**Тема 9. Інформаційна безпека фінансово-кредитних установ**

*9.1. Інформаційні ризики та інформаційні загрози в банківській діяльності.*

*9.2. Управління інформаційними ризиками в діяльності банків.*

*9.3. Інформація з обмеженим доступом у банківській діяльності.*

*9.4. Система захисту інформації в банку.*

*9.5. Протидія інформаційно-психологічному впливу в діяльності банку.*

Сьогодні вже загальновизнаним є положення про домінуючу роль інформації у розвитку суспільства. Інформаційний розвиток, пов’язаний із прогресом знань, інтелектуалізацією суспільства, обумовлює нові підходи у взаємовідносинах різних суб’єктів — від безпосередньо громадян аж до міжнародних відносин. Водночас необхідно звернути увагу на особливість інформаційної складової саме в сьогоднішніх умовах . Справа у тому, що інформаційна складова завжди мала місце в діяльності людства, будь-який вид громадського, економічного, технічного розвитку завжди був пов’язаний з інформаційним забезпеченням. Досягнення практично в усіх сферах життєдіяльності базувалися на інтелектуальних здобутках, які насамперед характеризувались інформаційно. Більше того, наукові відкриття, передбачення, гіпотези з’являлися задовго до їх матеріального втілення, будучи основою для прогресу. Чому ж саме сьогодні мова йде про інформаційне суспільство, домінуючу роль інформації у його розвитку, основу удосконалення будь-яких політичних, технічних, економічних процесів?

Пояснюється це насамперед формуванням на сучасному етапі розвитку суспільства кількох факторів:

* + значною мірою збільшились обсяги інформації.
  + в останні роки збільшилися темпи зміни інформаційних характеристик. На відміну від минулих років повне оновлення інформації здійснюється один раз у сім років. Така ситуація обумовлює необхідність швидкого впровадження у практику
  + наявність великих обсягів не завжди об’єктивної інформації, швидка зміна інформаційних характеристик, а також можливість отримати певні переваги за рахунок інформації у суспільних взаємовідносинах зумовили необхідність формування суб’єктами зазначених відносин власного інформаційного ресурсу. Тобто сьогодні суспільний розвиток не може забезпечуватися лише фінансовими, матеріальними, кадровими ресурсами, а вимагає ще й відповідних інформаційних ресурсів;
  + інформація сьогодні існує не тільки як певна сума знань, а як і відповідний технологічний процес, котрий у поєднанні з іншими технологіями може суттєво впливати як на розвиток суспільства в цілому, так і на окремі його елементи. Зазначені технології здатні прискорювати або, навпаки, сповільнювати темпи суспільного розвитку, забезпечувати переваги розвитку окремих сфер, галузей чи концентрувати суспільні зусилля на певних напрямах. Більше того, інформаційні технології здатні формувати характер взаємовідносин у суспільстві — від мирного співіснування до суттєвих конфліктів. Здатність інформаційних технологій впливати на характер взаємовідносин у суспільстві обумовила сьогодні появу нового виду зброї — інформаційної, застосування якої несе в собі не менш негативні наслідки ніж зброя у звичайному розумінні цього слова;
  + сучасний рівень розвитку демократизації та технічного прогресу зумовив значне розширення доступу до інформації. Насамперед, збільшилося коло осіб, здатних отримати необхідну їм інформацію, знизився рівень закритості інформації, значно збільшилася кількість джерел інформації. Глобалізація суспільних та економічних відносин дає можливість отримувати інформацію практично з будь-якого інформаційного простору.

Таким чином, сучасні особливості інформаційного розвитку, безумовно, створюють і особливий характер взаємовідносин суб’єктів у будь-якій сфері діяльності, у тому числі і в банківській, а також накладають певний відбиток на характер самої діяльності та поведінку суб’єктів, що її здійснюють. Характеризуючи ці особливості з погляду безпеки підприємницької діяльності, необхідно зробити висновок про формування на ринку особливого виду відносин —інформаційних і, як наслідок, появи ще одного виду ризику — інформаційного. Наявність даного виду ризику формує можливість появи так званих інформаційних загроз, що, у свою чергу, обумовлює необхідність забезпечення безпеки підприємницької діяльності в інформаційній сфері, тобто створення такого виду безпеки, як інформаційна.

Сьогодні існує дуже багато точок зору щодо визначення суті інформаційної безпеки в бізнесі. Найбільш поширеною із них є думка про інформаційну безпеку як захист інформації, з чим не можна погодитися. Оскільки інформаційна діяльність суб’єктів підприємництва пов’язана з мінімізацією інформаційних ризиків, то інформаційна безпека має зачіпати всі складові такої діяльності, а саме: інформаційне забезпечення діяльності суб’єктів підприємництва, захист їх інформації та протидію негативному впливу інформаційних технологій, які можуть використовуватися суб’єктами підприємництва в їх взаємовідносинах. Виходячи з цього під інформаційною безпекою суб’єкта підприємництва, у тому числі і банку, доцільно розуміти стан, за якого здійснюється ефективне інформаційне забезпечення його діяльності, гарантований захист інформаційного ресурсу та належна протидія негативному інформаційному впливу. Тобто, структуру інформаційної безпеки суб’єкта підприємництва (банку) становлять три складові, наведені на рис. 7.1.

Інформаційна безпека суб’єкта підприємництва

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Інформаційне | | |  | Захист інформацій- | |  | Протидія негативному | | |
| забезпечення діяльності | | |  | ного ресурсу | |  | інформаційному впливу | | |
|  |  |  |  |  |  |  |  |  |  |

Рис. 7.1. Структура інформаційної безпеки суб’єкта підприємництва (банку)

**9.1. Інформаційні ризики та інформаційні загрози**

* 1. **банківській діяльності**

В умовах ринкової економіки головною формою взаємовідносин суб’єктів господарювання є конкуренція. Остання передбачає боротьбу виробників за найвигідніші умови діяльності, якіснішу продукцію та послуги, ефективний їх збут. За таких умов конкуренція є не одноразовим актом, а тривалим, а то й постійним процесом. Тобто у конкурентній боротьбі не буває постійних переможців, а тому така боротьба безперервна. Серед форм цієї боротьби не останнє місце займає добування конфіденційних відомостей, розкриття виробничих і комерційних таємниць, отримання й використання різної інформації без згоди власників. Для виконання таких дій створено цілу індустрію полювання за інформацією, в арсеналі якої є найсучасніші технічні, програмні засоби та технології, психотехнічні комунікації, заходи психологічного та соціального характеру, різні методики добування інформації.

Виходячи зі сказаного, можна зазначити, що інформаційна діяльність будь-якого суб’єкта підприємництва характеризується відповідним ступенем ризику. Отже, в ринкових умовах існує певна інформаційна небезпека для підприємства, банку в процесі їхньої діяльності на ринку.

Водночас слід звернути увагу на те, що інформація згідно з чинним законодавством є об’єктом права власності, а також об’єктом володіння, використання та розпорядження. Тобто на інформацію, її продукти та технології поширюється режим інституту майнових прав власності. Ураховуючи зазначене, необхідно вказати, що ризики, які виникають під час інформаційної діяльності (інформаційні ризики) суб’єктів підприємництва, виходять за межі загальновідомого технічного поняття і набувають властивостей суто майнових чи фінансових ризиків. У зв’язку з цим, виходячи із загальної класифікації ризиків і враховуючи введення інформації в систему товарних відносин, інформаційні ризики слід відносити і враховувати як майнові або виробничі ризики. Оскільки інформаційні ризики мають особливий характер, дії підприємств, банків, пов’язані з урахуванням і мінімізацією таких ризиків, мають також певні особливості.

Отже, з огляду на всі вищезазначені аспекти інформаційної діяльності та інформаційних взаємовідносин суб’єктів господарювання можна дійти висновку, що інформаційні ризики

— це ймовірність витоку, руйнування та втрати наявної у суб’єкта та необхідної для його діяльності інформації,

* використання ним необ’єктивної інформації,
* відсутність необхідної для прийняття правильних рішень інформації,
* можливість поширення в інформаційному середовищі невигідної, негативної чи небезпечної для суб’єкта господарювання інформації, що, зрештою, може завдавати йому збитків, матеріальної або моральної шкоди.

Оскільки сучасна діяльність банків значною мірою перебуває в інформаційній площині, банки, як ніхто інший із суб’єктів підприємництва, є об’єктами інформаційних загроз і впливу інформаційних ризиків.

Інформаційні ризики за своїм походженням поділяються на три категорії:

* + ризики, пов’язані з втратою (витоком, руйнуванням, знищенням) інформації. Особливо це небезпечно, коли існує ризик втрати такої важливої для банку і його клієнтів інформації, як банківська таємниця, або іншої інформації з обмеженим доступом;
  + ризики, пов’язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація);
  + ризики, пов’язані з інформаційним впливом на діяльність банків (поширення неправдивої та негативної для банків інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів банків, інформаційний тероризм).

Оскільки в умовах ринкової економіки ризик є однією із властивостей економічної діяльності, а для підприємницької діяльності ризик є однією з її складових, можна зазначити, що виключити ризик з інформаційних взаємовідносин суб’єктів підприємництва, зокрема й банків, узагалі неможливо.

Існування конкурентної боротьби та наявність зазначених ризиків породжує певні загрози для відомостей, які використовуються підприємствами та банками. Водночас діяльність останніх супроводжується безперервним процесом планування та прийняття рішень, що, у свою чергу, потребує надійного інформаційного забезпечення. Разом з тим участь населення в економічному житті формує потребу об’єктивного та всебічного інформування його про діяльність суб’єктів господарювання, бо довіра населення відіграє неабияку роль не лише у формуванні попиту на продукцію та послуги підприємств банків, а й загалом зумовлює перспективи їх розвитку.

На жаль, під час конкурентної боротьби існує загроза не лише неправомірних посягань на інформацію конкуруючих суб’єктів, а й постійно здійснюється інформаційний вплив на споживачів продукції та послуг, який не завжди є об’єктивним і таким, що сприяє правильному формуванню уявлення про продукцію, послуги та суб’єктів, які їх виробляють чи надають.

Отже, в інформаційних взаємовідносинах суб’єктів господарювання можуть виникати два види загроз:

* + загрози, пов’язані з посяганням на їх інформаційні ресурси (переважно ту частину, яка має обмежений доступ)
  + загрози інформації,
  + загрози, що виникають під час формування інформаційного середовища (умов) діяльності таких суб’єктів,
  + інформаційні загрози.

Як свідчить досвід, основними способами реалізації таких загроз є:

* маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації);
* порушення встановленого порядку інформаційного обміну,
* несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів,
* протиправне збирання і використання інформації;
* руйнування та використання з протиправною метою чужих інформаційних ресурсів;
* інформаційний тероризм (поширення комп’ютерних «вірусів», установлення програмних та апаратних пристроїв, призначених для несанкціонованого отримання інформації),
* упровадження радіоелектронних приладів перехоплення інформації,
* незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем,
* нав’язування фальшивої інформації, оприлюднення компрометуючої інформації та ін.).

Розглядаючи загрози банківській інформації, найбільш поширеними з них можна вважати: розголошення банківської інформації, її викрадення, модифікація чи знищення, незаконне використання інформації, несанкціонований доступ до інформації, що охороняється банком.

Розголошення інформації розуміють як протиправні умисні чи необережні дії посадових чи інших осіб, які призвели до несанкціонованого, без службової необхідності оголошення відомостей, щодо яких установлений певний порядок їх розкриття. Воно може здійснюватися через повідомлення, передачі, пересилання, публікації, втрати чи іншим способом оприлюднення зазначених відомостей.

Викраденням інформації є таємне вилучення носіїв інформації (документів, електронних носіїв, відео- та аудиозаписів) з метою подальшого їх використання іншою особою чи передання їх такій особі.

Знищенням є приведення носіїв інформації (документів, електронних носіїв, аудіо-, відеозаписів та інших носіїв, що мають матеріальний характер) до стану, непридатний для їх подальшого використання, або ж до неможливості використання інформації, яка на них зберігалася

Модифікацією інформації є внесення змін до змісту інформації, яка містилася на певних носіях, або ж до самих носіїв (комп’ютерних програм), у результаті чого використання даної інформації стає неможливим взагалі чи така інформація потребує суттєвого уточнення та аналізу.

Незаконне використання інформації означає використання певних даних, знань, технологій, які на праві власності належать певній юридичній чи фізичній особі, без її згоди або з порушенням установленого порядку їх використання особами, яким така інформація відома у зв’язку з їхнього службовою чи іншою діяльністю.

Несанкціонованим буде також доступ до інформації з порушенням установлених правил доступу до неї.

Зазначені загрози мають загальний характер і однаково стосуються всіх видів інформації: документованої, електронної, знань та ін. Звичайно, кожному з видів інформації притаманні додатково й інші, властиві тільки конкретним видам інформації загрози. Розглядати кожен з таких випадків, мабуть, буде недоцільно, оскільки вжиття заходів щодо захисту та протидії зазначеним видам загроз забезпечить безпечний стан будь-якої інформації з високим ступенем гарантії. Водночас, оскільки банківська діяльність тісно пов’ язана з комп’ютерними інформаційними технологіями, деякі особливості загроз таким технологіям слід було б навести, передусім з погляду подальшої інформатизації суспільства та перспектив його розвитку.

Насамперед слід звернути увагу на загрози, пов’язані з глобалізацією інформаційних і телекомунікаційних технологій. У зв’язку з процесом міжнародної інтеграції та глобалізації обсяги та різноманітність загроз значно розширилися. Банки можуть зазнавати інформаційного удару щодо своїх інформаційних та фінансових ресурсів із глобального інформаційного простору. Серед найпоширеніших глобальних загроз — комп’ютерний тероризм і комп’ютерне хуліганство. Значне поширення Інтернет-технологій і відносна анонімність користувачів спровокували появу так званих хакерів, крекерів, телефонних фанатів — людей, які вважають своїм обов’язком здійснити певні протиправні дії в мережі Інтернету як самовираження на глобальному рівні. Як правило, такі особи є добре обізнаними з комп’ютерними технологіями, є їх фанатами і тому можуть на досить професійному рівні проникати в комп’ютерні системи. Вони є катастрофічно небезпечні для банківських комп’ютерних технологій, оскільки не тільки руйнують системи їх захисту, а можуть отримати досить важливу банківську інформацію. А поширене останнім часом комп’ютерне хуліганство зумовило появу фактів , пов’ язаних з так званим електронним пограбуванням банків. Щороку банки світу від протиправних дій різного роду хакерів, крекерів, комп’ютерних хуліганів зазнають мільярдні збитки та втрачають величезні обсяги інформації.

Захист банківських інформаційних технологій, які використовуються у платіжних системах банків , є досить специфічним і займає окреме місце в забезпеченні банківської безпеки.

