МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Державний вищий навчальний заклад
«КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені ВАДИМА ГЕТЬМАНА»

М. І. ЗУБОК, С. М. ЯРЕМЕНКО

БЕЗПЕКА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Підручник

Рекомендовано
Міністерством освіти і науки,
молоді та спорту України

1906 КНЕУ
КИЇВ 2012

УДК 336.719.2(075.8)
ББК 65.262.101-134
З 91

Рецензенти

О. Д. Вовчак, д-р екон. наук, проф.
(Університет банківської справи Національного банку України)

Н. П. Шульга, д-р екон. наук, проф.
(Київський національний торговельно-економічний університет)

В. В. Крутов, д-р юрид. наук, проф.
(Український союз промисловців і підприємців)

Гриф надано Міністерством освіти і науки, молоді та спорту України
Лист № 1/11-201 від 13.01.2011

Зубок, М. І.
З 91 Безпека банківської діяльності : підручник / М. І. Зубок, С. М. Яременко. — К. : КНЕУ, 2012. — 477, [3] с.
ISBN 978–966–483–616–3

У підручнику викладено умови та сучасні підходи до організації банківської безпеки в Україні, розкриваються теоретичні основи безпеки банківського бізнесу. Основна увага приділяється розгляду діяльності банків щодо забезпечення їх інформаційної, економічної, кадрової безпеки, протидії різноманітним загрозам, а також захисту їхніх інтересів у разі виникнення екстремальних ситуацій. Матеріали підручника базуються на положеннях чинних правових норм, результатах наукових досліджень, досвіді вітчизняних та іноземних банків щодо забезпечення їх безпеки.

Для студентів економічних та інших спеціальностей, а також усіх, хто вивчає або опікується банківською справою та здійснює забезпечення її безпеки.

УДК 336.719.2(075.8)
ББК 65.262.101-134

ISBN 978–966–483–616–3

Навчальне видання

ЗУБОК Микола Іванович
ЯРЕМЕНКО Світлана Миколаївна

БЕЗПЕКА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Підручник

Редактор *Л. Тютюник*
Коректор *Т. Мизгаєва*
Верстка *М. Матвійчук*

Підп. до друку 11.04.12. Формат 60×84/16. Папір офсет. № 1.
Гарнітура Тип Таймс. Друк офсет. Ум. друк. арк. 27,71.
Обл.-вид. арк. 31,55. Наклад 300 пр. Зам. № 10-4060

Державний вищий навчальний заклад
«Київський національний економічний університет імені Вадима Гетьмана»
03680, м. Київ, проспект Перемоги, 54/1

Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи (серія ДК, № 235 від 07.11.2000)

Тел./факс (044) 537-61-41; тел. (044) 537-61-44
E-mail: publish@kneu.kiev.ua

Для нотаток

Для нотаток

ЗМІСТ

ВСТУП

Безпека як соціально-економічне явище в сьогоднішніх умовах є одним із глобальних проблем розвитку цивілізації. Жодне з рішень щодо забезпечення життєдіяльності сучасних соціальних систем не може бути ефективно реалізоване без урахування заходів безпеки. Більше того, питання безпеки мають глобальний і всеохопний характер, стосуються всіх сфер життєдіяльності людини, функціонування будь-яких організацій, розвитку соціальних систем. Світове співавторство все частіше звертається до питань забезпечення безпеки свого розвитку.

Важливість забезпечення безпеки в усіх сферах та галузях життєдіяльності суспільства обумовлена насамперед тим, що сучасне світове суспільство зазнало суттєвих змін у своєму розвитку, досягло такого рівня, коли подальше його удосконалення здійснюється в умовах все більшої невідомості та непередбачуваності. За таких умов будь-які дії, що спрямовуються на досягнення перспективних результатів, обов'язково характеризуються високим рівнем ризику.

Ризик формується під впливом різного роду дестабілізувальних факторів, які, у свою чергу, зумовлені як природними умовами, так і певними наслідками розвитку світового співтовариства. До того ж, уже зараз можна спостерігати тенденцію до активізації зазначених факторів, насамперед з погляду створення для суспільства різного роду небезпек і загроз. Беручи це до уваги, для ефективного розвитку як суспільства в цілому, так і окремих його організацій та осіб необхідно обов'язково враховувати існування дестабілізувальних факторів і можливості виникнення під їх впливом небезпек і загроз. За таких умов виникає необхідність прогнозування впливу зазначених небезпек і загроз на свою діяльність і вжиття відповідних заходів захисту та протидії їм. А оскільки заходи захисту та протидії небезпекам і загрозам є головним змістом функціонування будь-якої системи безпеки, діяльність щодо врахування дестабілізувальних факторів і можливості формування під їх впливом певних небезпек і загроз, а також вжиття заходів захисту і протидії їм в умовах вибору буде не чим

іншим, як управлінням безпекою відповідної соціальної системи. Виходячи ж з того, що розвиток будь-якої соціальної системи має комплексний характер, управління безпекою є складовою управління соціальною системою. Тобто в даний час ефективне управління соціальними системи, організаціями, галузями потребує не тільки економічних, природничих, технічних та інших знань, а й знань законів розвитку та безпеки життєдіяльності людей і створених ними систем забезпечення такої життєдіяльності. За таких умов безпека стає галуззю знань, без яких неможливий ефективний та перспективний розвиток будь-якого суспільства. Знання безпеки є складовою професійної компетенції всіх фахівців та життєво необхідною потребою будь-якої людини взагалі.

Водночас слід звернути увагу на те, що безпека, з одного боку, є сферою забезпечення діяльності певних суб'єктів, а з другого — самостійним видом господарської діяльності, зокрема з надання охоронних, інформаційних та інших послуг. Як сфера забезпечення вона завжди пов'язана з певними об'єктами або ж певною діяльністю і завжди є конкретною та цілеспрямованою. Забезпечуючи захист об'єкта та протидію його загрозам, безпека формує певну систему заходів та залучає до них усіх представників об'єкта, а також суб'єктів, які співпрацюють з ним. Водночас вона поширює свій вплив лише в межах діяльності об'єкта.

Будучи самостійним видом господарської діяльності, безпека формує певний перелік послуг, які надаються суб'єктам господарювання в комплексі або за окремими їх видами залежно від потреби клієнтів. Тобто тут безпека утворює відповідну сферу бізнесу і є рівноправним суб'єктом ринку послуг безпеки. Основним видом господарської діяльності буде вироблення та надання послуг з охорони, захисту інформації, інформаційного забезпечення, детективної діяльності і т. п.

Таким чином, сфера застосування безпеки досить широка і стосується практично всіх сторін життєдіяльності людини, функціонування організацій та соціальних систем.

Стосовно ж банківської діяльності слід зазначити, що, перебуваючи в умовах різного роду соціальних, правових, економічних та інших перетворень, обумовлених переходом суспільства до ринкової економіки, вони зазнали суттєвого впливу різноманітних факторів, що були наслідками таких перетворень. Здебільшого такі фактори мали негативний вплив як на розвиток вітчизняної банківської системи в цілому, так і

окремих банків. За роки незалежності припинили свою діяльність близько сотні вітчизняних банків, що призвело до мільярдних збитків для економіки країни та її громадян і суб'єктів господарювання. Більше того, стабільність вітчизняної банківської системи є нестійкою і вона залежить не тільки від різного роду соціальних, політичних, економічних змін, а й досить хворобливо реагує на помилки в організації безпеки діяльності окремих її суб'єктів.

З метою мінімізації загроз, що виникають від впливу вищевказаних факторів, банки з моменту становлення вітчизняної банківської системи прагнуть забезпечувати захист своєї діяльності, не лише використовуючи можливості держави, але й створюючи власні системи безпеки. Останні ж з тим чи тим рівнем ефективності здійснюють захист банків від різного роду загроз та небезпек. Разом з тим, створюючи власні системи безпеки, банки певні функції таких систем покладають безпосередньо на власний персонал, який у такий спосіб стає одним з елементів системи безпеки банків. Звичайно, покладаючи зазначені функції на свій персонал, банки очікують грамотного та кваліфікованого їх виконання, останнє ж може забезпечуватися тільки через оволодіння певним обсягом знань теорії та практики безпеки. Реалізація ж банківськими працівниками зазначених знань у процесі виконання відповідних функцій з питань безпеки буде здійс-нюватись через компетентну та адекватну поведінку кожного працівника на певній посаді у банківській діяльності.

Таким чином, забезпечення безпеки банківської діяльності є однією з умов ефективного банківського бізнесу, складовою якісного управління діяльністю банків, а також однією зі складових професійної компетентності фахівця банківської справи.

Розділ 1

«БЕЗПЕКА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ» ЯК НАВЧАЛЬНА ДИСЦИПЛІНА

Вивчивши матеріал цього розділу, ви будете ***знати:***

- ✓ *сутність безпеки як соціального явища й умови життєдіяльності;*
- ✓ *мету, завдання, об'єкт, предмет дисципліни «Безпека банківської діяльності»;*
- ✓ *сучасні методологічні підходи до вивчення дисципліни;*
- ✓ *структуру і логіку дисципліни;*
- ✓ *взаємозв'язок дисципліни «Безпека банківської діяльності» з іншими безпекознавчими дисциплінами та наукою безпекознавства,*

а також ***уміти:***

- ✓ *орієнтуватись у наукових і фахових джерелах з питань безпеки підприємницької діяльності та банківської безпеки, знаходити необхідну інформацію для поглибленого розуміння і наукового дослідження проблем безпеки бізнесу;*
- ✓ *визначати обсяги знань і вмінь з питань безпеки банківської діяльності, необхідні для формування професійних компетенцій фахівця банківської справи.*

1.1. Безпека та її забезпечення в банківській діяльності як предмет вивчення і наукового дослідження

Актуальність вивчення теорії безпеки визначається складністю проблем сучасного розвитку суспільства і потребами практики забезпечення його безпеки в умовах глобальних зрушень і змін у всіх сферах життєдіяльності як в Україні, так і у світі в цілому. Дослідження природи і суті феномену безпеки дозволяє не тільки зрозуміти її як явище у суспільних та міжнародних відносинах, а й вивчити методологію її забезпечення в країні й окремими суб'єктами, а також громадянами. А це, у свою чергу, формує основи для розробки теорії безпеки конкретних соціальних систем та організацій, що має важливе значення для розуміння природи і причин трансформації змісту безпеки на кожному з етапів її розвитку. Водночас формування об'єктивного розуміння поняття «безпека» є досить складним, оскільки в ньому не відображено характеру інтересу, що проявляється до безпеки. Але як і будь-який феномен, дане поняття має різні значення залежно від об'єкта, щодо якого спрямовуються дії, безпеки, або суб'єкта, який здійснює на неї вплив. Тобто, говорячи про безпеку, обов'язковим є визначення об'єкта, стосовно якого вона здійснює свою дію. Якщо мова йде про безпеку банківської діяльності, то мабуть необхідно говорити, з одного боку, про банк як про суб'єкта фінансових відносин, з другого — про його діяльність як процес практичної реалізації зазначених відносин і аж з третього — про безпеку банку. За таких умов формування об'єктивного уявлення про суть безпеки як певного феномену стає досить складним без розуміння так званого «родового» її поняття.

Водночас на «родове» поняття безпеки претендує в даний час досить багато точок зору, які суттєво різняться між собою. Так, аналізуючи поняття безпеки, дане в Законі України «Про основи національної безпеки України», можна зазначити, що воно відбиває не теоретичний, а практичний підхід до розуміння феномену безпеки, оскільки пов'язане з об'єктом, яким є держава. Існуючі інші підходи також є певною мірою односторонніми, пов'язаними з різними категоріями (небезпеки, загрози, стану, діяльності і т. і.), без яких суть безпеки втрачає

свою самостійність. Тобто сучасні уявлення про безпеку демонструють неоднозначність.

Разом з тим, незважаючи на велику різноманітність підходів до розуміння поняття «безпека», вважаємо за доцільне зупинитись на одному з них, який з погляду авторів, заслуговує особливої уваги і найповніше відбиває сутність безпеки. Природно, що життєдіяльність будь-якого суб'єкта чи особи обумовлюється необхідністю забезпечувати певний обсяг їхніх особистих, суспільних, виробничих та інших потреб. Забезпечення цих потреб вимагає певних взаємовідносин з суб'єктами господарювання, людьми, природним, інформаційним, політичним чи якимось іншим середовищем, яке через особливості свого існування здійснює певний вплив на суб'єкта чи особу. У процесі взаємовідносин, персональної чи колективної діяльності та під впливом зазначеного середовища суб'єкт, особа зазнають відповідних змін, які є не чим іншим, як адаптацією суб'єкта чи особи до умов своєї життєдіяльності. Останні ж утворюються як самим процесом життєдіяльності та взаємовідносин, що існують у певному середовищі, так і особливостями особистої поведінки суб'єктів та осіб, а також силами природи. Водночас адаптація суб'єктів та осіб до умов існування передбачає насамперед дії, пов'язані з формуванням безпечної поведінки у зазначених умовах як відповідної реакції на особливості таких умов та їх зміни. Ураховуючи ж що особливості та зміни в середовищі існування суб'єкта, особи мають постійний характер, процес адаптації також набирає рис постійності, формуючи певну властивість поведінки зазначених суб'єктів і осіб. Тобто прагнення до забезпечення безпечної поведінки суб'єктів та осіб, обумовлене особливостями і змінами середовища їх існування і є природною властивістю життєдіяльності будь-якого суб'єкта чи особи. Водночас особливості середовища та зміни, що відбуваються в ньому, формують певну динаміку в забезпеченні безпеки суб'єктів, осіб, яка, в свою чергу, впливає на їх стан. Тобто, розглядаючи безпеку з такого погляду, можна зазначити, що за своєю суттю вона характеризує відповідний стан суб'єкта чи особи в конкретний момент їх існування. Водночас зазначений стан буде характеризуватися здатністю суб'єкта, особи зберігати свої можливості під впливом особливостей функціонування певного середовища та змін, що відбуваються в ньому, протистояти їм та забезпечувати свої потреби. Ураховуючи ж, що особливості та зміни в середовищі мають постійний характер і є досить

різноманітними, безпека являтиме собою певний комплекс дій, що формують відповідний стан суб'єкта, особи. Підтримання зазначеного стану за таких умов буде являти собою не що інше, як відповідну потребу суб'єкта, особи. Отже, сутність безпеки характеризується певним комплексом понять, таких як стан, властивість та здатність суб'єкта, особи забезпечувати свою адаптацію до відповідних умов їх існування.

Змісту цих понять, їх трансформація в банківській діяльності розглядатиметься в наступних розділах підручника. Водночас ефективне опанування всіх процесів забезпечення безпеки банківської діяльності може бути здійснене лише через усвідомлення даного підходу до розуміння суті поняття «безпека».

1.2. Мета, завдання, об'єкт, предмет, методологія й інформаційна база вивчення дисципліни «Безпека банківської діяльності»

Метою навчальної дисципліни є формування у студентів усвідомленого розуміння необхідності вжиття заходів безпеки в сучасних умовах банківської діяльності, уміння забезпечувати безпечні умови роботи на своєму робочому місці, якісно й ефективно виконувати заходи безпеки, передбачені в банку.

Для досягнення поставленої мети в підручнику передбачено розв'язання таких завдань:

- ✓ розкрити умови та причини, за яких у банківській діяльності виникає необхідність вживати заходи безпеки, розроблювати й упроваджувати елементи захисту інтересів банків у технологіях проведення банківських операцій, формувати безпечну поведінку їх працівників при виконанні своїх посадових обов'язків;
- ✓ викласти основи знань з науки безпекознавства: сутність, види, принципи безпеки, основні наукові теорії щодо формування змісту безпеки, місце науки безпекознавства в системі наук; роль і місце безпеки в забезпеченні підприємницької діяльності та життєдіяльності людини;
- ✓ розкрити форми та методи забезпечення безпеки в діяльності банківських установ, роль і місце банківських працівників у підтриманні встановленого в банку режиму безпеки; сформувати у студентів безпечну поведінку при

✓ навчити студентів використовувати набуті знання в роботі з клієнтами банку, підтримувати безпечні взаємовідносини з колегами й іншими суб'єктами, грамотно проводити заходи безпеки при проведенні банківських операцій;

✓ сформувати у студентів відповідальне ставлення до власної безпеки та безпеки банківської діяльності, уміння удосконалювати свою професійну компетенцію на засадах безпечної поведінки та діяльності.

Об'єктом дисципліни є діяльність банку щодо забезпечення ним власної безпеки на ринку банківських послуг. Предмет дисципліни — взаємовідносини, що виникають у банку при забезпеченні безпеки його діяльності.

Теоретичним підґрунтям вивчення дисципліни є: економічна теорія, яка вивчає економічні відносини, економічні закони і форми їх прояву на ринку банківських послуг; право, що здійснює регулювання взаємовідносин суб'єктів ринку банківських послуг і трудові взаємовідносини працівників банків; психологія та соціологія, які обґрунтовують природу та мотивацію поведінки людей за певних обставин; теорія управління як кореляційний зв'язок поведінки людей і діяльності суб'єктів господарювання.

Говорячи про методологію вивчення дисципліни «Безпека банківської діяльності», необхідно правильно розуміти саме поняття «методологія». У даному разі під методологією розуміється сукупність принципів, методів, прийомів дослідження будь-якого об'єкта. Водночас методологія це не просто набір методів, а в певний спосіб сформована ідеологія науково-аналітичної роботи, яка в кінцевому підсумку формує відповідний науково-пізнавальний рівень вивчення об'єкта і певний світогляд людини.

Загальнометодологічну основу вивчення дисципліни становлять методи:

- синергетичний, відповідно до якого безпека має розглядатись у її історичній ретроспективі та перспективі, відповідно до її місця і ролі у сукупній системі безпекознавчих наук, відповідно до об'єктивних потреб існування організації та людини;
- діалектичний, який вимагає розглядати всі аспекти забезпечення безпеки у взаємозв'язку та взаємообумовленості, динаміці та розвитку; з урахуванням закону перетворення

• системно-структурний метод, який дозволяє вивчати безпеку банківської діяльності як певну комплексну систему, з багатьма взаємопов'язаними і взаємозалежними елементами, які своїм функціонуванням забезпечують необхідну цілісність системи. Такий метод дає змогу виявити системоутворювальні елементи безпеки, якими для банківської діяльності є економічна й інформаційна безпека, які якраз і забезпечують стійкість системи.

За допомогою цього методу вивчається взаємозв'язок банківської безпеки з системами безпеки держави, зокрема її фінансової безпеки;

• статистичний метод характеризує безпеку з кількісної сторони: показники умов діяльності системи безпеки, її ефективності, темпи розвитку і т. п.;

Крім зазначених методів при вивченні дисципліни застосовуються і нетрадиційні методи пізнання: спостереження, абстрагування і концентрації, порівняння та зіставлення, аналіз і синтез, аналогія та прогнозування.

Інформаційну базу дисципліни становлять насамперед нормативно-правові акти вітчизняного законодавства з питань господарської, зокрема банківської, діяльності, інформаційних і трудових взаємовідносин, інших видів права. Великий обсяг інформаційних джерел становить навчальна література з питань безпеки підприємницької діяльності. Останнім часом з'явилися вітчизняні навчальні посібники з різних видів безпеки бізнесу, значна частка яких присвячена питанням забезпечення економічної безпеки.

До зазначених джерел слід додати: монографії, дисертації, наукові статті, тези виступів, які містять цікаві ідеї та результати наукових досліджень сучасного стану та перспектив розвитку безпеки підприємницької діяльності, у тому числі і на ринку банківських послуг.

Для розширення кругозору з питань безпеки підприємницької діяльності доцільним буде використання спеціалізованих видань, таких як журнали «Бизнес и безопасность», «Вісник Національного банку України», а також інтернетресурсу, зокрема інформація, що подається на сайтах http://www.bezpeka.com, http://kiev-security.org.ua**,** http://antiraider.ua та ін.

1.3. Структура і логіка дисципліни

Структура дисципліни обумовлюється загальною логікою формування і розвитку забезпечення безпеки підприємницької діяльності, методологією вивчення змісту роботи банківських установ щодо забезпечення їх безпеки.

Перший розділ розкрив безпеку банківської діяльності як навчальну дисципліну, її роль і місце в системі науки безпекознавства та формуванні фахівця банківської справи. У ньому дисципліна подається як предмет вивчення та як наукова дисципліна, визначаються її мета, основні завдання, об'єкт та предмет, розкриваються методологія вивчення й інформаційна база дисципліни. У розділі також висвітлюється зв'язок дисципліни з іншими складовими науки безпекознавства та предметами, що забезпечують підготовку студентів, до професійної компетенції яких входять знання питань безпеки підприємницької діяльності.

Другий розділ присвячений розгляду умов, які в даний час склалися на ринку банківських послуг України у сфері забезпечення безпеки банків. Зокрема, розглядається вплив політичних, економічних, правових, соціальних умов на організацію банківської безпеки, еволюцію становлення банківської безпеки та стан забезпечення безпеки вітчизняних банків на даний час, аналізуються причини, через які банківська безпека має певні проблеми.

У третьому розділі висвітлено основи безпеки банківської діяльності. Певна частина матеріалу присвячена теоретичним засадам науки безпекознавства, аналізу поглядів на безпеку взагалі і банківської діяльності зокрема. Розділ розглядає суть, мету, основні завдання, об'єкти, види безпеки банківської діяльності, принципи і вимоги до неї, визначає роль, місце та функції працівників банків у забезпеченні банківської безпеки.

Четвертий розділ розкриває природу, умови та причини формування загроз банківській діяльності, ознаки їх прояву у банках. Значне місце приділяється характеристикам таких загроз, як банківське шахрайство, розкрадання коштів і майна банків, втягування банків у незаконну фінансову діяльність через відмивання коштів отриманих незаконним способом. Особлива увага звертається на такі загрози, як рейдерство та терористичні

дії як найбільш небезпечні і такі, що за своєю актуальністю потребують значних зусиль банківської безпеки з протидії їм.

Продовження розгляду загроз банківській діяльності здійснюється у п'ятому розділі, який розкриває особливості конкурентних взаємовідносин суб'єктів ринку банківських послуг з погляду недобросовісної конкуренції. У розділі висвітлюються види та форми недобросовісної конкуренції у взаємовідносинах банків. Значна увага приділяється особливостям промислового шпигунства в банківській діяльності, формам і методам впливу промислових шпигунів на банківських працівників з метою отримання інформації.

Шостий розділ розкриває охорону банків як одну із форм безпеки. Насамперед у ньому подаються вимоги до технічної укріпленості банків, обґрунтовується необхідність інженерно-технічного захисту банківських установ. Важливе місце відводиться питанням організації охорони банківських установ як процесу формування їх безпеки та встановлення відповідного режиму їх функціонування. Розділ також розкриває поняття та зміст режиму безпеки, дає характеристику банку як режимному об'єкту насамперед з позицій пропускного та внутрішньооб'єктового режиму.

У сьомому розділі подається матеріал, що характеризує ще один вид безпеки банківської діяльності — інформаційну безпеку. Ураховуючи, що інформація в сьогоднішніх умовах є одним із найголовніших чинників, який разом із капіталом забезпечує успіх у підприємницькій, у тому числі і банківській діяльності, безпека має враховувати ризики банку в інформаційній сфері, чому і присвячена перша частина розділу. У розділі робиться висновок про постійність інформаційних ризиків та умови трансформації їх у інформаційні загрози на ринку, необхідність управління такими ризиками в сукупності управління ризиками банківської діяльності.

Відповідно до особливої ролі банків у сфері інформаційних відносин розділ розкриває умови формування в банках інформації з обмеженим доступом, зокрема банківської та комерційної таємниці, а також конфіденційної інформації. Тут же вказуються загрози банківській інформації та засади формування системи інформаційної безпеки банків.

У розділі обґрунтовується особлива тенденція сучасного розвитку інформаційних технологій — перетворення інформації у вид інтелектуальної зброї, яка може застосуватися проти банку у вигляді інформаційно-психологічного впливу. Розділ розкриває

заходи протидії банків щодо такого впливу.

У восьмому розділі розглядається інформаційна діяльність банку на ринку банківських послуг. Насамперед надаються заходи щодо інформаційного забезпечення діяльності банків і формуванню ними інформаційних ресурсів. Розкриваються форми та методи інформаційно-аналітичної роботи в банках, її організація, правила визначення сфер інформаційної уваги банків, об'єктів та джерел інформації, формування інформаційних каналів, способи проведення інформаційних операцій на ринку банківських послуг.

Основне місце в підручнику займає дев'ятий розділ — «Економічна безпека банку». Становлячи основу безпеки банку, економічна безпека зосереджує свої зусилля на таких напрямах, як захист матеріальних ресурсів і банківських операцій. Спираючись на нормативно-правові положення чинного законодавства та документи Національного банку України, у розділі акцентується увага на заходах захисту технологій проведення кредитних, валютних, касових операцій, операцій з цінними паперами та неторговельних операцій. Значна увага приділена технологіям захисту кредитних операцій на всіх етапах їх розвитку. Розглядається роль і місце підрозділів банку, задіяних у проведенні кредитних операцій, їх функції з питань забезпечення безпеки таких операцій. Значне місце відводиться етапу повернення проблемної кредитної заборгованості, зокрема розкриваються способи управління такою заборгованістю при різних якісних характеристиках кредитного портфеля банку. Тут подаються методи роботи банку щодо повернення кредитних боргів за різних умов взаємовідносин з боржниками.

У розділі також висвітлюються особливості забезпечення фінансової безпеки банків в умовах глобалізації та інтеграції капіталу, забезпечення економічної безпеки у разі призначення до банку тимчасової адміністрації. Тут також міститься матеріал щодо діяльності банків з протидії втягування їх у незаконну фінансову діяльність, дається алгоритм роботи банку як суб'єкта первинного фінансового моніторингу у разі виявлення сумнівних операцій.

Розділ також містить матеріал щодо протидії рейдерським посяганням на ринку банківських послуг, подаються заходи, які можуть виконувати банки щодо попередження та захисту їх від рейдерських атак.

У десятому розділі розглядаються питання забезпечення кадрової безпеки в банках. Кадрова безпека подається як система, що складається з двох елементів — мотиваційного та режимного.

Мотиваційний — заснований на забезпеченні банком потреб та інтересів працівників, а режимний — на заходах обмеження та зобов'язань діяльності і поведінки працівників із питань, що стосуються роботи в банку. Окремо викладено методику управління кадровою безпекою банку, яка заснована на формуванні та реалізації корпоративного інтересу банку, його працівників і держави з питань їх безпеки.

Питання дії банківських установ в екстремальних умовах розглядаються в одинадцятому розділі. Тут розкриваються дії банку в умовах психологічних та ідеологічних диверсій, здійснення в банках терористичних актів, виникнення актів громадянської непокори, техногенних аварій і катастроф на сусідніх підприємствах, у тому числі і з викидом отруйних і радіоактивних речовин, пожеж і стихійного лиха.

Теоретичний матеріал розділів суттєво доповнюють схеми, таблиці, діаграми, які розміщені безпосередньо за текстом та в додатках до розділів і які певною мірою ілюструють викладені в розділах положення.

За такого порядку викладення змісту підручника логіка вивчення дисципліни полягає в опануванні студентами знань за певним алгоритмом, від причин і умов формування загроз банківській діяльності, які обумовлюють необхідність безпеки банків, до форм і методів її забезпечення на всіх етапах банківського виробництва.

1.4. Безпека банківської діяльності в системі інших безпекознавчих дисциплін та науки безпекознавства

Безпека банківської діяльності разом з іншими безпекознавчими дисциплінами та науками становить науку безпекознавства. Різноманітність проблем, що існують у сфері забезпечення безпеки життєдіяльності людини, взаємовідносинах суб'єктів господарювання та організацій, сформувала необхідність вивчення їх з різних сторін багатьма навчальними дисциплінами та науками. З появою у навчальному процесі та в наукових дослідженнях безпекознавчого напряму зростає потреба в інтегрованих знаннях про безпеку, сформованих із різних галузей та наукових напрямів. За таких умов глибоко

опанувати безпеку діяльності банків неможливо лише на дисципліні «Безпека банківської діяльності». Тут корисно знати, в яких науках та дисциплінах розглядаються інші специфічні питання забезпечення безпеки, які використовуються інструменти, вживаються заходи. Відповідь на ці питання можна знайти в суміжних галузях знань. Для орієнтації студентів, котрі бажають доповнити свої знання з інших питань науки безпекознавства, у табл. 1.1. подано перелік дисциплін і наук, які пов'язані з безпекою банківської діяльності.

Економічна безпека вивчає процеси та взаємовідносини у сфері захисту економічних інтересів держави, суб'єкта господарювання, громадянина, забезпечення стійкості та живучості їх економічної системи та можливостей.

Національна безпека України охоплює різні напрями забезпечення захисту державного суверенітету та незалежності країни, визначає політику держави у сфері національної безпеки, її суб'єктів та об'єкти, заходи щодо формування системи безпеки країни.

Інформаційна безпека вивчає діяльність у сфері формування інформаційних ресурсів, захисту інформації та протидії інформаційно-психологічному впливу на різних рівнях взаємовідносин: державному, між суб'єктами господарювання, організаціями та державними органами, між громадянами та у їх взаємовідносинах із різними структурами.

Таблиця 1.1

ВЗАЄМОЗВ'ЯЗОК ТЕМ ДИСЦИПЛІНИ «БЕЗПЕКА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ» З ІНШИМИ ДИСЦИПЛІНАМИ ТА НАУКАМИ

Теми	Економічна безпека	Національна безпека України	Інформаційна безпека	Організація служби безпеки	Менеджмент безпеки	Безпека соціальних систем	Правове регулювання безпеки	Безпека життєдіяльності	Безпека підприємництва	Фінансова безпека	Комерційна розвідка
Умови організації безпеки банківської діяльності	+	+	+	+		+	+	+	+	+	

Основи безпеки банківської діяльності	+	+	+	+	+	+	+	+			+
Загрози банківській діяльності	+		+		+	+		+	+	+	
Недобросовісна конкуренція та промислове шпигунство в банках	+		+		+		+		+		+
Охорона і режим у банку	+		+	+	+		+	+			
Інформаційна безпека банку		+	+	+	+		+	+	+	+	+
Інформаційне забезпечення діяльності банку		+	+	+		+	+		+	+	+
Економічна безпека банку	+	+		+	+	+	+	+	+	+	
Забезпечення безпеки банку в роботі з кадрами	+		+	+	+	+	+	+	+	+	
Дії установ банків в екстремальних умовах	+	+	+	+	+	+	+	+	+	+	

Організація служби безпеки вивчає структуру, форми, методи організації безпеки діяльності суб'єктів підприємництва як елемент управлінської діяльності.

Менеджмент безпеки — наука управління функцією безпеки соціальних систем.

Правове регулювання безпеки вивчає основи правового регулювання взаємовідносин суб'єктів і громадян у різних сферах життєдіяльності, правові засади їх захисту та розвитку.

Фінансова безпека вивчає форми, методи, заходи забезпечення фінансової стійкості та фінансової незалежності держави, суб'єкта господарювання та громадянина в різних умовах їх функціонування.

Комерційна розвідка як елемент інформаційного забезпечення вивчає організацію, форми та методи добування інформації, необхідної для забезпечення комерційної діяльності суб'єктів підприємництва.

Безпека підприємництва (бізнесу) вивчає основи забезпечення безпеки підприємницької діяльності, особливості організації системи безпеки комерційного підприємства та умови безпечного його функціонування.

Безпека життєдіяльності — наука про забезпечення захисту матеріального світу і суспільства від негативної дії природних та

техногенних явищ. Вона опікується забезпеченням безпеки існування людини у природному середовищі та виробничому процесі, а також забезпеченням екологічної безпеки.

Безпека соціальних систем вивчає процеси, що виникають під час захисту суспільства, соціальних груп, людини, держави, різних організацій, об'єднань. У її структурі обґрунтовуються форми та методи попередження, протидії, нейтралізації небезпечного стану (кризи) як фактору, що утворює загрозу для існування і розвитку зазначених об'єктів.

Ефективність вивчення дисципліни «Безпека банківської діяльності» буде вищою, коли вона вивчатиметься у тісному зв'язку з іншими фаховими дисциплінами, насамперед з такими, як «Правознавство», «Економіка підприємств», «Менеджмент», «Маркетинг», «Гроші та кредит», «Економіка праці і соціально-трудові відносини», «Банківські операції», «Аналіз банківської діяльності». Саме названі дисципліни формують підґрунтя для глибшого опанування знань з безпеки банківської діяльності. Базуючись на вказаних знаннях у фахівця банківської справи — випускника вузу мають бути сформовані наступні професійні компетенції:

- уміння забезпечувати свою власну безпеку при виконанні посадових обов'язків у банку;
- підтримання встановленого в банку режиму безпеки в процесі банківської діяльності;
- уміння розпізнавати небезпечні ситуації та загрози у процесі проведення банківських операцій, вживати адекватних заходів щодо їх нейтралізації та ліквідації;
- уміння удосконалювати свої професійні компетенції, набувати нових знань і досвіду, творчо їх використовувати в процесі своєї діяльності в банку.

Зазначені компетенції формуються, зокрема, і через опанування матеріалу даного підручника відповідно до тематики та графіка вивчення дисципліни. Формуванню вмінь як правил поведінки сприятимуть наведені в кінці кожного з розділів завдання для індивідуальної роботи.

РЕЗЮМЕ

Безпека банківської діяльності є складовою науки безпекознавства, концептуальною основою якої є ідеологія безпекотворення. Наука безпекознавства виходить з того, що

безпека є своєрідною сферою існування людини, нації, держави, суспільства, організації у середовищі їх існування. Звідси безпека поступово стає необхідним атрибутом, властивістю, що характеризує здатність певного об'єкта (у даному випадку банку) до надійного існування та розвитку.

Відповідно до цього метою підручника є систематизований виклад основних положень теорії безпекознавства у сфері банківської діяльності та засад практичної реалізації вимог безпеки і розвитку в процесах банківського виробництва. У підручнику категорія безпеки подається не як предмет, а як інструмент досягнення мети діяльності банку.

Усі розділи підручника розроблено на результатах наукових досліджень, проведених авторами та іншими науковцями з відповідних проблем безпекотворення, а також на досвіді забезпечення вітчизняними банками безпеки їх діяльності. Матеріали розділів апробовано в навчальному процесі ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана», Київському національному торговельно-економічному університеті, Університеті економіки і права «Крок», Міжнародному університету фінансів при викладенні дисциплін «Безпека банківської діяльності», «Економічна безпека», «Управління фінансово-економічною безпекою банків».

Терміни і поняття

Безпека

Завдання дисципліни «Безпека банківської діяльності»

Інформаційна база вивчення дисципліни «Безпека банківської діяльності».

Мета дисципліни «Безпека банківської діяльності»

Методологія вивчення дисципліни «Безпека банківської діяльності»

Об'єкт дисципліни «Безпека банківської діяльності»

Предмет дисципліни «Безпека банківської діяльності»

Питання та завдання для перевірки знань

1. Що вивчає дисципліна «Безпека банківської діяльності»?

2. У чому полягає актуальність безпеки для банківської діяльності?

3. Дайте характеристику безпеці як відповідного стану банку.

4. Розкрийте безпеку як певну властивість банку.

5. У чому полягає мета дисципліни «Безпека банківської діяльності»?

6. Що є об'єктом та предметом дисципліни «Безпека банківської діяльності»?

7. Охарактеризуйте методологію дисципліни «Безпека банківської діяльності».

8. У чому полягає логіка дисципліни «Безпека банківської діяльності»?

9. Обґрунтуйте роль та місце дисципліни «Безпека банківської діяльності» в системі безпекознавчих дисциплін.

10. Розкрийте основні наукові характеристики безпеки банківської діяльності як складової науки безпекознавства.

11. У чому полягає взаємозв'язок дисциплін «Безпека банківської діяльності» і «Національна безпека України»?

12. Які положення, необхідні для глибшого опанування матеріалу дисципліни «Безпека банківської діяльності» розкриває дисципліна «Безпека соціальних систем»?

13. Які із зазначених у підручнику компетенцій є, на ваш погляд, найбільш актуальними для банківського фахівця?

14. Як уміння та навички з безпеки формуватимуть безпечні правила поведінки банківського працівника?

15. Назвіть теоретичні засади вивчення дисципліни «Безпека банківської діяльності».

Література для поглибленого вивчення

1. *Зубок М. І.* Безпека банківської діяльності : навч. посібник / Зубок М. І. — К. : КНЕУ, 2002. — 190 с.

2. *Зубок М. І.* Методичні рекомендації та завдання до самостійної роботи студентів з безпекознавчих дисциплін / М. І. Зубок — К. : КНТЕУ, 2010. — 86 с.

3. *Ліпкан В. А.* Безпекознавство : навч. посібник / Ліпкан В. А. — К.: Вид-во Європ. ун-ту, 2003. — 208 с.

4. *Минаев Г. А.* Безопасность организации : учебник / Минаев Г. А. — К. : КНТ, 2009. — 440 с.

5. Про основи національної безпеки України // Закон України від 19.06.2003 р. — № 964-IV зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

6. *Рыбалкин Н. Н.* Философия безопасности : учеб. пособие / Рыбалкин Н. Н. — М. : МПСИ, 2006. — 296 с.
7. *Ярочкин В. И.* Секьюритология / Ярочкин В. И. — М. : Ось-89, 2000. — 400 с.

Розділ 2

УМОВИ ОРГАНІЗАЦІЇ ТА СТАН БЕЗПЕКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Вивчивши матеріал цього розділу, ви будете ***знати****:*

- ✓ *характер політичних, економічних, соціальних, правових умов та їх вплив на організацію безпеки підприємницької діяльності;*
- ✓ *основні характеристики стану та напрями розвитку банківської безпеки в Україні;*
- ✓ *об'єктивні та суб'єктивні чинники, що впливають на формування режиму безпеки у вітчизняних банках,*

а також ***уміти:***

- ✓ *аналізувати ситуацію, що складається у сфері безпеки бізнесу як у країні в цілому, так і безпосередньо в конкретному банку;*
- ✓ *виявляти актуальні проблеми у забезпеченні безпеки банківської діяльності, причини їх формування та тенденції поширення.*

Становлення та розвиток безпеки вітчизняного бізнесу, у тому числі і банківського, здійснювалися під впливом специфічних умов, які складалися на тому чи тому етапі розвитку пострадянської України та які продовжують впливати на організацію безпеки підприємницьких структур і сьогодні. З огляду на ці умови український варіант забезпечення безпеки бізнесу має свою специфіку порівняно з аналогічною

діяльністю не тільки розвинутих країн, а й країн пострадянського простору. Ці особливості притаманні і забезпеченню безпеки банківської діяльності. Більше того, враховуючи, що банки зрозуміли необхідність забезпечення безпеки власної діяльності одними із найперших, їх безпека на даний час є найдосконалішою з усіх суб'єктів підприємництва. Разом з тим саме банківська безпека зазнала найбільших трансформацій від впливу українських реалій.

Насамперед слід зазначити, що вітчизняний банківський сектор є недостатньо стійким до різного роду коливань політичної, економічної чи соціальної ситуації в країні. Незначні зміни тієї чи тієї ситуації обов'язково позначаються на ритмі роботи банків, формуючи для них додаткові ризики. Подібне можна було спостерігати восени 2004 р. під час «помаранчевої революції», у кінці 2008 і на початку 2009 р. під впливом світової економічної кризи. Обсяг вітчизняного ринку банківських послуг з різних причин не забезпечує необхідної фінансову стійкості банків, не дає можливості формувати достатній капітал для протидії негативним фактором, що утворюються під впливом змін політичної, економічної чи будь-якої іншої ситуації. За таких умов банки час від часу опиняються в складних ситуаціях і змушені концентрувати свою увагу більше на забезпеченні власної живучості. А оскільки, у структурі банківської системи значну кількість становлять малі банки, які найбільше потерпають від зазначених змін, складається враження, що вся вітчизняна банківська система є досить вразливою і нестабільною. Останнє, у свою чергу, є фактором, який суттєво впливає на довіру до банків і, як наслідок, на їх стійкість на ринку.

Водночас український феномен входження в ринкові відносини наклав свій відбиток і на різні сфери життєдіяльності країни: політичну, економічну, соціальну, а також на взаємовідносини, що регулюються правовими та моральними нормами. Характеризуючи зазначені сфери з точки зору організації безпеки вітчизняного бізнесу, ми звертаємо увагу лише на ті особливості, які суттєво впливають на становлення та розвиток безпеки підприємницької діяльності, формують певні ризики та загрози для вітчизняного підприємництва і обов'язково мають бути враховані при організації системи безпеки суб'єктів господарювання, у тому числі і банків.

2.1. Умови організації безпеки банківської діяльності

Найбільш характерними й показовими для організації безпеки банківського бізнесу є внутрішньополітичні, економічні, соціальні та правові умови.

Характеризуючи внутрішньополітичні умови організації безпеки бізнесу в Україні слід зазначити, що основною їх особливістю за час існування України як незалежної держави є боротьба за владу. Історія пострадянської України багата прикладами такої боротьби та її результатів, яка, на жаль, не сприяла як ефективному становленню та розвитку вітчизняного бізнесу, так і якісній організації його безпеки. Перманентна боротьба за владу формувала різного роду антагонізми у протистоянні окремих політичних організацій, за якими стояв той чи той економічний інтерес. Використовуючи різні важелі, вони реалізовували свої прагнення, у тому числі і за рахунок істотного економічного, владного, правового, соціального впливу на економічну складову своїх політичних супротивників. Час від часу в бізнесі можна спостерігати масштабні скандали з переслідуванням певних осіб, кризи діяльності та розорення економічних суб'єктів, у тому числі і досить потужних, обмеження діяльності певних суб'єктів господарювання та їхніх угруповань через їх дискредитацію або штучне створення невигідних умов для здійснення ними підприємницької діяльності. Вирішення політичних конфліктів нерідко здійснюється через усунення політичних конкурентів від їх бізнесу як головного фактору їхньої політичної стійкості.

У зв'язку з такою ситуацією у бізнесі виникають особливого роду загрози, які по своїй небезпечності перевершують будь-які інші тому, що здійснюють свій вплив комплексно, масштабно, активно і тотально. Такі загрози торкаються, як правило, малого і середнього бізнесу, а оскільки банки у переважній своїй більшості якраз і є представниками зазначених рівнів бізнесу, остільки вказані загрози можуть бути притаманні і їхніх діяльності. А пам'ятаючи про комплексний характер загроз і їх масштабність, протистояти таким загрозам, захищатися від них досить складно. У такому разі підприємницька діяльність, у тому числі і на ринку банківських послуг, має підпорядковуватися не тільки законам ринкової економіки, а і серйозно враховувати

розстановку й інтереси політичних сил у країні. Якраз урахування таких особливостей і побудова відповідних механізмів поведінки стосовно них і є однією з особливостей організації безпеки вітчизняного бізнесу, в тому числі і банківського.

Крім зазначеного, не можна не звернути увагу на ще одну вітчизняну особливість, а саме корупцію. За висловлюванням одного із західних дослідників корупції в країнах СНД, Україна з Росією належать до найкорумпованіших країн світу. Можливість такого стану корупції в Україні обґрунтовує вітчизняний дослідник А. Нездоля мотивуючи це, з одного боку, посиленням соціально-економічної кризи в країні і необхідністю вижити в ній, утриматись, як кажуть, «на плаву», а з іншого — прагненням державного чиновництва стрімко розбагатіти за умов законодавчої плутанини і відсутності суворого правового контролю з боку влади. За таких умов, на думку дослідника, корупція в Україні плодиться майже в геометричній прогресії [127]. Звичайно, що такий стан з корупцією не може не позначитись і на вітчизняному бізнесі, який для забезпечення своєї живучості мусить ураховувати не тільки особливості внутрішньополітичної ситуації в країні, а й поведінку владного чиновництва. Більше того, вітчизняні й іноземні дослідники вказують, що корупція в країнах перехідного періоду може набувати системного характеру, коли вона не може бути ні ліквідована, ні обминута. За таких умов інтереси виживання бізнесу обумовлюють необхідність зважати на об'єктивну обставинами ведення бізнесу, що й можна спостерігати в Україні.

Водночас корупція трансформувалась і в сам бізнес, тобто уразила його внутрішньо. Бізнес-чиновництво (керівники підприємств, провідні менеджери) перейняли практику поведінки своїх державних колег і часто-густо перетворили свої посади та функції в такі, що дають можливість додаткового заробітку. Відомі в практиці відкати, пільгові угоди (у тому числі і кредити), так зване кумівство та інші аналогічні дії якраз і вказують на наявність корупції безпосередньо в самих бізнес-структурах. За даними МВС України, у 2008 р. у банках було викрито 50 фактів хабарництва з боку банківських службовців за видачу кредитів [116].

Найважливішою ж і болючою проблемою в Україні є відсутність суспільно-державної ідеології, спрямованої на формування відповідного менталітету громадян, який би

забезпечував об'єктивне розуміння ними необхідності політичних, економічних, соціальних перетворень та адекватну їх поведінку в умовах переходу країни до ринкової економіки.

Насправді ж менталітет громадян частково відстає від тих перетворень, які здійснює країна, а частково деформує їх розуміння, особливо стосовно ролі й участі громадян у таких перетвореннях. Як наслідки загрози бізнесу можуть виникати від неприйняття його частиною громадян взагалі як форми суспільно-економічних відносин. Інша ж частина громадян вважає будь-яку свою діяльність, у тому числі протиправну та аморальну, як бізнес, всіляко відстоюючи своє місце в суспільстві. Ще хтось паразитує на ситуації або свідомо чи несвідомо використовує її у своїх інтересах. Тобто внутрішньополітична ситуація в країні є досить складною для організації безпеки бізнесу і обумовлює необхідність суттєвого її врахування у захисті його інтересів.

Що ж стосується економічних умов, то тут мають місце кілька особливостей, які впливають на організацію безпеки бізнесу. Незважаючи на ейфорійні заяви Україна за своїми економічними можливостями залишається бідною. Попри значну економічну спадщину Радянського Союзу, яка дісталась Україні, остання не змогла ефективно її зберегти та використати. За даними, наведеними згаданим вище дослідником А. Нездолею в одній із цього праць, Україна тільки за перші п'ять років своєї самостійності втратила більше ніж на 400 млрд дол. своїх активів, що вдвічі перевищує шкоду, заподіяну за роки Другої світової війни. Основними причинами тут були неефективна державна економічна політика, безгосподарність, масові крадіжки, незнання та невміння керувати виробництвом в умовах ринку, а також відсутність досвіду роботи з іноземними партнерами. Ці та інші причини призвели до падіння виробництва за сім років незалежності України більше ніж утричі [127]. Звичайно, що наслідки такого катастрофічного економічного стресу не можна було швидко подолати в умовах становлення ринкової економіки та нестабільної політичної ситуації. Сучасна ж фінансова криза ще більше загострила і без того непросту економічну ситуацію.

Однією з умов забезпечення безпеки діяльності банків є достатність капіталу. Як відомо, основний капітал банки формують за рахунок залучення коштів населення і суб'єктів господарювання. Разом з тим обсяг залучення коштів залежить від рівня достатку населення і прибутковості господарств. Однак,

за офіційними даними, частка збиткових підприємств в Україні досить висока: 2007 р. — 28,9 %, 2008 р. — 33,9 %, станом на 01.03.2010 р. — 52,5% [135]. А якщо врахувати суб'єктів, що ведуть хоч і не збиткову діяльність, але в той же час не мають істотного прибутку або приховують свої фінансові результати чи здійснюють бартерні операції, то частка суб'єктів господарювання, які не можуть суттєво впливати на формування капіталу банків може бути ще більшою 50 %. Тобто фінансові результати діяльності вітчизняних суб'єктів господарювання такі, що не можуть забезпечити достатній для стійкої діяльності всіх банків фінансовий ресурс. За таких умов діяльність вітчизняних банків практично завжди перебуває під загрозою втрати ними своєї ліквідності. Щонайменші коливання ситуації в економіці чи на фінансових ринках будуть відбиватися на діяльності банків, створюючи для них додаткові ризики та напруженість відносин із клієнтами.

Істотно збільшити свій ресурс банки могли б за рахунок коштів населення. За даними Національного банку України, доходи населення у 2008 р. становили 856,6 млрд грн, з яких 371,1 млрд грн — заробітна плата. Водночас у структурі витрат населення приріст фінансових активів становив 52,1 млрд грн, які потенційно могли опинитися в банках як депозити населення [139]. Разом з тим, як зазначає Асоціація українських банків, сьогодні «на рахунках» у населення перебуває від 40 до 60 млрд дол. США і не надходять вони до банків з однієї причини — недовіри до вітчизняної банківської системи [134]. За таких умов одним із завдань банківської безпеки має бути забезпечення інформаційного впливу на населення країни як потенційного інвестора банків з метою активізації його до взаємовідносин з банками, насамперед через банківські вклади, а іншим — захист коштів населення у процесі банківської діяльності.

Поряд з цим важливе місце в ієрархії економічних особливостей займає тіньова економіка, яка, за деякими даними, становить від 30 до 60 % ВВП України. Обсяги готівки поза банками дорівнювали у 2008 р. 186,7 млрд грн [139]. Основними сферами, де тіньова економіка має найбільше поширення є сільське господарство, будівництво, деревообробна промисловість, сфера діяльності з нерухомістю, торгівля автомобілями, легка промисловість, нафтопереробна, рибна та хімічна промисловість, оптова торгівля. Для майже 25 млн громадян тіньова економіка є основним джерелом доходів, а близько 40 % молоді великих міст і прикордонних регіонів

зайнято саме в тіньовій економіці [135]. Тобто тіньова економіка є досить потужною сферою незаконної, неофіційної та кримінальної діяльності, в якій задіяна значна кількість населення країни і яка вже сформувала певне ставлення до неї. Така ситуація має два негативні аспекти для банків. Насамперед вона небезпечна тим, що банки втягуються в незаконну діяльність, передусім, через участь у легалізації тіньових коштів. У другому ж аспекті її існування значно обмежує можливості законного формування банками фінансового ресурсу. Крім того, уражена діяльністю в тіньовому секторі свідомість громадян формує і відповідну їх поведінку, яка недалека від кримінальної і яка може бути перенесена на відносини з банками. Небезпечність ситуації полягає ще і в тому, що тіньова економіка створює підґрунтя для корупції й організованої злочинності і саме через кримінальний вплив може створювати загрози для банківської діялності.

Сучасна українська тіньова економіка набула професійних рис, стала більш досконалою, виверткою, отримала серйозні впливові зв'язки, а по деяких галузях сформувався її міжнародний характер. Протистояти її наступу банкам досить складно і небезпечно, тому їх безпека має знайти механізми забезпечення вимушеного, але безпечного співіснування.

Специфікою вітчизняних економічних умов є дисбаланс між малим, середнім та великим бізнесом. Більш-менш ефективно може розвиватися лише великий бізнес, створюючи потужні бізнес-угруповання, які об'єднують різних за напрямами та сферами діяльності суб'єктів, формуючи напівзамкнуті цикли підприємництва і обмежуючи економічний простір для малого та середнього бізнесу. Специфікою поведінки на ринку цих угруповань є агресивність, яка формує такі відносини, як суперництво та протиборство. У результаті для інших суб'єктів бізнесу створюється атмосфера виживання, обмеженої діяльності та постійної загрози недобросовісної конкуренції. Банки, організовуючи свою безпеку, повинні враховувати такий фактор і вживати відповідних заходів у боротьбі за життєвий простір.

На відміну від західних ринків банківських послуг характерною особливістю вітчизняного ринку є платіжна криза практично всіх як реальних, так і потенційних клієнтів банку. Криза характерна для всього часу існування незалежної України, в окремі періоди посилюючись чи, навпаки, спадаючи. Особливість української платіжної кризи є те, що вона не обов'язково збігається із загальноекономічною чи галузевою

кризою. Платіжна криза української економіки здебільшого обумовлюється особливою поведінкою вітчизняних суб'єктів господарювання та населення. В основі такої поведінки — свідоме порушення взятих на себе зобов'язань, пов'язане зі штучним затягуванням повернення боргів або ж створення умов до взагалі їх неповернення. У країні утворився певний прошарок підприємців, які здійснюють свою діяльність за рахунок несвоєчасного повернення коштів, поставки товарів, виконання робіт і т. п. Така ситуація утворює підвищений ризик взаємовідносин суб'єктів підприємництва, найбільшою мірою торкаючись саме банківської діяльності.

Окремо слід звернути увагу на особливості діяльності банків як економічних суб'єктів країни. Зазначені особливості обумовлюють певні риси поведінки банків на ринку та їх взаємовідносин з клієнтами і звичайно мають вплив на банківську безпеку, і не тільки в позитивному аспекті. Розглядаючи особливості банківської діяльності в Україні необхідно зазначити, що вони обумовлені як об'єктивними, так і суб'єктивними чинниками. До перших можна віднести значну концентрацію банківського капіталу в невеликої кількості банків: 8 % банків (I група) мають близько 65% зобов'язань (54% регулятивного капіталу) та 62% активів (63% кредитного портфеля). Як показує досвід, втрата платоспроможності і ліквідності хоч би одним з таких банків не тільки викликає негативні наслідки у фінансовій системі, а й значною мірою відбивається на соціальній та економічній ситуації в країні, роботі суб'єктів, які були клієнтами зазначеного банку.

Звертає на себе увагу і те, що інституційна структура банківської системи України залишається недостатньо розвинутою. Про це свідчить значна кількість малих банків (приблизно 65%) для яких характерні досить ризикова і недостатньо ефективна діяльність, низький рівень капіталізації.

Останнім часом набули небезпечної тенденції дії подібних банків і у кредитній діяльності, коли банки видають довгострокові кредити під заставу короткострокових (до одного року) вкладів. Більше того, як правило, діяльність таких банків зосереджується на обслуговуванні незначної кількості ресурсних клієнтів і залученні до співпраці з банками великої кількості населення, приваблюючи та заохочуючи його ефективною рекламою. Стійкість таких банків до різних інфляційних коливань та непередбачених ситуацій, пов'язаних з фінансовими загрозами (неповернення чи несвоєчасне повернення кредитів,

невиконання клієнтами зобов'язань за банківськими гарантіями та ін.) досить низька і може різко понижуватись у таких умовах, аж до втрати (тимчасової, а то й повної) їх ліквідності. Прикладом цього є ситуація на ринку банківських послуг наприкінці 2008 початку 2009 р., коли близько 80% банків, яким Національний банк України призначено тимчасові адміністрації, були саме малі банки.

Водночас необхідно зазначити, що зростання розриву між строковими депозитами банків та їх регуляторним капіталом, з одного боку, і кредитним портфелем, з другого досить тривожним симптомом для всієї банківської системи України. Так, за даними Асоціації українських банків, відношення довгострокових кредитів до довгострокових депозитів і регуляторного капіталу в 2004 р. становило 1,1, у 2005 р. — 1,4, у 2006 — 1,6, у 2007 — 1,7 [134]. Зазначена тенденція зберігається й досі.

Слід вказати і на значні територіальні диспропорції в розміщенні банків. Більше половини діючих банків розміщені в столичному регіоні, у деяких регіонах взагалі немає діючих банків — юридичні особи. Водночас у банківській системі недостатньо інтенсивно відбуваються процеси консолідації банків через створення банківських об'єднань, що могло б підвищити стійкість банків до всіляких криз і їх відповідальність перед своїми клієнтами.

Велике значення у формуванні загроз ліквідності банків має рівень їх капіталізації, який в окремих з них неадекватний ризикам діяльності банків і недостатній для забезпечення стабільного функціонування і розвитку банківської системи в цілому. Про це можуть свідчити такі тенденції: а) незбалансоване зростання капіталу, активів і зобов'язань банків. У деяких банках граничний рівень нормативу адекватності регулятивного капіталу не перевищує 10%. Значна кількість банків ще до настання кризи мали рейтингову оцінку капіталу за системою CAMELS — «3», «4», «5», тобто мали проблеми щодо достатності та якості капіталу. До того ж частина банків має недостатню якість капіталу, що знижує захисну його функцію. Серед причин недостатньої капіталізації банків можна назвати слабку ресурсну базу суб'єктів господарювання в країні взагалі, що змушує банки йти на підвищений ризик при вкладанні своїх коштів. Як наслідок такого ризику випливає друга причина — недостатній рівень отримуваного прибутку. До інших причин можна віднести недостатню привабливість та обмежену кількість

банківських операцій, а також недостатню довіру до банків, особливо з боку населення країни.

Чинником, що впливає на формування загроз діяльності банків, є існування порівняно значного ризику ліквідності активів банків. У деяких банках частка високоліквідних активів не перевищує 10%. Насамперед така ситуація створюється через недостатню ефективність управління активами і пасивами банків.

До зазначених вище чинників слід також віднести високу концентрацію кредитних операцій банків (понад 60% від усіх операцій) і, як наслідок, зменшення ступеня диверсифікації вкладання банківських коштів, що, у свою чергу, призводить до підвищення ризику їх витрачання. Крім того, за даними аналітичних звітів Національного банку України в банківській системі існує високий ризик галузевої концентрації банківських кредитів, наявність і зростання негативно класифікованих (сумнівні та безнадійні до повернення) кредитів, особливо для банків третьої групи. За останніми даними банківських експертів, проблема зростання обсягів проблемних кредитів значно загострюється, обсяг таких кредитів станом на 1 серпня 2009 р. по банківській системі дорівнював майже 20% [139]. Такі обсяги перебувають уже поза критичною межею, яка становив 10% від обсягів кредитного портфеля.

Як показує досвід, втрата банками своєї ліквідності та платоспроможності пов'язана передусім з негативною кредитною діяльністю банків. Це підтверджується і вивченням матеріалів з постанов Правління Національного банку України про відкликання банківської ліцензії і запровадження процедури ліквідації банків. Як на одну з найважливіших причин, що зумовлює ліквідацію банків, у зазначених постановах вказується на ризикову кредитну політику банків, яка призвела до втрати значної частини ресурсів банків і, як наслідок, до настання їх неплатоспроможності. Результати вивчення матеріалів ліквідації банків свідчать про те, що негативна кредитна діяльність є головною причиною втрати банками своїх активів і доходів і такою, що домінує у формуванні їх неплатоспроможності. Надмірне захоплення кредитними вкладаннями призвели до того, що тільки за споживчим та іпотечним кредитуванням фізичних осіб вимоги банків станом на 1 січня 2008 р. досягли 22,6% ВВП. Причому таке фінансування банками населення не формувало умов для адекватного розвитку вітчизняного виробництва як бази для отримання громадянами доходів. Кошти в основному було витрачено на нарощування імпорту споживчих товарів [139].

Крім суттєвої загрози банкам, яку спричиняють кредитні ризики, спостерігається також і тенденція до зростання валютних ризиків. Особливо така ситуація характерна для банків, в яких велику частку займають операції з нерезидентами, спостерігається випереджувальна динаміка активних і пасивних операцій в іноземній валюті порівняно з операціями в національній валюті або зростання частки активів у іноземній валюті в загальній сумі активів певного банку. До цього слід додати небажану для певного кола банків тенденцію зростання валютних ризиків при здійсненні кредитно-депозитних операцій. Нерідко кредити в іноземній валюті перевищують валютні депозити. Ситуація ускладнюється і тим, що банки захоплюються валютним кредитуванням своїх клієнтів не враховуючи, що останні не завжди мають доходи в іноземній валюті. Наприклад, на початок 2008 р. кредити домашнім господарствам в іноземній валюті становили 63,6% від загальної суми кредитів таким суб'єктам. До яких наслідків це призвело, нам уже відомо.

Вітчизняний банківський сектор має ще одну особливу характеристику — істотну присутність іноземного капіталу на ринку банківських послуг. На даний час із 199 банків 52 (26%) мають іноземний капітал, у 17 (9%) з яких цей капітал становить 100% статутного фонду. Частка ж іноземного капіталу в сукупному статутному фонді банків України дорівнює 36,9%. Водночас необхідно зазначити, що присутність іноземного капіталу на ринку банківських послуг України створює йому як певні переваги, так і потенційні загрози. Так, за досвідом діяльності транснаціональних банків у європейських країнах існує ризик проникнення «ефектів зараження» на фінансовий ринок України при виникненні певних негараздів у зазначених банках чи країнах їх походження. Крім того, у разі настання критичних ситуацій з дочірніми структурами таких банків в інших країнах є приклади відмежування материнських банків від проблем своїх дочірніх структур. Таке відмежування може мати різні причини, але результати для нас завжди будуть негативними.

Особливої уваги заслуговує проблема недотримання нормативів банківської діяльності. За даними Національного банку України, найчастіше порушуються нормативи Н7 (максимальний розмір кредитного ризику на одного контрагента), Н9 (максимальний розмір кредитів, гарантій та поручительств, наданих одному інвестору), норматив Н13-2 (норматив загальної короткої відкритої валютної позиції), що призводить до нестійкої

діяльності банків і, як наслідок, втрати ними платоспроможності та ліквідності.

Важливим моментом у функціонуванні банківської системи України є й те, що в сукупних активах банків на суму 932,8 млрд грн їх власний капітал становить лише 112,2 млрд грн (12%) [139]. Така ситуація формує підвищений ризик рейдерських атак на банки, у рейдерів завжди існує спокуса отримати величезні активи за мізерну ціну.

Разом з об'єктивними чинниками, що можуть формувати загрози діяльності і ліквідності банків, суттєве значення для створення таких загроз мають і причини суб'єктивного характеру. Серед них першу сходинку займає стійкий стан криміналізації, який існує в банківській діяльності. Так, за даними МВС України у 2008 р. у кредитно-фінансовій сфері скоєно 6930 злочинів, з яких 3,2 тис. у сфері банківської діяльності (за участі працівників, клієнтів і партнерів банків, тобто майже по 16 злочинів у кожному з банків [121]. Слід зазначити, що подібна динаміка злочинів, скоєних у банківській сфері, зберігається з 2001 р. Найчастіше в банках трапляються злочини, пов'язані з порушенням правил службової діяльності (перевищення повноважень, зловживання службовими обов'язками) посадових осіб банків чи осіб, що мають істотну участь у банках, недбалість посадових осіб банків, крадіжки банківських коштів самостійно чи у змові з клієнтами банків або іншими особами.

Сьогодні окремі банки втягуються у кримінальний процес легалізації (відмивання) грошей, отриманих незаконним способом, для чого вступають у змову з фіктивними фірмами, за допомогою яких через кореспондентські рахунки банків незаконно перераховуються за межі держави мільйони гривень.

Особливо уражені злочинами такі банківські операції, як кредитні, валютні, операції з готівкою та пластиковими платіжними засобами.

Крім безпосередньо незаконних фінансових операцій у банках важливе місце займають злочинні посягання на їх матеріальні цінності, інформаційні ресурси. Нерідко вилучення з банків грошей є наслідком злочинів, пов'язаних з несанкціонованим проникненням до банківської інформаційної комп'ютерної системи (банківської платіжної системи).

Друге місце серед суб'єктивних чинників займає професійна діяльність керівництва та персоналу банків. Прагнучи до мінімізації ризиків банківської діяльності і не маючи для цього

суттєвих важелів, банки спрямовують свої зусилля до власних клієнтів, максимально експлуатуючи їхні можливості. Підвищені проценти, різного роду комісії, додаткові умови, що обмежують права клієнтів, усе це інструменти, якими банки прагнуть забезпечити свій захист від негараздів економічної, політичної чи будь-якої іншої ситуації. Банківські технології, як правило, не містять суттєвих елементів захисту, а поведінка працівників банків не спрямовується до упередження загроз. Традиційно банки починають вживати заходів захисту вже в ситуаціях, коли загрози є незворотними або ж почали свій негативний вплив на банк. Персонал банків, недостатньо підготовлений з погляду виконання заходів безпеки, часто неспроможний протистояти злочинним посяганням на власність банків, є безпечним у процесі банківського виробництва.

До суб'єктивних факторів, які створюють загрози діяльності банків, що можуть призвести до втрати ними власної платоспроможності та ліквідності, слід віднести і не завжди ефективне управління активами та пасивами банків, а також діяльністю банків взагалі. Керівництво банків недостатньо використовує всі можливі важелі управлінського характеру для створення ситуації, яка б сприяла зниженню ризику проведення банківських операцій. У деяких випадках відсутня управлінська наполегливість при виконанні прийнятих рішень, особливо в питаннях оперативного реагування та загрози, що виникають навколо банків. Нерідкими є дії керівництва і власників банків, якими порушуються встановлені банківські нормативи, особливо ті, що впливають на ліквідність банків. Усе це певною мірою відбивається на діяльності банків, сприяє створенню умов для виникнення різних негативних ситуацій.

Слід також звернути увагу на недосконаліть, а подекуди й повну відсутність реальних і якісних методик оцінювання ризиків, що супроводжують банківську діяльність. Нерідко існуючі методики мають загальний характер і не висвітлюють певної загрози для тієї чи тієї банківської операції.

Усе це разом призводить до того, що вітчизняні банки здійснюють свою діяльність під впливом надзвичайно високих ризиків.

Важливою особливістю соціальних умов, які суттєво впливають на організацію безпеки бізнесу, у тому числі і банківського, є значна криміналізація підприємницької діяльності та суспільства взагалі. У країні щороку реєструється біля 600 тис. злочинів, 40% з яких мають економічний характер.

Гостроти ситуації додала остання фінансова криза, особливо це відбилося на банках. Порівняно з 2008 р. кількість злочинів у банківській сфері в 2009 р. зросла на 22%. Останнім часом злочини в банках урізноманітнились і зачіпають практично всі сфери банківської діяльності. Відомі випадки злочинів в особливо великих розмірах під час проведення касових операцій (один із банків у 2009 р. видав клієнту 1400 тис. фальшивих гривень), розрахункових операцій за участі фіктивних і так званих буферних підприємств (тільки в одному випадку через п'ять вітчизняних банків було незаконно конвертовано та перераховано за кордон понад 1 млрд грн), кредитних операцій, операцій з пластиковими платіжними засобами та цінними паперами, а також інших банківських операцій. В умовах кризи збільшилася кількість злочинів із фінансовими інструментами, насамперед акціями та векселями. Тільки у другому півріччі 2008 р. загальний обсяг операцій з підробленими векселями склав 3,5 млрд грн [80].

Значно зросла кількість нападів на банківські установи з метою заволодіння готівкою. Якщо за 2008 р. таких нападів було скоєно 103, то тільки за перше півріччя 2009 р. кількість подібних нападів уже становила 109 [136].

Однією з особливостей сучасної злочинності є її організований характер і формування злочинних угруповань, у тому числі й у фінансових установах. Фахівці зазначають, що в результаті кризи, загрози втрати або втрата роботи багатьма громадянами, невідповідності заробітної плати існуючому прожитковому мінімуму, можливості практично легально здійснювати в економіці злочинну діяльність у злочинних угруповань з'явилася потужна фінансова і матеріальна база, зв'язки у владних колах, підвищився професійний рівень економічних злочинів, усе частіше їх скоєння здійснюється на високій науковій основі. Тобто злочинність у сьогоднішніх умовах дістала досить якісну основу, що робить її більше небезпечною, зухвалою та агресивною. Хронічні життєві негаразди, хитке фінансово-матеріальне становище, відсутність стійких перспектив значною мірою позначаються на моралі як суспільства в цілому, так і окремих громадян, формуючи у такий спосіб соціальну базу для злочинності. Тобто організація безпеки бізнесу вже тривалий час здійснюється в умовах не тільки значної його криміналізації, а й за наявності передумов для її існування. Тому одним із головних завдань вітчизняного бізнесу є забезпечення його живучості саме в таких умовах.

Ще однією особливістю соціальних умов є значне розшарування населення в доходах. Досить велика частина громадян має достаток, що межує з бідністю, і прагне забезпечити своє виживання будь-якими способами, у тому числі і такими, що є не зовсім законними. У цієї частини громадян формується і відповідна поведінка, вони є основним джерелом дрібних правопорушень і злочинів. Такі громадяни можуть вдаватися до шахрайських дій з коштами, матеріальними цінностями, іноді до крадіжок, нападів, завжди виправдовуючи свої дії крайньою необхідністю.

Варто звернути увагу й на досить незначний середній клас в Україні, настільки незначний, що на відміну від іноземних країн він не може суттєво впливати на розвиток економічних процесів, у тому числі і бізнесу. Банківський сектор, формуючи свої фінансові ресурси, не може заявити, що окремі його банки — це якраз банки середнього класу й акцентувати роботу саме з його представниками. Мало того, що клас мізерний за кількістю, він ще незначний і за рівнем достатку, до того ж останній у даного класу не є постійним і гарантованим.

Слід також звернути увагу і на те, що в Україні існують прошарки населення хоч і незначні за обсягом, але такі, на які необхідно зважати в усіх аспектах соціального життя. Насамперед ідеться про молодих людей у віці до 30 років, які ніколи і ніде не працювали, живуть за рахунок своїх рідних, випадкового підробітку, дрібного злодійства та жебрацтва. Тривалий термін такого життя сформував у цієї категорії людей менталітет утриманця, нероби, пасивну поведінку, байдужість та агресивність у взаємовідносинах.

Крім вказаного прошарку з'явився ще один — дрібний торговець. Уся країна покрита ринками, величезні маси людей чимось торгують, щоденно прагнуть отримати «свіжу» копійку. Разом з тим, щоб реалізувати свій не завжди якісний і такий, що мало користується попитом товар, дрібні торговці вдаються до обману, підробок, порушення моральних, а то й правових норм. З поведінки таких людей поступово зникають такі якості, як об'єктивна доброзичливість, взаємоповага і взаємодопомога, усе більше з'являються у їхньому характері користь, обман, недовіра і т. п.

Як про певний прошарок можна говорити і про нелегальних мігрантів в Україні. Люди, які не мають практично ніякого правового статусу, живучи в країні напівлегально, вони, проте, не хочуть залишати Україну. Перебування їх у країні часто

обумовлено неприйнятну поведінку, екзотичні хвороби, національні угруповання з особливими взаємовідносинами. Як правило, такі особи не збагачують країну ні своїми інтелектуальними здобутками, ні матеріальним надбанням.

Звичайно, що така ситуація не може бути сприятливою для розвитку вітчизняного бізнесу, якісної та ефективної конкуренції та економічного прогресу, її наявність — це додаткові загрози для підприємницької діяльності, відволікання значного трудового ресурсу у сферу діяльності, яка не забезпечує формування ВВП країни.

Слід мати на увазі ще одну особливість соціальних умов, характерних саме для України. Щорічно населення країни зменшується на 300—500 тис. осіб, що означає зникнення одного цілого великого міста обласного масштабу [135]. За даними ООН, за такої динаміки скорочення населення Україна в 2050 р. буде мати не більше 26 млн осіб, вік кожного третього з яких перевищуватиме 60 років. Тобто вітчизняний бізнес може чекати кадровий голод, до підприємств і організацій можуть прийти некваліфіковані працівники (а то і фізично нездорові), трудовий ресурс країни можуть становити вихідці з інших країн. Проблему депопуляції населення суттєво доповнює проблема здоров'я сучасних українців. Сьогодні ця проблема надзвичайно турбує 76% громадян, вона перебуває на першому місці в рейтингу сучасних соціальних проблем. Тобто бізнес уже в найближчому майбутньому може отримати не зовсім здорових (якщо не сказати хворих) працівників, які будуть нездатні ефективно вирішувати завдання розвитку конкурентоспроможного бізнесу.

До цієї проблеми впритул наблизилась інша — проблема компетенції сучасних фахівців. Комерціалізація освіти сформувала ситуацію, за якої основним її досягненням є кількість дипломованих спеціалістів. Водночас якість їх фахової підготовки, здатність практично виконувати завдання підприємницької діяльності в конкретних умовах безпосередньо на підприємстві, у банку, як правило, не висока. За інформацією одного із керівників банків, із 100 атестованих його банком для прийняття на роботу випускників вузів — тільки два показують відмінні знання, ще 36 осіб — знання на рівні задовільно і добре, а 68 випускників за своїм рівнем підготовки не можуть претендувати на роботу в банках взагалі. Зазначена проблема сьогодні є досить актуальною не тільки для банків, а й практично для всіх галузей. Підприємці змушені вживати додаткових заходів щодо підготовки та адаптації молодих фахівців до умов

вітчизняного виробництва і підприємницької діяльності. Надзвичайність даної проблеми трансформується для бізнесу в одну із кадрових загроз, яку підприємці мусять ураховувати при організації безпеки своєї діяльності.

Характеризуючи соціальні умови, не можна оминути увагою трансформацію особистості самого українця, яка відбулась у ньому за роки незалежності. За відсутності раціональної ідеологічної складової в державній політиці, суттєвого зниження виховної роботи в сім'ї, школі, вузі, колективі наші громадяни особливо у віці до 30 років значною мірою знизили моральні якості. Такі показники моралі, як доброта, людяність, чутливість, терпимість, порядність, відповідальність, патріотизм не завжди є основою поведінки та взаємовідносин сучасних українців. Це, звичайно, позначається не тільки на їхніх взаємовідносинах між собою, а й стає керівним чинником у ставленні до роботи, колективу, громадської діяльності. Тобто порушились моральна безпека як окремого громадянина, так і суспільства в цілому. За таких умов у частини людей формувалися певні переконання в правильності їх аморальної поведінки за сучасних умов, їх життєдіяльність поступово перетворюються у боротьбу за виживання з усіма атрибутами саме боротьби. Якраз на основі боротьби і будуються їх взаємовідносини та поведінка в сім'ї, колективі, суспільстві.

Ці та інші характеристики й особливості соціальних умов формують у країні постійну соціальну напруженість, яка в будь-який момент може спалахнути локальними або масштабними конфліктами, створюючи суттєві загрози та перешкоди розвитку вітчизняному бізнесу.

Правові умови організації безпеки бізнесу характеризуються насамперед відсутністю будь-яких спеціальних законодавчих актів з питань безпеки підприємницької діяльності. За майже двадцятирічну історію своєї незалежності українські законодавці не змогли прийняти жодного з актів, які регулювали б відносини у сфері безпеки бізнесу. Виникла певна колізія, коли існуюча в країні діяльність має попит, знайшла свого споживача, об'єднала сотні тисяч громадян у різних підприємствах та організаціях, але досі не отримала правового регулювання. В Україні це перший випадок, коли існуюча легальна діяльність протягом такого тривалого періоду залишається неврегульованою.

Відсутність законодавчого регулювання змушує суб'єктів, так чи інакше задіяних у забезпеченні безпеки бізнесу, посилатись на

правові норми, які повною мірою торкаються їх діяльності або окремих її сторін. Такі норми містить цивільне, інформаційне, кримінальне, господарське, конкурентне, трудове право та інші види права. Окрім того, суб'єкти, що надають послуги безпеки бізнесу та здійснюють свою діяльність безпосередньо у структурах бізнесу, посилаються на чинні підзаконні акти різних міністерств і відомств, місцевих органів влади та формують власну нормативно-правову базу. Ураховуючи, що будь-яка діяльність регулюється чотирма нормами права (Конституція України, законодавчі акти, підзаконні акти, що приймаються центральними та місцевими органами виконавчої влади, нормативно-правові документи суб'єктів господарювання), а також що державних правових актів з цих питань майже немає, суб'єкти підприємництва регулюють взаємовідносини у сфері безпеки їхньої діяльності в основному власними нормативно-правовими документами. Водночас виходячи з того, що не всі фахівці з безпеки бізнесу є компетентними у нормотворчій роботі, такі документи не завжди є якісними і не можуть ефективно впливати на організацію безпеки бізнесу.

