяльністю і коли у цьому не було службової необхідності |
| Втручання у роботу інформаційної системи банку | Будь-які зловмисні дії, що впливають на обробку, зберігання, введення, записування, перетворення, зчитування, зберіган­­ня інформації, що здійснюються за допомогою технічних і програмних засобів, включаючи обмін через канали передачі даних у банківській мережі |
| Знищення інформації | Втрата інформації, коли вона перестає існувати для банку, який має право власності на неї в повному чи обмеженому обсязі. Як знищення, втрату інформації треба розглядати і її блокування, тобто припинення доступу до інформації користувачам (персоналу банківської установи) |
| Перекручення інформації | Зміна змісту банківської інформації, порушення її цілісності, в тому числі і часткове знищення |
| Переривання інформаційних процесів | Припинення нормальної обробки банківської інформації, наприклад, внаслідок руйнування обчислювальних засобів. Воно може мати серйозні наслідки навіть у тому випадку, коли сама інформація ніяких впливів не зазнає |
| Руйнування інформації | Безповоротна зміна банківської інформації, наприклад, стирання даних з диска |
| Крадіжка інформації | Читання або копіювання банківської інформації з метою отримання даних, які можуть бути використані або зловмисником, або третьою стороною |
| Пошкодження інформації | Зміна інформації із застосуванням вірусних вредоносних програм, що робить неможливим користування цією інформацією персоналом банку |

Найчастіше несанкціонований доступ здійснюється щодо такої інформації:

платіжні документи;

внутрішні платіжні документи;

кредитні документи;

документи на грошові перекази;

персональні дані клієнтів та працівників банку;

статистичні звіти;

інші документи, які містять інформацію з обмеженим

доступом.

Отримувачами цієї конфіденційної інформації

спецслужби конкурентів;

кримінальні елементи;

ЗМІ;

різні інформаційні, детективні агентства;

промислові шпигуни.

Передавачами та приймачами виступають різноманітні технічні засоби, тайники, кур’єри, зв’язківці.

Джерела інформації: люди, документи, публікації, технічні засоби забезпечення виробничої діяльності, продукція, промислові та виробничі відходи.

Причинами виникнення загроз інформаційній безпеці є: 1) низький рівень підготовки персоналу і відсутність можливості підвищення кВа­ліфікації; 2) відсутність програми забезпечення інформаційної без­пеки банку; 3) відсутність плану нейтралізації інформаційних загроз; 4) низька якість програмного забезпечення та комп’ютерної техніки; 5) неправиль­на інтеграція даних у нові інформаційні системи; 6) введення непра­вдивих даних клієнтами; 7) помилки, що допускаються персоналом у ході вводу інформації.

Існує багато каналів витоку інформації: акустичні та акустопере­роблювальні, електромагнітні (у тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії і т. д.).

Ці канали передачі інформації використовуються як при мимовільному витоку інформації, так і під час зумисного розголосу.

Характеристики каналів витоку інформації та природи їх створення знайшли відображення в табл. 6.2, складеній на основі опрацювання джерела [13].