В реалізації загроз банківській інформації важливе місце займають канали її витоку, до яких можна віднести: візуально-оптичні, акустичні та акустоперероблювальні, електромагнітні (у тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії тощо).

Візуально-оптичні канали створюються як оптичний шлях від об’єкта інформації до її отримувача. Для цього необхідні енергетичні, часові та простірні умови і відповідні технічні засоби. Створенню таких каналів сприяють відповідні характеристики об’єкта інформації: конфігурація, поведінка, діяльність і т. п. Особлива цінність інформації, отриманої через такий канал, полягає в тому, що вона є максимально достовірною, оперативною і може служити документальним підтвердженням отриманих відомостей.

Джерелом створення акустичного каналу є 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 та ін.

Звукові коливання від голосу людини, інших звуків створюють акустичні хвилі, які, поширюються у просторі і взаємодіючи з відповідними перешкодами, викликають у них змінний тиск (двері, вікна, стіни, підлога, різноманітні прилади), приводячи їх у коливальний режим. Впливаючи на спеціальні прилади (мікрофони), звукові коливання створюють у них відповідні електромагнітні хвилі, які передаються на відстань і несуть в собі створену звуковими коливаннями інформацію.

Акустичні канали створюються:

♦ за рахунок поширюються акустичних (механічних) коливань у вільному повітряному просторі (переговори на відкритому просторі, у приміщенні при відкритих вікнах, квартирках, дверях, витік через вентиляційні канали);

♦ за рахунок впливу звукових коливань на елементи і конструкції будівель (стіни, стеля, підлога, вікна, двері, вентиляційна система, труби водопостачання, опалення, мережі кондиціонування);

♦ за рахунок дії звукових коливань на технічні засоби обробки інформації (мікрофонний ефект, акустична модуляція і т. п.).

Електромагнітні канали за своєю фізичною природою та експлуатаційними особливостями технічних засобів, які забезпечують виробничу діяльність, є найбільш небезпечними і досить поширеними каналами отримання інформації. Такі канали створюються через наявність у технічних засобах, які використовуються у виробництві, джерел небезпечних сигналів. Насамперед до таких джерел відносять перероблювачів, якими є прилади, що трансформують зміни однієї фізичної величини в зміни іншої. У термінах електроніки перероблювач визначається як прилад, що перетворює неелектричну величину в електронний сигнал, або навпаки. Хороші знання роботи перероблювачів дозволяють визначати можливі неконтрольовані прояви фізичних полів, які і створюють електромагнітні канали витоку (передання) інформації. Водночас з огляду на ідентичність технічних та конструктивних рішень, електронних схем технічних засобів обробки інформації і забезпечення виробничої діяльності підприємств і банків, усім їм потенційно властиві ті чи ті канали витоку (передавання) інформації. Тому у будь-якому разі використання технічних засобів обробки та передавання інформації створює загрозу її безконтрольного витоку (передання).

Матеріально-речові канали отримання інформації створюються через вивчення відходів виробничої діяльності (зіпсовані документи або їх фрагменти, чернетки різного роду поміток, записів, листів і т. п.), викрадення, несанкціоноване ознайомлення, копіювання, фотографування, відеозапис документів, креслень, планів, зразків технічних або програмних засобів.

Водночас доцільно звернути увагу, що найчастішими і найбезпечнішими за обсягом збитків є загрози, що створюються помилками працівників банку, які працюють з різними видами

інформації або обслуговують інформаційні системи. До 65% втрат банків є наслідком ненавмисних помилок, некоректності та недбалості банківських працівників під час роботи з інформацією

Крім того, до факторів, які створюють умови витоку (передання) інформації, за дослідженнями спецслужб, відносять фактори, наведені в табл.

**ФАКТОРИ, ЩО СТВОРЮЮТЬ УМОВИ ВИТОКУ ІНФОРМАЦІЇ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Фактор** | **Відсоток** |  |  |
|  |  |  |  |  |
| 1. | Надмірна балакучість співробітників підприємств, фірм, банків | 32 |  |  |
| 2. | Прагнення працівників підприємств, фірм, банків заробляти | 24 |  |  |
| гроші будь-яким способом і будь-якою ціною | |  |  |
|  |  |  |
|  |  |  |  |  |
| 3. | Відсутність на підприємстві, фірмі, у банку системи заходів, | 14 |  |  |
| направлених на захист інформації | |  |  |
|  |  |  |
|  |  |  |  |  |
|  |  |  | |  |
|  |  |  |  |  |
| 4. | Звичка співробітників підприємств, фірм, банків ділитись один | 12 |  |  |
| з одним почутими новинами, чутками, інформацією | |  |  |
|  |  |  |
|  |  |  |  |  |
| 5. | Безконтрольне використання інформаційних систем | 10 |  |  |
|  |  |  |  |  |
| 6. | Наявність передумов для виникнення серед співробітників | 8 |  |  |
| конфліктних ситуацій | |  |  |
|  |  |  |
|  |  |  |  |  |

Інформаційні загрози пов’язані насамперед з впливом на банк та його середовище, основним інструментом якого є інформація. До таких загроз слід віднести дискредитацію банку (поширення негативної неправдивої інформації про банк, маніпулювання індивідуальною та колективною свідомістю працівників, клієнтів, акціонерів банку та громадян, дезінформація різних осіб і суб’єктів у взаємовідносинах з банком, поширення негативних чуток про банк, здійснення актів інформаційного тероризму та провокування інформаційних конфліктів, втягування банку в інформаційну війну).

Суб’єкти, якій у такий спосіб здійснюють вплив на банк, виходять із того, що людина живе в реальному світі, але сприймає його через систему комунікацій. Тому, створивши нові комунікаційні технології та включивши в них відомі стандарти надання інформації, можна викривити реальний світ, замінивши його інформаційним в уявленні споживачів

інформації . Тобто інформаційний простір банку є досить керованим і залежно від того, хто має можливість ним керувати, таким буде і сам простір, а з ним і банк. Вплив на споживачів інформації в таких умовах здійснюється через формування відповідних схем надання інформаційних повідомлень, коментарів, точок зору експертів, поширення чуток, наведення прикладів і порівнянь, як правило, досить актуальних та гострих. В інформаційний простір банку протягом певного терміну по багатьох каналах подається об’ємна інформація. Перебуваючи під впливом стандартної побудови системи подання інформації, споживачі останньої сприймають її як реальну, а не штучно створену. Метою таких дій є формування для банку умов, в яких йому складно буде здійснювати свою діяльність, банк втрачатиме свій імідж, а з ним і конкурентоспроможність на ринку.

**9.2. Управління інформаційними ризиками в діяльності банків**

Пошук заходів з попередження шкоди, заподіяної від реалізації інформаційних загроз, може бути забезпечено через систему управління інформаційними ризиками.

Зазначена система управління має забезпечувати не тільки надійний захист інформаційних ресурсів, а й сприяти ідентифікації інформаційних ризиків, виявленню факторів та умов їх появи й забезпечувати їх мінімізацію у процесі діяльності суб’єкта господарювання.

Процес управління інформаційними ризиками передбачає проведення процедур аналізу, оцінювання, контролю і мінімізації ризиків.

Аналіз ризиків передбачає їх визначення та оцінювання. Під час визначення ризиків установлюють, які саме інформаційні ризики можуть існувати чи існують в діяльності суб’єкта господарювання (у нашому випадку банку) або в процесі проведення ним конкретної комерційної (банківської) операції, як вони можуть вплинути на діяльність чи операцію та яка існує ймовірність настання негативних наслідків від дії ризику.

Оцінювання інформаційного ризику передбачає визначення обсягу шкоди, яку може зазнати суб’єкт унаслідок вияву зазначеного ризику.

Контроль інформаційних ризиків передбачає проведення заходів щодо з’ясування умов, за яких такі ризики можуть бути мінімальними, суттєвими або значними.

Мінімізація інформаційних ризиків передбачає вжиття заходів , спрямованих на зниження ймовірності негативного впливу ризиків, їх уникнення або зменшення їх розміру. Одним з напрямів мінімізації інформаційних ризиків, коли неможливо їх уникнути, може бути розподіл їх вартості в часі, аби зменшити одночасний тиск ризику в певні моменти діяльності суб’єкта чи здійснення ним певної операції.

Найпоширенішим варіантом мінімізації інформаційних ризиків є передання їх іншому суб’єкту, передусім за рахунок страхування ризиків.

Ураховуючи значну роль інформації в діяльності банків, система управління їх інформаційними ризиками має включати певні підсистеми:

* підсистему захисту інформації;
* підсистему збирання інформації та інформаційних досліджень;
* підсистему протидії інформаційному впливу;
* управляючу підсистему.

Основними завданнями підсистеми захисту інформації банку мають бути:

* виявлення інформації, що підлягає захисту,
* визначення місць зосередження та носіїв інформації, яка підлягає захисту,
* визначення можливих способів несанкціонованого доступу до такої інформації, розроблення й упровадження організаційних, правових, технічних, програмних, криптографічних та апаратних заходів захисту інформації.

З огляду на те, що в банках зосереджені доволі значні обсяги інформації з обмеженим доступом (банківська, комерційна таємниці, конфіденційна інформація), та те, що банки є єдиними (крім державних режимних установ) серед суб’єктів підприємницької діяльності, на кого в законодавчому порядку покладено захист чужих таємниць (клієнтів банків), питання аналізу, контролю та мінімізації втрати інформації для банків є доволі важливими. Звідси головним в аналізі ризиків втрати інформації є виявлення способів несанкціонованого доступу до інформації банку та її найбільш уразливих носіїв.

Під час проведення такого аналізу слід виходити з того, що інформація банку зосереджена переважно в двох групах її носіїв: комп’ютерній інформаційній мережі та у працівників банку. Тобто несанкціонований доступ до інформації може бути здійснено, з одного боку, через технічні й програмні засоби, а з другого — за допомогою засобів інтелектуального та психологічного характеру. Оскільки поведінка людей, зокрема працівників банку, є доволі непередбачуваною, а телекомунікаційні системи банку в умовах значного розвитку штучного інтелекту є уразливими, можна говорити, що ризики втратити банками їх інформацію зосереджені головним чином на таких її носіях, як персонал і телекомунікаційні системи.

Оцінювання ризиків втрати інформації в банку передбачає визначення вартості інформаційних ресурсів, щодо яких існує ризик втрати, та самого ризику як імовірності реалізації певної загрози, у цьому разі пов’язаної з втратою інформації. Вартість інформації оцінюється через її комерційну цінність, яка, у свою чергу , визначається через розміри збитків (шкоди), які можуть настати у зв’язку з її втратою, обсягом (перспективами) вигоди, яку може отримати банк, використовуючи наявну в нього інформацію , а також витрати, пов’язані з виробленням, отриманням і захистом такої інформації. Щодо банківської таємниці, то її цінність може бути визначена через обсяги залучених коштів від клієнтів банку, інформацію про комерційну та фінансову діяльність яких він зберігає.

На оцінювання власне ризику як імовірності реалізації певної загрози щодо відповідної інформації банку впливає кілька показників. Головними серед них є привабливість інформації для суб’єктів загроз, її цінність, актуальність, доступність, рівень захисту. Через ці показники визначається рівень критичності інформації. Скажімо, для інформації про фінансову діяльність клієнтів банку рівень критичності може бути доволі високий, незважаючи на вжиття банком заходів її захисту. Це насамперед пов’язане з тим, що доступ до такої інформації має значна кількість осіб (операціоністи, бухгалтерські працівники, працівники кредитного та інших підрозділів банку, працівники його телекомунікаційних систем , служби безпеки), а в проведенні платежів задіяно дуже багато технічних засобів та інформаційних мереж, за допомогою яких така інформація передається. Ризик доступу до зазначеної інформації буде тим вищим, чим активніше здійснює свої фінансові операції клієнт ( проведення платежів, отримання кредитів, операції з цінними паперами, валютою, пластиковими платіжними засобами). Крім того, береться до уваги ділова активність клієнта, його роль і місце на ринку, конкурентна поведінка. У цьому разі інформація про клієнта банку буде доволі привабливою для його конкурентів і вони намагатимуться її отримати.

Якщо клієнт обслуговується лише в одному банку, то ризик посягань на його інформацію підвищується порівняно з тим, коли свої фінансові операції він диверсифікує в різних банківських установах. Виходячи з цього ймовірність реалізації загроз, як і, власне, ризик втрати інформації, може бути високою (коли всі зазначені вище показники набувають суттєвої актуальності), середньою (за умов високої актуальності хоча б одного показника) і звичайною (для клієнтів банку, які не відрізняються високою активністю на ринку).

Контроль ризиків втрати інформації в банку забезпечується проведенням періодичних перевірок та аналізом стійкості інформаційної його системи до внутрішніх

та зовнішніх загроз, своєчасного виявлення уразливих місць в її захисті. Крім того, на основі постійного моніторингу інформаційного середовища діяльності банку виявляють ознаки небезпек і загроз банківській інформації. Особливу увагу приділяють виявленню суб’єктів (як фізичних, так і юридичних осіб), взаємовідносини банку з якими можуть створювати для нього певні ризики втрати інформації, а також суб’єктів, діяльність яких може бути спрямована на несанкціоноване оволодіння банківською інформацією.

Тут слід звернути увагу і на ризики, що випливають з поведінки персоналу як одного з небезпечних джерел витоку банківської інформації. У цьому разі персонал банку можна розглядати як активний елемент інформаційної системи банку, здатний бути не тільки творцем і джерелом інформації, а й суб’єктом протиправних дій щодо інформаційних об’єктів. Працівники банку можуть як володіти інформацією, так і поширювати її в межах своїх функціональних обов’язків. Крім того, вони здатні її аналізувати, узагальнювати, робити відповідні висновки, а за певних умов — розголошувати, продавати, незаконно використовувати або незаконно передавати третім особам. На можливість посягань на інформацію банку з боку його працівників вказують результати досліджень іноземних фахівців щодо структури

виробничих колективів (рис. 7.3) . Тобто зі 100% працівників банку 75% можуть здійснити посягання на банківську інформацію.

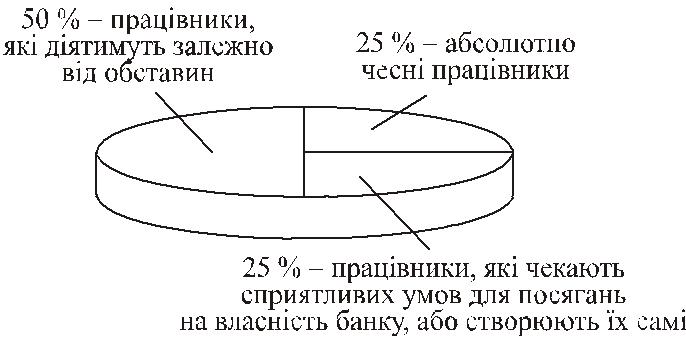


Рис. 7.3. Структура виробничих колективів за критерієм готовності до посягань на інформацію суб’єкта господарювання

Питання мінімізації ризику втрати інформації є доволі серйозним для банків, однак чи всі ризики необхідно мінімізувати, якщо так, то до якого ступеня? З досвіду відомо: хоч як банки чи інші суб’єкти намагалися виключити ризик втрати інформації, зробити це майже неможливо. Крім того, керівництво банків повинно бути орієнтоване на певний ризик втрати інформації, щоб виникнення якоїсь непередбаченої ситуації не стало проблемою, яку неможливо вирішити. У цьому разі банки завжди передбачатимуть дії на випадок втрати інформації, розраховувати свої можливості щодо ліквідації наслідків і бути готовими до неадекватного розвитку ситуації в інформаційних взаємовідносинах зі своїми клієнтами, акціонерами, партнерами та іншими суб’єктами.