Разом з тим, велика кількість правових норм, які міститься у різних правових актах і які можна використати для регулювання взаємовідносин у сфері безпеки бізнесу, переважній більшості фахівців мало відома, оскільки стосується різних галузей права і потребує спеціальних правових знань. Така ситуація дає можливість державним органам і чиновникам обмежувати діяльність суб'єктів безпеки бізнесу, у тому числі і враховуючи тимчасове незнання певних спеціальних галузевих норм права фахівцями безпеки.

Відсутність спеціальних законодавчих норм з організації безпеки бізнесу не створює умов для формування статусу працівника системи безпеки, його прав, функцій, форм та способів діяльності. Дії таких працівників практично завжди можуть бути оголошені поза законом, з усіма наслідками, що виникають від цього. Більше того, відсутність зазначеного законодавства не формує відповідальності за порушення встановленого суб'єктом господарювання режиму безпеки, а з цим і відповідної поведінки працівників, клієнтів, керівників, власників. Через це зусилля фахівців безпеки по створенню відповідного режиму безпеки на підприємстві, у банку не завжди досягають очікуваної ефективності.

Слід звернути увагу ще на одну особливість сьогоднішніх правових умов у сфері забезпечення безпеки бізнесу. В умовах неповного та неконкретного законодавчого поля діяльність в

окремих сферах економіки практично повністю регулюється підзаконними актами, що робить таку діяльність залежною від певного органу. Наприклад, така ситуація склалася на ринку охоронних послуг, де абсолютну монополію має МВС, від якого і залежать перспективи діяльності приватних підприємств, що надають аналогічні послуги. Тобто, здійснюючи діяльність у сфері безпеки бізнесу, її суб'єкти завжди перебувають під загрозою потрапляння в немилість певному державному органу, тому мусять знаходити різні форми та способи адаптації до такої ситуації.

2.2. Характеристика сучасного стану безпеки банківської діяльності

З огляду на те, що в Україні забезпечення безпеки бізнесу склалося в самостійний вид діяльності, набуло легального характеру та визнано практично всіма суб'єктами державної влади, доцільно дати характеристику сучасному стану зазначеної діяльності. Насамперед слід вказати, що незважаючи на суттєве поширення заходів безпеки в підприємницьку діяльність безпека бізнесу все ж таки не набула системного характеру. Забезпечення безпеки діяльності того чи того суб'єкта підприємництва обмежується функціями відповідного підрозділу безпеки або договірними відносинами з суб'єктами, що надають послуги з тих чи тих питань безпеки. Діяльність служб безпеки суб'єктів підприємництва, як правило, розпорошена між окремими напрямами діяльності зазначених суб'єктів і має умовно-комплексний характер. У забезпечення безпеки не залучено персоналу суб'єкта господарювання, зазвичай він є лише джерелом загроз. Структури безпеки, як правило, заповнені колишніми правоохоронцями, які, маючи суттєві знання і досвід щодо захисту законності і державних інтересів, автоматично перенесли методи своєї професійної роботи і на безпеку бізнесу. Водночас висока конкуренція та багатовекторність діяльності суб'єктів бізнесу потребує захисту їх інтересів у різних сферах функціонування; правовій, економічній, соціальній, міжнародній, політичній, що, звичайно, вимагає досить глибоких спеціальних знань. Оперуючи знаннями та досвідом тільки правоохоронної діяльності, колишні працівники міліції, прокуратури, служби безпеки, Збройних сил, інших силових структур не завжди

спроможні забезпечити комплексну безпеку підприємницької діяльності. Водночас система підготовки фахівців з безпеки бізнесу тільки народжується, а за відсутності спеціального законодавства зазнає суттєвого впливу різного роду відомств, органів і посадових осіб.

За таких умов вітчизняна безпека бізнесу певною мірою пасивна, не має упереджувальну характеру і здебільшого залежна від керівництва суб'єктів господарювання. Слід також зауважити, що не всі форми та види безпеки розвинені однаково. Найбільшого розвитку досягла охорона та охоронна діяльність, найменшого — інформаційна, економічна та кадрова безпека.

Таким чином, проаналізувавши умови організації безпеки бізнесу та її стан у банківському секторі економіки України можна зробити висновки:

- у країні існують загрози вітчизняному бізнесу, природа яких не обумовлюється сферою підприємницької діяльності і взаємовідносинами в ній. Такі загрози характерні для особливих взаємовідносин у сфері внутрішньополітичної діяльності і породжуються боротьбою за владу;
- певною мірою можна говорити про наявність підґрунтя для утворення загроз бізнесу через власний персонал. Умови виховання та підготовки фахівців обумовлюють формування специфічних загроз — непрофесіоналізму в бізнесі як на виконавчому, так і на управлінському рівнях;
- відсутність повноцінного правового регулювання взаємовідносин у сфері безпеки бізнесу змушує сили безпеки діяти на межі порушення закону, з досить високим ступенем ризику і не завжди ефективно;
- існування в економіці країни значного і потужного тіньового сектору обумовлює втягування суб'єктів господарювання в не завжди законну діяльність, суттєво збільшуючи ризик їх функціонування на ринку, посилюючи агресивність взаємовідносин у боротьбі за безпечніші й ефективніші умови діяльності;
- обмежені економічні можливості суб'єктів господарювання змушують їх фінансувати власну безпеку в досить незначних обсягах, часто на межі її мінімального функціонування; крім того, недостатні можливості формування фінансового ресурсу та фінансування бізнес-проектів зумовлює для суб'єктів підприємництва постійний ризик втрати своєї ліквідності;
- дисбаланс великого, середнього та малого бізнесу загострює взаємовідносини суб'єктів внутрішнього ринку, посилюючи

- низька платоспроможність громадян та суб'єктів господарювання обумовлює значні обсяги прострочених боргів, що вимушує кредиторів відволікати певні кадрові та фінансові ресурси для повернення своїх коштів, а також зменшує економічні можливості ведення бізнесу;
- особливі умови ведення бізнесу в Україні обумовили досить ризикову специфіку діяльності вітчизняної банківської системи, за якої найменші зміни політичної, економічної, соціальної ситуації суттєво відбиваються на вітчизняних банках. Звертає на себе увагу і те, що в захисті свого бізнесу банки переважно вдаються до шаблонних заходів, у тому числі і безпеки, які у специфічних українських умовах не завжди дають позитивний результат;
- незважаючи на наявність великої кількості безробітних у вітчизняному бізнесі існує кадровий голод на професіоналів, здатних ефективно, на сучасному рівні забезпечувати функціонування та розвиток українського підприємництва і його безпеку;
- безпека бізнесу не має державної підтримки, діє несистемно, розпорошено, не створюючи попереджувального характеру протидії існуючим загрозам і не має впливу на ринок.

У цілому ж сучасний український бізнес здійснює свою діяльність у потужному силовому полі. В умовах ринку на нього впливають різні сили — як легальні, так і нелегальні. Насамперед на нього тисне сама держава, змушуючи здійснювати свою діяльність в умовах недосконалого законодавства і відсутності ефективних інструментів захисту. Додатково бізнес досить істотно відчуває силу корумпованого чиновництва, яка спирається на недосконалу нормативно-правову базу, владні можливості та міць державного апарату. Крім того, силове поле бізнесу доповнюють інтелектуальні та фінансові можливості партнерів і конкурентів, а також сила криміналу, що спирається на організовану злочинність. За таких умов безпека бізнесу стає не тільки досить актуальною, а й обов'язковим і постійним атрибутом вітчизняного підприємництва, у тому числі й на ринку банківських послуг.

РЕЗЮМЕ

Розглядаючи сучасний український бізнес, у тому числі й на ринку банківських послуг з погляду забезпечення його безпеки, необхідно зазначити, що незважаючи на двадцятирічний термін існування України як незалежної держави безпека вітчизняного бізнесу перебуває поки що у стані становлення. Більше того, стан становлення безпеки сьогодні задовольняє і сам бізнес, і державу, оскільки, з одного боку, не вимагає значних затрат, а з другого — дає змогу правоохоронній системі держави зберігати відповідну монополію. Разом з тим об'єктивно такий стан не можна вважати прийнятним для розвитку бізнесу оскільки даний баланс швидко порушується навіть за незначних змін внутрішньої ситуації чи зовнішньополітичних відносин. Непередбачені трансформації і загрози, які виникають у бізнесі від зазначених змін, суттєво впливають на його ефективність і вимагають посиленої уваги з боку сил безпеки підприємницької діяльності.

Терміни і поняття

Економічні умови організації безпеки бізнесу
Корупція
Криміналізація підприємницької діяльності
Платіжна криза
Політичні умови організації безпеки бізнесу
Правові умови організації безпеки бізнесу
Соціальні умови організації безпеки бізнесу
Тіньова економіка

Питання та завдання для перевірки знань

1. Чим мотивується необхідність забезпечення безпеки бізнесу взагалі і банківського зокрема?
2. Яка особливість внутрішньополітичних умов організації безпеки бізнесу в Україні?
3. Чому підприємницька діяльність, у тому числі і на ринку банківських послуг має враховувати розстановку й інтереси політичних сил у країні?
4. Як корупція впливає на організацію забезпечення безпеки бізнесу в країні?

5. Чому дисбаланс великого, середнього та малого бізнесу загострює взаємовідносини суб'єктів внутрішнього ринку?

6. Як низька платоспроможність громадян і суб'єктів господарювання впливає на ефективність банківської діяльності?

7. Яка основна особливість економічних умов організації безпеки бізнесу в Україні?

8. Як тіньова економіка може створювати загрози для банківської діяльності?

9. Як особливості діяльності банків можуть впливати на організацію забезпечення безпеки їхньої діяльності?

10. Які переваги та недоліки має присутність іноземного капіталу на ринку банківських послуг України?

11. Які основні особливості соціальних умов організації безпеки підприємницької діяльності в Україні?

12. Які загрози для підприємницької діяльності створює наявність нелегальної міграції в Україні?

13. Що таке кадровий голод? Які кадрові загрози слід враховувати при організації підприємницької діяльності?

14. Що є основною особливістю правових умов організації безпеки бізнесу в Україні?

15. У чому полягають основні проблеми забезпечення безпеки бізнесу на сучасному етапі розвитку ринкових відносин в Україні?

Література для поглибленого вивчення

1. *Крутов В. В.* Від патріотичного виховання, боротьби з тероризмом… до недержавної системи національної безпеки / Крутов В. В. — К. : Преса України, 2009. — 592 с.

2. *Крутов В. В.* Становлення та розвиток недержавної системи безпеки підприємництва в Україні : монографія / Крутов В. В. — К. : Фенікс, 2008. — 496 с.

3. *Нездоля А. И.* Украина третьего тысячелетия: Союз демократических сил / Нездоля А. И. — Донецк : Каштан, 2005. — 459 с.

4. *Стрельбицька Л. М.* Банківське безпекознавство: навч. посіб. / Стрельбицька Л. М., Стрельбицький М. П., Гіжевський В. К. — К.: Кондор, 2007. — 601 с.

5. Управління фінансово-економічною безпекою : монографія / [Кириченко Р. А., Лаптєв С. М., Пригунов П. Я. та ін.] — К. : Ун-т економіки та права «Крок», 2010. — 480 с.

Розділ 3

ОСНОВИ БЕЗПЕКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *основні наукові підходи до розуміння поняття «безпека бізнесу», критерії його визначення;*
- ✓ *мету банківської безпеки та її завдання;*
- ✓ *види, принципи банківської безпеки та вимоги до неї;*
- ✓ *форми реалізації заходів безпеки та її об'єкти в банку;*
- ✓ *функції керівних органів та персоналу банку з формування та дотримання режиму його безпеки;*
- ✓ *заходи із забезпечення безпеки банківської діяльності;*
- ✓ *структуру підрозділу безпеки банку,*

*а також **уміти**:*

- ✓ *визначати обсяги повноважень і відповідальності персоналу банку щодо дотримання встановленого режиму безпеки;*
- ✓ *формувати перелік завдань з питань безпеки в діяльності банку, а також напрями зосередження зусиль сил безпеки;*
- ✓ *визначати об'єкти для захисту силами безпеки банку в процесі банківської діяльності.*

3.1. Поняття безпеки бізнесу як предмет наукової полеміки

Будь-яка особа, фахівець, підприємець, які виходять на ринок і планують займатися власним бізнесом, повинні знати, що в цій сфері діяльності незацікавлених осіб немає. Тому тут мають бути досить глибокі професійні знання як щодо розвитку бізнесу, так і

щодо забезпечення його безпеки. Водночас сучасні уявлення про безпеку взагалі і бізнесу зокрема досить різноманітні, у тому числі і серед фахівців, які професійно зайняті у цій сфері.

Незважаючи на чималий термін розвитку підприємницької діяльності в Україні та інших країнах СНД зазначене поняття розуміють по-різному, навіть коли воно подається у відповідних правових актах. Водночас, досліджуючи це поняття, можна бачити, що залежно від умов, в яких реалізується безпека об'єктів, щодо яких вона застосовується, та інтересів підприємців безпека проявляє себе по різному. Насамперед безпека тісно пов'язана з видом підприємницької діяльності, яку вона забезпечує. Тобто безпеки взагалі не буває. Вона завжди конкретна, і конкретизація її обумовлюється насамперед діяльністю суб'єкта підприємництва. Тому говорячи про безпеку ми маємо на увазі об'єкт і його безпеку: державу і її безпеку, банки та їх безпеку і т. д.

Конкретизуючи поняття безпеки безпосередньо до банківської діяльності і розглядаючи різні точки зору науковців і банківських фахівців стосовно безпеки банків, можна спостерігати кілька сталих напрямків, щодо яких обґрунтовується суть безпеки. Певна частина авторів вважають, що безпеку слід розуміти як певний стан захищеності банку від загроз його діяльності. В обґрунтуванні такого розуміння вони виходять з того, що стан захищеності має адекватно мінімізувати ризики банківської діяльності і забезпечувати ефективну реалізацію інтересів банків. Водночас, розглядаючи поняття захищеності (захисту) як певну дію банку, необхідно вказати, що вона передбачає формування такої системи його безпеки, яка не допустила б реалізації загроз щодо будь-якої сфери діяльності банку. Разом з тим поняття захищеності подається як пасивна дія банку щодо ізоляції його від загроз, попередження їх та недопущення проникнення до банку і його діяльності. Ототожнення поняття безпеки банків з поняттям стану їх захищеності призводить до уявлення, що в банку можна створити потужну систему режиму його діяльності, яка виключала б реалізацію будь-яких загроз йому і чим потужніше ця система, тим ефективнішою є організація безпеки банку. За таких умов банк може перетворитися в недоступну, самоізольовану структуру не тільки для зловмисників, а й для інших суб'єктів, що суттєво позначиться на його розвитку. Крім того, створення потужної системи захищеності банку вимагає врахування всіх можливих загроз його діяльності, що, з одного боку, призводить до суттєвих витрат на безпеку, а з другого,

враховуючи різноманітність загроз, до створення абсолютної захищеності банку, що виступило б характеристикою його стану. У практиці діяльності банків, таке створити неможливо. Загроза є лише формою вираження агресивного наміру, тому будувати безпеку банку на основі формування тільки системи його захисту від загроз немає сенсу. Виходячи з викладеного можна констатувати, що розуміння безпеки банків і їхньої діяльності, як стану захищеності не може вважатися повним, оскільки воно не відображає об'єктивної суті поняття безпеки банківської діяльності.

Інша точка зору, яка існує серед вітчизняних та деяких іноземних науковців і фахівців, пов'язана з певною сукупністю заходів, дій, спрямованих на забезпечення життєдіяльності об'єкта, формування умов його розвитку і т. п. Аналізуючи такий підхід, варто звернути увагу на те, що сукупність заходів та дій хоча і спрямована на забезпечення життєдіяльності, але не трансформована в нього й існує сама по собі. З іншого ж боку, зведення певної сукупності заходів чи дій до поняття безпеки суттєво звужує безпеку і утворює ситуацію, за якої безпека може існувати самостійно без свого об'єкта. За такого підходу головна умова існування безпеки — створення досконалої системи її заходів та факторів. Як показує практика підприємницької діяльності (у тому числі і в банківській сфері) такий підхід не є зовсім правильним.

Ще одна точка зору пов'язана з ототожненням безпеки з цілеспрямованою діяльністю щодо:

- виявлення, попередження, послаблення, усунення, нейтралізації загроз діяльності банків;
- формування умов для ефективного розвитку банків;
- захисту об'єктів банківської власності, інформації, фінансових ресурсів та банківських операцій і т. п.

Тут слід звернути увагу на те, що в даному разі діяльність подається через певні завдання, які стоять перед безпекою і спрямовані на досягнення кінцевого результату — мети безпеки. Тому не можна зводити безпеку тільки до її завдань.

Існує також думка, що безпека — це відповідний стан об'єкта, у даному разі банку. Хоча такий підхід і є найбільш оптимальним, але акцентування уваги тільки на ньому не дає повного уявлення про безпеку. Насамперед тут упускається динаміка розвитку банку, що є одним із головних чинників живучості його на ринку.

Крім зазначених підходів до розуміння безпеки існують і інші, які відбивають як значне звуження поняття безпеки, так і досить широке, комплексне її визначення, що обумовлено прагненням до врахування якомога більшого числа функцій безпеки. Тобто сучасні уявлення про безпеку бізнесу, у тому числі і банківського, демонструють суттєву різноманітність і неоднозначність точок зору, що пояснює складність і об'ємність безпеки, різнобічність її застосування. Єдине розуміння цього поняття поки що є проблемним. Але враховуючи, що на сьогодні вітчизняний бізнес сформував не тільки відповідні структури безпеки, а й започаткував їх ефективну діяльність, розуміння цього поняття можна визначити через практику функціонування безпеки бізнесу. Аналіз зазначеної практики показує, що для повнішого розуміння безпеки бізнесу підходить комплексне її визначення через три характеристики об'єкта: стан, властивість і здатність (рис. 3.1).

Рис. 3.1. Триєдине визначення безпеки банківської діяльності

Розглядаючи сутність безпеки, неважко помітити, що її існування тісно пов'язане з іншою категорією — небезпекою. Обидві ці категорії характеризують різні сторони об'єкта, його якість, властивості, стан. Водночас безпеки не буває без небезпеки. Більше того, безпека набуває свого значення тільки за наявності різного роду небезпек і загроз. За таких умов наявність безпеки завжди припускатиме наявність небезпек і загроз і аж ніяк не може їх виключати, на чому наголошують деякі автори. Не може бути абсолютної безпеки, вона являє собою певну реакцію на небезпеки і є похідною від неї та існує виключно відносно небезпеки чи загрози. У цьому проявляється конкретність безпеки. Невідповідність безпеки конкретній небезпеці, загрозі або ж її відповідність уявній небезпеці призводить до формування систем безпеки, спрямованих на

забезпечення самих себе (безпека для безпеки), що на практиці нерідко шкодить об'єкту, заради якого будується така система безпеки.

Розуміння можливості постійного існування ризику, небезпек і загроз особливо в умовах підприємницької діяльності чи взагалі життєдіяльності людини, природно формує захисну функцію в їх поведінці у тому чи тому середовищі. Тобто, формуючи власну безпеку, об'єкт свідомо допускає існування небезпек і загроз як стосовно його як об'єкта, так і стосовно його діяльності. Отже, безпека являє собою специфічну форму самозбереження людини і результатів її діяльності (об'єкт — банк у даному разі є результатом діяльності людини) в певному середовищі (у даному разі на ринку банківських послуг). Прагнучи до безпеки, об'єкт розуміє свою залежність від небезпеки і свою здатність протистояти їй.

Таким чином, існування безпеки як певної характеристики об'єкта є об'єктивним і незалежним явищем у його взаємовідносинах із середовищем свого існування. Більше того, безпека тільки тоді має сенс, коли вона існує в певній гармонії з небезпекою. Порушення такої гармонії призводить до шкоди об'єкту, пов'язаної, з одного боку, з втратами перспектив розвитку, а з другого — з домінуванням безпеки в діяльності об'єкта, що, зрештою негативно впливає на об'єкт. Звідси випливає висновок, що, по-перше, ніяка безпека не може бути абсолютною, виключати існування небезпек і загроз як таких, по-друге, безпека — це форма існування об'єкта в середовищі небезпек і загроз і по-третє — безпека завжди має бути спрямована на виявлення небезпек і загроз, захист від них і протидію їм. Ураховуючи ж непостійність будь-якого середовища, в якому здійснює свою діяльність об'єкт (банк), безпека завжди має бути динамічною, тобто гнучкою відповідно до рівня небезпек і загроз, що існують у кожний конкретний момент для об'єкта.

3.2. Методологічні засади банківської безпеки

Оскільки безпека — це форма існування об'єкта (банку) в середовищі небезпек і загроз можемо зазначити, що кінцевий результат безпеки (реалізації її заходів) може збігатися з кінцевим результатом діяльності самого об'єкта. Отже, метою

безпеки банківської діяльності може бути виключення можливості заподіяння банку збитків або упущення вигоди та забезпечення ефективного його функціонування на ринку. Критерієм же ефективності функціонування банку на ринку, в даному разі має бути стабільність економічного (насамперед фінансового) розвитку банку. Даний критерій характеризує дві основні функції банківської діяльності — стабільність як підтримання відповідних показників діяльності банку на певному рівні протягом визначених термінів і тим самим забезпечення його стійкості до впливу небезпек і загроз, а також розвиток як абсолютна і відносна зміна показників банку, що характеризують його стан з погляду перспектив діяльності.

Очевидно, що досягнення необхідного рівня безпеки за показниками зазначеного критерію не може здійснюватися в банку якимись окремими його силами та засобами або покладатись на певний підрозділ. Зауважимо, що це завдання всього банку, всіх його підрозділів і всього персоналу. А тому, основні завдання безпеки банківської діяльності мають охоплювати всі сфери такої діяльності та бути спрямованими на досягнення мети безпеки.

Серед таких завдань мають бути:

- захист законних інтересів банку і його працівників;
- профілактика, попередження та нейтралізація правопорушень і злочинів у банку;
- своєчасне виявлення реальних і потенційних загроз банку, причин і умов, які можуть сприяти їх виникненню, проведення заходів щодо нейтралізації небезпек і загроз та протидії їм;
- оперативне реагування елементів структури банку на загрози, що виникають, та негативні тенденції розвитку зовнішньої і внутрішньої ситуацій;
- виявлення та формування причин і умов, сприятливих для реалізації банком своїх основних інтересів;
- виховання та навчання персоналу банку з питань безпеки;
- послаблення шкідливих наслідків від акцій конкурентів або злочинців з підриву безпеки банку;
- збереження й ефективне використання фінансових, матеріальних та інформаційних ресурсів банку.

Виконання зазначених завдань здійснюють через повсякденну діяльність усіх установ і підрозділів банку та проведення ними спеціальних заходів і операцій з безпеки. Банк має забезпечувати свою безпеку всією сукупністю своєї економічної, інтелектуальної, фізичної, технічної могутності.

Цілеспрямованість діяльності банку щодо забезпечення власної безпеки досягається дотриманням відповідних принципів та вимог.

Організація забезпечення безпеки банку здійснюється на основі принципу централізованого управління стратегічними напрямами даної діяльності на рівні керівництва банку. Крім того, основними принципами банківської безпеки є:

законність: заходи, що виконуються в рамках, необхідних для забезпечення безпеки банку, базуються на вимогах Конституції України, чинних законів, постанов Кабінету Міністрів, указів Президента України, нормативних актах Національного банку України, вимогах документів центральних та місцевих органів влади, а також нормативно-правових документів банку;

самостійність і відповідальність: банки повинні самостійно, власними силами та засобами забезпечувати безпеку своєї діяльності, беручи на себе відповідальність за ефективність та результативність безпеки, у тому числі і захист тих ресурсів (фінансових та інформаційних), які тимчасово передали їм їхні клієнти;

економічна доцільність: заходи безпеки не повинні призводити до погіршення умов діяльності та стану банку, перешкоджати реалізації його інтересів; витрати на проведення заходів безпеки мають бути адекватними їх ефективності;

компетентність: виконання заходів безпеки має здійснюватися грамотно, на високому професійному рівні, насамперед тими фахівцями, які є у цій справі професіоналами, з урахуванням специфіки діяльності банків;

цілеспрямованість: заходи безпеки мають здійснюватись у строгій відповідності до завдань банківської діяльності та виконуватися згідно з прийнятою в банку Концепцією безпеки;

конфіденційність: заходи безпеки проводяться переважно на конфіденційній основі, про результати виконання заходів безпеки інформується керівництво банку і за його рішенням інші особи, робота яких пов’язана з необхідністю володіння відповідною інформацією.

Надійність та ефективність безпеки визначаються через реалізацію відповідних вимог, серед них:

безперервність безпеки: забезпечення безпеки не може бути одноразовим актом. Це безперервний процес, який включає обґрунтування та реалізацію найраціональніших форм, методів, способів і шляхів створення, удосконалення і розвитку системи безпеки, безперервне управління нею, контроль за

функціонуванням;

плановість безпеки: заходи безпеки не можуть бути хаотичними або відставати від фактичних подій. Плановість передбачає запобіжний характер безпеки;

конкретність безпеки: захисту підлягають конкретні об'єкти, загроза яким може завдати шкоди банку;

активність безпеки: постійне прагнення до виявлення загроз банку, своєчасної й ефективної їх нейтралізації;

комплексність безпеки: для забезпечення безпеки необхідно застосовувати різні форми і методи захисту від загроз та протидії їм.

Реалізація принципів і вимог безпеки неможлива без конкретизації самого об'єкта безпеки, його структури, взаємозв'язків, форм функціонування. Тому, обравши основним об'єктом безпеки банківської діяльності банк, необхідно визначити елементи його структури, стосовно якої безпека має забезпечувати свій вплив, формуючи відповідний безпечний режим його функціонування. Причому зазначені елементи структури необов'язково будуть збігатися зі структурою установ і підрозділів, у даному разі мають визначитися насамперед ті елементи, від функціонування яких найбільшою мірою залежить ефективність діяльності банку. Обираючи такі елементи, треба пам'ятати, що вони повинні мати не тільки суттєве значення в діяльності банку, а й бути взаємопов'язані між собою, тобто банк може отримати позитивний результат тільки за умови ефективної безпечної діяльності всіх елементів, і водночас втрати чи інші негаразди в банку можуть настати через дестабілізацію будь-якого з таких елементів чи порушення взаємозв'язку між ними. Досвід забезпечення безпеки банківської діяльності показав, що основними такими елементами є: персонал банку, фінанси банку, його матеріальні цінності та інформація, що використовується в його діяльності особливо та її частина, що має обмежений доступ.

Персонал банку є головним елементом, через який реалізуються всі види банківської діяльності, взаємовідносини банку із зовнішнім середовищем і забезпечується його розвиток. Разом з тим персонал є досить ризиковим і непередбачуваним елементом у структурі банку і від його лояльності до банку, дисциплінованості, рівня професійної підготовки залежить якість і в цілому результат роботи банку. Водночас саме через персонал банк забезпечує проведення заходів безпеки. Як показує досвід та численні висловлювання різних авторів, сьогодні переважна частина керівників банківських установ дедалі глибше

усвідомлюють роль і місце своїх співробітників у створенні і підтриманні ефективного режиму безпеки діяльності банку [30, 75, 167, 183]. Працівники, елементом професійної компетенції яких є вміння забезпечувати власну безпеку та безпеку своєї діяльності на робочому місці, є основною запорукою забезпечення надійного режиму безпеки будь-якого банку.

Фінанси банку як елемент, стосовно якого має вживати заходів безпека банку, включають національну та іноземну валюти, розрахунки банку та банківські операції, фінансові документи, дорогоцінні метали, каміння та коштовності, цінні папери, якими володіє банк та за збереження яких він відповідає. Визначення даного елементу як такого, що їм має опікуватися банківська безпека, є актуальним тому, що фінансова діяльність і фінансові ресурси банку є практично єдиним видом послуг і товару якими оперує банк у своїй діяльності і за допомогою яких забезпечується його стійкість та незалежність на ринку.

Матеріальні цінності — банківські споруди, окремі приміщення, обладнання, технічні засоби, засоби комунікації та інформатизації, транспорт, різне устаткування, за допомогою яких банк здійснює свою діяльність. Сукупна вартість матеріальних цінностей в активах банків сягає подекуди 20% і більше. Втрата їх або тимчасове виведення з ладу не тільки завдає банку матеріальної шкоди, а й досить негативно впливає на ритм його діяльності, створює передумови для упущення вигоди і недоотримання доходу.

Загальновідомо, що сучасний розвиток будь-якої діяльності практично неможливий без широкого використання інформації. Банки досягли свого сучасного розвитку, завдячуючи насамперед широкому застосуванню інформаційних технологій у своїй діяльності. Тому інформація поряд з фінансовим ресурсом банку є досить важливим елементом у його діяльності. Існування інформації у різних видах — знання, документи, електронна інформація — робить її досить уразливою, а широке її використання в банках формує істотні загрози для банківської діяльності.

Разом з тим чинне законодавство і практика комерційної діяльності передбачають наявність серед інформаційного ресурсу банку особливу категорію інформації — відомості з обмеженим доступом, які головним чином і становлять той елемент структури банківської діяльності, щодо якого безпека банків і здійснює свій вплив.

Ураховуючи, що забезпечення безпеки банківської діяльності здійснюється в межах конкретного банку та його установ, останній тут буде суб'єктом, а зазначені вище елементи — об'єктами його безпеки.

У практиці забезпечення безпеки банківської діяльності великого значення набуває класифікація безпеки за її видами. Особливо така класифікація необхідна при організації безпеки в конкретних умовах банківської діяльності.

Залежно від походження загроз, джерел їх формування безпека поділяється на внутрішню та зовнішню. В основу такого поділу покладено різні підходи до організації безпеки, форми та методи застосування сил та засобів безпеки. Якщо при забезпеченні внутрішньої безпеки банки прагнуть мінімізувати загрози, які можуть надходити насамперед від персоналу та технологій банківського виробництва, то зовнішня безпека орієнтується передусім на загрози, що можуть утворюватися від недобросовісної поведінки клієнтів, злочинних посягань кримінальних елементів, актів недобросовісної конкуренції банків-конкурентів, негативних дій щодо банків інших суб'єктів. Звичайно заходи безпеки та методики їх застосування матимуть тут суттєві відмінності, і тому така класифікація визнана практикою діяльності сил безпеки як оптимальна.

З іншого боку, визначення об'єктів безпеки банківської діяльності обумовлює ще один підхід до класифікації видів безпеки, зокрема стосовно формування певних її напрямів за сукупністю відповідних заходів. Наприклад, персонал як об'єкт буде обумовлюватиме такий вид безпеки, як кадрова безпека, котра у свою чергу, поєднуватиме особисту та колективну безпеку. Особисту безпеку слід розуміти як здатність кожного працівника банку протистояти загрозам його здоров'ю, життю і професійній діяльності на основі оволодіння нормами і правилами безпечної поведінки. Досягається додержанням усіма працівниками заходів застереження, передбачених умовами роботи і нормами особистої поведінки: проведенням спеціальних заходів безпеки щодо працівників банку; вивченням кожним працівником правил поведінки у складних умовах та екстремальних ситуаціях, грамотними діями в них.

Водночас колективна безпека передбачає здатність підрозділів банку забезпечувати ефективний режим роботи в умовах діяльності різноманітних дестабілізувальних факторів. Досягається створенням доброзичливої, спокійної обстановки у колективах, додержанням принципів справедливості, грамотним

стимулюванням праці; постійним вивченням психологічної обстановки в колективах, своєчасним виявленням підвищеної напруженості у взаємовідносинах працівників, попередженням і швидким вирішенням конфліктних ситуацій; виконанням режимних заходів, охороною території, будівель і приміщень; постійною перевіркою стану будівель і обладнання, проведенням атестації приміщень, виконанням протипожежних заходів.

Поряд з цим фінанси та матеріальні цінності банку як об'єкти його безпеки обумовлюють ще один вид банківської безпеки — економічну безпеку. У даному випадку економічна безпека банку може розглядатись як стан банку, за якого забезпечується ефективне проведення ним операцій і угод, гарантоване збереження і раціональне використання фінансових ресурсів, матеріальних засобів і цінностей, грамотна експлуатація техніки й обладнання установ банків. Досягається створенням ефективного комплексу заходів захисту електронної системи платежів банку і попередження витоку коштів за допомогою фальсифікації фінансових документів; наявністю надійних місць зберігання готівки та цінностей; умілою експлуатацією технічних засобів, транспорту та обладнання банку; грамотною організацією охорони та режимних заходів у банку; створенням обстановки бережливого ставлення до майна банку, суворої і неминучої відповідальності за крадіжки матеріальних засобів та їх псування; ефективним плануванням заходів і додержанням правил пожежної безпеки; зваженою політикою керівництва банку в усіх сферах банківської діяльності, що забезпечує виправданий ризик та ефективне вкладання грошей; всебічним знанням і врахуванням особливостей ситуації у регіонах, країні та за її межами залежно від масштабів угод, прогнозуванням її розвитку і змін; наявністю інформації про внутрішнє та зовнішнє середовище діяльності банку, ділову, фінансову і виробничу активність клієнтів, їх правовий статус.

Наступним видом банківської безпеки можна вважати інформаційну безпеку, яку слід розуміти як стан інформаційних ресурсів банку, за якого забезпечується необхідний рівень інформованості його керівництва, персоналу, а також зовнішнього середовища, та ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз. Крім того, в умовах значного поширення інформаційних технологій впливу і перетворення окремих із них у один із видів інтелектуальної зброї важливою складовою інформаційної безпеки є протидія інформаційно-психологічному впливу на банк. Досягається

інформаційна безпека організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу в банку, аналітичною обробкою інформації; організацією системи інформаційного забезпечення рішень керівництва банку; категоріюванням банківської інформації та виробленням відповідних заходів щодо її захисту; дотриманням відповідних режимів інформаційної діяльності банку; виконанням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів витоку інформації та їх перетинанням, широкою пропагандою досягнень, переваг і перспектив банку.

Становлення та розвиток банківської безпеки відбувався під впливом різного роду факторів, які відчутно впливали на діяльність банків. На початку 90-х років минулого століття з виникненням комерційних банків банківська система зазнала досить відчутного впливу різного роду кримінальних посягань, що здійснювались у вигляді крадіжок і пограбувань банківських коштів і цінностей. Об'єктивно виникла необхідність забезпечити надійну охорону банківських установ, причому таку охорону, яка відповідала б умовам та специфіці банківської діяльності і була б не досить дорогою. Так, поряд з міліцейською охороною починають з'являтися власні сили охорони банків. Тобто забезпечення безпеки банків здійснювалось на той період лише на рівні заходів охорони, що було виправдано, оскільки її необхідність була досить актуальною.

Згодом, у середині 90-х років, у банківській діяльності стрімко почало поширюватись шахрайство з фінансовими ресурсами, недобросовісна конкуренція, різного роду посягання на банківську інформацію, від чого банки зазнавали досить істотних збитків. Виникла необхідність удосконалити безпеку банків, насамперед через установлення в банках особливого режиму їх функціонування. А це вимагало не тільки виконання нових функцій банківської безпеки, а й підвищення її якісного рівня. У банках установлюються відповідні режими їх безпеки, що насамперед було пов'язано з формуванням відповідних режимів використання фінансових ресурсів, банківської інформації, взаємовідносин із клієнтами, становленням внутрішньобанківської безпеки.

Бурхливий розвиток інформаційних технологій, систем автоматизації банківського виробництва, якісні зміни

інформаційного середовища банків висунули на одне з перших місць необхідність формування інформаційного ресурсу для забезпечення банківської діяльності. Достатність фінансових ресурсів сама по собі вже не вирішувала проблеми ефективної діяльності, необхідно було мати об'єктивні знання про сфери, регіони, об'єкти вкладання коштів з тим, щоб гарантовано отримати прибуток. І тому в кінці 90-х років банківська безпека починає виконувати ще одну функцію — інформаційного забезпечення банківської діяльності. Ураховуючи відставання правового регулювання безпеки бізнесу від реалій її розвитку, зазначена функція трансформувалася в інформаційно-аналітичне забезпечення діяльності банків на основі здійснення інформаційного моніторингу та інформаційного аудиту в середовищі відкритої інформації. З формуванням даної функції можна вважати, що становлення банківської безпеки завершилося.

Таким чином, сьогодні безпека банківської діяльності функціонує у трьох таких формах: охорони, режиму та інформаційно-аналітичного забезпечення. Заходи, що реалізуються у кожній з цих форм, використовуються в усіх видах безпеки, стосовно всіх її об'єктів і практично в усіх сферах банківської діяльності.

Характеризуючи банківську безпеку сьогодні, можна стверджувати, що основними підвалинами успіху є грамотна її організація, на що, на жаль, не завжди звертають увагу банківські керівники. Водночас правильно організована безпека відповідно до її принципів і вимог, з урахуванням особливостей діяльності конкретних установ банків та стану середовища їх функціонування може забезпечити високу ефективність і надійність роботи банків.

Організація безпеки в банку починається з вироблення відповідної Концепції (точки зору банку щодо забезпечення власної безпеки), відповідно до якої надалі і будується система безпеки. Концепція безпеки, як правило, приймається вищим керівним органом банку. Вона включає: характеристику ринку банківських послуг, особливості діяльності банку, можливі загрози йому, визначення основної мети та завдань безпеки банку, складу сил безпеки та їх функцій, структури системи безпеки та форми її діяльності, видів та порядку забезпечення виконання завдань безпеки, інші питання.

Основними організаторами безпеки є керівники установ банків. З питань безпеки до їхніх функцій належать такі:

- визначення мети безпеки банку, основних її завдань та напрямів зосередження зусиль безпеки;
- створення сприятливих умов для діяльності сил безпеки банку відповідно до їх функцій;
- контроль ефективності функціонування системи безпеки банку.

Керівник підрозділу безпеки є безпосереднім організатором проведення заходів безпеки у процесі діяльності банку. Він відповідає за організацію та ефективне проведення заходів безпеки, своєчасне інформування керівного складу банку про виникнення загроз. Особлива відповідальність керівника підрозділу безпеки полягає у своєчасному проведенні заходів, спрямованих на попередження дій конкурентів, недобросовісних клієнтів і працівників, кримінальних елементів, які можуть завдати шкоди банку.

До основних функцій керівника підрозділу безпеки банку можна віднести: керівництво роботою підрозділу безпеки, планування заходів безпеки банку, організація роботи сил безпеки щодо виконання заходів безпеки, інформування керівництва банку щодо стану безпеки банку та наявності загроз його діяльності, комплектування підрозділу безпеки, організація розроблення нормативно-правових документів з питань безпеки, контроль стану безпеки банку.

Великого значення з точки зору ефективності безпеки банківської діяльності набуває процес організації безпеки. Процес організації безпеки банку здійснюється на підставі аналізу загроз банку та основних завдань його діяльності, рішення керівника установи банку щодо організації безпеки її діяльності, наявності правових підстав для організації безпеки та можливості установи банку щодо забезпечення (фінансового, матеріального, кадрового, наукового і т. п.) функціонування створеної системи безпеки. У подальшому виконуються заходи щодо процесу організації безпеки установи банку (рис. 3.2).

Рис. 3.2. Структура процесу організації безпеки банку

Великого значення в процесі організації безпеки набуває визначення заходів безпеки та структури її сил. Оскільки до складу сил безпеки мають бути залучені всі підрозділи банку відповідно до їх функцій, заходи безпеки матимуть як загальний характер (стосуватись усіх підрозділів), так і певну специфіку для підрозділів безпеки банку. Виходячи з досвіду забезпечення безпеки банківської діяльності до загальних заходів безпеки слід віднести:

- забезпечення організаційно-правового впливу на діяльність та поведінку персоналу і клієнтів банку з питань дотримання ними встановленого в банку режиму безпеки;
- підбір, перевірка і контроль роботи персоналу, розроблення ефективної кадрової політики і програм стимулювання праці;
- введення внутрішньооб'єктового режиму діяльності банку;
- удосконалення технологій банківського виробництва, введення в них елементів захисту;
- формування позитивного іміджу банку;
- планування і забезпечення діяльності банку в кризових та екстремальних ситуаціях;
- забезпечення безпеки споруд і будівель установ банків, їх комунікаційних систем;
- створення систем сповіщення персоналу банку;

• установлення відповідальності за порушення правил безпеки банківської діяльності.

Спеціальними заходами можуть бути:

✓ проведення інформаційно-аналітичної роботи (ведення комерційної розвідки) в банку з метою формування його інформаційного ресурсу;

✓ інформаційно-аналітичні дослідження клієнтів, партнерів і конкурентів банку під час проведення банківських операцій;

✓ взаємодія з правоохоронними органами з питань забезпечення безпеки діяльності банку;

✓ проведення заходів з протидії виявленню, локалізації дій та актів недобросовісної конкуренції і промислового шпигунства;

✓ організація охорони банку;

✓ захист інформаційних ресурсів банку і проведення заходів з протидії інформаційно-психологічного впливу на банк, організація спеціального діловодства;

✓ проведення службових розслідувань у банку;

✓ проведення заходів щодо дезінформації конкурентів;

✓ забезпечення впливу на недобросовісних клієнтів, боржників і зловмисників щодо відшкодування банку заподіяних з їх вини збитків.

Виконання заходів безпеки забезпечується через діяльність сил безпеки і використання різноманітних засобів. Залежно від форми організації безпеки до її забезпечення можуть залучатися: підрозділи безпеки банків, спеціалізовані фірми, організації, які надають банкам послуги безпеки, підрозділи та персонал банків. До засобів безпеки відносять технічні засоби охорони, програмні й технічні засоби захисту інформації, спеціальні засоби і техніка, інженерно-технічні засоби обмеження доступу, засоби зв'язку, обробки і передання інформації та інше обладнання і техніка, які використовуються для забезпечення ефективної реалізації заходів безпеки.

Підрозділи безпеки у банках створюються відповідно до сфер, напрямів діяльності банків, завдань безпеки та форм її організації. Крім того, на структуру підрозділів впливатимуть можливості банку, обсяг операцій, що він проводить, політика керівництва банку щодо організації безпеки. Як варіант, структура підрозділу (служби, управління, департаменту) безпеки може бути такою:

• керівник підрозділу;

• експертна група для оперативного вирішення проблем, що раптово виникають (може складатися з 3–4 працівників, як

• підрозділ охорони (може включати групи: охорони території та об'єктів, інкасації, особистих охоронців, технічних засобів охорони);

• інформаційно-аналітичний підрозділ (може включати групи: збирання інформації, обробки інформації, зв'язків із пресою, технічну);

• підрозділ захисту інформації (може включати групи: режиму; психологічного контролю; зовнішнього захисту — для взаємодії з правоохоронними органами, підрозділами безпеки інших банків, охоронними та детективними фірмами, органами влади; фінансової безпеки та технічну).

Зазвичай підрозділ безпеки у своїй структурі має групи чи окремо фахівців відповідно до форм організації безпеки. Практика банківської діяльності показує, що банки можуть у структурі сил безпеки мати й інші підрозділи: економічної, внутрішньої безпеки, захисту операцій з пластиковими платіжними засобами, роботи з проблемною кредитною заборгованістю та ін. Незалежно від структури зазначених підрозділів безпеки банків на них можуть покладатися такі функції:

адміністративно-розпорядницька — реалізується через розроблення, установлення і підтримку в банку різних режимів безпеки, визначення повноважень, прав, обов'язків і відповідальності службовців банку з питань забезпечення безпеки;

обліково-контрольна — забезпечується через організацію своєчасного виявлення реальних і потенційних загроз діяльності банку, контролю за джерелами таких загроз і несприятливими для банку ситуаціями і факторами; виявлення критичних напрямів фінансово-комерційної діяльності банку; накопичення інформації з проблем забезпечення безпеки банку;

соціально-кадрова — реалізується через участь підрозділу безпеки в підборі, перевірці і розстановці кадрів; виявлення негативних тенденцій у колективах підрозділів банку, можливих причин та умов виникнення соціального напруження; попередження і локалізації можливих конфліктів; формування у службовців банку почуття відповідальності за забезпечення безпеки банку;

організаційно-управлінська — реалізується через організаційне, матеріально-технічне і технологічне забезпечення

режимів безпеки в банку;

методична — реалізується через виявлення, накопичення й упровадження в банку позитивного досвіду з організації банківської безпеки; організації навчання працівників банку з питань безпеки; розроблення методик роботи персоналу банку і підрозділу безпеки щодо забезпечення безпеки проведення банківських операцій;

інформаційно-аналітична — забезпечується через цілеспрямоване збирання, накопичення, обробку і розподіл відповідної інформації, створення для цього необхідних технічних і програмних засобів.

Завершенням організації безпеки банку є створення відповідної системи безпеки, яку можна розуміти як сукупність заходів, технологій їх виконання, сил і засобів безпеки, спрямованих на формування здатності банку протистояти різноманітним загрозам його діяльності. Тобто, основними складовими системи безпеки банку є сили, засоби, способи забезпечення безпеки та технології виконання зазначених способів. Формування досконалої системи безпеки банку залежить від умов та особливостей його діяльності, можливостей банку та часу, який відводиться на створення такої системи.

Оскільки система безпеки банку спирається на його персонал (сили безпеки), у банку виробляються загальні обов'язки персоналу щодо підтримання встановленого режиму безпеки, а крім того, кожен працівник має свої специфічні, відповідно до його посади, обов'язки щодо забезпечення безпеки банку на конкретному робочому місці. До загальних обов'язків щодо дотримання встановленого в банку режиму безпеки можна віднести:

- дотримання працівниками встановленого в банку режиму безпеки;
- зберігання в таємниці всіх службових відомостей, про які відомо працівникам банку у зв'язку з виконанням ними посадових обов'язків, утримання інших службовців від розголошення відомостей, які є банківською чи комерційною таємницею або конфіденційною інформацією банку;
- виконання встановленого порядку і правил роботи з документами й виробами всіх категорій таємності, а також з клієнтами, партнерами та відвідувачами банку;
- за вимогами представників підрозділу безпеки надавати для перевірки матеріали, що рахуються за працівником банку, в яких є відомості, що становлять банківську або комерційну таємницю чи

- ретельне і з необхідною ефективністю виконання встановлених правил і порядку проведення банківських операцій, запобігання заподіянню банку збитків або шкоди, не допускати порушення встановлених в банку заходів безпеки при проведенні банківських операцій;
- дотримання встановлених правил ведення службових переговорів і передання інформації на всіх лініях зв'язку, використання розмножувальної техніки та роботи з програмними засобами;
- не використовувати на роботі та в приміщеннях банку власну кіно-, відео- і фотоапаратуру, технічні засоби банку з корисливою метою та як розважальні засоби;
- знати, кому з працівників банку дозволено працювати з відомостями, до яких допущено даного працівника, і в якому обсязі такі відомості можуть доводитись до цих працівників. У випадках спроби сторонніх осіб чи організацій отримати інформацію, що становить банківську або комерційну таємницю та конфіденційну інформацію, працівники банку зобов'язані повідомляти про це безпосереднього керівника та службу безпеки.

Таким чином, ураховуючи основні теоретичні засади безпеки банківської діяльності можна стверджувати, що вона являє собою, з одного боку, невід'ємну частину банківської діяльності, а з другого — складний і трудомісткий процес, який вимагає досить серйозних інтелектуальних, матеріальних, фінансових, фізичних зусиль. Разом з тим, зазначені зусилля мають спиратися на грамотні, науково обґрунтовані та досліджені практикою погляди професіоналів, здатних фактично реалізувати будь-яку концепцію безпеки того чи того суб'єкта господарювання.

РЕЗЮМЕ

Незважаючи на значний досвід забезпечення безпеки підприємницької діяльності в зарубіжних країнах та безпосередньо в Україні, продовжує точитись полеміка щодо сутності поняття «безпека бізнесу». Відсутність відповідних правових норм з даного питання обумовлює не тільки різні підходи до визначення суті поняття, а й різну ефективність забезпечення безпеки.

Разом з тим в Україні напрацьовано певні теоретичні та організаційні засади безпеки підприємницької діяльності, які формують відповідну методологію її забезпечення безпосередньо в діяльності суб'єктів господарювання. Зокрема, існують обґрунтовані твердження щодо мети та завдань безпеки, її видів, принципів і вимог до неї, об'єктів безпеки існує практично єдине розуміння щодо класифікації форм безпеки, ролі і місця персоналу суб'єктів господарювання у формуванні та дотриманні режимів безпеки, немає розбіжності в розумінні та практичному застосуванні заходів безпеки.

Ці та інші засади дають змогу ефективно організовувати безпеку підприємницької діяльності в усіх сферах економіки, у тому числі і на ринку банківських послуг.

Терміни і поняття

Безпека банківської діяльності
Види безпеки банківської діяльності
Вимоги до безпеки банківської діяльності
Завдання безпеки банківської діяльності
Мета безпеки банківської діяльності
Об'єкти безпеки банківської діяльності
Підрозділ безпеки банку
Принципи безпеки банківської діяльності
Система безпеки банку
Стабільність економічного розвитку банку
Структура процесу організації безпеки банку

Питання для перевірки знань

1. Від чого залежить ефективність безпеки банківської діяльності?

2. Чому розуміння безпеки банків та їхньої діяльності як стану захищеності не може вважатися повним і є таким, що не відображає об'єктивної суті поняття безпеки банківської діяльності?

3. Чому, даючи визначення поняття безпеки, слід керуватися такими характеристиками, як стан, властивість і здатність?

4. Як співвідносяться між собою поняття «безпека» і «небезпека»?

5. Що є метою безпеки банківської діяльності?

6. Якщо одним із завдань безпеки банківської діяльності є захист інтересів працівників банків, то чи значить це, що банківська безпека повинна передбачати охорону їхньої власності?

7. Що має передбачати принцип централізованого управління забезпеченням безпеки банківської діяльності?

8. Що слід розуміти під вимогою безперервності безпеки банківської діяльності?

9. Чому саме працівники є основною запорукою забезпечення надійного режиму безпеки банку?

10. Як може впливати особиста безпека працівника на забезпечення безпеки діяльності банку?

11. Що передбачає Концепція безпеки банку?

12. Яким чином може реалізовуватися методична функція підрозділу безпеки банку?

13. Хто має здійснювати контроль виконання заходів безпеки в банку?

14. Чи можна вважати якісне виконання працівниками банку своїх посадових обов'язків одним із елементів забезпечення його безпеки?

15. З яких елементів складається система безпеки банку?

ЗАВДАННЯ ДЛЯ ІНДИВІДУАЛЬНОЇ РОБОТИ

1. Розробивши Концепцію безпеки діяльності банку, начальник підрозділу безпеки подав документ на розгляд Правлінню банку. Через деякий час документ повернули з резолюцією одного із заступників керівника банку, в якій ішлося про необхідність ознайомлення з документом керівників інших підрозділів. Останні ж під час ознайомлення висловили незгоду з багатьма положеннями Концепції. У свою чергу, начальник підрозділу безпеки зауважив,

що вони — не фахівці у цій справі і не можуть судити про доцільність та правильність положень Концепції. З'явились ознаки конфліктної ситуації. Чому так сталось і як уникнути конфлікту?

2. Ви — керівник служби безпеки банку. Одного разу до вас звернувся керівник установи банку і сказав, що витрати на забезпечення безпеки діяльності банку є дуже великими і в майбутньому це може призвести до збитків банку. Ураховуючи це, він поставив вам завдання перевірити доцільність таких витрат і розглянути питання щодо можливості їх зниження, аби тим самим дотримуватися такого принципу безпеки, як економічна доцільність. Як ви будуватимете свою роботу, щоб виконати розпорядження керівника банку?

3. Ви — працівник банку щойно призначений на посаду. У перший свій робочий день з вами провів інструктаж працівник підрозділу безпеки, де він ознайомив вас з обов'язками працівника банку щодо виконання вимог безпеки діяльності вашого банку. Зокрема, він зазначив, що в процесі своєї роботи в банку ви не повинні допускати порушень установлених у банку заходів безпеки, але яких саме він не пояснив. Як ви гадаєте, які саме заходи безпеки мав на увазі працівник підрозділу безпеки, яких ви, як працівник банку, повинні дотримуватися?

Література для поглибленого вивчення

1. *Гамза В. А.* Безопасность банковской деятельности / В. А. Гамза, И. Б. Ткачук. — М. : Маркет, 2010. — 408 с.
2. *Зубок М. І.* Безпека банків : навч. посіб. / Зубок М. І. — К. : КНТЕУ, 2002. — 306 с.
3. *Зубок М. І.* Безпека банківської діяльності : навч. посіб. / Зубок М. І. — К. : КНЕУ, 2002. — 190 с.
4. *Зубок М. І.* Безпека бізнесу : навчальний посібник у схемах і таблицях / Зубок М. І., Позднишев Є. В., Яременко С. М. — К.: КНЕУ, 2008. — 480 с.
5. *Зубок М. І.* Основи безпеки комерційної діяльності підприємств та банків : навч.-метод. посіб. / Зубок М. І. — К. : КНТЕУ, 2005. — 201 с.

Розділ 4

ЗАГРОЗИ БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *еволюцію загроз банківській діяльності, ознаки їх реалізації безпосередньо в банку;*
- ✓ *види та динаміку загроз на вітчизняному ринку банківських послуг;*
- ✓ *форми та методи шахрайських посягань на кошти банків під час проведення банківських операцій;*
- ✓ *основні способи втягування банків у незаконну фінансову діяльність;*
- ✓ *ознаки та способи рейдерських посягань на власність банків;*
- ✓ *сутність тероризму та його загрози вітчизняним банкам особливо в умовах глобалізації та інтеграції капіталу,*

*а також **уміти**:*

- ✓ *виявляти загрози банківській діяльності в процесі виконання своїх обов'язків у банках, визначати їх джерела та причини;*
- ✓ *обґрунтовувати небезпечність загроз і можливі наслідки їх реалізації для діяльності банку;*

✓ *визначати умови ймовірності виникнення загроз на різних етапах банківської діяльності.*

4.1. Формування та класифікація загроз банківській діяльності

Розглядаючи безпеку банківської діяльності як систему протидії різного роду небезпекам і загрозам та захисту від них виникає необхідність ретельніше вивчити саму суть небезпеки та загрози, їх еволюцію, причини та умови виникнення, а також негативне значення для банків.

Незважаючи на досить часте застосування в банківській діяльності таких понять, як ризик, небезпека, загроза, сьогодні існує досить багато точок зору щодо визначення їх суті та об'єктивного розуміння. Водночас правильне розуміння даних понять формує і відповідну реакцію на них, насамперед з погляду ефективного забезпечення банківської безпеки. Узагальнюючи думки науковців та фахівців, зайнятих у сфері безпеки бізнесу, та використовуючи власний досвід, автори дійшли висновку, що еволюція загроз здійснюється за схемою, наведеною на рис. 4.1.

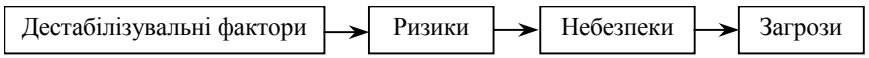

Рис. 4.1. Еволюція загроз

Дестабілізуючими факторами є певні процеси, явища, поведінка, які своєю дією здатні змінювати ситуацію, формуючи несприятливі умови для певної діяльності (в даному разі банківської), визначаючи її характер або окремі риси і зумовлюючи відповідні відхилення від планових нормативів та стандартів. Один і той самий фактор в одному випадку (для одного банку) може бути сприятливим, а за інших умов (для іншого банку) зовсім ні. Наприклад, дестабілізуючими факторами для банків є інфляція, обмеженість джерел залучення фінансових ресурсів, певна поведінка окремих осіб, громадських об'єднань, обмеженість надійних клієнтів та безліч інших.

При потраплянні банків у зону дії дестабілізуючих факторів їх сукупність або відсутність адекватної реакції на них з боку банків формує певний ризик в діяльності останніх. Стосовно розуміння поняття «ризик» існує також багато різних підходів,

але, враховуючи його економічну суть, ми можемо схилитися до тих тверджень, які вбачають у цьому понятті імовірність одержання негативного результату. У даному разі мається на увазі ймовірність отримання негативного результату в банківській діяльності від впливу саме дестабілізуючих факторів. Імовірність отримання негативного результату розуміється як математична числова характеристика ступеня можливості появи такого результату, тобто тут ризик розуміється як вираз випадковості. За таких умов, визначивши через певну масу випадковостей відповідну закономірність, можна визначити і величину ризику для дії тих чи тих дестабілізуючих факторів у банківській діяльності. На основі подібних розрахунків можуть бути розроблені відповідні методики мінімізації ризиків як забезпечення впливу на ситуацію, що створюється дестабілізуючими факторами. Головним же завданням банківської безпеки тут буде виявлення джерел, які формують дестабілізуючі фактори, визначення умов та причин формування таких факторів і підстав, за яких такі фактори можуть припиняти чи послаблювати свою негативну дію щодо банків.

Оскільки в банківській діяльності як виду комерції обов'язково присутній ризик і ця діяльність завжди здійснюється в ситуаціях невизначеності, необхідність своєчасного і об'єктивного встановлення наявності та впливу дестабілізуючих факторів є досить актуальною і такою, що забезпечує живучість банків на ринку.

Ризики у разі відсутності заходів їх мінімізації чи ігнорування їх мають властивість накопичуватись або зростати і формувати небезпечні ситуації в будь-якій діяльності, у тому числі і в банківській. Аналіз різних трактувань поняття небезпеки показує, що остання характеризує певний стан об'єкта, ситуації, поведінки. Небезпечну ситуацію, поведінку розуміють як таку, що містить ненадійність, шкоду, взагалі негатив. Але водночас слід розуміти, що небезпека сама по собі не завдає шкоди, вона може реалізовуватися тільки через певну загрозу. Негативний прояв небезпеки здійснюється лише за відповідних умов, за яких небезпека формується в загрозу і набуває властивості діяти — погрожувати відповідним негативом. Тобто на відміну від небезпеки, яка характеризує певний стан ситуації, поведінки, явища, загроза являє собою відповідну небезпечну дію, яка формується і проявляється за наявності необхідних і достатніх для цього умов. Виходячи з цього слід зазначити, що загрози завжди конкретні. Конкретність їх проявляється в тому, що вони

мають свого суб'єкта, свій об'єкт і предмет (спосіб впливу). Якщо властивістю небезпек є їх накопичення, то властивістю загроз є їх формування в масі небезпек. У більш небезпечному середовищі імовірність формування загроз збільшується, і навпаки, у середовищі з меншою небезпекою імовірність формування загроз зменшується.

За ступенем сформованості загрози поділяються на потенційні (характеризують небезпечну ситуацію, в якій за певних умов можуть сформуватися загрози) і реальні (в наявності ситуація, в якій загрози уже повністю сформувались і мають конкретну спрямованість: суб'єкт, об'єкт, спосіб реалізації, факт їх безпосередньої дії характеризується лише часом.

Таким чином, під загрозою банківській діяльності можна розуміти потенційні чи реальні дії певних суб'єктів, здатні завдати конкретному банку матеріальної або моральної (шкодити іміджу банку) шкоди.

Існує досить багато підходів до класифікації загроз: за походженням, за спрямованістю, за ступенем сформованості, за сферою діяльності, за ступенем суб'єктивного сприйняття і т. д. Не вдаючись до розкриття всіх підходів до класифікації загроз, зупинимося лише на тих із них, які мають суттєве значення для розгляду питань, пов'язаних із забезпеченням безпеки банківської діяльності. Насамперед важливою є класифікація за походженням суб'єктів загроз. Тут загрози класифікуються як внутрішні та зовнішні.

Внутрішні загрози банку обумовлюються насамперед непрофесійною діяльністю його працівників, недобросовісною, конфліктною, злочинною їх поведінкою. Крім того, внутрішні загрози можуть утворюватися від використання недосконалих, неефективних технологій банківського виробництва або інформаційного забезпечення, неадекватного банківській діяльності внутрішньооб'єктового режиму в установах банків. За всіх умов джерелом таких загроз є персонал банку, особи, що залучені до забезпечення його діяльності, а також самі банківські технології.

Найпоширенішою серед загроз, які надходять від персоналу банку, є непрофесійна його діяльність, особливо на низовій ланці виконавців. Крім того, значне місце в таких загрозах займає шахрайство з фінансовими ресурсами банку, фінансовими інструментами, пластиковими платіжними засобами. Слід звернути увагу, що за обсягами завданої банкам шкоди їх працівниками, шахрайство стоїть на першому місці. Причому

схеми шахрайських дій, як правило, кожного разу застосовуються більш досконалі, а то й зовсім нові.

Поширеними в банку є і крадіжки майна або безпосередньо коштів, скоєні його персоналом. Значне місце займає фальсифікація документів, касових та бухгалтерських книг, договорів, сум на банківських рахунках, підроблення документів, оплата особистих рахунків коштами банків, «відкати» за надані послуги, використання створених працівниками банків фіктивних фірм, незаконне використання з корисливою метою майна банків, штучне внесення змін у бухгалтерський облік, приховане (під виглядом отримання авансових сум) кредитування, несанкціоноване поширення банківської інформації, модифікація електронної інформації в системі електронних платежів, оплата невиконаних робіт, створення конфліктних ситуацій у колективах та ін. Як бачимо, перелік негараздів, які може отримати банк від своїх працівників досить великий і такі негаразди мають тенденцію до ускладнення.

Динаміку розвитку банківської злочинності можна простежити на основі даних, наведених у табл. 4.1.

Таблиця 4.1

ДИНАМІКА РОЗВИТКУ БАНКІВСЬКОЇ ЗЛОЧИННОСТІ ЗА 1996—2009 РР.

Показник	Роки								
	1996	1997	1998	1999	2000	2001	2002	2008	2009
Кількість злочинів, скоєних безпосередньо в банках (за участі його працівників)	765	1078	953	1005	927	657	877	1264	1531

Особливо вплинула на банківську злочинність фінансово-економічна криза 2008—2009 рр. Банківська злочинність у цей період зростала не тільки кількісно, а й масштабно. Кожен шостий злочин (уього — 724) — зі збитками понад 100000,00 грн (у 2008 р. — 675), 137 злочинів — зі збитками понад 1 млн грн (у 2008 р. — 81). Загальна сума збитків банків за порушеними кримінальними справами склала 200,06 млн грн (у 2008 р. — 89,6 млн грн) [143; 144; 169].

Аналіз розкритих у банках злочинів показує, що останнім часом вони концентруються навколо зловживання працівниками банків службовим становищем, шахрайства з фінансовими

ресурсами, розкрадання грошових коштів та майна банків. Об'єктом посягань були кредитні ресурси та фонди, майно банків та заставне майно клієнтів.

Органи МВС України повідомляють, що службові особи банків розкрадають кошти вкладників, які перебувають на депозитних рахунках, через підробку банківських документів та переказування грошових коштів на розрахункові рахунки інших суб'єктів господарювання, які перебувають у змові зі службовцями банків; розкрадають кошти банків, оформлюючи фіктивні кредитні угоди на втрачені документи громадян або використовуючи завірені копії документів вкладників, котрі мали чи мають банківські депозити; отримують хабарі, переважно за надані кредити; оформлюють кредити на підставних осіб, без відома позичальників; по фіктивних документах перераховують кошти банків за кордон на власні рахунки; видають клієнтам фальшиві банкноти і т. п. [73; 120]. То ж не дивно, що тільки за 2009 рік до кримінальної відповідальності притягнуто 903 особи, з яких 52 — керівники філій і відділень банківських установ, 153 — інші службові особи банків та 272 особи, що учинили злочини у складі груп [136].

Наведені вище дані свідчать про те, що працівники банків можуть створювати досить суттєві загрози, і за певних умов їхня «діяльність» може завдавати банкам істотної шкоди.

Водночас необхідно звернути увагу на особливість суспільної оцінки банківської злочинності.

Існує думка, що загрози можуть спричиняти тільки недобросовісні працівники, або такі, що мають негативні вади характеру, поведінки чи ті, хто у минулому мав проблеми з законом та притягувався до відповідальності. Практика показує, що це хибна думка, до створення загроз можуть вдаватись і звичайні працівники, які не характеризуються зазначеними недоліками, але через певні обставини можуть спокуситись або ж бути змушеними порушувати певні правила роботи чи законодавства, щиро переживаючи за прояв такого негативу в їхній поведінці.

Практика забезпечення банківської безпеки показує, що основними причинами формування загроз у діяльності і поведінці персоналу банків є:

- непрофесійні дії працівників банків;
- низький стан виховної та профілактичної роботи в банках;
- недосконала система заробітної плати і стимулювання праці персоналу банків;

- порушення правил кадрової роботи, невідповідність кадрової політики умовам роботи банків;
- психологічні та комунікаційні особливості працівників банків;
- відсутність нормативної бази банків, яка встановлювала б режими їх діяльності та правила поведінки персоналу;
- низький стан трудової і виробничої дисципліни, слабка вимогливість керівного складу банків до персоналу;
- відсутність адекватної ситуації системи кадрової безпеки в банках.

Загрози, що виникають унаслідок недосконалих технологій можуть обумовлюватися використанням високозатратних матеріалів, обладнання, програмного забезпечення, у цілому технологій, а також технологій, у яких відсутні елементи захисту або такі елементи неадекватні ситуації, в яких проводиться та чи інша банківська операція. Сюди ж слід віднести і недосконаліть або взагалі відсутність методик, які регулювали б дії різних підрозділів банку при проведенні певних операцій, узгоджували такі дії щодо впливу на ситуацію, забезпечували контроль за проведенням операцій по всіх їх етапах. Такі недоліки формують певні передумови і для негативної поведінки окремих працівників, пов'язаної з безконтрольним використанням коштів банків, порушенням режимів їхньої діяльності.

Основними суб'єктами зовнішніх загроз для банків можуть бути:

- їх конкуренти;
- особи, що здійснюють кримінальну діяльність, та кримінальні угруповання;
- клієнти та партнери банків;
- органи контролю та нагляду;
- окремі недобросовісні працівники державних установ, правоохоронних органів та органів влади;
- засоби масової інформації;
- колишні працівники банків;
- спецслужби іноземних держав, пов'язані з ними особи і організації, метою діяльності яких є добування економічної інформації;
- особи та організації, що займаються рейдерською діяльністю;
- особи та організації, в діях яких є ознаки терористичної діяльності.

Крім того, зовнішні загрози для банків можуть зумовлюватися стихійними лихами та техногенними аваріями і катастрофами,

що можуть виникати поблизу установ банків і своїми уражаючими факторами загрожувати їм.

Особливий вид загроз для діяльності банків може створюватися через певну політичну ситуацію як у країні, так і в окремих її регіонах. Розбалансованість у діяльності органів влади, негативні наслідки реформування економіки, корупція, загострення кримінальної ситуації, обмеження демократичних досягнень суспільства можуть створювати ситуації тривалого чи навіть постійного підвищеного ризику в діяльності банку, агресивної поведінки до банків з боку їхніх клієнтів, недовіри населення до банків. Результатом, як правило, є відплив залучених банками коштів, зниження їх ліквідності та платоспроможності.

Приклад негативного впливу негараздів, пов'язаних з політичною й економічною нестабільністю можна спостерігати в трансформації довіри населення до вітчизняних банків. Зміни рівня довіри до банків у період політичної та економічної кризи 2008—2009 рр. в українському суспільстві проілюстровано даними, наведеними в табл. 4.2.

Таблиця 4.2

ЗМІНИ РІВНЯ ДОВІРИ ДО БАНКІВ У ПЕРІОД ПОЛІТИЧНОЇ ТА ЕКОНОМІЧНОЇ КРИЗИ 2008—2009 РР. В УКРАЇНСЬКОМУ СУСПІЛЬСТВІ

Рівень недовіри, % «абсолютно не довіряю» та «не довіряю»			Рівень довіри, % «абсолютно довіряю» та «довіряю»			Баланс довіри і недовіри		
09.07	11.08	03.09	09.07	11.08	03.09	09.07	11.08	03.09
28,4	56,4	55,1	26,9	11,7	8,5	–1,5	–44,7	–46,6

Така ситуація обернулася для банків загрозою відпливу депозитних коштів. З 1 січня 2008 р. до 1 жовтня 2009 р. із рахунків гривневих депозитів у вітчизняних банках було знято 29,226 млрд грн, а з валютних — 3,74 млрд дол. США [139]. За даними Асоціації українських банків, у першому кварталі 2009 р. відплив з депозитних рахунків досяг 47 млрд грн, тоді як у 2008 р. за аналогічний період приплив коштів по банківській системі становив 15 млрд грн [134].

Зовнішні загрози проявляються в діяльності банків як недобросовісна конкуренція, розбійні напади на банки з метою заволодіння його коштами, розголошення банківської інформації, що має обмежений доступ, неповернення (несвоєчасне

повернення) банківських коштів, створення несприятливої моральної обстановки навколо банків поширенням негативної інформації про їхню діяльність, дестабілізація роботи установ банків від численних перевірок, примушення банків до проведення неефективних, збиткових операцій, незаконне поглинання банків іншими банками чи організаціями, замахи на працівників банків та захоплення їх у заручники, обмеження діяльності банків певними актами органів влади чи іншими державними органами, руйнування будівель банків, виведення з ладу їх обладнання і т. п. Звичайно, наявність такого негативу для банків завжди призводить не тільки до дестабілізації їхньої роботи, а й до втрати ними ліквідності і навіть ліквідації їх. Принаймні, банки в таких ситуаціях не можуть якісно здійснювати покладені на них функції, фінансувати економіку країни та забезпечувати фінансову стабільність держави. Тобто зовнішні загрози досить суттєво впливають не тільки на безпеку самих банків, а й через них загрожують національній безпеці держави, у чому і полягає їх особлива небезпечність.

Відповідно до сфери поширення та об'єктів впливу загрози поділяються на економічні, фінансові та інтелектуальні.

Економічні загрози можуть реалізовуватись у формі корупції, шахрайства, недобросовісної конкуренції, використання банками неефективних технологій банківського виробництва, рейдерства. Реалізація таких загроз веде до заподіяння збитків банкам, упущення ними вигоди або взагалі втрати ліквідності.

Основними причинами виникнення економічних загроз можуть бути: недостатня адаптація банківської системи до постійно змінюваних умов ринку; загальна неплатоспроможність суб'єктів господарювання; зростаюча злочинність; споживчий менталітет значної кількості громадян; низький рівень трудової дисципліни та відповідальності працівників банківських установ; недостатнє правове регулювання банківської діяльності; низький професійний рівень частини керівного складу і працівників банку та ін.

Фізичні загрози реалізуються у формі крадіжок, пограбувань майна та коштів банків, поломок, виведення із ладу обладнання банків, неефективної його експлуатації. Унаслідок реалізації таких загроз завдаються збитки банкам, пов'язані з втратою їхньої власності та необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних ресурсів. Основними причинами фізичних загроз є неефективна кадрова політика банку, низька професійна підготовка

банківських фахівців, недостатній рівень охорони та режим безпеки установ банків, низький контроль стану роботи працівників банків.

Інтелектуальні загрози проявляються як розголошення або неправомірне використання банківської інформації, дискредитація банків на ринку банківських послуг, а також можуть бути реалізованими у формі різного роду соціальних конфліктів навколо банківських установ або в них самих. Крім того, до інтелектуальних загроз слід віднести проведення проти банків психологічних та ідеологічних диверсій. Результатом реалізації таких загроз можуть бути збитки банків, погіршення їх іміджу, соціальна чи психологічна напруженість навколо установ банків або в їх колективах, дестабілізація внутрішньої роботи банків. Причинами таких загроз, як правило, є загострення конкуренції на регіональних ринках банківських послуг, неефективна кадрова політика банків, порушення принципу гласності результатів банківської діяльності, відсутність або низька ефективність заходів інформаційного режиму в банках, порушення банками банківського законодавства.

Реалізація загроз має свої особливості відповідно до об'єктів загроз. Для повнішого розуміння можна зазначити, що основними об'єктами загроз банку можуть бути персонал, фінанси, матеріальні цінності та інформація банку.

Що стосується персоналу банку, то загрози можуть призводити до моральних або фізичних страждань окремих осіб через вбивство їхніх близьких, родичів або друзів, захоплення заручників, психологічний терор чи шантаж, заподіяння тілесних ушкоджень, вимагання, втрати матеріальних цінностей і т. п.

Загрози фінансам банку можуть реалізовуватися через крадіжки фінансових ресурсів банку, шахрайство з коштами банку, фальсифікацію фінансових документів та інструментів, підробку банкнот, збитки від недосконалих технологій банківського виробництва.

Матеріальним цінностям банку може загрожувати пошкодження будівель, приміщень та іншої нерухомості, виведення з ладу засобів зв'язку і систем комунального обслуговування, пошкодження, крадіжки банківського обладнання, техніки, транспортних засобів.

Інформаційні загрози можуть реалізовуватися через несанкціоноване ознайомлення сторонніх осіб з відомостями банку, що мають обмежений доступ, модифікацію банківської інформації, її знищення або розголошення.

4.2. Банківське шахрайство і зловживання службовим становищем працівників банків

Однією з найбільш поширених загроз діяльності банків, яка за своїм походженням може бути як внутрішньою, так і зовнішньою, є банківське шахрайство. Правова оцінка шахрайства дана у Кримінальному кодексі України, де шахрайство визначається як зловживання довірою, обман з метою введення власника матеріальних цінностей або коштів в оману і на тій основі добровільного передання ним своєї власності шахраям.

Слід зазначити, що в умовах народження і становлення ринкових відносин шахрайство є досить поширеним явищем, оскільки звичайні, і нестандартні форми бізнесу можуть здійснюватися в рамках чинного законодавства. Інколи просто неможливо визначити, що мається на увазі: нова форма бізнесу, афера чи незловмисно допущена помилка. Тому небезпечність шахрайства завжди була і є досить актуальною, особливо в банківській сфері, коли банк може непомітно втратити значний капітал.

Основною особливістю шахрайства є те, що в основу заволодіння чужим майном чи правом на майно зловмисник покладає обман і зловживання довірою, у результаті чого власник добровільно передає належне йому майно чи уступає право на нього (рис. 4.2).

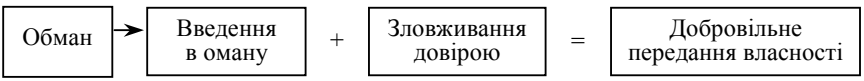

Рис. 4.2. Формула шахрайства

Основними видами шахрайського обману в банках є надання неправдивих відомостей клієнтами або іншими особами про себе і свою діяльність, приховування обставин і фактів, здійснення фіктивного підприємництва, фальсифікація товарів і послуг. Зловживання довірою відбувається як через цивільно-правові відносини, так і переданням власності (права власності) без застережень і відповідного оформлення.