Таблиця 6.2

**Характеристики каналів витоку банківської інформації**

|  |  |  |
| --- | --- | --- |
| Канали витоку інформації | Природа створення | Характеристика |
| Візуально-оптичні канали | Створюється через оптичний шлях від об’єкта інформації (банку) до її отримувача. Ство­ренню зазначених каналів спри­яють такі характеристики об’єкта інформації: відповідні його розмі­ри, власна яскравість і конт­раст­ність | Цінність інформації, отриманої через такий канал, полягає в тому, що вона є максимально достовірною, оперативною і може служити документальним підтвердженням отриманих да­них |
| Акустичні канали | Створюються: за рахунок поши­рення акустичних коливань у вільному просторі (переговори на відкритому прос­торі, при відкритих вікнах, две­рях, венти­ляційних каналах); за рахунок впливу звукових коли­вань на елементи і конструкції будівель банку, викликаючи їх вібра­цію; за ра­хунок дії звукових коливань на технічні засоби обробки інфор­мації (мікрофонний ефект, акус­тична модуляція) | Інформація передається через тіла та механізми, які здійсню­ють вібрацію, або коливання, такі як голосові зв’язки людини, елементи машин, що руха­ються, телефонні апарати, зву­копідсилювальні системи, гуч­номовні засоби, засоби звуко­запису та звуковідновлення |
| Електромагнітні канали | Створюються через наявність у технічних засобах, які використо­вуються банком, джерел небез­печних сигналів, які створюють електромагнітні канали витоку (передання) банківської інформації | За своєю фізичною природою та експлуатаційними особли­во­стями технічних засобів елект­ромагнітні канали є найбільш небезпечними і досить поши­реними каналами отримання інформації. Використання тех.­нічних засобів обробки та пере­дання інформації створює за­грозу її безконтрольного витоку |
| Матеріально-речові канали | Створюються через вивчення зі­псованих банківських документів або їх фраг­ментів, чернеток, різного роду поміток, записів, листів) | Робота каналів пов’язана з ви­краденням, несанкціонованим ознайомленням, копіюванням, фотографуванням, відеозапи­сом банківських документів, зразків програмних засобів |

Заходи захисту інформації в засобах і мережах передачі інформації включають:

апаратні;

програмні;

криптографічні.

Крім того, існують фізичні, законодавчі і профілактичні заходи.

Загальна характеристика засобів захисту наведена в табл. 6.3.

Таблиця 6.3

**Характеристика засобів захисту банківської інформації**

|  |  |
| --- | --- |
| Засоби захисту | Характеристика |
| 1 | 2 |
| 1. Апаратні | Призначення: перешкоджання візуальному спостереженню і дистанційному підслуховуванню; нейтралізація паразитних електромагнітних випромінювань і наводок; виявлення техніч­них засобів підслуховування і магнітного запису, несанкціо­новано встановлених або таких, які принесено до банку; захист банківської інформації, що передається засобами зв’язку і міститься в системах автоматизованої обробки даних |
| 1.1. Організаційні | Заходи обмежувального характеру, які передбачають регламентацію доступу і використання технічних засобів передавання й обробки банківської інформації |
| 1.2. Організаційно- технічні | Забезпечують блокування можливих каналів витоку банківської інформації через технічні засоби за допомогою спеціальних технічних засобів, які встановлюються на елементи приміщень банку і технічних засобів, потенційно створюючи канали витоку банківської інформації |
| 1.3. Технічні | Заходи, які забезпечують використання спеціальних, захищених від побічних випромінювань технічних засобів передавання й обробки конфіденційної інформації банку |
| 2. Програмні | Система спеціальних програм, включених до складу програмного забезпечення комп’ютерів та інформаційних систем банку, які реалізують функції захисту конфіденційної інформації від неправомірних дій і програми їх обробки.  Забезпечують захист банківської інформації від несанкціо­нованого доступу до неї, копіювання її або руйнування. За допомогою програмних засобів здійснюється: ідентифікація об’єктів і суб’єктів; розмежування доступу до інформаційних ресур­сів банку; контроль і реєстрація дій з інформацією і програмами |