Водночас для зниження (мінімізації) ризику втрати інформації банки мають вживати відповідних заходів, диференціюючи їх відповідно до певних загроз. Серед таких заходів насамперед мають бути:

* формування правових умов захисту інформації безпосередньо у банку.

Під такими умовами слід розуміти розроблення нормативно-правових документів банку стосовно захисту всіх видів інформації (документованої, електронної, а також інформації, яка існує у вигляді знань працівників банку). Зазначеними документами мають регулюватися взаємовідносини банку з його працівниками, клієнтами, партнерами, іншими

* створення системи захисту інформації, яка функціонує в банківській інформаційній мережі.

Зазначена система має передбачати комплекс організаційних, технічних, апаратних, криптографічних заходів і забезпечувати гарантований захист від посягань на електронну інформацію банку;

* + забезпечення контролю за носіями інформації, насамперед працівниками банку, стосовно дотримання ними встановленого режиму захисту інформації, своєчасне реагування на всі збої в захисті інформації, що зберігається та функціонує в інформаційних мережах банку;
  + запровадження надійної системи документообігу в банку (службового та спеціального діловодства), яка виключала б можливість несанкціонованого доступу до банківських документів, їх втрати, знищення чи модифікації;
  + забезпечення надійної охорони банків, особливо з погляду виключення можливості несанкціонованого доступу до них та їх винесення документів чи електронних носіїв інформації.

Отже, управління інформаційними ризиками з позиції мінімізації загроз утрати інформації в банку є доволі трудомістким і багатогранним процесом, який охоплює різні види організаційної, правової, інженерно-технічної, кадрової та безпосередньо інформаційної роботи.

Управління ризиками, що виникають у процесі формування банками інформаційного ресурсу, мають особливий характер. Річ в тім, що тут існує певна проблема, пов’язана з необхідністю суттєвого інформаційного забезпечення діяльності банків і відсутністю для цього відповідного правового регулювання. Нині в Україні немає законодавства, яке регулювало б права, умови та порядок доступу банків до джерел інформації, необхідної їм для забезпечення банківської діяльності. Відсутність такого законодавства створює безліч ризиків, що виникають у процесі інформаційного забезпечення насамперед банківських операцій. Аналіз ризиків, які можуть виникати під час формування інформаційного ресурсу банку за умов відсутності необхідного правового регулювання, показує, що найпоширенішими з них можуть бути ризик відсутності необхідної банку інформації, ризик отримання та використання неповної, необ’єктивної інформації, ризик дезінформації. Особливу небезпеку створюють ризики, які

виникають під час інформаційно-аналітичного дослідження клієнтів банків.

Ризик відсутності інформації може виникати, коли банку в короткі терміни потрібна буде конкретна інформація, або коли об’єкти й джерела певної інформації невідомі. Особливо такі ситуації можуть бути характерними у кредитній діяльності банків, під час проведення операцій із пластиковими платіжними засобами, а також у процесі прийняття управлінських рішень, особливо у процесі фінансового моніторингу сумнівних операцій та ідентифікації осіб, стосовно яких є підозра в легалізації (відмиванні) коштів, отриманих незаконним способом. Відсутність необхідної банку інформації призводить до прийняття необ’єктивних рішень і, як наслідок, до неефективних дій банку на ринку банківських послуг.

Ризик отримання та використання неповної та необ’єктивної інформації існує завжди, і саме такою ситуацією, як правило, характеризується діяльність банків. Ситуація невизначеності у прийнятті рішень є характерною для бізнес-діяльності, але тут важливим є те, щоб ризик використання такої інформації не призводив до неефективної діяльності та збитків. Тобто якщо ризик відсутності інформації є менш імовірним для банків, то ризик отримання та використання неповної чи необ’єктивної інформації практично завжди має місце в діяльності банків. Водночас і перший, і другий ризики мають бути враховані при здійсненні конкретних дій чи проведенні банком конкретної операції.

Ризик дезінформації банку стосовно умов, суб’єктів, мети взаємовідносин з банком може виникати через загострені взаємовідносини з конкурентами чи недобросовісну поведінку клієнтів. Річ у тім, що в перших двох випадках ризики (ризик відсутності інформації та ризик використання неповної чи необ’єктивної інформації) мають об’єктивний характер через те, що певні суб’єкти намагаються захистити свою інформацію, а банк, навпаки, — отримати її, водночас ризик дезінформації банку створюється певними суб’єктами штучно, з метою введення банку в оману. За таких умов ризик дезінформації зазвичай завжди матиме суттєві негативні наслідки для банку. Тому банки, забезпечуючи свою діяльність в інформаційному сенсі й формуючи свої інформаційні ресурси, повинні звертати особливу увагу на наявність ризику дезінформації.

Слід пам’ятати, що обсяги дезінформації різко зростають у так звані критичні періоди, які характеризуються:

♦ зростанням напруженості у відносинах із суб’єктами конфлікту;

♦ відсутністю об’єктивної інформації та невизначеністю ситуації в інформаційному середовищі банку;

♦ необхідністю інформації для прийняття швидких та адекватних рішень сторонами конфлікту.

За таких умовах виникає особлива небезпека дезінформуючого впливу на банк, оскільки дезінформація може будуватися на мінімальних обсягах об’єктивної інформації

Особлива небезпека за таких умов полягає у тому, що

дезінформаційний вплив здійснюється за допомогою незадіяних до цього джерел, які маскуються як внутрішні, тобто банківські, що сприяє підвищенню рівня довіри до такої інформації. Більше того, за умов загострення конфлікту дезінформація може подаватися з кількох джерел, до того ж упродовж певного періоду, тобто щодо банку починає проводитися серйозна інформаційна кампанія.

Оцінювання ризиків, пов’язаних з формуванням інформаційного ресурсу, може визначатися через ціну (вартість) певної банківської операції, щодо якої здійснюється інформаційне забезпечення, або обсяги прибутку , які може отримати банк у разі прийняття рішення на основі об’єктивної інформації. Тобто ціна ризику визначається обсягом зроблених банком вкладень та очікуваного прибутку. Водночас обсяги операцій чи прибутків не можуть повною мірою давати оцінку ризикам, пов’язаним з формування інформаційного ресурсу.

Такими обсягами може вимірюватися ризик відсутності інформації, тоді як на оцінювання інших ризиків суттєво впливатиме якість інформації, якою забезпечується певна операція чи рішення.

Показниками якості інформації є її достовірність , повнота та актуальність. Достовірною вважається інформація, отримана з двох і більше незалежних джерел або одного надійного джерела, а також та, об’єктивність якої підтверджена додатковою перевіркою. Повною буде інформація, з якої можна скласти характеристику об’єкта, достатню для формування об’єктивного уявлення про нього. Актуальною вважається інформація, в якій на цей час має потребу банк. За таких умов інформація, яка є достовірною, повною та актуальною, вважатиметься якісною зі ступенем ризику її використання, який можна прийняти.

Інформація, щодо якої є сумніви стосовно її достовірності, з якої неможливо скласти необхідні характеристики про об’єкт зацікавленості та яка неповністю відповідає нагальним потребам банку, буде вважатись низької якості (неякісною). Усі інші характеристики якості інформації, які перебувають у межах від неякісної до якісної вважатимуться такими, що формують певний ризик використання інформації. Тобто під час використання якісної інформації ризики можуть бути мінімальними й вони можуть бути прийняті банком. За неякісної інформації ризики можуть бути доволі суттєвими, і за таких умов доцільно відмовитися від певних дій чи вжити додаткових заходів з підвищення якості інформації. В усіх інших випадках слід вживати заходів щодо мінімізації як інформаційних ризиків, так і ризиків, пов’язаних з тими чи тими діями банку.

Використання якісної інформації може формувати рівень ризику з коефіцієнтом від 0 до 0,2, неякісної — від 0,5 до 1,0. Усі інші коефіцієнти приймаються для інформації, яка за своєю якістю вища, ніж така, що може вважатися неякісною. За таких умов, оцінювання ризику формування інформаційного ресурсу для інформаційного забезпечення певної банківської операції чи рішення визначатиметься як добуток від обсягу операції (угоди, рішення) та відповідного коефіцієнта якості інформації.

Контроль ризиків, пов’язаних з формуванням інформаційного ресурсу, передбачає проведення аналітичної роботи з усіма видами інформації, яку отримує банк і планує використати для забезпечення його діяльності. Під час аналітичної роботи інформація узагальнюється, порівнюється, переперевіряється, відомості щодо яких є сумнів у їх достовірності, вилучаються з

інформаційного ресурсу. Уся інформація підлягає обробці, у результаті якої отримуються інформаційні дані, використання яких матиме мінімальний ризик для банку.

Крім того, з метою контролю ризиків, що можуть виникати під час формування інформаційного ресурсу, банки намагаються встановити постійні та надійні зв’язки з джерелами інформації, підтримувати стабільні взаємовідносини з ними. Водночас банки дбають про розширення мережі джерел інформації, аби забезпечити її отримання з якомога більшої кількості джерел і здійснювати контроль не лише за надходженням інформації, а й за поведінкою самих джерел.

Мінімізація ризиків, що виникають під час формування інформаційного ресурсу банку, інформаційного забезпечення його операцій та управлінських рішень, здійснюється через проведення відповідних заходів, передусім інформаційного спрямування. Насамперед звертається увага на організацію інформаційно-аналітичної роботи в банку , яка повинна виконуватись як один з необхідних видів інформаційного забезпечення банківської діяльності. Ця робота має передбачати збирання та обробку інформації з різних джерел різними підрозділами банку. На жаль, у більшості банків цьому питанню не приділяють належної уваги, у кращому разі завдання інформаційно-аналітичної роботи покладають на службу безпеки і цим обмежуються. Тому інформація зазвичай є неповною та односторонньо висвітлює події, явище, об’єкти. Коли ж у банку організовується інформаційно-аналітична робота як один з елементів його інформаційного забезпечення, то формування інформаційних ресурсів здійснюється системно на трьох інформаційних рівнях: інформація від маркетингової діяльності, інформація від проведення інформаційного моніторингу і досліджень клієнтів та інформація, отримана від заходів комерційної розвідки. Крім того, така робота передбачає періодичне проведення в підрозділах банку інформаційного аудиту, під час якого виявляється необхідна для забезпечення конкретної діяльності банку та його операцій юридична, комерційна, фінансова, технологічна та інша інформація.

Уся інформація, отримана від маркетингової діяльності, інформаційного моніторингу та аудиту, а також комерційної розвідки, узагальнюється, аналізується, за необхідності перевіряється та формується у відповідні бази даних. Тобто основними засадами мінімізації ризиків під час формування інформаційних ресурсів банку є створення власної інформаційної бази даних. Якраз зазначена база

має стати головним джерелом інформації для інформаційного забезпечення банківських операцій та управлінських рішень. Водночас така база має постійно поновлюватись і доповнюватись, щоб не допустити її старіння й формування певного ризику її використання.

Стосовно ж інформаційного забезпечення кожної конкретної банківської операції, особливо тих, які пов’язані з вкладанням коштів банку, банківськими гарантіями та зобов’язаннями банків, останні зазвичай здійснюють інформаційно-аналітичні дослідження клієнтів незалежно від того, чи є відповідна інформація про цих клієнтів у базах даних банків, чи її немає.

Інформаційно-аналітичне дослідження проводиться щодо правового статусу, фінансових можливостей, історії взаємовідносин з банками, судами, правоохоронними та податковими органами, комерційної діяльності відповідних клієнтів. Повнота інформації про клієнта формує певний ризик взаємовідносин з ним. Зокрема, з практики діяльності банків відомо, що під час проведення кредитних операцій деякі банки України та Росії визначають так званий ризик помилки вибору позичальника , в основу якого покладено повноту інформації, що характеризує кожного конкретного позичальника. Так, низький ризик визначається за умов, коли наявність інформації про позичальника становить не менш як 90%, необхідної банку. До позичальників з низьким ризиком відносять тих суб’єктів, щодо яких отримана інформація дає змогу зробити висновки про відсутність в їхній діяльності кримінальних зв’язків, стабільну комерційну діяльність, позитивну кредитну історію, багатопрофільну діяльність, наявність філій, хороший фінансовий стан.

Малий ризик визначається, коли банк отримав не менш як 80% необхідної йому інформації про позичальника й коли така інформація дає змогу характеризувати його як суб’єкта, у

діяльності якого немає кримінальних зв’язків, підтримується стабільна комерційна діяльність на основі перспективного бізнесу, що здійснюється за участі багатьох партнерів. Крім того, отримана інформація дає можливість дійти висновку про хороший фінансовий стан та позитивну кредитну історію позичальника.

Середній ризик визначають для позичальників, про яких банк отримав не менш як 70% необхідної йому інформації . У цьому разі інформаційні характеристики можуть вказувати на діяльність позичальника в ризиковій сфері бізнесу, факти несвоєчасного повернення кредитів і сплати податків або відсутність досвіду роботи з кредитними коштами, велику кількість рахунків у різних банках, частина з яких (рахунків) є непрацюючими.

Високий ризик визначають для позичальників, про яких банк отримав не менше 60% необхідної йому інформації, що свідчить про факти неповернення кредитів у діяльності позичальника, судові розгляди справ за позовами до позичальника, наявність кредиторських боргів, часту реорганізацію структури позичальника, велику плинність кадрів, нестійкий фінансовий стан, факти недобросовісної конкуренції, до яких вдається позичальник.

Дуже високий ризик визначається за умов, коли банк отримує менш як 60% необхідної йому інформації про позичальника. До того ж ця інформація характеризує останнього як такого, у якого немає ознак реальної господарської діяльності, є непорозуміння з правоохоронними органами та факти недбалого ставлення до виконання своїх зобов’язань, а також з отриманої інформації неможливо скласти об’єктивний висновок про фінансовий стан позичальника та можливості й перспективи його підприємницької діяльності.

За такого підходу в сукупності з іншими видами ризику, які розраховуються у банку, можна буде зробити об’єктивний висновок щодо надійності позичальника в його взаємовідносинах з банком.