Однією з мотиваційних засад шахрайства, особливо на ринку банківських послуг, є загальний інтерес до грошей. Деякі фахівці банківської справи цілком логічно стверджують, що в банківській діяльності незацікавлених осіб немає. Тому використання банківських коштів має здійснюватися виключно на високопрофесійній основі, маючи про об'єкт вкладання коштів об'єктивну інформацію, яка сформована на основі власних знань, а не отриману від самого об'єкта. Недотримання цього принципу якраз і дає змогу шахраям реалізувати свій шахрайський задум. Один із фахівців у сфері забезпечення соціально-економічної безпеки професор Дзлієв М. І., маючи на увазі шахрайство, стверджує, що у сфері фінансів мистецтво нападу набагато випереджає мистецтво захисту, а у світі достатньо людей, здатних переконати будь-кого в будь-чому, як і людей, здатних піддатися на такі переконання [90]. Тому шахрайство у фінансовій сфері і залишається таким живучим, незважаючи на всілякі протидії йому. Слід також враховувати, що підприємницька діяльність, у тому числі і на ринку банківських послуг, здійснюється в умовах досить великої кількості різного роду нормативних актів. Жоден юрист чи фінансовий працівник не може оволодіти всією сукупністю положень, інструкцій, правил, наказів, що постійно змінюються, особливостями їх застосування на практиці, на які може спиратися шахрай, вводячи їх в оману.

Тут слід також зазначити, що шахраї, як правило, досить професійно володіють не тільки мистецтвом обману, а й сферою знань, у якій вони здійснюють шахрайство. Практика показує, що неграмотних шахраїв не буває. Шахраї перетворюють свої знання в своєрідний шахрайський бізнес. Вдала шахрайська операція є ознакою професійної майстерності шахраїв.

Успішність шахрайських дій забезпечується привабливістю обману, який спрямовано на те, щоб зацікавити жертву у вигідності взаємовідносин саме для нього чи його організації. Привабливість базується на вигоді, великих прибутках, простоті дій тощо. Саме ця привабливість і є тим гачком, на який час від часу потрапляють і працівники банків.

Найбільш уражені шахрайством кредитні, вексельні, карткові та розрахункові операції. Найбільш масовим, ефективним для шахраїв і, як правило, безкарним продовжує залишатися шахрайство з банківськими кредитами.

Шахрайські злочини скоюються, як правило, в рамках легальної господарської і банківської діяльності клієнтів і

банків. Така діяльність до того ж є основою для скоєння шахрайських дій. Основні зусилля шахраїв у процесі отримання кредитів направлені на введення в оману банку щодо ефективності своєї діяльності та чесних намірів щодо використання кредитних коштів. Виходячи з цього шахраї подають у банк неправдиві, підроблені документи, фальсифіковану інформацію, завищені показники своєї діяльності, показують офіси, засоби виробництва, які їм не належать, прикриваються наполегливим проханням високопосадових осіб. Для забезпечення надають гарантії від осіб, неспроможних гарантувати кредитну угоду, з різним порушенням оформляють заставу, неправильно проводять страхування кредитного ризику і т. п. Але це все робиться з усмішкою, обіцяються значні позитивні результати та персональна подяка. Тобто в наявності всі ознаки шахрайських дій, обман та введення в оману. А метою їх є прагнення створити в банку уявлення про перспективне підприємство й ефективну його діяльність.

Як правило, отримавши кредит, такі особи якщо відразу не зникають, то намагаються зробити все для того, щоб його не повертати: переводять усі активи на інші підприємства, знаходять підстави, за якими кредитні угоди можуть бути визнані недійсними, вишукують причини для зменшення розміру процентів, обґрунтовують необхідність пролонгації з метою затягування терміну повернення кредитних коштів. Сьогодні відомо багато шахрайських схем отримання і неповернення кредитних коштів — від простого зникнення позичальників до висококваліфікованого обґрунтування неможливості і законності їх неповернення. Нижче наводяться кілька таких схем, відомих з практики банківської діяльності.

1. Відкривається Фірма. Отримавши кредит у банку «Альфа» під свої активи, вона засновує нові фірми Ф = 1, Ф = 2, Ф = 3. Останні під гарантію Фірми отримують кредити в банках «Ліра», «Ялта», «РІД». З метою обґрунтування кредитної угоди між ними укладаються угоди. За рахунок нових кредитів погашаються минулі позики. Ураховуючи, що розмір кредитів невеликий, їх погашення протягом визначеного терміну проводиться справно. Після ряду угод Фірма і засновані нею Ф = 1, Ф = 2, Ф = 3 починають вважатися для банків достатньо надійними (що й потрібно було шахраям). Через деякий час Фірма і Ф = 1, Ф = 2, Ф = 3 отримують великі кредити і… зникають.

2. Фірма О одержала кредит у банку Б для закупівлі товару. При цьому повернення кредиту забезпечувалося заставою, якою був сам товар. Закупивши товар, фірма О відразу його реалізує за готівку. Після чого починаються довгі пояснення, прохання про пролонгацію, а на закінчення фірма О реорганізується в іншу, самоліквідується або оголошує себе банкрутом.

3. Фірма Д, що діє в Україні як дилер закордонної компанії, укладає від імені останньої контракт із фірмою К на поставку обладнання. Фірма К одержує для реалізації угоди в українському банку кредит, сума якого як передоплата переводиться на рахунок компанії в закордонний банк. Водночас іноземна компанія одержує в цьому банку кредит, гарантуючи його повернення коштами, зазначеними в контракті з українською фірмою К. У результаті цього, отримані кошти не надходять на рахунки компанії, а відразу приймаються банком як повернення кредиту. Через деякий час (один—два тижні) після отримання коштів від фірми К компанія оголошує себе банкрутом і реорганізується в іншу структуру. Ліквідаційна комісія не показує фірму К в списку кредиторів компанії тому, що гроші фірми на рахунках останньої відсутні.

4. Банк 1 свого часу надав Фірмі кредит, остання ж з настанням терміну повернення кредитних коштів повернути їх не може, маючи при цьому безрадісні перспективи на майбутнє. За таких умов Банк 1 пропонує своєму боржникові отримати кредит у Банку 2, за рахунок якого погасити борг перед Банком 1. При цьому рекомендує Банку 2 Фірму як порядного і надійного позичальника. Після отримання кредиту в Банку 2 Фірма повертає борг Банку 1, а з часом його проблеми стають проблемами Банку 2.

Поряд з такими схемами дій щодо використання кредитних коштів, шахраї вдаються до подібного із заставою, гарантіями, порукою, страхуванням кредитних ризиків. Обман щодо наявності предметів застави, права власності на них, їх ліквідності, підміна, використання предметів застави під час кредитної операції — все це шахрайство з заставою. Неправомірність підписів договорів гарантії чи поруки, відсутність фінансових можливостей гаранта, поручителя гарантувати кредитну угоду, неправомірне використання імені відомих фірм в угодах про гарантію або поруку, родинні або інші близькі зв'язки позичальників і гарантів (поручителів) — це також приклади шахрайства у кредитній діяльності банків.

Відсутність правил страхування у страхових компаній, страхування тільки суми кредиту, а не ризику неповернення кредитних коштів, несвоєчасна проплата страхового внеску, незначні можливості страхових компаній — дії, відомі з практики шахрайства щодо банківських кредитів.

Значна частина шахрайських дій пов'язана з юридичними колізіями або ж взагалі з юридичною безграмотністю банківських працівників. Мова йде про так звані юридичні бомби. Заклавши їх у договори, шахраї можуть потім з легкістю не виконувати своїх обов'язків перед банком.

Наприклад, договір може підписати керівник суб'єкта-позичальника, який не має на це права або має право, але воно обмежене певною сумою, яка менша ніж сума кредиту. У результаті такі договори за законом є недійсними, а кредитні кошти використовуються шахраями певний час безкоштовно або взагалі не повертаються. Також поширеною є практика створення фіктивних фірм, які відкривають на підставних осіб, і якщо принципово не ставиться до їх перевірки, наслідки співпраці з такими позичальниками можуть також бути не на користь банку.

Шахрайство в банках здійснюється не тільки у процесі кредитних операцій. Досить часті випадки шахрайських дій і під час інших банківських операцій. Основною особливістю у таких випадках є те, що шахрайські дії скоюються тут, як правило, працівниками банків або за безпосередньою їх участі. Світова практика показує, що в дрібних банках шахрайство з боку працівників банків скоюється частіше ніж у великих. Це пов'язано насамперед із сумісництвом у дрібних банках кількох функцій банківського виробництва однією посадовою особою, що дозволяє їй здійснити шахрайство виконуючи одну функцію й приховати його виконанням іншої. Ось два приклади:

1. Працівник підрозділу цінних паперів, уступивши в зговір з держателем підроблених чи крадених цінних паперів, зловживаючи своїм посадовим становищем, розміщує їх у портфелі боргових зобов'язань банку. Іншим разом він змінює свої, які втратили високу прибутковість, цінні папери на цінні папери, які належать банку, вносячи при цьому відповідні зміни в реєстр.

2. Фірма отримує в банку В під гарантію банку А кредит, кошти від якого присвоюються керівництвом фірми і банку А.

Коли настає термін платежу, але фірма і не повертає кредитних коштів, банк В виставляє претензію її гаранту — банку А. Останній оформляє і видає фірмі кредит на суму, яка необхідна для погашення заборгованості. У цьому разі збиткова операція банку щодо надання гарантії перетворюється в активну кредитну операцію. Виграно час, а неповернений кредит — звичайна на сьогодні справа.

Шахрайство може мати місце навіть тоді, коли банк не вкладає, а залучає кошти. Тобто розгалуженість шахрайських дій досить широка й охоплює практично всі сфери діяльності банків. Ось один із прикладів:

Фірма Ф = 1 відкрила в банку Б = 1 депозитний рахунок, перерахувавши на нього 5000 грн. Під нього отримала кредит на суму 4000 грн. Водночас Фірма Ф = 2 пред'явила в банк Б = 1 чек на суму 3000 грн. З використанням створених коштів фірма провела ряд операцій. Під залишок коштів отримала кредит на суму 1500 грн.

Через деякий час виявилося, що депозитний вклад фірми Ф = 1 створений від помилково перерахованих банком Б = 2 коштів на суму 5000 грн і їх необхідно повернути. А чек, наданий фірмою Ф = 2 виявився досить якісною підробкою.

В останні роки (2008—2010) кількість випадків шахрайства зросла на 36,7%. Як зазначають фахівці, таке зростання обумовлене фінансово-економічною кризою, негативних наслідків від якої найбільше зазнали банки [173].

Поряд з шахрайством значну загрозу діяльності банків можуть становити зловживання службовим становищем працівників банків, яке може виявлятися у двох формах протиправних дій: використання посадових повноважень з корисливою метою та перевищення посадових повноважень із корисливою метою. У першому випадку це може здійснюватися через:

- штучне створення посадовцями виключного свого становища в управлінських або технологічних лініях;
- отримання матеріальної винагороди за послуги, виконання яких передбачено посадовими обов'язками;
- лобіювання збиткових, безперспективних рішень і проектів, які сприяють створенню вигідних позицій конкурентам, окремим клієнтам або з метою отримання матеріальної винагороди;
- створення нерівноцінних умов роботи для своїх підлеглих, вимагання від них виконання роботи, не пов'язаної із

• умисне затягування вирішення службових чи виробничих питань з метою примушування до надання матеріальної винагороди чи акцентування виключного значення власного становища;

• необгрунтоване створення сприятливих умов для надання послуг банком власним комерційним структурам, родичам, близьким або особам, які виражають матеріальну подяку.

У другому випадку зловживання службовим становищем може виражатися в такому:

✓ прийняття рішень не притаманних посадовому становищу або функціям посадової особи;

✓ виступи, заяви від імені банку без отримання на це необхідних повноважень;

✓ представлення інтересів установи банку без отримання на те відповідних повноважень;

✓ підписування документів, не передбачених функціональними обов'язками або посадовими повноваженнями;

✓ надання вказівок, розпоряджень із перевищенням повноважень або таких, що не передбачені функціональним призначенням;

✓ надання гарантій, прийняття зобов'язань від імені банку без наявності на те відповідних повноважень.

Зловживання посадовим становищем, як правило, є похідним від якихось інших економічних злочинів або є одним з інструментів таких злочинів. Тобто за зловживанням службовим становищем працівників банку можуть приховуватися гучніші й серйозніші справи.

Розвиток економічних відносин стимулює появу нових форм банківського виробництва з використанням сучасних технічних досягнень. Такі форми обумовлені і постійним зростанням кількості інформаційних операцій, що виконуються в банках, їх різними видами. Тому виникають загрози втрати капіталу банку, які безпосередньо не мають економічного характеру, але результати реалізації їх призводять до значних збитків банків.

Проникнення зловмисників до платіжних систем банків через інформаційні банківські системи є досить небезпечним і непередбачуваним явищем. Особливо поширеною є загроза посягання на капітал банку через несанкціоновані прийоми використання пластикових платіжних засобів. Втрати банків від реалізації таких загроз за деякими підрахунками становлять понад

15% від загальних втрат. Найпоширенішими протиправними діями з пластиковими картками є незаконне використання оригіналів карток (загублених, викрадених), використання карток, не отриманих власником, часткова підробка карток, додаткові сліпи, зроблені працівниками пунктів торговельної мережі та ін. За таких умов картковий бізнес хоч і є прибутковим, але вимагає великого ступеня захисту для себе, це звичайно необхідно розуміти і вживати всіх заходів безпеки.

Значну загрозу для вітчизняних банків становлять іноземні схеми шахрайства, до яких наші банки бувають не готові. Банківська система України знає приклади коли іноземні шахраї досить активно втілювали у своїй діяльності такі методи шахрайства, як проведення операцій з так званими першокласними банківськими інструментами (гарантіями, акредитивами, чеками та ін.). Привабливість операцій з першокласними банківськими інструментами ґрунтувалася на прагненні вкладників отримати великий прибуток.

Шахраї ж, реалізуючи свої злочинні схеми, використовують підроблені, прострочені, недійсні та інші банківські інструменти. Маскуючи свою мету, вони стверджують, що банки в усьому світі беруть участь у такій діяльності. За їх словами, ці першокласні банківські інструменти не відображаються в банківських звітах і тому можуть приносити значний прибуток за короткий проміжок часу. Такі операції, за твердженням шахраїв, ураховуються в балансах тільки при виконанні відповідних зобов'язань. Шахраї намагаються сформувати у своїх «клієнтів» уявлення про те, що операції здійснюються тільки за допомогою «завіреного телекса» за принципом «банк для банку», а засобами зв'язку служать звичайні банківські комунікації з участю «банківського консультанта». До того ж такі операції проводяться під час короткочасного покращення ринкової кон'юнктури. Не допускаються ніякі телефонні дзвінки, які, на думку шахраїв, можуть призвести до розголошення конфіденційної інформації. Тобто ознаками таких операцій є строга їх таємність і короткостроковість.

Ще одна ознака — міф про те, що банківські інструменти призначені для ексклюзивних клієнтів, які здійснюють операції з такими інструментами на вторинних ринках. Вважається, що емітовані відомими банками такі інструменти мають безмежну ліквідність. Інструменти пропонуються шахраями з гарантією 10—14% річних, тоді як банки фіксують ставку близько 4—6%.

Різновидом закордонного шахрайства є так звані нігерійські листи, які дійшли до України в 1997 р., а подекуди трапляються і зараз. Їх автори із далекої африканської країни пропонують суттєві вигоди особам, згодним надати свої банківські рахунки для виконання деяких фінансових операцій. Тих, хто повірив таким листам і здійснив співробітництво з їх авторами, очікувало глибоке розчарування, ані прибутків, ані власних грошей вони більше не отримали, а звертатись, як правило, ні до кого.

Пільги офшорного бізнесу, які надаються керівництвом ряду країн, також використовуються міжнародними шахраями, насамперед для реєстрації різноманітних фінансових установ. Особливо привабливими для них є компанії у фінансових центрах Богамських островів і Кіпру. В інтернеті та іноземних періодичних виданнях досить багато реклами банків, розташованих в офшорних зонах, які обіцяють значні проценти і серйозні податкові пільги.

Ще одним із видів загроз, які мають тенденцію до значного поширення, є загрози, пов'язані із заподіянням збитків банком через комп'ютерні мережі. Сьогодні неможливо уявити банк, який би не використовував у своїй діяльності комп'ютерні інформаційні мережі (автоматизовані банківські системи), активне використання яких обумовило навіть появу нового терміна — «електронні гроші». Водночас, незважаючи на досить розвинену в банках систему комп'ютерної комунікації, вжиття заходів щодо її захисту, практика показує, що вона не є абсолютно надійною. Час від часу злочинці проникають до банківських комп'ютерних мереж, електронної фінансової інформації, завдаючи банкам та їх клієнтам значних збитків. Виходячи з іноземного досвіду, сьогодні можна говорити про наявність тенденції до збільшення питомої ваги втрат банків, заподіяних їм через комп'ютерні злочини в загальній частині матеріальних втрат. Найбільш поширеними є загрози, пов'язані з незаконним використанням інформації пластикових платіжних засобів та комп'ютерної банківської інформації. Загрози інформації пластикових платіжних засобів реалізуються через використання спеціального програмного забезпечення, за допомогою якого визначаються номери рахунків таких засобів, паролі доступу до них, іншу необхідну інформацію. Виявлена інформація використовується для скоєння злочинів щодо незаконного зняття коштів клієнтів банків або для її поширення, продажу тощо.

Ефективність дій електронних шахраїв характеризується такими показниками: кількість шахрайських операцій із пластиковими

платіжними засобами у 2009 р. зросла в 6,5 разу порівняно з 2008 р., а збитки від дії карткових шахраїв становили 12,970 млн грн [111].

Водночас досить динамічно розвиваються загрози, пов'язані з підробкою пластикових платіжних засобів, розкрадання банківських коштів з використанням електронно-обчислювальної техніки. В останньому випадку банківські працівники або сторонні особи, досить добре обізнані з системою обробки, передавання та захисту електронної фінансової інформації банків, проникають до місця зосередження такої інформації, знімають гроші з електронних рахунків та переказують їх на підставні фірми або присвоюють.

Останнім часом почастішали випадки несанкціонованого списання коштів із рахунків клієнтів під час здійснення розрахунків за допомогою систем дистанційного обслуговування «клієнт—банк», «клієнт—інтернет—банк» шляхом хакерських атак на комп'ютери клієнтів банків. За таких умов не можна заперечувати, що уже в найближчому майбутньому основні проблеми банків можуть бути зосереджені саме у сфері використання автоматизованих банківських систем.

4.3. Загрози, пов'язані з утягуванням банків у незаконну фінансову діяльність

Наявність у країні тіньового сектору економіки зумовила трансформацію грошового обігу і формувало позабанкового фінансового ринку. Обсяги даного ринку настільки значні, що здатні впливати на розвиток економіки країни. Разом з тим тіньові кошти мають обмежене використання в офіційній економіці і тому їх власники постійно прагнуть надати їм легального походження.

Основними сегментами тіньової економіки та механізмами формування тіньових прибутків є: корупція, ухилення від оподаткування прибутків, нелегальний експорт капіталів; незаконна приватизація державної власності; розкрадання цінностей; нелегальні валютні і зовнішньоекономічні операції (контрабанда); випуск і реалізація неврахованої продукції та послуг; кримінальні злочини; фінансове шахрайство [172]. А основними сферами, де тіньова економіка в Україні має найбільше поширення, є: сільське господарство; будівництво; деревообробка; діяльність з нерухомістю; легка, нафтопереробна, рибна та хімічна промисловість; оптова торгівля [116].

Значні обсяги тіньового сектору економіки не тільки впливають на економічні процеси в країні, а й формують певний менталітет частини населення, яка отримує свої доходи з даної сфери. За даними опитувань, до 40% молоді великих міст і прикордонних регіонів зайнято в тіньовій економіці, а для майже 2,5 млн українських громадян тіньова економіка є основним джерелом доходу. За таких умов ця частина населення виправдовує існування тіньового сектору і для себе вважає законним [172].

Важливим показником функціонування тіньового сектору є обсяг коштів, що здійснюють обіг поза офіційною сферою. Показовими в цьому плані є дані, наведені в одному з періодичних видань [172], які якраз характеризують динаміку зростання обсягу готівки поза банківським обігом (табл. 4.3).

Таблиця 4.3

ОБСЯГ ГОТІВКИ ПОЗА БАНКІВСЬКИМ ОБІГОМ ЗА 2003—2008 РР.

Показник	Роки					
	2003	2004	2005	2006	2007	2008
Обсяги коштів поза банками, млрд грн	32,3	41,8	60,2	75	111,1	188,7

Співвідношення тіньового сектору до офіційної економіки наведено у табл. 4.4.

Таблиця 4.4

СПІВВІДНОШЕННЯ ТІНЬОВОГО СЕКТОРУ ДО ОФІЦІЙНОЇ ЕКОНОМІКИ ЗА 2003—2008 РР.

Показник	Роки					
	2003	2004	2005	2006	2007	2008
Тіньовий сектор,% від ВВП	27	28	30	29	26	28

Граничними вважаються обсяги такого показника 30% від ВВП, перевищення його загрожує економічній безпеці країни.

Особливої актуальності проблема тінізації економіки набуває у банківській сфері. Оскільки можливості щодо використання тіньових коштів обмежені, власники таких коштів вишукують способи їх легалізації (відмивання). У схемах відмивання тіньових коштів головна роль відводиться банкам, які тим самим втягуються в незаконну фінансову діяльність. У країні існує мережа фіктивних комерційних структур, які займаються

конвертацією безготівкових коштів у готівкову валюту. З метою втягування банків у діяльність з відмивання незаконно отриманих коштів при деяких банках спеціально створювалися «конвертаційні центри» та фіктивні фірми. Через систему рахунків закордонних банків-нерезидентів та деяких українських банків здійснювалося незаконне переведення безготівкових коштів у готівку та їх конвертація в іноземну валюту. Після зарахування коштів на рахунок «буферної» фірми і їх перерахування на кореспондентський рахунок іноземного банку дії злочинців можуть бути такими:

- переведення безготівкових гривень у готівку переказуванням їх на відкритий рахунок «підставній» фізичній особі і далі отримання коштів зазначеною особою з використанням пластикової картки;
- конвертація безготівкової гривні у безготівкову іноземну валюту переказуванням коштів на рахунок фірми з офшорної зони та подальшого перерахування їх на відповідний рахунок закордонної компанії.

Якщо банки з певних причин будуть втягнуті в тіньову діяльність, їм можуть загрожувати певні санкції з боку держави та погіршення іміджу на ринку банківських послуг.

4.4. Рейдерство як одна з актуальних загроз діяльності банків

Характерною рисою новітньої історії розвитку вітчизняного підприємництва є зростаюча кількість операцій, пов'язаних із злиттям, перетворенням та приєднанням суб'єктів господарювання, яке часто проявляється в досить агресивній формі, так званому недружньому поглинанні, або рейдерстві. Останнє нині поширилося в Україні настільки масштабно, що стало створювати певну загрозу економічному розвитку країни. Більше того, рейдерство поступово поширює свій вплив на фінансовий сектор економіки, зокрема банки, страхові компанії та інших субєктів фінансового ринку. Головне завдання рейдера, як і будь-якого бізнесмена, — отримати прибуток. Але досягнення даної мети рейдери здійснюють не через виробництво певної продукції, а перепродажем субєктів господарювання, над якими вони отримали контроль через недружнє поглинання. Недружнє поглинання вигідне тим, що

дії щодо заволодіння підприємством чи банком значно простіші, дешевші і прибутковіші для рейдерів, ніж пошук компромісів із власниками, спроби переконати їх продати вигідний бізнес та ще за незначну ціну. Адже рейдерів цікавлять виключно ліквідні підприємства та банки, які ведуть вигідний і перспективний бізнес, мають значні активи. Тому рейдерство досить високодохідний бізнес. За деякими даними, рентабельність рейдерського бізнесу становить від 500 до 2000 % і більше.

Серйозність рейдерських загроз обумовлюється тим, що в разі потрапляння банку, навіть великого, під вплив професійних рейдерів йому буде дуже складно вийти з такої ситуації без серйозних втрат. Насамперед це пояснюється тим, що для проведення рейдерських операцій зловмисники, як правило, мають досить потужний адміністративний ресурс, «своїх» суддів, налагоджені зв'язки з правоохоронними органами, державними виконавцями. Сьогодні рейдерський бізнес володіє досить професійними юридичними й аналітичними службами, значним фінансовим ресурсом, забезпечений підтримкою лояльних суддів, зв'язками в різних державних органах.

Практика показує, що спроба захвату банку рейдерами може мотивуватись їх бажанням отримати доступ до ліквідних банківських активів, вивести з гри конкурента, яким є банк, отримати права, якими переважно володіє банк стосовно предметів застави, оренди, землі тощо.

Якщо ж говорити про ідеологічну суть рейдерства, то можна зазначити, що на першому місці в цьому явищі стоїть фінансово-спекулятивний капітал, де само отримання прибутку становить 99% усіх його складових. Тобто рейдерство, як правило, не забезпечує розвитку, в його основі досить проста схема — «купи і продай». Інвестування в отриману власність, забезпечення її розвитку і прибуткового функціонування рейдери можуть здійснювати тільки стосовно досить прибуткового бізнесу, банки якраз і належать, з погляду рейдерів, до такого виду бізнесу. В інших випадках придбана рейдерами власність зразу ж реалізується, причому здебільшого реалізуються найбільш ліквідні активи — земля і нерухомість.

Формуванню спекулятивної моделі економіки значною мірою сприяла і сама держава. Остання, на жаль, не має чіткої і ясної позиції стосовно рейдерства. Сьогодні держава однаково сприймає як підприємців, які вклали кошти в певне виробництво, забезпечили ефективне і прибуткове його функціонування, так і

тих, хто просто щось придбав і перепродав. Вважається, що і в першому, і в другому випадку це — рівноцінний бізнес, і перші, і другі підприємці сплачують однаковий податок і для обох їх держава створює однакові умови. Звичайно, що в такому разі бізнес «купи—продай» набагато вигідніший і, безумовно, він буде розвиватися активніше, навіть незважаючи на те, що шкодитиме економіці держави.

Якщо ж детальніше розглядати причини виникнення та поширення рейдерства в нашій країні, то тут слід звернути увагу на таке.

На даний час на ринку злиття і поглинання відсутні правила гри. Недоліки вітчизняного законодавства, яке регулює корпоративні відносини, є досить значними і з успіхом використовуються рейдерами. З огляду на це варто зазначити, що рейдери є досить підготовленими юристами, здатними ефективно маніпулювати нормами вітчизняного права, ураховуючи можливість їх подвійного, а то й потрійного трактування. Так, наприклад, питання захисту дрібних власників акцій, передбачене в нашому законодавстві, доведено рейдерами до абсурду, але водночас вкладається в рамки закону. Акціонер, який має у власності 0,02% акцій, може подати до суду позов щодо відновлення порушених адміністрацією акціонерного товариства його прав стосовно вступу у володіння своєю власністю. За таких умов суд може накласти арешт на все рухоме і нерухоме майно товариства до вирішення питання по суті в такий спосіб заблокувати роботу зазначеного товариства. Чинне законодавство також не передбачає прямої заборони на ведення подвійних реєстрів акціонерних товариств, здійснювати зміну їх керівництва акціонерами, які є власниками незначних пакетів акцій, кримінальної відповідальності за силовий захват підприємств, банків. Крім того, у законодавстві не передбачено порядку здійснення контролю за рухом акцій акціонерного товариства на вторинному ринку, що дає змогу рейдерам таємно формувати значні пакети акцій і використовувати їх для рейдерської атаки. А враховуючи, що банки є виключно акціонерними товариствами, така ситуація містить істотну загрозу банківському бізнесу.

Не зовсім урегульовано і порядок доступу до реєстрів акціонерів, реєстрації змін у керівництві підприємств, банків.

Ще однією правовою прогалиною є відсутність обмеження юрисдикції судів у зв’язку з їх територіальним розташуванням. Сьогодні суд розміщений в одному регіоні, може розглядати і

виносити рішення щодо ситуації, яка склалася на тому чи тому підприємстві, у банку іншого регіону. Отже, рейдери можуть отримати цілком законне рішення суду, розташованого в будь-якому регіоні країни, яке використовується для забезпечення рейдерської атаки, незважаючи навіть на те, що може існувати інше, зовсім протилежне, рішення суду, який розташований у тому самому регіоні, що й об'єкт спору.

Причиною появи та поширення рейдерства є й те, що вартість певної частини банків значно нижча від їхніх активів, нерідко різниця становить кілька десятків і сотень разів. Скажімо, банк зі статутним капіталом 10 млн євро може володіти активами в кілька десятків мільярдів гривень. Звичайно, така ситуація провокуватиме рейдерів до захоплення зазначених банків, коли, витративши кілька мільйонів, можна отримати активи в десятки мільйонів, а то й мільярдів.

До причин, що сприяють рейдерству, належить і концентрація активів у власності однієї чи невеликої групи осіб, коли виникає можливість однією рейдерською атакою захопити такі активи без суттєвих затрат коштів і часу.

Причинами, що створюють сприятливі умови рейдерству, можна вважати і велику кількість дрібних акціонерів акціонерних товариств. Особливо це стосується банків, де власниками акцій є їх працівники та велика кількість фізичних осіб. Отримуючи незначну заробітну плату і мізерні дивіденди, такі особи, як правило, без особливих роздумів продають свої акції тим, хто пропонує за них в 10—15 разів більше їх номінальної вартості, що, зрештою дає змогу рейдерам сформувати необхідний їм пакет акцій.

Суттєвою причиною рейдерства є корупція у владних структурах та судових органах. Якраз останні відіграють ключову роль у рейдерських схемах. Це за їхніми ухвалами чи рішеннями рейдери отримують законні підстави до своїх дій і здійснюють безпосередні заходи, спрямовані на зміну керівництва підприємств, банків, що є об'єктами рейдерських атак. А відсутність або формальність заходів захисту прав підприємців від рейдерів з боку владних структур робить ситуацію досить сприятливою для рейдерських атак.

Таким чином, результати аналізу ситуації, яка склалася в країні сьогодні, вказує на те, що, на жаль, у нас існують всі умови для рейдерства, яке, за своєю суттю, можна вважати економічним тероризмом.

Практика показує, що рейдерські захоплення мають певну структуру і здійснюються відповідно до визначених схем. На першому етапі рейдерських дій вивчається ситуація на ринку банківських послуг і виявляються об'єкти, які є найпривабливішими для рейдерів. Основними критеріями вибору таких об'єктів є, по-перше, прибутковість і значні активи (насамперед їх ліквідність), а по-друге, доступність об'єктів для рейдерських атак. З цією метою рейдери здійснюють збір необхідної їм інформації. Якраз збір останньої і є першим етапом рейдерського захоплення того чи того банку. На цьому етапі рейдери здійснюють спроби отримати копії статутних та установчих документів банків, відомості про їх внутрішню фінансову політику, керівників та провідних менеджерів, майно та інші активи. Крім того, вивчаються реальні економічні показники діяльності банків, оцінюються основні активи — об'єкти нерухомості та земля, наявність корпоративних клієнтів, обсяги та якість кредитного портфеля, визначається наявність і ліквідність предметів застави, а також обсяги кредиторської заборгованості банків. Особливі зусилля рейдери докладають для отримання реєстру акціонерів банків. Тут існує досить багато методів — від банального підкупу працівників реєстратора до різного роду опитування працівників банків та подання до Єдиного державного реєстру юридичних осіб фіктивних документів про зміну керівництва акціонерного товариства і ознайомлення нового керівника з реєстром.

Водночас рейдери накопичують компрометувальну інформацію на керівництво, головного бухгалтера та провідних менеджерів банку або провокують їх на якісь незаконні чи аморальні дії з метою формування компромату.

На цьому етапі рейдерами оцінюється стійкість банку до рейдерської атаки. Тут оцінюється система охорони банку та його об'єктів, сили, що застосовуються в охороні (власні підрозділи, залучені підприємства, що надають послуги охорони, державна служба охорони при МВС). Також вивчається здатність банку мобілізувати для свого захисту суд, прокуратуру, місцеві та інші органи влади. Особлива увага приділяється зв'язкам власників банку, передусім з точки зору зацікавленості високопосадових чиновників у об'єкті, який визначається для рейдерського захоплення. У разі, коли захист об'єкта визначається як суттєвий, розробляються заходи, нейтралізації потенційних захисників.

Захоплення банків — другий етап рейдерських дій, тут існують три основні схеми:

1. *Захоплення через акціонерний капітал*. У цьому разі рейдери прагнуть скупити акції певного банку, як правило, у дрібних власників. Для цього проводиться відповідна робота з акціонерами, спрямована на переконання у більшій вигідності продати акції, ніж їх утримувати. Така робота проводиться, як правило, без її розголошення й оприлюднення.

Скупивши 10—15% акцій (кількість, достатня для ініціювання проведення зборів акціонерів з необхідним порядком денним), рейдери отримують можливість доступу до конфіденційної інформації банку і вивчення його об'єктивного стану. Надалі рейдери ініціюють скликання зборів акціонерів і, як правило, вносять до порядку денного питання про ефективність роботи керівництва банку та його заміну. У цей період проводяться заходи щодо оприлюднення компрометувальну інформації про діяльність керівництва банку та організовується «обурення громадськості», пікетування банку, акти саботажу, бойкоту і т. п. Для забезпечення захоплення може ініціюватися порушення кримінальних справ стосовно керівників та основних менеджерів банку, депутатські запити, а також поширюватися негативна інформація у засобах масової інформації про результати діяльності банку. У разі відмови провести такі збори з боку основних власників рейдери отримують право провести їх самими, що у більшості випадків і трапляється. Якщо ж збори скликано, але рішення прийнято не на користь рейдерів, останні добиваються визнання його незаконним через суд, або нескінченними новими зборами. Більше того, на період спорів з іншими власниками можуть звертатися до суду з проханням накласти арешт на мажоритарний пакет акцій, мотивуючи це тим, що порушуються права та інтереси інших акціонерів. У цьому разі мажоритарщики лишаються права голосу, а рейдери скликають нові збори акціонерів і приймають необхідні їм рішення, в тому числі і щодо зміни керівництва банку.

Якщо рейдери отримують позитивне для них рішення судів, а виконанню його протидіють інші власники, вони звертаються до виконавчої служби з проханням примусового забезпечення виконання рішення суду. За таких умов якраз і може здійснюватися силове захоплення банку. В окремих випадках силовий захват може здійснюватись і на підставі рішення зборів акціонерів. У цьому разі силове захоплення, зазвичай,

здійснюється силами приватних структур, переважно тих, що надають послуги охорони. Отримавши доступ до печатки банку й основних його документів та власності, рейдери використовують своє право на власний розсуд.

2. *Захоплення через кредиторську заборгованість*. У цьому разі у рейдери скуповують прострочені кредиторські борги банку, як правило, у дрібних кредиторів, які згодом консолідуються і надаються боржникові для одночасної сплати. Враховуючи, що, як правило, у банку можливості для одночасної оплати всіх боргів зазвичай відсутні, ініціюється запровадження процедури тимчасової адміністрації. За таких умов рейдери проводять через Національний банк України рішення про призначення свого тимчасового адміністратора, який надалі і здійснює рейдерський задум. Якщо тимчасовим адміністратором призначено іншу особу, рейдери проводять роботу щодо його підкупу або заміни. Банк, що перебуває у стані тимчасової адміністрації непідконтрольний ні власникам, ні менеджменту і рейдери роблять з ним все, що їм необхідно.

3. *Захоплення через органи управління*. Найслабшою ланкою будь-якого суб'єкта господарювання є його топ-менеджмент, тобто органи управління. Це люди, на слабкостях яких насамперед грає рейдер. Наділений великими повноваженнями керівник банку може сприяти швидкому виведенню ліквідних активів зі свого банку в підконтрольні рейдеру структури. У такому разі власники банку залишаються з акціями, які нічого не варті. Більш того, менеджмент може легко спровокувати фінансові проблеми в банку. Тобто залучення на свій бік керівництва банку, яким зацікавилися рейдери, є однією із форм рейдерського захвату. Переконання керівництва банку діяти на користь рейдерів здійснюється різноманітними способами: підкупом, шантажем, погрозами, кримінальним переслідуванням та ін. У багатьох випадках рейдерам вдається залучити або спровокувати керівництво банків до дій, які їм необхідні.

Незважаючи на складність та трудомісткість рейдерських дій, вони досить активно поширюються і стають новим атрибутом вітчизняного ринку банківських послуг. А враховуючи високу залежність рейдерства від інтелектуальної його складової та стан його розвитку можна вважати, що ним займаються досить підготовлені, досвідчені та творчі професіонали своєї справи. За таких умов рейдерство є досить серйозною загрозою для банків, протистояти якій можуть

лише ті суб'єкти, які здатні вживати адекватних заходів захисту та протидії рейдерам.

4.5. Загрози тероризму

Україна — одна з небагатьох країн світу, де тероризм не є гострою проблемою її суспільного життя. Разом з тим час від часу ми маємо приклади терористичних дій стосовно певних організацій, установ та окремих осіб, у тому числі і в банківській системі. Такі факти, як убивства, захват заручників, загроза підриву чи підрив вибухових пристроїв уже не є рідкісними у нашому житті. Водночас в умовах міжнародної інтеграції та глобалізації країна відчуває подих тероризму у новому його вигляді: кібертероризм, біотероризм, економічний тероризм, що має досить широкий спектр дії, не тільки зачіпає інтереси конкретних суб'єктів і осіб, а й негативно впливає на життєдіяльність цілих регіонів країни, галузей економіки, систему управління господарством. Водночас якщо зараз Україна не відчуває серйозного терористичного впливу, то не можна не помічати існування факторів, які здатні обумовити появу тероризму і в Україні на рівні, що здатний дестабілізувати її суспільний розвиток та економіку. Насамперед мова йде про існування певного комплексу таких факторів у різних сферах життєдіяльності: політичній, економічній, соціальній, ідеологічній та ін.

До політичних факторів можна віднести такі:

- загострення політичної боротьби партій та їх об'єднань в окремі періоди політичного життя країни, відсутність досвіду цивілізованої політичної боротьби;
- суперечності між задекларованими демократичними принципами та їх реалізацією;
- відсутність належної взаємодії між органами влади на всіх рівнях і населення щодо забезпечення безконфліктного розвитку міжнаціональних та міжрелігійних відносин;
- недостатня ефективність політичних реформ.

Економічними факторами можна вважати:

- ❖ велике розшарування населення за рівнем життя;
- ❖ явне і приховане безробіття значної частини населення;
- ❖ криміналізація економіки.

Серед соціальних факторів можна виділити:

▪ розмежування суспільства (формування прошарків і груп населення з протилежними інтересами);

▪ відсутність ефективної системи соціальних гарантій населення;

▪ різке зниження соціального захисту населення, скорочення терміну (тривалості) життя, зростання гострих і хронічних хвороб;

▪ високий рівень злочинності в суспільстві;

▪ зниження духовних, моральних, патріотичних якостей і рівня культури населення;

▪ пропаганда засобами масової інформації культу жорстокої поведінки і насилля;

▪ націоналістична політика окремих політичних діячів у боротьбі за владу в умовах багатонаціональної країни;

▪ наявність радикальних з ознаками екстремізму молодіжних угрупувань (скинхеди…).

До правових факторів належать:

✓ низькі правова грамотність та правова культура населення, яка не дозволяє оцінити рівень своєї відповідальності за певні дії та їх наслідки;

✓ недостатність досвіду застосування законодавства у сфері протидії тероризму.

Основними ідеологічними факторами можуть бути:

♦ відсутність єдиної послідовної державної політики у сфері ідеології громадянського суспільства;

♦ поширення ідеології нігілізму, антипатріотизму, несприйняття загальновизнаних цінностей, нехтування економічними інтересами у взаємовідносинах і оцінках поведінки громадян;

♦ відсутність ефективної системи виховання законослухняної поведінки громадян.

Наявність цих та інших факторів вказує на те, що в країні існує певний ризик виникнення та поширення тероризму. Діяльність всіх суб'єктів господарювання, у тому числі і банків, має враховувати його існування. Банки є досить привабливим об'єктом як для терористів, так і для організованих злочинних груп, у діяльності яких можуть бути акти терористичного характеру: підриви вибухових пристроїв, захоплення заручників, залякування або фізичне усунення конкурентів. Організовані злочинні угруповання досить часто є одним із суб'єктів терористичної діяльності і

використовують залякування, насильницькі дії в різних їх формах як головні засоби впливу на суб'єктів, котрі становлять для них певний інтерес, особливо в перерозподілі сфер впливу, власності, фінансових потоків, видів злочинної діяльності. Банки або ж окремі їхні працівники можуть потрапляти в поле зору таких угруповань з різних причин і ставати їх жертвами. В окремих випадках банківська діяльність або ж окремі установи можуть зазнавати шкоди від терористичних дій терористичних організацій чи злочинних угруповань, спрямованих не безпосередньо на них, а через вплив на інших суб'єктів (клієнтів, акціонерів, сусідніх установ, організацій, об'єктів).

За певних умов банки можуть стати об'єктом інтересу злочинців чи терористів суто опосередковано як інструмент, за допомогою якого може бути завдано шкоди іншим суб'єктам. Це пояснюється тим, що в останні роки терористична діяльність стала більш організованою та керованою, що пов'язано з виконанням таких функцій, як розвідка, координація, різного роду забезпечення, у тому числі і фінансове, такої діяльності. З метою забезпечення виконання терористичних актів до банку можуть проникати певні особи з досить конкретною метою сприяння терористичній діяльності або ж може здійснюватися цілеспрямований вплив на окремих працівників задля виконання певних дій, необхідних терористам. І перший, і другий варіанти шкодитимуть банку і його діяльності.

Слід звернути увагу і на те, що в Україні, як і в усьому світі, існує досить багато потенційно небезпечних об'єктів, аварії, на яких можуть створити загрозу життю і здоров'ю населення та промисловим об'єктам або ж обумовлювати значні екологічні наслідки (табл. 4.5). За певних умов стосовно таких об'єктів зберігається імовірність скоєння терористичних актів і банки, що перебувають у зоні ураження від аварій на таких об'єктах можуть також зазнавати досить значної шкоди. Наприклад, диверсія на великому паливно- чи енергонасиченому об'єкті може створити осередок ураження площею до 1,5 км^2, в якому можуть опинитися до 15 тис. постраждалих, з яких до 2 тис. можуть загинути [3].

Важливою особливістю сучасного тероризму є інформаційний тероризм (кібертероризм).

Таблиця 4.5

ПОТЕНЦІЙНО-НЕБЕЗПЕЧНІ ОБ'ЄКТИ

Об'єкти	Загрози об'єктам
Атомні електростанції	Диверсії на ядерних реакторах чи технологічні збої в управлінні реакторами
Гідроелектростанції	Диверсії на плотинах, їх руйнування
Склади паливно-мастильних матеріалів, нафтопереробні підприємства	Диверсії, руйнування конструкцій, порушення технологій роботи
Пункти управління на транспорті, вузли зв'язку, радіо- та телецентри	Опромінювання генераторами електромагнітних імпульсів
Системи водопостачання підприємств харчової і м'ясомолочної промисловості	Зараження біологічними та отруйними речовинами
Підприємства хімічної промисловості, наукові установи з ядерними установами, об'єкти із запасами токсичних речовин	Диверсії руйнування систем захисту, ємностей, де зберігаються небезпечні речовини та матеріали
Висотні адміністративні та житлові будівлі	Підрив, виведення з ладу систем життєзабезпечення, руйнування будівель
Станції метро, стадіони, концертні та виставкові зали, вокзали, лікувально-профілактичні установи, торговельні центри	Диверсії, пожежі, хімічні атаки

Розвиток і широке впровадження в практику електронної обчислювальної техніки і створення на її базі засобів електронного зв'язку, передавання даних та обмін інформацією забезпечили формування нового виду технологій — інформаційних. Інформаційні технології являють собою сукупність способів реалізації інформаційних процесів (пошуку, збору, накопичення, обробки кодування, зберігання, отримання, поширення, надання, сприйняття) в різних областях життєдіяльності людини. Зазначені технології сьогодні становлять основу управління діяльністю будь-якої виробничої системи, у тому числі й у банківській діяльності. Будучи різними елементами інформаційної інфраструктури (технічні засоби зберігання електронної інформації — сервери, робочі

комп'ютери, комп'ютерні мережі, засоби контролю, захисту та передавання інформації), інформаційні технології залишаються досить уразливими до зовнішнього впливу на них. За таких умов банківське виробництво, що базується на зазначених технологіях, завжди перебуває під загрозою критичного впливу на нього кібертероризму. З цієї точки зору банківська діяльність є найбільш незахищеною, оскільки об'єктом дій терористів можуть бути інформаційні технології банків, які на сьогодні є найбільш уразливими з урахуванням можливостей терористів.

Терористичні дії на банківські інформаційні технології можуть здійснюватися в кількох варіантах:

- злом систем захисту і проникнення до банківської комп'ютерної інформації, виведення її з ладу або використання з іншою метою;
- ураження комп'ютерних програм банків вірусами, руйнування інформаційних масивів, блокування роботи банківських інформаційних систем;
- перехоплення управління банківськими платіжними системами, проведення несанкціонованих платежів, блокування інформаційного обміну в системах.

Отже, під загрозою інформаційного тероризму в банківській діяльності можна розуміти потенційну або реальну можливість певних суб'єктів здійснити атаку на електронну інформацію банку, інформаційну його інфраструктуру задля отримання доступу до місця зберігання чи систем передавання фінансової інформації, дестабілізації роботи банку та викрадення його коштів.

Ще однією особливістю сучасного тероризму, що створює небезпеку для банківської діяльності є електромагнітний тероризм, який використовує джерела потужних мікрохвильових випромінювань для функціонального подавлення радіоелектронних засобів. Електромагнітний тероризм спрямовує свою дію безпосередньо на радіоелектронні засоби, які становлять матеріальну базу інформаційних технологій, а також на системи електрозабезпечення, охоронні системи, радіостанції, засоби телекомунікації. Такі дії терористів можуть спрямовуватись як безпосередньо проти банків, так і щодо інших об'єктів, у зоні дії на які електромагнітного випромінювання може опинитися банківська установа. Крім того, застосування електромагнітного випромінювання може бути одним із елементів масштабної терористичної операції зловмисників або ж одним із видів забезпечення такої операції.

Останнім часом загострення отримала загроза терористичної діяльності з використанням зброї масового знищення. Принаймні проблеми забезпечення міжнародної безпеки від так званого супертероризму (терористичні дії з використанням зброї масового знищення) вже існують. Прискорення процесів глобалізації як характерної особливості сучасного світового розвитку висвітили дві тенденції — поширення зброї масового знищення і посилення міжнародного тероризму, що в найближчому майбутньому може стати постійним і системним фактором внутрішнього і міжнародного життя країн.

Найбільш доступним для терористів і не менш сильним за своєю дією є біологічна зброя. Засоби ураження, виготовлені на основі сучасних досягнень біотехнології і генної інженерії, за своїми масштабами та морально-психологічним ефектом у разі їх використання терористами можуть набагато перевершити наслідки застосування інших засобів.

Глобалізація, науково-технічний прогрес, розширення локальних конфліктів ведуть до розмивання меж між локальним і глобальним, внутрішнім і міжнародним, ідеологічним і кримінальним тероризмом. Використання біологічної зброї в терористичній діяльності (біотероризм) не пов'язується з вирішенням конкретної проблеми чи впливом на певний об'єкт. Біотероризм має необмежену мету, одним із варіантів якої є провокування в країні системної кризи у взаємовідносинах певних політичних угруповань, конкурентних взаємовідносинах суб'єктів того чи іншого ринку. Акції біотероризму спрямовуються на створення конфліктів між різними політичними угрупованнями, суб'єктами міжнародних взаємовідносин. З метою розвитку системної кризи терористи багато своїх завдань бачать у тому, щоб підірвати, дестабілізувати роботу певних економічних (у тому числі і фінансових) інституцій через масові хвороби їх працівників, клієнтів, партнерів, населення певного регіону, а також через паніку та неадекватну поведінку громадян. Прикладом такої ситуації можуть бути події з поширенням так званого пташиного та свинячого грипу. Тобто за умов поширення біотероризму загрозами для банків можуть бути наслідки, які виникають під його впливом у суспільстві. Опинившись в осередку інфекційних захворювань банківські установи можуть бути змушені обмежувати, а то й припиняти свою діяльність відповідно до вимог карантинних заходів. До того ж банк ніяк не може впливати на зміну такої ситуації і, безумовно, зазнає збитків від

вимушеної бездіяльності, періодичного проведення заходів дезінфекції, відпусток у зв'язку з хворобою своїх працівників та ін.

Характеризуючи загрози тероризму для банківської діяльності, можна сказати, що, безумовно, вони належать до найнебезпечніших, мають різний характер дії, досить масштабні, а за своїм впливом на банківські установи можуть формувати катастрофічні наслідки.

Останнім часом все більш актуальними стають процеси глобалізації та інтеграції.

Характерною рисою глобалізації у сфері економіки, безперечно, буде інтернаціоналізація капіталу. Значне зростання обсягів міжнародного руху капіталу між країнами у різних його формах зумовить формування глобальної матеріальної, інформаційної, організаційно-економічної інфраструктури, яка має забезпечити міжнародне співробітництво. У центрі такої інфраструктури опиняться банки. Якраз від надійності їхньої діяльності і залежатиме ефективність нашої участі у процесах глобалізації. За таких умов чинне місце в реформуванні вітчизняного банківського сектору, з погляду його готовності до участі в процесі глобалізації, має зайняти попередження загроз банківській діяльності, які несе в собі глобалізація та інтеграція. Тут слід врахувати, що поряд з позитивними перспективами глобалізація формує і досить суттєві ризики та загрози, які пов'язані насамперед з посиленням нестійкості національної економіки, багато в чому залежної від іноземних партнерів через інтернаціоналізацію виробництва та поглиблення нерівномірного розвитку як економік країн, так і окремих компаній. Для банків нестійкість економіки насамперед буде пов'язана з непередбачуваним та несподіваним коливанням основних макроекономічних показників (валютних курсів, процентних ставок тощо). Атмосфера невизначеності в прогнозуванні діяльності банків посилиться.

Певні ризики та загрози будуть обумовлені і стрімким формуванням єдиного загальносвітового фінансово-інформаційного простору на базі нових комп'ютерно-інформаційних технологій. Насамперед це сприятиме посиленню інформаційно-психологічного впливу на масову та індивідуальну свідомість громадян країни, а крім того забезпечить більшу відкритість банків, що може збільшити загрозу несанкціонованого доступу до їхньої інформації. Разом з тим посилення інформаційної складової в діяльності банків в умовах

глобалізації змінить ставлення банків до якості своїх інформаційних ресурсів, від яких залежатиме ефективність фінансових рішень керівництва банків.

Проблеми, які обумовлюються глобалізацією і в яких формуються загрози банкам, практично неможливо адекватно оцінити і вивчити не тільки на рівні одного банку, а навіть на рівні однієї країни. Більше того, глобальні сили, що формуються в процесі глобалізації, можуть ставати настільки потужними, що їх існування і подальший розвиток може загрожувати безпеці окремих країн.

Глобалізація діяльності банків може призвести до втрати державою свого впливу на розвиток фінансової складової національної економіки. Значна частка доходів банків, в яких домінує іноземний капітал, випливатиме за межі країни. Так, за даними іноземних досліджень до 75% доданої вартості, отриманої в результаті діяльності міжнародних корпорацій, використовується на користь економік країн їх базування.

Швидкий і вільний рух великих обсягів капіталу значною мірою підвищить інтенсивність діяльності банків, що, у свою чергу, збільшить ризик професійних і технологічних помилок. Безперечно, що за таких умов банківська діяльність має базуватися на системному та комплексному підході з виділенням пріоритетів для фінансової й інформаційної безпеки. Великого значення тут набуває і контроль фінансових потоків, виключення можливості використання клієнтами тіньового капіталу чи проведення ними незаконних фінансових операцій. Крім того, суттєвим буде питання недопущення потрапляння банків у фінансову залежність від інших фінансових суб'єктів, запобігання недобросовісній конкуренції з боку іноземних банків.

Очевидно, що найінтенсивнішим буде рух капіталів через прямі інвестиції, які змінять баланс короткострокового і довгострокового кредитування. Питома вага довгострокового кредитування у структурі кредитних портфелів банків значно збільшиться, що вимагатиме суттєвої перебудови кредитної діяльності банків, орієнтованої на довгострокове кредитування.

Крім того, збільшення масштабів міжнародної міграції робочої сили і зменшення кількості зайнятого населення може спричинили значний вплив міжнародної злочинності на банківську діяльність.

Таким чином, процеси глобалізації, формуючи в цілому сприятливі умови для розвитку діяльності банків, водночас створюють додаткові ризики та загрози, які мають суттєві

відмінності від уже добре відомих, до яких адаптувалися системи банківської безпеки.

Резюме

Підводячи підсумок аналізу загроз банківській діяльності, можна зробити такі висновки:

- діяльність банків здійснюється в умовах постійної дії тих чи тих загроз, які мають різноманітне спрямування та є доволі масштабними;
- загрози досить динамічні, швидко адаптуються до зміни умов функціонування банківських послуг та особливостей діяльності конкретних банків;
- реалізація загроз завжди призводить до негативних економічних наслідків, насамперед фінансових збитків банків;
- загрози мають як конкретну спрямованість щодо певного банку, так і глобальний характер, впливаючи на банки опосередковано;
- об'єктами загроз у банківській діяльності завжди є персонал банків, фінансові, матеріальні та інформаційні ресурси.

Аналізуючи загрози з точки зору суб'єктів загроз та причин їх формування, необхідно наголосити, що значна частина загроз створюється безпосередньо в банках і походить від їх персоналу. На жаль, за сьогоднішніх реалій банки не можуть суттєво впливати на мінімізацію таких загроз і будувати упереджені системи протидії їм. Загрози персоналу не концентруються на посадах чи напрямах банківської діяльності, вони однаково небезпечні і можуть формуватися за будь-яких умов і при здійсненні всіх видів банківських операцій, а також у процесі управління банком.

Ураховуючи зазначене банки мають вживати адекватних заходів захисту і протидії існуючим та потенційним загрозам на основі формування комплексних систем безпеки, орієнтованих на сучасні наукові та технічні досягнення.

Терміни і поняття

Банківське шахрайство
Внутрішні загрози
Дестабілізувальні фактори
Загроза банківській діяльності

Загрози тероризиму
Загрози, пов'язані з утягуванням банків у незаконну фінансову діяльність
Зловживання службовим становищем
Зовнішні загрози
Рейдерство

Питання для перевірки знань

1. Що слід розуміти під загрозою банківській діяльності?
2. Чим обумовлюється виникнення внутрішніх загроз діяльності банків?
3. Чи можуть створювати загрози банку його консультанти та радники?
4. Загрози якого характеру (зовнішнього чи внутрішнього) є найбільш небезпечними для банку?
5. Як реалізуються економічні, фізичні та інтелектуальні загрози?
6. Чи можна вважати загрозою для банку оприлюднення правдивих, але не вигідних для нього відомостей?
7. Що таке шахрайство?
8. Чи можна вважати шахрайськими дії суб'єкта, який допустив обман свого партнера, ввів його в оману і зловживав його довірою, але це не призвело до добровільної передачі партнером своєї власності суб'єкту?
9. Які загрози можуть виникати в умовах глобалізації та інтеграції капіталів?
10. У яких формах реалізується зловживання службовим становищем працівників банків?
11. У який спосіб здійснюється реалізація загроз, пов'язаних з утягуванням банків у незаконну фінансову діяльність?
12. Чому рейдерство слід розглядати як одну з актуальних загроз діяльності банків?
13. Які причини виникнення та поширення рейдерства в Україні?
14. З яких етапів складається рейдерська атака на банк?
15. Чому банки стають об'єктом інтересу злочинців чи терористів?

Завдання для індивідуальної роботи

1. Ви — працівник кредитного підрозділу банку. Одного разу на вашу адресу електронною поштою надійшов лист від одного з банків, у якому містилося застереження щодо співпраці з деякими ненадійними клієнтами і нижче був наведений перелік таких клієнтів. Серед них був і клієнт, який нещодавно отримав кредит у вашому банку, але він не допускав прострочення кредитних виплат, а також прострочення платежів щодо сплати процентів. Чи візьмете до уваги ви дану інформацію? Чи будуть існувати для банку які-небудь загрози за цих умов?

2. Ви — працівник підрозділу безпеки. Одного разу до вашого банку звернулося підприємство щодо можливості отримання кредиту для закупівлі товару. В цілому надані підприємством документи не викликали ніяких сумнівів, але в процесі перевірки клієнта стало відомо, що директор підприємства є засновником ще кількох фірм, його дружина — головний бухгалтер цих фірм, а син є директором фірми, в якої підприємство має намір закуповувати товар. Як ви вважаєте, чи матиме вплив на прийняття рішення про кредитування даного підприємства така інформація? Чого в даному разі слід остерігатися?

3. Ви — працівник відділу готівково-грошового обігу, тимчасово виконуєте обов'язки начальника відділу. На штатній посаді працюєте понад 15 років. Перспектив щодо підвищення в посаді немає. Одного разу до вас звернулась ваша колега з повідомленням про нестачу в касі 5 грн. При цьому вона зазначила, що причиною нестачі стали помилки в оформленні документів місячної давності. З метою ліквідації нестачі колега пропонує переробити документи, звертаючи вашу увагу на те, що дозвіл на такі дії неодноразово надавався попереднім керівником відділу. Як ви будете діяти в такій ситуації?

Література для поглибленого вивчення

1. Барановський О. О. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : [монографія] / Барановський О. О. — К.: КНТЕУ, 2004. — 759 с.

2. Гамза В. А. Безопасность банковской деятельности / В. А. Гамза, И. Б. Ткачук. — М. : Маркет, 2010. — 408 с.

3. Зубок М. І. Безпека бізнесу : навчальний посібник у схемах і таблицях / Зубок М. І., Позднишев Є. В., Яременко С. М. — К. : КНЕУ, 2008. — 480 с.
4. Павлов А. В. Основы организации безопасности банков / Павлов А. В. — М. : Изд. центр «Академия», 2010. — 128 с.
5. Ярочкин В. И. Безопасность банковских систем / Ярочкин В. И. — М. : Ось-89, 2004. — 416 с.

Розділ 5

НЕДОБРОСОВІСНА КОНКУРЕНЦІЯ ТА ПРОМИСЛОВЕ ШПИГУНСТВО В БАНКАХ

Вивчивши матеріал цього розділу, ви будете ***знати****:*

- ✓ *суть недобросовісної конкуренції та її місце у взаємовідносинах банків;*
- ✓ *основні види та форми недобросовісної конкуренції в банківській діяльності;*
- ✓ *правову оцінку недобросовісної конкуренції за вітчизняним і міжнародним правом;*
- ✓ *суть, об'єкт та форми діяльності промислового шпигунства в банках;*
- ✓ *методи роботи промислових шпигунів щодо залучення банківських працівників до шпигунських дій,*

а також ***уміти****:*

- ✓ *виявляти ознаки дій з недобросовісної конкуренції і промислового шпигунства при роботі в банку;*
- ✓ *розпізнавати дії, спрямовані на вас з метою залучення до шпигунської діяльності в банку.*

5.1. Недобросовісна конкуренція у взаємовідносинах банків

У системі взаємовідносин суб'єктів ринку існують різні за суттю, взаєморозумінням і напруженістю стосунки. Залежно від становища суб'єкта ринку, зміни його інтересів, кон'юнктури ринку ці стосунки можуть перебувати у площині як повного порозуміння, так і антагоністичного протиборства. Визначають кілька видів взаємовідносин, які відбивають стан стосунків суб'єктів ринку у процесі їх комерційної діяльності, серед них:

- *співпраця* — спільні і тісні ділові відносини суб'єктів господарювання на основі загальних інтересів з метою удосконалення методів роботи, направленої на збільшення прибутків;
- *взаємодія* — узгоджені дії суб'єктів господарювання щодо мети, місця (регіону) і часу для досягнення максимального ефекту в отриманні вигоди і прибутку;
- *конкуренція* — змагання суб'єктів господарювання з метою здобуття переваг над іншими суб'єктами ринку завдяки власним досягненням;
- *суперництво* — антагоністичні дії суб'єктів господарювання, побудовані на непримиримості позицій, інтересів і методів роботи щодо отримання переваг на ринку;
- *протиборство* — гостра антагоністична боротьба суб'єктів господарювання за завоювання і монопольне володіння ринком, у процесі якої застосовуються дуже жорсткі заходи впливу на суперників.

Конкуренція займає центральне місце у взаємовідносинах суб'єктів ринку і характеризується переходом від їх спільних, партнерських дій на ринку до дій, пов'язаних із обмеженням можливостей конкуруючих суперників як через вплив на умови функціонування ринку, так і на самих суперників та середовище їхньої діяльності.

Розглядаючи конкуренцію як обов'язковий атрибут ринкових відносин та рушійну силу розвитку економіки, слід звернути увагу на те, що виробнича діяльність в умовах конкуренції, повинна відповідати таким вимогам:

✓ підвищення якості товарів і послуг;

✓ зниження цін і надання пільг;
✓ розвиток до- і післяпродажного обслуговування;
✓ розроблення нових видів товарів і послуг з використанням наукових і технічних досягнень тощо.

Отже, конкуренція — важливий інструмент ринку і основна складова взаємовідносин його суб'єктів. Водночас вона є потужним засобом удосконалення виробництва і якості товарів та послуг, розвитку економіки країни і задоволення споживчого попиту. Разом з тим ринок — це насамперед економічна свобода. Ринкова діяльність регулюється кон'юнктурою ринку та відповідними правовими і моральними нормами. Правові засади регулювання ринкової поведінки (конкуренції) визначаються державою через установлення відповідних норм здійснення підприємницької діяльності. Моральні норми складають у процесі взаємовідносин суб'єктів ринку, і зазвичай базуються вони на певних традиціях.

Водночас в основі ринкових відносин знаходяться вигода суб'єктів ринку. У боротьбі за досягнення вигоди суб'єкти ринку вдаються до різних дій і поведінки, у тому числі і таких, що не зовсім відповідають нормам права та ринкової моралі. Так, поряд з конкуренцією, започаткованою на чесних, добросовісних відносинах, з'являється і недобросовісна конкуренція.

Згідно з Законом України «Про захист від недобросовісної конкуренції» під недобросовісною конкуренцією розуміють будь-які дії у конкуренції, що суперечать торговельним та іншим чесним звичаям у господарській діяльності [56]. Міжнародна ж практика недобросовісну конкуренцію визначає як будь-який акт конкуренції, що суперечить чесним звичаям у промислових та торговельних справах [34]. Порівняння суті визначення недобросовісної конкуренції та її змісту за вітчизняним і міжнародним правом дається на рис. 5.1.

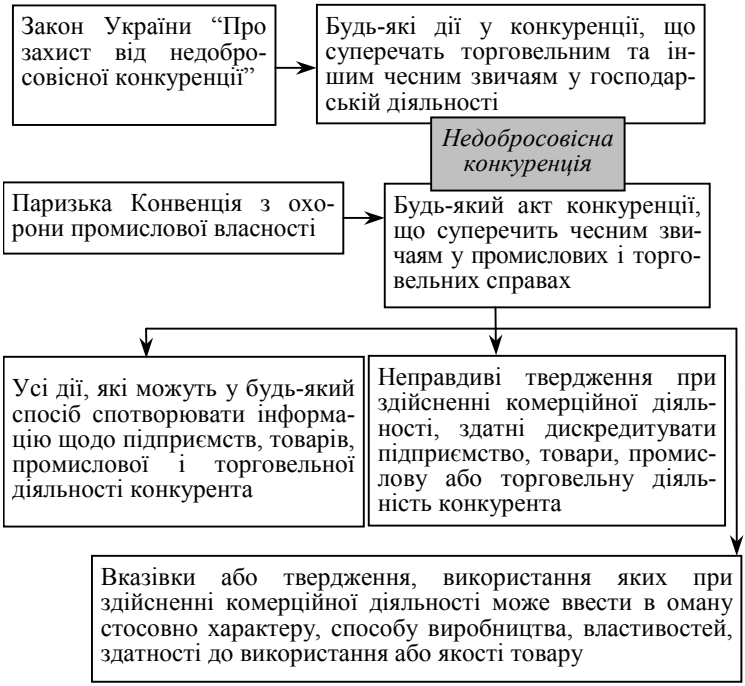

Рис. 5.1. Недобросовісна конкуренція згідно з вітчизняним і міжнародним правом

Метою недобросовісної конкуренції є забезпечення або закріплення своїх позицій чи переваг на ринку за рахунок послаблення можливостей конкурентів. Оскільки така діяльність руйнує конкурентні відносини і завдає істотної шкоди конкуренції і конкурентам — суб'єктам підприємницької діяльності, а також споживачам вона заборонена законом і стосовно неї встановлюється певна відповідальність. Законодавство забороняє недобросовісну (нечесну) поведінку підприємців, яка завдає шкоди інтересам інших підприємців і водночас створює загрозу суспільним інтересам у забезпеченні ефективних конкурентних процесів в економіці в цілому. Водночас вітчизняне законодавство не встановлює вичерпного змісту порушень конкуренції, як недобросовісних дій конкуруючих суб'єктів, оскільки з розвитком ринкових відносин можуть з'являтись і нові види антиконкурентної їх поведінки.

Заборона недобросовісної конкуренції зафіксована у ст. 42

Конституції України [24]. Безпосередній перелік заборонених дій, що визначаються недобросовісною конкуренцією, дається у главах 2–4 Закону України «Про захист від недобросовісної конкуренції». Зокрема, у законі визначено три види правопорушень: а) неправомірне використання ділової репутації суб'єкта господарювання; б) створення перешкод суб'єктам господарювання у процесі конкуренції та досягнення неправомірних переваг; в) неправомірне збирання, розголошення та використання комерційної таємниці (рис. 5.2) [56].

Виходячи з визначення недобросовісної конкуренції та змісту дій, пов'язаних з нею можна вважати, що основним у виявленні ознак недобросовісної конкуренції є будь-яка поведінка, засіб конкурентної боротьби, які суперечать звичаям чесної підприємницької практики, пов'язані з порушенням прийнятих на ринку норм і правил, що мають місце у відносинах між конкуруючими суб'єктами.

Отже, недобросовісна конкуренція стосується насамперед сфери моральних (а не правових) відносин. Водночас виходячи із суті визначення поняття недобросовісної конкуренції вона може виникати лише між конкуруючими суб'єктами незалежно від об'єкта конкуренції.

Невідповідність же чесним звичаям підприємницької діяльності є нічим іншим як обманом, тому будь-який обман як нечесна поведінка суб'єкта може вважатись і недобросовісною конкуренцією.

Рис. 5.2. Види та форми недобросовісної конкуренції

Обман у взаємовідносинах суб'єктів ринку виникає, як правило, коли останні перебувають у стані суперництва або протиборства. Але якщо об'єктом недобросовісної конкуренції у суперництві є зазвичай споживач, клієнт прихильність якого прагнуть завоювати суперники, то у протиборстві об'єктом стають самі суперники, їхні дії спрямовуються на приниження можливостей одним одного. У першому випадку, як правило, проводиться широка агітаційна та контрагітаційна робота, у тому числі й із застосуванням дезінформації щодо якостей, переваг власної продукції (послуг), і навпаки, щодо низьких характеристик, слабких можливостей суперника. У другому ж протиборство відбувається по двох напрямах: економічному й інформаційному. Тут можливе переманювання працівників, клієнтів, викрадення, копіювання розробок, нових зразків продукції, несанкціонований доступ до інформації з обмеженим доступом, бойкот тощо. Щодо інформаційного напряму, то тут здійснюється поширення інформації про порушення законодавства конкурентом, злочинні його дії, різке зниження фінансових можливостей стосовно виконання зобов'язань перед кредитором, клієнтами, всіляко ініціюється проведення перевірок, відплив клієнтів. За всіх умов інформаційна складова протиборства конкурентів спрямовується на дестабілізацію їхньої діяльності. Звичайно, і в першому, і в другому випадках широко використовуються обман, дезінформація, поширення негативної та неправдивої інформації про конкуруючих суперників.

Водночас, даючи недобросовісній конкуренції правову оцінку, необхідно зазначити, що певна частина її дій має прямо протизаконний характер. Тут слід звернути увагу на те, що в практиці конкурентних відносин існує таке поняття, як кримінальна конкуренція. З погляду підприємців та правоохоронних структур кримінальна конкуренція розуміється як участь певних організацій чи окремих фізичних осіб у суперництві з економічними суб'єктами задля досягнення поставленої мети в різних сферах життєдіяльності з використанням заборонних законом методів і засобів діяльності. Тобто основною відмінністю тут є таке: якщо дії з недобросовісної конкуренції зосереджуються переважно в економічній та інформаційній сфері (демпінг, зловживання монопольним становищем, поширення неправдивої, негативної інформації, недотримання стандартів вироблення продукції, надання послуг, таємна домовленість і т. п.), то основною ознакою кримінальної конкуренції є порушення законодавства

(використання заборонених законом методів і засобів діяльності: незаконна, фіктивна діяльність, легалізація незаконно отриманих доходів і їх використання в економічному суперництві, незаконне отримання кредитів або умисне їх неповернення, корупція тощо). Основними методами кримінальної конкуренції можуть бути промислове шпигунство, шантаж, залякування, крадіжки, підкуп та ін. Як правило, в такій конкуренції беруть участь не економічно потужні суб'єкти, а структури, які мають достатній тіньовий капітал, корумповані зв'язки, а то й зв'язки з кримінальним світом. Звичайно, такі дії порушують етику бізнесу, знижують його ділову активність, утискують цивілізоване підприємництво.

Основними ознаками кримінальної конкуренції можуть бути:

- порушення закону в конкурентних відносинах суб'єктів ринку;
- однобічний характер кримінальної конкуренції, оскільки кримінальні методи і засоби конкурентних відносин застосовує лише одна сторона;
- у кримінальній конкуренції беруть участь не тільки економічні суб'єкти, їм можуть сприяти кримінальні елементи, корумповані чиновники, мафіозні структури;
- кримінальна конкуренція діє, як правило, досить цілеспрямовано, зосереджуючи свої зусилля проти конкретного економічного суб'єкта;
- у результаті дій кримінальної конкуренції економічним суб'єктам завдається не тільки матеріальна шкода, а й шкода іміджу їхньої діяльності;
- у кримінальній конкуренції не так важливі витрати на заходи, що вживаються, як мета, заради якої вона проводиться.

На сьогодні поняття кримінальна конкуренція не має офіційного тлумачення, як правило, використання незаконних методів і засобів у конкурентній боротьбі трактується як недобросовісна конкуренція, але суть таких дій, безумовно, має кримінальний характер і отримує відповідну правову оцінку.

Беручи до уваги ситуацію, що склалася на ринку банківських послуг можна вважати, що сьогоднішні її особливості загострили конкурентну боротьбу банків. Практично всі операції, які проводять банки, здійснюються в умовах підвищеного ризику, пов'язаного не тільки зі складною економічною ситуацією, а й з посиленням агресивної поведінки банків у взаємовідносинах між собою. У деяких випадках такі взаємовідносини набувають антагоністичного, безкомпромісного характеру і здійснюються в умовах жорсткої конфронтації. Поряд з взаємовизнаними

методами конкуренції, направленими на удосконалення банківського виробництва, вироблення ефективніших форм і способів отримання прибутку, досить часто використовуються методи недобросовісної конкуренції.

Особливо такі взаємовідносини загострились і в період останньої кризи, коли банки опинились в умовах обмежених можливостей щодо формування своїх фінансових ресурсів через розорення підприємств і втрату роботи громадянами.

Основною метою недобросовісної конкуренції в банківській сфері є прагнення банку-конкурента поліпшити або закріпити своє становище чи здобути перевагу на ринку за рахунок послаблення позицій конкуруючих банків і введення в оману клієнтів. Жертви недобросовісної конкуренції відчувають її результати, як правило, через зміни на ринку банківських послуг, насамперед як несподівані для себе негативні умови.

Недобросовісну конкуренцію проти банків можуть вести як самі конкуруючі банки, так і за допомогою клієнтів, партнерів, кримінальних елементів, інших суб'єктів.

Особливістю недобросовісної конкуренції через клієнтів можуть бути неправомірні вимоги створення більш вигідних або сприятливих для них умов укладання угод, отримання кредитів, проведення інших операцій та обслуговування в банку. Крім того, через клієнтів можуть поширюватися неправдиві, неточні або неповні відомості про банк, особливо у випадках простроченої заборгованості йому, та ін. Характерним є вплив клієнтів на службовців банку з метою запоруки та позитивного вирішення вигідних для клієнтів справ, утягування банківських працівників у протиправну діяльність. Клієнти можуть здійснювати збір інформації про діяльність банку, у тому числі таємної та конфіденційної, наглядати за окремими працівниками та організовувати їх підкуп, знаходити канали витоку інформації, вивчати характер і особливості діяльності банку.

Серед дій недобросовісної конкуренції, що можуть застосовуватися банками-конкурентами, можна вважати такі:

- зманювання клієнтів і співробітників з одного банку до іншого;
- зрив угод і договорів через поширення неправдивої інформації;
- незаконне отримання конфіденційної і таємної інформації та її використання з метою завдати шкоди банку;
- шантаж і компрометація керівництва і провідних співробітників банку;
- поширення неправдивих, неточних або перекручених,

• зловживання домінуючим становищем банку на ринку банківських послуг та ін.

У деяких випадках прийоми недобросовісної конкуренції можуть застосовуватись і через партнерів банку. Насамперед — це передання інформації щодо клієнтів, акціонерів, а також інших партнерів.

Відомі випадки проведення дій недобросовісної конкуренції кримінальними елементами, зокрема з метою просування на ринок «своїх» суб'єктів господарювання, а також прагнення встановити контроль над окремими банками. Як правило, у таких випадках спочатку створювалися різноманітні перешкоди діяльності банків, а потім надавались умови і пропозиції щодо їх усунення.

Причинами, які обумовлюють недобросовісну конкуренцію, у тому числі і на ринку банківських послуг, є корупція і тінізація економіки, вузькість ринків діяльності суб'єктів господарювання, розходження інтересів ділових партнерів, недостатня професійна підготовка спеціалістів і керівників комерційних структур, неефективні технології виробництва та застаріле обладнання, що використовуються підприємствами та банками, жорстка податкова політика, значна криміналізація всіх сфер життя і діяльності населення.

Говорячи про недобросовісну конкуренцію на ринку банківських послуг, необхідно звернути увагу на більш прихований її характер порівняно з іншими економічними ринками. Насамперед це пов'язано з довірою до банків взагалі, коли будь-яка боротьба між банками або за участі інших структур однозначно призводить до різкого відпливу клієнтів, зниження фінансового ресурсу, настороженості всіх суб'єктів ринку, і хвиля негараздів, яка спрямована на банк — жертву недобросовісної конкуренції, обов'язково відіб'ється на інших банках. Тому дії з недобросовісної конкуренції дуже важко розпізнавати та виокремлювати їх серед інших загроз. Тут важливо мати на увазі ознаки дій недобросовісної конкуренції, які можуть вказувати на те, що причина негараздів, які спіткали той чи інший банк випливають саме з недобросовісної конкуренції. Перелік таких ознак вказано в Додатку 1.