Закінчення табл. 6.3

|  |  |
| --- | --- |
| 1 | 2 |
| 3. Криптографічні | Використання спеціальних пристроїв, програм, виконання відповідних дій, які роблять сигнал, що передається, абсолютно незрозумілим для сторонніх осіб. Тобто криптографічні заходи забезпечують такий захист інформації, за якого у разі перехоплення її і обробки будь-якими способами вона може бути дешифрована тільки протягом часу, який потрібен їй для втрати своєї цінності. Для цього використовуються різноманітні спеціальні засоби шифрування, кодування та інших видів методів перетворення інформації (документів, мови, телеграфних повідомлень тощо) |
| 4. Фізичні | Засоби захисту засновані на створенні фізичних перешкод для зловмисника, які перегороджують йому шлях до інформації (сувора система пропуску на територію і в приміщення з апаратурою або з носіями інформації). Ці засоби дають захист тільки від "зовнішніх" зловмисників і не захищають інформацію від тих осіб, які володіють правом входу в приміщення |
| 5. Законодавчі | Законодавчі акти, які регламентують правила використання й обробки банківської інформації обмеженого доступу і вста­нов­люють кримінальну відповідальність за порушення цих правил |
| 6. Профілактичні | Спрямовані на попередження витоку банківської інформації як навмисного, так і мимовільного характеру (ефективний підбір персоналу; контроль за дотриманням персоналом банку інформаційної безпеки, аналіз способів витоку інформації, що мали місце в минулому; розмежування банківської інформації за ступенем таємності) |

Вибір засобів захисту інформації в банківських установах є надто складним завданням, оскільки банк вважає за потрібне досягти абсолютного захисту і водночас обрати зі значного розмаїття технічних і програмних засобів найбільш ефективних і дієвих для умов функціонування конкретного банку.

**6.3. Правове регулювання захисту таємниць банків**

Згідно з Законом України “Про банки і банківську діяльність”, *банківською таємницею* є будь-яка інформація, що стосується клієнта, якою банк володіє на законних підставах (за винятком, якщо така інформація складає державну таємницю), тобто інформація про діяльність і фінансовий стан клієнта, що стала відома банку у процесі його обслуговування і взаємовідносин з ним або з третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди клієнту [24].

У Законі України “Про інформацію” “*конфіденційна інформація”*  – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов». Ця інформація належить до інформації з обмеженим доступом [28].

Структурно вся банківська інформація ділиться на відкриту та інформацію з обмеженим доступом (рис. 6.1) [13].

Конфіденційна

Банківська інформація

З обмеженим доступом

Відкрита

Таємна

Банківська таємниця

Комерційна таємниця

Рис. 6.1. **Структура банківської інформації**

Відповідно до пункту 1 статті 1076 Цивільного кодексу України, відомості, що складають банківську таємницю, можуть бути надані банком органам державної влади та їх посадовим особам виключно у випадках та в порядку, встановлених законом України «Про банки і банківську діяльність», а саме: органам прокуратури України, СБУ, МВС України на їх письмові вимоги щодо операцій за рахунками конкретної юридичної особи або фізичної особи – суб’єкта підприємницької діяльності за конкретний проміжок часу; податковим органам України на їх письмову вимогу з питань оподаткування або валютного контролю щодо операцій за рахунками конкретної юридичної особи або фізичної особи — суб’єкта підприємницької діяльності за конкретний проміжок часу.

Правовий режим доступу до них банківської таємниці встановлено Законом України «Про банки і банківську діяльність». Інформація, що становить банківську таємницю фізичних осіб – клієнтів банку, розкривається банком на письмовий запит або з письмового дозволу власника інформації, а також на письмову вимогу або за рішенням суду. Водночас банківська таємниця юридичних осіб – клієнтів банку, крім зазначених умов, розкривається у таких випадках:

Банкам заборонено надавати інформацію про клієнтів іншого банку, навіть якщо їхні імена вказуються в документах, угодах і операціях клієнта.

Слід розрізняти поняття банківської та комерційної таємниць, конфіденційної інформації, оскільки до цих видів інформації різний доступ.

Комерційною таємницею не можуть бути [13]:

відомості зі статутних документів і документів, які дають право здій­нювати підприємницьку діяльність;

інформація за всіма формами державної звітності;

дані, які необхідні для обчислення податків та інших обов’язкових платежів;

відомості про чисельність і склад працівників, їх зарплату в цілому, за професіями і посадами, про наявність вільних місць;

відомості про участь посадових осіб у кооперативах, малих підпри­ємствах, союзах, об’єднаннях та інших суб’єктах підприємництва;

інформація про забруднення навколишнього середовища, пору­шення умов безпеки праці;

відомості, які відповідно до чинного законодавства підлягають опублікуванню.