На жаль, в умовах відсутності правового регулювання збирання необхідної банкам інформації чимало з них ведуть таку роботу не надто успішно й з ризиком , який не завжди дає змогу ефективно використовувати отриману інформацію. За таких умов банки не повсякчас активно вдаються до такої роботи, а тому нерідко зазнають втрати від неправильно застосованої або недостатньої інформації під час прийняття тих чи тих рішень або проведення банківських операцій . Особливо від цього потерпають кредитні операції банків, які найбільше потребують об’єктивної інформації.

В нинішніх умовах, коли інформаційні технології набули значного поширення в усіх сферах діяльності, великого значення набувають аналіз, оцінювання, контроль і мінімізація ризиків інформаційного впливу.

Інформаційний вплив — це використання спеціальних інформаційних технологій з метою формування або зміни поведінки окремих осіб чи груп осіб (колективів, соціальних груп) стосовно певних подій, об’єктів, діяльності. Формування або зміна поведінки залежно від того, на кого спрямована дія інформаційних технологій, може здійснюватися через застосування технологій маніпулювання індивідуальною або масовою свідомістю. Технології маніпулювання свідомістю здатні викликати в людей певне ставлення до суб’єкта чи організації (недовіру, розчарування, огиду та ін.), а також сформувати певну поведінку (страйки, демонстрації, саботаж, акти масової непокори, безлад). За таких умов основними видами ризику інформаційного впливу для банку можуть бути:

* + ризик втрати іміджу банку на ринку банківських послуг;
  + ризик конфліктних ситуацій із власним персоналом, клієнтами, акціонерами, державними органами;
  + ризик блокування роботи банку через численні перевірки його діяльності.

Зауважимо, що здійснюючи свою діяльність, банки активно використовують можливості та умови інформаційного середовища, а тому можуть у будь-який час зазнати дії ризиків інформаційного впливу. Різке якісне зростання інформаційних технологій та інформаційних продуктів поступово формує нові способи застосування інформації як виду інтелектуальної зброї. Тому, здійснюючи аналіз ризиків інформаційного впливу, банки мають визначитися, з яким саме видом ризику вони можуть стикатися на певному етапі своєї діяльності або під час здійснення відповідної банківської операції. Слід зауважити, що ризики інформаційного впливу можуть мати постійний характер як результат певних відносин банків із різними суб’єктами, або формуватись як наслідок цілеспрямованої дії певних суб’єктів. В останньому разі найхарактернішими є так звані інформаційні атаки, коли з різних джерел одночасно або в невеликий проміжок часу в інформаційне середовище банку подається негативна для нього інформація. Найімовірніше, що інформаційні атаки можуть здійснюватися за умов, коли банк перебуває в стані конфронтації або конкурентного суперництва чи протиборства з певними суб’єктами ринку або іншими особами. Якраз за таких умов ризик потрапляння банку в ситуацію активного нагнітання навколо нього негативної інформації буде доволі істотним. У цьому разі, як наслідок, виникають інші види ризиків, уже іншого характеру ― зниження або втрати іміджу, втрати клієнтів, зменшення обсягів операцій, отримання збитків. Основними формами інформаційних атак, унаслідок яких може виникати ризик зниження іміджу банку, є поширення чуток про недоліки в діяльності банку, порушення його ліквідності та платоспроможності, безпідставне акцентування уваги в засобах масової інформації та виступах на окремих негативних випадках і подіях, що відбулись у банку, особливо пов’язаних із втратою ним коштів, поширення недостовірної та компрометуючої інформації стосовно окремих посадових осіб банку, тенденційне висвітлення окремих фактів із діяльності банку, модифікація виступів, публікацій, викладених посадовими особами банку у процесі проведення інформаційних заходів (прес-конференцій, круглих столів, спеціальних телевізійних передач).

Основними методами, які використовуються в інформаційних технологіях впливу і внаслідок дії яких для банків може настати ризик втрати іміджу та інші види ризиків, є:

* + інтрига — прихована послідовна система дій, яка через непряму мотивацію використовує сподівання, прагнення окремих людей, колективів чи соціальних груп на досягнення певної мети;
  + ажіотаж ― нарощування інтенсивності інформаційних повідомлень, зокрема й резонансних, і створення інформаційного завантаження середовища банку відомостями сенсаційного характеру;
  + мозаїка подій — штучно створені події, які «вбудовуються» в загальну тематику подій і подаються в інформаційне середовище банку;
  + провокація — «вбудовані» в загальну тематику мозаїки подій, факти, неправдиві твердження, які породжують в уявлення суб’єктів інформаційного середовища доволі значні для них події та у зв’язку з цим можуть мотивувати їх до певної поведінки щодо банку;
  + інсинуація — надання в інформаційне середовище певних відомостей з метою введення в оману його суб’єктів або ославлення певних подій, фактів чи осіб, пов’язаних з банком;
  + інспірація — поширення інформації, здатної викликати у відповідних суб’єктів негативну реакцію щодо банку, його діяльності чи певних його посадових осіб (підбурювання);
  + корекція — спеціально підібране доповнення інформаційних характеристик діяльності банку або подій, пов’язаних з ним, з метою формування чи утримання необхідного уявлення в суб’єктів інформаційного середовища про банк або зазначені події;
  + інкорпорація — вбудова видуманих або дійсних подій у загальну тематику подання інформації.

Особливістю поведінки сучасної громадськості є підвищена чутливість до інформаційного впливу, насамперед сприйняття інформаційних продуктів, що мають сенсаційний характер. Така довіра до слова та образу, логічного твердження ґрунтується на поступовому впровадженні у свідомість громадян неправильної істини про непогрішимість тверджень та ідей, що професійно пояснюються (нав’язуються) суспільству різноманітними експертами, критиками, аналітиками, оглядачами, черговими «борцями за краще майбутнє» та іншими особами. Як наслідок — громадяни стають «затиснутими» компетентністю таких осіб і в умовах тотального інформаційного перевантаження загальною інформацією та інформаційного вакууму в необхідній їм інформації починають вірити в ті відомості, які подаються в інформаційне середовище за допомогою відповідних технологій і методів. Тобто здійснюється відповідний вплив на свідомість, а отже, й на поведінку громадян, якими можуть бути працівники банку, його акціонери чи клієнти.

В такий же спосіб може поширюватись інформація, що створює ризик потрапляння банку в різні конфліктні ситуації. Ризик блокування роботи банку через численні перевірки його діяльності створюється поширенням в інформаційному середовищі та безпосередньо в органах контролю і нагляду негативної інформації про діяльність банку.

Під час аналізу ризиків інформаційного впливу насамперед вивчаються умови взаємовідносин банку із зовнішнім інформаційним середовищем, окремими його суб’єктами та власним персоналом . У процесі вивчення виявляються найбільш критичні відносини, з яких може надходити відповідна загроза й з’являтися певні ризики інформаційного впливу. На підставі результатів вивчення зазначених умов прогнозуються ймовірність та можливі терміни появи відповідного ризику впливу.

Оцінювання ризиків впливу спрямовується на визначення сфери діяльності та взаємовідносин банку, щодо яких може поширюватися негативна для банку інформація в той чи той період його діяльності, і в такий спосіб виникати певний ризик. Методик визначення розміру моральної чи матеріальної шкоди за результатами реалізації ризиків інформаційного впливу поки що не існує.

В процесі контролю ризиків здійснюється моніторинг інформаційного середовища банку з погляду виявлення ознак, які можуть указувати на передумови появи або безпосередню появу ризиків інформаційного впливу.

Для мінімізації інформаційних ризиків впливу банки вдаються до таких заходів:

1. періодичне поширення через різні інформаційні канали позитивної інформації про банк, оприлюднення його досягнень та активна реклама послуг;
2. періодичне інформування інформаційного середовища банку, насамперед персоналу, акціонерів і клієнтів про результати роботи банку;
3. формування банківського патріотизму у персоналу та акціонерів банку, пропаганда позитивного іміджу банку на ринку;
4. проведення спеціальних інформаційних операцій стосовно зміни об’єктів інформаційного впливу, дезорієнтації суб’єктів, що вдаються до заходів впливу, контрпропаганди та антикопроментації.

Серед ризиків інформаційного впливу особливу небезпеку становить ризик потрапляння банку під дію інформаційного тероризму, що є нині доволі ймовірним. Ураховуючи відчутні наслідки, до яких можуть призвести дії інформаційного тероризму, банки не повинні ігнорувати такий вид ризиків і мають виробляти відповідну політику щодо їх мінімізації. Насамперед має проводитися постійний аналіз та оцінювання таких ризиків. У процесі аналізу банки повинні визначити, наскільки уразливі до атак інформаційного тероризму їх комунікаційні системи та мережі, особливо засоби, мережі та інформації, які обслуговують платіжну систему. Має визначатися ступінь доступності інформаційних систем і мереж для атак інформаційного тероризму. Крім того, вивчається діяльність банку з погляду її вразливості щодо інформаційних атак компрометуючими матеріалами, визначається критична межа, за якої пропаганда та реклама банку будуть неефективними під впливом заходів інформаційного тероризму. Тобто встановлюється межа, за якою інформаційний вплив від актів тероризму призведе до руйнування іміджу банку, його взаємовідносин з клієнтами , породжуватиме конфліктні ситуації в банківських колективах та ін.

За результатами аналізу визначається ступінь уразливості діяльності банку та його інформаційних мереж і систем щодо атак інформаційного тероризму. Далі робиться припущення про те, які саме ризики інформаційного тероризму найімовірніші для банку (ризик порушення роботи, руйнування інформаційних мереж і систем банку , вилучення електронної інформації, викрадення коштів тощо чи ризики втрати іміджу банку від атак компрометуючими матеріалами) та можливі періоди чи обставини, за яких такі ризики будуть найімовірнішими.

* процесі оцінювання ризиків інформаційного тероризму визначається, які наслідки можуть настати для банку через інформаційні атаки терористів як з погляду економічного, так і з погляду іміджу банку. Тут можна формувати певні прогнози щодо таких наслідків (втрата клієнтів, звільнення провідних працівників з роботи в банку, втрата інформації, що має обмежений доступ, викрадення коштів з рахунків банку та його клієнтів, руйнування програмного забезпечення роботи інформаційної мережі банку та його інформаційних систем). Щодо конкретного визначення обсягу шкоди, завданої актами інформаційного тероризму, то тут поки що немає якихось підходів. Практично неможливо передбачити, а тим більше прорахувати обсяги можливої шкоди від таких дій. Тому під час оцінювання зазначених ризиків обмежуються можливими категоріями наслідків, які можуть наступи у зв’язку з інформаційними атаками терористів.

Під час контролю ризиків інформаційного тероризму виявляють ознаки підготовки терористичних актів, насамперед інформаційних атак. Крім того, вивчаються умови, за яких такі атаки можуть бути найімовірнішими, та з’ясовуються причини, що впливають на формування таких умов. Якраз виявлення та контроль зазначених умов і причин і є основним предметом роботи з контролю ризиків інформаційного тероризму. Головне завдання контролю полягає в тому, щоб звузити велику різноманітність варіантів дій терористів і контролювати найбільш можливі та небезпечні.

Мінімізація ж зазначених ризиків здійснюється проведенням заходів захисту технічного, програмного, криптографічного, апаратного, адміністративного, правового характеру власних інформаційних мереж і систем, а також заходів формування стійкого іміджу банку на ринку банківських послуг, пропаганди його послуг і реклами банківських продуктів. Крім того, проводиться низка заходів щодо згуртування колективів працівників банку, формування в них банківського патріотизму. Важливою частиною заходів мінімізації ризиків інформаційного тероризму є заходи з формування довіри до банку та його менеджменту з боку клієнтів та акціонерів.

На мінімізацію ризиків інформаційного тероризму мають спрямовуватися заходи з виявлення та перетинання інформаційних каналів, через які можуть здійснюватися інформаційні атаки.

Зауважимо, що дії, пов’язані з інформаційним тероризмом, є для банку не лише небезпечними, а й такими, від яких побудувати гарантовану систему захисту, що виключала б можливість проведення актів інформаційного тероризму, майже неможливо. Тому банки мають передбачати заходи своєї поведінки на випадок здійснення таких актів, передусім спрямовані на забезпечення виживання в умовах інформаційних атак, а також заходи щодо ліквідації їх наслідків.

Підсумовуючи, зазначимо, що інформаційні ризики необхідно розглядати не як окремо взяті, а разом з іншими ризиками банківської діяльності. Саме в такий спосіб можна прийняти правильне рішення щодо ризику проведення певної операції чи діяльності банку загалом: прийняти ризики, тобто погодитися на можливі втрати у процесі негативного впливу ризику; вжити заходів щодо зниження ризику; передати ризик іншому суб’єкту (компенсацію можливих збитків покласти, скажімо, на страхову компанію або трансформувати інформаційний ризик в інші види ризику, з нижчим рівнем втрат). Водночас за певних умов інформаційні ризики можуть бути головними серед тих ризиків, яких зазнає банк у своїй діяльності.

**9.3. Інформація з обмеженим доступом у банківській діяльності**

Ефективність захисту інформації великою мірою залежатиме від правильного визначення об’єкта захисту. З цієї точки зору важливим є правильне й однозначне визначення поняття «інформація». Відповідно до Закону України «Про інформацію» під інформацією розуміють документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі

Цивільний Кодекс України уточнює, що події та явища, про які іде мова у визначенні змісту зазначеного поняття повинні обов’язково мати місце (зараз чи в минулому) у суспільстві… і т.д. [68]. Водночас дещо відмінне визначення поняття «інформація» дає Закон України «Про захист економічної конкуренції» [57] згідно з яким інформація — це відомості в будь-якій формі і вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації, фотографії, голограми, кіно, відеоматеріали, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості. Незалежно від того, як подаються пояснення, всі правові норми вказують, що інформацією є документовані чи оголошені відомості, які можуть міститись на різноманітних носіях. Тобто захисту мають підлягати відомості, які є у розпорядженні банку і які відтворюють (характеризують) події та явища (діяльність), що відбуваються в банку.

Оскільки метою захисту інформації є обмеження доступу до неї, необхідно звернути увагу на структуру банківської інформації якраз з точки зору доступу до неї.

Закон України «Про інформацію» установлює, що за режимом доступу інформація поділяється на відкриту та з обмеженим доступом, а остання ж — на конфіденційну й таємну [60]. До конфіденційної інформації закон відносить будь-які відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Тут слід звернути особливу увагу на те, як законодавець регулює право власника інформації на її захист. Положення вищезазначеного закону передбачають, що громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаної за власні кошти, або такою, що є предметом їх ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, у тому числі належність її до категорії конфіденційної, та встановлюють до неї систему (способи) захисту. Таким чином, право встановлювати відповідний режим доступу до інформації мають особи (юридичні та фізичні), які володіють інформацією практично будь-якого характеру. За таких умов банк має право обмежити доступ до власної інформації, у тому числі і щодо якої він став володільцем в результаті її придбання або яка не є його власністю, але яка є предметом його інтересу (будь-які відомості, отримані банком у результаті проведення заходів інформаційного забезпечення його діяльності).