Розглядаючи конкурентні відносини, не можна залишити поза увагою зловживання окремих банків домінуючим становищем на ринку банківських послуг, що може створювати істотні загрози

банківській діяльності. Аналіз поведінки банків на вітчизняному ринку банківських послуг показує, що такі дії мають місце, хоча вони і не мають активного характеру, але все ж таки за певних умов завдають шкоди деяким банкам. Тут мова може йти про встановлення банками певних умов надання послуг, які неможливо було б установити за умов існування значної для них конкуренції, особливо на регіональному рівні, установлення різних умов банківського обслуговування для рівнозначних клієнтів без об'єктивно обґрунтованих причин; відсутність компромісів у взаємовідносинах з іншими банками; штучне обмеження доступу до необхідної інформації про банк суб'єктам, які не можуть отримати подібні послуги в інших банках через недостатню конкуренцію; створення перешкод виходу інших банків у нові регіони, сфери економіки, виробленню нових банківських продуктів.

Основними ознаками, які можуть вказувати на монопольні тенденції в діяльності окремих банків, слід вважати:

- активне вироблення та якісне надання банківських послуг, великий асортимент послуг, прагнення банку до тісної співпраці з клієнтами;
- постійне просування своїх послуг у різні сфери економіки та на різні регіони, розширення мережі банківських установ;
- активна реклама, пропаганда і агітація;
- лобіювання своїх інтересів в органах влади;
- недоброзичливе, зверхнє ставлення до діяльності інших банків, незалежна поведінка на ринку, агресивність у відносинах при вирішенні спірних питань з іншими банками.

Звичайно, що такі ознаки не обов'язково вказуватимуть на зловживання банком монопольним становищем, але за їх наявності слід вважати, що така можливість потенційно існує.

За вчинення дій, що визнаються недобросовісною конкуренцією, законодавство передбачає санкції, які мають різну галузеву належність.

Розмір санкцій і порядок обчислення їх залежить від суб'єкта правопорушення, а саме: є він суб'єктом господарювання чи ні. Вчинення дій, визначених чинним законодавством як недобросовісна конкуренція, тягне за собою накладання на них Антимонопольним комітетом України відповідних стягнень.

Стаття 164-3 Кодексу України про адміністративні правопорушення [23] встановлює, що незаконне копіювання форми, упаковки, зовнішнього оформлення, а так само імітація, копіювання, пряме відтворення товару іншого підприємця,

самовільне використання його імені тягне за собою накладення штрафу від 30 до 44 неоподатковуваних мінімумів доходу громадян з конфіскацією виготовленої продукції, знарядь виробництва і сировини чи без такої. За умисне поширення неправдивих або неточних відомостей, які можуть завдати шкоди діловій репутації або майновим інтересам іншого підприємця, передбачається накладення штрафу від 5 до 9 неоподатковуваних мінімумів доходів громадян. Отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця тягне за собою накладення штрафу від 9 до 18 неоподатковуваних мінімумів доходів громадян.

Згідно зі статтею 229 Кримінального кодексу України [27] незаконне використання чужого товарного знака для товарів і послуг фірмового (зареєстрованого) найменування, маркування товару, якщо це було пов'язано з отриманням доходу у великих розмірах, карається штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк з конфіскацією відповідної продукції та знарядь і матеріалів, які спеціально використовувалися для її виготовлення. Використання товарного знака визнається незаконним і створює склад злочину, якщо таке завдало шкоди інтересам суб'єкта підприємницької діяльності (власникові знака або іншим суб'єктам) або такі дії були пов'язані з отриманням доходу у великих розмірах (300 і більше разів перевищує неоподатковуваний мінімум доходів громадян). Незаконне використання чужого товарного знака вчиняється умисно з метою отримання прибутку.

За умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також за незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, ст.231 Кримінального кодексу України передбачено покарання у вигляді штрафу від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до п'яти років, або позбавленням волі на строк до трьох років [27].

Згідно зі ст. 232 Кримінального кодексу України за умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною чи службовою діяльністю, якщо воно вчинене з корисливих чи з

інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років або позбавленням волі на той самий строк [27].

Цивільно-правовою санкцією за недобросовісну конкуренцію є відшкодування збитків. Особи, яким завдано шкоди внаслідок вчинення дій, визначених Законом України «Про захист від недобросовісної конкуренції» [56] як недобросовісна конкуренція, можуть звернутися до суду з позовом про її відшкодування.

За ст. 26 Закону України «Про захист від недобросовісної конкуренції» у разі встановлення факту дискредитації суб'єкта господарювання органи Антимонопольного комітету України мають право прийняти рішення про офіційне спростування за рахунок порушника поширених ним неправдивих, неточних або неповних відомостей у строк і спосіб, визначені законодавством або цим рішенням. Отже, санкцією є спонукання порушника до провадження дій щодо офіційного спростування зазначених відомостей за його рахунок [56].

Отже, вчинення таких дій, як недобросовісна конкуренція тягне за собою адміністративну, цивільну та кримінальну відповідальність. Важливим є те, що при кваліфікації певної поведінки суб'єктів господарювання як недобросовісної конкуренції треба довести, що суб'єкти господарювання:

- виробляють однакові або схожі товари (роботи, послуги);
- діють на одному ринку;
- між ними існує конкурентна ситуація.

Лише в разі доведення існування сукупності цих ознак у відносинах між суб'єктами господарювання, можна говорити про те, що між ними існують саме конкурентні взаємовідносини і в разі порушення ведення чесних правил цих відносин можливе притягнення винного суб'єкта до юридичної відповідальності, згідно із законодавством України.

5.2. Промислове шпигунство в банківській діяльності

Досить несприятливі умови діяльності банку створюються у разі ведення проти нього промислового шпигунства. Такі дії можуть завдати йому дуже великої шкоди як матеріального, так і іміджевого характеру.

Основним об'єктом промислових шпигунів є інформація, причому інформація, основу якої становить комерційна та банківська таємниця. Саме відомості, віднесені до такої категорії інформації, є найбільш цікавими для конкурентів банку і саме вони є об'єктом пильної уваги промислових шпигунів.

Сьогодні практично немає чіткого визначення поняття «промислове шпигунство». Найбільш повне, з юридичної точки зору, визначення дає Міжнародна організація кримінальної поліції (Інтерпол): «…це придбання будь-яким обманним шляхом інтелектуальної власності, яка належить будь-якій юридичній особі і яка була створена або законно придбана цією юридичною особою з метою виробництва, що має або може мати промислову цінність...».

Одне з визначень промислового шпигунства міститься у ст. 54 Типового проекту законодавства, розробленого Міжнародною радою з охорони промислової власності. «Промисловим шпигунством є використання, розголошення або передання без погодження з власником інформації, відомостей про способи виробництва і використання техніки, які не публікувалися в пресі і є недоступними для відкритого ознайомлення особою, якій відомий таємний характер цих відомостей, якщо автор вжив відповідних заходів щодо охорони їх таємності».

Існує багато різних форм і методів промислового шпигунства. Але попри їх численність вони обумовлені переважно самою природою промислового шпигунства як таємною формою конкурентної боротьби.

Аналізуючи різні точки зору щодо змісту поняття «промислове шпигунство», слід звернути увагу на дві основні особливості:

- об'єктом діяльності промислових шпигунів завжди є інформація стосовно якої власником установлюється обмежений доступ. Згідно з вітчизняним законодавством це можуть бути відомості таємного чи конфіденційного характеру;
- отримання таких відомостей завжди здійснюється з подоланням ужитих власником заходів захисту, причому немає ніякого значення, які це заходи: технічного, інтелектуального, організаційного чи будь-якого іншого характеру. Тобто

Отже, з метою повнішого розуміння суті промислового шпигунства йому можна дати таке визначення: під промисловим шпигунством слід розуміти діяльність, в основу якої покладено сукупність спеціальних заходів, спрямованих на отримання інформації з обмеженим доступом, яка охороняється певним суб'єктом.

Історія промислового шпигунства сягає своїм корінням у глибину віків так далеко, що неможливо встановити навіть приблизний період його зародження. Найбільш давній приклад цього ремесла наведений відомим французьким письменником Роні Старшим (Жозеф Анрі Беке) у книзі «Боротьба за вогонь». Герої книги — первісні люди — відправляються в сусіднє плем'я, аби викрасти таємницю здобування вогню. Хоч покарання було страшним (прикутого до гір Кавказу Прометея кожного дня шматував орел), але таємниця була викрита і вогонь передано тим, хто їм ще не користувався. Хоч як би там було, та у міфі про Прометея ми знаходимо ознаки дій, які зараз називають промисловим шпигунством.

Серед історичних прикладів промислового шпигунства можна згадати викрадення таємниці виробництва фарфору в Китаї французькими промисловцями, а в останніх — англійським агентом Бріаном; викрадення таємниць виробництва високоякісної сталі у Континентальної гільдії плавильників (Бельгія, Німеччина, Північна Італія, Богемія, Іспанія) англійським шпигуном Фолі у XIX ст.; викрадення японськими агентами таємниць виготовлення шовку, способу шліфування лінз тощо.

У розвинутих країнах сьогодні промислове шпигунство значно поширене. Так, наприклад, у США з 1986 р. легально існує «Товариство фахівців зі здобування відомостей про конкурентів», яке налічує майже 1500 постійних членів. В Японії тільки в одному Токіо діє близько 400 відомств і бюро, які так чи інакше займаються промисловим шпигунством.

Ринкова економіка породжує конкуренцію. Остання потребує знань, інформації про ринок і його суб'єктів. Тому слід добре усвідомити, що з переходом до ринкових відносин ми одночасно отримуємо як постійно існуючі їх риси — недобросовісну конкуренцію і промислове шпигунство, які неможливо повністю

усунути (інакше ми повинні відмовитись від ринкових умов). Їх треба враховувати у підприємницькій діяльності, запобігати їм, виявляти факти і нейтралізувати наслідки.

Оскільки об'єктом промислового шпигунства є інформація з обмеженим доступом, великого значення набуває виявлення джерел (носіїв) інформації, до яких якраз і прагнуть отримати доступ промислові шпигуни. Такими носіями можуть бути різного роду документи (фінансові, правові, з питань кадрової роботи, розвитку банку, його технологій, системи безпеки), електронні носії (диски, дискети, комп'ютерна техніка), креслення, схеми, карти, плани, патенти, розрахунки, протоколи, акти, аудіо- та відео матеріали, а також працівники банків, клієнти, партнери та інші особи, які можуть бути обізнані з таємницями банку.

Суб'єктами ж промислового шпигунства, тобто особами, які безпосередньо організовують та здійснюють заходи з отримання інформації, можуть бути підрозділи безпеки інших банків, підприємств, організацій, детективні агентства та приватні детективи, спецслужби держави. Зазначені суб'єкти отримують необхідну їм інформацію як безпосередньо, так і через своїх агентів, якими можуть бути працівники та клієнти банків, їх партнери, радники, консультанти, журналісти, представники органів контролю та нагляду, окремі державні службовці.

Тут слід звернути увагу на те, що банки-конкуренти та інші суб'єкти можуть не тільки вдаватися до самостійних дій зі збору інформації, а й звертатися до суб'єктів, які професійно займаються питаннями інформаційної роботи, і така робота є змістом їх бізнесу. В Україні хоча на сьогодні офіційно і не існує детективної діяльності, але разом з тим функціонують досить багато консалтингових фірм, компаній і підприємств, які надають різного роду інформаційні послуги, у тому числі і пов'язані зі збором інформації. Тому в конкурентних відносинах банків цілком реальна присутність інших суб'єктів, які не мають ніякого стосунку до банків, але їхня діяльність може істотно шкодити банківським установам. В окремих випадках банки самі створюють подібних суб'єктів або ж інші структури безпеки, однією із функцій яких є інформаційне забезпечення банківської діяльності, у тому числі і з застосуванням промислового шпигунства.

Водночас, аналізуючи чинне конкурентне законодавство, необхідно зазначити, що неправомірне збирання інформації, яка становить комерційну таємницю, та схилення до її розголошення

є діями недобросовісної конкуренції. Тобто промислове шпигунство, основу якого якраз і становлять дії з протиправного добування комерційної таємниці, у тому числі і через спонукання відповідних осіб до розголошення відомих їм таємниць, є однією із форм недобросовісної конкуренції.

Головне місце у діяльності промислових шпигунів займають три основні джерела необхідної їм інформації: людина як виробник і носій інформації, документ як зберігач інформації, процес виробництва як матеріальне втілення інформації. Тому промислові шпигуни поєднують методи своєї нелегальної діяльності з легальним збором інформації, тобто інформаційною роботою.

У сучасних умовах більшість конкуруючих банків віддають перевагу збиранню інформації про конкурентів легальними методами, використовуючи офіційні джерела: відвідування банків, аналіз відкритих матеріалів про їх діяльність, установлення необхідних взаємовідносин з банківськими установами і міжбанківськими організаціями, клієнтами банків, укладення угод і договорів, участь у конференціях та інших форумах, де обговорюються проблеми діяльності банків.

Разом з тим наявність відкритої інформації не завжди задовольняє потреби банків. Тому збирання найбільш цінної інформації ведеться, як правило, нелегально та напівлегально.

Сьогодні найбільш відомими і поширеними формами нелегального та напівлегального збирання інформації є:

- анкетування фахівців банку-конкурента під виглядом запрошення їх на роботу;
- підкуп службовців банку-конкурента, засилання до такого банку агентів, установлення спеціальних технічних засобів у його приміщеннях для несанкціонованого отримання інформації;
- опитування фахівців конкурента на виставках, конгресах, конференціях, семінарах;
- спостереження за діяльністю установ банку та його персоналом;
- неправдиві переговори з банком-конкурентом;
- посягання (викрадення) на інтелектуальну власність банку-конкурента;
- підслуховування розмов, вивідування інформації;
- шантаж і різні форми тиску на працівників і клієнтів банку як на джерела інформації;
- викрадення документів, програмних засобів;
- збирання інформації через закордонні філії, партнерів, клієнтів, спільних постачальників, консультантів, радників,

Слід звернути увагу, що змістом промислового шпигунства є не тільки отримання інформації, за певних умов промислові шпигуни можуть вдаватися до модифікації (зміни) банківської інформації, знищення її носіїв, руйнування інформації, особливо на електронних носіях, компрометації інформації чи її носіїв, несанкціонованого оприлюднення інформації.

Промислових шпигунів може цікавити діяльність і особисте життя керівників та представників вищого менеджменту конкуруючих фірм, банків, особливості їх поведінки, близьке оточення та стосунки з ним.

Наведені форми промислового шпигунства можуть реалізовуватися різними методами. Наприклад, неправдивий прийом на роботу починають з вивчення кола осіб, які можуть знати необхідну промисловим шпигунам інформацію. Після вибору особи уточнюються найбільш популярні періодичні видання, які цікавлять дану особу, в них дається оголошення з пропозицією вигідних умов роботи такого фахівця. Як правило, умови роботи в таких оголошеннях значно кращі, ніж ті, що має зараз фахівець. Останній відвідує конкуруючий банк, заповнює необхідні анкети, зустрічається з майбутнім керівництвом і, бажаючи показати себе з кращого боку, розповідає не тільки те, що він робить сам, а й те, чим займається його підрозділ або банк у цілому.

Через деякий час фахівець отримує ввічливу відповідь з відмовою і продовжує працювати на своєму місці, нічого не підозрюючи. А конкуруючий банк уже отримав необхідну йому інформацію.

Увага промислових шпигунів може приділятись і негативним рисам поведінки та хибам працівників конкуруючих структур. Якщо такі риси відсутні, то негативна поведінка, помилки можуть бути спровоковані. Це і неконтрольована поведінка працівників у стані сп'яніння, матеріальна подяка за незначні дії на користь когось із клієнтів, надання позик на пільгових умовах тощо.

Історія промислового шпигунства дає дуже багато прикладів залучення до неправомірного збору інформації працівників відповідних інформаційних об'єктів. Потенційними зрадниками промислові шпигуни вважають розгніваних, заляканих, жадібних, гордовитих і зарозумілих людей. А серед обставин, за яких людина може стати зрадником, можуть бути нагальні матеріальні потреби, страх після скоєння порушення, наркотична, алкогольна чи якась інша залежність, ігнорування

працівника колективом, конфлікти працівника з керівництвом, сімейні негаразди, інші потреби (у відпочинку, лікуванні, навчанні).

Професіонали промислового шпигунства вказують, що в основі залучення носія інформації до роботи на них є кілька факторів, найбільш поширений тут — гроші. Крім того, досить часто фігурують такі фактори, як ідеологія, секс, компромат, особливості характеру. Основні характеристики потенційних зрадників, здатних до роботи на промислових шпигунів, вказані у Додатку 2.

У процесі залучення працівників банку, підприємства до роботи на промислових шпигунів останні, як правило, дотримуються такого алгоритму:

- вивчення працівників, які працюють на ділянках і напрямах, що є об'єктом зацікавленості промислових шпигунів;
- виявлення серед працівників осіб, які негативно ставляться до банку чи його керівництва, невдоволені умовами роботи;
- виявлення серед працівників осіб, щодо яких є інформація про їх протиправну (злочинну) діяльність;
- виявлення серед працівників осіб, яким притаманні певні вади (пияцтво, наркотична залежність, захоплення азартними іграми, або тих, які мають хронічні та небезпечні хвороби, приховують від оточуючих певні проступки);
- використання отриманої негативної інформації для впливу на працівників з метою залучення їх до роботи на промислових шпигунів;
- штучне створення ситуацій з метою отримання (формування) негативної інформації про осіб, щодо яких є наміри залучення до роботи на промислових шпигунів.

За всіх умов уникнути від співпраці з професійно підготовленими шпигунами самостійно працівникові досить складно. Як правило, промислові шпигуни діють щодо особи, яку з їх погляду доцільно було б залучити до роботи на них досить наполегливо, активно і тривалий час.

Якщо працівник банку починає працювати на конкурентів або на когось іншого, то це приходить не одразу і не раптом. Перш ніж прийняти рішення зробити такий крок, нормальна людина повинна мати досить вагомі підстави. Слід підкреслити, що людина, як правило, прагне до стабільності у житті і не стане через дрібниці ламати свою долю і кар'єру. Отже, конкуренти шукатимуть передусім тих людей, яких обставини змушують змінити свій спосіб життя. В окремих випадках вони спеціально

створюватимуть такі обставини.

Пропозиції щодо роботи на конкурентів можуть здійснюватись у формах: за винагороду продати інформацію, яка містить банківську або комерційну таємницю, і таку, що є конфіденційною; таємно працювати на конкурентів, отримуючи за це одноразову або постійну винагороду; перейти на роботу до банку-конкурента з подальшим використанням таємниць, інтелектуальної власності банку на користь конкурента.

Ознаками, які можуть вказувати на спроби втягування працівників банку до співробітництва з конкурентами або іншими структурами, можуть бути:

- під час розмов із службовцями з будь-якого приводу ставляться запитання, що стосуються різних сторін та способу життя когось із працівників, його ставлення до роботи та керівництва;
- спостереження за окремими працівниками: вивчення звичок, улюблених місць проведення свого дозвілля, хобі тощо;
- участь однієї і тієї ж особи у позаслужбових зустрічах і заходах, необґрунтовано часта матеріальна і грошова вдячність за незначні послуги;
- втягування службовця або близьких йому людей у різні сумнівні угоди, ризикові компанії, надання грошей у борг, створення інтимних ситуацій, залучення до протизаконних дій.

Якщо ж промисловим шпигунам вдалося залучити когось із службовців до роботи на себе, то цим особам вони можуть рекомендувати такі форми поведінки:

✓ не давати ніякого приводу, щоб звернути на себе увагу керівництва банку або товаришів по роботі;

✓ мати відмінну поведінку, не відмовлятися від позаурочної й додаткової роботи;

✓ утримуватися від знайомств, які б могли завдати шкоди діяльності такого службовця;

✓ не вступати в особисті і колективні конфлікти, займати нейтральну позицію в конфліктних ситуаціях.

Крім того, їм рекомендують використовувати всі обставини для подальшого просування по службі.

Звичайно, що подібні зміни у поведінці окремих працівників банку не повинні залишатися непоміченими.

Серед завдань працівникам, залученим до роботи на промислових шпигунів, можуть бути дії щодо дискредитації діяльності банку, його керівництва і провідних фахівців. Відомі факти використання промисловими шпигунами своєї агентури з

метою ураження комп'ютерними «вірусами» програмного забезпечення інших банків.

Ознаками наявності у банку агентури конкурентів може бути поява різноманітних негативних чуток, пліток між працівниками банку, анонімних листів, що надходять до служби безпеки і керівництва банку, втрата службових документів у підрозділах банку, оприлюднення або використання конкурентами інформації банку з обмеженим доступом. Як правило, залучені працівники ведуть себе більш активно, виступають як поборники прав своїх товаришів по роботі, мають найбільшу обізнаність у ситуації, прагнуть до позицій лідера в колективі.

Спостереження за конкуруючим банком, як правило, ведеться постійно, і при цьому застосовуються різні методи.

Насамперед це вивчення всіх документів і публікацій, де йдеться про конкуруючу структуру, безпосереднє спостереження за характером угод і умовами їх складання, складом клієнтів, поведінкою керівного складу і представників вищого менеджменту, повсякденною діяльністю установ банку.

Результати спостереження аналізують і систематизують, з ними складають відповідні звіти, а разом з іншими даними роблять необхідні висновки. Спостереження може здійснюватися службовцями самого банку, спеціалістами відповідних структур конкурента, підкупленими працівниками третіх осіб, у тому числі й клієнтами.

Великої шкоди завдає отримання інформації з документів. Це може бути здійснено різними методами: копіюванням таємних та конфіденційних документів, фотографуванням їх, складанням окремих витягів із документів, несанкціонованим ознайомленням з ними представників конкуруючих структур. Особливо цінна інформація може отримуватися навіть через викрадення документів. Таке здійснюється під час розробляння документів, їх переміщення (у тому числі і при пересиланні), роботи з ними посадових осіб, а також під час зберігання.

Засилання агентів до банку може відбуватися як через пряме наймання на роботу, зазвичай кваліфікованого фахівця на ключову посаду, так і через тимчасове використання працівників для виконання роботи (ремонт, обслуговування, консультації тощо). Такі люди є найбільш ефективним джерелом інформації, і їх важко викрити.

Значну зацікавленість промислових шпигунів викликають плани діяльності банку, технології отримання прибутку, система управління діяльністю банку, організація його безпеки, продукти

інтелектуальної власності.

Практика показує, що ведення недобросовісної конкуренції і промислового шпигунства не передбачає створення для цього спеціальних штатних структур. Але така діяльність з тими чи тими умовностями все ж таки має ознаки організації (керівні органи, посередницькі ланки і безпосередні виконавці). Як правило, керівництво такою діяльністю здійснюється у відповідних службах і підрозділах безпеки, маркетингу, кадрів, зв'язку з пресою та ін. У цих підрозділах плануються шпигунські дії, виробляються методи їх реалізації, обумовлюються терміни і підбираються виконавці. Тут зосереджувалась уся аналітична робота і обробка отриманої інформації.

Якщо до шпигунських дій залучаються відповідні фірми, то все керівництво такою діяльністю здійснюється останніми, а замовник формулює завдання і проводить оплату його виконання.

Посередницькими ланками є різного рівня зв'язківці, до яких надходить інформація з віддалених від головного офісу джерел.

Недобросовісна конкуренція і промислове шпигунство є невід'ємною частиною конкурентної боротьби, а з нею і всієї підприємницької діяльності. Ігнорувати їх існування і можливості настання негативних наслідків від такої діяльності в сучасних умовах немає ніяких підстав.

Розглядаючи питання про користь або шкоду недобросовісної конкуренції, і особливо промислового шпигунства, необхідно пам'ятати, що шкода для одного банку означає користь для іншого. Тому слід очікувати не зниження такої діяльності, а, навпаки, всебічного удосконалення і розвитку. Поряд з новими способами з'явиться і нова техніка промислового шпигунства, інші засоби впливу на конкурентів. У таких умовах службам безпеки слід прогнозувати шпигунську діяльність конкурентів та інших структур, визначати об'єкти їх підвищеної зацікавленості, проводити заходи попередження і нейтралізації шпигунських дій.

РЕЗЮМЕ

Взаємовідносини банків на ринку банківських послуг не завжди є доброзичливими і порядними. У багатьох випадках такі взаємовідносини мають відверто суперницький характер, із застосуванням не зовсім чесних, якщо не сказати,

негативних заходів до конкурентів. Такі дії заведено називати недобросовісною конкуренцією. Поширення недобросовісної конкуренції найбільш характерне для етапу становлення ринкових відносин, що спостерігається якраз в Україні. Негативна спрямованість недобросовісної конкуренції у взаємовідносинах банків стримує їх розвиток та зменшує можливості щодо обслуговування клієнтів, руйнує зв'язки банків і призводить до втрати ними свого іміджу та конкурентоспроможності. Нерідко акти недобросовісної конкуренції завершуються рейдерськими атаками.

Різновидом недобросовісної конкуренції є промислове шпигунство, об'єктом його посягань — банківська інформація. Під вплив промислових шпигунів потрапляють банківські працівники, які через різного роду шпигунські схеми можуть ставати на шлях зрадництва і протиправних дій. Водночас історія промислового шпигунства залишила по собі досить ознак, якими характеризується практична реалізація зазначених вище схем, знаючи які можна розпізнавати і запобігати шпигунському впливу із залучення до шпигунської діяльності.

Терміни і поняття

Види недобросовісної конкуренції
Кримінальна конкуренція
Мета недобросовісної конкуренції
Методи роботи промислових шпигунів
Недобросовісна конкуренція
Промислове шпигунство
Суб'єкти промислового шпигунства
Форми недобросовісної конкуренції

Питання для перевірки знань

1. У яких формах взаємовідносин суб'єктів ринку прояви недобросовісної конкуренції найбільш імовірні?
2. Яким вимогам має відповідати виробнича діяльність в умовах конкуренції?
3. Які дії визначаються чинним законодавством як недобросовісна конкуренція?

4. У чому полягає мета недобросовісної конкуренції в банківській сфері?

5. Які існують види та форми недобросовісної конкуренції згідно з чинним законодавством України?

6. У чому полягає відмінність між недобросовісною та кримінальною конкуренцією?

7. Хто може вести недобросовісну конкуренцію проти банку?

8. Чи можуть займатися недобросовісною конкуренцією проти банку його працівники?

9. Якими мають бути дії банку при виявленні фактів оприлюднення конкурентами негативної про нього інформації?

10. Яка відповідальність може наступи за дії, кваліфіковані як недобросовісна конкуренція?

11. У чому полягає суть промислового шпигунства?

12. Як співвідносяться недобросовісна конкуренція і промислове шпигунство?

13. На яку поведінку працівників слід звернути увагу насамперед як на таку, що може вказувати на його шпигунську діяльність?

14. Якого алгоритму дотримуються промислові шпигуни у процесі залучення працівників банку до роботи?

15. Що становить основу захисту інформації банку від посягань суб'єктів промислового шпигунства?

Завдання для індивідуальної роботи

1. Одного разу у пресі з'явилася негативна для банку, але правдива інформація. Банк не став її спростовувати або заперечувати і взагалі ніяк не відреагував на неї. Через деякий час в мережі Інтернет з'явилась електронна копія документа банку, оприлюднення якого може серйозно зашкодити репутації банку. Одночасно в інформаційному середовищі банку з'явилися чутки про відмивання власниками банку коштів, отриманих незаконним способом саме у власному банку.

Яких заходів необхідно вжити банку щодо спростування негативної інформації та протидії негативного її впливу на персонал, клієнтів та акціонерів банку?

2. Ви — керівник підрозділу безпеки банку. У зв'язку з тим, що останнім часом у банку виявлено випадки викрадення документів, програмних засобів, які використовуються в

банку, керівництвом банку було прийнято рішення про виявлення причин втрати банком документів та обставин, що сприяли цьому. Зробіть пропозиції щодо виконання зазначеного рішення.

3. Ви — керівник установи банку. Нещодавно ваш банк уклав угоду про співробітництво з однією зі страхових компаній. Дане співробітництво прогнозувалося вигідним як для банку, так і для страхової компанії. Однак через тиждень після підписання вищевказаної угоди страхова компанія зажадала розірвати цей договір, причому нічим це не мотивуючи. Окрім того, керівник підрозділу безпеки доповів вам, що існують чутки, що керівник страхової компанії отримав матеріальну винагороду за розірвання угоди з банком, а також він збирається укласти угоду про співробітництво з одним із банків-конкурентів. Як ви діятимете в такій ситуації?

Література для поглибленого вивчення

1. *Бержье Ж.* Промышленный шпионаж / Бержье Ж. — К. : НПП «Норматив», 1997. — 136 с.
2. *Гамза В. А.* Безопасность банковской деятельности / В. А. Гамза, И. Б. Ткачук. — М. : Маркет, 2010. — 408 с.
3. *Зубок М. І.* Безпека бізнесу : навчальний посібник у схемах і таблицях / Зубок М. І., Позднишев Є. В., Яременко С. М. — К. : КНЕУ, 2008. — 480 с.
4. *Ковров А. В.* Предатели: «пятая колона» в организации / Ковров А. В. — М. : Арсин, 1999. — 120 с.
5. *Ортинський В. Л.* Економічна безпека підприємств, організацій та установ : навч. посіб. / Ортинський В. Л., Керницький І. С., Живко З. Б. — К. : Правова єдність, 2009. — 544 с.

Розділ 6

ОХОРОНА І РЕЖИМ У БАНКУ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *основи організації охорони установ банків, вимоги до їх технічної укріпленості;*
- ✓ *умови і способи охорони банків, роль та обов'язки персоналу банку в забезпеченні встановленого режиму охорони;*
- ✓ *режими охорони установ банків та їх вимоги,*

*а також **уміти**:*

- ✓ *грамотно виконувати заходи охорони, передбачені відповідним режимом при здійсненні роботи в банку;*
- ✓ *захищати свої права у взаємовідносинах із суб'єктами охорони банку;*
- ✓ *забезпечувати безпечну поведінку при проведенні в банку різних режимних заходів.*

6.1. Обладнання і технічна укріпленість банків

Питання охорони банківських об'єктів завжди було актуальним, але особливо загострилося в останні роки, коли сплеск нападів на установи банків досяг значних показників. Тільки за три місяці 2009 р. зловмисники нападали на відділення банків, інкасаторські машини, банкомати та обмінні пункти аж 62

рази. За першу половину 2009 р. таких нападів було скоєно уже 109, а за весь рік — 204. Грабіжники викрали з банків біля 2 млн грн [79]. Особливої гостроти ситуація набуває через велику загрозу життю та здоров'ю людей, працівникам банків, їхнім клієнтам, іншим особам. Непоодинокими є випадки загибелі та поранення від рук нападників інкасаторів, касових працівників, охоронників банків.

Аналіз показує, що нападники об'єктом посягань переважно обирають установи, в яких велика імовірність наявності готівки — невеликі відділення, що входять до розгалуженої мережі банку, який обслуговує пенсіонерів, комунальні платежі, активно здійснює грошові перекази, або ж установи, які часто не гребують участю у конвертаційних схемах. Середній вік злочинців — 20—30 років, як правило, діють вони групами по дві—три особи, більша частина з них безробітні, дехто раніше мав проблеми із законом. Напади не бувають випадковими, як правило, злочинці вивчають місце розташування установи, внутрішнє розміщення та устаткування приміщень, систему охорони, шляхи підходу та відступу. Напад триває не більше 5 хвилин, якщо злочинці натрапляють на істотний опір з боку працівників банку, вони можуть застосовувати зброю та залишають місце злочину. Нерідко злочинці діють у змові з банківськими працівниками або ж влаштовуються самі на роботу в банк.

Розглядаючи причини активізації нападів на банки та їх пограбувань необхідно звернути увагу на таке:

- рівень охорони так званих дрібних банківських установ залишається низьким. За даними Державної служби охорони при МВС України станом на початок 2009 р. з 21000 банківських установ, зареєстрованих в Україні, 15,7 тис. не мали елементарних умов безпечної роботи своїх працівників та зберігання цінностей [146];
- небажання банкірів підвищувати рівень охорони своїх установ через незначні суми викрадених нападниками коштів порівняно з вартістю заходів охорони та сумою викрадених коштів самими працівниками банків. Фахівці банківської безпеки оцінюють витрати на поліпшення охорони одного відділення банку щонайменше в 100 тис. грн. Ураховуючи, що в Україні діє близько 21 тис. банківських установ, загальні витрати на удосконалення їх охорони можуть сягати 2 млрд грн. За таких умов банкіри передусім прагнуть до підвищення контролю за своїми працівниками й удосконалення заходів попередження шахрайства у

• негаразди соціальної ситуації, результатом яких є значна кількість людей, що залишилися без засобів проживання. Саме з цієї категорії людей вийшла більша частина грабіжників банків;

• низький рівень розкриття злочинів, пов'язаних з пограбуванням банків, більша частина злочинців залишаються не тільки непокараними, а й не знайденими.

Незважаючи на ці та інші причини, що обумовили негативні тенденції у захисті власності та коштів банків, останні мають дбати про свою охорону, удосконалювати її адекватно до тих загроз, що виникають у різні періоди банківської діяльності.

Охорону банків розуміють як комплекс організаційних та спеціальних заходів, направлених на обмеження доступу, захист території, приміщень і об'єктів банку від протиправних посягань. Реалізація заходів охорони забезпечує досягнення банком певного ступеня його безпеки.

Метою охорони є виключення можливості несанкціонованого проникнення на територію банку та викрадення (знищення, пошкодження) коштів, матеріальних цінностей чи заподіяння шкоди персоналу, створення умов для безпечної планової роботи підрозділів банку.

Охорона банків має комплексний характер і забезпечується як спеціальними заходами, так і відповідним обладнанням споруд банківських установ.

У зв'язку з цим важливою умовою ефективної охорони банків є відповідність банківських споруд і приміщень вимогам і нормам інженерного та охоронного обладнання, їх технічної укріпленості.

При будівництві, реконструкції або ремонті банківських споруд необхідно враховувати досвід забезпечення безпеки діяльності банків, стан криміногенної ситуації в регіоні й країні в цілому, вимоги нормативних документів Національного банку, Міністерства внутрішніх справ України, а також будівельних норм щодо технічного стану приміщень установ банків. Крім виконання власне інженерних технологій будівництва, що забезпечують безпеку існування самої споруди, обов'язковим є виконання певних норм щодо технічної укріпленості приміщень і споруд, обладнання їх спеціальними охоронними засобами.

Національний банк України прямо зобов'язує керівників банків забезпечити відповідність банківських приміщень вимогам, що визначені в нормативно-правових актах України та Державних будівельних нормах України (ДБН В. 2.2—9-99), а

також їх захист засобами інженерно-технічного укріплення, охоронної сигналізації, фізичної охорони [35].

Таким чином, охорона банків як комплекс заходів являє собою сукупність заходів технічної укріпленості банківських установ, що мають відповідати встановленим нормам і забезпечувати їх захист від несанкціонованого проникнення, технічної охорони, яка має забезпечити своєчасне виявлення факту несанкціонованого проникнення та фізичної охорони, яка має забезпечити припинення злочинних дій зловмисників (рис. 6.1).

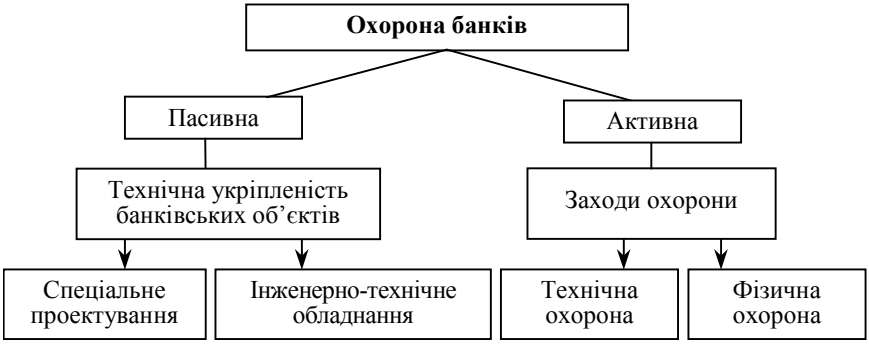

Рис. 6.1. Структура охорони банків

Основу охорони об'єктів банку становить їх технічна укріпленість, під якою розуміють: спеціальне конструювання, обладнання і оснащення споруд, приміщень і території банківських об'єктів, спрямоване на забезпечення їх захисту від несанкціонованого проникнення і злому. Основні вимоги до банківських об'єктів викладені у Положенні про вимоги щодо технічного стану та організації охорони приміщень банків України, затвердженому постановою Правління Національного банку України від 29 грудня 2007 р. №493 з наступними змінами і доповненнями. В узагальненому вигляді вимоги до технічної укріпленості об'єктів, що охороняються, можна висловити так: багаторубіжний захист об'єктів, міцність і стійкість будівель і споруд та їх комунікацій, спеціальне укріплення найбільш уразливих зон, місць і ділянок, наявність робочого, чергового та тривожного освітлення, засобів і мереж зв'язку, аварійного і резервного електроживлення, запасних виходів з об'єкта, спеціальне обладнання місць несення служби силами охорони та ін.

Надійність охорони банківських об'єктів і майна банків

забезпечується через установлення кількох рубежів захисту. Як правило, першим рубежем забезпечується захист території банку, на якій розташовані відповідні споруди, другим — захист самих споруд і третім — захист приміщень банківського офісу та цінностей, які містяться в них.

Територія банку — це відповідно обладнана ділянка місцевості з розташованими на ній спорудами, сховищами, іншими будівлями, необхідними для забезпечення його роботи. Загальний вигляд території може являти собою заблокований суцільною огорожею двір з відокремленим в'їздом. Розміщення на території двору об'єктів інших організацій, прокладання транзитних комунікаційних тунелів і прохідних каналів не допускається. Майданчик двору повинен забезпечувати маневр і розворот спеціального транспорту. По периметру огорожі двору встановлюється освітлення та інженерні засоби захисту. В окремих випадках при вході на територію банку може обладнуватися контрольно-пропускний пункт. При розташуванні банківських офісів у місцях, де неможливо виокремити ділянку місцевості для двору, територія як перший рубіж охорони банку може бути відсутня. У цьому випадку основна увагу приділяється технічному укріпленню будівлі банку та її приміщень.

Кількість входів і виходів у будівлю банку повинна бути мінімальною і відповідати протипожежним нормам. Вони мають бути розташовані у зоні спостереження охорони та забезпечувати найкоротші шляхи проходу найбільш відвідуваних приміщень банківської будівлі, а також дозволяти швидко їх блокувати охороною у разі надходження сигналу тривоги. На центральному вході, як правило, облаштовується контрольно-пропускний пункт та бюро перепусток.

Основні вимоги до обладнання центрального входу:

- усунення можливості несанкціонованого проникнення до банку сторонніх осіб;
- забезпечення зручності проходу в банк;
- відповідність естетичним нормам.

З огляду на ці вимоги основним критерієм обладнання входу має бути ефективність управління доступом до банку. Варіантами обладнання входу можуть бути:

- установлення одностулкових дверей, що обертаються, з боковими завісами. Такі двері можуть бути дерев'яними, не менше 40 мм завтовшки; додатково встановлюють ґратчасті металеві двері, що відчиняються всередину будівлі;
- установлення дверей, що обертаються, з фіксацією кута

• обладнання шлюзових входів (установка двох послідовних дверей, що обертаються або ковзають на завісах. Їх замки з'єднуються так, щоб одні двері можна було відчинити лише після того, як інші вже зачинені);

• установлення на входах «карткових» турнікетів. У даному разі документом для проходу в банк може бути індивідуальна картка співробітника.

Останнім часом широко застосовують автоматизовані системи контролю доступу. Принцип функціонування такої системи такий: кожний працівник одержує індивідуальну картку з зазначеним на ній особистим кодом, на вході встановлюють спеціальні пристрої, які зчитують інформацію з таких карток. Інформація потрапляє в систему, яка на основі аналізу даних про власника картки реагує відповідно:

• відчиняє двері та реєструє присутність власника на робочому місці;

• вмикає сигнал тривоги.

Така система дає можливість одночасно контролювати багато об'єктів, запам'ятовувати інформацію про всіх осіб, які входять чи виходять з банку, обмежувати доступ (у вихідні дні, у певний час, певних осіб), контролювати кілька зон, кілька груп відвідувачів, блокувати двері тощо.

Структура банківських приміщень та їх склад визначаються специфікою роботи установи банку і обирається за рішенням керівника банку.

Приміщення установ банків, у яких здійснюються операції з готівкою та іншими цінностями, конфіденційними відомостями, а також відомостями, які становлять банківську і комерційну таємницю, доцільно обладнувати спеціальними засобами захисту, що запобігають їх прослуховуванню, а розміщення їх у будівлі має виключати можливість спостереження сторонніми особами за роботою персоналу в цих приміщеннях.

Усі приміщення установ банків розміщуються з урахуванням забезпечення оптимальних маршрутів клієнтів і створення максимуму зручностей під час їх обслуговування. При цьому доцільно не допускати перетинання шляхів руху клієнтів і транспортування готівки та інших цінностей, а також виключати можливість спостереження клієнтами і сторонніми особами за переміщенням готівки та інших цінностей і роботою з ними персоналу банку.

Віконні прорізи приміщень перших, цокольних, підвальних поверхів банків, касового вузла, виготовлення і обробки ламінованих карт, служби захисту інформації, архівів, служби безпеки, а також тих, що прилягають до пожежних драбин, покрівель прибудов, вентиляційні канали, люки, шлюзи та інші комунікаційні прорізи та отвори розміром понад 150 × 150 мм, які прокладені в приміщення, що охороняються, захищаються від несанкціонованого проникнення.

Електроустаткування установ банків улаштовується відповідно до вимог чинних в Україні нормативних документів.

Прилади серверної, міжбанківських електронних розрахунків та електронної пошти обладнуються резервним живленням.

Аварійне живлення апаратури охоронної, охоронно-пожежної і тривожної сигналізації має забезпечувати їх роботу протягом не менше 12 годин роботи у разі відключення основних джерел електропостачання.

Внутрішні приміщення касового вузла мають бути ізольованими від інших приміщень банку і недоступними для сторонніх осіб.

Перелік необхідних приміщень касового вузла установи банку визначається керівником установи залежно від обсягу банківських операцій, що виконуються банком, і специфіки його роботи.

Сховище цінностей та його двері або сейф, що використовується банківською установою як сховище цінностей, повинні мати сертифікат відповідності Держстандарту України.

Кабіни касирів, як правило, розташовуються в єдиному блоці, зорієнтовані фронтом до касового залу, з урахуванням зручного підходу клієнтів. Ці кабіни відділяються від касового залу інженерно-технічними засобами, що забезпечують зручне обслуговування клієнтів та безпечні умови при роботі з готівкою та іншими цінностями.

Захист серверної здійснюється екрануванням приміщення, а приміщення електронного архіву — або екрануванням приміщення, або використанням електронних екранів. Такі приміщення, як правило, не мають вікон.

Для контролю наявності ознак пожежі приміщення обладнують засобами пожежної сигналізації. При цьому використовують теплові, димові, світлові і комбіновані сповіщувачі. Їх (за винятком світлових) установлюють у приміщеннях на стелі (в одному приміщенні не менше двох теплових сповіщувачів). Один тепловий сповіщувач повинен

контролювати не більше 50 м² площі.

Останнім часом велика перевага надається охоронному телебаченню. Воно приваблює тим, що дає можливість не тільки встановлювати факт порушення режиму охорони, а й контролювати обстановку у динаміці її розвитку, визначати небезпеку дій та вести приховане спостереження і здійснювати відеозапис.

Для охорони банку може бути створено одну або кілька мереж телебачення. Вони забезпечують спостереження за зовнішньою (навколо банку) і внутрішньою (в окремих приміщеннях — касових та операційних залах, приймальнях керівного складу банку, сховищах тощо) обстановкою. Монітори виводять на відповідний пост охорони, де розміщується чергова зміна охоронників. У деяких банках створюють центральний пост телевізійного спостереження, куди виводяться монітори всіх мереж охоронного телебачення. На такому посту чергує одна з груп охорони банку, працює технічна група з обслуговування і ремонту телевізійної апаратури. Пост обладнується засобами зв'язку (у тому числі і радіозв'язку) та сигналізації.

Обов'язковою складовою технічної укріпленості банку є охоронне освітлення, яке може бути двох видів: чергове і тривожне.

Чергове освітлення призначене для постійного використання у неробочий час, ввечері і вночі, навколо і в середині банку. Воно повинно мати резервне електроживлення на випадок аварії або вимкнення електромережі.

Тривожне освітлення вмикається при надходженні сигналу тривоги від засобів охоронної сигналізації. Крім цього, за сигналом тривоги додатково до освітлення можуть включатися і звукові пристрої (дзвінки, сирени тощо).

Одним із заходів технічної укріпленості банку є використання засобів фізичного захисту, до яких належать природні та штучні бар'єри, особливі конструкції периметрів, проходів, приміщень, зони безпеки.

Природні та штучні бар'єри служать для протидії несанкціонованому проникненню на територію банку. До природних бар'єрів відносяться особливе розташування установ банку. Основними штучними бар'єрами є огорожі території, де розміщується банк. Практика свідчить, що огорожі складної конфігурації можуть затримати порушника на досить тривалий час.

Особливі конструкції периметрів, проходів, приміщень,

сховищ є обов'язковими для банку з точки зору безпеки. Такі конструкції повинні протистояти будь-яким способам фізичної дії з боку злочинних елементів.

Важливим заходом технічної укріпленості банку є планування його споруд і приміщень за зонами безпеки, які враховують ступені важливості різних елементів банку з точки зору заподіяння шкоди від різних видів загроз. Оптимальне розташування зон безпеки і розміщення в них ефективних технічних засобів виявлення, відбиття і ліквідації наслідків протиправних дій становить основу інженерно-технічного захисту банку.

Зони безпеки повинні розташовуватись у банку послідовно, від огорожі навколо території банку до сховищ, створюючи ланцюг перешкод, які чергуються і які доведеться долати злочинцям. Чим складніші і надійніші перешкоди на їх шляху, тим більше часу необхідно їм для подолання кожної зони і тим більша ймовірність того, що розташовані у кожній зоні засоби охорони допоможуть виявити порушників і своєчасно подати сигнал тривоги.

6.2. Організація охорони установ банків

Охорона банків організовується відповідно до вимог існуючих правових норм, які регламентують порядок, організацію охорони та обладнання банківських установ. Основним документом в банку з охорони є Акт з організації охорони установи банку, в якому визначаються вимоги до технічного стану приміщень та обладнання їх технічними засобами охоронної сигналізації, суб'єкти, що залучаються до охорони установи банку, вид охорони та способи, а також інші питання. Зміст акту та відомості, що в ньому вказуються, мають базуватися на вимогах Положення про вимоги щодо технічного стану і організації охорони приміщень банків України, затвердженого постановою Правління Національного банку України від 29 грудня 2007 р. № 493 зі змінами, внесеними постановою Правління Національного банку України від 10 липня 2009 р. №398. Крім того, на організацію охорони банків впливатимуть положення Інструкції з організації охорони установ банків Державною службою

охорони при Міністерстві внутрішніх справ України, затвердженою наказом Міністерства внутрішніх справ України від 23 серпня 2005 р. № 700 (для випадків коли установи банків охороняються підрозділами Державної служби охорони при Міністерстві внутрішніх справ України), Ліцензійних умов провадження господарської діяльності з надання послуг, пов'язаних з охороною державної та іншої власності, надання послуг з охорони громадян, затверджені наказом Міністерства внутрішніх справ України від 01 грудня 2009 р. № 505, Постанови Кабінету Міністрів України «Про порядок продажу, придбання, реєстрації, обліку і застосування спеціальних засобів самооборони, заряджених речовинами сльозоточивої та дратівливої дії» від 07 вересня 1993 р. № 706.

В основі розроблення системи охорони банку та організації її функціонування лежить принцип створення послідовних рубежів безпеки, на яких загрози мають бути своєчасно виявлені, а їх поширенню протистоятимуть надійні перешкоди. Ефективність системи охорони банку можна оцінити тривалістю часу з моменту виникнення загрози до початку її ліквідації.

Вибір форм, методів і засобів охорони залежить від таких факторів:

- можливі способи злочинних посягань на банки;
- характеристика технічної укріпленості установ банків;
- наявність уразливих місць у технічній укріпленості установ банку;
- умови місцевості, де розташовані установи банку, їх конструктивні особливості;
- режим і характер роботи установ банку, розмір грошових і матеріальних цінностей;
- режим охорони установ банку;
- якісно-кількісні характеристики сил охорони;
- технічна оснащеність сил охорони.

Основними принципами охорони банківських об'єктів є:

- законність — усі заходи охорони мають випливати з вимог і положень нормативно-правових актів, не порушувати прав, свободи, честі і гідності громадян, не створювати загрози власності та діяльності банку;
- пасивність та активність охорони — заходи охорони повинні поєднувати дії щодо захисту об'єктів та протидії протиправним посяганням на них;
- скритність та демонстративність охорони — охорона об'єктів не може бути повністю скритою, про те, що вони

• економічна доцільність — вартість послуг охорони, утримання власних сил і засобів охорони не повинна перевищувати вартості цінностей, що охороняються;

• конкретність — заходи охорони мають бути спрямовані на захист конкретних об'єктів, цінностей, забезпечення відповідного режиму діяльності конкретної установи банку;

• безперервність — банківські об'єкти повинні завжди залишатися під охороною.

Установи банків організовують охорону власною службою охорони або залучають до охорони на договірних засадах спеціальні підрозділи Міністерства внутрішніх справ України чи юридичні особи, яким надано право на здійснення охоронної діяльності (надання охоронних послуг) згідно з чинним законодавством України. Вибір сил охорони покладається на керівника установи банку.

Для вирішення питання про прийняття банківської установи під охорону силами підрозділів МВС її керівники направляють до регіонального управління (відділу) Державної служби охорони (ДСО) лист з проханням здійснити первинне обстеження установи. На основі листа проводиться обстеження об'єктів банківської установи міжвідомчою комісією у складі представників регіонального управління (відділу) ДСО, територіального органу внутрішніх справ, підрозділу ДСО, пожежної охорони, регіонального управління відповідного банку та керівника установи банку, що обстежується. Комісія повинна визначити вид та систему охорони, заходи технічної укріпленості, оснащення засобами охоронно-пожежної сигналізації (ОПС) і тривожної сигналізації (ТС), безпеки, зв'язку тощо. За результатами обстеження складається акт. Крім того, актом оформляється прийняття в експлуатацію засобів охоронної, охоронно-пожежної і тривожної сигналізації, установлених в установі банку.

Прийняття об'єкта під охорону оформляється договором між органом охорони і банком. Одночасно з договором складається дислокація, в якій вказуються об'єкти, що підлягають охороні, час та вид охорони.

Юридичні особи, які мають право надавати послуги охорони, здійснюють прийняття установи банку під охорону за домовленістю сторін або так само, як і з підрозділами МВС.

Відповідно до використання сил та засобів охорони остання поділяється на фізичну та технічну. У свою чергу, фізична охорона здійснюється силами фізичних осіб через установлення стаціонарних постів, виділення груп для супроводження вантажів і цінностей, патрульних груп, груп охорони посадових осіб банку.

Технічна ж охорона забезпечується встановленням у визначених місцях технічних засобів охорони (ТЗО), які поділяються на засоби затримання, засоби охоронної та засоби пожежної сигналізації, засоби спостереження за територією і приміщеннями установи банку, обладнання для реєстрації внесення (винесення) заборонених матеріалів і виробів.

За рішенням керівника установи банку залежно від обсягів готівки та інших цінностей, строків їх зберігання, місця розташування установи банку, облаштування касового вузла, інших умов може обиратись один із таких видів охорони:

- цілодобова фізична охорона з підключенням відповідних технічних засобів охорони для спостереження сил охорони;
- у робочий час — фізична охорона з підключенням відповідних технічних засобів охорони для спостереження сил охорони, у неробочий час — охорона тільки за допомогою відповідних технічних засобів охорони, що підключені для спостереження сил охорони;
- цілодобова охорона тільки за допомогою відповідних технічних засобів охорони, що підключаються для спостереження сил охорони.

Обраний вид охорони є обов'язковим на час перебування відповідних обсягів готівки і цінностей у банку. Потреба у використанні відповідного виду охорони, за відсутності передбачених відповідними документами НБУ обсягів готівки та цінностей визначається керівником установ банку. При збільшені готівки та цінностей в установі банку її керівник має своєчасно вжити заходів щодо посилення охорони, технічної укріпленості приміщень установи, інших заходів для забезпечення надійного їх зберігання. Відомості про охорону банку є банківською таємницею і не підлягають розголошенню.

Керівник банку або уповноважена ним особа при організації охорони визначає:

- організацію пропускного та внутрішньооб'єктового режимів;
- місця встановлення технічних засобів охорони та їх кількість;
- технічні засоби охорони для забезпечення відповідного

- конкретні (мінімально можливі) терміни оперативного реагування сил охорони на сигнали технічних засобів охорони;
- дії працівників банку і сил охорони у разі спрацювання технічних засобів охорони, а також їх дії у непередбачених ситуаціях;
- взаємодію між різними суб'єктами охорони, якщо має місце залучення до виконання завдань охорони різних суб'єктів;
- порядок реагування касових працівників банків у разі вчинення протиправних дій, графік проведення тренувань та інструктажів з ними;
- порядок взаємодії з органами внутрішніх справ у разі нападу, злочинного посягання, спрацювання сигналізації та для інших ситуацій.

Безпосереднє виконання роботи з організації охорони банківських об'єктів покладається на керівника служби охорони або ж керівника служби безпеки банку. Досвід організації охорони банків показує, що вказані керівники у таких випадках мають дотримуватися такого алгоритму роботи: вивчення об'єктів охорони та визначення найбільш уразливих місць у їх захисті; вивчення можливих загроз банківським об'єктам; визначення мети, завдань, видів і режиму охорони об'єктів банку; визначення складу сил та засобів охорони і розроблення штатного розкладу підрозділу охорони (проведення переговорів із залученими силами охорони та обстеження банківських об'єктів міжвідомчою комісією); розроблення нормативно-правових документів з питань охорони; підбір і розстановка персоналу підрозділу охорони; визначення та планування заходів охорони; організація приймання об'єктів під охорону (підписання договору із залученими силами про охорону об'єктів); забезпечення заходів охорони та контроль їх ефективності.

У разі пожежі наряд охорони або працівники банку повідомляють про це пожежну охорону, чергового органу внутрішніх справ і управління (відділу) охорони, керівника банку і вживають заходів щодо врятування цінностей і майна.

При загоранні в грошових сховищах не дозволяється відкривати їх і порушувати цілісність печаток до прибуття посадових осіб об'єкта, відповідальних за зберігання цінностей.

Кількісний склад сил охорони на один цілодобовий пост визначають за діючою плановою нормою робочого часу працівників, які безпосередньо забезпечують охорону банку. За

специфікою роботи особовий склад сил охорони може нести службу вдень і вночі за 8-, 12-, 24-годинним графіком чергування.

Загалом діяльність сил охорони передбачає виконання трьох груп завдань:

- аналітичні, пов'язані з отриманням інформації про загрози охороні банку та джерела таких загроз, а також аналізом стану охорони банку;
- процедурно-відбивні, пов'язані з організацією охорони об'єктів установи банку, своєчасною реакцією сил охорони на виникнення загроз, відбиттям і локалізацією посягань на об'єкти охорони банку, взаємодією сил охорони з ДСО, ліквідацією наслідків посягань і відновленням режиму охорони;
- попереджувальні, пов'язані зі створенням іміджу сильного і надійного режиму охорони, своєчасним виявленням ознак підготовки посягань на об'єкти охорони, завчасним зосередженням сил і засобів охорони на загрозливих ділянках та об'єктах охорони, проведенням заходів дезінформації зловмисників.

До виконання завдань охорони можуть залучатись особи, які досягли 18-річного віку і відповідають кваліфікаційним вимогам, визначеними наказом Міністерства праці та соціальної політики України від 23 грудня 2004 р. №336 "Про затвердження Випуску 1 «Професії працівників що є загальними для всіх видів економічної діяльності»" Довідника кваліфікаційних характеристик професій працівників.

Керівник підрозділу охорони має відповідати кваліфікаційним вимогам, викладеним у Ліцензійних умовах провадження господарської діяльності з надання послуг, пов'язаних з охороною державної та іншої власності, надання послуг з охорони громадян, затверджених наказом МВС України від 01 грудня 2009 р. № 505.

Не залучаються до охоронної діяльності особи:

- які не досягли повноліття;
- які за станом здоров'я і фізичного розвитку відповідно до висновку закладу охорони здоров'я не можуть виконувати обов'язки з охорони майна та громадян;
- які перебувають на обліку в органах охорони здоров'я з приводу психічної хвороби, алкоголізму чи наркоманії;
- визнані судом недієздатними або обмежено дієздатними;
- які мають непогашену чи не зняту судимість за умисні злочини;

- яким у судовому порядку заборонено займатись охоронною діяльністю або роботою, пов'язаною з матеріальною відповідальністю;
- які не зареєстровані за місцем проживання в установленому законом порядку;
- які ухиляються від призову на строкову військову службу, військового обліку та спеціальних зборів.

З огляду на те, що персонал банку відіграє важливу роль у забезпеченні встановленого режиму охорони, на нього покладаються такі обов'язки:

✓ знати встановлений у банку режим охорони та виконувати його вимоги;

✓ забезпечувати надійне зберігання пропускних документів, нікому їх не передавати. У разі їх втрати негайно повідомити про це службу охорони банку і свого безпосереднього керівника;

✓ ретельно дотримуватися правил внутрішнього трудового розпорядку роботи, установленого в банку;

✓ надавати доступ на територію банку виключно в межах своїх повноважень;

✓ забезпечувати контроль за обладнанням та майном, яке надано в користування працівникові для забезпечення виконання його обов'язків;

✓ негайно повідомляти службу охорони про підозрілу поведінку відвідувачів, клієнтів банку чи інших осіб.

6.3. Режими охорони

Охорона несе в собі велику низку заходів обмеження. Водночас підприємництво та обмеження за своєю природою суперечливі, і мистецтво розроблення режиму охорони полягає саме в тому, щоб знайти оптимальне поєднання заходів заборони з інтересами підприємницької діяльності. Відповідно до цього охорона установ банку функціонує у вигляді встановлення відповідних її режимів: пропускного і внутрішньооб'єктового.

Пропускний режим передбачає встановлення в банку відповідного порядку допуску в банк працівників банку, його клієнтів та відвідувачів; встановлення відповідного порядку переміщення за межі банку матеріальних цінностей; обладнання периметру території банку засобами, що виключають

несанкціонований доступ; організацію бюро перепусток та контрольно-пропускного пункту, обладнання їх необхідними засобами та документами, що мають забезпечити виконання пропускного режиму; визначення переліку посадових осіб, які мають право надавати допуск до входу в банк; відповідне обладнання входу в банк (камери зберігання, гардероб, металошукачі і т. і.).

Для забезпечення функціонування пропускного режиму запроваджуються пропускні документи: посвідчення та перепустки. Перепустки бувають:

♦ *постійні* — видаються особам, які перебувають у штаті банку, працівникам охорони та особам, які обслуговують ТЗО. Строк дії таких перепусток вказується у бланку самої перепустки. Вона пред'являється без документів, що засвідчують особу, на ній має бути фотографія особи, засвідчена печаткою банку. У деяких випадках для штатних працівників установи банку видаються відповідні індивідуальні посвідчення, які також можуть використовуватись як документи на право доступу в банк;

♦ *тимчасові* — як правило, для штатних працівників на період терміну випробування, осіб, що працюють за трудовою угодою або у складі тимчасових колективів. Строк дії таких перепусток до півроку;

♦ *разові* — для всіх відвідувачів. Така перепустка одноразова і дійсна протягом робочого дня тільки на одне відвідування банку. Після завершення роботи в банку перепустку підписує особа, яка її замовляла, при цьому вказується час вибуття відвідувача, потім її здають на пропускному пункті. Черговий фіксує час вибуття відвідувача у відповідному журналі;

♦ *перепустки для клієнтів операційних підрозділів* — для представників підприємств, які обслуговуються в даній установі банку;

♦ *матеріальні* — дають право винесення (вивезення) з банку вказаних у них матеріальних цінностей.

Форма і зміст бланків перепусток виконуються друкарським способом.

Підставою для видачі разової перепустки є заявка. Як виняток, підставою може бути усне розпорядження керівника банку, його заступників, начальника служби безпеки, начальника охорони банку. В останньому разі таке розпорядження фіксується в книзі прийому відвідувачів.

У заявці на перепустку вказуються:

- прізвище, ім’я та по батькові відвідувача, його паспортні дані;
- мета відвідування банку;
- дата і час відвідування;
- дані посадової особи, яка приймає відвідувача;
- підпис особи, яка за наказом по банку має право замовляти перепустки.

Тимчасові та постійні перепустки видаються за списками, засвідченими керівниками підрозділів банку, на осіб, які наказом керівника банку призначені на посаду або виконують у банку відповідну роботу не менше як тиждень.

Вхід у приміщення установ банку за службовими посвідченнями може бути дозволено протягом робочого дня народним депутатам України, членам Уряду України та членам правління Національного банку України, фельд’єгерям вузла спецзв’язку Головного управління Держфельдслужби України, депутатам місцевих рад народних депутатів, державним уповноваженим Антимонопольного комітету України (АКУ) і представникам територіальних відділень АКУ, прокурорам. Працівники НБУ, правоохоронних органів, органів АКУ, інспектори енергонагляду, котлонагляду, працівники санітарно-епідеміологічної служби та пожежного нагляду за рішенням керівника банку можуть проходити за особистими посвідченнями за наявності відповідних приписів на перевірку установи банку.

Чергові спеціальних служб (електрики, сантехніки та ін.), що працюють по змінах, допускаються в банк за перепустками відповідно до затвердженого графіка змін.

Розмежування доступу в приміщення і на територію банку здійснюється за допомогою відповідних шифрів (кодів), що проставляються у перепустках.

Клієнти і відвідувачі проходять на територію банку, яка охороняється, за відповідними перепустками, як виняток, вони можуть проходити у супроводі відповідальної особи банку. В останньому випадку вихід їх з банку здійснюється також у супроводі відповідальної особи. Клієнти мають право проносити через пропускний пункт особисті речі індивідуального користування (кейси, портфелі, целофанові пакети, дамські сумочки і т. п.).

Час проходу на територію банку, яка охороняється, визначається правилами внутрішнього розпорядку роботи банку.

У разі виявлення осіб, які проходять у банк з неправильно оформленими, недійсними, оголошеними втраченими перепустками, такі особи та надані ними перепустки

затримуються і з ними проводить роботу служба безпеки банку.

Майно й інші предмети, які викликають підозру, можуть бути перевірені у присутності і з дозволу їх власника. У разі виявлення заборонених до внесення в банк речей або ознак, які вказують на небезпечність речей, особи — власники таких речей, підозрілі речі затримуються і передаються в службу безпеки банку. За необхідності про такі випадки повідомляють відповідні підрозділи органів МВС України.

Працівники охорони, які виконують свої обов'язки, за відповідних умов можуть затримати працівників банку та відвідувачів і здійснити їх огляд. Затримання вказаних осіб може здійснюватися лише за таких умов: особа здійснила дії, які мають ознаки злочину, особа вчиняє дії, пов'язані з несанкціонованим проникненням у банк; на одязі особи, її тілі та особистих речах є сліди скоєння крадіжки; на скоєння особою крадіжки вказує інформація технічних засобів охорони або на це вказують очевидці, особа уникає проведення охороною заходів контролю або намагається уникнути її затримання.

Огляду силами охорони банку підлягають лише особисті речі затриманої особи. При цьому представники охорони, що в даний час виконують обов'язки з охорони об'єкта, мають дотримуватися такого порядку огляду:

- ❖ запропонувати особі пред'явити особисті речі для огляду, обґрунтувавши таку пропозицію, або ж запропонувати пред'явити цінності, документи, які викрадено в банку чи які заборонено виносити за його межі;
- ❖ перевірити цінності, документи щодо їх відповідності банківській власності;
- ❖ у разі відмови про добровільне пред'явлення речей представники охорони складають акт відмови. У таких випадках огляд затриманих осіб здійснюється міліцією;
- ❖ за результатами огляду вилучаються цінності та документи щодо яких очевидною є відповідність їх банківській власності, і це підтверджується особою, у якої вилучено зазначені речі і майно. За фактом вилучення складається відповідний акт, до якого надається опис вилучених цінностей (речей) чи документів.

Переміщення матеріальних цінностей з місця їх зберігання в інші місця здійснюється в дозвільному порядку. Підставою для переміщення матеріальних цінностей є письмове розпорядження керівника установи банку матеріально відповідальній за них особі. Матеріальні цінності переміщуються у супроводі охорони. Вивезення (винесення) матеріальних цінностей за межі установи

банку здійснюється уповноваженою особою, яка отримала матеріальні цінності під звіт або в інший спосіб отримала їх у законному порядку.

Матеріальні цінності виносяться з установи банку, якщо є:

♦ особа, яка отримала матеріальні цінності під звіт, купила їх за власний рахунок або за довіреністю придбала їх для іншої особи;

♦ довіреність на отримання матеріальних цінностей, документ який посвідчує особу;

♦ накладна встановленої форми, яка підтверджує видачу (передання) матеріальних цінностей;

♦ перепустка на право вивезення (винесення) матеріальних цінностей за межі установи банку, в якій вказана назва майна, кількість місць, вид упаковки, прізвище, ім'я, по батькові особи та дата і час отримання нею майна зі складу (підрозділу установи банку).

У разі пожежі, аварії, стихійного лиха евакуація майна відбувається під контролем керівників підрозділів, персоналом установ банку або спеціально створеними евакуаційними командами за заздалегідь підготовленими описами матеріальних цінностей. Розпорядження про евакуацію матеріальних цінностей у такому разі дає керівник установи банку. Сили охорони забезпечують охорону майна в місцях їх евакуації.

Зауважимо, що перепустка на винесення матеріальних цінностей не дає права на вхід у приміщення банку або вихід із нього без перепустки встановленого зразка.

На осіб, яким необхідно працювати у вихідні та святкові дні, складається заявка для разової перепустки, де вказуються характер робіт, час їх проведення, прізвища та ініціали осіб, залучених до роботи. На основі заявки видається наказ по банку із зазначенням часу проведення робіт, зони доступу осіб, що виконуватимуть роботи, виписується разова перепустка, де вказується кількість осіб і протягом якого часу вони працюватимуть.

У разі необхідності перебування в приміщенні банку в позаробочий час складається поіменний список, де зазначаються особи, які проводитимуть роботи, час проведення робіт і зона доступу. Список підписує керівник установи банку.

Внутрішньооб'єктовий режим банку — установлений у певній установі банку порядок виконання внутрішнього розпорядку роботи, спрямований на забезпечення безпеки банківського виробництва, схоронності матеріальних цінностей та інформаційних ресурсів, захист персоналу і відвідувачів.

Внутрішньооб'єктовий режим включає:

✓ розроблення та введення в дію внутрішнього розпорядку роботи установи банку;

✓ порядок допуску працівників банку до режимних приміщень;

✓ порядок відкривання, закривання і здавання під охорону робочих приміщень;

✓ порядок видачі і зберігання ключів від робочих приміщень, металевих печаток для опечатування дверей приміщень;

✓ порядок дій працівників банку та сил охорони у разі виявлення порушень відбитків печаток, відмови роботи індивідуальних карток, втрати ключів, карток, перепусток або металевих печаток;

✓ порядок дій сил охорони і персоналу банку у позаштатних ситуаціях (при пожежах, стихійних лихах, нападі на установу банку та ін.);

✓ порядок доступу у приміщення в неробочий час, вихідні та святкові дні;

✓ обов'язки працівників банку щодо додержання вимог внутрішньооб'єктового режиму та відповідальність за його порушення.

Забезпечуючи пропускний і внутрішньооб'єктовий режим у банку, сили охорони спрямовують свої зусилля на виявлення, запобігання та припинення несанкціонованого проникнення в банк та несанкціонованого перебування осіб у банку; протиправного заволодіння майном, цінностями та документами банку або протиправного їх використання; умисного пошкодження або знищення майна, інших цінностей банку; протиправних посягань на особисту безпеку працівників та відвідувачів банку; заподіяння майнової шкоди банку через очевидні порушення техніки безпеки та належних умов зберігання майна.

У разі прямого нападу на банківські об'єкти, що охороняються, безпосередньої загрози життю та здоров'ю охоронників, які охороняють об'єкт, щодо якого скоюється напад, працівників та відвідувачів, які перебувають на об'єкті, протиправних дій щодо персоналу охорони під час виконання ним службових завдань, охоронники мають право застосовувати проти порушників заходи необхідної оборони відповідно до чинного законодавства. Відбиття нападу може здійснюватися застосуванням спеціальних засобів індивідуального захисту та активною обороною з використанням допоміжних знарядь та фізичної сили. За наявності вогнепальної зброї та службових собак охоронники за відповідних умов та в

установленому порядку можуть застосовувати їх для відбиття нападу [55].

Охорона банківських об'єктів, як правило, здійснюється стаціонарними постами, постами на контрольно-пропускних пунктах, технічними засобами охорони. Останні можуть використовуватись автономно для охорони окремих об'єктів, підсилення режиму охорони на окремих ділянках зон охорони, контролю за виконанням обов'язків охоронниками, документування подій, що відбуваються в зоні охорони, подавання сигналів тривоги у зв'язку з порушенням режиму охорони, для регулювання доступу до установи банку тощо.

За порушення встановленого в банку режиму охорони може наступи дисциплінарна відповідальність відповідно до вимог зазначеного режиму та в порядку, передбаченому Кодексом законів про працю України; адміністративна відповідальність — за порушення порядку зберігання і застосування зброї і спеціальних засобів індивідуального захисту й активної оборони; кримінальна — за невиконання або неналежне виконання обов'язків щодо охорони майна.

Резюме

Охорона банків є важливою і невід'ємною складовою забезпечення їх безпеки, спрямованою на захист та протидію загрозам посягання на матеріальні об'єкти та цінності банків. Забезпечення охорони здійснюється відповідно до вимог Національного банку України згідно з його нормативно-правовими документами.

Важливе місце в охороні банківських установ відводиться технічній укріпленості та охоронному обладнанню їх приміщень, яке має здійснюватися згідно з вимогами Державних будівельних норм.

Охорона банків здійснюється власними або залученими силами цілодобово. Режим охорони визначається відповідно до обсягів готівки і цінностей з якими здійснює операції банківська установа. Працівники банків мають строго дотримуватися вимог установленого в установах режиму охорони і безумовно виконувати його. За порушення режиму охорони може наступи дисциплінарна відповідальність.

Терміни і поняття

Внутрішньооб'єктовий режим
Мета охорони банків
Охорона банків
Перепустки
Принципи охорони банку
Пропускний режим
Сили охорони банку
Система охорони банку
Територія банку
Технічна охорона
Технічна укріпленість
Фізична охорона

Питання для перевірки знань

1. Що слід розуміти під охороною банків?
2. У чому полягає мета охорони банків?
3. Що є основою охорони об'єктів банку?
4. З якою метою застосовується чергове освітлення в банку?
5. Якими правовими нормами регламентується порядок організації охорони банків?
6. На що вказує принцип активності та пасивності охорони банків?
7. У чому полягає практична реалізація принципу демонстративності в системі охорони банку?
8. На яких засадах взаємодіють банки і ДСО при МВС України щодо здійснення охорони банків?
9. Хто встановлює правила пропускного режиму у банку?
10. Як здійснюється допуск у банк його працівників?
11. Як організовується винесення за межі банку його матеріальних цінностей?
12. Чи має право охорона банку здійснювати огляд особистих речей працівників банку?
13. Як здійснюється допуск до установи банку у вихідні та святкові дні?
14. Як регулюється допуск працівників банку до його режимних приміщень?
15. Яку відповідальність має нести працівник банку у разі втрати пропускних документів?

Завдання для індивідуальної роботи

1. Ви — один із керівників комерційного банку. Сьогодні постало питання про організацію охорони об'єктів вашої установи. Яким структурам ви надасте перевагу для охорони банку (ДСО при МВС України, охоронним підприємствам, власній охороні) якщо знаєте, що найближчим часом банк відкриватиме кілька філій та створюватиме додаткові об'єкти?

2. Ви — працівник служби охорони банку. До приміщення банку увійшов відвідувач і сказав, що він хоче зустрітися з керівником банку. На ваше запитання, чи призначалася йому така зустріч і чи замовляли йому перепустку, він відповів, що він працівник Генеральної прокуратури, йому не потрібна перепустка до банку, що згідно з чинним законодавством він має право вільного доступу до банку, тим більше, що у нього є постанова на проведення виїмки документів і він хотів би зустрітися з керівником банку. Ви не допустили даного відвідувача до приміщення банку, оскільки засумнівалися в тому, що він має право вільного доступу. Чи правильною була ваша поведінка і поведінка працівника Генеральної прокуратури в даній ситуації? Обґрунтуйте свою відповідь.

3. Ви — працівник банку. Сталося так, що ви загубили свою перепустку, але враховуючи те, що ви давно працюєте в банку і вас охорона добре знає вам деякий час вдавалося проходити до робочого місця. Але одного разу на контрольно-пропускному пункті було затримано особу, яка для проходу в банк подала вашу перепустку. Яка відповідальність може наступи для вас у зв'язку з втратою перепустки і зазначеною подією?

Література для поглибленого вивчення

1. *Бурунов Г.* Основы частной охранной деятельности / Г. Бурунов, Н.Горбачева — Запорожье : ПП «Павел», 2000. — 134 с.

2. *Захаров О. Ю.* Обеспечение комплексной безопасности предпринимательской деятельности / Захаров О. Ю. — М. : АСТ «Астрель», 2008. — 320 с.

3. *Зубок М. І.* Безпека бізнесу : навчальний посібник у схемах і

4. *Зубок М. І.* Охорона та охоронна діяльність : навч. посіб. для студ. вищ. навч. закл. / Зубок М. І. — К. : КНТЕУ, 2006. — 172 с.
5. *Курило В. І.* Правові засади охоронної діяльності : навч. посіб. / Курило В. І. — К. : Кондор, 2005. — 182 с.