Порядок доступу до відомостей, що становлять комерційну таємницю, визначає керівник банку. Цією ж статтею надається право керівникові визначати склад і обсяг таких відомостей. Так само визначено і режим доступу до конфіденційної інформації. Власникам конфіденційної інформації надано право самим включати її до категорії конфіденційної, визначати режим доступу до неї та встановлювати систему (способи) її захисту.

**6.4. Нормативна база банку із забезпечення інформаційної безпеки**

Типовий перелік нормативних українських банків щодо захисту його інформації з обмеженим доступом [13]:

Положення про організацію роботи з інформацією, що становить банківську і комерційну таємницю та є конфіденційною.

Інструкція про порядок підготовки, обліку, обігу, зберігання та знищення документів, справ, видань і матеріалів, що містять банківську та комерційну таємницю банку.

Інструкція про порядок виконання документів, що надходять у банк від правоохоронних органів, судів та інших державних установ.

Положення про забезпечення безпеки при наданні послуг за міжнародними банківськими платіжними картками.

Інструкція про порядок надання доступу користувачам до автоматизованих банківських систем.

Інструкція про проведення службових розслідувань в установах банку.

Положення про порядок підготовки, надсилання, обробки та зберігання електронних документів при використанні електронної пошти.

Інструкція щодо дій у разі компрометації криптографічних ключів в установах банку.

Інструкція зі знищення на електронних носіях документів, які містять ключові дані, конфіденційну інформацію, банківську або комерційну таємницю.

Положення про технічний захист інформації у банку.

Технологічна інструкція служби фінансової безпеки.

Положення про порядок одержання доступу до локальної обчислювальної мережі та ресурсів систем електронної обробки інформації.

Положення про режимні приміщення банку.

Угоди про конфіденційність з клієнтами, партнерами та іншими суб’єктами, з якими банк вступає у правовідносини, різного характеру пам’ятки, інструкції, заяви.

Список осіб, яким у повному обсязі може доводитись інформація, що становить банківську і комерційну таємницю та є конфіденційною.

Розглянемо основні нормативні документи банку з інформаційної безпеки. Положення про комерційну таємницю і конфіденційну інформацію містить [13]:

склад відомостей, що становлять комерційну таємницю та конфіденційну інформацію банку;

порядок захисту конфіденційної інформації в установах банку;

відповідальність за організацію заходів захисту;

відповідальність за розголошення конфіденційних відомостей.

Положення про організацію роботи з інформацією, що становить банківську і комерційну таємницю та є конфіденційною включає таку інформацію [13]:

права співробітників банку та інших осіб щодо отримання інформації з обмеженим доступом;

обов'язки посадових осіб і службовців банку щодо роботи з грифованими документами;

правила ведення конфіденційних переговорів за допомогою засобів зв'язку, спілкування з клієнтами та відвідувачами;

правила оформлення доступу до інформації з обмеженим доступом, порядок розроблення, зберігання, пересилання та руху грифованих документів в установах банку;

загальні обов'язки персоналу банку щодо зберігання його таємниць;

порядок доступу на засідання і наради, де обговорюються питання, в яких присутня інформація з обмеженим доступом;

інші питання, що регулюють правила доступу до інформації з обмеженим доступом.

Заходи банку з забезпечення інформаційної безпеки мають бути продуктивними, тобто відношення доходів банку до витрат на забезпечення інформаційної безпеки має бути якнайбільшим.

Зростати має і коефіцієнт інформаційної озброєності, тобто співвідношення витрат на придбання інформаційних технологій і комп’ютерних програм з захисту інформації до середньооблікової чисельності банківських працівників.