До таємної інформації законодавець відносить інформацію, яка містить відомості, що становлять державну та іншу, передбачену законом, таємницю (банківську , комерційну, військову, лікарську та ін.), розголошення якої завдає шкоди особі, суспільству, державі [60]. Виходячи з вищезазначеного структура банківської інформації за режимом доступу може мати такий вигляд (рис. 7.6).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  | Банківська інформація | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  | Відкрита | |  |
|  |  | З обмеженим доступом | | | | | | | |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Таємна | | | |  |  |  |  | Конфіденційна | | |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | | |  |  |  |  | | | | | |  |  |  |
| Банківська таємниця | | |  |  |  | Комерційна таємниця | | | | | |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



Рис. 7.6. Структура банківської інформації за режимом доступу

Безумовно, головну увагу банки мають приділяти інформації з обмеженим доступом, тому саме ця інформація в банку і є об’єктом захисту.

Найважливішою в системі захисту банківської інформації є таємна інформація: банківська та комерційна таємниця. Відповідно до ст. 60 Закону України «Про банки і банківську діяльність» [49] банківська таємниця — це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку

* процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

Виходячи з даного визначення можна зазначити, що власником інформації, яка становить банківську таємницю, є клієнт, а банк є лише її утримувачем і зобов’язаним суб’ єктом обмежувати доступ до неї. Слід також звернути увагу на те, що положення, присвячені основним засадам банківської таємниці, містяться і в Цивільному Кодексі України (ст. 1076) [68], згідно з якими банк гарантує таємницю банківського рахунку, операцій за рахунком та відомостей про клієнта. Водночас ч. 2 ст. 60 Закону України «Про банки і банківську діяльність» [49] вказує, що складовими банківської таємниці також є:

* відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
* операції, які були проведені на користь чи за дорученням клієнтів, здійснені ним угоди;
* фінансово-економічний стан клієнта;
* відомості про системи охорони банку та клієнтів;
* інформація про організаційно-правову структуру юридичної особи клієнта, її керівників, напрями діяльності;
* відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
* інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню (ст. 70 Закону України «Про банки і банківську діяльність» [49]);
* коди, що використовуються банками для захисту інформації. Банківську таємницю також становить інформація про банки

чи клієнтів, що збирається під час проведення банківського нагляду.

Слід звернути увагу, що статус банківської таємниці діє навіть тоді, коли клієнт припинив взаємовідносини з банком, оскільки законом не передбачено, що такий статус припиняється з втратою зазначених відносин.

Установивши перелік відомостей, що становлять банківську таємницю, законодавець разом з тим поклав на банк певні обов’язки щодо організації її захисту. Так, відповідно до ст. 61 Закону України «Про банки і банківську діяльність» [49] банки зобов’язані:

* обмежувати коло осіб, що мають доступ до інформації, яка становить банківську таємницю;
* організовувати спеціальне діловодство з документами, що містять банківську таємницю;
* застосовувати технічні засоби для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
* застосовувати застереження щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Крім того, керівники та службовці банку зобов’язані не розголошувати та не використовувати з вигодою для себе чи третіх осіб конфіденційну інформацію, яка стала їм відома при виконанні службових обов’язків. Це ж стосується і приватних осіб, які під час виконання своїх функцій або надання послуг банку отримали доступ до конфіденційної інформації.

Забезпечуючи захист банківської таємниці, законодавець установив і особливий порядок розкриття відомостей, які становлять таку таємницю, зокрема, у ст. 62 Закону України «Про банки і банківську діяльність» [49] визначено, що інформація, яка містить банківську таємницю, розкривається банками:

а) на письмовий запит або з письмового дозволу власника такої інформації;

б) за рішенням суду;

в) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України — на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи — суб’єкта підприємницької діяльності за конкретний проміжок часу;

г) органам Державної податкової служби України на їх письмову вимогу щодо наявності банківських рахунків;

д) центральному органу влади зі спеціальним статусом з питань фінансового моніторингу на його запит щодо фінансових операцій, пов’язаних з фінансовими операціями, що стали об’єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, а також учасників зазначених операцій;

є) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому виконанню відповідно до ЗУ «Про виконання провадження» стосовно стану рахунків конкретної

юридичної особи або фізичної особи, — суб’єкта підприємницької діяльності.

Крім того, банк має право надавати інформацію, що становить банківську таємницю, іншим банкам та Національному банку України в обсягах, необхідних при наданні кредитів, банківських гарантій; особі (у тому числі уповноваженій діяти від імені держави), на користь якої відчужуються активи та зобов’язання банку, при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації.

Законодавець не поширює обмеження щодо розкриття банківської таємниці на службовців Національного банку України чи уповноважених ними осіб, які здійснюють функції банківського нагляду або валютного контролю. Разом з тим Національний банк України має право розкривати інформацію, що містить банківську таємницю, Міністерству фінансів України у разі, коли держава бере участь у капіталізації цих банків. Відповідно до Правил зберігання, захисту, використання та розкриття банківської таємниці, затверджених постановою Правління Національного банку України 14 липня 2006 р. № 267 (далі — Правила) [46], останній має право для здійснення своїх функцій одержувати від банків інформацію, що містить банківську таємницю, та пояснення стосовно отриманої інформації і проведених операцій. При цьому банки зобов’язуються надавати Національному банку України інформацію, що містить банківську таємницю, у формі документів чи їх копій (договори, установчі документи, виписки за рахунками) під час проведення заходів банківського нагляду, пояснень щодо проведених банком операцій та з окремих питань банківської діяльності, звітів. Банки зобов’ язуються також забезпечити інспекторам Національного банку України та іншим уповноваженим ним особам вільний доступ до всіх документів та інформації, що містить банківську таємницю під час здійснення перевірок банків.

Розкриття інформації, яка становить банківську таємницю, здійснюється лише за письмовими запитами. Щодо державних органів законодавець установив вимоги до змісту та оформлення такого запиту, який:

♦ має бути викладено на бланку державного органу встановленої форми;

♦ повинен бути підписаний керівником державного органу (чи його заступником) та скріплений гербовою печаткою;

♦ має містити передбачені Законом України «Про банки і банківську діяльність» [49] підстави для отримання необхідної інформації;

♦ має містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації;

Відповідно до Правил до запитів державних органів має додаватися перелік найменувань конкретних юридичних осіб або прізвищ, імен, по-батькові фізичних осіб — суб’єктів підприємницької діяльності та номерів їх рахунків. Якщо зазначені вимоги до письмового запиту не виконані, то банк може відмовити в розкритті інформації, яка запитується і яка є банківською таємницею.

Письмовий запит чи дозвіл клієнта про розкриття його банківської таємниці складається у довільній формі. Письмовий запит (дозвіл) фізичної особи — клієнта банку має бути підписаний цією особою. Її підпис засвідчується підписом керівника банку чи уповноваженою ним особою та відбитком печатки банку чи нотаріально.

Письмовий запит (дозвіл) юридичної особи підписується керівником або уповноваженою ним особою та скріплюється печаткою юридичної особи.

Запит (дозвіл) клієнта може бути включено до договору про надання банківських послуг. Крім того, у договорі можуть бути викладені підстави та межі розкриття інформації, що становить банківську таємницю клієнта.

Відповідь на запити щодо розкриття інформації, яка становить банківську таємницю банк надає в терміни, визначені законами, якими керуються відповідні державні органи (для органів боротьби із організованою злочинністю — негайно, а якщо це неможливо, то в термін не пізніше до 10 днів, для органів прокуратури — у терміни, вказані в запитах таких органів). У разі відсутності в законах прямих вказівок на такі терміни банки зобов’язані розкрити інформацію, що становить банківську таємницю, або дати мотивовану відмову протягом десяти робочих днів з дня надходження запиту.

Банкам забороняється надавати інформацію про клієнтів іншого банку, навіть якщо вони зазначені в документах, договорах та операціях клієнтів якщо про таке не зазначено в дозволі клієнта іншого банку або у вимозі чи рішенні суду. При цьому надання інформації про рух коштів по рахунках здійснюється без зазначення контрагентів за операціями у разі надходження до банку запиту іншого банку щодо надання інформації, необхідної для забезпечення ідентифікації ним свого клієнта, з’ясування суті та мети проведення клієнтом певної операції або перевірки наданої клієнтом інформації, банк протягом десяти робочих днів з дня отримання запиту зобов’язаний безоплатно надати відповідну інформацію.

Виїмка документів, які містять інформацію, що становить банківську таємницю, проводиться лише за вмотивованою постановою судді в порядку, передбаченому Кримінально-процесуальним кодексом України. У цьому разі банк зобов’язаний виготовити копії документів, які підлягають виїмці. Зазначені копії разом з другим примірником протоколу виїмки залишаються в банку.

Інформування банком спеціально уповноваженого органу з розкриттям інформації, що становить банківську таємницю, здійснюється відповідно до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму» [53] та Положення про здійснення банками фінансового моніторингу, затвердженого постановою Правління Національного банку України [38].

Таким чином, банківська таємниця розкривається лише обмеженому колу осіб (власник таємниці, суд, органи прокуратури, Служба безпеки України, Міністерство внутрішніх справ України, Антимонопольний комітет України, Державна податкова служба України, центральний орган влади зі спеціальним статусом з питань фінансового моніторингу, органи ДПС, інші банки, державні нотаріальні контори та приватні нотаріуси, іноземні консульські установи, службовці Національного банку України, орган банківського нагляду іншої держави), лише в установленому законом та правовими документами Національного банку України порядку, в строго визначеному обсязі.

Відповідно до вимог Національного банку України банки зобов’язані за погодженням з клієнтом відображати в договорах, що укладаються між ними, застереження щодо збереження банківської таємниці та відповідальності за її незаконне розголошення або використання [46].

Працівники банків, службові особи, які відповідно до своїх посадових обов’язків обізнані з інформацією, що становить банківську таємницю зобов’язані не розголошувати та не використовувати її, у тому числі і на користь третіх осіб. Суб’єкти, які мають доступ до банківської таємниці, у тому числі і банки, у своїх нормативних документах повинні встановити особливий порядок реєстрації, використання, зберігання та доступу до документів (у тому числі й електронних), що містять банківську таємницю.

Узагальнюючи викладене, необхідно вказати, що основними особливостями банківської таємниці як інформації з обмеженим доступом є такі: зміст банківської таємниці визначено законом, законодавець установив вичерпний перелік відомостей, які становлять банківську таємницю, зміст банківської таємниці для всіх банків є одним і тим же; банківська таємниця не є різновидом інших таємниць, а становить самостійний вид таємної інформації; інформація, що становить банківську таємницю, стосується насамперед клієнтів банків, причому режимом таємності охоплюються відомості, які банки отримують від своїх клієнтів офіційно, у процесі безпосереднього здійснення своєї діяльності; розголошення такої інформації обов’язково має завдавати шкоди клієнту. Слід також зазначити, що інформацію про клієнта банк може отримати як безпосередньо від нього, так і від інших (третіх) осіб, з якими банк вступає в певні взаємовідносини. Причому останні можуть і не бути клієнтами банку, наприклад його контрагенти. Тому інформація, яка становить банківську таємницю може міститись як у документах, що характеризують взаємовідносини банку і клієнта, так і в документах стосовно взаємовідносин банку з особами, які надають йому відповідні послуги.

Характеризуючи інформацію з обмеженим доступом банку слід звернути увагу на те, що банк як юридична особа, що здійснює господарську діяльність виробляє свою власну інформацію, яка може бути для нього досить важливою та цінною. У банку при розробленні нових технологій банківського виробництва, нових банківських продуктів створюються насичені різноманітними відомостями інформаційні об’єкти, які, за банківським законодавством, не можуть бути банківською таємницею. Тому банк має захищати такі об’єкти застосуванням інших видів таємниць, зокрема комерційної.

Відповідно до ст. 505 Цивільного Кодексу України [68] комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її

складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв’язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Згідно зі ст. 162 Господарського Кодексу України [4] суб’єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умови, що ця інформація має комерційну цінність у зв’язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до охорони її конфіденційності. Законодавець також установив обмеження до переліку відомостей, які можуть становити комерційну таємницю. Зокрема, відповідно до постанови Кабінету Міністрів України від 9 серпня 1993 р. № 611 комерційну таємницю не можуть становити:

* установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
* інформація за всіма встановленими формами державної звітності;
* дані, необхідні для перевірки обчислення і сплати податків та інших обов’язкових платежів;
* відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями і посадами, а також наявність вільних робочих місць;
* документи про сплату податків і обов’язкових платежів;
* інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров’ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
* документи про платоспроможність;
* відомості про участь посадових осіб суб’єкта господарювання в кооперативах, малих підприємствах, спілках,
  + - відомості, що відповідно до чинного законодавства підлягають оголошенню.

Таким чином, основними ознаками комерційної таємниці є: комерційна цінність інформації, склад відомостей, що становлять комерційну таємницю визначає їх власник, інформація є невідомою третім особам і до неї немає вільного доступу, володілець інформації вживає заходів для її охорони і таємності, інформація не повинна бути об’єктом інших таємниць.

Виходячи з вищезазначеного кожен суб’єкт господарювання, у тому числі і банк, самостійно визначає склад відомостей, які становлять його комерційну таємницю. Тобто зміст комерційної таємниці на відміну від банківської таємниці у кожному банку буде різним. Одні й ті самі відомості можуть бути в одному банку таємними, а в іншому — зовсім ні. За таких умов великого значення набуває процес формування переліку відомостей, що становлять комерційну таємницю. З одного боку, зазначений перелік повинен надійно захищати цінну для банку інформацію, а з другого — не обмежувати його інформаційну діяльність на ринку банківських послуг. Практика роботи банків має певні приклади організації роботи щодо визначення відомостей, які становлять комерційну таємницю. Узагальнення цієї практики дало можливість сформувати такий варіант.

* + - * банку відповідним наказом визначається комісія, на яку покладається завдання складання переліку відомостей, що становлять його комерційну таємницю. Водночас цим наказом керівники всіх банківських підрозділів зобов’язуються виокремити відомості по своїх напрямах роботи, які, на їх погляд, мають обмеження доступу до них через надання їм категорії комерційної таємниці. Пропозиції підрозділів надходять до зазначеної вище комісії, яка їх обробляє, перевіряє щодо відповідності вимогам чинного законодавства, формує й узгоджує в підрозділах остаточний перелік зазначених відомостей. Цей перелік надається керівникові банку і відповідним наказом (постановою Правління банку) вводиться в дію. Одночасно в наказі (постанові) визначаються особи, яким інформація, що становить комерційну таємницю, може розкриватися в повному обсязі. Як правило, це члени Правління та Спостережної ради банку. Крім того, наказом (постановою) визначаються завдання щодо організації в банку системи захисту інформації з обмеженим доступом.