Розділ 7

ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *суть, мету, та завдання інформаційної безпеки банку;*
- ✓ *умови формування інформаційних ризиків у банківській діяльності, їх види та методи управління ними;*
- ✓ *основні інформаційні загрози й негативні наслідки їх реалізації в банківській діяльності;*
- ✓ *структуру інформації банку, заходи банку щодо захисту інформації з обмеженим доступом;*
- ✓ *умови формування, функціонування та розкриття банківської таємниці в банках;*
- ✓ *заходи з протидії інформаційно-психологічному впливу в системі безпеки банку,*

*а також **уміти**:*

- ✓ *виявляти інформаційні загрози в діяльності банку та забезпечувати захист від них при виконанні своїх посадових обов'язків у банку;*
- ✓ *вживати заходів щодо управління інформаційними ризиками при проведенні банківськими підрозділами операцій та наданні послуг клієнтам банків;*
- ✓ *забезпечувати захист інформації банку з обмеженим доступом при виконанні посадових обов'язків на своєму робочому місці;*

✓ *вживати заходів щодо протидії інформаційно-психологічному впливу на банк та його персонал у процесі банківської діяльності.*

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. Будь-яка діяльність, сфера, взаємовідносини характеризуються не просто великими обсягами інформації, а такими, що у звичайному режимі її сприйняття опанувати її неможливо. Так, за останні 35 років у світі вироблено більше інформації, ніж за 5 тис. років до цього. Підраховано, що один примірник газети «Нью-Йорк Таймс» містить інформації більше, ніж її міг отримати мешканець Англії за все життя [150]. Подвоєння знань з 1900 р. здійснювалося кожні 50 років, з 1950 р. подвоєння відбувалося вже кожні 10 років, з 1970 р. — кожні п'ять років, а з 1990 р. — щорічно [17]. Більше того, інформаційні характеристики існують як об'єктивно, так і природно чи штучно викривленими, що значно доповнює обсяги інформації та вимагає обов'язкової її обробки;

❖ 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 й 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.

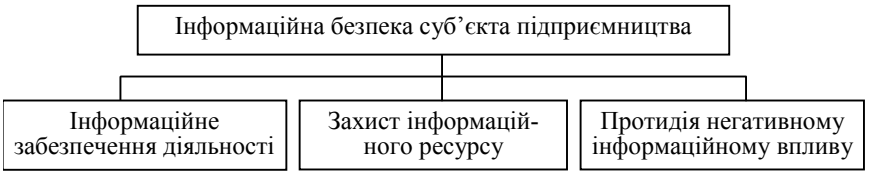

Рис. 7.1. Структура інформаційної безпеки суб'єкта підприємництва (банку)

Водночас правильний погляд на організацію інформаційної безпеки можна зробити лише з аналізу сучасних інформаційних відносин, які складаються в даному разі на ринку банківських послуг та інтересів суб'єктів цих відносин з використання інформації (рис. 7.2).

Безумовно, що у процесі цих взаємовідносин та реалізації інтересів виникають певні інформаційні ризики, інтенсивність та небезпечність яких характеризується станом самих

взаємовідносин. Скажімо, в умовах інформаційного співробітництва та взаємодії ризики будуть мінімальними і обумовлюватимуться переважно зовнішніми чинниками, що утворюються в середовищі суб'єктів, які співпрацюють чи взаємодіють. І навпаки, коли суб'єкти інформаційних взаємовідносин перебувають у стані суперництва або протиборства ці ризики зростатимуть і матимуть досить небезпечний характер.

Рис. 7.2. Інформаційні взаємовідносини суб'єктів ринку банківських послуг

7.1. Інформаційні ризики та інформаційні загрози в 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 її 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, а також 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 і 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 та 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 необгрунтоване 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 аудіозаписів) 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 зберігалась.

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. Враховуючи зазначене та те, що безпека електронної інформації банків забезпечується здебільшого своїй технічними, апаратними та програмними засобами, питання комп'ютерної безпеки банків не розглядаються в даному виданні і становлять предмет інших видань, де вони подаються більш глибоко і професійно ([1, 2] та ін.).

У 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 [1]. Крім того, до факторів, які створюють умови витоку (передання) інформації, за дослідженнями спецслужб, відносять фактори, наведені в табл. 7.1.

Таблиця 7.1

ФАКТОРИ, ЩО СТВОРЮЮТЬ УМОВИ ВИТОКУ ІНФОРМАЦІЇ

Фактор	Відсоток
1. Надмірна балакучість співробітників підприємств, фірм, банків	32
2. Прагнення працівників підприємств, фірм, банків заробляти гроші будь-яким способом і будь-якою ціною	24
3. Відсутність на підприємстві, фірмі, у банку системи заходів, направлених на захист інформації	14

Закінчення табл. 7.1

Фактор	Відсоток
4. Звичка співробітників підприємств, фірм, банків ділитись один з одним почутими новинами, чутками, інформацією	12
5. Безконтрольне використання інформаційних систем	10
6. Наявність передумов для виникнення серед співробітників конфліктних ситуацій	8

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.

7.2. 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 і 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.

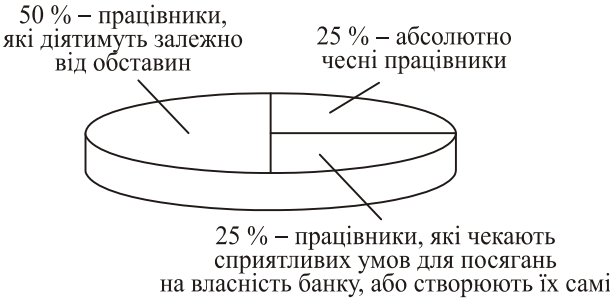

Рис. 7.3. Структура виробничих колективів за критерієм готовності до посягань на інформацію суб'єкта господарювання

Питання мінімізації ризику втрати інформації є доволі серйозним для банків, однак чи всі ризики необхідно мінімізувати, і 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 у 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 (рис. 7.4).

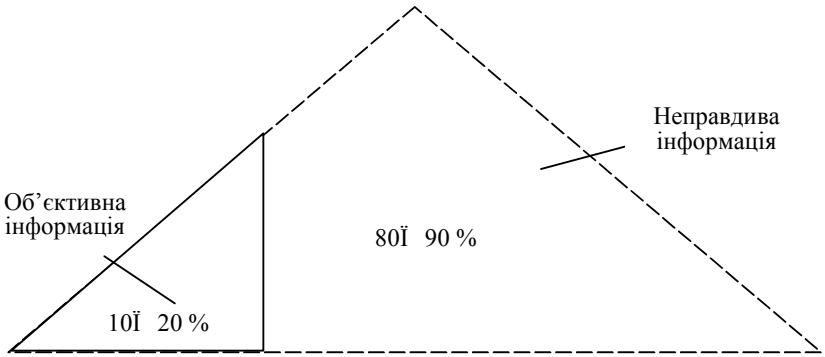

Рис. 7.4. Схема побудови дезінформаційних повідомлень в умовах загострення конфлікту

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 й 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 й 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 (рис. 7.5).

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.

Рис. 7.5. Складові інформаційного забезпечення банківських операцій

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.

У 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.

У 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.

У 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:

- періодичне поширення через різні інформаційні канали позитивної інформації про банк, оприлюднення його досягнень та активна реклама послуг;
- періодичне інформування інформаційного середовища банку, насамперед персоналу, акціонерів і клієнтів про результати роботи банку;
- формування банківського патріотизму у персоналу та акціонерів банку, пропаганда позитивного іміджу банку на ринку;
- 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.

У 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.

7.3. 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 [60]. 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).

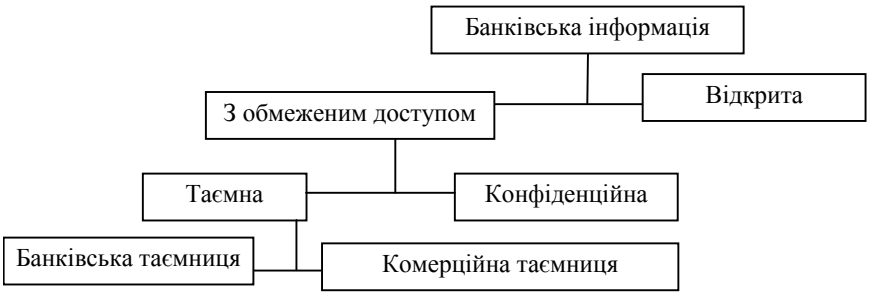

Рис. 7.6. Структура банківської інформації за режимом доступу

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 у 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.

У 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, за

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.

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

7.4. 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 і 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

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 з 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.

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.

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 її захищеності. Тому визначення ступеня вразливості інформації у 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.

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

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;

- 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 є 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

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

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:

- визначення осіб, яким надано право доступу до інформації банку в повному обсязі;
- визначення осіб, яким надано право доступу до інформації банку в частині, що їх стосується;
- установлення порядку доступу до інформації банку та повноважень осіб щодо її використання;
- визначення порядку та правил використання носіїв інформації в процесі банківської діяльності працівниками банку;
- 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

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.

З 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;

- 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

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,

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.

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

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

багатоступеневий облік усіх процедур і операцій, що проводяться з 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-

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.

У 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 її 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);

❖ 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;

— 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

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.

Терміни і поняття

Банківська таємниця
Викрадення інформації
Знищення інформації
Інформаційна безпека банку
Інформаційний вплив
Інформаційний тероризм
Інформаційні загрози
Інформаційні ризики
Інформація банку
Канали витоку інформації
Комерційна таємниця
Конфіденційна інформація
Модифікація інформації
Незаконне використання інформації
Організація спеціального діловодства
Політика безпеки
Протидія інформаційно-психологічному впливу в діяльності банку
Розголошення інформації
Система захисту інформації банку
Система управління інформаційними ризиками
Таємна інформація

Питання для перевірки знань

1. Що становить структуру інформаційної безпеки банків?
2. Як здійснюється реалізація інформаційних загроз, що виникають у інформаційних взаємовідносинах суб'єктів господарювання?

3. Що слід розуміти під поняттям «розголошення інформації»?

4. З яких елементів складається процес управління інформаційними ризиками?

5. Яких заходів треба вжити банку для зниження (мінімізації) ризику втрати ним інформації?

6. Яку інформацію банку можна віднести до банківської таємниці?

7. За яких умов банк може розкривати інформацію, яка становить банківську таємницю його клієнтів — фізичних осіб?

8. Чи має право банк надавати інформацію, що становить банківську таємницю іншим банкам?

9. У який термін надається інформація, що становить банківську або комерційну таємницю на запити підрозділів з боротьби з організованою злочинністю?

10. За яких умов здійснюється виїмка документів, які містять інформацію, що становить банківську таємницю?

11. Яка інформація банку не може становити його комерційну таємницю?

12. Хто у банку визначає належність певних відомостей до комерційної таємниці?

13. Яка відповідальність для працівників банку може настати за розголошення банківської або комерційної таємниці?

14. Що є результатом проведення службового розслідування банку у разі виявлення фактів несанкціонованого витоку інформації банку з обмеженим доступом?

15. Що включає алгоритм роботи з організації системи захисту інформації банку?

Завдання для індивідуальної роботи

1. Начальник підрозділу безпеки банківської діяльності подав на розгляд Правління банку проект Положення про комерційну таємницю банку. У процесі його вивчення у членів Правління виникли питання щодо доцільності надання статусу комерційної таємниці деяким видам інформації. Перед начальником підрозділу безпеки було поставлене запитання: якими критеріями він користувався, визначаючи відомості, що мають бути комерційної таємницею банку, якщо частка останнього на ринку банківських послуг становить понад 15%. Крім того, через банк здійснюється фінансування майже 80% державних програм у

сфері сільського господарства. Як би ви відповіли на це запитання?

2. Ви — співробітник підрозділу безпеки банку — викрили канал витоку інформації. Після доповіді начальникові підрозділу останній запропонував вам розробити заходи щодо локалізації і перекриття даного каналу. Причому ці заходи мають передбачати тільки організаційні рішення. Що потрібно буде вам зробити, щоб виконати доручення свого шефа?

3. Ви — керівник операційної бухгалтерії банку. До банку поштою надійшов запит від районного відділу Державної податкової служби, в якому запитувалась інформація про залишок коштів на рахунку одного із клієнтів банку — фізичної особи. Запит був виконаний на бланку державного органу, підписаний заступником керівника районного відділу, засвідчений печаткою, а також містив посилання на норми законів, відносно яких районний відділ Державної податкової служби мав право на отримання вказаної інформації, яка є банківською таємницею. Після розгляду запиту керівником банку, він потрапив до вас з резолюцією: «Керівникові операційної бухгалтерії. До виконання».

Яку відповідь ви надасте районному відділу Державної податкової служби?

Література для поглибленого вивчення

1. *Бєгун В. І.* Інформаційна безпека : навч. посіб. / Бегун В. І. — К. : КНЕУ, 2008. — 280 с.
2. *Гришина Н. В.* Комплексная система защиты информации на предприятии : учеб. пособ. / Гришина Н. В. — М. : ФОРУМ, 2009. — 240 с.
3. *Зубок М. І.* Інформаційна безпека : навч. посіб. для студ. вищ. навч. закл. / Зубок М. І. — К. : КНТЕУ, 2005. — 133 с.
4. Информационно-психологическая безопасность в эпоху глобализации : учеб. пособ. / Петрик В. М., Остроухов В. В., Штоквиш А. А. [и др.]; под ред. В. В. Остроухова — К. : ГУИКТ, 2008. — 544 с.
5. *Кормич Б. А.* Інформаційна безпека: організаційно-правові основи / Кормич Б. А. — К. : Кондор, 2004. — 384 с.
6. *Степанов Е. А.* Информационная безопасность и защита информации / Е. А. Степанов, И. К. Корнеев. — М. : Инфра-М, 2001. — 304 с.

7. *Шейнов В. П.* Скрытое управление человеком (психология манипулирования) / Шейнов В. П. — М. : АСТ, 2001. — 848 с.

Розділ 8

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ БАНКУ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *призначення та основні види інформаційного забезпечення діяльності банку;*
- ✓ *зміст інформаційного ресурсу банку, шляхи його формування та використання;*
- ✓ *організацію інформаційно-аналітичної роботи в банку, об'єкти та джерела інформації для забезпечення діяльності банку;*
- ✓ *основи проведення спеціальних інформаційних операцій та заходів комерційної розвідки в діяльності банку;*
- ✓ *способи збору інформації для забезпечення заходів безпеки банку,*

*а також **уміти**:*

- ✓ *у ролі спеціаліста-аналітика банківського підрозділу збирати та обробляти інформацію, готувати необхідні інформаційні документи;*
- ✓ *грамотно використовувати інформаційні ресурси банків для забезпечення його діяльності;*
- ✓ *ефективно працювати з доступними банківському працівникові джерелами інформації, формувати з них необхідні знання для якісного виконання своїх посадових обов'язків.*

Нинішню епоху без сумніву можна назвати інформаційною. Сьогодні інформація стала найдорожчим і найбільш ліквідним товаром, який дає змогу отримувати величезні прибутки тим суб'єктам, які вирвалися вперед в інформаційних перегонах. Для повнішого розуміння особливостей цих інформаційних перегонів у сьогоднішньому вимірі необхідно звернути увагу на появу і швидкий розвиток нової парадигми управління — менеджмент, заснований предусім на знаннях. Сучасна ситуація в підприємництві характеризується ускладненням комерційних схем, умов укладання угод, використанням складних комплексних продуктів, посиленням конкуренції суб'єктів ринку. Особливо це стосується ринку фінансових послуг. Сучасні банки стали потужними акціонерними структурами зі складною господарською структурою та управлінськими зв'язками. Фінансові потоки, рух капіталів, управління ресурсами і персоналом стає все більш складним завданням, що пов'язано із зростанням обсягів звітності і документообороту, збільшенням швидкості інформаційних потоків, які з використанням сучасних інформаційних технологій потребують найвищого рівня управління банківською діяльністю. Якраз потреба в такому рівні управління і формує головну проблему сьогодення в управлінській діяльності.

За сучасних умов органи управління потребують не просто знань, а конкретних і об'єктивних знань. Простого інформування вже недостатньо. Жоден з органів управління сьогодні не в змозі вести самостійно обробку всього масиву інформації, який надходить до нього, вибирати необхідні йому знання. Більше того, органи управління, як правило, не є компетентними в технологіях обробки інформації. До того ж, управлінська діяльність потребує все більшої децентралізації, залишаючи за центральними органами лише стратегічні рішення. Потоки інформації, які надходять до них мають бути скороченими і поділеними з урахуванням проміжних ланок, яким має бути делеговане право управління поточною діяльністю банку. а це, у свою чергу, потребуватиме і розподілу в інформаційному забезпеченні. Для забезпечення стратегічного управління діяльністю банку його центральні органи мають отримувати інформацію переважно прогностичного характеру, яка дає змогу оцінити варіанти рішень, планів, сценаріїв розвитку банку, реалізації майбутніх проектів, а також відстежувати тенденції змін на ринку банківських послуг.

Водночас проміжні ланки управління мають отримати інформацію, що характеризує сучасну ситуацію в банку, стан його діяльності, у тому числі і по окремих напрямах. Безумовно, ефективним такий підхід до управління діяльністю будь-якого суб'єкта, у тому числі і банку, буде за умов потужного інформаційного забезпечення. Сучасне підприємство, банк не може ефективно розвиватися, не здійснюючи інформаційного забезпечення своєї діяльності. Сьогодні головним у бізнес-процесі стає не сам капітал, а знання про те, куди його треба вкласти, щоб гарантовано отримати прибуток. Тобто сучасна ситуація в бізнес-діяльності обумовлює кілька висновків:

- для забезпечення ефективної діяльності і розвитку підприємництва поряд з фінансовими, матеріальними, кадровими конче потрібні ще й інформаційні ресурси;
- формуванням таких ресурсів мають займатися досить компетентні фахівці, професіонали в галузі інформаційних технологій і аналітичної роботи;
- робота, пов'язана з формуванням зазначених ресурсів має складати на підприємстві, у банку окремий вид їхньої діяльності. Водночас інформаційний ресурс є важливою компонентою їх економіки, важливою складовою виробничої та комерційної діяльності.

8.1. Інформаційний ресурс банку і його характеристики

Даючи характеристику інформаційному ресурсу банку, варто зазначити, що він являє собою сукупність інформації, яка перебуває у власності чи в розпорядженні банку і використовується ним для забезпечення його діяльності.

Структуру інформаційного ресурсу з точки зору його змісту становить правова інформація (нормативно-правові документи банку, інші правові документи та матеріали); комерційна інформація (характеристика ринку та його суб'єктів, умови комерційної діяльності); ділова інформація (ділові зв'язки, партнери, взаємовідносини з ними та інша інформація, яка може бути використана в ділових переговорах); інформація про персонал (відомості, що містяться в особових справах працівників); інформація про ринки (аналітичні характеристики

ринків, сфер економіки, на яких працює та планує працювати банк); інформація про сферу діяльності (технології банківського виробництва, методи забезпечення діяльності банку, плани розвитку); інші види інформації (статистична, про клієнтів, наукова, про забезпечення безпеки банку тощо).

Таким чином інформаційні ресурси як сукупність інформації мають певні особливості. На відміну від інших видів ресурсів, які існують у певній матеріальній формі, інформаційні ресурси представлені трьома категоріями: документами на паперових і електронних носіях, зразками продукції та інтелектом (знаннями) працівників банку.

Важливою особливістю інформаційних ресурсів є їх багатофункціональність, вони можуть нести освітню, аналітичну, комерційну, інформувальну, маскувальну функції та функцію впливу. Така багатофункціональність інформаційних ресурсів обумовлює різнонаправлене їх використання. Зокрема, інформаційні ресурси банку можуть використовуватись для:

- ✓ формування знань працівників банку, необхідних їм для забезпечення своєї професійної діяльності;
- ✓ створення нормативно-правових документів банку, що регулюють окремі види його діяльності та поведінку на ринку;
- ✓ формування управлінських та виробничих рішень;
- ✓ розробляння нових банківських продуктів та послуг;
- ✓ формування іміджу банку на ринку банківських послуг, забезпечення інформаційного впливу в його інформаційному середовищі;
- ✓ проведення наукових та інших досліджень, необхідних для забезпечення банківської діяльності;
- ✓ забезпечення безпеки діяльності банку, ефективного проведення банківських, господарських та інших операцій;
- ✓ проведення інформаційно-аналітичних досліджень клієнтів, партнерів, контрагентів;
- ✓ формування перспектив розвитку банку.

З огляду на важливість інформаційного ресурсу та особливу роль, яку він виконує в банку, постає питання про умови та зміст роботи з його формування. Як зазначалося вище, інформаційний ресурс є результатом роботи підприємства, банку з інформаційного забезпечення їхньої діяльності. Тобто формування інформаційного ресурсу банку має здійснюватися через проведення роботи з його інформаційного забезпечення. У свою чергу, структуру інформаційного забезпечення складають такі види інформаційної діяльності, як маркетингові

дослідження, інформаційно-аналітична робота і комерційна розвідка.

Організовуючи інформаційне забезпечення діяльності банку та формування його інформаційного ресурсу, не можна не враховувати властивості інформації, які роблять її особливим видом банківського ресурсу. Інформація є формою існування знань, за допомогою неї подаються кількісні та якісні характеристики об'єктів, подій, процесів, вона є змістом різного роду документів, ідей, інтелектуальних продуктів. Інформація є відповідним видом впливу (реклама, пропаганда, управлінські та виробничі рішення, імідж). Крім того, інформація може бути формою комерції як товар, а також одним із видів інтелектуальної зброї. Таким чином, різноманітність властивостей інформації вимагає від банку вести інформаційну роботу в різних сферах інформаційного середовища, з різними категоріями суб'єктів. Разом з тим інформація в інформаційному середовищі перебуває в диверсифікованому вигляді. Окремі інформаційні характеристики знаходяться у різних носіїв, надавались у середовище через різні канали, протягом тривалого часу, перебувають у різноманітному вигляді (відкриті повідомлення, чутки, дезінформація, витік відомостей обмеженого доступу і тощо). Досліджуючи характер існування інформації в інформаційному середовищі, науковці та фахівці-аналітики доходять висновку про наявність тенденції до збільшення відкритої інформації в характеристиках певних об'єктів, подій, процесів. Якщо раніше з відкритих джерел можна було отримати до 80% необхідної інформації, то на даний час обсяг цінної інформації, яка отримується із відкритих джерел, зріс до 95% [162]. Причинами зазначеної тенденції є стрімко зростаюча кількість користувачів мережі Інтернету і можливості оперативно подати в ній будь-яку інформацію; розвиток комп'ютерних засобів обробки та аналізу інформації; необхідність підвищення відкритості бізнес-діяльності для досягнення успіху в конкурентному змаганні.

Крім того, сьогодні досить помітна ще одна тенденція — швидке оновлення інформації в інформаційному середовищі, що унеможливлює організацію інформаційної роботи суб'єкта лише в одній якійсь формі: маркетингових досліджень, інформаційно-аналітичної роботи чи комерційної розвідки.

За таких умов організація інформаційного забезпечення діяльності мусить мати комплексний характер і здійснюватись у

різних сферах інформаційного середовища. Крім того, інформаційне забезпечення має відповідати таким вимогам:

- законності — здійснюватися в межах чинного законодавства;
- безперервності — інформаційні ресурси банку для забезпечення їх високої якості мають постійно оновлюватися;
- активності — сили, задіяні в інформаційному забезпеченні, повинні постійно прагнути до отримання інформації;
- високої технічної оснащеності — інформаційна робота банку повинна спиратися на сучасні комп'ютерні засоби та технології збору і обробки інформації;
- компетентності — особи, які виконують завдання інформаційного забезпечення банку, мають бути професіоналами у своїй галузі, здатними на високому професійному рівні виконувати свої обов'язки.

Важливе місце в досягненні ефективного інформаційного забезпечення банку займає його організація. Водночас організація інформаційного забезпечення, незважаючи на єдину мету здійснюється окремо по кожному з видів забезпечення: маркетингових досліджень, інформаційно-аналітичної роботи і комерційної роботи. Оскільки організація маркетингових досліджень не є предметом безпеки банків, основну увагу тут буде приділено інформаційно-аналітичній роботі та комерційній розвідці.

8.2. Інформаційно-аналітична робота в банку

Інформаційно-аналітичну роботу (ІАР) розуміють як діяльність, пов'язану зі збором і обробкою відкритої інформації, формуванням відповідних інформаційних документів та наданням їх керівництву суб'єкта господарювання, у даному разі банку. Тобто ІАР — це насамперед діяльність у середовищі відкритої інформації, причому діяльність, пов'язана зі збором інформації, її обробкою та формуванням відповідних інформаційних документів. Кінцевим етапом ІАР є інформування керівництва банку. Структуру ІАР подано на рис. 8.1.

Основним в організації ІАР є визначення сфер інформаційної уваги, об'єктів і джерел інформації, оскільки це дозволяє більш конкретизувати і спрямувати дану роботу, концентрувати зусилля банку на найбільш важливих її напрямах. Справа в тому,

що інформаційне середовище діяльності банку є досить глобальним, а обсяги інформації в ньому такими, що не дають можливості ефективно, з виконанням зазначених вимог здійснювати інформаційне забезпечення діяльності банку. За таких умов банки та інші суб'єкти підприємницької діяльності змушені визначати окремі сфери інформаційного середовища, з яких вони мають отримувати необхідну їм інформацію і в яких здійснювати свою інформаційну діяльність. Таким чином, сфера інформаційної уваги банку являє собою сегмент інформаційного середовища, в якому він забезпечує стратегічні, тактичні та оперативні інформаційні інтереси і завдання. З огляду на специфіку діяльності банків та структуру їх інформаційного простору сфера інформаційної уваги може включати: сферу інтересів, що може бути представлена інформацією про об'єкти, регіони, галузі економіки, до яких прагне проникнути банк у майбутньому, події, які характеризують відповідні ринки; сферу впливу, яка характеризується інформацією про події, об'єкти, що можуть впливати на поточну діяльність банку; сферу безпосередньої діяльності — інформацію про об'єкти та події, які характеризують ту чи іншу банківської операцію, що здійснюється в банку на даний час, або впливають на її проведення.

Рис. 8.1. Структура інформаційно-аналітичної роботи банку

Як правило, банки забезпечують роботу в усіх сферах інформаційної уваги і використовують інформацію: сфери інтересів — як стратегічну для прийняття рішень щодо довгострокових угод, договорів, планування перспектив розвитку банку; сфери впливу — як тактичну для прийняття рішень щодо співробітництва з партнерами, інвестування (вкладання) коштів у нові проекти, протидії недобросовісній конкуренції, визначення поведінки на ринку в той чи той проміжок часу; сфери безпосередньої інформаційної діяльності — як оперативну для прийняття рішень щодо безпосереднього здійснення конкретної операції, укладання конкретної угоди.

Основними факторами, які безпосередньо обумовлюють визначення сфер інформаційної уваги можуть бути: сфери і галузі економіки, бізнесу, в яких здійснює свою діяльність банк, плани його розвитку; стан конкуренції на ринку банківських послуг, агресивність конкурентної боротьби, наявність, види, небезпечність загроз банку; умови та особливості поточної діяльності банку; необхідність формування (підтримання)

позитивного іміджу банку в його інформаційному середовищі; інтереси банку та особливості його поведінки на ринку.

Зазвичай інформація у сферах інформаційної уваги банків, як і взагалі в інформаційному його середовищі існує не взагалі, а зосереджена в певних місцях, які заведено називати об'єктами інформації. У даному разі під об'єктом інформації доцільно розуміти установу, організацію, виробництво, захід, у яких зосереджена необхідна банку інформація. Тобто об'єктами інформації для банку можна вважати інші банки, установи засобів масової інформації, установи, організації клієнтів, контрагентів, партнерів, громадські та політичні організації, органи влади та їх установи, науково-дослідні установи, правоохоронні органи й судові установи, детективні та охоронні агентства й організації, рекламні агентства, з'їзди, конференції, виставки, презентації і т. і.

Водночас зосереджена на вказаних об'єктах інформація міститься на відповідних носіях, якими, у свою чергу, можуть бути працівники зазначених вище установ і організацій, а також самого банку, продукція засобів масової інформації, документи, рекламні продукти, аудіо- та відеоматеріали, комп'ютерна техніка й електронні носії інформації, продукція суб'єктів господарювання, виставкові експозиції, наукові, навчальні та інші видання тощо.

Таким чином, організовуючи ІАР банки мають визначатися не тільки зі сферами інформаційної уваги, а й з об'єктами інформації та її джерелами, тобто визначити, які з об'єктів і джерел мають становити для банку найбільший інтерес.

Водночас важливим залишається завдання отримання інформації. Як правило, банківські служби безпеки для отримання інформації з відкритих джерел формують так звані інформаційні канали, по яких інформація і потрапляє до банку. Під інформаційним каналом зазвичай розуміють сукупність джерел інформації засобів та методів їх подання до споживачів інформаційних продуктів. Перелік і характеристика інформаційних каналів подано на рис. 8.2.

Рис. 8.2. Інформаційні канали в ІАР банку

Ураховуючи відкритий характер інформації, яка як було вже вказано вище використовується в ІАР, інформаційні канали також мають легальний характер і формуються на добровільних засадах банку з постачальниками інформації. Серед найпоширеніших на даний час каналів отримання інформації, які використовуються банками, можна вказати такі:

- укладання договорів на інформаційне співробітництво зі спеціалізованими підприємствами, основою діяльності яких є надання інформаційних послуг;
- підписка на періодичні видання друкованих засобів інформації та організація приймання радіо- та телепередач спеціальним підрозділом банку;
- робота з персоналом банку, організація періодичного проведення соціально-психологічних досліджень в установах банку;
- створення (участь) громадських організацій і отримання інформації через громадську діяльність останніх;
- взаємообмін інформацією з іншими банками та фінансовими установами, правоохоронними та іншими органами;
- замовлення інформаційних продуктів через науково-дослідні установи, інформаційні та рекламні агентства;

- робота на ринку праці, формування «Кадрового резерву»;
- формування інституту аналітиків у банку;
- отримання інформації та експертних висновків по запитах банку від державних та інших установ і організацій;
- збір чуток.

Важливим моментом у функціонуванні інформаційних каналів є правове регулювання збору інформації. Тут слід звернути увагу на положення ст. 34 Конституції України [24], в якій зазначається, що кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір. Це право може обмежуватися на законних підставах в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання злочинам, для охорони здоров'я населення та захисту репутації або прав інших людей, для запобігання розголошенню інформації, отриманої конфіденційно, або для підтримання авторитету й неупередженості правосуддя. Право вільного збору інформації, визначене конституційною нормою, конкретизоване ст. 9 Закону України «Про інформацію» [60], в якій, зокрема, вказується: «Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного отримання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій». Тобто законодавець визнав законність дій, пов'язаних зі збором інформації, як право кожного суб'єкта держави. Водночас законність дій щодо збору інформації регламентується регулюванням доступу до певних видів інформації. Так, відповідно до ст. 29 Закону України «Про інформацію» [60] доступ до відкритої інформації забезпечується через а) систематичну публікацію її в офіційних друкованих виданнях; б) поширення її засобами масової інформації; в) безпосереднє надання її заінтересованим громадянам, юридичним особам, державним органам. Щодо останнього пункту, то безпосереднє отримання інформації може передбачати одержання позитивної відповіді на звернення, результат виконання умов договору на створення інформаційної продукції чи надання інформаційних послуг, перехід права власності на інформацію за договором, створення її самим банком.

Конкретизуючи безпосередньо право банку збирати необхідну інформацію для забезпечення його діяльності, слід звернутися до норм Закону України «Про банки і банківську діяльність» [49].

Так, відповідно до ст. 49 зазначеного закону банк зобов'язаний перевіряти кредитоспроможність позичальників та наявність забезпечення кредитів. Оскільки результати перевірки мають інформаційні характеристики, то можна розуміти, що банк зобов'язаний отримувати інформацію про позичальників, яка характеризувала б їх стан кредитоспроможності. Крім того, відповідно до положень вказаного вище закону банк має право витребувати у своїх клієнтів документи і відомості, необхідні для з'ясування їх особи, суті діяльності та фінансового стану.

Суттєвих прав щодо отримання інформації про своїх клієнтів банк набуває у разі необхідності їх ідентифікації у випадках, передбачених законодавством, яке регулює взаємовідносини у сфері запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом. Тут для підтвердження особи клієнта банк має право витребувати передбачену законодавством інформацію, яка стосується ідентифікації цієї особи та її керівників у органів державної влади, які здійснюють контроль або нагляд за діяльністю банків чи інших юридичних осіб, а також здійснювати передбачені законом заходи щодо збору інформації з інших джерел. Тобто перевірити клієнта банк може через отримання доступу до інформації про нього безпосередньо від самого клієнта, державних органів або інших юридичних осіб. Право банку як фінансової установи щодо отримання інформації з метою ідентифікації клієнтів передбачено також і Законом України «Про фінансові послуги та державне регулювання ринків фінансових послуг» [160] де вказується, що фінансова установа має право витребувати, а клієнт зобов'язаний надати документи та передбачені законодавством відомості, необхідні для з'ясування його особи.

Слід також додати, що відповідно до ст. 62 Закону України «Про банки і банківську діяльність» [49] банки мають право надавати загальну інформацію, у тому числі і таку, що становить банківську таємницю, іншим банкам в обсягах, необхідних при наданні кредитів та банківських гарантій. Тобто банк має право отримувати інформацію про клієнтів інших банків, якщо останні вступають з ним у кредитні відносини чи відносини, пов'язані з наданням клієнтам банківських гарантій.

Разом з тим право банку отримувати необхідну йому інформацію передбачено також і Законом України «Про організацію формування та обігу кредитних історій» [64]. Так, відповідно до ст. 11 даного закону банк може витребувати у кредитних бюро інформацію із кредитних історій. Однак бюро

надає інформацію, що являє собою кредитну історію, виключно тим банкам, які є учасниками бюро на підставах, передбачених зазначеним вище законом.

Характеризуючи правові засади отримання та збору необхідної банку інформації, слід звернути увагу на те, що законодавець не встановлює переліку документів чи інформації, які банк має право витребувати, але разом з тим зобов'язує суб'єктів, до яких звертається банк, надавати їх банку.

Таким чином, банк має відповідні правові підстави для збору й отримання необхідної йому інформації для формування інформаційного ресурсу і забезпечення власної діяльності. Для реалізації наданого банкам права щодо отримання та збору інформації вони розробляють відповідні методики та способи. Використовуючи наявні інформаційні канали, банки зосереджують увагу переважно на двох формах збору інформації, якими є інформаційний аудит і інформаційний моніторинг.

Інформаційний аудит — це інформаційне обстеження сфери інформаційної уваги чи певних об'єктів (об'єкта) з метою отримання, вивчення й оцінки необхідної суб'єкту аудиту (у даному разі банку) інформації. Основними технологіями інформаційного аудиту є: пошук та вивчення інформації про конкретний об'єкт безпосередньо на самому об'єкті; пошук та вивчення інформації про конкретний об'єкт через його зв'язки (ділові, комерційні, організаційні та ін.); пошук та вивчення інформації про конкретний об'єкт через спеціальне обстеження відповідної сфери інформаційної уваги банку. Зміст операцій по кожній з технологій подано в Додатку 10.

Інформаційний моніторинг — це контроль надходження інформації в інформаційне середовище, з метою виявлення важливої та цінної інформації і її використання для забезпечення діяльності банку.

Технологіями, які використовуються під час інформаційного моніторингу є: контроль інформації, яка надходить в інформаційне середовище банку за визначеними ознаками та індикаторами; контроль інформації, яка надходить в інформаційне середовище банку по визначених джерелах; суцільний контроль інформації, яка з'являється в інформаційному середовищі банку. Зміст операцій по кожній із технологій подається в Додатку 11.

Основними методами збору інформації в банку є: систематизація інформації, яка надходить у банк від його клієнтів. Взагалі банківські клієнти є досить важливим джерелом

інформації для банку. Тому ретельне вивчення інформації, наданої ними, про їх стан та діяльність, зв'язки, історію, а також аналіз їх фінансових потоків є досить важливим завданням у зборі інформації, формуванні інформаційного ресурсу банку.

Надання інформаційних запитів до відповідних установ та організацій і отримання відповіді на них є також важливим методом збору інформації, саме таким способом збирається найбільш достовірна та цінна інформація; інформаційна взаємодія банку з різними суб'єктами (як державними, так і недержавними) також дає досить позитивні результати у зборі необхідної банку інформації.

Робота з рекламними та пропагандистськими матеріалами, різного роду оголошеннями, також є одним із методів збору інформації. За рекламним оголошенням, наприклад, можна оцінити фінансове становище суб'єкта, кількість офісів і адреси їх розташування. Регіон розташування впливає на орендну плату. Якщо, скажімо, офісів два і більше, розташовані вони в різних районах міста, то можна думати, що суб'єкт розвивається досить успішно і його фінансовий стан може бути стабільним. Про фінансові можливості суб'єкта може говорити і кількість телефонів в офісі суб'єкта, чим їх більше тим пристойнішим може бути його фінансовий стан.

Періодичне опитування, що проводиться банком у своєму сегменті ринку, є також важливим методом збору інформації. Нарешті, це постійна робота з друкованими засобами інформації. Відкрита преса традиційно є найбільш ємним і популярним інформаційним каналом. Головне тут системний підхід до аналізу матеріалів преси, що, на жаль, не досить полюбляють робити служби безпеки вітчизняних банків. Водночас іноземні фахівці вказують, що якраз системний аналіз матеріалів преси дає змогу отримати практично всі необхідні їм відомості. Преса дає уявлення про ситуацію не просто в цифрах і фактах, а на зрозумілій читачеві мові, хай навіть на рівні чуток, пліток чи певного відчуття, що дає змогу зв'язати всі ці складові в цілісну картину, яка характеризує певні події, тенденції, поведінку ринку чи окремих його суб'єктів. Матеріали засобів масової інформації дають можливість зіставити, уточнити і доповнити новими відомостями інформацію, отриману з інших джерел, формувати нові напрями для поточної роботи зі збору інформації.

Інформація, яка зібрана банком у процесі формування інформаційного ресурсу, являє собою відомості, що потребують

подальшої обробки. Структура процесу аналітичної обробки інформації відображена на рис. 8.3.

У процесі накопичення інформації здійснюється формування обсягів інформації, достатніх для проведення аналітичної оцінки подій чи певних об'єктів. Обсяги інформації формуються з різних джерел незалежно від часу її виявлення та достовірності.

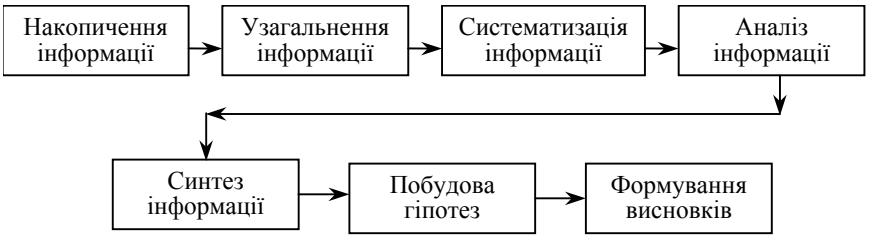

Рис. 8.3. Структура та алгоритм процесу аналітичної обробки інформації

При узагальненні інформації на основі однорідних ознак, загальних характеристик, властивостей здійснюється поєднання фактів, подій, повідомлень, формування загального поняття чи загальних положень.

Класифікація подій, фактів, об'єктів, узагальнених понять і положень, виявлення закономірності у їх виникненні, розвитку та функціонуванні — проводяться під час систематизації інформації.

У процесі аналізу інформації вивчаються події, факти по окремих елементах, виявляються зв'язки між ними. Водночас синтез інформації передбачає вивчення тих самих подій, фактів, об'єктів у їх взаємозв'язку, взаємовідносинах між собою та з іншими явищами, умовами, об'єктами.

При побудові гіпотез здійснюється формування припущень щодо причин, умов та розвитку подій, фактів, об'єктів, залежно від ситуації, що складається на ринку, та можливих рішень, які може прийняти керівництво банку.

На основі сформованих гіпотез здійснюється вироблення кінцевого підсумку обробки інформації у вигляді одного або кількох можливих варіантів, що характеризують стан ситуації (об'єкта) та перспективи її (його) розвитку.

Під час обробки інформації, яка характеризує об'єкт, що у певний спосіб може загрожувати банку, існує певний алгоритм аналітичної оцінки такого об'єкта. Спочатку визначається

існуючий (економічний, юридичний, соціальний) стан об'єкта, закономірності і тенденції його розвитку. У наступному вивчаються його можливості, потенціал, реальність та напрями загроз, які можуть надходити від нього, і далі прогнозуються наміри об'єкта, вірогідність негативних його дій стосовно банку, у тому числі за терміном, місцем і обсягом, наслідки, які можуть настати для банку в результаті реалізації зазначених загроз.

Сформовані висновки та пропозиції надаються керівництву та іншим особам у вигляді інформаційних документів. Сьогодні основними інформаційними документами є:

- інформаційні повідомлення — надання інформації, особливо важливого значення у вигляді усного чи письмового виклади;
- інформаційні доповіді — комплексний і всебічний виклад проблеми з використанням усієї наявної щодо неї інформації;
- інформаційні довідки — опис окремих характеристик конкретних подій або об'єктів;
- інформаційні огляди — опис основних інформаційних повідомлень за визначений період у формі резюме з класифікацією по рубриках;
- інформаційні зведення — опис загальної картини існуючих подій;
- інформаційні прогнози — короткий огляд подій, фактів, виклад висновків за їх наслідками і можливим розвитком ситуації з відповідним обґрунтуванням.

Аналітичні та інші матеріали, документи, що становлять інформаційний ресурс зберігаються у справах поточного та архівного зберігання. Окремі матеріали та документи зберігаються у вигляді досьє. Досьє являє собою всебічну характеристику певних об'єктів з детальним їх описом та підтверджувальним матеріалами. Як правило, досьє заводяться на найбільш важливі об'єкти (фізичні та юридичні особи), які можуть становити загрозу банку або створити йому суттєву конкуренцію.

На всі об'єкти, до яких банк має (чи мав у минулому) певний інтерес, складається картотека, де містяться загальні їх характеристики, як правило, статистичні дані.

Банки створюють електронні бази даних, куди надається інформація про різні сфери діяльності банку та його інтересів, клієнтів, партнерів, контрагентів, а також персонал. Звичайно, що й електронні бази даних, і досьє та картотеки, а також поточні та

архівні справи відповідно захищаються від несанкціонованого доступу до них.

8.3. Інформаційне супроводження діяльності банку

Формування інформаційного ресурсу є важливим але не єдиним завданням інформаційно-аналітичної роботи в банку. Не менш важливе місце посідає ще одне завдання — інформаційне супроводження діяльності банку. Однозначно, що інформаційний ресурс буде активно використовуватися для забезпечення діяльності банку, але в процесі управління, проведення банком операцій, у господарській діяльності можуть виникати ситуації, які будуть вимагати додаткової, нової інформації. Звичайно, забезпечення діяльності банку в таких ситуаціях здійснюватиметься через виконання ІАР. У таких випадках проводяться інформаційно-аналітичне дослідження нових клієнтів, контрагентів та партнерів, з якими банк планує вступити в певні взаємовідносини; інформаційно-аналітичне дослідження та контроль персоналу під час прийому працівників на роботу, у процесі роботи та при звільненні; інформаційний контроль банківських та господарських операцій; інформаційно-аналітичне забезпечення роботи щодо повернення дебіторської заборгованості; забезпечення інформаційного впливу в інформаційному середовищі банку.

Інформаційне супроводження діяльності банку потребує оперативної реакції служби безпеки та її інформаційних підрозділів на події, що відбуваються навколо банку, зміни поведінки окремих його клієнтів, контрагентів і партнерів, а в деяких випадках і працівників. Звичайно, у таких умовах необхідна об'єктивна інформація насамперед про суб'єктів зазначених подій, причому така, яку можна швидко зібрати. Тут можна було б скористатись інформацією з єдиного державного реєстру та послугами інформаційних агентств.

Останнім часом було прийнято ряд нормативних документів, які зробили більш доступною інформацію з єдиного державного реєстру.

Сьогодні в Україні існують такі Державні реєстри, з яких суб'єкт господарювання за відповідною процедурою може отримати необхідну йому інформацію:

1. Єдиний державний реєстр виконавчих проваджень (Положення про Єдиний державний реєстр виконавчих проваджень затверджене наказом Міністерства юстиції від 20 травня 2003 р. № 43/5). Відповідно до п. 5.1 Положення кожна фізична та юридична особа має право доступу до відомостей про торги та майно, що реалізується. Пошук інформації про майно, що реалізується, здійснюється за такими реквізитами: вид майна, що реалізується; поштова адреса (місцезнаходження) рухомого майна; початкова ціна продажу; населений пункт, у якому проводяться торги; найменування організації, яка проводить торги. Пунктом 6.1 Положення передбачено, що інформація з Єдиного реєстру про наявність виконавчих проваджень (у тому числі завершених) відносно боржників — юридичних осіб та фізичних осіб — підприємців надається у вигляді скорочених витягів у паперовій або електронній формі на запити будь-яких фізичних та юридичних осіб. Таким чином, подавши запит установленого зразка, банк має змогу отримати інформацію про відкриті виконавчі провадження як щодо самого банку, так і стосовно його клієнтів, контрагентів чи партнерів, про які з різних причин банку могло бути невідомо.

2. Єдиний реєстр довіреностей (Положення про Єдиний реєстр довіреностей затверджене наказом Міністерства юстиції України від 28 грудня 2006 р. № 111/5); Пунктом 3.2 Положення передбачено, що скорочені витяги з реєстру надаються на письмовий запит будь-якої фізичної чи юридичної особи. Відповідно до п. 3.1.1 Положення скорочений витяг містить таку інформацію: реєстраційний номер і дату реєстрації довіреності (її дубліката) в Єдиному реєстрі; номери та серії спеціальних бланків нотаріальних документів, на яких викладено текст довіреності (її дубліката) — для довіреностей, посвідчених у нотаріальному порядку; дату посвідчення довіреності (дата видачі її дубліката); строк дії довіреності; номер запису в реєстрі для реєстрації нотаріальних дій, за яким посвідчено довіреність (видано дублікат довіреності); відомості про посвідчення довіреності в порядку передоручення або відомості про припинення дії довіреності. Крім цього, перевірити бланки документів, складених нотаріально, можна за такою Інтернет-адресою:
http:rnb.informjust.ua/pages/default.aspx.

3. Єдиний реєстр заборон відчуження об’єктів нерухомого майна (Положення про Єдиний реєстр затверджене наказом Міністерства юстиції України від 9 червня 1999 р. № 31/5).

4. Реєстр прав власності на нерухоме майно (Тимчасове положення затверджене наказом Міністерства юстиції України від 7 лютого 2002 р. № 7/5). Відповідно до п. 5.1.1, п. 5.1.2 Положення право на отримання витягу та інформації з Реєстру прав мають: власник (власники), його спадкоємці та правонаступники юридичних осіб, уповноважені особи; суд, органи внутрішніх справ, органи прокуратури, органи державної податкової служби, державні виконавці, нотаріуси, органи Служби безпеки України та інші органи державної влади (посадові особи), якщо запит зроблено у зв'язку із здійсненням ними повноважень, визначених чинним законодавством України. Витяг із зазначеного Реєстру містить таку інформацію: реєстраційний номер нерухомого майна; адресу (місцезнаходження) нерухомого майна; підстави виникнення чи припинення права власності; відомості про власника (власників); форму власності; вид і розмір часток спільної власності; опис нерухомого майна (розміри земельної ділянки, на якій розташований об'єкт; найменування будівель, споруд та їх літеровка; призначення майна; матеріали стін кожної будівлі та споруди; розмір житлової та нежитлової площі; процент зношеності тощо); вартість (вартість будівель і споруд за даними інвентаризації, у тому числі й самочинно збудованих, прибудованих чи реконструйованих, з урахуванням фізичного зносу та діючої індексації); особливі позначки реєстратора (дані, у разі їх наявності, про самочинно збудовані, прибудовані чи реконструйовані об'єкти, про накладення арешту та/або заборони, про перебування майна у податковій заставі тощо); термін чинності; дату видачі витягу з Реєстру прав; прізвище,

Інформацією з даного реєстру банк може контролювати відповідність балансових даних про його нерухоме майно правовим підставам щодо володіння ним.

5. Державний реєстр іпотек (Тимчасовий порядок затверджений Постановою КМУ від 31 березня 2004 р. № 410). Відповідно до п. 29 зазначеного Порядку будь-яка фізична чи юридична особа має право отримати витяг з нього. Для цього подається запит про наявність або відсутність запису в Реєстрі про обтяження і зміну умов обтяження нерухомого майна іпотекою, відступлення прав за іпотечним договором, передання, видачу дубліката заставної та видачу нової заставної, видачу витягу про державну реєстрацію обтяження майна іпотекою. У витягу із зазначеного реєстру міститься така інформація: дата реєстрації обтяження майна іпотекою; порядковий номер запису; відомості про іпотекодавця (майнового поручителя), іпотекодержателя, а також боржника за основним зобов'язанням, якщо він не є іпотекодавцем; відомості про відступлення прав за іпотечним договором; опис предмета іпотеки, достатній для його ідентифікації, та/або його реєстраційні дані; розмір основного зобов'язання; строк виконання основного зобов'язання в повному обсязі; посилання на випуск заставної або її відсутність, у разі реєстрації заставної — реквізити заставної; відмітка про те, що іпотека є наступною; підстава внесення запису до Реєстру (іпотечний договір чи рішення суду); відомості про реєстратора. Ця інформація вкрай необхідна банку, особливо в операціях іпотечного кредитування.

6. Державний реєстр правочинів (Тимчасовий порядок затверджений постановою Кабінету Міністрів України від 26 травня 2004 р. № 671). Пунктом 18 зазначеного порядку передбачено, що витяг із реєстру видається на запит сторін правочину або уповноважених ними осіб. У п. 11 зазначається, що витяг містить таку інформацію: порядковий номер запису та дата державної реєстрації; відомості про сторін правочину; опис нерухомого майна, щодо якого вчиняється правочин, достатній для його ідентифікації, та/або його реєстраційні дані; строк дії правочину; відомості про нотаріальне посвідчення правочину; відомості про реєстратора.

7. Державний реєстр обтяжень рухомого майна (Порядок затверджено постановою Кабінету Міністрів України від 5 липня 2004 р. № 830). Пунктом 28 зазначеного Порядку передбачено,

8. Єдиний державний реєстр судових рішень (Порядок затверджено постановою Кабінету Міністрів України від 25 травня 2006 р. № 740). Відповідно до п. 20 зазначеного Порядку доступ до реєстру судових рішень здійснюється безоплатно через офіційний веб-портал Державної судової адміністрації. Користувачам Реєстру надається можливість пошуку, перегляду, роздрукування електронних копій судових рішень, копіювання їх текстів у цілому або частин відповідно до режиму доступу до судових рішень, унесених до Реєстру за останніх п'ять років. Порядок надання інформації за попередній період визначається держателем реєстру. Доступ здійснюється за такою Інтернет адресою: http:rnb.informjust.ua/pages/default.aspx.

З огляду на існування в Україні інформаційного ринку, необхідну інформацію можна отримати насамперед у суб'єктів такого ринку. Значним обсягом необхідної банку інформації можуть володіти інформаційні агентства. Наприклад, інформаційне агентство УНІАН надає такі інформаційні послуги:

УНІАН-Анонс — анонси найважливіших подій, які відбуватимуться найближчими днями. Виходить двічі на день. У понеділок та четвер виходить основний випуск (з повідомленнями про події наступних трьох—чотирьох днів) українською та російською мовами (о 16-й та о 19-й годині), додаткові випуски (про події наступного дня). У п'яницю і суботу — один раз на день о 18-й годині;

УНІАН-Бізнес-On-line — оперативні економічні новини у режимі реального часу. Виходять п'ять днів на тиждень російською мовою. Загальний обсяг — до 100 повідомлень у день;

УНІАН-Бізнес — економічні новини за тиждень та коментарі до них, аналітичні статті. Виходить щосуботи, російською мовою, обсяг — від 25 сторінок;

УНІАН-Зв'язок — інформаційні повідомлення про найважливіші події в галузі зв'язку, інформатики та технологій, які відбулися в Україні протягом тижня. Коментарі, аналітичні статті, офіційні документи (рішення уряду та парламенту), новини іноземних компаній. Виходить російською мовою у вівторок — 2 випуски, обсяг — до 200 сторінок на тиждень та ін.

Інформаційні послуги надаються агентством УНІАН на платній основі.

Інформаційне агентство «Інтерфакс-Україна» — компанія в структурі міжнародної інформаційної групи Interfax Information Services — працює на ринку політичної та економічної інформації України з 1992 р. Серед інформаційних продуктів, що надаються інформаційним агентством є такі:

Ефір-Україна — є оригінальною інформаційно-аналітичною системою, розрахованою на широке коло користувачів, які цікавляться станом світової економіки, фінансів і ринків України, Росії та країн СНД. Її структура включає розділи загальнополітичної, економічної, біржової та аналітичної інформації, які можуть цікавити банки і фінансово-інвестиційні організації, аналітичні служби, трейдерів, інвесторів.

Користувачі системи можуть одночасно отримувати інформацію про хід торгів у ПФТС, на ММВБ, МФБ, РТС, СПВБ і ФБСП; котирування з брокерських майданчиків, міжнародну фінансову інформацію (Standart & Poor's), новини та інформаційно-аналітичні матеріали, фондові індекси в режимі реального часу. Котирувальна інформація включає котирування першого і другого порядків, архів за кілька років. Аналітичний модуль дає можливість виконати графічний і технічний аналіз.

Крім того, отримання необхідної інформації під час інформаційного супроводження діяльності банку може здійснюватися від різного роду консалтингових та інших підприємств, які надають інформаційні послуги, а також за рахунок діяльності власних сил безпеки і їх інформаційних підрозділів.

8.4. Спеціальні інформаційні операції та комерційна розвідка в діяльності банків

Важливим завданням інформаційної роботи банку в сучасних

умовах є забезпечення впливу на його інформаційне середовище з метою формування позитивного іміджу банку на ринку, маскування роботи з розроблення нових банківських продуктів та дезінформації конкурентів чи кримінальних елементів у разі реального існування загроз від них. Забезпечення інформаційного впливу здійснюється проведенням спеціальних інформаційних операцій.

Під спеціальними інформаційними операціями, які проводить банк, розуміють комплекс спеціальних інформаційних заходів, які проводяться протягом конкретно визначеного часу в інформаційному середовищі банку з метою формування (підтримання, відновлення) його позитивного іміджу, захисту від негативного інформаційного впливу та дезорієнтації конкурентів і кримінальних елементів, які є суб'єктами загроз банку. Тобто спеціальні інформаційні операції можуть проводитися банком для забезпечення вигідного впливу на політику органів влади (насамперед Національного банку України) у разі необхідності вирішення важливих для банку завдань; формування сприятливої громадської думки про банк, його керівництво і персонал; зміцнення (підвищення, відновлення) авторитету банку і довіри до нього з боку партнерів і клієнтів; стратегічної і тактичної дезінформації конкурентів, опонентів та інших суб'єктів, від яких можуть надходити (надходять) загрози банку.

Основною відмітною особливістю інформаційних операцій є надання інформації в інформаційне середовище через концентрацію різноманітних інформаційних заходів із використанням багатьох інформаційних каналів протягом конкретно визначеного часу.

Видами спеціальних інформаційних операцій є:

✓ пропаганда — активне поширення в інформаційному середовищі інформації про досягнення, переваги, масштаби діяльності банку, вигідність взаємовідносин з ним по різних напрямах його діяльності. Особливістю сьогодення є пропаганда не установи банку, а так званого бренду банку, його комерційного найменування. Тобто пропагується певна ідеологія поведінки на ринку, з чим якраз і пов'язується високий результат. У пропаганді використовуються пропагандистські та агітаційні матеріали: листівки, буклети, відеоматеріали, публікації ЗМІ і т. п.;

✓ контрпропаганда — інформаційна реакція банку на комунікативні дії конкурентів чи інших суб'єктів, якими вони

✓ дезінформація — поширення в інформаційному середовищі викривлених або неправдивих відомостей з метою введення в оману конкурентів, кримінальних елементів, інших суб'єктів, що загрожують банку, стосовно істинних намірів діяльності банку. Захист інтересів банку за допомогою актів дезінформації може здійснюватися по різних напрямах, залежно від особливостей ситуації, в якій у той чи той період своєї діяльності перебуває банк. Зокрема, такими напрямами можуть бути:

- введення в оману конкурентів стосовно термінів проведення банком заходів щодо підвищення своєї конкурентоспроможності, подання на ринок нових послуг, проведення реорганізації банку і т. п.;
- створення ілюзії підготовки до крупномасштабних інвестицій банку в певні сфери економіки чи регіони або конкретних суб'єктів;
- широке висвітлення «проблем» банку в окремих сферах його діяльності, критика низької якості банківських продуктів;
- «витік» спеціально занижених чи завищених економічних чи інших показників діяльності банку, перебільшення чи зниження негативного впливу політичних, соціальних, економічних або інших умов на перспективи розвитку певних напрямів банківської діяльності.

Зміст дезінформуючої інформації завжди базується на певній частині правдивих відомостей, дійсних подіях та фактах. Водночас зазначені об'єктивні відомості доповнюються інформацією, яка може не відповідати дійсності, але бути на певний час досить актуальною;

✓ чутки — усна інформація з невизначеним ступенем достовірності, що стихійно поширюється в інформаційному середовищі банку з метою захисту його інтересів. Чутки є неформальним каналом комунікації, по якому можна отримати до 80% інформації, яка в принципі не буде суттєво суперечити об'єктивній ситуації [89]. Оскільки чутками інформація передається значно швидше, ніж каналами формального спілкування банк може формувати необхідні йому чутки для запланованого поширення в інформаційне середовище необхідних йому відомостей. Отримуючи зворотну реакцію на чутки, банк може коригувати свою діяльність, плани та поведінку на ринку банківських послуг. А враховуючи, що чутки є більш впливовою інформацією, банк може використовувати їх для:

• формування і підтримки іміджу банку на ринку банківських послуг;

• прикриття проникнення банку в нові регіони чи сфери економіки, розроблення нових банківських продуктів;

• уведення в оману суб'єктів загроз банку;

• захисту від негативного впливу чужих чуток, які ганьблять банк;

• підготовки суб'єктів ринку до відповідних дій банку;

• зниження напруженості в банківських колективах, середовищі клієнтів та акціонерів;

• забезпечення впливу на клієнтів банку, просування на ринок нових банківських продуктів;

• отримання незалежної думки певних груп громадян про діяльність банку та якість його послуг;

• вивчення настрою в колективах підрозділів та установ банку;

• привернення уваги до відповідної події, ситуації на ринку банківських послуг чи в діяльності банку;

• протидії певному інформаційному повідомленню, яке невигідне банку.

Звичайно, такий значний обсяг діяльності, який покладено на ІАР, потребує відповідних сил та засобів. За іноземним та вітчизняним досвідом ІАР, пов'язана із забезпеченням безпеки банку, покладається безпосередньо на підрозділи банківської безпеки. Водночас зазначені підрозділи створюють у своїй структурі спеціальні сили та засоби, функціями яких, з одного боку, є безпосереднє здійснення заходів ІАР, а з другого — координація її у структурах банку. Банки, служби безпеки яких приділяють значну увагу ІАР організовують її у такий спосіб. Відповідно до нормативно-правових документів банку в структурі банківських підрозділів створюються інститут спеціалістів-аналітиків (економіст-аналітик, інженер-аналітик, юрисконсульт-аналітик і т. п.), основним завданням яких є аналіз інформації, що функціонує у підрозділах, та надання його результатів безпосереднім керівникам і в службу безпеки банку. Зокрема до їх обов'язків входять:

❖ аналіз ефективності технологій банківського виробництва, що використовуються у підрозділі;

❖ аналітична оцінка клієнтів, їх можливостей, характеру та перспектив відносин з ними за напрямом діяльності, який забезпечує підрозділ;

❖ інформаційно-аналітичне дослідження ринку банківських послуг у сегменті, який обслуговує підрозділ;

❖ аналіз результатів діяльності підрозділу за певний період, виявлення факторів, які негативно чи позитивно впливають на такі результати;

❖ пропозиції по оптимізації форм і методів діяльності підрозділу відповідно до умов, що складаються в банківській діяльності в той чи інший період.

Виконання заходів, що стосуються отримання інформації із зовнішніх джерел, інформаційного супроводження діяльності банку на стратегічному рівні та пов'язані із проведенням спеціальних інформаційних операцій, покладається на підрозділ інформаційно-аналітичної роботи служби безпеки банку.

На даний час багато розмов точиться навколо розвідувальної діяльності в бізнесі. Можна чути про конкурентну, ділову, економічну, комерційну розвідку, бізнес-розвідку, промислове шпигунство і т. п. Разом з тим усі ці романтичні та інтригуючі назви по суті розкривають одну й ту саму діяльність — отримання необхідної для діяльності суб'єктів господарювання інформації з джерел, доступ до яких обмежений. Професіонали знають, що коли застосовується поняття «розвідка», то це означає, що така діяльність не обмежується роботою з відкритими джерелами інформації. Тому натяки деяких авторів на те, що шпигунство ґрунтується на незаконних методах добування інформації, а розвідка — на законних, м'яко кажучи, є не зовсім об'єктивним розумінням даного питання. Усім давно відомо, що діяльність сил розвідки будь-якого походження спрямовується насамперед на здобування певних таємниць, стосовно яких їх власники вживають заходів захисту. Порушення таких заходів чи оминання їх вже буде неправомірними.

У деяких країнах законодавство щодо захисту інформації є недосконалим (у тому числі й в Україні), і професійні розвідники знаходять шляхи отримання таємної інформації насамперед через прогалини в правових нормах із захисту інформації та в організації захисту своїх таємниць їх власниками. Основною ж особливістю розвідувальної діяльності є не стільки незаконність її дій щодо проникнення до інформації з обмеженим доступом, скільки таємний її характер. Саме таємничість форм, методів, взаємовідносин, що встановлюються під час отримання інформації, невідомість конкретних суб'єктів, задіяних у розвідувальній діяльності, а то й самого факту такої діяльності робить розвідку Розвідкою. Інформація ж, яку отримують банки в результаті розвідувальних дій, має здебільшого комерційний

характер і використовується насамперед для забезпечення їх комерційної діяльності. Основним змістом цієї інформації є характеристика ділових стосунків об'єктів інформації, конкурентів, інших суб'єктів, їх поведінка на ринку, наміри в комерційній діяльності.

У зв'язку з цим автори вважають, що розвідувальні дії суб'єктів підприємництва, насамперед пов'язані із забезпеченням їхньої комерційної діяльності (що і є предметом підприємництва), тому таким діям більш притаманна назва «комерційна розвідка». А оскільки, як показує практика, такі дії мають місце у вітчизняному бізнесі, у тому числі і в банках, автори вважають доцільним розглянути деякі аспекти розвідувального забезпечення діяльності банків. Тут слід звернути увагу на те, що до розвідувальних дій вдаються лише великі банки, оскільки їхні можливості дають змогу забезпечити таку діяльність як професійно та матеріально, так і з правової точки зору.

Як правило, діяльність сил розвідки таких банків спрямовються на виконання стратегічних завдань, необхідних для забезпечення їх розвитку. Сучасні методи розвідки активно використовують переваги банків як суб'єктів вітчизняної економіки, насамперед з т. з. доступу до інформації, можливості різних громадських та політичних організацій, у тому числі й ті, що створені ними самими, фонди та інші неурядові організації. Через такі організації, а в деяких випадках і безпосередньо банками фінансується діяльність певних структур, зайнятих у науковій діяльності, виробленні та обґрунтуванні перспектив розвитку галузей економіки. Крім фінансування банки через зазначені організації беруть участь у цій роботі, впливають на її хід та зміст виходячи з власних інтересів. Такий підхід дає змогу банкам не тільки отримувати необхідну їм стратегічну інформацію, а й розширювати сферу свого впливу та реалізації власних інтересів аж до політичних аспектів. Причому такий підхід дає змогу банкам утримувати свою позицію на ринку незалежно від зміни економічної та політичної ситуації в країні.

У цьому самому напрямі діють банки, формуючи в певних політичних чи інших організаціях так званий інститут агентів впливу. Проводячи відповідні заходи організаційного, фінансового та інформаційного характеру, банки спрямовують на ключові посади в зазначені організації своїх представників, які за тим реалізують політику та інтереси банків безпосередньо в цих організаціях, а через них і в інших структурах та сферах.

Що ж до дій розвідки, пов'язаних з отриманням інформації з обмеженим доступом, то відповідно до чинного законодавства така інформація може бути отримана лише з дозволу її власника. Тобто силам розвідки необхідно провести роботи з власником, розпорядником чи принаймні володільцем такої інформації. В арсеналі розвідки достатньо методів формування позитивних для неї відносин з подібними суб'єктами і, як показує практика, силам розвідки доволі часто вдається отримати доступ до інформації, яка їх цікавить саме через зазначених суб'єктів.

Слід також звернути увагу і на норми чинного законодавства, які визначають умови доступу до інформації, що є конфіденційною чи таємною. Так, згідно зі ст. 162 Господарського кодексу України [4] особа, яка самостійно і добросовісно одержала інформацію, що є комерційною таємницею, має право використовувати цю інформацію на свій розсуд. Тлумачення поняття «самостійно» подається українськими словниками як — здійснення своїми силами, з власної ініціативи, без сторонньої допомоги [83]. Таке розуміння зазначеного поняття означає, що право збирати інформацію, яка є комерційною таємницею, можливе тільки за умов, передбачених ст. 162 Господарського Кодексу України [4], наприклад, у разі, коли інформація отримана у зв'язку з якимось недоглядом власника інформації. До речі, однією з ознак належності інформації до комерційної таємниці є вжиття до неї заходів захисту, одним з яких є запровадження спеціального діловодства. Як показує досвід, сучасні суб'єкти господарювання, власники інформації з обмеженим доступом проводять заходи спеціального діловодства лише за рідкісним винятком. Тому дії комерційної розвідки, щодо отримання інформації з обмеженим доступом у таких суб'єктів будуть правомірними, оскільки їх інформація не набула ознак таємності. Але за всіх умов подібні дії є досить ризикованими і потребують серйозного професіоналізму та глибоких правових знань.

Важливе місце у ІАР займає інформування керівництва та працівників банку. Як показує досвід, така робота організовується в порядку, наведеному на рис. 8.4.

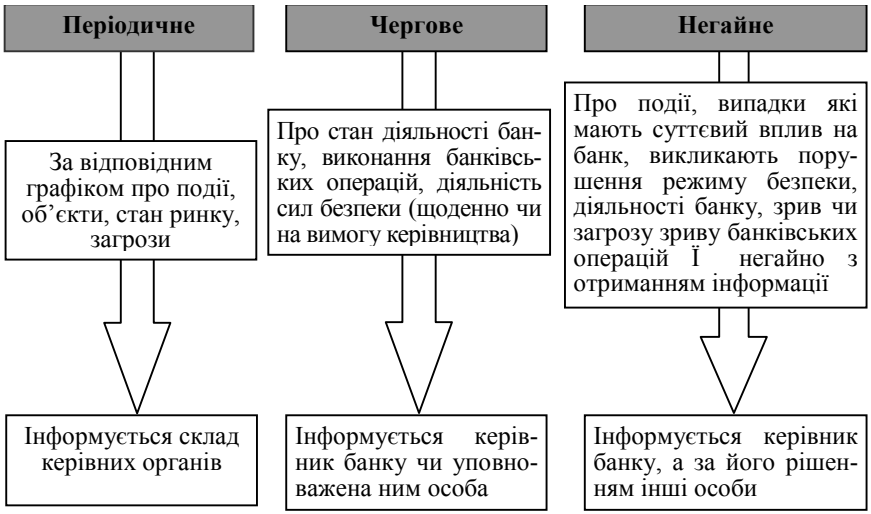

Рис. 8.4. Порядок інформування керівництва та персоналу банку

Основними вимогами до процедури інформування є: відповідність потребам осіб, яким надається інформація, конкретність, обґрунтованість і достовірність, своєчасність, зручна форма і зрозумілість інформації.

Для того щоб інформація, яка надається певним особам у процесі інформування, була переконливою і спонукала їх до прийняття необхідних рішень, доцільно дотримуватися таких порад:

♦ висвітлення в матеріалах інформування небезпек і загроз має поєднуватися з негативними наслідками, які можуть настати для банку у разі їх реалізації;

♦ у разі реальної загрози показники, що характеризують захисні функції банку, подаються такими, що не можуть гарантувати його захист при реалізації зазначених небезпек і загроз;

♦ обґрунтування можливих шляхів, термінів та умов реалізації небезпек і загроз щодо діяльності банку;

♦ розрахунок обсягів утрат, шкоди, яких може бути завдано банку від реалізації небезпек і загроз;

♦ надання інформації про можливі способи, шляхи, заходи, застосування яких сприятиме мінімізації небезпек і загроз з обґрунтуванням можливого розвитку ситуації;

♦ обґрунтування результатів від вжиття запропонованих заходів, використання шляхів і способів мінімізації небезпек і

Таким чином, інформаційне забезпечення діяльності банку є важливою умовою отримання ним позитивного результату, суттєвим елементом його безпеки та головною підставою високого статусу банку на ринку. Водночас інформаційне забезпечення є досить складним, трудомістким видом діяльності, який вимагає до себе постійної уваги.

Резюме

Інформаційне забезпечення — необхідна умова будь-якої діяльності в ринкових умовах, воно спрямоване на мінімізацію ризику втрат банку від недостатності знань при прийнятті рішень щодо здійснення певної діяльності чи проведення банківської операції. Основу інформаційного забезпечення становить формування інформаційного ресурсу банку. Цей процес здійснюється у формі інформаційно-аналітичної роботи, організація якої покладається на підрозділ безпеки. Інформаційно-аналітична робота виконується кожним підрозділом банку, а її результати зосереджуються і опрацьовуються підрозділом безпеки. Інформування зацікавлених осіб здійснюється через виконання і надання їм відповідних інформаційних документів.

Забезпечення впливу банку на його інформаційне середовище здійснюється проведенням спеціальних інформаційних операцій: пропаганда, контрпропаганда, дезінформація, чутки.

Важливе місце в інформаційному забезпеченні банку надається комерційній розвідці, яка спрямовує свої зусилля на добування інформації спеціальними заходами, переважно конфіденційного характеру.

Терміни і поняття

Дезінформація
Інформаційне супроводження діяльності банку
Інформаційний аудит
Інформаційний моніторинг
Інформаційний ресурс банку
Інформаційні документи
Інформаційні канали

Інформаційно-аналітична робота
Інформування керівництва та працівників банку
Комерційна розвідка
Контрпропаганда
Об'єкт інформації
Пропаганда
Спеціальні інформаційні операції
Структура інформаційно-аналітичної роботи
Сфера інформаційної уваги банку
Чутки

Питання для перевірки знань

1. Чому інформація вважається одним із головних ресурсів у діяльності банків?
2. Яким вимогам має відповідати організація інформаційного забезпечення діяльності банку?
3. Які елементи складають структуру інформаційно-аналітичної роботи банку?
4. На кого покладається організація інформаційно-аналітичної роботи в банку?
5. Чи можна вважати чутки джерелом отримання інформації банку?
6. Що належить до основних технологій інформаційного аудиту?
7. З якою метою банк проводить інформаційний моніторинг?
8. Як здійснюється процес обробки інформації у процесі інформаційно-аналітичної роботи банку?
9. В якому вигляді надаються керівництву та іншим особам результати інформаційно-аналітичної роботи?
10. Як зберігається інформація, отримана у процесі інформаційно-аналітичної роботи?
11. З яких джерел банк може отримати необхідну йому інформацію у процесі інформаційного супроводження своєї діяльності?
12. На кого покладається безпосереднє виконання заходів інформаційно-аналітичної роботи в банку?
13. Як економіст-аналітик здійснює заходи інформаційного аудиту у своєму підрозділі?
14. Чи може банк збирати інформацію, яка є комерційною таємницею інших банків?

15. Як здійснюється організація інформування керівництва та працівників банку у процесі інформаційного забезпечення діяльності банку?

Завдання для індивідуальної роботи

1. Ви — керівник підрозділу безпеки банку. У зв'язку з тим, що банк планує в майбутньому розширяти свою діяльність у регіонах країни, керівник банку доручив вам організувати роботу щодо формуванню каналів інформації та проведення інформаційного моніторингу стосовно отримання об'єктивної інформації про характеристики зазначених регіонів і конкурентне середовище. Окрім того, керівник просив надати йому звіт про проведену роботу з висновками і прогнозами. Як ви будуватимете свою роботу, щоб виконати доручення керівника банку?

2. Ви — керівник установи банку. На одній із зустрічей ви випадково стали свідком розмови двох осіб, які говорили про те, що ходять чутки стосовно одного з керівників найбільшого заводу регіону (завод є клієнтом вашого банку), якого, як випливало з розмови, звинувачують у хабарництві і проти нього відкрито кримінальну справу. Як ви гадаєте, чи варто серйозно ставитися до інформації, яку ви почули і чому?

3. Ви — керівник підрозділу безпеки банку. Розпорядженням керівництва банку вашому підрозділу доручено готувати щомісячне інформаційне зведення стосовно інформації, яка поширюється в зовнішньому інформаційному середовищі про банк. Окрім того, зведення повинно мати прогноз розвитку ситуації, яка, за даними зведення, складається навколо банку, з відповідним обґрунтуванням. Як ви будете організовувати свою роботу, щоб виконати поставлене перед вами завдання?

Література для поглибленого вивчення

1. *Деревицкий А. А.* Коммерческая разведка / Деревицкий А. А. — СПб. : Питер, 2006. — 208 с.
2. *Доронин А. И.* Бизнес-разведка / Доронин А. И. — М. : Ось-89, 2007. — 528 с.

3. *Зубок М. І.* Безпека бізнесу : навчальний посібник у схемах і таблицях / Зубок М. І., Позднишев Є. В., Яременко С. М. — К. : КНЕУ, 2008. — 480 с.
4. *Зубок М. І.* Інформаційно-аналітичне забезпечення підприємницької діяльності : навч. посіб. для студ. вищ. навч. закл. / Зубок М. І. — К. : КНТЕУ, 2007. — 156 с.
5. *Нежданов И. Ю*. Аналитическая разведка для бизнеса / Нежданов И. Ю. — М. : Ось-89, 2008. — 336 с.
6. *Хант Ч.* Разведка на службе вашего предприятия / Ч. Хант, В. Зартарьян. — К. : Укрзакордонсервис, 1992. — 160 с.
7. *Ярочкин В. И.* Корпоративная разведка / В. И. Ярочкин, Я. В. Бузанова. — М. : Ось-89, 2004. — 228 с.

Розділ 9

ЕКОНОМІЧНА БЕЗПЕКА БАНКУ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *суть економічної безпеки банку та її основні характеристики;*
- ✓ *основні напрями та заходи забезпечення економічної безпеки банку;*
- ✓ *систему захисту матеріальних ресурсів банку;*
- ✓ *основи фінансової безпеки банку та захисту банківських операцій;*
- ✓ *заходи з протидії втягуванню банку в незаконну фінансову діяльність;*
- ✓ *особливості забезпечення фінансової безпеки банку в умовах глобалізації;*
- ✓ *заходи банку з протидії рейдерським посяганням;*
- ✓ *методику роботи банку щодо забезпечення його економічної безпеки під час призначення до нього тимчасової адміністрації,*

*а також **уміти**:*

- ✓ *забезпечувати захист матеріальних цінностей банку при виконанні посадових обов'язків, грамотно вживати заходів з контролю за ними;*
- ✓ *якісно виконувати заходи захисту банківських операцій, правильно застосовувати прийоми і способи виявлення загроз банківським операціям та протидії їм;*
- ✓ *виявляти фінансові операції клієнтів сумнівного та протиправного характеру, вживати заходів щодо перетинання їх;*
- ✓ *виявляти ознаки шахрайських схем із коштами банку, у межах своїх повноважень вживати заходів щодо їх локалізації та ліквідації.*

9.1. Економічна безпека банку та її основні характеристики

Економічна безпека є видом банківської безпеки і займає провідне місце в системі його безпеки. Особлива значимість економічної безпеки банку обумовлюється низкою чинників як зовнішнього, так і внутрішнього характеру. По-перше, необхідність і важливість економічної безпеки обумовлені різноманітністю інтересів суб'єктів ринку банківських послуг. Прагнення до збільшення прибутків суб'єктів ринку загострює конкурентну боротьбу, а остання, у свою чергу, завжди перебувала в площині економічної безпеки.