Конфіденційна інформація як вид інформації з обмеженим доступом, що є в банку, може мати подвійний характер. З одного боку, це інформація банку, яка з тих чи тих причин не отримала категорії таємної, та інформація про персонал банку, що зберігається в особових справах та документах про оплату праці. Якщо перелік відомостей, що становить конфіденційну інформацію банку, визначається в тому самому порядку, що й для комерційної таємниці, то зміст конфіденційної інформації про працівників дається у Законі України «Про інформацію» та забезпечується відповідно до Закону України «Про захист персональних даних» і Рішення Конституційного суду України від 30 листопада 1997 р. № 5-зп (справа К.Г. Устименка). Зокрема, до конфіденційної інформації про особу належать відомості про освіту, сімейний стан , релігійність, стан здоров’я, дату і місце народження, майновий стан, інші персональні дані (адреса, рік народження, національність). Банк зобов’язаний забезпечити конфіденційність таких даних, зібраних ним на своїх працівників під час прийняття та у процесі їх роботи в банку.

За посягання на банківську та комерційну таємницю законодавство України передбачає кримінальну, адміністративну, цивільну та дисциплінарну відповідальність.

Тут слід виділити дві основні групи суб’єктів посягань на інформацію банку. Особи, що незаконно заволоділи інформацією банку та його працівники , контрагенти, партнери й державні службовці тобто особи, що правомірно отримали таку інформацію, але порушили зобов’язання щодо збереження її в таємниці.

Кримінальна відповідальність передбачена за умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності (під поняттям «істотна шкода» розуміють шкоду, яка у матеріальному вираженні дорівнює або є більшою за мінімальний розмір великої шкоди, що дорівнює — 300 неоподатковуваних мінімумів доходів громадян) [27, ст. 231].

Стаття 232 Кримінального кодексу України [27] передбачає, що кримінальна відповідальність настає також за умисне розголошення комерційної або банківської таємниці, без згоди її власника, особою, якій ця таємниця відома у зв’язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб’єкту господарської діяльності.

Адміністративна відповідальність може наступи у разі отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації чи майну банку або його клієнтові [23, ст. 164 (3)].

Цивільно-правова відповідальність настає за порушення договірних зобов’язань майнового характеру або за заподіяння майнової чи немайнової (моральної) шкоди, і може виражатись у позбавленні правопорушника певних благ матеріального характеру, у зміні невиконаного обов’язку новим, у приєднанні до невиконаного обов’язку нового, додаткового.

Цивільний кодекс України відносить інформацію до об’єктів цивільних прав. Стаття 200 Кодексу [68] визначає, що суб’єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями.

Крім того, ст.49 Закону України «Про інформацію» [60] закріплює, що матеріальна чи моральна шкода, завдана фізичним або юридичним особам правопорушенням, учиненим суб’єктом інформаційної діяльності, відшкодовується добровільно або на підставі рішення суду.

Незаконне використання, збирання інформації без дозволу її законного власника спричиняє настання відповідальності за порушення немайнових прав, що виражається у заподіянні моральної шкоди. Крім того, відповідно до ст. 1076 Цивільного кодексу України [68] у разі розголошення банком відомостей, що становлять банківську таємницю, клієнт має право вимагати від банку відшкодування заподіяних збитків та моральної шкоди.

Дисциплінарна відповідальність може наступи для працівників банку за скоєння дисциплінарних проступків, які виявляються в порушенні трудової дисципліни.

Тут слід зазначити, що притягнення до дисциплінарної відповідальності працівника банку може відбуватися: а) якщо ним порушено вимоги Посадової інструкції, якою передбачено обов’язок працівника зберігати, не розголошувати, не використовувати на власний розсуд і т. п. певні відомості; б) якщо в нормативних документах, які регулюють технології банківського виробництва і якими має керуватися працівник, зазначено правила поводження з інформацією, а він їх порушує; в) якщо подібні правила передбачено в умовах трудового договору. Так, при укладанні трудового договору згідно зі ст. 21 Кодексу законів про працю України працівник зобов’язується виконувати умови внутрішнього трудового розпорядку, однією з вимог якого може бути зберігання в таємниці певної інформації. Крім того, може бути передбачено також укладання окремої угоди про конфіденційність. Разом з тим необхідно зауважити, що притягнення працівників банку до відповідальності за посягання на інформацію чи порушення правил поводження з нею має здійснюватися за певним порядком. Як правило, прийняттю рішення про притягнення працівника до відповідальності має передувати проведення службового розслідування, метою якого є установлення обставин, умов і причин виявлення фактів посягання на інформацію банку, встановлення осіб безпосередньо причетних до цього, з вини або за сприяння яких мали місце такі факти , вироблення пропозицій і рекомендацій щодо усунення причин і недоліків у роботі банку та відшкодування заподіяних ним збитків, притягнення до відповідальності осіб, які спричинили або сприяли витоку інформації.

Службові розслідування проводяться у разі виявлення фактів несанкціонованого витоку інформації банку з обмеженим доступом, унаслідок чого йому заподіяно матеріальної шкоди або це вплинуло на погіршення його іміджу.

Рішення про проведення службового розслідування приймається керівником банку, його заступниками, головним бухгалтером, керівниками установ банку.

Найчастіше службові розслідування проводяться фахівцями служби безпеки, а за відсутності таких фахівців спеціально призначеними керівником банку особами. Коли для проведення службового розслідування необхідно залучити фахівців інших підрозділів можуть створюватися відповідні комісії.

До участі у проведенні службового розслідування не повинні залучатися посадові особи, якщо мають місце обставини, які можуть викликати їх особисту зацікавленість у результатах розслідування.

При проведенні службових розслідувань особи, які залучені до цього, мають право:

* отримувати від працівників банку усні та письмові пояснення щодо факту, який розслідується, а також консультації фахівців банку з питань службового розслідування;
* вивчати відповідні документи як у паперовому, так і в електронному вигляді, знімати з них копії та отримувати
* збирати з дотриманням вимог законодавства інформацію, необхідну для встановлення об’єктивної суті подій, фактів, випадків, осіб, причетних до них, робити відповідні запити до підрозділів і установ банку.

В окремих випадках фахівці або голова комісії можуть отримувати роз’яснення у посадових осіб та керівництва установ банку.

З дозволу керівника банку (установи банку) фахівцями (комісіями), які проводять службове розслідування, можуть подаватися запити до інших установ, організацій та правоохоронних органів.

Особи, які проводять службове розслідування, несуть персональну відповідальність згідно з чинним законодавством за повноту та об’єктивність висновків, зроблених ними за результатами розслідування, розголошення інформації, отриманої у процесі розслідування.

Фахівці (члени комісії), які проводять службове розслідування, забезпечуються необхідними для роботи документами, програмно-апаратним, технічними засобами, автотранспортом та іншим обладнанням і технікою. Працівники банку зобов’язані надавати їм допомогу в установленні причин та умов виникнення фактів, за якими проводиться службове розслідування, давати пояснення, інформацію та консультації стосовно питань розслідувань.

За результатами службового розслідування складається акт або доповідна записка, де зазначається:

* суть та обставини, що характеризують факти, випадки, за якими проводиться розслідування, учасники та їх дії, у тому числі такі, що суперечать установленим правилам, посадовим обов’язкам, нормативно-правовим документам, які діють у банку, умови, що сприяли скоєнню порушень або іншим діям;
* характеристика шкоди, заподіяної банку, прогноз її впливу на його подальшу діяльність;
* причини, що призвели до таких фактів та особи, з вини яких допущено ці факти;
* заходи щодо відшкодування заподіяної банку шкоди, захисту честі та гідності посадових осіб банку, пропозиції щодо усунення причин та умов, що сприяли виникненню фактів, загрози.

Посадова особа, яка призначила службове розслідування у десятиденний термін розглядає акт або доповідну записку та приймає відповідне рішення. У разі необхідності така посадова особа може заслухати особу, яка проводила службове розслідування, або членів комісії, а також осіб, з вини яких допущено те чи те порушення.

Матеріали службового розслідування є підставою для прийняття керівником банку рішення про притягнення винних осіб до дисциплінарної або іншої відповідальності згідно з чинним законодавством.

* певних випадках за рішенням керівника банку може бути ініційовано подання матеріалів до правоохоронних органів, суду, Антимонопольного комітету України тощо.

**9.4. Система захисту інформації в банку**

Як інформаційний об’єкт банк являє собою єдиний комплекс компонентів, пов’язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Зазначені компоненти в процесі функціонування банку можуть змінюватися, на них можуть здійснювати вплив різного роду внутрішні та зовнішні чинники, які складно прогнозувати та оцінювати. Велику кількість компонентів, які формують банк як об’єкт інформатизації, можна подати сукупністю чотирьох груп: персонал, технічні засоби інформатизації, програмне забезпечення, документи. Зазначені групи у своєму функціонуванні зазнають впливу різного роду специфічних факторів і, взаємодіючи між собою, впливають одна на одну, формуючи відповідний стан інформаційної безпеки банку. Як показує практика, робота з кожною з цих груп щодо забезпечення інформаційної безпеки чи , зокрема, щодо захисту інформації призводить до покращення якостей безпеки по одних параметрах

1. погіршення по інших, що вимагає комплексного підходу до забезпечення інформаційної безпеки банку.

Висока інформатизація та автоматизація виробничого процесу банку не виключає звичайних взаємовідносин персоналу банку з його клієнтами, а значні обсяги електронних документів аж ніяк не призводять до зменшення документооборот паперових носіїв інформації. Тобто забезпечення інформаційної безпеки і такої її

197

складової, як захист інформації, неможливо здійснити лише організаційними чи технічними заходами, або, скажімо, програмними чи криптографічними. Дії щодо забезпечення інформаційної безпеки повинні являти собою регулярний процес, що здійснюється на всіх напрямах діяльності банку на основі комплексного застосування всіх заходів і засобів безпеки. При цьому засоби, заходи та методи безпеки найбільш раціональним способом об’єднуються в єдиний цілісний механізм не тільки для захисту від зловмисників, а й від некомпетентних, недобросовісних працівників банку та різних непередбачуваних ситуацій. Тобто забезпечення інформаційної безпеки як і кожної

1. її складових мусить мати системний та комплексний характер. Системність заходів інформаційної безпеки має передбачати таке: високий ступінь захищеності інформації банків як головну

характеристику її якісного стану; заходами безпеки охоплюються всі інформаційні ресурси

банку всієї його структури; діяльність щодо забезпечення інформаційної безпеки є

безперервною і плановою, на основі єдиної концепції безпеки; забезпечення інформаційної безпеки здійснюється у тісній

єдності з поточною діяльністю банку.

Комплексний характер системи забезпечує оптимізацію заходів і засобів, що використовуються нею задля створення необхідного балансу вимог і можливостей інформаційної безпеки банку. Комплексний підхід обумовлюється ще й тим, що загрози інформації банку мають різноманітний характер, перекриття яких потребує застосування багатьох, різних за призначенням заходів і засобів. Крім того, значний спектр банківських операцій, велика регіональна розпорошеність банківських установ, специфічність поведінки персоналу та клієнтів банків створюють суттєві особливості діяльності банків і вимагають адекватної реакції їх систем безпеки. Водночас адекватність реакції передбачає узгоджені дії всіх сил і засобів безпеки, що можливо лише за системного підходу. Більше того, забезпечення безпеки в сучасних умовах має здійснюватись як на технологічному, так і на логічному рівнях, що має забезпечувати врахування всіх факторів і особливостей, які впливають на безпеку банку, а також усіх компонентів інформаційної роботи: збору, обробки, зберігання, передавання, використання інформації. За таких умов системність та комплексність банківської безпеки, у тому числі й у сфері захисту інформації є обов’язковою умовою її високої ефективності.

198

Система захисту інформації банку — це організована сукупність об’єктів і суб’єктів захисту інформації, заходів, методів і засобів, що використовуються для захисту. Основна мета створення системи захисту інформації — забезпечення надійності зберігання і використання інформації в банку.

Ураховуючи складність системи захисту інформації банку, необхідність її функціонування в умовах невизначеності, побудова такої системи має базуватися на відповідних принципах.

Принцип законності передбачає відповідність заходів захисту інформації, що використовуються в банку законодавству України. Інший принцип — повнота інформації, що захищається, обумовлює необхідність захисту не тільки інформації з обмеженим доступом, а й іншої банківської інформації, втрата якої може завдати шкоди банку. Реалізація даного принципу дає можливість забезпечувати захист усіх об’єктів інтелектуальної власності банку.

Відповідно до принципу обґрунтованості захисту інформації визначається доцільність надання відповідного грифу певним відомостям, виявляються економічні та інші наслідки, що можуть наступи від застосування заходів захисту інформації. Це, у свою чергу, дозволить більш раціонально та продуктивно здійснювати витрати на захист інформації.

Принципи повної участі та персональної відповідальності передбачають поширення обов’язку захищати інформацію на всіх осіб, що працюють з інформаційними продуктами (програмами, документами, характеристиками і т. п.) банку, а також вимагають відповідальності кожного із працівників банку чи інших осіб за порушення заходів захисту інформації.

Принцип превентивності передбачає плановість заходів захисту інформації, застосування їх з метою виявлення, перетинання та локалізації загроз інформації банку.

Важливе значення у захисті інформації має політика безпеки банку. Політика безпеки — це прийнята в банку сукупність норм, правил, рекомендацій згідно з якими будується система його безпеки та управління нею. Вона реалізується за допомогою організаційних заходів і програмно-технічних засобів, які визначають архітектуру системи захисту та за допомогою засобів управління механізмами захисту. Для кожного конкретного банку політика безпеки є індивідуальною і залежить від особливостей технологій банківського виробництва, змісту інформаційної діяльності та умов роботи банку.

199

Відповідно до прийнятої в банку політики безпеки проводяться організаційні заходи щодо створення системи захисту інформації. Нині в банках напрацьовано відповідний алгоритм роботи з організації системи захисту інформації, який включає такі дії:

визначення вразливості інформації банку (виявлення в інформаційній системі банку місць, використання яких зловмисниками може завдати шкоди інформаційним ресурсам і в цілому банку);

визначення мети, завдань та об’єктів захисту інформації; вибір форм, способів і засобів захисту інформації; формування елементів системи захисту інформації, її сил

та засобів; створення нормативної бази банку з питань захисту

інформації; планування функціонування системи, використання нею

сил та засобів захисту інформації у відповідності до особливостей діяльності банку;

забезпечення взаємодії всіх елементів системи між собою та з іншими компонентами, які згідно з політикою безпеки можуть бути задіяні для захисту банківської інформації;

забезпечення функціонування системи (матеріальне, фінансове, наукове та ін.);

контроль стану захищеності інформації, надійності функціонування системи та ефективності заходів, що вживаються нею.