По-друге, обмеженість фінансових ресурсів банків і джерел їх створення вимагає від них розроблення досить ефективних технологій банківського виробництва, застосування економічних інструментів підтримання ліквідності та конкурентоспроможності банків на необхідному рівні, якісного використання їх ресурсної бази.

По-третє, нестабільна економічна ситуація в державі, досить несподівані і різкі її зміни обумовлюють готовність банку в деякі періоди своєї діяльності до роботи в майже кризових умовах, з досить високим ступенем ризику, іноді на межі втрати своєї ліквідності. Усе це вимагає від банків вироблення адекватної економічної політики, економічної поведінки на ринку банківських послуг, поєднання принципів раціональності і

доцільного ризику при вкладанні коштів.

По-четверте, зростання економічної злочинності, насамперед у кредитно-фінансовій сфері, ставить банківську діяльність у ряд досить ризикових, що обумовлює високу відповідальність банків перед своїми клієнтами, вкладниками і акціонерами. У зв'язку з цим усі заходи безпеки спрямовуються і концентруються якраз навколо економічної безпеки, що й визначає її місце у системі безпеки банківської діяльності.

Аналіз точок зору різних авторів та фахівців щодо змісту економічної безпеки свідчить, що існує певна кількість тлумачень суті економічної безпеки, які мають певні розбіжності. Узагальнюючи ці тлумачення, можна дійти висновку, що всі вони зводяться до двох підходів: перший підхід базується на використанні поняття загрози, а другий — на економічних поняттях досягнення мети функціонування банку (прибутку). Існують також і інші визначення, які певною мірою поєднують зазначені вище підходи.

З погляду авторів другий підхід більш чітко відбиває сутність економічної безпеки банку, тому далі всі питання розглядатимуться якраз з даної точки зору. Відповідно до такого підходу під економічною безпекою банку будемо розуміти стан, за якого забезпечується економічний розвиток і стабільність діяльності банку, гарантований захист його ресурсів, здатність адекватно і без суттєвих втрат реагувати на зміни внутрішньої і зовнішньої ситуації.

Суть економічної безпеки банку реалізується в системі її критеріїв і показників. Критерієм економічної безпеки є оцінка економічного стану банку. Критеріальна оцінка економічної безпеки базується на оцінках: ресурсного потенціалу банку і можливостей його розвитку; рівня ефективності використання ресурсів; рівня можливостей банку протистояти загрозам його економічній безпеці та самостійно ліквідовувати їх; конкурентоспроможності банку; цілісності та масштабів структури банку; ефективності кадрової політики банку.

У системі показників економічної безпеки доцільно виділити: темпи зростання прибутковості та посилення економічної стабільності; рівень матеріального і соціального забезпечення працівників банку; розмір боргових зобов'язань банку; структуру дебіторської заборгованості; обсяги використання тіньового капіталу та ін. Для економічної безпеки важливе значення мають не стільки самі показники, скільки їх порогове значення, тобто допустимі величини, недотримання яких перешкоджатиме

нормальному розвитку діяльності банку, призводитиме до формування негативних тенденцій у його економічній безпеці. Найвищий ступінь економічної безпеки банку досягається за умови, що весь комплекс показників перебуває в рамках допустимих меж порогових значень, а порогове значення одного показника досягається не за рахунок іншого.

Виходячи із суті економічної безпеки банку в основу його економічної стратегії має бути покладена ідеологія стабільності та розвитку, яка враховує стратегічні перспективи й інтереси банку на ринку банківських послуг.

Слід зазначити, що розвиток банку — один із компонентів і умов забезпечення його економічної безпеки. Якщо банк в економічному плані не досягає розвитку, то в нього скорочуються можливості до виживання, опірності, пристосовуваності до внутрішніх і зовнішніх чинників. Тобто економічний розвиток банку забезпечує його стійкість на ринку — одну зі складових економічної безпеки.

Тому основна мета стратегії економічної безпеки полягатиме в забезпеченні економічного зростання банку.

У свою чергу, забезпечення економічного зростання завжди залежатиме від платоспроможного попиту на послуги банку. Низький попит на банківські послуги призводить до їх звуження, зменшення ресурсної бази банку і, як наслідок, до порушення його ліквідності. Платоспроможний попит формується як об'єктивними причинами, так і суб'єктивними. Причому обидві причини досить збалансовані і порушення такого балансу з будь-якого боку веде до гальмування економічного зростання банку. За таких умов банки з урахуванням наявної економічної ситуації, яка створюються в державі, повинні постійно працювати над розширенням своїх послуг, удосконаленням технологій банківського виробництва, привабливістю взаємовідносин із клієнтами, розраховувати свої послуги на всі верстви населення, орієнтуючись як на багатих, так і на малозабезпечених клієнтів. Тут досить важливим може бути розосередження попиту як за регіональним принципом, так і з погляду розширення спектра банківських операцій і послуг. Тобто основним завданням має бути формування послуг і розроблення банками операцій, які за будь-яких умов забезпечували б платоспроможний попит на них. А критерієм виконання вищезазначеного завдання буде рівень уміння кожного банку формувати такий попит на свої послуги.

Під стабільністю банку розуміють здатність банку зберігати свій стан навіть у разі непередбачених фінансових втрат. Рівень

стабільності банку — це максимальний або допустимий рівень непередбачених втрат, за якого ще зберігається стан нормального функціонування, але у разі перевищення цього рівня може настати банкрутство банку.

Важливим моментом стабільної роботи банку є ефективна, гнучка політика управління активами й пасивами банків. У цьому особлива роль належить інформаційно-аналітичному забезпеченню діяльності банку. Для гарантованого залучення і використання коштів банкам украй важливо знати пріоритети державної підтримки, об'єктивну ситуацію з насиченістю і дефіцитом ринку банківських послуг, його структурою і можливостями окремих суб'єктів, прогнози розвитку. За наявності у керівництва банків такої інформації, може бути вироблена ефективніша тактика поведінки, правила і параметри діяльності банків навіть на невеликі проміжки їх розвитку і разом з цим завжди буде можливість ефективніше і обґрунтовано будувати стратегію кожного з банків.

Важливим, особливо в українських умовах, для стабільності роботи банку є його здатність утримувати свої кошти від їх розкрадання та незаконного використання, насамперед під час проведення банківських операцій.

Ще одним із найважливіших елементів стратегії економічної безпеки банків (крім забезпечення економічного зростання і стабільності) є забезпечення стійкості їх капіталу. Проблема стійкості капіталу банку за сучасних умов є чи не однією з найважливіших і забезпечує можливість банкам підтримувати свою ліквідність в умовах тривалого впливу на них різноманітних негативних тенденцій. Виживання банків на ринку за різкого коливання валютних курсів, змін у законодавстві, кон'юнктури ринку може бути забезпечено їх високоліквідними активами (у тому числі дорогоцінними металами, державними цінними паперами та паперами інших прибуткових суб'єктів господарювання, іноземною валютою тощо), багатопрофільністю діяльності, розгалуженою структурою банківських установ, а також активним проведенням заходів безпеки.

Крім того, виходячи з тенденцій, яких набули останнім часом вітчизняні банки, можна говорити про те, що загальновідомих заходів забезпечення стійкості капіталу банків уже недостатньо. Особливо це виявилося під час фінансової кризи та поширеної останнім часом практики рейдерських посягань на відкриті акціонерні товариства, у тому числі і банки. Ураховуючи зазначену ситуацію, додатковими заходами забезпечення

стійкості капіталу банків могли б бути:

- обов'язкова повна капіталізація банків з самого початку їхньої діяльності;
- забезпечення живучості капіталу банку за рахунок його переливання між суб'єктами банківського об'єднання або ж суб'єктами фінансово-промислової групи. Тобто банки стають елементами відповідної структури, капітал якої використовується залежно від інтересів та умов функціонування
- даної структури;
- раціональне використання фінансових ресурсів та активна робота щодо мінімізації втрат у процесі діяльності банків;
- формування стабільних джерел фінансових ресурсів;
- страхування ризиків банківської діяльності;
- прагнення до збільшення обсягів власного капіталу в структурі капіталу банку;
- забезпечення діяльності банку та підтримання його ліквідності обмеженими силами та засобами в умовах дії екстремальних ситуацій.

Розуміння необхідності вжиття цих та інших заходів разом із заходами щодо забезпечення розвитку банків та якісне їх здійснення, безумовно, буде сприяти підвищенню економічної безпеки банків у сучасних умовах їхньої діяльності.

Характеризуючи сучасний стан економічної безпеки вітчизняних банків, слід звернути увагу на те, що, незважаючи на формування певних підрозділів (економічної безпеки), декларацію намірів щодо формування сучасних систем безпеки та визначення відповідних заходів, економічна безпека банків не набула того значення, яке повинно їй відводитись у діяльності комерційних банків. Заходи економічної безпеки у більшості своїй спрямовані на виявлення, локалізацію, усунення правопорушень, що скоюються працівниками банків у матеріальній та інтелектуальній сфері. Однак вони недостатньо враховують управлінську сферу та сферу зовнішніх економічних взаємовідносин банків. Крім того, сучасні заходи безпеки банків мають відокремлений характер навіть у межах однієї сфери їх застосування. Попереджуючи порушення в одному місці, безпека банків не поширює своїх дій на інші можливі осередки порушень і відновлює свій вплив тільки у разі виявлення нових порушень.

Звертає на себе увагу і той факт, що підрозділи безпеки банку у більшості своїй необачно взяли на себе відповідальність за стан безпеки відповідних сфер банківської діяльності, залишивши безвідповідальними суб'єктів, які здійснюють діяльність у цих

сферах. Так, організовуючи безпеку матеріальних цінностей, поза увагою залишено облік, контроль їх наявності та якості, регулювання взаємовідносин адміністрації банків і працівників щодо використання таких цінностей. Безпека спрямовує свої зусилля на виключення можливості несанкціонованого доступу до цінностей та відшкодування шкоди, завданої банкам посяганнями на їх матеріальні цінності, не формуючи умов, в яких зазначені посягання не могли б утворюватися взагалі. Від того в банках мають місце втрати матеріальних цінностей на значні суми, які виявляються під час щорічних інвентаризацій, і не завжди є підстави притягувати когось до матеріальної відповідальності.

Економічна безпека не виділяється банками в окремий вид безпеки, а її заходи виконуються в загальному порядку діяльності сил безпеки банків. Що ж стосується невеликих банків або ж відділень чи філій банків, то там взагалі заходи економічної безпеки не проводяться, або проводяться на пасивному рівні — захисту. Особливим же недоліком є те, що банківська безпека традиційно вважається функцією спеціального підрозділу — служби безпеки і ніяк не трансформується до інших підрозділів банку.

Економічна безпека як основа безпеки діяльності банків має бути зосереджена на головних напрямах банківської діяльності, насамперед тих, де сконцентровані фінанси банків — матеріальному і фінансовому. Як показує досвід, близько 20% своїх фінансових ресурсів банки витрачають на формування основних засобів, понад 50% використовується в банківських операціях, ще 20% становлять витрати на забезпечення діяльності [70]. За таких умов очевидно, що основні зусилля банківської безпеки мають бути зосереджені саме на захисті матеріальних цінностей та банківських операцій.

Акцентуючи увагу на провідній ролі економічної безпеки в системі безпеки банку, варто зауважити, що вона сама також мусить мати системний та комплексний характер. Системність економічної безпеки банку має забезпечуватися через певну впорядкованість заходів безпеки, формування відповідного алгоритму їх застосування, базуватися на єдиних технологіях забезпечення безпеки та централізованому управлінні ними. У свою чергу, комплексний підхід в економічній безпеці банку реалізується через застосування заходів фінансового, правового, інформаційного, соціально-психологічного, технічного та іншого

характеру, а також використанням можливостей усіх структур банку.

Застосування зазначених та інших заходів економічної безпеки має забезпечити формування відповідних режимів діяльності банку:

- ❖ режиму формування та використання ресурсів банку;
- ❖ режиму поведінки персоналу в різних умовах виробничої діяльності;
- ❖ режиму захисту інформації банку;
- ❖ особливого режиму функціонування банку в умовах дії несприятливих факторів економічної, політичної, соціальної ситуації в країні.

Крім того, комплексна система економічної безпеки має забезпечити відповідні режими поведінки самого банку на ринку банківських послуг з урахуванням змін на ньому та в країні. Тут можуть запроваджуватися такі режими: режим економії, режим активізації, режим виживання і т. д.

Комплексний підхід до формування відповідного режиму буде забезпечуватися через участь усіх структур банку в ньому, а також проведенням заходів по різних видах економічної безпеки: фінансовій, інформаційній, кадровій, безпеки матеріальних ресурсів, що, у свою чергу, забезпечить оперативність та своєчасність реагування банку на будь-які зміни ситуації на ринку, в цілому в країні та конкретно в банку.

Виходячи з викладеного можна зробити висновок, що підрозділи безпеки банку мають виконувати в системі економічної безпеки лише спеціальні функції: охоронні, режимні, інформаційні, контрольні, а заходи безпеки в технологіях банківського виробництва мають покладатися на підрозділи банку з установленням відповідальності за їх проведення і результати.

9.2. Захист матеріальних ресурсів банку

Вище вже зазначалося, що економічна безпека банку зосереджує свої зусилля насамперед на двох основних напрямах: захисті матеріальних ресурсів (матеріальних цінностей) та захисті фінансових ресурсів, насамперед обігових коштів. Такий підхід грунтується на практиці комерційної діяльності суб'єктів

підприємництва, у тому числі і банків, а вона, у свою чергу, вказує на природу формування капіталу суб'єкта господарювання, який базується на матеріальних ресурсах і обігових коштах. Матеріальні ресурси, передусім засоби виробництва, які базуються на сучасному обладнанні і передових технологіях, є однією з важливих складових структури капіталу і основою для формування прибутку. Головним призначенням обігових коштів є формування та нарощування капіталу, а інструментом тут є комерційні та банківські операції.

Характеризуючи роль матеріальних ресурсів у структурі капіталу банку та його діяльності можна говорити, що їх захист є важливою умовою забезпечення економічної безпеки банку. Водночас під захистом тут мається на увазі не просто комплекс заходів, а головне гарантія збереження ресурсів і забезпечення їх ефективного функціонування. Розв'язуючи питання захисту матеріальних ресурсів, необхідно зосередити увагу на двох факторах: виявленні загроз матеріальним цінностям і формування ефективної системи захисту від них.

Аналізуючи досвід банків щодо протидії загрозам, можна бачити, що серед загроз матеріальним ресурсам банку переважають внутрішні загрози, а тому система заходів захисту цих ресурсів має бути насамперед зорієнтована на запобігання реалізації саме цих загроз. Тут слід звернути увагу на ті особливості зазначених загроз, які характерні саме для сьогодення. Практика банківської діяльності показує, що більшість загроз матеріальним цінностям банків реалізуються у вигляді крадіжок (75—80% усіх загроз матеріальним цінностям). Причому правоохоронці акцентують увагу на існуванні тенденції до збільшення кількості дрібних крадіжок і розширення кола осіб, які такі крадіжки скоїли вперше. Більше того, вони відзначають підвищену активність саме молодих людей до такого виду посягань на банківську власність, особливо у віці 25—35 років, близько 40% з яких молоді жінки. Крім того, помічено, що близько 90%, а то й більше, крадіжок скоюються працівниками банків, оскільки саме вони найбільш обізнані зі слабкими місцями в системі захисту матеріальних цінностей у власному банку [114].

За таких умов заходи захисту матеріальних цінностей у банку мають бути досить потужними і надійними.

Потужність же заходів захисту, у свою чергу, залежатиме від фінансових, інтелектуальних, технічних та інших можливостей самого банку.

Виходячи з цього банки будують систему захисту своїх матеріальних ресурсів, орієнтуючись на власні можливості, максимально використовуючи для цього організаційні заходи та власну структуру. Крім того, заходи захисту запроваджуються не як окремі дії з мінімізації загроз матеріальним ресурсам. Вони формуються у відповідну систему взаємопов'язаних дій та поведінки, спрямовану на запобігання, виявлення, локалізацію, усунення загроз та ліквідацію їх наслідків. Система поєднує в собі заходи регулювання, обмеження і заборони, доступу, контролю та відповідальності. У загальному вигляді система заходів захисту матеріальних ресурсів охоплює: суворий і безумовний облік усіх цінностей банку, персональну відповідальність посадових осіб за правильне зберігання, стан, грамотну експлуатацію технічних засобів і обладнання, організацію надійної охорони цінностей, періодичний контроль наявності та стану цінностей, формування нормативно-правової бази, яка регулювала б порядок їх експлуатації, обслуговування та збереження.

Разом з тим система захисту є одним з елементів безпеки матеріальних ресурсів банку, яка крім зазначених включає такі заходи: інженерно-технічні, технологічні, правові тощо. Наприклад, заходи інженерно-технічної безпеки матеріальних ресурсів можуть включати:

- дотримання встановлених стандартів (норм) при створенні матеріальних об'єктів;
- сертифікацію і ліцензування експлуатації матеріальних об'єктів та обладнання;
- дотримання встановлених режимів експлуатації матеріальних об'єктів, технічних засобів та обладнання;
- діагностику стану матеріальних об'єктів та їх систем;
- своєчасну профілактику, обслуговування та ремонт систем, обладнання, технічних та інженерних засобів, що забезпечують їх діяльність.

Облік матеріальних цінностей має передбачати облік їх наявності, руху та експлуатації. Не важко вирішити питання обліку матеріальних цінностей, коли їх одиниці чи десятки або навіть сотні. Складніше, коли їх тисячі чи десятки тисяч і коли значна їх частина перебуває в постійному русі між установами, підрозділами, матеріально відповідальними особами банку. Проте у таких умовах і необхідно звертати увагу на забезпечення безумовного їх обліку.

Банки, як правило, справляються з обліком наявності матеріальних цінностей. Гірше справи з обліком їх руху. На практиці доводиться спостерігати суттєві прогалини в обліку руху матеріальних цінностей, у результаті чого банкам завдається збитків на десятки, а то й сотні тисяч гривень.

Система захисту матеріальних цінностей у цьому разі повинна передбачати інститут матеріально відповідальних осіб, через яких має забезпечуватися рух матеріальних цінностей. Причому, як показує досвід діяльності банків, кількість таких осіб визначається не за видами матеріальних цінностей, а за обсягами матеріальної відповідальності. Наявність матеріально відповідальної особи, у підзвіті якої перебувають цінності на мільйони гривень, зовсім не означає, що такі збитки в разі потреби будуть покриті. Тому, очевидно, правильно підходять до розв'язання даного питання ті банки, де матеріально відповідальні особи визначаються відповідно до обсягів матеріальних цінностей і підрозділів, захист яких вони забезпечують.

Матеріальні цінності за відповідними документами передаються зі складів матеріально-відповідальним особам, а від них — за разовими документами до користувачів. Зазначені документи подаються бухгалтерії для обліку. Зміна користувачів матеріальних цінностей, передання останніх у ремонт, на склади здійснюються тільки через матеріально відповідальних осіб. За таких умов бухгалтерія завжди матиме об'єктивну картину про місцезнаходження тих чи тих матеріальних цінностей незалежно від їх кількості й інтенсивності руху, а також безпосередньо відповідальних за них осіб.

Облік експлуатації матеріальних цінностей здійснюється з тим, щоб знати якісний стан матеріальних об'єктів. Як свідчить практика, облік експлуатації матеріальних об'єктів здійснюється в основному через урахування їх зносу (амортизації). Водночас інтенсивна експлуатація окремого обладнання може призвести до того, що може достроково втратитить свої властивості і створюватиме загрозу в подальшій роботі. Тут мають обов'язково братися до уваги час та умови експлуатації, види технічного обслуговування, кількість та обсяги ремонтів тощо. Якраз ці показники характеризуватимуть якість матеріальних цінностей. Облік експлуатації (крім амортизації) мають виконувати особи, що працюють з матеріальними об'єктами (користувачі). Такий підхід виключить можливість раптового

виникнення загроз з боку матеріальних об'єктів та забезпечить плановий характер їх експлуатації.

Проте зазначений підхід до обліку матеріальних цінностей сам по собі не забезпечить гарантованого їх захисту. Він має застосовуватися у сукупності з іншими заходами, зокрема встановленням безумовної персональної відповідальності за пошкодження, неграмотну експлуатацію, знищення, викрадення, нестачу матеріальних цінностей.

Відповідно до чинного законодавства за шкоду, заподіяну суб'єкту господарювання при виконанні трудових обов'язків, працівники, з вини яких заподіяно шкоду, несуть повну матеріальну відповідальність (у розмірі прямої дійсної шкоди) або обмежену матеріальну відповідальність (не більше від свого середнього місячного заробітку).

Повна матеріальна відповідальність може наставати у випадках, коли:

а) між працівником і банком укладено письмовий договір про взяття на себе працівником повної матеріальної відповідальності за незабезпечення цілості майна, цінностей, переданих йому на зберігання або для інших цілей. Утім такий договір може бути укладено лише з працівниками, які обіймають посади, виконують роботи, безпосередньо пов'язані зі зберіганням, обробкою, продажем (відпусканням), перевезенням або застосуванням у процесі виробництва, переданих їм цінностей. Перелік таких робіт і посад має встановлюватися Кабінетом Міністрів України. Тобто банк, укладаючи з працівниками договір повної матеріальної відповідальності, має передбачити в штатному розкладі та в посадових інструкціях відповідні посади та роботи, які не суперечили б умовам, визначеним чинним законодавством;

б) майно та інші цінності були одержані працівником під звіт за разовою довіреністю або іншими разовими документами. Тож рух матеріальних цінностей банку має обов'язково документуватися разовими документами (довіреностями, актами, накладними тощо) і в жодному разі — записами в журналах обліку, картках тощо;

в) шкоди завдано діями працівника, які мають ознаки діянь, що переслідуються у кримінальному порядку. У таких випадках, перш ніж притягнути особу до матеріальної відповідальності, необхідно довести, що її дії мають кримінальний характер. Тут банк повинен звертатися до правоохоронних органів, ініціювати порушення кримінальної справи і виступати за нею цивільним позивачем;

г) шкоди завдано працівником, який був у нетверезому стані;

д) шкоди завдано нестачею, умисним знищенням (зіпсуванням) цінностей, виданих йому в користування;

є) шкоди завдано не в процесі виконання трудових обов'язків;

ж) відповідно до законодавства на працівників покладено повну матеріальну відповідальність за шкоду, заподіяну банку.

Для забезпечення дієвості системи захисту матеріальних цінностей банк має розробити власні нормативні документи, які б регулювали порядок, терміни, умови роботи з матеріальними цінностями, давали тлумачення б певних дій та поведінки працівників, порядок доведення до працівників вимог банку, чітко визначали межі робочого часу тощо, тобто встановлювали підстави, за яких банк може звертатися до суду з клопотанням про притягнення до повної матеріальної відповідальності винних осіб.

Обмежена матеріальна відповідальність може наставати за зіпсування або знищення матеріальних цінностей через свою недбалість і застосовуватись до всіх працівників банку.

Зважаючи ж на те, що матеріальна відповідальність може наставати лише за умови, коли шкоди заподіяно винними протиправними діями працівників, виникає необхідність урегулювати порядок використання матеріальних цінностей банку. Тобто стосовно всіх цінностей, які використовуються в процесі банківського виробництва, мають бути розроблені інструкції з їх експлуатації, а стосовно інших цінностей — інструкції про роботу (операції) з ними. Крім того, з огляду на те, що матеріальна відповідальність може наставати за шкоду, заподіяну внаслідок порушення покладених на працівників трудових обов'язків, потрібно, щоб у всіх видах договорів (угод) на співпрацю з працівниками, у посадових інструкціях було чітко визначено їхні обов'язки, умови та обсяги відповідальності, без можливості подвійного трактування.

Отже, якщо законодавство визначає умови відшкодування суб'єкту господарювання завданої йому шкоди втратою, пошкодженням чи знищенням матеріальних цінностей, то підстави для такого відшкодування формує сам суб'єкт.

Тут слід зазначити, що врегулюванню підлягає не тільки порядок зберігання, використання та охорони матеріальних цінностей, а й сама процедура притягнення до матеріальної відповідальності. Насамперед рішенню про притягнення працівника банку до матеріальної відповідальності має передувати службове розслідування. Підставами для його

проведення має бути наказ (розпорядження) керівника установи банку про необхідність проведення службового розслідування та Інструкція банку про порядок проведення службових розслідувань.

Вихідними даними для початку розслідування мають бути: матеріали перевірок, інвентаризацій, ревізій, заяви посадових осіб про факти порушення зберігання матеріальних цінностей чи їх зникнення (пошкодження); довідки бухгалтерії установи банку про завданий збиток; посадові Інструкції працівників банку, які стосувалися до матеріальних цінностей, щодо заподіяння шкоди яким проводиться службове розслідування; нормативно-правові документи, які регулюють порядок використання (експлуатації, зберігання, охорони) матеріальних цінностей; опис технологій виробництва, в яких використовуються зазначені матеріальні цінності.

У процесі розслідування комісія або призначена особа (працівник підрозділу безпеки) вивчає матеріали ревізій, перевірок, інвентаризацій, заяви певних осіб, умови, в яких здійснювалося використання (експлуатація) матеріальних цінностей. За необхідності отримуються пояснення певних осіб, збираються повідомлення, що стосуються предмета розслідування, висновки експертів, додаткові документи. Вивчення зазначених матеріалів спрямовується на встановлення зв'язку між діями певних осіб, вимогами технологій, нормативних документів, умов діяльності та виявлення можливих порушень, особливостей поведінки, можливості зовнішнього впливу.

По завершенні службового розслідування робляться висновки, в яких вказуються:

— причини заподіяння шкоди банку;

— причетні особи та ступінь їх причетності до збитку;

— які конкретно вимоги та яких документів, посадових інструкцій, технологій порушено;

— рекомендації щодо відшкодування збитку та притягнення причетних осіб до відповідальності;

— рекомендації щодо недопущення подібних фактів.

Досить важливим елементом системи захисту матеріальних цінностей є їх охорона. Слід зазначити, що основне призначення охорони — установити відповідний режим доступу до матеріальних цінностей та виключити будь-які можливості посягання на них. Але на практиці охорона, як правило, забезпечує захист не самих цінностей, а місць їх зберігання чи експлуатації. За таких умов банк має чітко визначити

повноваження та межі відповідальності сил охорони у сфері захисту матеріальних цінностей. Як доводить практика, до функцій охорони банків у таких випадках відносять:

— забезпечення пропускного режиму до банку;

— забезпечення режиму доступу до місць зберігання (експлуатації) цінностей;

— контроль додержання встановленого порядку виносу (вносу) матеріальних цінностей з (до) банку;

— захист місць зберігання цінностей;

— захист транспортування цінностей;

— контроль додержання правил пожежної безпеки при охороні цінностей.

Якщо проблема пропускного режиму добре вирішується банками, то внутрішньооб'єктовий режим підтримується не завжди ефективно, перш передусім через невизначеність, неконкретність функцій охорони в цьому питанні. Тут має бути визначено: що конкретно захищають сили охорони (надається перелік); який існує порядок здачі під охорону і зняти з-під охорони об'єктів; як здійснюється доступ до цінностей; умови відповідальності охорони; дії охорони щодо захисту місць зберігання цінностей (чи їх самих). Такі питання визначаються знову ж таки в нормативно-правових документах банку.

Важливого значення в системі захисту матеріальних цінностей набуває контроль, насамперед контроль їх наявності, стану, умов зберігання чи експлуатації. Тут система передбачає різні види контролю. Перше — це щоденний контроль матеріальних цінностей кожним працівником на своєму робочому місці. Друге — періодичний контроль матеріальних цінностей у підрозділах. Зазвичай контроль організовується і проводиться керівниками підрозділів через перевірки наявності цінностей. Такі перевірки можуть про водитися щотижня або ж щомісяця.

У частині установ банків стосовно цінностей, які зберігаються на складах або у великих обсягах, використовуються в банківському виробництві (наприклад комп'ютерна техніка), можуть проводитися перевірки за графіком раптових перевірок за рішенням керівника установи. Метою таких перевірок є встановлення наявного стану цінностей на певну дату та запобігання несанкціонованому їх використанню чи реалізації. Такі перевірки можуть проводитися два—чотири рази на рік.

Безумовно, що обов'язковим є щорічні інвентаризації майнових активів банку, які проводяться спеціально створеними комісіями згідно з наказом керівника установи банку.

Контроль не тільки дає можливість установити наявність і стан матеріальних цінностей, а й запобігає поширенню різного роду загроз їм, оскільки за результатами контролю вживаються заходи з усунення причин виникнення зазначених загроз та заходи стосовно відшкодування шкоди, завданої нестачею, пошкодженням, виведенням з ладу матеріальних об'єктів. Після проведення інвентаризації весь облік матеріальних цінностей має бути приведений у відповідність до наявного майна. Невідшкодоване майно має бути списане на витрати банку.

Ще одним елементом системи захисту матеріальних цінностей є створення в установі банку необхідної нормативно-правової бази, яка регулювала б як відносини у сфері матеріально-технічного забезпечення процесу банківського виробництва та діяльності банку, так і порядок експлуатації обладнання банківських установ. Мають бути врегульовані буквально всі питання щодо використання матеріальних цінностей: придбання, обліку, одержання, експлуатації, зберігання, перевірки, охорони, руху, відшкодування шкоди і т. п. Тільки за таких умов система може ефективно функціонувати, оскільки саме зазначені документи поєднують усі елементи системи й обумовлюють їх вплив на поведінку працівників банку, взаємовідносини в ході експлуатації матеріальних цінностей, їх використання в процесі експлуатації матеріальних цінностей та під час проведення банківських операцій.

Слід також додати, що надходження матеріальних цінностей до банку має обґрунтовуватися відповідними документами (накладними, чеками купівлі-продажу, актами передання тощо), на основі яких вони приймаються до обліку. Якщо матеріальні цінності не передбачається використовувати найближчим часом, вони передаються на склад (до сховища) на зберігання, якщо ж передбачається їх експлуатація, тоді вони зі складу передаються відповідальним особам під звіт.

Доступ до матеріальних цінностей, які перебувають на складах (у сховищах) дозволяється тільки особам, які відповідають за їх зберігання. Відповідно до своїх посадових обов'язків такі посадові особи зобов'язані забезпечити необхідні умови щодо надійного зберігання матеріальних цінностей, виключення можливості їх псування, пошкодження, виходу з ладу. За встановленим у банках порядком для перевірки наявності і контролю якості матеріальних цінностей, які зберігаються на складах (у

сховищах) допускаються окремі працівники (керівники підрозділів банку) або спеціально створені комісії.

Матеріальні цінності, передані під звіт відповідальним особам, використовуються ними або під їхнім контролем працівниками банку згідно з установленими правилами їх експлуатації відповідно до тих чи тих технологій банківських операцій чи заходів забезпечення діяльності банку.

Ремонт та обслуговування обладнання і техніки проводиться у встановленому порядку силами установи банку або на договірних засадах спеціалізованими організаціями. Передання матеріальних цінностей з-під звіту однієї особи під звіт іншій, від однієї установи — до іншої здійснюється згідно з актом приймання-передавання відповідними комісіями, які зазначають наявність, стан, комплектність та придатність до експлуатації матеріальних цінностей, які передаються.

Таким чином, системний підхід до захисту матеріальних цінностей та застосування відповідного комплексу заходів за чіткої їх організації і контролю може забезпечити надійне їх зберігання та ефективну експлуатацію в установах банку.

9.3. Фінансова безпека банку

Фінансова безпека банку є головним елементом його економічної безпеки. Водночас певною мірою вона є самостійним елементом і являє собою такий стан фінансових ресурсів банку, за якого забезпечується його ефективна (прибуткова) діяльність, захист фінансових інтересів та здатність зберігати свої фінансові можливості під впливом різного роду небезпек і загроз. Тобто основна увагу фінансової безпеки має бути спрямована на забезпечення ефективного використання фінансових ресурсів і підтримання їх на достатньому для ефективної діяльності банку рівні за будь-яких умов. Останнє ж передбачає активну його діяльність щодо залучення фінансових ресурсів та їх ефективного вкладання. Виходячи з цього можна зауважити, що фінансова безпека охоплює всі сторони фінансової діяльності банку і забезпечує його стійкість та конкурентоспроможність у процесі функціонування.

Метою ж фінансової безпеки банку є забезпечення фінансової стійкості та фінансової незалежності банку, недопущення втрати та неефективного використання ним своїх фінансових ресурсів.

Основними завданнями фінансової безпеки є:

❖ моніторинг і прогнозування факторів, що визначають загрози фінансовій безпеці банку;

❖ формування оптимальної структури боргових (дебіторських та кредиторських) зобов'язань банку;

❖ протидія злочинним посяганням на фінансові ресурси банку та уражаючим факторам надзвичайних ситуацій;

❖ визначення повноважень і функцій посадових осіб банку в його фінансово-господарській діяльності;

❖ моніторинг індикаторів фінансової безпеки банку;

❖ визначення пріоритетів і оптимізація використання фінансових ресурсів;

❖ збереження і нарощування фінансових ресурсів банку;

❖ забезпечення балансу доходів і витрат у діяльності банку;

❖ забезпечення ліквідності та платоспроможності банку;

❖ формування умов для швидкого відновлення платоспроможності та ліквідності банку, адекватних обстановці фінансового стану у випадках негативного впливу на нього екстремальних ситуацій.

До об'єктів фінансової безпеки банку слід віднести:

— кошти (готівкові і безготівкові);

— фінансові розрахунки;

— фінансові документи;

— фінансові інструменти (акції, векселі, облігації, страхові поліси);

— дорогоцінні метали та коштовне каміння;

— фінансові відносини.

Особливий характер банківської діяльності, заснований на різних прийомах використання коштів, зумовлює і відповідні специфічні підходи до забезпечення фінансової безпеки банків.

Специфічність заходів фінансової безпеки полягає в тому, що вони мають поділятися на дві категорії — заходи загального (рис.9.1) та заходи спеціального характеру (рис. 9.2).

До заходів фінансової розвідки банку слід віднести:

• отримання інформації про фінансові можливості конкурентів і клієнтів банку;

• виявлення тіньової складової у фінансових ресурсах клієнтів;

- дослідження кредитної і податкової історії клієнтів;
- пошук прихованих фінансових ресурсів (активів) у процесі здійснення роботи щодо повернення простроченої дебіторської заборгованості;
- контроль законності використання фінансових ресурсів банку;
- визначення причин заподіяних банку збитків, упущеної вигоди і т. і.;
- контроль поведінки позичальників у процесі здійснення кредитного моніторингу;
- моніторинг фінансових ринків;
- визначення економічної потужності загроз (обсяг втрат, збитків, шкоди, упущеної вигоди і т. і.).

Рис. 9.1. Заходи фінансової безпеки загального характеру

Рис. 9.2. Заходи фінансової безпеки спеціального характеру

Заходами з протидії втягуванню банку в незаконну фінансову діяльність є:

- фінансовий моніторинг операцій клієнтів банку;
- перевірка надійності кредиторів і законного походження їх фінансових ресурсів;
- інформаційно-аналітичне супроводження банківських операцій;
- формування картотеки ненадійних клієнтів і партнерів;
- дотримання заходів безпеки у процесі співпраці з кредиторами, партнерами і клієнтами;
- моніторинг суб'єктів фондового ринку.

Сам же процес забезпечення фінансової безпеки банку являє собою сукупність заходів, спрямованих на формування фінансових ресурсів, запобігання збиткам та ефективне використання коштів у його фінансово-господарській діяльності. Безпосередньо заходи із забезпечення фінансової безпеки виконуються у чотири етапи:

1. Визначення загроз фінансовій безпеці банку, їх небезпечності та механізмів негативного впливу на фінансовий стан банку.
2. Визначення уразливих (слабких) місць і напрямів у фінансовій безпеці банку, розроблення та застосування заходів захисту та протидії негативному впливу загроз.
3. Визначення сильних сторін та переваг фінансової безпеки банку, проведення заходів щодо мінімізації ризиків використання коштів.
4. Формування (використання) сприятливих умов для здійснення фінансово-господарської діяльності банку, реалізація заходів захисту його господарських і банківських операцій.

Ураховуючи, що внутрішні загрози мають досить значну питому вагу в усій сукупності загроз банку, а також численні

приклади проведення банками операцій, які є для них неефективними, а то й збитковими, особливе місце у фінансовій безпеці має займати протидія неконтрольованому витоку з банку коштів. Здійснення заходів з протидії неконтрольованому витоку коштів є функцією майже всіх банківських підрозділів за постійного контролю служби безпеки та керівництва банків. Тут мають проводитися досить різноманітні заходи, серед яких:

— облік усіх видів коштів, фінансових документів і фінансових інструментів у банку;

— планування використання фінансових ресурсів банку;

— колективне прийняття рішень про здійснення великих платежів та об'ємних банківських операцій;

— визначення повноважень посадових осіб щодо використання коштів банку;

— дотримання принципу «чотирьох очей» при оформленні фінансових документів;

— правове регулювання порядку фінансування проектів, операцій, діяльності банку;

— визначення обсягів відповідальності посадових осіб за допущені порушення при використанні коштів банку;

— установлення спеціального порядку доступу до фінансових ресурсів банку;

— забезпечення надійного зберігання готівки, цінностей, банків фінансових документів та інструментів у банку;

— установлення спеціального порядку надання банком гарантій, акредитивів, авалювання векселів, прийняття банком зобов'язань за третіх осіб;

— використання кошторисного підходу до фінансування господарської діяльності банку.

Оскільки переважну частину фінансових ресурсів банку становлять обігові кошти, то важливого значення для фінансової безпеки набуває захист банківських операцій, де здійснюється найбільший обіг коштів. Тут слід звернути увагу на те, що банківські операції, є найбільш ризиковим видом діяльності банків, тому завжди потребують досконалого захисту.

9.3.1. Забезпечення безпеки банківських операцій

Кредитні операції. Останнім часом у кредитній діяльності банків склалася досить небезпечна тенденція, пов'язана з різким зростанням обсягів неповернення коштів за кредитними операціями.

За даними Національного банку України, частка таких кредитів становила 11,7% (станом на 1 вересня 2010 р.), тоді як ще два роки тому їх обсяги дорівнювали лише 1,6% від загальної суми наданих кредитів (рис. 9.3) [139]. Зростання обсягів проблемних кредитів банків формує істотну загрозу для банків, насамперед зниження їх можливості щодо відтворення ресурсів і підвищує ризик невиконання банками своїх зобов'язань перед клієнтами та кредиторами. Як вказує Національний банк України у своїх документах про запровадження ліквідаційної процедури в банках, саме збільшення обсягів неповернених кредитів було головною причиною втрати ними своєї ліквідності та платоспроможності.

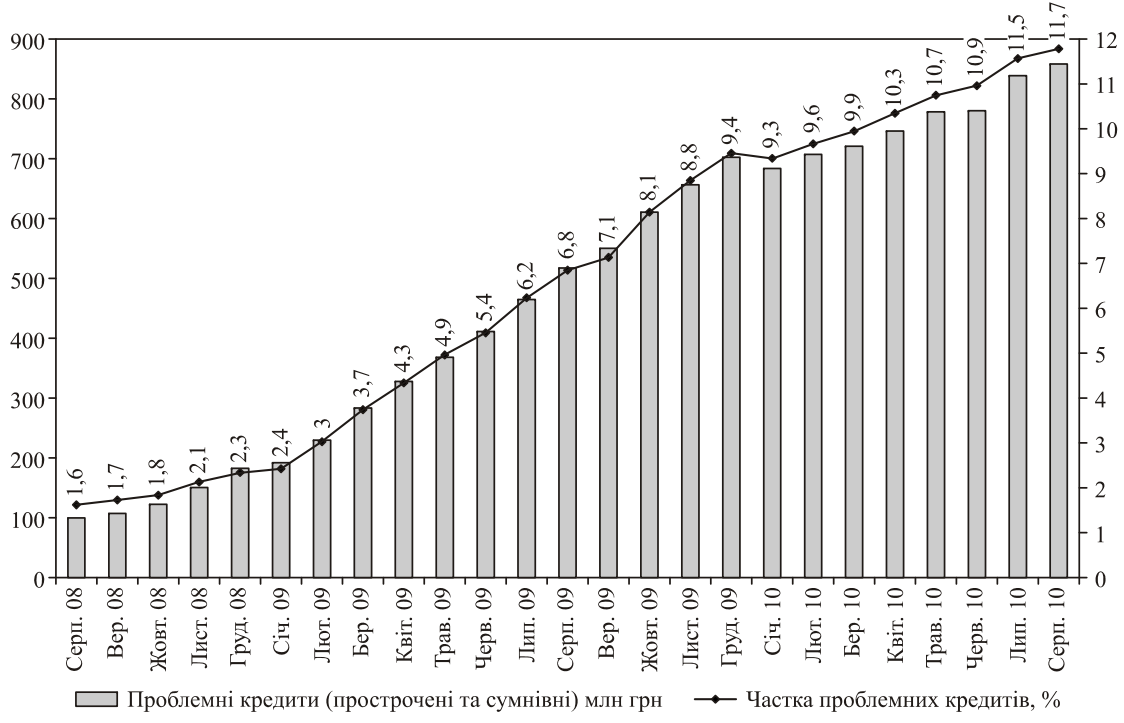

Рис. 9.3. Динаміка зростання проблемних кредитів у банківській системі України

Аналіз діяльності банків у сфері кредитування показує, що основними причинами, які створюють негативний результат, є:

- неадекватна реакція банків на зміни економічної ситуації в країні, особливо з погляду підвищення ризику комерційної діяльності, а також на стан, ефективність діяльності та перспективність економічних проектів позичальників. З появою ринкових умов, розвитком комерційної діяльності створилася ситуація, за якої правове регулювання підприємницької діяльності стало відставати від темпів її розвитку. З часом окремі види такої діяльності стали суперечити певним правовим нормам, що призвело до підвищеного ризику будь-якої комерційної операції. Крім того, наявність платіжної кризи, значні обсяги бартерних операцій у розрахунках суб'єктів господарювання, створення великих бізнес-структур, значно звузили ринок для окремих банків і загострили умови, зокрема, для кредитування, що також вплинуло на підвищення ризику кредитної діяльності банків.

Разом з тим спрощення умов отримання кредитних коштів, що мало місце в останні роки, обумовило активізацію різного роду злочинних елементів, особливо у сфері банківського шахрайства. За таких умов, банки, які своєчасно не врахували зростання активності злочинних елементів, не вжили адекватних заходів захисту кредитних операцій, зазнали серйозних втрат. Тут слід зауважити, що сьогодні кредитна діяльність банків здійснюється в умовах досить високого ризику, який за рівнем небезпеки створює для банків майже екстремальні умови;

— відсутність у технологіях кредитних операцій та методиках кредитування системних заходів захисту таких операцій, адекватного ситуації підходу до мінімізації ризиків їх проведення. Незважаючи на певний досвід банків і їх працівників у сфері кредитування, наявність у них відповідної нормативної бази, негативні показники від кредитної діяльності банків не зменшуються. У більшості випадків кредитні операції проводяться по шаблону, із застосуванням для захисту інтересів банку тільки певних видів забезпечення, що в сьогоднішніх умовах не завжди гарантує успіх;

— недосконаліть законодавчої бази для банківської діяльності взагалі і кредитної зокрема. Один із найактивніших і найризиковіших видів діяльності банків залишився без законодавчого регулювання. Загальні положення цивільного законодавства щодо кредитної діяльності банків не створюють сприятливих умов для ефективного забезпечення безпеки

— непрофесійні дії органів управління та персоналу банків щодо надання, і особливо супроводження, кредитів. Зусилля підрозділів установ банків не завжди сконцентровано в напрямі забезпечення безпеки кредитних операцій, а їхні дії не в повному обсязі бувають узгодженими і організованими. Посадові особи, задіяні у кредитній діяльності, не завжди мають об'єктивне уявлення про можливі загрози кредитним коштам при проведенні кредитних операцій, тому ефективність перевірки позичальників не в повною мірою забезпечує об'єктивну картину їх можливостей, стану та діяльності;

— недобросовісна поведінка, а подекуди і кримінальний характер діяльності позичальників. Як показує практика роботи правоохоронних органів, певна частина комерційних підприємств створюється заздалегідь задля протиправної, злочинної діяльності, направлену передусім на отримання коштів нечесним шляхом, у тому числі і незаконного отримання або використання кредитних коштів. Слід зауважити, що у ринковій економіці завжди існує ризик вкладання коштів як у банків, так і в підприємств. Тому на їх повернення впливатиме не тільки кримінальний характер діяльності позичальників, а й професійні якості та досвід роботи працівників підприємств, банків, поведінка контрагентів і партнерів, кон'юнктура ринку, зміни в правовому полі і т. п.

Усе наведене вище вказує на нагальну необхідність створювати певну систему заходів безпеки кредитних операцій банків.

Водночас досвід показує, що якоїсь єдиної системи заходів безпеки кредитних операцій, яка була б притаманна всім банкам, в Україні не існує. Усі банки, використовуючи існуючу законодавчу і нормативну базу, виробляють свої заходи і з тією чи тією ефективністю застосовують їх для захисту своєї кредитної діяльності.

Слід звернути увагу, що комерційним банкам надається право самостійно аналізувати, вивчати діяльність потенційних позичальників, визначати їх кредитоспроможність, прогнозувати ризик неповернення кредиту і приймати рішення про надання або відмову у наданні кредиту.

Як правило, заходи безпеки класифікуються за терміном

розвитку кредитних взаємовідносин банків з їх клієнтами: підготовка до надання кредиту і його надання, кредитний моніторинг у процесі кредитних операцій і робота щодо повернення кредитів. Особливо слід наголосити, що забезпечення безпеки кредитних операцій не є прерогативою чи завданням якогось одного підрозділу банку (наприклад, підрозділу безпеки), заходи безпеки реалізуються всіма підрозділами, задіяними у таких операціях. Досвід показує, що у проведенні кредитних операцій беруть участь, як правило, наступні підрозділи банків: кредитні, юридичні, маркетингові, банківських ризиків, безпеки, які є основними у забезпеченні заходів безпеки таких операцій. Інші підрозділи (ресурсні, фінансово-економічні, бухгалтерського обліку і т.п.) хоч і беруть участь у кредитній діяльності банків, але вона суттєвого впливу на забезпечення безпеки кредитних операцій не створює.

Під час підготовки до видачі кредиту основними заходами захисту кредитної операції можуть бути: інформаційно-аналітичне дослідження позичальників; колективне формування рішення про надання кредиту й індивідуальна відповідальність за повернення кредитних коштів; забезпечення виконання кредитних зобов'язань позичальника; формування безпечних для банку умов надання кредиту. Якраз зазначені заходи мають бути включені до змісту технології проведення кредитної операції.

Оскільки етап підготовки і видачі кредиту є чи не головним у структурі кредитної операції, особлива увага звертається на визначення кредитоспроможності позичальника.

Практика роботи банків та досвідчені фахівці банківської справи вказують на те, що в цілому механізм оцінки кредитоспроможності потенційних позичальників — юридичних осіб складається з двох етапів:

- аналіз фінансового стану позичальників;
- аналіз якісних показників його діяльності.

Оцінка фінансового стану позичальника здійснюється через вивчення та аналіз дотримання останнім обов'язкових економічних нормативів діяльності, установлених законодавством України; обсягів та якості активів і пасивів; обсягів і структури прибутків і збитків позичальника; рівня формування резервів у режимі страхування ризиків можливих втрат від здійснення активних операцій; стану виконання потенційним клієнтом зобов'язань у минулому та їх стан на момент отримання чергової позики.

Основними елементами аналізу якісних показників діяльності позичальника є:

✓ аналіз кредитної та податкової дисципліни, а також історії його діяльності і розвитку (найбільш критичними для підприємства є перші три—п'ять років його діяльності);

✓ аналіз ринкової позиції позичальника та ступеня його залежності від змін в економіці країни чи галузі, в якій здійснює свою діяльність позичальник. Тут мають значення такі фактори, як місцезнаходження позичальника, вид діяльності, яку він здійснює, метод операцій (виробництво, торгівля, посередництво і т. і.), юридична форма позичальника, наявність державних замовлень та державної підтримки, макроекономічна ситуація на ринку позичальника та стан розвитку галузі, в якій він здійснює свою діяльність;

✓ аналіз ефективності менеджменту позичальника (наявність у менеджерів досвіду роботи та рівень їх професійної компетентності у ключових сферах управління: виробництві, фінансах, збуті, частота зміни керівництва позичальника, наявність та якість бізнес-плану, наявність позитивних аудиторських висновків);

✓ наявність забезпечення повернення кредитних коштів [31].

Підрозділи безпеки при проведенні кредитних операцій, як правило, здійснюють інформаційно-аналітичне їх забезпечення. Ураховуючи зазначені в попередніх розділах критерії, безпосередньо на етапі підготовки до видачі і при видачі кредиту підрозділи безпеки здійснюють інформаційно-аналітичне дослідження позичальника, змістом якого є формування його характеристики та показників діяльності. Така характеристика включає два розділи: загальний і спеціальний. Загальний розділ складають такі відомості про позичальника:

— дата заснування підприємства, його походження, код реєстрації, коли приступило до діяльності, вид продукції (послуг), ринок збуту, засновники та власники;

— форма власності, організаційно-правова форма;

— статутний капітал;

— юридична та фактична адреса;

— місце розташування підприємства (територія, окрема будівля, частина будівлі, поверх, кімната чи кілька кімнат, приватна квартира);

— номери службових, домашніх та мобільних телефонів керівників та основних менеджерів підприємства, його факси, електронні адреси;

— керівники підприємства (прізвище, ім’я та по батькові, посади), досвід роботи взагалі та на даному підприємстві, зокрема, кваліфікація;

— хто приймає остаточні рішення на підприємстві;

— кількість працівників;

— основний вид діяльності;

— реалізація продукції (послуг) і канали збуту (обсяги реалізації, основні споживачі);

— система виробництва (основні комплектуючі, сировина, постачання, обладнання і технологія, робоча сила);

— структура підприємства, наявність дочірніх підприємств та підприємств, в яких позичальник виступає засновником, співзасновником або співвласником;

— основні партнери;

— нерухома власність підприємства (земельні ділянки, будівлі, обладнання, комунікації та ін.).

Спеціальний розділ включає відомості про:

- наявність осіб зацікавлених у позитивному вирішенні питання з кредитом;
- участь підприємства в державних програмах, наявність пільгових умов для ведення своєї діяльності в рамках конкретних програм;
- наявність на підприємстві служби безпеки, хто її очолює;
- взаємовідносини з кримінальним світом, правоохоронними органами, органами податкової служби, місцевої влади, наявність фактів розгляду справ у судах як за позовами підприємства, так і за позовами до нього;
- плинність кадрів;
- фактичну наявність підприємства, його офісів, місце проживання керівників і провідних менеджерів підприємства за вказаними адресами, факт виробничої діяльності підприємства;
- наявність на дочірніх підприємствах, підприємствах, де позичальник є засновником (співзасновником), власником (співвласником), підприємствах, з якими позичальник здійснює контрагентські або партнерські зв’язки, родичів, близьких, друзів керівників позичальника, його засновників або власників, а також працівників банку;
- кредитну історію позичальника (користування кредитами, яких банків, як і за яких умов поверталися кредити, досвід роботи з позичковими коштами);
- повноваження керівників та керівних органів щодо отримання кредитів;

• особи керівників, засновників та власників підприємства, крім тих, які входять до складу загальних відомостей (вік, посада, освіта, попередні місця роботи, сімейний стан, близьке оточення, житлові умови, наявність автотранспорту, корінні жителі чи іногородні або іноземці, якщо не корінні жителі, то на яких умовах проживають, спосіб життя, морально-етичні якості, вади і пристрасті, особливості характеру: агресивність, авторитарність, імпульсивність, комунікабельність, ділова репутація).

Крім питань, пов'язаних з інформаційно-аналітичним дослідженням позичальника підрозділ безпеки здійснює перевірку наданих документів з точки зору їх достовірності. Ураховуючи можливості підрозділів безпеки банків та існуючі правові умови їхньої діяльності ці заходи передбачають уточнення таких питань: чи складено документ за встановленою формою, чи має він необхідні реквізити (назву документа, дату складання, підписи посадових осіб, зрозумілий зміст). До неправильно оформлених документів можуть бути віднесені документи, на яких не були заповнені всі реквізити, підписано не особою, яка має повноваження підписувати такі документи, порушено спосіб заповнення документа, допущено виправлення в тексті.

Слід зазначити, що документи можуть бути оформлені правильно, але вони вважатимуться недійсними, якщо в них неправильно відображені виконані матеріальні операції, вказані фактично не здійснені (фіктивні) операції, включено підставних осіб. Окремі методи перевірки документів наведено в Додатку 12.

Залежно від повноти отриманої інформації, її змісту та достовірності підрозділ безпеки визначає ризик помилки вибору позичальника. При цьому для визначення зазначеного ризику може бути використано методики, подані на стор. 210—211 даного видання.

Установлення відповідного ступеня ризику помилки вибору позичальника суттєво впливатиме на характеристику його надійності і надалі на рішення про надання кредиту.

Юридичні підрозділи на даному етапі кредитної операції вивчають правомірність існування та діяльності підприємства-позичальника, наявність документів, наданих позичальником, та їх відповідність установленим у банку вимогам, забезпечують правову оцінку договорів позичальника з контрагентами в рамках реалізації його бізнес-плану, готують проекти кредитних та інших договорів, пов'язаних з проведенням банками кредитних операцій, здійснюють їх реєстрацію, облік та зберігання

оригіналів договорів.

Кредитні підрозділи на етапі підготовки до надання кредитів вивчають загальний стан підприємства-позичальника, його фінансові показники (ефективність, реалізація — прибуток, капітал, ліквідність), матеріали аудиту, кредитоспроможність позичальника, залежність позичальника від кредитних коштів (постійна, час від часу, тільки для реалізації даного проекту), уточнюють, як розрахована сума кредиту, та складають прогноз фінансових потреб, визначають, для чого конкретно буде використано кредит, чи враховано умови, на яких буде надано кредит, причини клопотання про отримання кредиту саме в цьому банку.

Крім того, кредитний підрозділ проводить оцінку бізнес-проекту позичальника у процесі якого аналізує структуру і динаміку витрат (за власними і позичковими коштами), календарний план організації робіт, динаміку випуску і реалізації продукції (робіт, послуг), розрахунок окупності, прибуток (у динаміці), рентабельність, структуру собівартості продукції, терміни та графіки окупності вкладень і повернення коштів банку.

Додатково кредитні підрозділи вивчають такі питання:

- як клієнт планує погашати кредит і в якому порядку;
- обсяги коштів, які клієнт отримує у процесі операційного циклу;
- чи має клієнт спеціальне джерело погашення кредиту.

Підрозділи маркетингу на зазначеному етапі вивчають кон'юнктуру ринку позичальника, визначають умови, рівень конкуренції на ньому, конкурентоспроможність позичальника та його перспективи на період дії кредитного договору, установлюють можливість змін кон'юнктури ринку протягом користування позичальником позичковими коштами, основних його конкурентів і ступінь їх впливу на позичальника у процесі комерційної діяльності, а також перспективність даного виду бізнесу.

Підрозділи банківських ризиків під час підготовки до видачі та видачі кредиту проводять дослідження забезпечення кредиту. Залежно від виду забезпечення вони:

- вивчають предмет застави, визначають його наявність, право власності заставодавця на нього, вартість (балансову та ринкову), його ліквідність, у тому числі і можливі зміни на момент повернення кредиту, склад і стан предмета застави, умови зберігання та умови страхування, чи не перебуває предмет

- вивчають можливості гарантів (поручителів), їх платоспроможність та повноваження осіб, що підписують документи про надання гарантії (поручительства), відповідність гарантії (поручительства) вимогам законодавства;
- вивчають можливості та платоспроможність страховиків, їх повноваження та умови страхування.

На основі отриманих від позичальника документів та даних інших підрозділів, задіяних у роботі з підготовки до видачі кредиту, підрозділи банківських ризиків досліджують надійність позичальника та визначають ступінь ризику банку при проведенні даної кредитної операції. Досвід забезпечення безпеки кредитних операцій банків показує, що вивчення і прогнозування стану підприємства-позичальника та ризику, пов'язаного з наданням кредиту, здійснюється на основі дослідження п'яти груп коефіцієнтів та їх динаміки: показники ліквідності, показники заборгованості, показники погашення боргу, показники ділової активності, показники рентабельності.

Відповідно до існуючих у тому чи тому банку порядку та методики підрозділи, задіяні у підготовці кредитної операції, на основі результатів вивчення позичальника та його діяльності надають кредитному комітету висновки, в яких викладають своє бачення можливості, умов, розміру надання кредиту та перспектив його повернення. Кожен із підрозділів має безпосередньо у своєму висновку вказати один із таких варіантів: можна надати кредит, відмовити в наданні кредиту, можна надати кредит за відповідних умов. Підрозділи банківських ризиків крім цього вказують можливий ступінь ризику банку при проведенні даної кредитної операції.

Усі документи від підрозділів банку отримуються кредитним інспектором, який вивчає їх і складає пояснювальну записку кредитному комітету, в якій відбиває сильні та слабкі сторони кредитної угоди, обґрунтовує деталі угоди, які не відповідають традиційній практиці банку, робить загальний висновок про можливість надання кредиту. Кредитний інспектор формує пакет документів щодо даної кредитної угоди і подає їх керівникові кредитного підрозділу, який перевіряє повноту документів, визначає якість аналізу кредитної заявки, підписує пояснювальну записку та направляє документи кредитному комітету.

Розгляд документів і прийняття рішення кредитними комітетами та керівництвом банку здійснюється відповідно до

порядку, установленому у кожному з банків.

Після прийняття позитивного рішення про надання кредиту і перерахування коштів на позичковий рахунок клієнта починається другий етап забезпечення безпеки кредитної операції, а саме — етап супроводження кредитної операції (кредитний моніторинг). Як показує досвід, якраз з причин недостатньо ефективного моніторингу кредитних операцій створюються досить негативні ситуації щодо повернення кредитних коштів.

Супроводження (кредитний моніторинг) кредитних операцій обов'язково має бути персоналізовано і також включати певні елементи захисту операцій. Це, по-перше, контроль виконання умов кредитної угоди (обов'язковий, конкретний і комплексний); по-друге, моніторинг ділової ситуації в діяльності позичальника; по-третє, адекватна реакція банку на зміну ситуації як в умовах діяльності позичальника, так і в його поведінці, у тому числі і керівників, і власників; по-четверте, санація кредитної угоди у разі виявлення ознак загрози кредитній операції. Під санацією тут розуміють спільні дії позичальника і банку щодо правового, фінансового, матеріального, інформаційного та інших питань вирішення проблем, що виникають у ході операції.

Метою кредитного моніторингу є виявлення ознак і обставин, які вказують на зміни умов виконання кредитної угоди і реалізації проекту позичальника, своєчасне вжиття заходів щодо повернення позичкових коштів. Досвід роботи банків показує, що до змісту кредитного моніторингу входять такі заходи контролю:

— контроль за цільовим використанням кредиту, платоспроможністю позичальника;

— контроль за виконанням графіка погашення кредиту і процентів за ним;

— контроль за наявністю і станом предмета застави, поведінкою і станом гарантів (поручителів) і страховиків;

— контроль за діяльністю партнерів (контрагентів) позичальника, поведінкою його керівників;

— контроль за ситуацією на ринку позичальника (у тому числі і правовою), змінами його кон'юнктури, господарською діяльністю та діловою активністю позичальника, його поведінки на ринку;

— контроль зв'язків позичальника.

При виявленні змін в умовах виконання кредитних угод або в діяльності позичальника, можуть плануватися і реалізовуватися

заходи, направлені на нейтралізацію проблемних ситуацій, які виникають у позичальника унаслідок сумісних його дій із банком. У деяких випадках вживаються заходи направлені на стимулювання дій позичальника щодо дотримання графіка погашення кредиту.

Основними ознаками, які можуть вказувати на можливість виникнення проблем з поверненням кредитів і які можуть бути виявлені у процесі кредитного моніторингу є:

- конфліктні ситуації в колективах підприємства-позичальника, його керівництві, у відносинах позичальника з його партнерами і клієнтами;
- суттєві зміни у структурі підприємства-позичальника, створення дочірніх та заснування інших підприємств з переданням у їх власність частки активів позичальника, зміни в кадровому забезпеченні, звільнення з роботи провідних фахівців і посадових осіб керівного складу;
- втрата позичальником клієнтів і партнерів, закриття філій, розпродаж майна;
- розрив на невизначений час договорів оренди;
- виїзд керівників підприємства-позичальника і членів їхніх сімей за кордон, розпродаж ними особистого майна;
- призупинення робіт щодо реалізації бізнес-проекту;
- наявність ознак порушення законодавства позичальником, його зв'язків з кримінальним світом;
- здійснення проплат з нових рахунків, повна відсутність коштів на рахунках протягом певного часу, погіршення фінансових показників позичальника (зниження прибутку, зменшення обсягів реалізації товару, посилення залежності від позичкових коштів, зменшення обсягів обігових коштів);
- затримки в наданні в банк фінансових звітів, прострочення основних платежів банку, погіршення взаємовідносин з банком (відмова від зустрічей, нема відповіді на телефонні дзвінки, уникнення відвідування банку);
- запити від інших банків, пов'язані з намірами позичальника отримати в них нові кредити;
- сімейні проблеми посадових осіб керівництва підприємства-позичальника (розлучення, виконання судових рішень, серйозні хвороби близьких та інші ситуації пов'язані з необхідністю додаткових витрат).

Подібні ознаки виявляються у процесі роботи всіх підрозділів банку, задіяних у моніторингу кредитної операції.

Кредитні підрозділи банків контролюють виконання графіка

погашення кредиту та сплати процентів, його цільове використання, фіксують наявність затримок у наданні банку відомостей і звітів, проводять аналіз поточної фінансової документації. Крім того, кредитними підрозділами періодично проводяться перевірки безпосередньо на підприємстві позичальника, зокрема перевіряється надходження матеріальних цінностей, придбаних за позичкові кошти, реальність виробничої діяльності щодо реалізації бізнес-проекту.

Підрозділи безпеки у процесі кредитного моніторингу здійснюють контроль поведінки позичальника, його ділової активності, появи нових комерційних зв'язків, загального режиму діяльності підприємства (кадрові зміни, конфліктні ситуації як на підприємстві, так і зовні його, зміни в організації виробництва і т. п.), наявність негативних відгуків про діяльність підприємства чи його власників або керівництва в засобах масової інформації, про поведінку керівників і засновників (власників) підприємства, їх здатність забезпечити належний стан і перспективи діяльності підприємства. Підрозділи безпеки тримають у полі зору соціальну ситуацію на підприємстві — позичальника, його взаємовідносини з правоохоронними органами, й особливо податковою службою.

Юридичні підрозділи здійснюють контроль правової ситуації з питань кредитування та вживають заходів щодо захисту інтересів банку у разі її змін. Крім того, вони забезпечують контроль дотримання позичальником установлених у договорах умов виконання зобов'язань та згідно з рішеннями керівних органів банку здійснюють юридичне оформлення змін виконання сторонами своїх зобов'язань або умов їх забезпечення.

Підрозділи банківських ризиків насамперед здійснюють вивчення ситуації щодо стану забезпечення повернення кредиту. Зокрема, з питань, що стосуються застави: чи не перезаставлено предмет застави, умови зберігання і стан предмета застави, чи не реалізовано (замінено), украдено предмет застави, дотримання передбачених договорами умов використання (експлуатації, оновлення) предметів застави.

У разі, якщо у заставі майнові права позичальника, підрозділи банківських ризиків контролюють терміни і ситуацію, коли майнові права позичальника перетворюються у конкретну продукцію і вживають заходів щодо прийняття останньої в заставу.

Щодо гарантів (поручителів), страховиків підрозділи банківських ризиків здійснюють контроль їх фінансового стану

та можливостей щодо виконання своїх зобов'язань.

Підрозділи маркетингу контролюють ситуацію на ринку позичальника, стан та зміни конкурентоспроможності його продукції, появу на ринку нових суб'єктів, здатних обмежити діяльність позичальника, зміни кон'юнктури ринку.

Проведення моніторингу фахівці банків радять здійснювати у такому порядку:

а) *перший етап* — визначення відповідності використання кредитних коштів меті, передбаченій кредитним договором, реальності придбання матеріальних цінностей за кредитні кошти, ознак намірів позичальника використати у подальшому кредитні кошти не за призначенням.

На даному етапі перевіряються документи, які можуть підтверджувати цільове використання кредиту. Такими документами можуть бути платіжні доручення, рахунки-фактури, митні декларації, складські розписки, довіреності і т. п. Ці документи повинні підтверджуватися наявними товарно-матеріальними цінностями. Досвід показує, що з зазначених документів доцільно знімати копії, які надалі включати до кредитної справи позичальника;

б) *другий етап* — перевіряються наявність і умови реалізації продукції та її зберігання. При цьому враховується відповідність ціни реалізації продукції передбаченій ціні у бізнес-плані, можливість оптової та роздрібної реалізації, наявність складських приміщень, мережі торгових пунктів, зміни кон'юнктури ринку, законодавства, оподаткування та ін.

Головна мета перевірки у процесі другого етапу — переконатися в реальності здійснення угоди й отримання позичальником доходу, який би дозволяв повернути банку кредитні кошти і проценти за їх використання;

в) *третій етап* — установлюється, чи реалізовано товар, чи до його реалізації позичальник ще не приступав, на що направлені дії позичальника: на повернення кредитних коштів, пролонгацію терміну дії кредитного договору, неповернення кредиту взагалі чи щось інше.

У кожному окремому випадку на кожному з етапів установлюються відповідні графіки проведення перевірок діяльності та документів позичальників.

Усі перевірки починаються з аналізу інформації, отриманої згідно з встановленим порядком від позичальника, після чого визначаються результати виконання угод за даними бухгалтерського обліку, проводяться виписки із розрахункових

рахунків, перевіряються дані журналів-ордерів за відповідними рахунками, книги обліку реалізації продукції. У разі необхідності проводяться переговори з керівництвом підприємства-позичальника, де уточнюються можливості щодо своєчасного погашення кредиту.

Крім того, перевіряється наявність застави, її стан та умови зберігання, а за певних умов — фінансовий стан гаранта (поручителя), страховика. На даному етапі досить важливим є вивчення характеру ділових відносин позичальника з іншими юридичними і фізичними особами, особливо усвідомлення суті їх фінансово-господарських відносин. Слід переконатися, що серед таких осіб відсутні підозрілі, фіктивні підприємства та фізичні особи (родичі, друзі, кримінальні елементи і т. п.). Доцільно також звернути увагу і на наявність фактів виділення зі складу структури підприємства позичальника підрозділів у самостійні юридичні особи, створення дочірніх підприємств, заснування інших суб'єктів господарювання та отримання корпоративних прав на підприємствах, які не входять до структури позичальника;

г) *четвертий етап* — настання терміну повернення кредиту.

Якщо кредит не повернуто і є клопотання позичальника про пролонгацію, робота щодо прийняття такого рішення проводиться практично у тому самому обсязі, що й при підготовці до надання кредиту. Слід зауважити, що пролонгація кредитів не тягне за собою автоматичного продовження терміну дії договорів забезпечення. Тому в обов'язковому порядку такі договори мають бути також пролонговані.

Коли кредит переведено до категорії прострочених, робота банку щодо повернення боргу може проводитись у такому порядку:

— доарбітражне врегулювання предмета спору:

- надання претензій боржникові;
- повідомлення страховиків (гарантів, поручителів) про невиконання позичальником своїх зобов'язань;
- модифікація кредитної угоди, санація кредитної угоди (сек'юритизація — продаж повністю або частково виданого кредиту, факторингові операції, капіталізація банком боргу позичальника і т. п.); реструктуризація кредитного боргу і терміну його повернення;
- реалізація забезпечення;
- надання позову до господарського суду;
- виконання судового рішення;

• банкрутство позичальника.

На даному етапі крім зазначеного вище особливе значення, як показує досвід роботи сил безпеки банків, має забезпечення додаткового впливу на боржників з метою стимулювання їхніх дій до повернення кредитних коштів. Насамперед слід вжити заходів щодо правового впливу, зокрема, використовуючи цивільно-правові або кримінально-правові засади.

У першому випадку виходячи з ситуації, яка складається з неповерненням коштів і необхідності обмежити діяльність боржника, особливо його дій щодо витрат коштів та реалізації майна, доцільно провести відповідні цивільно-правові процедури щодо накладання арешту на активи боржника та отримання законного права на управління його майном. Найбільш ефективним у цьому разі може бути використання інституту банкрутства без будь-яких попередніх заходів цивільно-правового характеру. У процесі процедури банкрутства право управління активами боржника переходить до арбітражного керуючого, основним завданням якого є формування сум коштів для повернення кредиторам боржника, у тому числі і за рахунок його майна.

За інших умов дійовим може бути прагнення банку до здійснення виконавчого напису на договорі застави та ініціювання роботи виконавчої служби. Є приклади, коли вже на цьому етапі боржники змінюють свою позицію та вдаються до дій щодо вирішення питання з погашенням боргу.

Для застосування кримінально-правових засад характерним є наявність у діях позичальника ознак порушень законодавчих норм кримінального спрямування. Такими порушеннями можуть бути: нецільове використання позичальником кредитних коштів, продаж або передання без відома банку предмета застави, розтрата будь-яким чином отриманих коштів, привласнення (або придбання незаконним способом) майна придбаного за кредитні кошти, обман кредитора та ін. У практичному плані дії банку щодо збору таких фактів будуть направлені на створення відповідної системи розмежування правомірного підприємницького ризику від неправомірного діяння, яке карається у кримінальному порядку. Маючи докази про зловживання позичальника, банк має підстави звернутися до правоохоронних органів із заявою про порушення кримінальної справи щодо такого позичальника, що саме по собі може спонукати останнього до повернення кредиту. Крім того, у разі порушення кримінальної справи з'являється можливість

обмежити позичальника у пересуванні і позбавити його можливості переховуватись або оголосити його розшук, накласти арешт на наявне у нього майно, предмети застави і т. п. До того ж у рамках кримінальної справи банк може заявити себе цивільним позивачем на суму непогашеного боргу.

У процесі роботи з повернення кредитних боргів концентруються зусилля всіх підрозділів банку, які беруть участь у кредитній роботі. Водночас усі вони розмежовують свою діяльність за такими напрямками:

а) кредитні підрозділи — проводять розрахунок суми заборгованості та надають його до юридичних підрозділів для проведення претензійної роботи, складають довідку про прострочений кредит і розробляють план заходів щодо його повернення, розробляють заходи санації кредитної угоди або такі, що пов'язані з погашенням боргу іншими способами економічного характеру (продажем боргу, його капіталізацією, уступкою права вимоги, процедурою банкрутства або ліквідації боржника);

б) підрозділи банківських ризиків — повідомляють страховиків, гарантів, поручителів про невиконання позичальником своїх зобов'язань та ведуть роботу з ними, здійснюють перевірку наявності предметів застави, визначають їх ліквідність та забезпечують виконання виконавчого напису на договорах застави, крім того, здійснюють взаємодію з органами виконавчої служби щодо погашення боргу через реалізацію предметів застави та майна боржників;

в) юридичні підрозділи — забезпечують претензійно-позовну роботу щодо боржників, представляють банки у судах у справах щодо погашення боргів, ведуть облік проведеної роботи та оскарження судових рішень, у яких порушено права банків у судах вищої інстанції;

г) підрозділи маркетингу — здійснюють аналіз кон'юнктури ринку продажу предметів застави та майна боржників, визначають інтереси конкурентів боржників банків щодо їх активів, забезпечують рекламне супроводження реалізації предметів застави та майна боржників із прилюдних торгів;

д) підрозділи безпеки — забезпечують пошук прихованих коштів, майна та інших джерел для погашення кредитної заборгованості позичальників, фактів кримінальних дій посадових осіб підприємств-позичальників, їхніх дебіторів та визначення можливостей відшкодування завданих банку збитків за рахунок дебіторської заборгованості позичальників, беруть

участь у роботі з повернення боргів іншими способами.

Таким чином, забезпечення безпеки кредитної діяльності банків — досить складний і трудомісткий процес, необхідної ефективності він може досягти тільки завдяки активним спільним діям усіх підрозділів банку, які тим чи іншим чином задіяні в кредитних операціях. До того ж заходи безпеки повинні проводитися цілеспрямовано і наполегливо, з необхідним ступенем активності протягом усієї кредитної операції, а не тільки на якомусь одному її етапі.

Розглядаючи питання забезпечення безпеки кредитних операцій, слід звернути увагу на те, що банки здебільшого здійснюють кредитну роботу досить шаблонно і традиційно. Елементи захисту кредитних операцій проводяться не як протидія можливим загрозам, а як традиція кредитної діяльності. Робота банківських підрозділів недостатньо сконцентрована навколо кожної кредитної операції та проблем, які виникають щодо неї, кожен підрозділ працює відокремлено. Результат такого підходу виявив себе під час фінансової кризи 2008—2009 рр. Банки не здатні були протистояти загрозам і кредити в масовому порядку ставали для банків проблемними.

Аналіз такої ситуації дає підстави вважати, що головною причиною тут була відсутність концентрації роботи з попередження виникнення та забезпечення повернення проблемних кредитних боргів. За таких умов з погляду безпеки доцільно було б організувати кредитну роботу банків у порядку, вказаному на рис. 9.4.

Рис. 9.4. Робота банку з організації безпеки кредитної діяльності

Водночас особливості кредитної діяльності банків у сьогоднішніх умовах вказують на виникнення нового напряму кредитної роботи — управління проблемними кредитами, що обумовлено наявністю постійного сегмента проблемної заборгованості у структурі кредитного портфеля банків, який за своїми обсягами створює суттєву загрозу їхній діяльності.