Вразливість інформації є одним із головних показників стану

* захищеності. Тому визначення ступеня вразливості інформації

1. процесі організації її захисту має досить суттєве значення. Зміст роботи щодо визначення вразливості інформації показано на рис. 7.7.

Результати, отримані у процесі визначення уразливості інформації, використовуються для встановлення складу інформації, яка підлягає безпосередньому захисту тобто об’єктів захисту. Загальний підхід тут полягає у тому, що захисту, підлягає вся інформація з обмеженим доступом і найбільш важлива частина відкритої інформації. При цьому інформація з обмеженим доступом повинна захищатися від втрати і несанкціонованого витоку, а відкрита — тільки від втрати.

200

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Аналіз цінності** |  | **Аналіз захищеності** |  | **Аналіз політики** |
| **інформації** |  | **інформації** |  | **захисту інформації** |
|  |  |  |  |  |

— актуальність інфор- — можливості технічних та — організація захисту

мації на даний час;програмних засобів, що вико- інформації в банку;

— роль конкретної ін- ристовуються для захисту ін- — ефективність захо-

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| формації у певній бан- | | | формації, їх стійкість; | дів захисту | інформа- |
| ківській | операції | або | — категорія інформації (кон- ції; | |  |
| планах розвитку банку; | | | фіденційна, таємна); | — характеристика по- | |
| — зацікавленість у по- | | | — вид інформації (знання, до- ведінки | | персоналу |
| дібній | інформації | ін- | кументи, електронна інформа- щодо збереження ін- | | |
| ших суб’єктів; | |  | ція); | формації; |  |

— наслідки втрати ін- — характеристика місць збері- — стан забезпечення

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| формації | | гання носіїв інформації, | | мож- | системи захисту інфор- | |  |
| *Чи є інформація цін-* | | ливість доступу до них; | |  | мації | |  |
| — можливість зміни або зни- | | | *Можливість витоку* | |  |
| *ною для осіб зацікавле-* | | щення інформації | |  |  |
| *них у її отриманні* | |  |  |  | *інформації з ініціати-* | |  |
|  |  | *Вірогідність несанкціоновано- ви працівників банку* | | | | |  |
|  |  | *го доступу до носіїв інформа-* | | |  |  |  |
|  |  | *ції* | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Висновок** | | **Висновок** | |  | **Висновок** | |  |



Рис. 7.7. Визначення уразливості інформації з обмеженим доступом в банку

Банки, як правило, не передбачають захисту відкритої інформації. Але ж відкритість інформації не лишає її цінності, а цінна інформація, безумовно, має захищатися, насамперед від втрати її. Захист такої інформації здійснюється за допомогою реєстрації її носіїв, обліку, контролю наявності. Разом з тим захист відкритої інформації не повинен обмежувати її загальнодоступність, але доступ до неї має бути контрольованим із дотриманням відповідних вимог щодо її збереження. Тобто відкрита інформація є об’єктом захисту, і стосовно неї мають проводитися певні заходи в системі захисту інформації. Загальною ж основою для вибору об’єкта захисту є цінність інформації. Критеріями ж цінності можуть бути: необхідність інформації для правового забезпечення діяльності банку; необхідність інформації для здійснення виробничої діяльності банку; необхідність інформації для ефективного управління діяльністю банку, об’єктивного прийняття управлінських рішень, організації прибуткової діяльності банку; необхідність інформації для формування ресурсної бази банку та забезпечення його безпеки. Разом з тим основним і визначальним критерієм у

201

виборі об’єкта захисту інформації є можливість отримання від використання певної інформації переваг за рахунок її невідомості третім особам. Критерій має дві складові: невідомість інформації для третіх осіб і отримання вигоди через що невідомість.

Водночас система захисту інформації банку у своєму функціонуванні має конкретний характер і потребує однозначної конкретизації об’єктів захисту. Інформація, на яку спрямовуються зусилля системи захисту не існує сама по собі, а фіксується (відбивається) у відповідних матеріальних об’єктах або пам’яті людей , тобто вона існує на відповідних носіях. Таким чином, обираючи об’єкт захисту, ми маємо визначити певний перелік носіїв невідомої третім особам інформації, за рахунок якої банк отримує певні переваги у своїй діяльності. Тобто це можуть бути відповідні документи, матеріали (у тому числі магнітні, магнітооптичні, оптичні та інші засоби), вироби (засоби відображення, обробки, відновлення, передання інформації), мережі зв’язку та передання даних, а також працівники банку. Захист цих об’єктів має здійснюватися регулюванням доступу до них, установленням відповідного порядку їх використання (діяльності) та формуванням умов зберігання. Якраз ці заходи і складають структуру системи захисту інформації.

Зазначені заходи в системі захисту інформації здійснюється за допомогою технічних, програмних і правових засобів. До технічних засобів регулювання доступу можна віднести кодовані замки на вході в приміщення, міститься відповідна інформація, установлення засобів і систем пропуску на територію банку, спеціальні прилади та пристрої, що регулюють доступ до інформації, яка зберігається в комп’ютерах. За допомогою програмних засобів розмежовується доступ до інформації в інформаційних комп’ютерних системах і мережах банку. Правові засоби є загальними, вони встановлюють як порядок роботи з інформаційними ресурсами банку, так і умови та правила використання технічних і програмних засобів захисту інформації.

На сьогодні вітчизняними банками напрацьовано певний досвід формування нормативно-правової бази з питань захисту інформації.

Насамперед відповідні положення про захист комерційної таємниці включаються до Статуту банку. Зокрема, у них вказується право банку на:

* комерційну таємницю;

202

* самостійне визначення складу й обсягу відомостей, що становлять комерційну таємницю і конфіденційну інформацію банку;
* захист комерційної таємниці.

Такі положення, зафіксовані в Статуті, дають банку юридичне право організовувати захист таємниць банку; включати вимоги щодо захисту комерційної таємниці в усі договори й угоди комерційного характеру; домагатися відшкодування збитків, заподіяних посяганням на інформацію; видавати нормативні та інші документи з питань захисту банківської і комерційної таємниці; створювати відповідні підрозділи захисту таємниць банку.

Одним із важливих нормативних документів банку з питань захисту інформації є Положення про комерційну таємницю і конфіденційну інформацію, в якому дається перелік відомостей, що становлять комерційну таємницю та конфіденційну інформацію банку, порядок їх визначення, терміни дії певної категорії обмеження та умови їх зняття. У цьому документі вказуються також обов’язки персоналу по дотриманню режиму захисту інформації та відповідальність за його порушення.

Порядок захисту інформації, організації роботи з нею визначається відповідно до Положення про організацію роботи з інформацією, що становить банківську і комерційну таємницю та

* конфіденційною. Положення передбачає: права співробітників банку та інших осіб щодо отримання інформації з обмеженим доступом, обов’язки посадових осіб і службовців банку щодо роботи з грифованими документами, виробами та засобами, правила ведення 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; порядок доступу на засідання і наради, де обговорюються питання, в яких є комерційна таємниця банку; інші питання, що регулюють правила доступу до інформації з обмеженим доступом.

До нормативної бази банку з питань захисту інформації також відносять зобов’язання службовців банку про зберігання комерційної таємниці, угоди про конфіденційність з клієнтами, партнерами та іншими суб’єктами, з якими банк вступає у правовідносини, різного характеру пам’ятки, інструкції, заяви тощо.

До цього типу документів належить внутрішній розпорядок

203

роботи та розпорядження щодо організації доступу в установу банку.

Як приклад, нижче наводиться перелік нормативних актів одного із українських банків щодо захисту його інформації з обмеженим доступом.

1. Положення про комерційну таємницю і конфіденційну інформацію банку та правила їх зберігання.
2. Інструкція про порядок підготовки, обліку, обігу, зберігання та знищення документів, справ, видань і матеріалів, що містять банківську та комерційну таємницю банку.
3. Інструкція про порядок виконання документів, що надходять у банк від правоохоронних органів, судів та інших державних установ.
4. Положення про забезпечення безпеки при наданні послуг за міжнародними банківськими платіжними картками.
5. Інструкція про порядок надання доступу користувачам до автоматизованих банківських систем.
6. Інструкція про проведення службових розслідувань в установах банку.
7. Положення про порядок підготовки, надсилання, обробки та зберігання електронних документів при використанні електронної пошти.
8. Інструкція щодо дій у разі компрометації криптографічних ключів в установах банку.
9. Інструкція зі знищення на електронних носіях документів, які містять ключові дані, конфіденційну інформацію, банківську або комерційну таємницю.
10. Положення про технічний захист інформації у банку.
11. Технологічна інструкція служби фінансової безпеки.
12. Положення про порядок одержання доступу до локальної обчислювальної мережі та ресурсів систем електронної обробки інформації.
13. Положення про режимні приміщення банку.

Таким чином, нормативна база безпеки не потребує якихось великих зусиль і витрат для її створення, але вона є основою для правового захисту як таємниць банку, так і всієї його діяльності.

Зазначені вище заходи системи захисту інформації банку формують відповідні завдання системи, повний зміст яких наведено в Додатку 3.

Особливим об’єктом захисту інформації банку є його персонал, у пам’ яті якого зосереджено величезний масив інформації, у тому числі і такої, що є надзвичайно цінною для

204

банку. У цьому сенсі працівники банку як жодна інформації характеризуються з точки зору її захисту позитивними та негативними рисами. Позитивним є те, що без згоди банку із пам’яті працівників ніяка інформація ні за яких умов не може бути вилучена, вони можуть об’єктивно оцінювати важливість інформації, якою володіють, і відповідно до цього ставитися до неї, вони також можуть ранжувати споживачів їхньої інформації, знаючи кому і яку інформацію можна довірити.

Негативним є те, що працівники можуть помилятися в щирості таких споживачів, бути не повністю компетентним у важливості інформації, якою володіють, їх дії багато в чому залежать від емоційного стану, характеру, власних потреб. За цих умов система захисту інформації щодо такого об’єкта захисту, як працівники банку має вживати заходи регламентування роботи працівників з інформацією, установлювати відповідні обмеження та заборони, а також у певний спосіб мотивувати поведінку працівників до дотримання встановленого режиму захисту інформації.

Регламентування роботи працівників з інформацією банку здійснюється через:

1. визначення осіб, яким надано право доступу до інформації банку в повному обсязі;
2. визначення осіб, яким надано право доступу до інформації банку в частині, що їх стосується;
3. установлення порядку доступу до інформації банку та повноважень осіб щодо її використання;
4. визначення порядку та правил використання носіїв інформації в процесі банківської діяльності працівниками банку;
5. визначення порядку та правил зберігання інформації, вироблення, обліку та пересилання електронних і паперових документів.

Заборони та обмеження досягаються виключенням фізичної та іншої можливості доступу до інформації, яка згідно з повноваженнями працівників банку йому не повинна їм доводитися. Крім того, обмеження доступу здійснюється і виконанням певних завдань чи робіт окремими частинами групою працівників, кожен з яких не обізнаний зі змістом інформації, яка повністю характеризує завдання (обсяг роботи).

Мотивації у забезпеченні захисту інформації, якою володіють працівники, формуються через зацікавленість працівників у виконанні ними заходів захисту. Основними методами тут є: формування у працівників банківського патріотизму; матеріальна

205

та кар’єрна вигода дотримання заходів захисту; відповідне ставлення колективу до осіб, що порушують установлені в банку правила захисту інформації, зручність виконання зазначених заходів і т. п.

Важливе значення мають заходи протидії потраплянню працівників банку під вплив осіб, зацікавлених в отриманні банківської інформації (конкурентів, промислових шпигунів і т. п.). Як правило, підрозділи безпеки порушують у банках відповідні методики роботи з персоналом щодо протидії витоку інформації, якою володіють працівники банків. Зазвичай до змісту таких методик включаються такі питання:

визначення готовності кандидатів на роботу в банк до зрадництва, легкої наживи, аморальної поведінки;

формування сприятливих умов роботи кожному із працівників;

формування умов та можливостей максимального заробітку та кар’єри;

вжиття заходів гарантованого захисту інформаційних об’єктів та регламентування доступу до джерел інформації;

установлення відповідальності за посягання на інформацію банку;

пропаганда захисту таємниць банку як однієї з умов ефективного його розвитку та забезпечення добробуту працівників, вжиття заходів із профілактики недобросовісної їх поведінки;

контроль роботи, поведінки та зв’язків працівників банку, обізнаних з його таємницями;

установлення в банку суворого пропускного режиму;

контроль наявності документів, стану документообігу, у тому числі й у комп’ютерних мережах банку, переговорів через засоби зв’язку, установлені в банку;

аналіз можливих способів посягання на інформацію банку та методів протидії їм з практики роботи інших банків.

1. питань захисту інформації працівники банку зобов’язані:

* зберігати в таємниці всі службові відомості, з якими вони ознайомлені у зв’язку зі своєю роботою в банку;
* виконувати встановлений порядок і правила роботи з документами та інформацією, які мають таємний або конфіденційний характер;
* знати, кому із працівників і в якому обсязі дозволено працювати з відомостями обмеженого доступу;

206

* на вимогу працівників підрозділу безпеки банку надавати документи, матеріали, електронні носії інформації для перевірки;
* не користуватися на робочому місці власними засобами зберігання та передання інформації, фото- та відеоапаратурою;
* дотримуватись установлених правил передання (пересилання, обробки) інформації службових документів, ведення службових переговорів, у тому числі і через засоби зв’язку;
* негайно доповідати безпосередньому керівникові про втрату документів службового призначення, особливо тих, що мають гриф таємності;
* своєчасно інформувати підрозділ безпеки банку про спроби сторонніх осіб отримати інформацію банку таємного чи конфіденційного характеру.

Захист інтересів банку у взаємовідносинах з персоналом, допущеним до його таємниць, здійснюється через правове закріплення таких взаємовідносин у відповідних документах (Додаток 4).

При звільненні працівників з роботи в банку захист інформації здійснюється через виконання таких заходів: отримання від працівників, які звільняються, усіх матеріалів конфіденційного та таємного характеру, що обліковуються за ним, з оформленням відповідного акта; передання працівниками, що звільняються, перепусток, печаток, штампів, ключів, сейфів тощо уповноваженим від банку особам; проведення бесіди з працівниками, які звільняються з роботи, про необхідність збереження в таємниці всіх відомостей таємного та конфіденційного характеру, які були їм відомі під час роботи в банку, підписання зобов’язань про нерозголошення ними цих відомостей; попередження працівників про відповідальність за розголошення чи використання таємних та конфіденційних відомостей, що належать банку. Підписані працівниками зобов’язання зберігаються в їх особових справах протягом усього терміну зберігання справ.

Практика забезпечення безпеки банківської діяльності знає приклади, коли витік цінної для банку інформації здійснювався мимовільно, без злого наміру, через недоопрацювання певних питань чи не врахування особливостей ситуації, яка склалась навколо банку. Система захисту інформації у зв’язку з цим має поширювати свій вплив і на такі випадки, зокрема щодо пропагандистських, рекламних заходів, публікації звітів, проспектів емісії акцій, оголошень та інших заходів, які

207

проводяться банком з оприлюдненням певної інформації в інформаційному середовищі. Тут інформація має надаватись у так званому диверсифікованому вигляді. Диверсифікація в даному випадку передбачає надання інформації різними інформаційними каналами, через різних суб’єктів, окремими частками, з перервою у часі. За певних умов може бути доцільним надання неповної інформації або ж у формі коротких заяв, повідомлень, прес-релізів, без будь-яких коментарів. В окремих випадках може необхідно буде згадати давно забуте слово цензура, особливо для інформації, яка активно поширюється банком в інформаційне середовище. У даному разі заходи цензури передбачатимуть:

* аналіз інформації стосовно належності її до такої, що має обмежений доступ;
* перевірку об’єктивності інформації та відповідності її чинному законодавству;
* порівняння змісту інформації, що надається для оприлюднення із змістом попередньо оприлюдненої задля виявлення або суперечності одної одній, або ознак конфіденційності в сукупності повідомлень;
* аналіз інформації з погляду її сприйняття інформаційним середовищем;
* узагальнення всієї інформації, що надана в інформаційне середовище, та виявлення критичної межі її змісту для врахування у подальшій роботі.

Представники державних установ (за винятком тих, що передбачені ст. 62 Закону України «Про банки і банківську діяльність») отримують право доступу до інформації банку відповідно до своїх повноважень за рішенням керівника установи банку в порядку, передбаченому останнім. Представники інших суб’єктів господарювання, установ та організацій отримують доступ до банківської інформації в межах і в порядку, передбаченому відповідними договірними документами. У разі виникнення екстремальних ситуацій доступ до інформації банку відповідним особам (представникам правоохоронних органів, органів МНС, іншим особам) надається за рішенням керівника установи банку в межах питань, які стосуються вирішення екстремальних ситуацій.

Однією з особливостей сьогодення є поширене використання різноманітних електронних засобів для отримання інформації з акустичного каналу. За таких умов система захисту інформації банку має передбачати нормативне регулювання питань,

208

пов’язаних із правилами користування технічними засобами накопичення, обробки, зберігання та передавання інформації. Крім того, доцільно буде включити в перелік заходів захисту інформації періодичне проведення атестації окремих приміщень банку щодо наявності в них пристроїв електронної розвідки. До заходів протидії витоку інформації через спеціальні електронні пристрої знімання інформації слід включити спеціальне інженерно-технічне обладнання приміщення, де зберігається, оброблюється інформація з обмеженим доступом та обговорюються важливі для банку питання. Сюди ж слід додати і використання спеціальних технічних засобів виявлення пристроїв електронної розвідки та періодичний огляд засобів і мереж зв’язку, місць їх розташування. Безперечно система захисту інформації повинна забезпечувати технічний захист інформації, яка оприлюднюється під час переговорів, нарад та інших видів конфіденційного спілкування.

* 1. захисті інформації банку важливе місце відводиться організації спеціального діловодства. Діловодство розуміють як систему заходів щодо документаційного забезпечення діяльності банку. Основним правилом в організації діловодства

1. банку і захисту його інформаційних ресурсів є забезпечення розмежування потоків відкритої інформації й інформації з обмеженим доступом. За таких умов у банку має бути

організоване службове діловодство (забезпечення документообороту відкритої інформації) і спеціальне діловодство, яке забезпечує документооборот інформаційних матеріалів таємного та конфіденційного характеру. Водночас у процесі руху документів конфіденційного та таємного характеру збільшується кількість осіб, обізнаних з цінною інформацією банку, а з тим і розширюються потенційні можливості втрати конфіденційної та таємної інформації, збільшується ризик розголошення її персоналом банку, витоку через технічні засоби, зникнення документів. За таких умов документооборот як процес руху документованої інформації з обмеженим доступом також стає об’єктом захисту. Головним у конфіденційному документооборот стає формування спеціалізованої технології руху документів, яка забезпечувала б необхідну безпеку інформації на будь-якому з етапів її обороту. Тому захищений документооборот має являти собою контрольний рух документів конфіденційного та таємного характеру по регламентованих пунктах приймання, обробки, розгляду, виконання, використання, зберігання в жорстких

209

умовах організаційного і технологічного забезпечення безпеки як носіїв інформації, так і її самої. У такому разі в доповнення до правил службового документообороту конфіденційний документооборот додатково включає такі заходи:

обмеження доступу персоналу до документів, справ і баз даних діловою, службовою та виробничою необхідністю;

персональна відповідальність посадових осіб за надання дозволу на доступ працівників банку до відомостей і документів конфіденційного і таємного характеру;

жорстка регламентація порядку роботи з документами, справами, базами даних для всього персоналу.

Документооборот як головна складова діловодства базується на відповідній систематизації документів у банку, якою є номенклатура справ. Згідно з номенклатурою справ усі документи групуються у відповідні групи (справи) і обліковуються та зберігаються по таких групах (справах). Номенклатура справ є єдиною для всього банку. Документооборот здійснюється відповідно до номенклатури справ і поділяється на вхідний, вихідний та внутрішній документопотоки. Вхідний документопотік спеціального діловодства включає: приймання, облік і первинну обробку пакетів, конвертів і незаконвертованих документів, що надійшли до установи банку; облік документів і формування довідково-інформаційного банку даних по документах; попередній розгляд і розподіл документів; розгляд документів керівниками і надання їх на виконання;ознайомлення з документами виконавців, використання чи виконання документів.

Вихідний та внутрішній документопотоки включають: вироблення документів (визначення грифу таємності та облік носія майбутнього документа, розроблення документа, облік підготовленого документа та його виготовлення; контроль вироблення документів); обробка виданих документів (експедиційна обробка і відправлення їх адресатам, передавання внутрішніх документів відповідним підрозділам банку); систематизація вироблених документів відповідно до номенклатури справ, оформлення їх по справах; підготовка і направлення справ до архіву банку відповідно до встановленого порядку архівації документів. Усі документи, справи і носії інформації повинні мати інвентарний номер.

Спеціальне діловодство в установах банків є централізованим

1. забезпечується відповідним підрозділом. Основною особливістю документообороту в спеціальному діловодстві є

210

багатоступеневий облік усіх процедур і операцій, що проводяться

* документами. Зміст зазначених процедур і операцій конфіденційного документообороту розкрито в Додатках 5—9.

**7.5. Протидія інформаційно-психологічному впливу в діяльності банку**

Інформаційно-психологічний вплив на сьогодні не новина. Як уже було з’ясовано вище, він широко застосовується в різних сферах суспільних взаємовідносин, в тому числі і в підприємницькій діяльності. Разом з тим звертає на себе увагу ситуація, за якої розвиток засобів та заходів інформаційно-психологічного впливу значно випереджає розвиток діяльності із захисту від нього, і особливо протидії йому. Обережність, з якою підрозділи безпеки суб’єктів господарювання здійснюють діяльність щодо протидії інформаційно-психологічному впливу абсолютно неадекватна тим загрозам , які останній несе в собі. У даному разі ми ведемо мову саме про ту ситуацію, коли за допомогою заходів інформаційно-психологічного впливу створюються загрози діяльності суб’єктів підприємництва.

Розглядаючи питання протидії інформаційно-психологічну впливу, слід звернути увагу на те, що він є одним із інструментів інформаційного протиборства або вищої його стадії інформаційної війни суб’єктів ринку. У даному разі заходи інформаційно-психологічного впливу застосовуються з метою заподіяння шкоди суб’єкту, стосовно якого вони вживаються.

Захист банку від інформаційно-психологічного впливу, як правило, здійснюється через мінімізацію ризику отримання негативного результату від нього. Водночас в інформаційній війні тільки заходами мінімізації вказаного ризику суттєвої зміни ситуації не досягти. Тут необхідно значно активізувати свою діяльність у даному напрямі, забезпечивши насамперед протидію інформаційно-психологічному впливу. Важливим моментом у цьому разі є вибір об’єкта протидії. Безперечно, власний персонал не може бути таким об’єктом, його необхідно захищати, а не впливати на нього з погляду руйнації тих інформаційно-психологічних конструкцій, які з ’являються у нього під чужим впливом. Об’єктом тут має бути інформаційне середовище, через яке поширюються заходи інформаційно-

211

психологічного впливу, з одного боку, а з другого — сам суб’єкт, який є зацікавленою стороною в поширенні такого впливу, а також суб’єкти, через які поширюється такий вплив. Тобто тут важливо усвідомити, що протидія має здійснюватися не з метою захисту. Основна мета протидії інформаційно-психологічному впливу — припинення цього впливу. Важливим тут буде зрив та нейтралізація заходів інформаційно-психологічного впливу, що проводяться проти банку.

Аналізуючи механізми інформаційного протиборства та інформаційної війни, можна сказати, що моделі інформаційно-психологічного впливу практично однакові в різних сферах людської життєдіяльності. Використовуються лише різні їх модифікації.

* + повсякденній діяльності людина зазвичай не має часу детально аналізувати складний механізм здійснення інформаційного протиборства. Для прийняття рішень вона використовує значно спрощені моделі, наявні точки зору, які характеризують певні події, випадки, суб’єктів діяльності, конкретних осіб. Враховуючи таку ситуацію при здійсненні інформаційно-психологічного впливу важливим є формування таких моделей і надання їх в інформаційний простір або конкретному об’єкту. Такий підхід значно спрощує розуміння процесів, що відбуваються, для споживачів інформації. Адаптація таких моделей в інформаційному просторі та у свідомості людини практично є програмуванням її психіки. Досвід ведення інформаційних війн наказує, що існує кілька моделей, які в різних комбінаціях застосовуються для забезпечення інформаційно-психологічного впливу на протидіючі сторони. Тобто протидія впливу — це не що інше, як такий самий вплив з метою руйнування методології, задумів, технологій проведення інформаційного протиборства.

Зважаючи на те, що в центрі інформаційного протиборства чи інформаційної війни знаходиться людина, інформаційно-психологічний вплив спрямовується на найбільш вразливі сфери

* психіки. Такими сферами є:
* мотиваційна (ціннісні орієнтири, переконання);
* сфера потреб та інтересів, бажань, потягів;
* інтелектуально-пізнавальна (знання, пам’ять, мислення);
* емоційно-вольова (емоції, почуття, настрої, вольові процеси);
* комунікативна (характер і особливості спілкування,

взаємини з людьми, міжособисті сприйняття);

212

* функціональна (виконання службових і посадових обов’язків, дисциплінованість) [150].

Якраз з урахуванням зазначених сфер, завдань та умов і формуються моделі впливу. Крім того, особливостями моделей впливу в інформаційно-психологічній протидії є те, що вони практично завжди виступають руйнівними і спрямовуються на дискредитацію конкретного суб’єкта протидії і заходів впливу, що ним проводяться. Хоча в окремих випадках вплив у протидії може мати і стимулювальний характер.

Якщо об’єктом протидії впливу обирається інформаційне середовище банк готує і проводить за відповідними технологіями (моделями) заходи контрпропаганди, спрямовані на руйнування ефекту, якого очікують суб’єкти, що ведуть проти банку інформаційну війну. З метою посилення протидії банку інформаційно-психологічному впливу в інформаційному середовищі можуть формуватися групи підтримки, однодумців, громадські об’єднання з клієнтів, акціонерів банку, інших осіб щодо поширення сформованих банком моделей протидії в інформаційному середовищі. В окремих випадках можуть проводиться певні акції: мітинги, демонстрації, пікети, громадські вимоги на підтримку банку. За таких умов буде здійснюватися не тільки гуртування громадян навколо банку, а й відповідна трансформація колективної свідомості. Доповненням до цього може бути поширення позитивних для банку та руйнівних для технологій інформаційно-психологічного впливу чуток і міфів.

Коли ж об’єктом протидії обирається суб’єкт, яким ініціюється чи здійснюється інформаційно-психологічний вплив, то тут можуть передбачатись інші заходи та формуватися для них відповідні моделі протидії, зокрема:

виявлення суб’єкта, яким ініціюється проведення інформаційно-психологічного впливу на банк та суб’єктів, через яких здійснюється такий вплив;

розкриття негативного змісту діяльності зазначених

суб’єктів у засобах масової інформації та іншим способом в інформаційному середовищі банку;

звернення до органів влади, правоохоронних органів, Антимонопольного комітету, суду, громадськості з вимогами щодо припинення здійснення щодо банку негативного інформаційно-психологічного впливу;

213

залучення до протидії інших суб’єктів (банків-партнерів, клієнтів, акціонерів) та вжиття спільних заходів щодо протидії інформаційно-психологічному впливу;

формування компрометуючих інформаційних моделей протидії та поширення їх в інформаційному середовищі щодо суб’єктів, якими проводяться дії інформаційно-психологічного впливу на банк.

Звичайно, виконання зазначеної роботи для підрозділів безпеки банків є новим, і здебільшого вони не готові до таких дій. Але водночас саме ці підрозділи за своїм функціональним призначенням є найбільш придатними для виконання заходів протидії інформаційно-психологічному впливу на банк. Якраз вони володіють інформацією, необхідною для організації і проведення таких дій, а опанування технологіями протидії забезпечить їм необхідні умови для ефективної їх реалізації у разі інформаційного протиборства чи інформаційної війни на ринку банківських послуг.

***РЕЗЮМЕ***

Інформаційна безпека займає важливе місце в системі безпеки банку. Оскільки всі види банківської діяльності мають інформаційні характеристики, які існують на різноманітних носіях, втрата останніх або несанкціонований доступ до них може завдати банку суттєвої шкоди. У зв’язку з цим важливим є формування ефективної системи захисту інформації, в основі якої має бути управління інформаційними ризиками банку.

Разом з тим працівники банку є важливим елементом системи захисту банківської інформації, адже саме через них зазначена система реалізує свої заходи і забезпечує надійне зберігання інформації. Тому працівники банків мають відповідні обов’язки щодо захисту всіх видів інформації та несуть відповідальність за якісне їх виконання. Водночас виконання зазначених обов’язків забезпечується глибокими знаннями умов, причин формування інформаційних загроз та загроз носіям інформації, правил і методів протидії їм і захисту інформації в діяльності кожного працівника при проведенні будь-яких банківських операцій. Саме працівник банку є провідною ланкою в системі захисту інформації в діяльності банку.

Слід також наголосити, що перетворення інформаційних технологій у певні види інтелектуальної зброї та її застосування в

214

інформаційному протиборстві потребує особливих знань і вмінь, щоб протистояти її негативному впливу на власну та колективну свідомість. За таких умов важливого значення набуває здатність банківського працівника розпізнавати загрози інформаційно-психологічного впливу, витримувати дію його вражаючих факторів та забезпечувати необхідну психологічну стійкість задля якісного і безпечного виконання своїх обов’язків при роботі в банку.