Під проблемними кредитами розуміють заборгованість за банківськими кредитами, за якою своєчасно не проведено один чи більше платежів та внаслідок інших обставин виникають підстави щодо сумніву стосовно повернення кредиту взагалі. Основними ознаками проблемного кредиту є: порушення терміну повернення чергового платежу за кредитом; зниження ринкової вартості предметів забезпечення; фінансові проблеми гарантів, поручителів, страховиків; призупинення робіт з виконання проектів, що фінансуються за кредитні кошти; непорозуміння позичальника зі своїми постачальниками, партнерами та

контрагентами; реорганізація суб'єкта господарювання позичальника; звернення позичальника за додатковими кредитами, припинення контактів із працівниками банку; безпричинне порушення графіка звітності про використання кредитних коштів; наявність збитків у діяльності позичальника; зниження ділової активності його діяльності і т. п. Якраз ці та інші ознаки вказують на виникнення фінансових труднощів у позичальника, непорозумінь у взаємовідносинах з партнерами по бізнесу, виробництву чи збуту, порушень стабільності в його роботі, особливо тієї її частини, що фінансується за банківські кошти. Така сукупність умов, що складається в діяльності позичальника, однозначно негативно впливатиме як на його стан і можливості, так і на формування перспектив подальшого функціонування. Тобто при визначенні проблемних кредитів необхідно розглядати сукупність негативних умов, обставин, що складаються навколо діяльності позичальника, пов'язаної з використанням кредитних коштів. Саме такі умови, обставини, дії і будуть тими ознаками, що мають вказувати на формування певних проблем у позичальника, пов'язаних із поверненням кредиту.

Питання управління проблемним кредитом слід розглядати саме з моменту його появи, тобто наявності в його характеристиках таких ознак, як, наприклад, прострочений термін повернення, відсутність можливості (бажання) у позичальника повернути кредит, зниження ринкової вартості предмета застави (відсутність предмета застави), неадекватна поведінка страховиків, гарантів, поручителів та ін. Національний банк України за визначеними ним показниками відносить такі кредити до прострочених і сумнівних.

Управління проблемними кредитами має починатися з їх ідентифікації у структурі кредитного портфеля. Ідентифікація якраз і спрямована на виявлення зазначених ознак у характеристиках кредитної заборгованості позичальників банків. Вона має проводитися час від часу в банках відповідно до встановленого графіка. У разі ж виявлення таких кредитів, як непоодинокі випадки, але в той же час за умов, що такі кредити не перевищують 10% структури кредитного портфеля (за іноземним досвідом питома вага нестандартних кредитів у структурі кредитного портфеля в 10% має вказувати на кризове становище банку [104]), управління проблемними кредитами може здійснюватися методами реабілітації чи ліквідації.

Під реабілітацією розуміється спільна з позичальником робота банку, спрямована на зміну умов кредитної угоди, за яких можливе створення ситуації коли позичальник матиме можливість розрахуватися з банком. До таких умов можна віднести пролонгацію кредитної угоди, реструктуризацію кредитного боргу, санацію кредитної угоди банком або іншими особами, проведення заходів, спрямованих на підвищення ліквідності позичальника, реорганізацію суб'єкта господарювання, тимчасове передання управління діяльністю суб'єкта господарювання особам, що залучені (запропоновані) банком, капіталізацію боргу та ін. Звичайно, метод реабілітації буде характерним лише для тих умов, коли і банк, і його боржник знаходять необхідне порозуміння стосовно вирішення проблем повернення кредитних коштів. Очевидним є і те, що для реалізації такого методу банки у своїй діяльності повинні виділити спеціальний напрям роботи з формуванням для цього спеціальних сил та засобів. Фахівці, залучені до такої роботи, повинні мати досвід кризового управління діяльністю суб'єкта господарювання. Вважається, що застосування цього методу може бути доцільним за умов, коли ймовірність повернення кредитного боргу від заходів реабілітації становить 90% і більше. Враховуючи, що подібні розрахунки провести досить складно, а методик, за допомогою яких можна було б ефективно їх скласти, практично не існує, фахівці банків при обранні методу реабілітації покладаються здебільшого на свою інтуїцію. Хоча тут слід зауважити, що даний метод може застосовуватись у тих випадках, коли у боржника є необхідні активи, збережено виробничу і комерційну діяльність та є добра воля до порозуміння з банком.

Основу застосування зазначеного методу управління кредитним боргом становить план реабілітації кредитної угоди (повернення кредиту). Цей план спрямований на виконання заходів, пов'язаних з усуненням причин, що унеможливлюють або утруднюють повернення кредиту та формування умов щодо повного його повернення.

Розробленню зазначеного плану передує ретельне вивчення та аналіз умов, що склалися навколо кредитної угоди та діяльності позичальника. За результатами вивчення та аналізу зазначених умов формується рішення про відповідні спільні дії позичальника та банку, серед яких:

- пролонгація кредитної угоди: здійснюється тоді, коли у позичальника виникли тимчасові труднощі, не пов'язані з

• реструктуризація кредитного боргу, тобто зміна графіка платежів і терміну повного повернення боргу: здійснюється, коли у позичальника немає можливостей на даний час повернути кредитний борг у повному обсязі, але його діяльність забезпечує можливість здійснити необхідні платежі банку протягом певного терміну;

• санація кредитної угоди: може проводитися банком або за його згодою іншою особою, коли діяльність позичальника є перспективною та здійснюється з позитивними тенденціями, але для завершення економічного проекту, фінансування якого проводиться за рахунок кредиту, бракує коштів. У цьому разі банк може докредитувати зазначений проект, взяти участь у фінансуванні проекту або ж зробити це, залучивши третіх осіб, диверсифікувавши у такий спосіб власні ризики;

• проведення заходів з підвищення ліквідності позичальника: здійснюється тільки на підставі істинних і чесних намірів повернути кредитний борг з боку керівництва позичальника. Серед зазначених заходів будуть такі, як скорочення витрат, пов'язаних з діяльністю позичальника (скорочення персоналу, відмова від оренди, певних послуг, обмеження чи припинення низькорентабельних, ризикових чи збиткових для позичальника операцій, реструктуризація інших боргових зобов'язань позичальника та ін.), повернення дебіторської заборгованості, повернення депозитів, продаж цінних паперів, які мають активний ринок, повернення коштів, укладених позичальником для формування статутного капіталу інших суб'єктів господарювання, продаж активів позичальника або ж деяких його філій і т. п.;

• реорганізація суб'єкта господарювання — позичальника банку: здійснюється за згодою його власників. Реорганізація проводиться без процедури банкрутства та ліквідації боржника як юридичної особи. Якщо в результаті реорганізації (злиття, приєднання, перетворення) буде змінено назва та організаційно-правова форма суб'єкта господарювання необхідно передбачити, щоб новий суб'єкт став правонаступником боргових зобов'язань позичальника за неповернутим кредитом;

• тимчасове передання управління діяльністю суб'єкта господарювання — боржника банку особам, залученим

• капіталізація боргу: передбачає отримання банком частки корпоративних прав на володіння підприємством боржника на суму, що дорівнює сумі боргу. Такі дії можливі тоді, коли причинами неповернення боргу є тимчасові негаразди позичальника, але його бізнес є перспективним і здійснюється в одній із бізнес-привабливих сфер. Надалі борг може бути погашеній коштами від прибутку, що його отримає банк як співвласник підприємства-боржника, або від продажу своєї частки корпоративних прав.

Метод реабілітації, як уже зазначалося вище, досить трудомісткий і складний, потребує наполегливої роботи не одного підрозділу банку протягом тривалого терміну. Тому розраховувати на те, що управління проблемним кредитом через його реабілітацію обов'язково принесе позитивні результати, можна тільки у разі цілеспрямованої, активної та тривалої роботи значного колективу.

Якщо ж коли реабілітація кредиту не дає позитивних результатів або зразу після аналізу кредитної заборгованості очевидно, що борг таким способом повернути не можна, банк удається до другого методу — ліквідація боржника. У процесі цього методу забезпечення повернення боргу банк здійснює через кредиторські вимоги до підприємства банкрута. Зауважимо, що банкрутство та ліквідація боржника — це останній шанс банку повернути хоч би які кошти від проблемного кредиту.

Ініціювання банкрутства може здійснюватись як самим банком, так і іншими суб'єктами, перед якими позичальник

також має борги. У разі ініціювання банком процедури банкрутства боржника банк має пропонувати суду кандидатуру свого арбітражного керуючого, з тим щоб забезпечити контроль за процедурою банкрутства та ліквідації. Коли ж ініціатива банкрутства не належить банку і йому не вдається лобіювати призначення свого кандидата арбітражним керуючим боржника, банк має ініціювати формування відповідного органу від кредиторів для нагляду за процедурою банкрутства та ліквідації, наприклад Комітету кредиторів, і по можливості очолити його. За всіх умов необхідно створити ситуацію, за якої арбітражний керуючий повинен періодично інформувати кредиторів про хід процедури банкрутства (ліквідації) та розрахунків із кредиторами.

У процесі банкрутства чи ліквідації арбітражним керуючим може бути прийняте рішення про реорганізацію боржника, у цьому разі необхідно забезпечити контроль за тим, щоб усі обов'язки боржника (у тому числі і за кредитом банку) перейшли до його правонаступника.

У деяких випадках боржники, намагаючись уникнути сплати кредитних боргів удаються до так званого фіктивного банкрутства, ініціюючи власне банкрутство в судах. Тут слід пам'ятати, що ознаки фіктивного банкрутства можуть бути виявлені в тому разі, якщо на дату подання заяви в суд у боржника були можливості задовольнити вимоги кредиторів у повному обсязі. Ці можливості розраховуються у такий спосіб: якщо ступінь платоспроможності боржника за поточними зобов'язаннями мала значення менше чи рівне трьом місяцям, то у боржника були всі умови та підстави для розрахунків з кредиторами в повному обсязі. У разі коли ж ступінь платоспроможності боржника за поточними зобов'язаннями перевищував ці значення, для таких підприємств має перевірятися значення коефіцієнта поточної ліквідності [104].

За всіх умов коли ж банк вдається до погашення боргу через ліквідацію боржника, можна говорити, що він уже зазнав збитків і не тільки у фінансовому плані, а й у плані свого іміджу, оскільки доведення ситуації до ліквідації власних клієнтів вказуватиме на недостатній рівень управління кредитною діяльністю (кредитними ризиками) банку.

Певні особливості управління проблемними кредитами виникають, коли їх частка в кредитному портфелі банку перевищує 10%. Така ситуація виникає, коли до банків застосовуються заходи фінансового оздоровлення або ж

призначається тимчасова адміністрація. У цих випадках управління проблемними кредитами починається з інвентаризації кредитного портфеля з метою об'єктивного визначення частки проблемних кредитів та їх класифікації відповідно до методів роботи з ними.

Насамперед визначається частка проблемних кредитів, повернення яких може бути забезпечене проведенням заходів правової роботи. Це передусім кредити, за якими не закінчений термін позовної давності, кредити, боржники яких мають відповідні активи, але повністю чи в частині не погоджуються з вимогами банку, кредити при використанні яких посадові особи боржників допустили порушення чинного законодавства, кредити повернення яких може бути забезпечене через проведення виконавчого провадження.

До другої категорії належать проблемні кредити, повернення яких може бути забезпечене різного роду економічними заходами.

Ще одну категорію становитиме частка проблемних кредитів, які доцільно передати колекторним підприємствам для роботи щодо їх повернення. Сюди ж можуть належати проблемні борги, які будуть пропонуватися до реалізації або уступки права вимоги на них.

Ще одна категорія проблемних боргів — це борги безнадійні до повернення, тобто ті, які не мають ніяких перспектив повернення і підлягають списанню на витрати банку або за рахунок сформованих ним страхових резервів. Визначення безнадійної заборгованості має здійснюватися відповідно до Податкового кодексу України [63]. Зокрема до безнадійної заборгованості належить:

— заборгованість за зобов'язаннями, за якою минув строк позовної давності;

— прострочена заборгованість, яка виявилася непогашеною внаслідок недостатності майна фізичної особи, за умови, що дії банку, направлені на примусове стягнення майна позичальника, не призвели до повного погашення заборгованості;

— заборгованість, яка виявилася непогашеною внаслідок недостатності майна:

• суб'єктів господарювання, оголошених банкрутами у встановленому законом порядку або знятих з реєстрації як суб'єктів господарювання у зв'язку з їх ліквідністю;

— заборгованість, яка виявилася непогашеною внаслідок недостатності коштів, одержаних від продажу на відкритих аукціонах (публічних торгах) та в інший спосіб, передбачений умовами договору застави, майна позичальника, переданого у заставу як забезпечення зазначеної заборгованості, за умови, що

інші юридичні дії банку щодо примусового стягнення іншого майна позичальника не призвели до повного покриття заборгованості;

— заборгованість, стягнення якої стало неможливим у зв'язку з дією обставин непереборної сили, стихійного лиха (форс-мажору), підтверджених у порядку, передбаченому законодавством;

— прострочена заборгованість померлих фізичних осіб, а також визнаних у судовому порядку безвісно відсутніми, оголошені померлими або недієздатними, а також прострочена заборгованість фізичних осіб, засуджених до позбавлення волі.

Ураховуючи специфіку формування проблемного боргу та особливості роботи щодо його повернення, можна запропонувати алгоритм управління проблемними кредитами в банку, наведений на рис. 9.5.

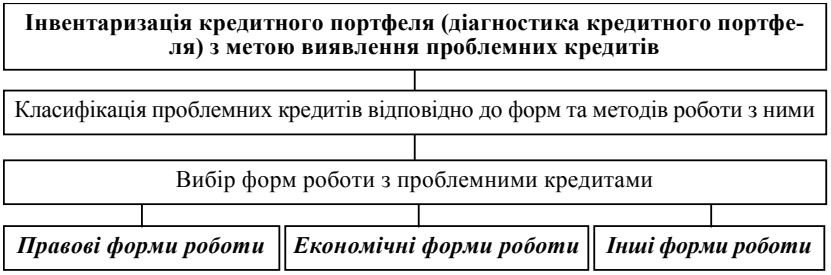

Рис. 9.5. Алгоритм управління проблемними кредитами в банку

Слід звернути увагу, що в управлінні проблемними кредитами важливе місце займають переговори з боржниками. Переговори — це перший і головний крок до порозуміння кредитора і боржника, саме під час переговорів знаходяться спільні інтереси сторін і способи вирішення проблемних питань.

З практики роботи банків можна дати деякі рекомендації з організації та методики проведення таких переговорів. Насамперед:

1. При проведенні переговорів слід прагнути, щоб у них брали участь тільки перші особи боржника або особи, які наділені правом приймати остаточні рішення.

2. До початку переговорів необхідно мати всю інформацію, що об'єктивно висвітлює історію утворення боргу, його обсяги, структуру, поведінку дебітора і т. п., а також слід виробити чітку позицію банку у справі про повернення боргу.

3. З боку банку в переговорах повинні брати участь не менше двох осіб.

4. Перед проведенням переговорів слід упевнитись у повноваженнях представників дебітора.

5. Наполягати на своїй позиції до максимально можливих меж, але мати компромісні варіанти рішень. Заперечувати щодо всіх питань, які обмежують права банку або в якимось інший спосіб суттєво зачіпають їх.

6. Не допускати проведення переговорів у кафе, ресторанах, лазнях із вживанням спиртних напоїв.

7. Вести протокол переговорів, усі досягнуті домовленості фіксувати в ньому або інших документах за підписом усіх учасників переговорів.

У разі, якщо переговори ведуться не по суті, неточно, затягуються, представники боржника не можуть погодитися з пропозиціями банку, а їх пропозиції не мають компромісного характеру, надалі їх проводити недоцільно.

Ураховуючи складність роботи з боржниками, особливо фізичними особами, банк має зробити все можливе, щоб зберегти взаємовідносини зі своїми клієнтами. Для цього він може розробляти та надавати своїм клієнтам відповідні рекомендації та пам'ятки стосовно поведінки в ситуації заборгованості перед банком. Прикладом тут є Пам'ятка позичальника, який має заборгованість перед банком за споживчим кредитом і потрапив у скрутне фінансове становище, розроблена Національним банком України (Додаток 13).

Важливою складовою управління проблемними кредитами є визначення сил і засобів для проведення роботи з такими кредитами. Насамперед, коли роботу з проблемними кредитами виділено в окремий напрям діяльності банку, для координації дій та керівництва такою роботою у банках, як правило, створюється відповідний дорадчий орган — Комітет, Комісія і т. п. Основними функціями зазначеного органу є організація діагностики (інвентаризації) кредитного портфеля

та класифікації проблемних кредитів, визначення конкретних завдань щодо роботи з кожним із кредитів, формування завдань відповідним підрозділам чи особам, контроль та координація виконання зазначених завдань, аналіз результатів роботи, вироблення нових підходів в управлінні (поверненні) проблемними кредитами.

Завдання з повернення кредитних боргів можуть бути покладені на відповідні підрозділи (кредитний, юридичний, безпеки, маркетингу, банківських ризиків). В окремих випадках із фахівців зазначених підрозділів, а також залучених фахівців можуть утворюватися відповідні тимчасові колективи (робочі групи) для безпосередньої роботи із проблемною категорією кредитних боргів. При цьому юристи займаються правовим напрямом роботи, кредитні фахівці — здійснюють роботу з економічного напряму, підрозділи (фахівці) банківських ризиків проводять роботу щодо повернення боргів за рахунок забезпечення кредитних угод (застава, страхування, гарантії, поручительство). Сили безпеки банку забезпечують взаємодію з колекторними підприємствами, правоохоронними органами, ведуть пошук прихованих боржниками активів, проводять роботу з їх дебіторами. Фахівці маркетингу вивчають кон'юнктуру ринку продажу боргів та майна боржників, контролюють вплив ситуації, що склалася в банку з проблемними боргами на його імідж.

Загалом же схема організації роботи з повернення проблемної заборгованості в банку має вигляд, показаний на рис. 9.6.

Таким чином, ефективність управління проблемними кредитами банку великою мірою залежить від якості організації роботи з ними, наполегливості й активності роботи всіх структур банку, формування сприятливих умов роботи залучених до цього сил, а також цілеспрямованої діяльності в цьому напрямі органів управління банку.

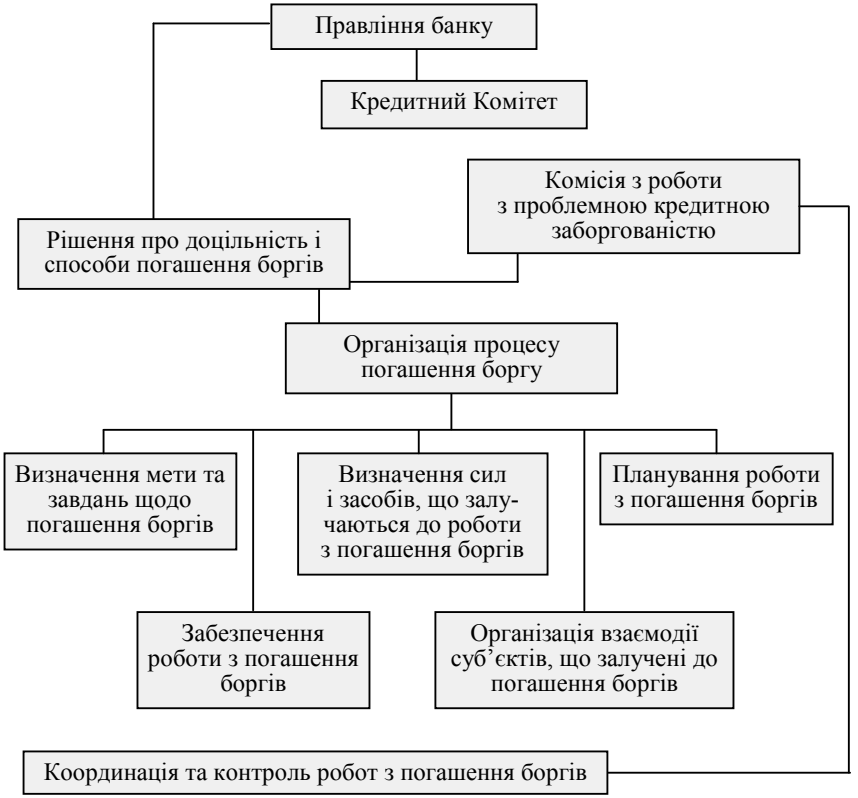

Рис. 9.6. Організація роботи банку з повернення проблемної кредитної заборгованості

Операції банку з цінними паперами. Оскільки банки ведуть свою діяльність у різних сферах фінансового ринку, забезпечення їх безпеки має здійснюватися незалежно від виду банківських операцій і перекривати всі можливі шляхи реалізації загроз. Більше того, чим складнішою є ситуація, тим активніше повинні діяти сили безпеки. Виходячи з цього підрозділи безпеки банків розробляють відповідні заходи щодо захисту всіх без винятку операцій, які проводять банки. При цьому значна увага приділяється забезпеченню безпеки роботи банків на фондовому ринку, особливо операціям з цінними паперами.

Операції з цінними паперами займають друге (після кредитних) місце за ступенем ризику. Якраз за цими операціями значна частина клієнтів банків і самі банки зазнають збитків,

втрачають можливості ефективного вкладання своїх коштів та отримання корпоративних прав перспективних підприємств. Саме діями шахраїв фондового ринку клієнти банків можуть отримати цінні папери безперспективних або неіснуючих емітентів, а в деяких випадках, вклавши кошти, і зовсім не отримати ніяких прав. Тому заходи безпеки банків насамперед спрямовуються на перевірку достовірності угод та відповідності стану емітентів заявленим умовам. Так, під час операцій банків з купівлі-продажу акцій велику увагу слід приділити перевірці прав власності їх держателя на ці акції. Тут слід керуватися положеннями Закону України «Про Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні» [62], згідно з якими іменні цінні папери, випущені в документарній формі (якщо умовами емісії спеціально не зазначено, що вони не підлягають передаванню), передаються новому власникові у порядку, установленому для відступлення права вимоги (цесії). У разі відчуження знерухомлених іменних цінних паперів право власності переходить до нового власника з моменту зарахування їх на рахунок власника у зберігача.

Право власності на цінні папери на пред'явника, випущені в документарній формі, переходить до нового власника з моменту їх передання (поставки).

Право власності на цінні папери, випущені в бездокументарній формі, переходить до нового власника з моменту зарахування їх на рахунок власника у зберігача.

Підтвердженням права власності на цінні папери є сертифікат, а в разі знерухомлення цінних паперів чи їх емісії в бездокументарній формі — виписка з рахунку у цінних паперах, яку зберігач зобов'язаний надавати власникові цінних паперів.

З цього приводу технологіями операцій купівлі-продажу повинна передбачатися предпоставка акцій покупцю (у разі, якщо банк є покупцем) чи їх передоплата (якщо банк є продавцем), а також обов'язкове отримання інформації від депозитарної установи або реєстратора цінних паперів. Доцільно також, щоб банк мав дозвіл ДКЦПФР на депозитарну діяльність зберігати цінні папери і сам зберігав би належні йому цінні папери. Крім того, має вивчатися фінансовий стан та перспективи емітента, його конкурентоспроможність, термін діяльності на ринку, основні держателі акцій, прибутковість акцій та їх стабільність. Оскільки банки ведуть операції з акціями постійно, доцільно створити інформаційні бази даних по основних емітентах, перспективи ефективної діяльності яких та

прибутковість їхніх акцій є стабільними. Діяльність же банків на ринку купівлі-продажу акцій повинна здійснюватись у тісній взаємодії з усіма суб'єктами національної депозитарної системи, передусім реєстраторами та зберігачами акцій.

З огляду на те, що банк сам може бути емітентом цінних паперів, великого значення набуває забезпечення безпеки процедури їх емісії та розміщення на ринку. Здійснюючи емісію акцій, слід чітко дотримуватись установленого порядку її проведення. Особливу увагу варто приділити матеріалам, які мають бути опубліковані у зв'язку з емісією акцій. З одного боку, вони мають розкривати всю необхідну інформацію про банк як емітента, а з другого — у них не повинна розкриватись інформація, яка самостійно чи в сукупності з уже оприлюдненою може становити відомості таємного чи конфіденційного характеру.

Розміщення акцій може здійснюватися через передоплати і через фондову біржу, але не раніше ніж через 30 днів після опублікування оголошення про їх випуск. У процесі розміщення акцій банк має здійснювати контроль за тим, хто стає власником його акцій, як вони концентруються по акціонерах. Усі акції реалізуються через укладання відповідних договорів. Кожному акціонеру видається свідоцтво про кількість і номінальну вартість акцій з підписом керівника банку і печаткою його установи. Під час емісії ніякі операції з щойно придбаними акціями на вторинному ринку не можуть проводитись, аж до повного її завершення і реєстрації її результатів ДКЦПРФ.

Водночас об'єктом уваги банків мають бути операції з його акціями на вторинному ринку. Контроль зміни у складі власників акціонерного капіталу набуває сьогодні особливого значення, насамперед через існування імовірності рейдерського захвату. Крім того, контроль має здійснюватись і з метою попередження конфліктів у середовищі акціонерів банку або ж недобросовісної поведінки окремих з них. Такий контроль має забезпечуватися добрими стосунками банку з реєстраторами операцій з його акціями та періодичними звітами реєстратора банку про стан реєстру його акцій.

На сьогодні банками напрацьовано значний досвід з питань забезпечення безпеки в роботі з акціями, який можна викласти у вигляді таких застережень:

— під час роботи з акціями доцільно забезпечувати розмежування функцій працівників банку щодо обліку акцій і торгівлі ними;

— емісія акцій проводиться за курсовою вартістю (номінальна плюс курсова надбавка);

— мінімальна номінальна вартість акції не може бути меншою, ніж одна копійка;

— конвертація інших цінних паперів в акції може проводитися тільки у разі, якщо це оговорено в проспекті емісії;

— ксерокопії акцій чи сертифікатів акцій не є цінними паперами і до операцій не приймаються;

— статусу цінного папера акція набуває з моменту закінчення емісії (видачі Державною комісією з цінних паперів і фондового ринку свідоцтва про реєстрацію емісії);

— відкрите (публічне) розміщення акцій забороняється раніше, ніж через 10 днів після опублікування проспекту їх емісії;

— обов'язковим має бути проведення моніторингу стану вторинного ринку обігу акцій, взаємодія з операторами вторинного ринку;

— банк здійснює розміщення або продаж кожної акції, яку воно викупило, за ціною, не нижчою від її ринкової вартості, що затверджується наглядовою радою, крім випадків, визначених Законом України «Про акціонерні товариства» [48];

— акціонерне товариство не має права розміщувати жодну акцію за ціною, нижчою від її номінальної вартості;

— в заставу приймаються тільки ті акції, які перебувають на балансі підприємства;

— найбільш доцільно, щоб фізичні особи надавали в заставу тільки іменні акції;

— у разі застави акцій договором має передбачатися, що у разі невиконання позичальником своїх зобов'язань за кредитом, він передає банку права власності на визначену кількість акцій;

— здійснення періодичних запитів до реєстратора (депозитарію) щодо стану реєстру (облікового реєстру) акцій емітента;

— вартість акцій сплачується в національній валюті, якщо в інвалюті, то це має передбачатися статутом акціонерного товариства, а на акціях вказуватися валютний номінал акції;

— акції повинні мати відповідну кількість ступенів захисту та містити інформацію відповідно до вимог ДКЦПФР;

— придбання акцій здійснюється на основі договору купівлі-продажу.

Вклади банку в цінні папери інших суб'єктів в банківській практиці називають інвестиціями. А будь-яка купівля та

перепродаж цінних паперів банком від свого імені, за власний рахунок та з власної ініціативи є інвестиційною діяльністю. Оскільки банк, вкладаючи у такий спосіб кошти, повною мірою ризикує, необхідно передбачити відповідні заходи безпеки його інвестиційних операцій. Основний зміст інвестиційної безпеки банку полягає в розробленні механізму захисту його інвестиційного портфеля. Серед заходів захисту можна назвати такі:

- оцінювання інвестиційних об'єктів з погляду перспектив їх розвитку, виявлення ознак, які можуть формувати негативні наслідки в діяльності зазначених об'єктів;
- диверсифікація об'єктів інвестиційних вкладень банку;
- строге дотримання встановлених нормативів інвестиційної діяльності;
- контроль діяльності об'єкта інвестування, вжиття заходів щодо дотримання ним планових показників, коригування інвестиційних проектів з метою забезпечення ефективного їх виконання;
- участь банку в управлінні інвестиційним проектом об'єкта інвестицій;
- свобода інвестиційної діяльності і прийняття банком конкретних рішень має забезпечуватися лише за наявності альтернативних можливостей.

У процесі інвестування конкретного об'єкта слід звернути увагу на таке:

- незвично високі дивіденди, які пропонує об'єкт;
- тиск на банк з вимогами якнайшвидше інвестувати кошти;
- ухилення об'єкта інвестування від сплати податків;
- сфера діяльності об'єкта є новою для даного регіону (галузі економіки);
- процес подібного інвестування об'єкта раніше мав скандали і конфлікти;
- параметри інвестиційного проекту не мають аудиторської перевірки або іншого фахового (експертного висновку);
- ефективність інвестиційного проекту забезпечується на підставі унікальних особистих здібностей окремого менеджера чи фахівця — організатора проекту;
- серед умов інвестування є такі, що обмежують вихід з нього і вилучення інвестиційних коштів.

За всіх умов інвестиційна діяльність банку загалом і кожна інвестиційна операція зокрема потребують ретельної перевірки об'єкта інвестиційних вкладень, його проекту, можливостей,

позиції та репутації на ринку, інвестиційної історії, контролю (моніторингу) всієї операції. Слід також передбачити заходи щодо впливу інвестора як на хід інвестиційної операції, так і на об'єкт інвестування та можливості відшкодування завданих банку збитків за негативного результату інвестиційних вкладень.

При проведенні банками вексельних операцій велике значення для їх безпеки матиме дотримання відповідних правил, викладених у Положенні Національного банку України про порядок здійснення банками операцій з векселями в національній валюті на території України (постанова Правління Національного банку України від 16 грудня 2002 р. № 508) [40]. Згідно з вказаними правилами банк може здійснювати такі операції з векселями: кредитні, торговельні, гарантійні, розрахункові, комісійні. Під час проведення зазначених операцій банк має ретельно вивчати фінансовий стан, кредито- та платоспроможність платників за векселями і зобов'язаних за векселями осіб, з якими він укладає угоди про проведення операцій.

Банки здійснюють операції з простими та переказними векселями за умови складання векселів у документарній формі на бланках з відповідним ступенем захисту та заповнення їх реквізитів відповідно до встановлених вимог.

Операції з переказними векселями здійснюються за умови заповнення чітко визначених реквізитів, а саме:

- назви «переказний вексель», яка включена до тексту документа і написана тією мовою, якою цей документ складений (вексель, який видається на території України, і місце платежу за яким також на території України, складається державною мовою. Найменування трасанта або векселедавця, інших зобов'язаних за векселем осіб зазначається тією мовою, якою визначене офіційне найменування в їх установчих документах);
- безумовного наказу сплатити визначену суму грошей;
- найменування особи, яка має сплатити (трасат);
- строку платежу;
- місця, у якому має здійснюватися платіж;
- найменування особи, якій або за наказом якої має здійснюватися платіж;
- дати і місця видачі векселя;
- підпису особи, яка видає вексель (трасант).

Банки здійснюють операції з простими векселями за умови заповнення чітко визначених реквізитів, а саме:

— назви «простий вексель», яка включена до тексту документа і написана тією мовою, якою цей документ складено;

— безумовного зобов'язання сплатити визначену суму грошей;

— строку платежу;

— місця, у якому має бути здійснений платіж;

— найменування особи, якій або за наказом якої має здійснюватися платіж;

— дати і місця видачі простого векселя;

— підпису особи, яка видає документ (векселедавець).

Банки здійснюють операції з векселями, виданими від імені фізичної особи, за умови зазначення додаткових реквізитів, а саме:

- прізвища, ім'я, по батькові;
- паспортних даних векселедавця-трасанта (серія та номер паспорта, найменування органу, що видав паспорт, та дата його видачі, місце проживання);
- індивідуального ідентифікаційного номера з Державного реєстру фізичних осіб — платників податків та інших обов'язкових платежів, наданого органом державної податкової служби (крім випадків відсутності індивідуального ідентифікаційного номера в осіб, які через свої релігійні або інші переконання відмовилися від прийняття індивідуального ідентифікаційного номера та офіційно повідомили про це відповідні державні органи);
- підпису, власноручно зазначеного фізичною особою або уповноваженою нею особою. Підпис скріплюється відбитком печатки (у разі її наявності).

Підпис на векселі (переказному або простому) від імені юридичної особи здійснюють власноручно керівник та головний бухгалтер або уповноважені ними особи. Підписи скріплюються відбитком печатки.

У разі підписання векселя на підставі довіреності у векселі обов'язково зазначається, що він підписаний на підставі довіреності (також можуть зазначатися дата її складання і номер) від імені визначеного банку — юридичної особи.

Слід звернути увагу, що переказний вексель може бути виданий у двох або більше тотожних примірниках, які мають містити порядкові номери в самому тексті векселя. В іншому разі кожний з них розглядається як окремий переказний вексель.

Кожний держатель переказного векселя та простого векселя має право знімати з них копії.

Копія векселя має точно відтворювати оригінал, уключаючи індосаменти й усі інші позначки, що містяться в ньому. Вона передається через індосамент і забезпечується авалем так само і з такими самими наслідками, що й оригінал.

У копії векселя зазначається особа, у якої зберігається оригінал векселя.

Дуже важливим моментом для прийняття ефективних рішень щодо проведення вексельних операцій та попередження шахрайства у вексельних операціях є проведення всебічної перевірки векселів. Перевірка проводиться експертизою векселів, яка може здійснюватися у трьох напрямах:

а) юридична експертиза, у процесі якої перевіряються:

- наявність і правильність заповнення всіх реквізитів векселя і безперервність ряду передавальних індосаментів;
- відповідність реквізитів і тексту векселя законодавству про вексельний обіг;
- дотримання змісту і юридичного значення тексту кожного реквізиту;
- дотримання товарного походження векселя;
- законність володіння векселем;
- аналіз дійсності підписів посадових осіб, якими зроблено підписи на векселі від імені юридичних осіб, зобов'язаних за векселем;
- повноваження представників, які підписали вексель від імені пред'явника.

Відсутність або неправильність хоча б одного з реквізитів може бути підставою для невизнання документа векселем;

б) економічна експертиза, метою якої є встановлення можливості оплати векселя в установлений термін. У процесі експертизи встановлюються випадки відмови суб'єктів ринку від придбання векселів даного емітента або від купівлі даного векселя з конкретним номером. Крім того, звертається увага на факти відсутності певних супровідних документів, наявність в ряду індосаментів підозрілих (фіктивних) суб'єктів, поведінку емітента при спробі одержати від нього додаткову інформацію. Поряд з перевіркою платоспроможності пред'явника векселя банк має проаналізувати фінансове становище платника, індосантів, які не зняли з себе відповідальності безоборотним застереженням;

в) експертиза фінансової надійності зобов'язаних за векселем осіб має включати:

— аналіз та оцінювання їх фінансового стану;

— визначення потенційної договірної ціни векселя, за якою банк купує (ураховує, приймає в заставу) вексель;

— в) експертиза бланків векселів охоплює:

- перевірку бланків на дійсність;
- аналіз векселя щодо фальсифікації, підробки або неправомірної зміни первинного тексту;
- перевірку бланку на наявність фізичних пошкоджень.

Експертиза бланків векселів завершується складанням відповідного акта. Якщо ж виявлено факт підробки, фальсифікації або відсутності певного елементу технічного захисту бланку, то такий факт за рішенням суду може бути підставою для визнання бланку недійсним.

У процесі роботи з векселем вітчизняними банками напрацьовано певний перелік застережень, серед яких:

— обов'язковість перевірки платоспроможності векселедавців (термін роботи з векселями, репутація, фінансовий стан, перспективи розвитку);

— надання переваги короткостроковим векселям, які менше залежать від змін економічної ситуації;

— при вексельних кредитах векселі повинні мати іменний індосамент на користь банку;

— векселедавець у разі передання векселя повинен пред'явити довідку про сплату державного мита;

— платіж за векселем на території України здійснюється тільки в безготівковій формі;

— протест у неплатежі за векселем, який підлягає оплаті на визначену дату або у визначений строк від дати складання чи пред'явлення, повинен бути здійснений або в день, коли вексель підлягає оплаті, або в один із двох наступних робочих днів;

— до обліку, під заставу і рефінансування доцільно приймати векселі видані тільки юридичними особами на основі здійснення реальних товарних і комерційних угод;

— вексель, виконаний на іноземній мові, повинен мати переклад тексту, завірений нотаріально;

— опротестовані векселі банк до операцій не приймає;

— векселі надаються в банк з їх реєстрами;

— якщо вексель виписано у валюті, якої немає в обігу в місці платежу, сума може бути виплачена в національній валюті за курсом НБУ на день настання терміну платежу;

— якщо штатним розкладом підприємства-векселедавця (індосанта) передбачено посаду головного бухгалтера, то вексель підписується і керівником і головним бухгалтером.

Заходи безпеки в операціях банку з векселями досить повно викладені в Положенні про порядок здійснення банками операцій з векселями в національній валюті на території України. То ж дотримання цих заходів має мінімізувати ризики банку та забезпечити йому надійний захист банківських коштів та збереження його конкурентоспроможності на ринку цінних паперів.

У разі опротестування векселів з метою уникнення будь-яких упущень в оформленні протесту банк при одержанні векселя від нотаріуса разом з актом про протест має звертати увагу на належне оформлення як самого надпису про протест на векселі, так і акта про протест, зокрема на обов'язкове зазначення проти кого і від імені кого вчинений протест.

Забезпечення безпеки банку в роботі з векселями має будуватись як комплекс заходів правового, організаційного, технологічного, економічного та спеціального характеру.

В основу заходів безпеки в роботі з векселями має бути покладено відповідні правила та норми, що регламентуються нормативно-правовими документами банку. У свою чергу, до організаційних заходів слід віднести: створення єдиної інформаційної бази даних про складені, видані, погашені, втрачені, вкрадені, підроблені векселі; особливий порядок зберігання векселів і їх бланків. Бланки векселів мають зберігатись у спеціальному приміщенні або ж у сховищі банку. на період операційного дня вони видаються працівникам банку, які відповідають за роботу з векселями. Отримання векселів та їх бланків оформлюється під розписку. Невикористані бланки і складені, але не видані векселі по закінченні операційного дня повертаються до місця їх зберігання. Оплачені (погашені) векселі зберігаються в бухгалтерії. Доцільно дотримуватися розмежування повноважень працівників, які беруть участь у вексельному обігу. Участь у процедурі складання, видачі, зберігання та прийняття до оплати векселів кількох працівників банку значно знижує ризик неправомірних дій з їх боку. Механізм розмежування повноважень реалізується через участь у видачі векселів:

— особи, що видає бланк векселя;

— осіб, що візують договір купівлі-продажу векселя;

— керівника установи банку і головного бухгалтера, що підписують вексель;

— особи, відповідальної за зберігання печатки, якою посвідчуються підписи на векселі.

Важливим у забезпеченні безпеки роботи банку з векселями також є захист інформації про вексельні операції і невикористані бланки векселів та індивіалізація відповідальності працівників, що беруть участь у видачі векселів.

До заходів технологічного характеру мають бути віднесені: опис процедури складання й умов видачі векселів. Вексель має видаватися векселеотримувачем лише після надходження коштів на рахунок банку, а технологія видачі векселя має передбачати виконання відповідних заходів щодо ідентифікації особи, яка отримує вексель як першого векселеотримувача; порядок документування проходження векселем процедур підготовки до складання і видачі, факту їх видачі чи погашення; зміст процедур перевірки при підготовці до сплати векселя. Тут як перша дія працівника банку при пред'явленні векселя до сплати має бути перевірка реквізитів наданого векселя згідно з відповідною базою даних векселів, що перебувають в обігу, а також погашених і заборонених до обігу (втрачених, украдених, підроблених); процедури, спрямовані на попередження повторного використання погашеного векселя; порядок роботи з наданими неплатоспроможними векселями.

У разі крадіжки з банку векселів про це робиться заява до правоохоронних органів і одночасно звернення до суду про визнання вкрадених векселів недійсними і про відновлення прав по них. Це дасть можливість попередити операції з вкраденими векселями і відновити свої права у зв'язку зі шкодою, заподіяною викраденням векселів.

Касові операції. Важливе місце у забезпеченні економічної безпеки банків має безпека касових операцій. Насамперед це пов'язано з тим, що якраз такі операції здійснюються безпосередньо з готівкою, посягання на яку мають найбільш активний та агресивний характер. Більше того, такі посягання, як правило, здійснюються відкрито та зухвало, з наявністю загрози життю та здоров'ю працівників банків і їх клієнтів. Ураховуючи зазначене цим операціям банки мають приділяти особливе значення з питань безпеки їх проведення.

Забезпечення безпеки касових операцій виконується у двох напрямах: особливим обладнанням приміщень банків, де проводяться такі операції, та робочих місць працівників банків, які проводять ці операції зайнятих у них, а також особливою поведінкою працівників банків під час здійснення ними касової роботи. У першому випадку відповідно до будівельних норм банківських споруд приміщення касових сховищ, прибуткових,

вечірніх і видаткових кас, інші приміщення касових вузлів, підходи (під'їзди) до них обладнуються необхідними засобами застереження, захисту, сповіщення і підлягають ретельній охороні.

Особлива поведінка працівників касових вузлів визначається відповідними нормативними актами, зокрема Інструкцією про касові операції в банках України, затвердженою постановою Правління Національного банку України від 14 серпня 2003 р. № 337 [19], Інструкцією про порядок організації та здійснення валютно-обмінних операцій на території України, затвердженою постановою Правління Національного банку України від 12 грудня 2002 р. № 502 [20], Інструкцією з організації перевезення валютних цінностей та інкасації коштів в установах банків України, затвердженою постановою Правління Національного банку України від 3 грудня 2003 р. № 520 [18], Положенням про здійснення уповноваженими банками операцій з банківськими металами, затвердженим постановою Правління Національного банку України від 6 серпня 2003 р. № 325 [39] та іншими документами нормативно-правового характеру.

Касовими операціями згідно з Інструкцією про касові операції в банках України є операції, які здійснює банк, а саме: видача готівки, приймання її та обмін непридатних до обігу банкнот (монет) на придатні до обігу банкноти (монети), банкнот — на монети, монет — на банкноти, банкнот (монет) одного номіналу — на банкноти (монети) іншого номіналу, вилучення з обігу сумнівних банкнот (монет), валютно-обмінні операції та операції з банківськими металами.

З точки зору безпеки банки під час здійснення касових операцій мають забезпечувати:

- визначення справжності та платіжності банкнот (монет);
- вилучення сумнівних банкнот (монет) на дослідження;
- належний внутрішній контроль за касовими операціями;
- створення безпечних умов роботи з готівкою та її зберігання;
- ідентифікацію клієнтів, які здійснюють операції з готівкою без відкриття рахунку на суму, що перевищує 50 000 грн або еквівалент цієї суми в іноземній валюті.

Для виконання касової роботи керівники установ банків повинні приділити особливу увагу підбору відповідного персоналу, звернути увагу на чесність, порядність, надійність майбутніх працівників, відсутність у них небажаних звичок та пристрастей, випадків зловживання службовим становищем та непорозуміння з законом. На всіх задіяних працівників у касовій

роботі заводяться особові справи, в яких в обов'язковому порядку повинні бути такі документи: заява про прийняття на роботу, автобіографія, копія наказу про призначення на посаду, виписки з протоколів про прийняття заліків щодо знань вимог відповідних нормативних документів, які регламентують порядок касової роботи, фотокартка, договір про матеріальну відповідальність, характеристика з останнього місця роботи.

Усі працівники, які здійснюють касові операції з готівкою, мають пройти певний відбір та повинні скласти залік з оформленням відповідного протоколу щодо знання вимог Інструкцій та внутрішніх положень про організацію роботи із здійснення касових операцій у межах тих питань, що належать до їх функціональних обов'язків.

Відповідальність за організацію, стан касової роботи, у тому числі і її безпеку, несуть керівник установи банку, головний бухгалтер, завідувач касою та керівник служби безпеки (останній тільки з питань безпеки).

Особлива увага приділяється забезпеченню безпеки проведення касових операцій, пов'язаних із прийманням банком готівки та її видачею. Такі операції здійснюються протягом операційного дня банку. Для приймання готівки після завершення операційного дня в банках організовуються вечірні каси, режим роботи яких визначається керівниками банківських установ.

Приймання готівки від клієнтів здійснюється через каси банків за відповідними прибутковими касовими документами.

У прибуткових касових документах працівник банку перевіряє повноту заповнення реквізитів і наявність та тотожність підписів відповідальних працівників банку із зразками підписів (у разі прийняття заяви на переказ готівки через операційних працівників).

Приймаючи від клієнта готівку, працівник повинен перерахувати банкноти суцільним поаркушним перерахуванням, а монети — за кружками. Робочі місця касових працівників, які здійснюють приймання та обробку готівки, мають бути обладнані приладами для контролю захисних елементів банкнот. Крім того, робоче місце з приймання готівки має бути обладнане так, щоб клієнт міг спостерігати за перерахуванням готівки. На столі касира не може бути ніяких інших грошей, окрім тих, які приймаються від особи, яка вносить гроші.

Під час приймання від клієнтів банку касових документів за операціями з готівкою без відкриття рахунку на суму, що перевищує 50000 грн або еквівалент цієї суми в іноземній валюті,

касовий працівник перевіряє належність пред'явленого паспорта або документа, що його замінює, та відповідність даних документа тим даним, що зазначені в касовому документі.

У разі, якщо клієнт не надав документів або відомостей, потрібних для з'ясування його особи, суті діяльності, фінансового стану, або у разі умисного надання неправдивих відомостей банк відмовляє клієнту в проведенні операції з готівкою та повертає клієнту касовий документ без виконання, зробивши на зворотному боці касового документа напис про причину його повернення (з обов'язковим посиланням на ст. 64 Закону України «Про банки і банківську діяльність») і зазначити дату його повернення (із засвідченням підписами виконавця та/або працівника, на якого покладено функції контролера, і відбитком печатки (штампа) банку).

Якщо операція з готівкою, яку здійснює клієнт, містить ознаки такої, що підлягає фінансовому моніторингу, то банк має право відмовити клієнту в її проведенні та повернути касовий документ без виконання, роблячи на зворотному боці касового документа напис про причину його повернення (з обов'язковим посиланням на частину другу ст. 7 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму») і зазначити дату його повернення [із засвідченням підписами виконавця та відповідального працівника, який приймає рішення щодо віднесення операції клієнта до операцій, які підлягають фінансовому моніторингу, і відбитком печатки (штампа) банку].

Видача готівки національної валюти з каси банку проводиться за такими документами:

— грошовими чеками — юридичним особам, їх відокремленим підрозділам, а також підприємцям;

— заявою на видачу готівки — фізичним особам з поточних, вкладних (депозитних) рахунків та фізичним і юридичним особам переказ без відкриття рахунку (з поданням юридичною особою довіреності на уповноважену особу) за операціями з клієнтами (видача кредиту тощо);

— документом на отримання переказу готівкою в національній валюті, установленим відповідною платіжною системою, — фізичним і юридичним особам (з поданням юридичною особою довіреності на уповноважену особу);

— видатковим касовим ордером — працівникам банку за внутрішньобанківськими операціями.

З каси банку готівка іноземної валюти видається за такими

видатковими документами:

— заявою на видачу готівки — юридичним особам, їх відокремленим підрозділам, а також підприємцям з їх поточних рахунків на цілі, передбачені нормативно-правовими актами; фізичним особам з їх поточних, вкладних (депозитних) рахунків і переказу без відкриття рахунку, а також за операціями з відшкодування банкнот іноземної валюти, прийнятих на інкасо;

— видатковим касовим ордером — працівникам банку за внутрішньобанківськими операціями;

— документами на отримання переказу в готівковій формі, установленими відповідною платіжною системою, — фізичним особам.

Отримавши видатковий касовий документ (заяву на видачу готівки, видатковий касовий ордер, грошовий чек), працівник банку зобов'язаний перевірити:

- повноту заповнення реквізитів на документі;
- наявність підписів посадових осіб банку, яким надано право підпису касових документів, і тотожність їх зразкам;
- належність пред'явленого паспорта або документа, що його замінює, отримувачу, відповідність даних паспорта тим даним, що зазначені в касовому документі;
- у разі отримання готівки за довіреністю — правильність оформлення довіреності на отримання готівки;
- наявність підпису отримувача.

Грошові чеки дійсні протягом 10 календарних днів з дня їх виписки, не враховуючи дня виписки. У разі зазначення дати на чеку дата та рік проставляється цифрами, а місяць — словом. На грошовому чеку обов'язково повинні бути відбиток печатки та підписи (підпис) уповноважених осіб (особи) клієнта відповідно до картки зразків підписів. Використання факсиміле не допускається.

Якщо клієнт отримує готівку за кількома видатковими документами з різних рахунків, то готівка видається за кожним документом окремо.

Видані з каси банку гроші одержувач повинен, не відходячи від каси, перевірити по пачках і корінцях, а окремі листи — поаркушним перерахунком в присутності касира, який видав гроші. Якщо клієнт виявив бажання перерахувати грошові білети поаркушно, а монети — за кружками, видача грошей має бути організована так, щоб з моменту одержання від видаткового касира грошей клієнт перебував у спеціально відведеному для перерахунку місці під наглядом касира-контролера банку.

У разі виявлення клієнтом під час перерахування готівки недостачі або надлишку банкнот (монет) у пачках, окремих корінцях або в мішечках з монетами в непошкодженій упаковці банк повинен вжити заходів щодо перевірки готівки і в разі підтвердження розбіжностей складається відповідний акт про розбіжності у двох примірниках, що засвідчується підписами осіб, які були присутні під час перерахування.

Претензії одержувача коштів щодо недостачі грошових білетів або монет не приймаються, якщо кошти не були перераховані ним, не відходячи від каси або в спеціальному приміщенні для перерахування грошей. Про це на видному місці біля видаткової каси має висіти оголошення.

Під час приймання, видачі, обробки грошових знаків національної та іноземної валюти касові працівники повинні визначати справжність і платіжність банкнот (монет), керуючись Правилами визначення платіжності та обміну банкнот і монет Національного банку України, затвердженими постановою Правління Національного банку України від 17 листопада 2004 р. № 547 [45], та з використанням довідкової інформації, що надається Національним банком України, банками-емітентами, Інтерполом або іншими уповноваженими установами.

Згідно з цими Правилами до платіжних належать банкноти (монети), які не мають ознак зношення і пошкодження, а також з дефектами та ознаками зношення і пошкодження в межах, визначених Правилами критеріїв.

Залежно від зовнішнього вигляду та ступеня зношення або пошкодження платіжні банкноти і монети поділяються на придатні та непридатні до обігу.

Непридатними до обігу вважаються платіжні банкноти (монети), які в процесі обігу набули ознак зношення та пошкодження, що встановлені Національним банком України, а також такі, що мають дефекти виробника і повинні вилучатися банками з обігу.

За ступенем зношення, пошкодження та наявності дефектів непридатні до обігу банкноти (монети), у свою чергу, поділяються на зношені банкноти і монети, значно зношені банкноти та банкноти і монети з дефектами виробника.

1. Зношені банкноти — це банкноти, які мають одну або більше з таких ознак зношення або пошкодження:

- потертості, часткова втрата фарби на зображеннях, розпушення паперу, втрату папером жорсткості;
- загальне або локальні забруднення, плями та написи

^{2}, колір яких контрастує з кольором навколишнього зображення або навколишньої незадрукованої ділянки банкноти;

- відбитки штампів площею понад 400мм^2, у тому числі видимі в ультрафіолетових променях, крім штампів про погашення;
- надриви або надрізи довжиною кожний понад 5 мм, у тому числі склеєні;
- отвори та проколи, відірвані краї або кути, площа кожного з яких більша, ніж 10 мм^2.

Зношені монети — це монети з ознаками хімічної дії, унаслідок чого змінився колір, або механічного пошкодження (спотворені елементи дизайну) за умови, що вони не мають надломів, надрізів та отворів, недеформовані і зберегли масу, зображення малого Державного Герба України, номіналу, назви розмінної одиниці та рельєф або текст на гурті, якщо він має бути згідно з офіційним повідомленням Національного банку.

Зношені банкноти і монети, якщо вони не мають ознак підроблення, повинні без обмежень прийматися фізичними й юридичними особами до всіх видів готівкових платежів, для переказів тощо. Окрім того, банки зобов'язані без обмежень приймати такі банкноти і монети разом з виручкою підприємств, установ і організацій, а також від фізичних і юридичних осіб до всіх видів готівкових платежів, для зарахування на рахунки, вклади, акредитиви та обміну на придатні до обігу банкноти і монети.

2. Значно зношені банкноти — це банкноти, які мають одну або більше з наведених нижче суттєвих ознак зношення або пошкодження (незалежно від наявності ознак зношення, зазначених у пункті 1):

- банкноти з утраченими частинами, якщо разом з отворами (дірками) збереглася ціла частина банкноти, площа якої не менше ніж 55% її початкової площі;
- банкноти, розірвані та розрізані на дві або більше частин, у тому числі склеєні, якщо не менше ніж 55% загальної площі частин, що залишилися, безумовно належать одній банкноті;
- банкноти, що складені (склеєні) з половин двох різних банкнот одного номіналу і дизайну, розірваних (розрізаних) навпіл, загальною площею не менше ніж 92% початкової площі банкноти;
- банкноти, пошкоджені вогнем, водою, різними рідинами або

Банки мають приймати без обмеження від юридичних і фізичних осіб для обміну на придатні до обігу банкноти, а також для зарахування на рахунки, вклади, акредитиви, для готівкових платежів тощо пошкоджені банкноти без ознак підробки, які:

— зберегли цілу частину, площею не менше, ніж 55% своєї початкової площі;

— розірвані (розрізані) на дві частини, на яких збереглись обидва однакові номери та серія, і загальна площа цих частин є не меншою, ніж 55% початкової площі банкноти.

Усі інші пошкоджені банкноти, які складені з двох або більше частин, банки мають вилучати як сумнівні щодо платіжності та в установленому порядку надсилати для проведення досліджень до відповідних територіальних управлінь Національного банку. За результатами цих досліджень експерт Національного банку оформляє відповідний акт, на підставі якого банкноти (монети) можуть бути визнані платіжними, неплатіжними чи підробленими.

Не приймаються банками та іншими юридичними особами лише банкноти, пошкоджені вогнем, водою, різними рідинами або хімікатами тощо, площа яких під час приймання та обробки може стати меншою, ніж 55% початкової площі банкноти. З метою обміну таких банкнот фізичні та юридичні особи мають звертатися безпосередньо до територіальних управлінь Національного банку, які зобов'язані прийняти рішення про обмін банкнот у присутності пред'явника або прийняти їх на дослідження за його заявою.

3. Банкноти і монети з дефектами виробника — це банкноти і монети з будь-якими відхиленнями від зразка, допущеними під час виготовлення (на банкнотах — відсутні графічні зображення, одна або кілька фарб, номери, немає або неправильно розміщений водяний знак або захисна стрічка, невідповідність водяного знака або захисної стрічки номіналу тощо; на монетах — тріщини, відколи, зміщення зображення, перевернуте зображення реверсу щодо аверсу, нечіткість чеканки тощо), які помилково випущені в обіг, але не втратили платіжності за ступенем зношення.

Банкноти та монети з дефектами виробника, якщо вони не мають ознак підроблення, банки зобов'язані без обмеження приймати від юридичних і фізичних осіб для обміну на придатні

до обігу банкноти та монети, а також для зарахування на рахунки, вклади, акредитиви та для готівкових платежів тощо.

Обмін банками непридатних до обігу банкнот і монет (зношених, значно зношених та з дефектами виробника) повинен здійснюватися безоплатно.

Крім непридатних до обігу банкнот і монет за ознаками зношення та дефекту виробника працівники кас особливо пильну увагу повинні приділяти виявленню підроблених банкнот (монет) та перероблених банкнот (монет).

Підроблені банкноти (монети) — це банкноти (монети), що виготовлені будь-яким способом, у тому числі промисловим, усупереч установленому законодавством України порядку та імітують (фальсифікують) справжні банкноти (монети), уведені Національним банком в обіг. До підроблених належать також перероблені банкноти (монети), на яких будь-яким способом (наклеюванням, малюванням, друкуванням тощо) змінені зображення, що визначають номінал, рік затвердження зразка (виготовлення), банк-емітент, інші реквізити та елементи дизайну, і які за зовнішнім виглядом можуть бути сприйняті як справжні банкноти (монети).

Банкноти і монети, що викликали сумнів касового працівника банку щодо справжності, та ті, на яких виявлені ознаки підроблення, банк зобов'язаний примусово, а справжні банкноти і монети, що викликали сумнів щодо платіжності, на бажання пред'явника в установленому порядку вилучати з обігу і передавати для досліджень та винесення остаточного висновку до відповідного територіального управління Національного банку.

У разі виявлення в одного клієнта двох або більше підроблених банкнот банк має терміново по телефону і не пізніше наступного робочого дня письмово, з поданням копії документа про вилучення, повідомити про це правоохоронний орган за місцезнаходженням банку.

До валютно-обмінних операцій з іноземною валютою і дорожніми та іменними чеками (далі — валютно-обмінні операції) належать:

а) купівля у фізичних осіб — резидентів і нерезидентів готівкової іноземної валюти за готівкові гривні;

б) продаж фізичним особам — резидентам готівкової іноземної валюти за готівкову гривню;

в) зворотний обмін фізичним особам — нерезидентам невикористаних готівкових гривень на готівкову іноземну

валюту;

г) купівля-продаж дорожніх чеків за готівкову іноземну валюту, а також купівля-продаж дорожніх чеків за готівкові гривні;

ґ) конвертація (обмін) готівкової іноземної валюти однієї іноземної держави на готівкову іноземну валюту іншої іноземної держави;

д) прийняття на інкасо банкнот іноземних держав та іменних чеків.

Причому операції, зазначені в абзацах б—д, на суму, що перевищує 15 000 грн, здійснюються лише через каси банку, фінансової установи, в операційному залі об'єкта поштового зв'язку після пред'явлення документа, що засвідчує особу, яка здійснює операцію з готівкою, із зазначенням у довідках та квитанціях прізвища, імені, по батькові (за наявності) особи, а на суму, що перевищує 50 000 грн, крім того, зазначаються серія та номер паспорта (іншого документа, що засвідчує особу), дата видачі та орган, що його видав, місце проживання (реєстрації), ідентифікаційний номер особи (за наявності).

Окрім того, банку (фінансовій установі) забороняється здійснювати операції з продажу іноземної валюти через касу банку (фінансової установи) одній особі в один операційний (робочий) день на суму, що перевищує в еквіваленті 80 000 грн, з метою запобігання використанню банківської системи для легалізації (відмивання) доходів, одержаних злочинним способом.

Під час здійснення валютно-обмінних операцій касовий працівник має перевіряти справжність і наявність ознак платіжності пред'явлених банкнот іноземних держав та дорожніх чеків. Для цього його робоче місце має бути обладнане відповідними приладами. Крім цього, на робочому місці необхідно мати відповідні нормативно-правові акти, довідники та інформацію щодо банкнот іноземної валюти, які є законним платіжним засобом на території відповідної іноземної держави, основних елементів їх захисту, про терміни обміну банкнот іноземної валюти, що вилучаються з обігу банками-емітентами.

Касир пункту обміну валюти має зберігати наявні цінності в сейфі. Під час обідньої перерви або тимчасової відсутності в приміщенні пункту обміну касир має опломбувати сейф з цінностями особистим пломбіром. Входити до приміщення пункту обміну валюти дозволяється лише особам, визначеним у наказі про відкриття пункту обміну валюти, та представникам

органів, уповноважених здійснювати перевірку пунктів обміну валюти згідно з чинним законодавством України

Як підтвердження здійснення валютно-обмінних операцій касовий працівник повинен надати клієнтові відповідну довідку або квитанцію встановленого зразка. Причому виправлення в заповненому тексті зазначених вище довідок та квитанцій не допускаються. Довідка або квитанція вважається недійсною, якщо реквізити каси або пункту обміну валюти, дані про здійснені операції, найменування банку (фінансової установи) або агента, що видав довідку чи квитанцію, не читаються або можливе подвійне читання відомостей на відбитку штампа пункту обміну валюти або каси банку (фінансової установи).

Уповноважені банки на підставі письмового дозволу Національного банку на здійснення операцій з валютними цінностями в частині проведення операцій з банківськими металами на міжнародних ринках та з урахуванням вимог Положення про здійснення уповноваженими банками операцій з банківськими металами мають право здійснювати такі види операцій з банківськими металами:

а) відкриття кореспондентських рахунків у банківських металах у банках-нерезидентах та проведення операцій з ними;

б) купівля-продаж банківських металів за іноземну валюту;

в) розміщення міжбанківських депозитів у банківських металах;

г) отримання міжбанківських кредитів у банківських металах;

г) надання та отримання банківських металів у заставу;

д) відповідальне зберігання банківських металів у банках-нерезидентах.

Уповноважені банки здійснюють операції з купівлі-продажу банківських металів:

- від свого імені за дорученням і за рахунок коштів клієнтів (у тому числі на підставі платіжних вимог на стягнення банківських металів, оформлених державними виконавцями);
- у межах лімітів відкритої валютної позиції банку.

Приймання банківських металів від клієнтів та видача клієнтам банківських металів здійснюється на підставі первинних документів, указаних у Положенні про здійснення уповноваженими банками операцій з банківськими металами. Окрім того, банк повинен визначити відповідальних працівників, які матимуть право підписувати відповідні первинні документи за операціями з банківськими металами та визначити систему контролю за їх здійсненням.

Під час виконання операцій з банківськими металами може застосовуватися система автоматизації банку, у тому числі така, що працює автономно. У разі її використання банк повинен визначити кількість підписів працівників банку, які будуть оформляти, контролювати та виконувати операцію з банківськими металами.

З метою ідентифікації клієнта:

— для фізичних осіб — резидентів, які здійснюють операції без відкриття рахунку з купівлі-продажу банківських металів на суму, що перевищує 50000 грн, або операції з обміну зливка (зливків) банківського металу на зливки (зливок) меншої (більшої) маси, або операції з конвертації одного банківського металу в інший, якщо вартість банківського металу, наданого клієнтом для обміну або конвертації, за офіційним (обліковим) курсом гривні до цього металу на день здійснення операції перевищує 50000 грн, у первинних документах мають зазначатися такі реквізити: прізвище, ім'я, по батькові цієї особи, дата народження, серія та номер паспорта (іншого документа, який посвідчує особу), дата видачі та орган, що його видав, місце проживання, ідентифікаційний номер;

— для фізичних осіб — нерезидентів, які здійснюють операції з банківським металом без відкриття рахунку, у первинних документах мають зазначатися такі реквізити: прізвище, ім'я, по батькові (у разі його наявності) цієї особи, дата народження, серія та номер паспорта (іншого документа, який посвідчує особу), дата видачі та орган, що його видав, громадянство, місце проживання або тимчасового перебування. Ці операції проводяться лише за умови пред'явлення нерезидентом касовому працівникові документа, який підтверджує джерела походження гривень/банківських металів;

— для юридичних осіб, які здійснюють операції з обміну зливка (зливків) банківського металу на зливки (зливок) меншої (більшої) маси без відкриття рахунку, у первинних документах мають зазначатися такі реквізити: найменування, юридична адреса, ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України, реквізити банку, у якому відкрито поточний рахунок у гривнях (із зазначенням його номера), прізвище, ім'я, по батькові особи, яка від імені цієї юридичної особи безпосередньо одержує або вносить банківські метали, дата народження, серія та номер паспорта (іншого документа, який посвідчує особу), дата видачі та орган, що його видав.

Якщо клієнт не надав документів або відомостей, потрібних для з'ясування його особи, суті діяльності, фінансового стану, або умисного надання неправдивих відомостей або, якщо операція з банківськими металами, яку здійснює клієнт, містить ознаки такої, що підлягає фінансовому моніторингу, то банк може відмовити клієнту в проведенні зазначеної операції з дотриманням вимог, визначених чинним законодавством.

Операції з приймання банківських металів або готівкових гривень від фізичних осіб — нерезидентів повинна здійснюватися за умови підтвердження джерел походження цих банківських металів або готівкових гривень.

Після завершення операції з банківськими металами клієнту видається відповідна квитанція. Заява про приймання (видачу) банківських металів складається з двох частин: власне заяви та квитанції до неї. У разі здійснення відповідної операції з банківськими металами заява про приймання (видачу) банківських металів залишається в банку, квитанція надається клієнту як підтвердження здійснення операції.

До компетенції банків віднесено визначення порядку перевезення валютних цінностей до власних підрозділів (філій, відділень) та їх вивезення у зворотному напрямі, перевезення валютних цінностей до/від банкоматів, пунктів обміну валют, перевезення валютних цінностей від каси банківської установи до клієнтів банку та між клієнтами банку, проведення інкасації коштів, зберігання та здавання сумок (мішків) з готівкою, що доставлені з маршруту інкасації та ін.

Залучення працівників до безпосередньої роботи з цінностями проводиться з дотриманням вимог законодавства про працю, після стажування та успішного складання заліків щодо знання вимог нормативно-правових актів Національного банку, внутрішніх положень банку, які регламентують роботу з перевезення валютних цінностей та інкасації коштів.

Для забезпечення схоронності валютних цінностей під час їх перевезення та інкасації з працівниками підрозділу інкасації — членами бригади інкасації укладається письмовий договір про повну індивідуальну матеріальну відповідальність або договір про колективну (бригадну) матеріальну відповідальність відповідно до законодавства.

Підрозділи інкасації під час перевезення валютних цінностей та інкасації коштів використовують власний оперативний автотранспорт, який може бути обладнаний спеціальними звуковими та світловими сигналами синього кольору в порядку,

визначеному нормативно-правовими актами Міністерства внутрішніх справ України.

Порядок придбання, зберігання, використання, застосування та вилучення вогнепальної зброї і боєприпасів до неї встановлюється нормативними актами Міністерства внутрішніх справ України.

Під час перевезення валютних цінностей та інкасації коштів обов'язково використовуються засоби радіозв'язку, що забезпечують надійний та постійний зв'язок, та індивідуальні засоби захисту (бронежилети), носіння яких незалежно від обсягів цінностей є обов'язковим під час перевезень валютних цінностей та інкасації коштів.

Не допускається виїзд бригади інкасаторів на маршрути з перевезення цінностей та інкасації коштів без проведення службових інструктажів під розписку у відповідному журналі.

Під час приймання (здавання) готівки інкасатори Національного банку пред'являють у банківській установі відповідальним особам службові посвідчення і доручення на перевезення валютних цінностей для приймання готівки.

Виявлені інкасаторами Національного банку пачки банкнот і мішечки з монетами, які не відповідають установленим правилам пакування, не приймаються.

Доставлені в банківську установу валютні цінності інкасатори Національного банку здають відповідальним особам згідно з описом цінностей і з дотриманням зазначених вище вимог.

Пачки з банкнотами і мішечки з монетою (упаковки з роликами), що доставлені інкасаторами Національного банку в пошкодженій або сумнівній упаковці, касові працівники приймають з поаркушним перерахуванням або перерахуванням за кружками в присутності всіх інкасаторів бригади інкасації після приймання всіх цінностей.

У разі виявлення під час перерахування недостач або надлишків готівки в пачках, окремих корінцях або в мішечках з монетою в пошкодженій упаковці складається акт про розбіжності, який підписують працівники банку та всі інкасатори бригади.

Банківські установи здійснюють перевезення валютних цінностей від/до територіальних управлінь, між банківськими установами власними підрозділами інкасації чи підрозділами інкасації інших банківських установ з прийманням (здаванням) валютних цінностей в боксах інкасації або інкасаторами Національного банку.

Інкасація коштів здійснюється підрозділом інкасації банківської установи з дотриманням вимог чинного законодавства. Складання маршрутів з інкасації здійснюється з урахуванням безпеки роботи інкасаторів на маршруті, а саме: протяжності маршруту та безпеки вибраного напрямку перевезення, часу роботи інкасаторів на маршруті, наявності вільних та освітлених під'їзних шляхів, часу заїзду для здійснення інкасації, обсягів готівки, що інкасується, тощо.

Банківська установа у внутрішньому документі визначає найбільшу суму проінкасованої готівки, що може зберігатися в оперативному автомобілі на маршруті інкасації. У разі перевищення цієї суми під час маршруту інкасатори здійснюють позачергову доставку готівки до банку згідно з порядком та особливостями, передбаченими у внутрішньому документі.

Операції з пластиковими платіжними засобами. Останнім часом значного поширення набувають операції банків з пластиковими платіжними картками. Разом з тим простежується тенденція до зростання втрат банків, які здійснюють такий вид діяльності, через шахрайство з пластиковими платіжними картками. Тому банки змушені звертати серйозну увагу на забезпечення безпеки цих операцій. На даний час у банківських установах напрацьовано відповідний досвід щодо забезпечення безпеки таких операцій, який у цілому базується на комплексному підході до організації їх захисту протягом усіх циклів, з яких ці операції складаються. Зокрема, такий підхід включає:

- розроблення і вдосконалення нормативної бази технологій, як самих платіжних карток, так і операцій з ними;
- протидію втратам банків від шахрайських дій у процесі емісії та еквайрингу;
- навчання співробітників банку та підприємств торгівлі (послуг) і складання ними кваліфікаційних іспитів на допуск до роботи з банківськими продуктами — платіжними картками.

Серед документів банку, які регулюють ті чи ті види його діяльності, відповідне місце займають документи щодо забезпечення банківської безпеки, у тому числі і операцій з платіжними картками. Базу для формування нормативних документів з безпеки операцій з платіжними картками створюють Законів України «Про платіжні системи та переказ коштів в Україні» [154] та «Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг», Положення Національного банку України

«Про порядок емісії спеціальних платіжних засобів і здійснення операцій з їх використанням», затверджене постановою Правління Національного банку України від 30 квітня 2010 р. № 223 та Положення Національного банку України «Про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем», затверджене постановою Правління Національного банку України від 25 вересня 2007 р. № 348. З огляду на особливість роботи з платіжними картками нормативному регулюванню підлягають такі питання:

- забезпечення безпеки роботи, пов'язаної з емісією платіжних карток;
- дії банку, направлені на мінімізацію ризиків від операцій з платіжними картками;
- забезпечення безпеки при наданні послуг з платіжними картками та роботі із заборгованістю клієнтів, що виникла внаслідок дебетово-кредитних та кредитних платіжних схем.

Навчання працівників банку задіяних у операціях з платіжними картками, має передбачати оволодіння необхідними навичками підготовки та складання договорів на надання відповідних послуг, перевірки клієнтів, прийняття рішення про співпрацю з конкретними клієнтами, дій щодо супроводження операцій з платіжними картками, а за умов порушення встановленого порядку (технології) — дій відповідно до умов порушення.

Основних втрат від шахрайств із платіжними картками зазнають банки-емітенти, оскільки практично всі відомі методи шахрайств побудовані на несанкціонованому списанні коштів з рахунків клієнтів емітента.

У мінімізації втрат банку під час процесу емісії можна виділити такі основні моменти забезпечення безпеки:

— забезпечення фізичної (захист та охорона приміщень і обладнання підрозділів, які виконують відповідну роботу з платіжними картками) і технологічної (забезпечення безпеки кожного технологічного циклу) безпеки процесу виробництва карток, процесування трансакцій і забезпечення процесу авторизації;

— забезпечення оптимального рівня перевірки персональних даних потенційних власників платіжних карток;

— забезпечення інформаційно-аналітичної діяльності щодо раннього виявлення шахрайських дій з платіжними картками.

Основним завданням безпеки під час процесу емісії є виключення можливості зникнення заготівок карток, збереження в

таємниці інформації щодо параметрів платіжних карток та недопущення зловживань у процедурі виготовлення карток працівниками банку.

Усі технологічні зони емісійного процесу (сховище для заготівок і персоналізованих карток, приміщення для ембосування, друкування ПІН-конвертів, приміщення авторизації, комп'ютерний зал) мають бути територіально розмежовані та обладнані певною системою охорони.

За оцінками банків попередня перевірка клієнтів є одним із найважливіших умов забезпечення безпеки роботи з платіжними картками і зниження обсягу втрат. Результати від цих заходів дають змогу виявити на початковому етапі роботи із заявником осіб, які прагнуть одержати пластикову картку шахрайським способом (за підробленими, недійсними документами, надання про себе неправдивої інформації тощо).

Дана робота може вестися по двох напрямах:

- попередня перевірка фізичних осіб і організацій при вирішенні питання про видачу платіжної картки;
- попередня перевірка юридичних осіб перед укладанням договору на еквайринг.

Для розв'язання завдання по першому напрямку деякі банки умовно розділяють клієнтів по групах ризику на основі двох головних принципів:

- можливості встановлення місцезнаходження клієнта;
- можливості стягнення допущеної заборгованості за операціями з використанням спеціальних платіжних засобів.

На цій основі всі заявники поділяються на дві групи:

— громадяни України (потенційні групи ризику — пенсіонери, домогосподарки, студенти, тимчасово не працюючі, особи з нестабільним рівнем доходу);

— не громадяни України (ближнє і дальнє зарубіжжя, співробітники представництв іноземних держав на території України).

Обов'язковими умовами для всіх клієнтів при вирішенні питання про видачу платіжної картки є наявність постійного джерела прибутків (роботи), дотримання правил про порядок реєстрації громадян на території України, контактні телефони, перевірка анкетних даних клієнта на предмет їхньої достовірності. За результатами перевірки робиться висновок про доцільність надання клієнту даного виду банківських послуг. Особлива увага приділяється клієнтам, які відносяться до категорії підвищеного ризику. Крім інформаційно-аналітичної

оцінки анкетних даних клієнта може бути здійснено виїзд за адресою, зазначеною в анкеті.

Обов'язковою умовою укладання договору на еквайринг є перевірка торгівельно-сервісних пунктів. Спочатку проводиться інформаційно-аналітична оцінка документів клієнта, а потім здійснюється виїзд на фірму. Під час виїзду можуть бути вирішені такі завдання:

- огляд фактичного місця розташування організації; зустріч із керівництвом фірми;
- ознайомлення з персоналом, відповідальним за проведення операцій по картках;
- організація обліку і збереження сліпів;
- організація контролю з боку керівництва фірми за роботою персоналу.

Залежно від умов, за якими здійснюються платіжні операції з використанням спеціальних платіжних засобів, можуть застосовуватися дебетова, дебетово-кредитна та кредитна платіжні схеми.

Дебетова схема передбачає здійснення користувачем платіжних операцій із використанням спеціального платіжного засобу в межах залишку коштів, які обліковуються на його рахунку, або за рахунок коштів споживача за наперед оплаченими спеціальними платіжними засобами, які обліковуються на рахунку емітента.

Під час застосування дебетово-кредитної схеми користувач здійснює платіжні операції з використанням спеціального платіжного засобу в межах залишку коштів, які обліковуються на його рахунку, а в разі їх недостатності або відсутності — за рахунок наданого банком кредиту.

Кредитна схема передбачає здійснення користувачем платіжних операцій з використанням спеціального платіжного засобу за рахунок коштів, наданих йому банком у кредит або в межах кредитної лінії.

Кредитна лінія під операції зі спеціальними платіжними засобами відкривається банком на певний термін і в межах установленого договором ліміту заборгованості або граничної суми кредитування. Строк дії кредитної лінії, яка відкривається під спеціальні платіжні засоби, установлюється договором.

Користувач на власний розсуд або відповідно до умов кредитного договору, якщо кредит має цільовий характер, частково або в повному обсязі використовує кредит протягом строку дії кредитного договору і зобов'язаний повернути кредит

та проценти за користування ним на умовах, установлених кредитним договором.

Організація роботи з клієнтами щодо проблемної заборгованості, за операціями з використанням спеціальних платіжних засобів здійснюється так само, як і з клієнтами, які мають кредитну заборгованість.

Як показує досвід більшості комерційних банків України — членів платіжних систем, платіжні засоби дозволяють оперувати тільки наявними на рахунку держателя картки коштами за допомогою безготівкових розрахунків.

Платіжні картки повинні прийматися для оплати товарів і різноманітних послуг підприємствами торгівлі і сервісних пунктів в Україні і за її межами (якщо картка міжнародна). У разі втрати картки її держатель зобов'язаний негайно сповістити про це банк-емітент.

У свою чергу, банк-емітент або визначена ним юридична особа під час отримання повідомлення та/або заяви про втрату спеціального платіжного засобу зобов'язаний ідентифікувати держателя і зафіксувати обставини, дату, годину та хвилини його звернення на умовах і в порядку, установлених договором. Крім того, після надходження вказаного повідомлення банк-емітент зобов'язаний негайно зупинити здійснення операцій з використанням цього спеціального платіжного засобу.

Залишок коштів на рахунку в разі втрати спеціального платіжного засобу або закінчення терміну його дії, а також розірвання чи припинення дії договору за дорученням власника рахунку перераховується на інші рахунки або видається готівкою з дотриманням термінів, установлених правилами платіжної системи та договором.

Емітенти карток повинні інформувати мережу сервісних організацій про номери карток, які визнані недійсними: украдені, загублені, фальсифіковані, фальшиві. Така інформація доводиться у вигляді списку номерів платіжних карток, який називається «стоп-листом». Це список карток, які повинні бути вилучені у клієнта, де б вони не пред'являлись до сплати.

Для підвищення якості карткового обслуговування населення в даний час широко використовуються банкомати. *Банкомат* — це програмно-технічний комплекс, що дає змогу держателю спеціального платіжного засобу здійснити самообслуговування за операціями з одержання коштів у готівковій формі, унесення їх для зарахування на відповідні рахунки, одержання інформації

щодо стану рахунків, а також виконати інші операції згідно з функціональними можливостями цього комплексу. Ще при оформленні картки клієнт одержує крім самої картки запечатаний конверт, що містить PIN-код — набір цифр або набір букв і цифр, відомий лише держателю спеціального платіжного засобу і потрібний для його ідентифікації під час здійснення операцій із використанням спеціального платіжного засобу (не знає PIN-код навіть банк; код автоматично наноситься на папір і запечатується в конверт при видачі картки; визначити PIN-код, звернувшись до комп'ютера в банку, неможливо, бо на магнітній смузі його теж немає).

Під час здійснення операції банкомат у певний момент запитує PIN-код. При спробі тричі набрати неправильний помилковий PIN-код банкомат захоплює картку. Теж відбувається, якщо результат авторизації негативний. Коли ж усе гаразд, держатель картки, може продовжити здійснення операції, а також, при бажанні — виписку про стан рахунку, сума на якому змінилася за командою пристрою.

Останнім часом спектр злочинних посягань на кошти клієнтів банків, що перебувають на карткових рахунках значно розширився. Поява фішингу банкоматів з так званими скімерами — обладнанням, що дає змогу знімати з магнітної стрічки пластикової картки інформацію, яка дозволяє виготовити дублікат картки. Ще одним способом посягання на карткову інформацію є встановлення спеціальної накладки на клавіатуру банкомату, яка дає можливість узнати PIN-код картки. Цікаво, що комплект із скімера і накладки можна вільно придбати через Інтернет, що робить такі посягання досить поширеними.

З метою попередження та захисту від цих та інших посягань на карткові кошти клієнтів банків було б доцільним ввести так зване SMS-інформування їх про проведені операції по карткових рахунках. У цьому разі про проведення будь-якої операції з використанням карткового рахунку клієнта йому надходить SMS-повідомлення і в такий спосіб він може контролювати наявність та витрати його коштів та відповідно реагувати на несанкціоновані ним операції.

Ще одним способом захисту картки є використання при її виготовленні мікропроцесора — спеціального чіпа. Підробити чіп досить складно.

В умовах поширення посягань на банкомати й операції, які вони проводять доцільно обладнувати їх системами відеоспостереження. Також відеокамера страхує банк на випадок,

коли клієнт хоче ввести банк в оману, що до його рахунку хтось має несанкціонований доступ і викрадає його кошти, коли насправді гроші знімаються ним самим.

Валютні та неторговельні операції. Серед операцій банків значне місце займають валютні операції. Тому захист таких операцій, особливо операцій, пов'язаних з міжнародними розрахунками, також має велике значення в системі економічної безпеки банків.

Однією з найбільш значимих сфер валютного й експортного контролю є операції по міжнародних торговельних розрахунках. Їхня важливість визначається насиченням валютного ринку України вільноконвертованою валютою, проблемою повернення коштів із-за кордону, стабілізацією курсу національної валюти.

Найбільш поширеною формою міжнародних розрахунків по експортно-імпортних операціях у нашій країні є акредитивна форма.

Банк, отримавши заяву на відкриття акредитиву, повинен ретельно проаналізувати і подану заяву, і наданий договір (контракт). Аналіз проводиться послідовним розглядом кожного пункту заяви щодо відповідності його наданому договору (контракту).

Важливим, з точки зору безпеки, моментом є розгляд наданих експортером документів і прийняття рішення за ними. Тут слід чітко керуватись принципом суворої відповідності тексту наданих документів умовам акредитива (банк може здійснити платіж тільки проти тих документів, які повністю відповідають акредитиву) та строків відвантаження товарів і надання документів (банк має право не здійснювати платежі за документами, які надані пізніше визначеної дати та терміну).

У разі позитивного розгляду заяви і прийняття рішення щодо відкриття акредитиву банк виконує відповідні дії, передбачені технологією таких операцій. Щодо елементів захисту технології проведення зазначеної операції, то слід звернути увагу на таке.

Банк-емітент відкриває акредитив за умови, що він забезпечений грошовими коштами наказодавця акредитива (покритий акредитив), або на підставі відкритих наказодавцю акредитива уповноваженим банком-емітентом кредитних ліній, або на підставі отриманих у кредит коштів, або на підставі гарантій, наданих третіми сторонами на користь уповноваженого банку-емітента, або на підставі забезпечення наказодавцем акредитива відповідною заставою, порукою тощо, або без будь-якого забезпечення згідно з внутрішніми положеннями уповноваженого банку-емітента (непокритий акредитив).

Якщо іноземна валюта грошового забезпечення акредитива відрізняється від виду іноземної валюти, у якій відкривається акредитив, визначеного умовами акредитива, то сума коштів грошового забезпечення акредитива за вимогою уповноваженого банку-емітента може бути збільшена на суму можливих ризиків від зміни курсів іноземних валют за умови, що це передбачено в заяві про відкриття акредитива та/або в договорі банківського рахунку та/або інших договорах, укладених між наказодавцем акредитива та уповноваженим банком-емітентом.

Якщо кошти грошового забезпечення надані в грошовій одиниці України, то в разі значного зростання курсу іноземної валюти або гривні в заяві про відкриття акредитива наказодавець акредитива повинен передбачити право уповноваженого банку-емітента списати (у день виконання платежу за акредитивом) з поточного рахунку наказодавця акредитива додаткову суму коштів у національній валюті для здійснення операції з купівлі іноземної валюти на міжбанківському валютному ринку України з метою забезпечення покриття за акредитивом у повному обсязі.

Під час перевірки документів, які надані бенефіціаром, необхідно спочатку впевнитися, що за зовнішніми ознаками вони відповідають умовам акредитива. Якщо в них виявлено якісь розбіжності, слід вважати, що такі документи не відповідають умовам акредитиву. І в такому разі банк повинен діяти відповідно до вимог, указаних у Положенні про порядок здійснення уповноваженими банками операцій за документарними акредитивами в розрахунках за зовнішньоекономічними операціями, затвердженому постановою Правління Національного банку України від 3 грудня 2003 р. №514.

Оцінюючи документи, необхідно:

- перевірити їх комплексність (наявність усіх перелічених в акредитиві документів у необхідній кількості примірників);
- перевірити правильність оформлення кожного документа та його відповідність вимогам акредитива (правильність заповнення реквізитів бланку документа, наявність підписів, печаток, штампів, передавальних надписів, віз, застережень або інших поміток, які обумовлені в акредитиві, або формою самого документа), а також впевнитись у відсутності явних слідів підробок;
- перевірити документи за змістом та цифровими даними (документи повинні відповідати вимогам акредитива і не містити ніяких суперечностей, весь комплект документів повинен

Також підлягають перевірці: транспортні документи, страхові документи, комерційні рахунки.

Крім того, банк повинен ретельно стежити за виконанням бенефіціаром решти умов акредитива:

- установлених в акредитиві строків;
- умов транспортування товару;
- умов, що стосуються кількісних та якісних характеристик товару;
- умов, що стосуються страхування товару та інших умов.

З метою попередження втрат від шахрайства при розрахунках за акредитивом банку слід отримати від особи, на користь якої видається акредитив відомості, що підтверджують факт реального існування організації-продавця, надійність контракту і наявність можливостей виконати поставку товару.

Таким чином, акредитивна форма розрахунків сама по собі є однією із захисних форм участі банків у міжнародних торговельних розрахунках. А проведення зазначених перевірок, передбачених технологією розрахунків за допомогою акредитивів, є важливим елементом захисту самої розрахункової операції.

Подібні елементи захисту застосовуються і при інших формах розрахунків — інкасо, гарантій. Важливим, з погляду безпеки, тут буде безумовне дотримання банками технологій проведення операцій, передбачених відповідними законодавчими та нормативними актами. Практично всі елементи захисту спрямовані на отримання банками інформації, яка б найбільшою мірою характеризувала об'єктивну сторону тієї чи тієї операції.

Одним із видів неторговельних операцій банків є операції з іменними і дорожніми чеками. Чек — паперовий розрахунковий документ установленої форми, що містить нічим не обумовлене письмове розпорядження чекодавця платнику про сплату чекодержателю зазначеної в ньому суми коштів протягом установленого строку. Сфера чекового обігу зазнає досить сильного впливу різного роду махінацій і зловживань, оскільки основним ідентифікатором власника чека часто є його підпис (насамперед іменні та дорожні чеки). Тому банки повинні приділяти досить серйозну увагу захисту таких операцій. Так, іменні чеки в основному повинні прийматися на інкасо. Тобто прийнятий чек після його перевірки на справжність (водяний знак, випуклість зображень, реакція на ультрафіолетове

випромінювання і т. п.), правильність заповнення, термін дії й оформлення відповідно всіх документів, відправляється іноземному банку, який, у свою чергу, також перевіряє справжність чека для виплати клієнту. Наявність подвійного контролю є неприваблівим для шахраїв, тому операції з іменними чеками, які приймаються на інкасо, часто обходяться ними. У даному разі зловживання може бути тільки за наявності змови шахрая і банківського працівника при перевірці документів. В останньому випадку слід забезпечувати контроль діяльності працівників, задіяних в операціях з чеками, періодичні перевірки їх роботи та документів, виконаних ними, а також перевіряти всі скарги та заяви, які надходять з приводу порушень правил проведення операцій з чеками.

Дорожній чек — це паперовий розрахунковий документ, що виражений в іноземній валюті та використовується як засіб міжнародних розрахунків неторговельного характеру і є грошовим зобов'язанням чекодавця виплатити зазначену в чеку суму чекодержателю (власникові), підпис якого проставляється в зазначеному місці під час продажу. Такі чеки друкуються на спеціальному папері і мають відповідні номінали, вид і захисні засоби.

Основними заходами безпеки в операціях з дорожніми чеками за досвідом банків можуть бути:

—операції з продажу дорожніх чеків фізичній особі-резиденту здійснюються після пред'явлення цією особою касиру каси банку (установи) або пункту обміну валюти банку (установи) паспорта громадянина України або довідки на проживання особи, яка мешкає в Україні, але не є громадянином України, та проїзного документа особи без громадянства для виїзду за кордон або паспорта для виїзду за кордон;

—операції з продажу дорожніх чеків фізичній особі-нерезиденту здійснюються після пред'явлення цією особою уповноваженому працівникові банку (установи) паспорта або іншого документа, що посвідчує особу, та за наявності підтверджених документів про джерела походження іноземної валюти у нерезидента. (У в'їзній митній декларації на ввезення готівкової іноземної валюти нерезидента робиться відмітка про продаж дорожніх чеків);

—після продажу дорожніх чеків фізична особа (резидент чи нерезидент) або уповноважений представник юридичної особи-резидента, або уповноважена особа представництва юридичної особи-нерезидента, що від'їжджають у службове відрядження, у присутності працівника банку (установи) ставлять свій підпис на

—під час купівлі (сплати) дорожніх чеків уповноважений працівник банку (установи), пункту обміну валют банку (установи):

- перевіряє паспорт або інший документ, що посвідчує особу, а також відсутність на дорожніх чеках виправлень або написів, які заважають прочитанню першого підпису власника;
- перевіряє реквізити дорожніх чеків на наявність захисних елементів дорожніх чеків і першого підпису чекодавця у відповідному місці;
- перевіряє відповідність першого підпису чекодержателя на дорожніх чеках його підпису в паспорті або іншому документі, що посвідчує особу;
- з'ясовує назву іноземної валюти, яку чекодержатель бажає одержати за дорожніми чеками;
- стежить за тим, як і де чекодержатель ставить другий підпис на дорожніх чеках згідно з правилами, установленими емітентом;
- у разі виникнення будь-яких сумнівів щодо дійсності підпису пропонує чекодержателю підписати дорожні чеки втретє на зворотному боці та записує паспортні дані; пропонує надати повідомлення про продаж дорожніх чеків, де зазначено їх кількість, серію, номер, назву іноземної валюти, номінал та загальну суму, а також є підпис чекодержателя;
- при виникненні серйозних сумнівів, а також при виплаті по чеку значних сум рекомендується зв'язатися з емітентом дорожнього чека і пересвідчитися, чи немає номера даного чека в списках вкрадених чи загублених;
- якщо чек є вкраденим чи загубленим, або особистість власника викликає певні сумніви, такий чек не оплачується і не повертається власникові. Про таке доцільно, не викликаючи підозри у власника чека, повідомити правоохоронні органи.

На безпеку валютних операцій уповноважених банків може мати значний вплив необдуманий вибір банків-кореспондентів за кордоном. При виборі банку-кореспондента необхідно керуватися інформаційними довідниками міжнародних рейтингових агентств, де містяться списки банків, оцінені за різними видами рейтингу. Відкриваючи коррахунок, необхідно вивчити установчі документи, баланс на останню звітну дату, список банків-кореспондентів даного банку, установити ліміти

коштів у розрахунках із банком-кореспондентом, домовитися про умови обслуговування рахунку, одержати зразки підписів співробітників банку, юридичну адресу, телефони та іншу необхідну інформацію. Більша частина порушень відбувається при здійсненні розрахунків по «лоро»-рахунках банків-кореспондентів, оскільки режим їх функціонування неврегульований (проплати за кордон за підробними документами, «відмивання» грошей за допомогою «лоро»-рахунків, коли «брудні» гроші, які накопичуються на рахунках іноземних банків, використовуються для оплати товару українського виробника і т. п.). З метою недопущення перелічених вище порушень банкам необхідно вимагати від українських резидентів, які перераховують іноземним партнерам гривню на «лоро»-рахунки, таких же документів суворої звітності (митних декларацій, контрактів), як і для проведення конвертаційних операцій на Українській міжбанківській валютній біржі, а для здійснення авансових платежів доцільно застосовувати різноманітні форми акредитивів, не видавати кредити нерезидентам у національній валюті. Якщо банк здійснює термінову купівлю національної валюти у нерезидента за валюту, бажано розраховуватися напряму, уникаючи посередників. Крім того, комерційним банкам корисно диверсифікувати торгівлю валютою, що дає змогу скоротити ризик неплатежів. Сюди може ввійти система одночасних розрахунків, за якої банк і центральна клірингова палата зобов'язані здійснювати одночасні розрахунки. При купівлі-продажу валюти існує також ризик неотримання прибутку, коли кошти не використовуються. Так, стандартний термін здійснення угоди «спот» — два робочі дні. Тому банкам при здійсненні перерахувань необхідно виходити з того, що робочі дні не включають суботи, неділі або свята в обох країнах, чиї валюти використовуються, угоди між американськими і канадськими доларами проводяться на наступний робочий день. На Середньому Сході FX ринки закриті по п'ятницях, але відкриті по суботах.

9.3.2. Протидія банку втягуванню його в незаконну фінансову діяльність

Наявність на ринку банківських послуг значних обсягів коштів, які мають незаконне або сумнівне походження, утворює для банків ризик втягування їх у незаконну фінансову діяльність. Мова йде не тільки про легалізацію (відмивання) незаконно отриманих коштів, а й про ризик формування банком свого фінансового ресурсу за рахунок таких коштів, створення і використання банком позабалансових фінансових інструментів, формування взаємовідних відносин з фіктивними організаціями і підприємствами. Усі ці дії так чи інакше створюють для банку загрозу протизаконної діяльності з очевидними для нього наслідками. Як правило, в операціях з легалізацією коштів злочинці відводять банкам провідне місце, тому одним із найважливіших завдань економічної безпеки банків є боротьба з так званим відмиванням грошей. Сьогодні цій проблемі приділяється досить велика увага як безпосередньо у нашій державі, так і на міжнародному банківському ринку. У контексті даного питання, з метою єдиного розуміння і вжиття необхідних заходів щодо протидії відмиванню грошей міжнародними та вітчизняними організаціями і установами прийнято ряд рішень і документів (Закон України «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними», Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму», Закон України «Про банки та банківську діяльність», Постанова Кабінету Міністрів України і Національного банку України від 28 серпня 01 р. №1124 «Про сорок рекомендацій групи з розроблення фінансових заходів боротьби з відмиванням брудних грошей (FATF), Положення про здійснення банками фінансового моніторингу, затвердженого постановою Правління Національного банку України від 14 травня 2003 р. №189).

Виконуючи вимоги міжнародних організацій та реалізуючи власні програми з боротьби з легалізацією незаконно отриманих коштів, Україна сформувала певну систему із запобігання і протидії проведенню сумнівних та незвичних фінансових операцій, спрямовану на здійснення контролю за операціями, які проводять суб'єкти господарювання і фізичні особи (рис.9.7).

Координацію заходів з протидії незаконно отриманих коштів здійснює Державний комітет фінансового моніторингу. До участі в проведенні контролю фінансових операцій юридичних і

фізичних осіб залучено досить багато суб'єктів, провідне місце серед яких займають банки.

Згідно з чинним законодавством контроль операцій проводиться у формі фінансового моніторингу, який має два рівні: первинний і державний.

У першому випадку — це сукупність заходів, які здійснюються суб'єктами первинного фінансового моніторингу, спрямованих на виконання вимог чинного законодавства, що включають проведення обов'язкового та внутрішнього фінансового моніторингу.

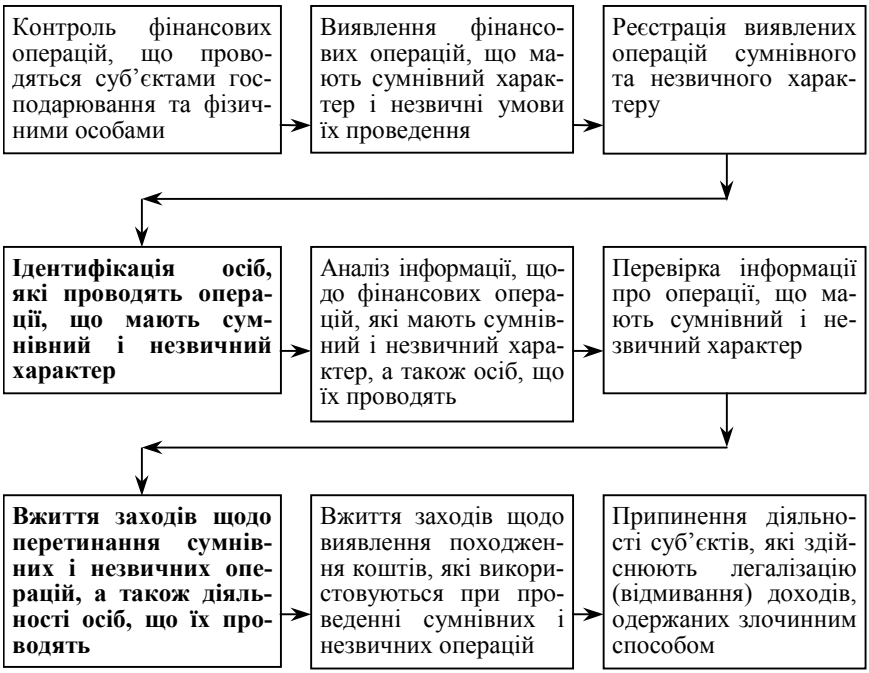

Рис. 9.7. Алгоритм дій з виявлення, перетинанню та припиненню діяльності з відмивання незаконно отриманих доходів

У другому випадку контроль має передбачати сукупність заходів, які здійснюються суб'єктами державного фінансового моніторингу, спрямованих на виконання вимог законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму.

Банки якраз є суб'єктами первинного фінансового моніторингу. Відповідно до чинного законодавства на них, як суб'єктів первинного фінансового моніторингу, покладаються такі завдання:

1) стати на облік у Спеціально уповноваженому органі як суб'єкт первинного фінансового моніторингу та в разі припинення своєї діяльності повідомити про це Спеціально уповноважений орган у визначеному Національним банком України порядку;

2) здійснювати ідентифікацію та вивчення клієнта у випадках, установлених законом;

3) забезпечувати виявлення фінансових операцій, що підлягають фінансовому моніторингу, до початку, у процесі, у день виникнення підозр, після їх проведення або при спробі їх проведення чи після відмови клієнта від їх проведення;

4) забезпечувати у своїй діяльності управління ризиками щодо легалізації (відмивання) доходів, одержаних злочинним способом, або фінансування тероризму та розробляти критерії ризиків;

5) забезпечувати реєстрацію фінансових операцій, що підлягають фінансовому моніторингу, не пізніше наступного робочого дня з дати їх виявлення;

6) повідомляти Спеціально уповноважений орган про:

а) фінансові операції, що підлягають обов'язковому фінансовому моніторингу, — протягом трьох робочих днів з дня їх реєстрації або спроби їх проведення;

б) фінансові операції, що підлягають внутрішньому фінансовому моніторингу, якщо є достатні підстави підозрювати, що вони пов'язані з легалізацією (відмиванням) доходів, одержаних злочинним способом, — у день виникнення підозр, але не пізніше, ніж через десять робочих днів з дня реєстрації таких операцій або спроби їх проведення;

в) виявлені фінансові операції, стосовно яких є достатні підстави підозрювати, що вони пов'язані, стосуються або призначені для фінансування тероризму, — у день їх виявлення або спроби їх проведення, а також інформувати про це визначені законом правоохоронні органи;

7) у разі отримання від Спеціально у повноваженого органу повідомлення про некоректне (неправильне) заповнення полів у повідомленні про фінансову операцію, що підлягає фінансовому моніторингу, подати протягом трьох робочих днів до Спеціально уповноваженого органу належно оформлене повідомлення про

цю фінансову операцію;

8) сприяти в межах чинного законодавства працівникам Спеціально уповноваженого органу в проведенні аналізу фінансових операцій;

9) надавати на запит Спеціально уповноваженого органу додаткову інформацію з приводу фінансових операцій, які стали об'єктом фінансового моніторингу, копії первинних документів, на підставі яких були проведені такі операції та пов'язані з ними фінансові операції, відомості про їх учасників, а також іншу інформацію, зокрема ту, що становить банківську або комерційну таємницю, таємницю страхування, копії документів, необхідні для виконання покладених на Спеціально уповноважений орган завдань, протягом п'яти робочих днів з дати надходження запиту;

10) надавати на запит Спеціально уповноваженого органу інформацію (у тому числі копії документів), необхідну для виконання ним запиту, що надійшов від уповноваженого органу іноземної держави, зокрема ту, що становить банківську або комерційну таємницю, протягом п'яти робочих днів з дати надходження запиту;

11) надавати на запит Спеціально уповноваженого органу інформацію щодо відстеження (моніторингу) фінансових операцій клієнта, операції якого стали об'єктом фінансового моніторингу. Порядок надання такої інформації встановлюється Спеціально уповноваженим органом за погодженням з відповідними суб'єктами державного фінансового моніторингу;

12) у разі неможливості забезпечити дотримання строків, установлених пунктами 9, 10, з об'єктивних причин, з урахуванням обсягу інформації, що запитується (форми її подання — електронної або письмової, копіювання або сканування, одержання даних з архівів тощо), погодити зі Спеціально уповноваженим органом протягом робочого дня в день одержання запиту, але не пізніше наступного робочого дня термін подання запитуваної інформації. Порядок погодження встановлюється Спеціально уповноваженим органом за погодженням з відповідними суб'єктами державного фінансового моніторингу;

13) надавати на запит відповідного суб'єкта державного фінансового моніторингу інформацію, необхідну для перевірки фактів порушення вимог законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним способом, або фінансуванню тероризму;

14) вживати заходів щодо запобігання розголошенню (зокрема особам, стосовно фінансових операцій яких проводиться перевірка) інформації, що подається Спеціально уповноваженому органу, та іншої інформації з питань фінансового моніторингу (у тому числі про факт подання такої інформації або отримання запиту від Спеціально уповноваженого органу);

15) зберігати документи щодо ідентифікації осіб, які провели фінансову операцію, що підлягає фінансовому моніторингу, а також усі документи, що стосуються ділових відносин з клієнтом, не менше п'яти років після завершення ділових відносин, а всі необхідні дані про операції — не менше п'яти років після завершення операції (при цьому строки зберігання документів можуть бути продовжені відповідним суб'єктом державного фінансового моніторингу у порядку, встановленому законодавством);

16) забезпечувати на документальний запит безперешкодний доступ суб'єктів державного фінансового моніторингу та правоохоронних органів до документів або інформації, що міститься в них, відповідно до вимог закону;

17) за дорученням Спеціально уповноваженого органу, наданим з метою виконання запиту уповноваженого органу іноземної держави про зупинення відповідної фінансової операції як такої, що може бути пов'язана з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму, зупиняти проведення або забезпечити моніторинг фінансової операції відповідної особи у порядку, установленому Спеціально уповноваженим органом за погодженням з відповідними суб'єктами державного фінансового моніторингу;

18) забезпечувати розроблення та постійне оновлення правил, програм проведення фінансового моніторингу з урахуванням вимог законодавства;

19) щорічно проводити внутрішні перевірки своєї діяльності щодо дотримання законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним способом, або фінансуванню тероризму;

20) забезпечувати підвищення кваліфікації працівників, відповідальних за проведення фінансового моніторингу, способом проходження навчання не рідше одного разу на три роки;

21) вживати на постійній основі заходів з підготовки персоналу до виявлення фінансових операцій, що підлягають

фінансовому моніторингу відповідно до чинного законодавства, шляхом проведення освітньої та практичної роботи;

22) виявляти фінансові операції, що підлягають обов'язковому фінансовому моніторингу відповідно до чинного законодавства;

23) проводити аналіз фінансових операцій, спрямований на виявлення тих, що підлягають внутрішньому фінансовому моніторингу відповідно до чинного законодавства;

24) з'ясовувати мету та характер майбутніх ділових відносин з клієнтами;

25) постійно оновлювати відповідно до законодавства та внутрішніх процедур інформацію про зміст діяльності клієнта та його фінансовий стан;

26) проводити аналіз відповідності фінансових операцій, що проводяться клієнтом, наявній інформації про зміст його діяльності та фінансовий стан;

27) вживати належних заходів для обмеження ризику зловживань, пов'язаних з послугами, що надаються з використанням новітніх технологій, зокрема забезпечують проведення операцій без безпосереднього контакту з клієнтом.

Банк як суб'єкт первинного фінансового моніторингу зобов'язаний самостійно здійснювати класифікацію своїх клієнтів з урахуванням критеріїв ризиків, визначених Спеціально уповноваженим органом та органами, що здійснюють регулювання та нагляд за їх діяльністю, під час проведення ними фінансових операцій, що можуть бути пов'язані з легалізацією (відмиванням) доходів, одержаних злочинним способом, або фінансуванням тероризму, і вживати застережних заходів щодо клієнтів, діяльність яких свідчить про підвищений ризик проведення ними таких операцій.

Для виконання поставлених завдань банки мають розробляти Правила проведення внутрішнього фінансового моніторингу та призначити особу (працівника банку), відповідальну за його проведення. Цей працівник має бути незалежним у своїй діяльності і підзвітним тільки керівникові банку, призначатися за посадою на рівні керівництва банку після узгодження його кандидатури з Національним банком України.

Основними вимогами до такого працівника мають бути: наявність вищої економічної або юридичної освіти, досвіду роботи в банку не менше трьох років або досвіду роботи на посаді керівника підрозділу у банках не менше одного року чи такого ж терміну роботи у сфері запобігання та протидії фінансовій злочинності, відсутність судимості за корисливі

злочини і бездоганна ділова репутація. Крім того, коли банк виконує функції професійного учасника ринку цінних паперів зазначений працівник повинен мати сертифікат Державної комісії з цінних паперів та фондового ринку про здійснення професійної діяльності на ринку цінних паперів.

Таким чином, зазначена посадова особа є основним і єдиним працівником установи банку, до компетенції якої належать практично всі питання пов'язані з діяльності банку щодо протидії легалізації (відмивання) коштів, отриманих злочинним способом.

Основу роботи банку щодо протидії легалізації (відмивання) коштів, отриманих злочинним способом, становить контроль фінансових операцій клієнтів з точки зору виявлення тих із них, що підлягають обов'язковому та внутрішньому фінансовому моніторингу. Перелік таких операцій установлено ст. 15 та ст. 16 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму». Так, обов'язковому фінансовому моніторингу підлягають операції на суму, що дорівнює чи перевищує 150 000 грн, у тому числі і її еквівалент в іноземній валюті та має одну або більше таких ознак:

1) переказ грошових коштів на анонімний (номерний) рахунок за кордон і надходження грошових коштів з анонімного (номерного) рахунку з-за кордону, а також переказ коштів на рахунок, відкритий у фінансовій установі в країні, що віднесена Кабінетом Міністрів України до переліку офшорних зон;

2) купівля-продаж чеків, дорожніх чеків або інших подібних платіжних засобів за готівку;

3) зарахування або переказ коштів, надання або отримання кредиту (позики), проведення інших фінансових операцій у разі, якщо хоча б одна із сторін — учасників фінансової операції є фізичною або юридичною особою, що має відповідну реєстрацію, місце проживання чи місцезнаходження в країні (на території), що не виконують чи неналежним чином виконують рекомендації міжнародних, міжурядових організацій, які здійснюють діяльність у сфері боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму, або однією із сторін є особа, яка має рахунок у банку, зареєстрованому у вищезазначеній країні (території);

4) зарахування на рахунок коштів у готівковій формі з їх подальшим переказом того самого або наступного операційного дня іншій особі;

5) зарахування коштів на поточний рахунок юридичної або фізичної особи — підприємця чи списання коштів з поточного рахунка юридичної або фізичної особи — підприємця, період діяльності якої не перевищує трьох місяців з дня реєстрації, або зарахування коштів на поточний рахунок чи списання готівки з поточного рахунка юридичної або фізичної особи — підприємця у разі, якщо операції на зазначеному рахунку не здійснювалися з дня його відкриття;

6) переказ особою коштів за кордон за відсутності зовнішньоекономічного договору (контракту);

7) обмін банкнот, особливо іноземної валюти, на банкноти іншого номіналу;

8) проведення фінансових операцій з цінними паперами на пред'явника, не депонованими в депозитарних установах;

9) проведення фінансових операцій з векселями з бланковим індосаментом або індосаментом на пред'явника;

10) одержання (сплата, переказ) страхового (перестрахового) платежу (страхового внеску, страхової премії);

11) проведення страхової виплати або страхового відшкодування;

12) виплата (передання) особі виграшу в лотерею, придбання фішок, жетонів, внесення в інший спосіб плати за право участі в азартній грі, виплата (передання) виграшу суб'єктом господарювання, який проводить азартні ігри;

13) здійснення розрахунків за зовнішньоекономічним контрактом, що не передбачає фактичного постачання на митну територію України товарів, робіт і послуг.

Водночас до операцій, що мають підлягати внутрішньому фінансовому моніторингу, законодавець відносить такі:

1. Заплутаний або незвичний характер фінансової операції чи сукупності пов'язаних між собою фінансових операцій, що не мають очевидного економічного сенсу або очевидної законної мети.

2. Невідповідність фінансової операції характеру та змісту діяльності клієнта.

3. Виявлення фактів неодноразового проведення фінансових операцій, характер яких дає підстави вважати, що метою їх здійснення є уникнення процедур обов'язкового фінансового моніторингу або ідентифікації (зокрема дві чи більше фінансові операції, що проводяться клієнтом протягом одного робочого дня з однією особою та можуть бути пов'язані між собою, за умови, що їх загальна сума дорівнює чи перевищує 150 000 гривень, у

тому числі і її еквівалент в іноземній валюті.

Крім того, внутрішній фінансовий моніторинг може здійснюватись і щодо інших фінансових операцій у разі коли у банку виникають підстави вважати, що фінансова операція проводиться з метою легалізації коштів або фінансування тероризму.

Виявлення операцій, що підлягають обов'язковому або внутрішньому фінансовому моніторингу здійснюється перед або після виконання такої операції клієнтом. Виявлені операції вивчаються з точки зору необхідності їх реєстрації. Як правило, у процесі вивчення здійснюється ідентифікація клієнта, якщо таке не було зроблено раніше (при відкритті рахунків у банку). Ідентифікація клієнтів банку є обов'язковою для тих з них, які відкривають у банку рахунки, здійснюють операції, що підлягають фінансовому моніторингу, або здійснюють операції з готівкою без відкриття рахунку на суму, що перевищує еквівалент 50 000 грн, а також осіб, які уповноважені діяти від імені зазначених клієнтів. Для проведення ідентифікації банки на підставі наданих клієнтами документів формують відповідні анкети. З метою ідентифікації та вивчення клієнтів банк з'ясовує таку інформацію:

а) для фізичних осіб — резидентів — прізвище, ім'я, по батькові, дату народження, серію, номер документа, що посвідчує особу, дату його видачі та орган, який видав документ, місце проживання або місце перебування, ідентифікаційний номер або серію та номер паспорта, в якому проставлено відмітку органів державної податкової служби про відмову від одержання ідентифікаційного номера;

б) для фізичних осіб — нерезидентів — прізвище, ім'я та по батькові (за наявності), дату народження, серію і номер паспорта (або іншого документа, що посвідчує особу), дату видачі та орган, що його видав, громадянство, про місце проживання або місце тимчасового перебування фізичної особи в Україні;

в) для фізичних осіб — підприємців — прізвище, ім'я та по батькові, дату народження, серію і номер паспорта (або іншого документа, що посвідчує особу), дату видачі та орган, що його видав, місце проживання або місце перебування фізичної особи — підприємця, реквізити свідоцтва про державну реєстрацію та орган, що його видав, реквізити банку, в якому відкрито рахунок, і номер банківського рахунку (за наявності);

г) для юридичних осіб — резидентів — повне найменування, місцезнаходження, реквізити свідоцтва про державну реєстрацію

та орган, що його видав; відомості про органи управління та їх склад; дані, що ідентифікують осіб, які мають право розпоряджатися рахунками і майном; відомості про власників істотної участі в юридичній особі; відомості про контролерів юридичної особи; ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України; реквізити банку, в якому відкрито рахунок, і номер банківського рахунку;

ґ) для юридичних осіб — нерезидентів — повне найменування, місцезнаходження та реквізити банку, в якому відкрито рахунок, номер банківського рахунку, відомості про органи управління та їх склад; дані, що ідентифікують осіб, які мають право розпоряджатися рахунками та майном; відомості про власників істотної участі в юридичній особі; відомості про контролерів юридичної особи, копія легалізованого витягу з торгового, банківського чи судового реєстру або нотаріально засвідчене реєстраційне посвідчення уповноваженого органу іноземної держави про реєстрацію відповідної юридичної особи.

Згідно з рекомендаціями FATF ідентифікації мають підлягати не тільки клієнти, а й беніфіціари. З метою ідентифікації беніфіціара необхідно встановити, кому у власність перейдуть кошти чи майно в результаті операції, що пропонується до проведення клієнтом банку. Якщо беніфіціаром є юридична особа, необхідно встановити, хто є її засновником і чи не є сторони такої угоди взаємозалежними особами. Особливій увазі мають підлягати разові угоди.

Значні кошти можуть відмиватися під виглядом прибутку від операцій з цінними паперами. Основними ознаками такого способу відмивання коштів можуть бути:

- операції неодноразово проводяться з одним чи кількома контрагентами і приносять постійно дохід або постійний збиток;
- регулювання проведення операцій щодо придбання і наступного перепродажу цінних паперів, які не мають котирування, не мають обігу на організованому ринку цінних паперів з використанням доходу для придбання високоліквідних цінних паперів;
- неодноразовий продаж і придбання і тих самих цінних паперів в угодах з одним і тим же суб’єктом.

У таких випадках банки можуть вдаватися до ідентифікації осіб, що проводять операції з вказаними ознаками, проводити реєстрацію операцій та приймати відповідні рішення по них.

Окремо рекомендації FATF звертають увагу на роботу банків з клієнтами — політичними діячами. Крім звичайних процедур перевірки стосовно таких клієнтів рекомендується більш ретельно підходити до питань установлення джерел коштів і порядку накопичення ними капіталу. Банкам рекомендується здійснювати постійний моніторинг ділових відносин таких осіб.

Незалежно від того, проведена ідентифікація клієнта чи ні, якщо ризик проведення клієнтом операції з легалізації коштів оцінюється банком як великий і така операція відповідає умовам проведення фінансового моніторингу вона підлягає обов'язковій реєстрації. У такому разі банк має також забезпечити перевірку наданої клієнтом інформації.

Реєстрація інформації здійснюється у відповідному електронному реєстрі банку. Рішення про внесення даних про ту чи ту операцію до реєстру приймає працівник відповідальний за проведення фінансового моніторингу в банку. Особливістю даного реєстру є те, що внесені до нього дані не підлягають коригуванню. У разі необхідності внесення якихось виправлень до реєстру (щодо певної операції) вноситься інформація про анулювання попередніх даних і заміну їх новими. Інформація з реєстру в установлений термін має бути надана Спеціально уповноваженому органу. За даними, отриманими банком про особу клієнта та про саму фінансову операцію, працівник, відповідальний за проведення фінансового моніторингу в банку, після внесення даних до реєстру приймає рішення щодо проведення чи відмови у проведенні операції (якщо інформація про операцію отримана до її проведення) та щодо надання або ненадання Спеціально уповноваженому органу інформації про таку операцію. На підставі прийнятого рішення інформація про операцію та ідентифікацію клієнта в конфіденційному порядку передається Спеціально уповноваженому органу. Слід звернути увагу, що про факт передавання зазначеному державному органу такої інформації забороняється повідомляти осіб, які здійснюють зазначену операцію або будь-яких третіх осіб.

Необхідно також звернути увагу на те, що основною фігурою в банку при проведенні ним контролю фінансових операцій клієнтів є працівники банку, які виконують відповідні функції щодо проведення операцій у банку. Саме працівники банку мають розпізнати ознаки сумнівної операції і прийняти миттєво рішення про подальші дії, які однозначно вплинуть на взаємовідносини банку з клієнтом. Тому працівники мають чітко знати як ознаки сумнівних операцій, так і особливості своєї

поведінки з клієнтами у таких випадках, для чого мають розроблятися відповідні нормативні документи, програми протидії легалізації коштів, отриманих злочинним способом. У загальних рисах схема роботи банку щодо протидії відмиванню незаконно отриманих коштів може мати вигяд такий, як це показано на рис.9.8.

Водночас ефективність роботи банків щодо виявлення операцій, які мають ознаки відмивання незаконно отриманих коштів, залежатиме від якості організації такої роботи, нормативного її регулювання, професійної компетентності фахівців, задіяних у цій роботі, знань способів відмивання коштів, які використовуються злочинцями, та української їх специфіки.

Особливістю українського «відмивання» коштів є те, що на відміну від інших економічно розвинутих країн, де здебільшого відмиваються кошти, отримані від торгівлі наркотиками, зброєю — в Україні, має місце відмивання прибутків, отриманих унаслідок вчинення фінансових злочинів, і передусім — приховування прибутків від оподаткування.

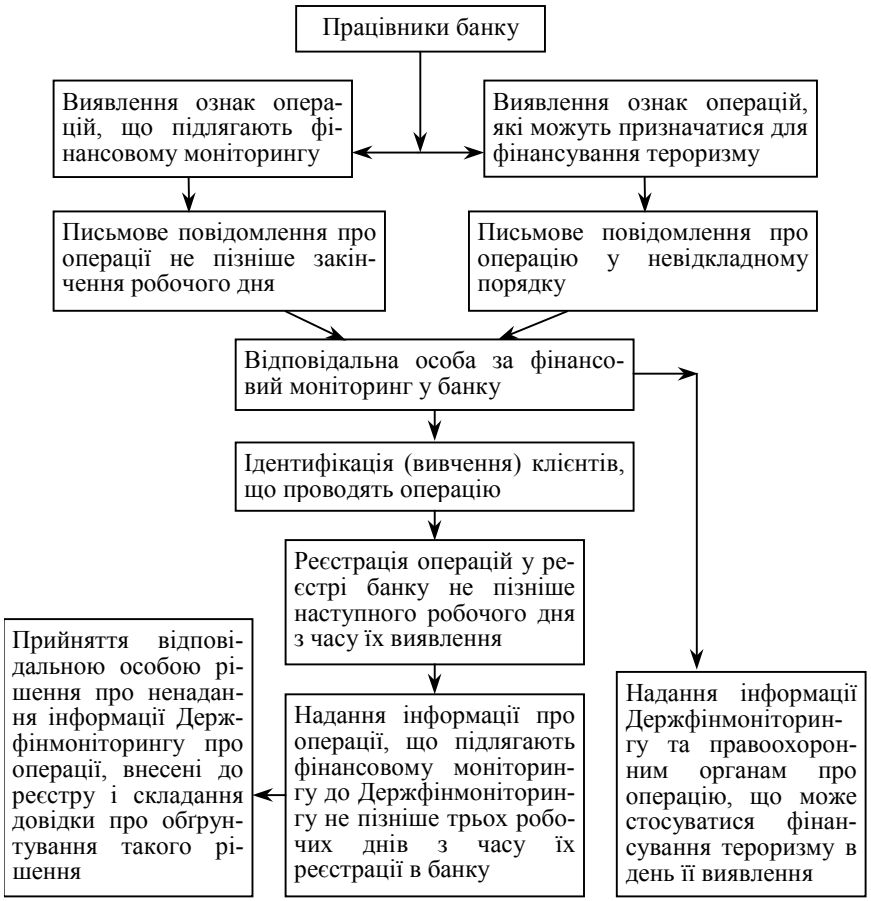

Рис. 9.8. Схема роботи банку щодо протидії відмиванню незаконно отриманих коштів

Необхідно також звернути увагу і на те, що вітчизняне відмивання найбільше відбувається у секторах так званих швидких грошей — у паливно-енергетичному й агропромисловому комплексах, на ринку підакцизних товарів, у кредитно-фінансовій системі, на фондовому ринку, у шоу бізнесі, зовнішньоекономічній діяльності.

Отже, боротьба з легалізацією (відмиванням) незаконно отриманих коштів має багатогранний характер, залучаючи значну кількість суб'єктів, важливе місце серед яких відводиться банкам. Саме через банки здійснюється понад 70% спроб легалізації

(відмивання) злочинних коштів. Тому від успіху діяльності банків у цьому напрямі буде суттєвим чином залежати не тільки рівень економічної безпеки банків, а й загальний успіх забезпечення економічної безпеки країни, принаймні у сфері боротьби з тіньовим сектором економіки.

Важливу роль у схемах «відмивання» грошей відіграють компанії розміщені в так званих офшорних зонах. Тому банки повинні звертати особливу увагу на діяльність таких компаній, і насамперед на їхні фінансові операції. Характерними особливостями існування компаній, заснованих в офшорних зонах є:

✓ засновниками компаній можуть бути особи — не громадяни даної країни, більше того, таким засновникам не обов'язково проживати в цій країні, крім того такі компанії можуть мати анонімних засновників;

✓ компанії мають право без обмежень відкривати і вести рахунки не тільки в країні, де вони зареєстровані, а й в інших країнах;

✓ компанії офшорних зон не платять податків за місцем реєстрації, сплачується тільки щорічний збір, необхідний для підтримки юридичного статусу компаній;

✓ за місцем реєстрації компанії надають фінансову звітність у спрощеній формі, що значно скорочує обсяг публічної інформації про них;

✓ компанії можуть мати номінальних директорів, які виконують тільки функції підтримки взаємовідносин компанії з державними органами країни. Керівництво господарською діяльністю компаній вони можуть і не здійснювати.

Такі умови досить привабливі і є практично закритими для здійснення різного роду шахрайських операцій, у тому числі таких, що стосуються відмивання грошей. Перелік офшорних зон періодично подається в Постановах Кабінету Міністрів України. Такі зони розташовані на Британських острівних регіонах, на близькому сході, у Центральній та південній Америці, Європі, Карибському регіоні, Африці та Тихоокеанському регіоні.

Боротьба з легалізацією незаконно отриманих коштів має зачіпати інтереси банку і з боку захисту власних фінансових ресурсів від наявності в них незаконних коштів. За таких умов при проведенні депозитних операцій і зарахуванні коштів на депозитні рахунки клієнтів банки мають перевіряти не тільки клієнтів, а й цікавитися походженням їх коштів. Нерідко результати фінансово-господарської діяльності суб'єктів

господарювання не створюють умов для формування значних коштів на їхніх депозитних рахунках. Однозначно можуть виникнути підозри стосовно джерел формування таких коштів. Інколи банки в прагненні формування фінансових ресурсів «закривають очі» на явно підозрілу поведінку рахунків своїх клієнтів. Наприклад, на значне, таке, що не відповідає обсягам обігу легального бізнесу клієнта, перевищення середніх показників залишків у касі над залишками коштів на розрахункових і поточних рахунках, або на накопичення на рахунках значних коштів і одноразове їх перерахування на рахунки різних підприємств, у тому числі і за кордон, тощо. Покриваючи таку поведінку клієнтів, банки самі втягуються в незаконну фінансову діяльність.

Відомі випадки використання банками так званих конвертаційних центрів, підставних фірм, суб'єктів, які надають сумнівні послуги.

Задля попередження такої поведінки вищі керівні органи банків мають створити певні правові документи, прямо забороняючи подібні дії, вести постійний контроль дій керівників поточною діяльністю банку, а також періодично проводити об'єктивні (а не формальні) ревізії та аудит результатів діяльності банківських установ, у тому числі і центральних офісів.

Тут слід зазначити, що в умовах ринкової економіки взагалі значно підвищується роль внутрішньобанківського контролю, так як звужуються функції зовнішніх суб'єктів контролю. Якщо організація внутрішньобанківського контролю згідно з чинним законодавством має бути покладена на керівника банку, то за певних обставин акціонери банку можуть хоча б частково взяти зазначені функції на себе, підпорядкувавши собі службу аудиту та ревізійну службу. Річний контроль діяльності банку міг би здійснюватись якраз під патронатом Ради акціонерів банку.

9.3.3. Особливості забезпечення фінансової безпеки банку в умовах глобалізації

Глобалізація створює зовсім нові умови для забезпечення фінансової безпеки банків, яка повинна ефективно перебудувати свою діяльність з тим, щоб гарантовано захистити банки від

викликів і загроз, які обумовлюються глобалізаційними процесами.

Водночас забезпечення фінансової безпеки банків буде неможливим без ефективного співробітництва сил безпеки банків з національними правоохоронними органами, з одного боку, і без міжнародної координації зусиль з силами безпеки іноземних банків, з іншого. Питання ефективної діяльності сил безпеки банків, за таких умов набуває рівня національного інтересу, передусім з точки зору забезпечення національної безпеки. Тобто забезпечення фінансової безпеки банків в умовах країни є пріоритетом не тільки одного банку чи банківської системи, а й має займати провідне місце у захисті економічних інтересів країни. Важливим фактором тут виступатиме державне регулювання взаємовідносин усіх суб'єктів, задіяних у забезпеченні безпеки національної економіки через формування відповідних правових норм.

Глобалізаційні процеси зобов'язують фінансову безпеку банків будувати свою діяльність з огляду на попередження загроз, тобто функціонування систем фінансової безпеки банків має базуватися на поєднанні заходів захисту та протидії загрозам, поширюючи такі заходи на всю структуру банківських установ.

Як показує іноземний досвід, такі підходи мають передбачати спільну діяльність сил безпеки як вітчизняних, так і іноземних суб'єктів протягом усього терміну дії їх взаємовідносин.

При забезпеченні фінансової безпеки банків важливо враховувати і зміни соціальної ситуації. Збільшення масштабів міжнародної міграції робочої сили і зменшення кількості зайнятого населення може зумовити посилення злочинного впливу на банківську діяльність, до чого також має бути готова фінансова безпека банків в умовах глобалізації. Тут необхідно звернути увагу не тільки і не стільки на створення систем охорони банків, скільки на роботу з персоналом, клієнтами, посилити пропаганду надійної та сильної системи захисту фінансових ресурсів банків, здатної протистояти будь-яким злочинним посяганням.

Водночас процеси глобалізації здатні суттєво змінити фінансову ситуацію в окремих країнах, посилити кризові явища в їх фінансово-економічній сфері. За таких умов банки мають бути здатними забезпечувати свою фінансову безпеку в умовах обмежених можливостей формування фінансових ресурсів. Іноземні інвестиції для банків можуть бути недоступними, а внутрішні ресурси під великим питанням, з одного боку, через

глобальну недовіру населення до банків, а з другого — через значне зниження активності діяльності суб'єктів господарювання. Залишається один єдиний механізм — надійне збереження та безпечне використання банками наявних ресурсів. У такому разі основним завданням фінансової безпеки (особливо в умовах фінансово-економічної кризи) буде забезпечення фінансового виживання банків та утримання хоча б мінімального рівня відтворення фінансових ресурсів (рис. 9.9).

Рис. 9.9. Завдання фінансової безпеки банків в умовах дії негативних факторів світової фінансової кризи

Таким чином, залишаючись провідною категорією в системі економічної безпеки, фінансова безпека банків потребує значних зусиль для її забезпечення, участі всіх структурних підрозділів, поширюючи свій сплив на всі сфери діяльності банків.

9.4. Протидія рейдерським посяганням на банки

Розглядаючи питання протидії рейдерським посяганням на банки, слід наголосити на тому, що вітчизняні банки поки що не навчилися сприймати проблему рейдерства всерйоз. Якщо проаналізувати сучасний стан захисту банків, то можна сказати, що створення серйозних перепон на шляху рейдерів для банків залишається проблемою. На жаль, етап захисту банків

починається тільки в момент рейдерського нападу або набагато пізніше, так як аналіз на зацікавленість рейдерів певним банком не проводиться.

Разом з тим слід зазначити, що на даний час існує певна низка заходів протидії рейдерським посяганням, у тому числі і на ринку банківських послуг. Пам'ятаючи про те, що першим етапом незаконного поглинання є розвідка, банки мають постійно звертати увагу на ознаки, що вказують на масштабний збір інформації про них. Насамперед слід знати джерела інформації про банк, на які звернуть увагу рейдери в першу чергу. Основними з таких джерел є Національний банк України, реєстратор — де зберігається реєстр кредиторів, органи податкової служби, бюро технічної інвентаризації, Асоціація українських банків, бюро кредитних історій. Саме з цими організаціями банку слід тримати тісні взаємовідносини та контролювати будь-які спроби отримати інформацію про банк через них. Отримавши інформацію про зацікавленість певних суб'єктів банком, вживаються заходи щодо ідентифікації суб'єктів і причин такої зацікавленості. Надалі дії банку будуть залежати від поведінки вказаних суб'єктів, але банк має вжити превентивних заходів щодо мінімізації ризику підпадання під рейдерську атаку. Серед них:

— формування захищеної корпоративної структури банку, тобто створення в банку такої системи управління його діяльністю і володіння власністю, яка б не дозволила рейдерам перебрати на себе управління банком і розпоряджатися його власністю без участі акціонерів. Сюди ж треба віднести і обмеження повноважень керівника банку щодо здійснення масштабних угод з фінансами і майном. Разом з тим керівник і провідні менеджери банку мають бути певною мірою мотивовані щодо ефективної своєї роботи, у тому числі і стосовно захисту від рейдерських посягань. Така мотивація може здійснюватися через участь зазначених осіб у акціонерному капіталі та прибутку банку, а також через ефективний контроль їх роботи;

— максимальна консолідація пакету акцій, бажано доведення його до контрольного. А якщо є можливість, то краще об'єднати всі акції під єдиним управлінням. Крім того, важливим буде встановлення і підтримка максимально можливої ціни на акції банку;

— підтримка тісних взаємовідносин з реєстратором акцій банку та контроль заходів, що вживаються ним щодо захисту реєстру акціонерів. Хороші стосунки з компанією-реєстратором

В окремих випадках банк може організувати власну компанію — реєстратора, єдиним засновником якої буде сам банк. Як правило, основним клієнтом такої компанії, а то і єдиним буде суб'єкт — засновник компанії, тобто банк;

- структурування банківського бізнесу з метою безпечного і конфіденційного володіння ним. Тут під структуруванням слід розуміти комплексну процедуру, яка дозволяє створити таку систему володіння і управління найбільш привабливими активами банку, яка зробить їх недосяжними для третіх осіб.

Ефективність дій банку щодо захисту від рейдерських атак залежатиме від своєчасного виявлення початку активізації рейдерів щодо банку. Однією з найбільш явних ознак є незвична поведінка міноритарних акціонерів. Від них починають надходити запити про фінансовий стан банку, плани його розвитку, роботу керівництва банку. До компанії-реєстратора надходять запити з вимогою надання витягу з реєстру кредиторів, а до Національного банку України чи Асоціації українських банків запити про надійність банку. У більшості випадків міноритарних акціонерів представляють їхні довірені особи.

Другою ознакою є звернення, знову ж таки міноритарних акціонерів, до суду з вимогою захистити їх права по несуттєвих питаннях, як правило, таких, що вирішуються без будь-яких заперечень банком. Характерно, що позови таких акціонерів подаються одночасно в кількох різних регіонах, що говорить про керованість судової процедури.

Ще однією ознакою є нездорова зацікавленість банком з боку засобів масової інформації, причому зацікавленість однобока і явно тенденційного і деструктивного характеру. Інколи подібною ознакою може бути зацікавленість банком сторонніх експертів, дослідників, консультантів, які нібито прагнуть вивчити досвід банку щодо виявлення причин його успіху в бізнесі.

Явною ознакою, що вказує на початок рейдерських дій, є погіршення відносин з місцевими органами влади, рішення яких обмежують діяльність банку. Одночасно банк підпадає

під тотальну перевірку всіх органів, які мають функції контролю.

Нерідко основним акціонерам банку, що утримують контрольний чи блокувальний пакет акцій, може надходити пропозиція продажу його певним особам як юридичним, так і фізичним.

Якщо помічено дві і більше подібних ознак, необхідно терміново вживати заходів до захисту власності банку, а для власників — свого бізнесу.

У цьому разі банк може вдатися до таких заходів:

— блокування пакета акцій з одночасним проведенням додаткової їх емісії. Такі дії можуть бути доцільними, коли у рейдерів перебуває пакет акцій, близький до блокуючого, і в банку немає інших способів щодо припинення їх дій;

— проведення контрскупки своїх акцій і також акцій компаній від імені яких проводиться рейдерська атака;

— структуризація активів банку, як правило, проводиться за рахунок переведення окремих установ банку до складу юридичних осіб — самостійних суб'єктів господарювання. Окремі матеріальні активи (транспортні засоби, комп'ютерна техніка, окремі будівлі) можуть бути власністю підприємств, які є власністю окремих власників банку і використовуватися банком у своїй діяльності на договірних засадах;

— проведення роботи з акціонерами, щодо недопущення продажу ними акцій банку, якими вони володіють;

— у разі виявлення суб'єкта, від якого надходить рейдерська атака, може бути доцільним проведення контррейдерських дій банку щодо його власності;

— проведення переговорів з рейдерами і знаходження компромісних варіантів;

— оприлюднення недобросовісної, злочинної поведінки рейдерів щодо банку і залучення уваги до таких фактів широкого загалу громадськості.

З метою попередження рейдерських посягань та ускладнення дій рейдерів доцільним може бути створення банківських об'єднань, спільне користування різних суб'єктів господарювання, у тому числі і банками, майновими активами (будівлями, землею і т. і.), збільшення акціонерного капіталу банку та мінімізація різниці між його обсягом і вартістю активів банку. Також до таких заходів слід віднести і мінімізацію простроченої кредиторської заборгованості банку, а також недопущення проведення банком операцій з порушенням чинного

законодавства та операцій з коштами, що мають незаконне походження.

Існує думка, що рейдерським нападам можуть піддатися лише невеликі банки. Спростовуючи цю позицію, слід нагадати історію з Промінвестбанком у 2008 р., коли банк ледве не було втрачено не тільки для його власників, а й для держави. Тому, незважаючи на потужність банківської структури, її місця в банківській ієрархії, для кожного з банків існує постійна загроза рейдерських посягань. Більш того, чим потужніший банк, тим загроза буде ставати все небезпечнішою. За таких умов найбільш надійним захистом банку від рейдерських посягань буде захист влади. Знаходження порозуміння з владними структурами, окремими впливовими у владі особами — запорука безпечного життя банкірів, у тому числі і щодо рейдерських загроз.

9.5. Забезпечення економічної безпеки банку в період роботи тимчасової адміністрації

Світова фінансова криза та особливості її українського варіанта суттєво вплинула на діяльність вітчизняних банків. Останні, маючи порівняно незначний фінансовий ресурс, зазнали досить суттєвих втрат своїх активів і опинилися на межі втрати своєї ліквідності та платоспроможності. Різке падіння можливостей формувати свої ресурси за рахунок залучення вкладів населення, обслуговування клієнтів, проведення активних операцій знизило показники стійкості капіталу банків, що, у свою чергу, призвело до порушення встановлених Національним банком України нормативів та змусило деякі з банків відновлювати свою дієздатність через призначення їм тимчасової адміністрації.

Метою тимчасової адміністрації є тимчасове призупинення розрахунків банку з кредиторами та накопичення коштів для відновлення ефективної його діяльності. Разом з тим, як показує досвід, поставлена мета досягається далеко не завжди в таких умовах, якими вони є сьогодні. Без сторонньої допомоги банкам дуже складно вийти з кризи і лише ефективне функціонування системи економічної безпеки банків під час роботи тимчасової адміністрації може бути запорукою успіху.

Більше того, у системі економічної безпеки банку в період роботи тимчасової адміністрації зосереджуються функції інформаційної, кадрової та фінансової безпеки.

Насамперед система економічної безпеки банку має передбачати особливу поведінку тимчасового адміністратора в процедурі як фінансового оздоровлення банку, так і взагалі у відновленні його платоспроможності. Оскільки тимчасовий адміністратор банку уособлює в собі всі органи управління діяльністю банку, вкрай важливо виключити можливість неконтрольованого впливу керівників банку на ситуацію, що склалася навколо нього та його діяльності. Відомі випадки, коли працівники банку, прагнучи приховати певні порушення в їх роботі, вживають заходів щодо вилучення документів, електронної інформації, здійснюють вплив на працівників банку з метою примусити їх до необхідних керівникам дій, у тому числі і під час роботи тимчасової адміністрації.

Тут тимчасовий адміністратор має однозначно вжити заходів щодо виключення доступу всіх керівників банку до банківських документів, інформації, оприлюднити своє рішення щодо позбавлення керівників банку, повноважень давати обов'язкові до виконання вказівки, укладати угоди чи будь-яким іншим способом впливати на діяльність банку. В окремих випадках тимчасовий адміністратор порушує клопотання перед Національним банком України про звільнення зазначених керівників з роботи в банку або ж вживає заходів щодо виключення можливості доступу таких осіб до банку.

За певних умов може виникати необхідність відсторонення від виконання обов'язків і окремих керівників установ (відділень, дирекцій) банку, щодо яких є підозра в їх недобросовісній поведінці і перешкоджанні діяльності тимчасового адміністратора та заходам, що проводяться відповідно до його рішень.

Особливо великого значення в процедурі тимчасової адміністрації набуває питання збереження активів банку. Як показує досвід, в окремих випадках тимчасовий адміністратор може змінювати вид та склад охорони певних об'єктів, особливо тих, яким існує реальна загроза їх пошкодження, крадіжки майна, а то і знищення (склади, каси, місця зберігання документів та електронної інформації), обмежувати доступ до об'єктів, утворювати додаткові пости охорони та в інший спосіб посилювати режим охорони банку.

Суттєве значення у роботі тимчасового адміністратора мають заходи з кадрової безпеки. Оскільки значна частина працівників

банку буде звільнена, слід посилити контроль за роботою і поведінкою персоналу. Для цього тимчасовому адміністратору необхідна буде власна команда фахівців, які очолять найважливіші напрями роботи (безпеки, юридичний, кредитний, валютний, касовий, цінних паперів, фінансовий, бухгалтерський, кадровий та ін.). Якщо тимчасовий адміністратор не має у своєму розпорядженні таких фахівців, то він підбирає їх із найбільш досвідчених і перевірених працівників банку. За клопотанням Національного банку України такі працівники можуть залучатися з інших банків чи фінансових установ. У разі, якщо тимчасовим адміністратором призначається службовець Національного банку України, його команда може формуватись із службовців Національного банку України. Крім того, в окремих випадках до складу тимчасової адміністрації можуть залучатися працівники державних установ та підрозділів, які мають досвід у фінансовій діяльності. Такі випадки можуть мати місце насамперед тоді, коли банк має у своєму статутному капіталі суттєву частку держави.

Зауважимо, що призначення тимчасової адміністрації практично завжди супроводжується певним соціальним напруженням навколо банку. За таких умов тимчасовому адміністратору необхідно буде мати фахівців, здатних організовувати і проводити заходи щодо зняття такого напруження та періодично інформувати громадськість, вкладників та клієнтів банку стосовно дій тимчасового адміністратора, спрямованих на виведення банку із кризи.

Особливі заходи слід у цей період вживати щодо інформаційної безпеки. Як показує досвід, інформаційна безпека повинна забезпечуватися по трьох напрямах: мінімізація інформаційних ризиків при прийнятті тимчасовим адміністратором антикризових рішень, захист інформації з обмеженим доступом та протидія інформаційно-психологічному впливу на індивідуальну та колективну свідомість працівників, клієнтів банку, а також громадськість.

З метою мінімізації інформаційних ризиків необхідно буде посилити роботу щодо формування інформаційного ресурсу банку, інформаційно-аналітичного дослідження стану та поведінки клієнтів, ринку банківських послуг, інформаційному аудиту боржників банку.

Для забезпечення захисту банківської інформації доцільним буде значне обмеження доступу до таємної та конфіденційної інформації банків, особливо банківської таємниці. А протидія

інформаційно-психологічному впливу має забезпечуватись активною пропагандою діяльності банку і його тимчасової адміністрації, швидким викриттям каналів подання негативної інформації та її спростуванням.

Але головним питанням у забезпеченні безпеки банку в даний період все ж таки є фінансова безпека. Остання має бути спрямована на формування фінансового ресурсу, недопущення його втрати і неефективного використання. Незалежно від існуючих у банку методик роботи з фінансами основними завданнями тимчасового адміністратора з фінансової безпеки будуть:

- моніторинг і прогнозування факторів, що обумовлюють загрози фінансовій безпеці банку;
- формування оптимальної структури боргових зобов'язань;
- визначення пріоритетів і оптимізація використання фінансових ресурсів;
- забезпечення балансу доходів і витрат у діяльності банку;
- протидія злочинним посяганням на фінансові ресурси банку та неефективного їх використання;
- розширення джерел та методів залучення фінансових ресурсів.

Велике значення у період роботи в банку тимчасової адміністрації має збереження фінансових ресурсів, так зване фінансове виживання. Тут слід вдатися до таких заходів як мінімізація витрат, перерозподіл коштів з метою оптимізації витрат, зниження собівартості послуг, економія коштів та строго цільове їх використання, формування умов для швидкої і ефективної віддачі від вкладання коштів. Водночас протидію неконтрольованому витоку коштів тимчасовий адміністратор здійснює за допомогою таких заходів: суворий і безумовний облік усіх коштів банку, планування використання коштів, забезпечення надійного зберігання коштів, цінностей та документів, установлення спеціального порядку доступу до фінансових ресурсів банку, контроль використання коштів та інші заходи.

Основні заходи фінансової безпеки тимчасовий адміністратор концентрує на чотирьох напрямах, зміст яких відображено на рис. 9.10.

Рис. 9.10. Заходи фінансової безпеки банку у період тимчасової адміністрації

Як правило, до зазначених заходів тимчасовий адміністратор залучає весь персонал і всі підрозділи банку, приділяючи основну увагу саме питанням безпеки його фінансів.

Отже, заходи безпеки банку під час роботи в ньому тимчасової адміністрації мають бути не тільки обов'язковими, а й охоплювати всі види діяльності тимчасової адміністрації щодо відновлення платоспроможності та ліквідності банку.

РЕЗЮМЕ

Економічна безпека банку є основною складовою його безпеки. Разом з тим вона сама має певну структуру і спрямовує свої зусилля на захист матеріальних та фінансових ресурсів банку. Основою забезпечення економічної безпеки банку є фінансова безпека. У свою чергу, забезпечення фінансової безпеки базується на захисті банківських операцій. В основу методології захисту банківських операцій покладено

елементи захисту технологій їх проведення на всіх етапах розвитку операцій: при їх підготовці, у процесі супроводження та на етапі завершення. Зазначені елементи спрямовані на виявлення ознак загроз операціям, їх оцінки та вжиття заходів щодо усунення загроз чи мінімізації ризику їх реалізації у процесі певної операції.

Важливим елементом забезпечення фінансової безпеки банку є протидія втягуванню його в незаконну фінансову діяльність, яка виконується через установлення контролю за проведенням фінансових операцій клієнтами банку, виявлення в них ознак сумнівних та протиправних.

Заходи економічної безпеки мають поширюватись і на протидію рейдерським посяганням на банк. Своєчасне виявлення підготовки рейдерських атак, виведення з-під удару рейдерів активів банку є особливо важливим для забезпечення економічної безпеки банку.

Особливо важливим для банку є забезпечення економічної безпеки під час фінансового оздоровлення та роботи тимчасової адміністрації. Тут необхідні особливі технології, пов'язані зі скороченням витрат банку, поверненням дебіторської заборгованості, відновленням ліквідності банку та залученням фінансових ресурсів, а також зі збереженням наявних активів банку.

Терміни і поняття

Економічна безпека банку

Забезпечення економічної безпеки банку в період роботи тимчасової адміністрації

Забезпечення фінансової безпеки банку

Заходи фінансової безпеки загального характеру

Заходи фінансової безпеки спеціального характеру

Критерії економічної безпеки банку

Організація роботи банку щодо повернення проблемної кредитної заборгованості

Проблемний кредит

Протидія рейдерським посяганням на банки

Робота банків щодо протидії легалізації (відмиванню) коштів, отриманих злочинним способом

Робота банку з організації кредитної діяльності

Система заходів захисту матеріальних ресурсів банку

Система показників економічної безпеки банку
Стратегія економічної безпеки банку
Управління проблемним кредитом
Фінансова безпека банку

Питання для перевірки знань

1. Чим зумовлюється актуальність забезпечення економічної безпеки банку?
2. Що слід розуміти під поняттям «економічна безпека банку»?
3. У чому полягає мета стратегії економічної безпеки банку?
4. Що має бути покладено в основу захисту матеріальних цінностей банку?
5. Як мають бути організовані перевірки матеріальних цінностей у банку?
6. За якими напрямами має бути організовано забезпечення фінансової безпеки банку?
7. Які підрозділи банку беруть участь у підготовці до кредитної операції і які завдання на даному етапі вони повинні виконати?
8. Як слід організувати кредитну роботу банків щодо повернення проблемної заборгованості?
9. Які банкноти слід вважати фальшивими? Якими мають бути дії касира у разі виявлення ним фальшивих банкнот?
10. Яких заходів слід вжити банку в разі виявлення клієнтом під час перерахування готівки недостач або надлишків банкнот (монет)?
11. Чи можуть прийматись до проведення банком операцій ксерокопії акцій чи сертифікатів?
12. Як слід організувати роботу з протидії відмиванню незаконно отриманих коштів?
13. Яких заходів слід застосовувати банку для забезпечення своєї фінансової безпеки в умовах дії негативних факторів світової фінансової кризи?
14. Які ознаки можуть вказувати на проведення рейдерських посягань проти банку?
15. Яких заходів слід вжити тимчасовому адміністратору для забезпечення фінансової безпеки банку в період тимчасової адміністрації?

Завдання для індивідуальної роботи

1. Ви — член інвентаризаційної комісії. Під час інвентаризації основних засобів банку виявлено майно, на якому не було інвентарних номерів. Майно придатне для використання. На ваше запитання, звідки це майно і чиє воно, ніхто з тих, хто працює в даному приміщенні, не міг дати відповіді. Усі посилались на те, що воно перебуває в приміщенні вже давно. Якими мають бути ваші дії як члена інвентаризаційної комісії стосовно зазначеного майна?

2. Ви — кредитний інспектор, здійснюєте супроводження однієї з кредитних операцій, у процесі якої виникла потреба перевірити цільове використання кредитних коштів. Вивчивши документи, що підтверджують використання позичальником кредитних коштів відповідно до договору, ви залишилися не повністю впевненими в об'єктивності інформації, яка містилася в них. До того ж ви отримали інформацію від деяких контрагентів позичальника, що останній розриває з ними зв'язки так і не розпочавши роботи.

Як ви будете діяти далі, щоб отримати об'єктивну інформацію про поведінку позичальника і використання ним кредитних коштів відповідно до договору?

3. Ви — працівник підрозділу з питань фінансового моніторингу. Під час розроблення вашим підрозділом програми ідентифікації та вивчення своїх клієнтів керівник підрозділу доручив вам розробити анкети клієнтів банку — як фізичних, так і юридичних осіб. Як ви будуватимете свою роботу, щоб виконати поставлене вам завдання? Яка саме інформація має вказуватися в анкетах, щоб банк зміг провести ідентифікацію своїх клієнтів? На якому етапі взаємовідносин з клієнтом банки формують відповідні анкети?

Література для поглибленого вивчення

1. *Барановський О. О.* Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : монографія / Барановський О. О. — К. : КНТЕУ, 2004. — 759 с.

2. *Богомолов В. А*. Экономическая безопасность: учебное пособие для студентов ВУЗов, обучающихся по специальностям экономики и управления / Богомолов В. А. — М. : ЮНИТИ-ДАНА, 2009 — 295 с.

3. *Гамза В. А*. Безопасность банковской деятельности / В. А. Гамза, И. Б. Ткачук. — М. : Маркет, 2010. — 408 с.

4. Економічна безпека / [Мельник П., Терангул Л. та ін.] ; за ред. З. С. Варналія. — К. : Знання, 2009. — 647 с.

5. *Павлов А. В*. Основы организации безопасности банков : учеб. пособие / Павлов А. В. — М. : Академия, 2010. — 128 с.

6. *Чуб О. О*. Банки в глобальній економіці : монографія / Чуб О. О. — К. : КНЕУ, 2009. — 340 с.

7. *Ярочкин В. И*. Безопасность банковских систем / Ярочкин В. И. — М. : Ось-89, 2004. — 416 с.

Розділ 10

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКУ В РОБОТІ З КАДРАМИ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *основи забезпечення кадрової безпеки в банках;*
- ✓ *заходи з мотивації персоналу банку до якісного виконання заходів безпеки;*
- ✓ *основи формування у персоналу банку банківського патріотизму та лояльності до банку;*
- ✓ *заходи безпеки при комплектуванні банку кадрами, у процесі його роботи та при звільненні;*
- ✓ *основи психології поведінки персоналу, клієнтів банку під час роботи з банківськими коштами;*
- ✓ *умови та причини виникнення конфліктів у колективах підрозділів банків, прийоми їх попередження та вирішення;*
- ✓ *корпоративний характер управління кадровою безпекою банку,*

*а також **уміти**:*

- ✓ *забезпечувати власну безпеку при виконанні посадових обов'язків у банку;*
- ✓ *грамотно та толерантно формувати свої взаємовідносини з керівництвом банку та колективами його підрозділів;*
- ✓ *виявляти ознаки недобросовісної чи протиправної поведінки працівників банків і клієнтів.*

10.1. Безпека як потреба працівника банку й умова його роботи

Кадри — це те єдине, що вирізняє і робить особливим сьогоднішній бізнес у конкурентній боротьбі. За ідентичності технологій формування прибутку, тієї самої кон'юнктури ринку, однакових умов функціонування підприємницьких структур, тільки кадри можуть забезпечити стабільність і розвиток або, навпаки, бути причиною розорення і банкротства комерційних підприємств і банків. За таких умов робота з кадрами стає найвагомішою складовою в організації сучасного вітчизняного підприємництва, а засади безпеки цієї роботи стають особливо актуальними.

Розглядаючи персонал банку з погляду безпеки, необхідно звернути увагу на те, що, з одного боку, персонал є одним із найсуттєвіших його активів, який банківська безпека має захищати з неменшою ефективністю, ніж інші активи, а з другого — персонал найбільш небезпечне джерело заподіяння шкоди банку, від якого банк, як не парадоксально, має будувати відповідну систему захисту. Така ситуація обумовлює особливий характер кадрової політики банку і відповідну організацію кадрової роботи. Водночас досвід забезпечення безпеки кадрової роботи показує, що останні підходить до вирішення цього питання однобоко, залишаючи поза увагою інтереси персоналу, насамперед інтереси з його безпеки. Тут слід відійти від стереотипу, що персонал, кожен конкретний працівник є лише певним "гвинтиком" у банківському виробництві, який прибув до банку задля формування благ самому банку та його власникам. Насправді кожен з працівників приходить на роботу до банку насамперед прагнучи задовольнити свої власні потреби та інтереси. І від того, якою мірою вони задовольняються в конкретному банку і залежатиме безпека поведінки працівників, а з нею — і всього банку. Тут варто зауважити, що потреби й інтереси стосуються не тільки фізичних чи інтелектуальних процесів життєдіяльності працівників, а й на прагнення, виконуючи роботу в банку, залишатися в безпеці. З цього погляду необхідно звернути увагу на загрози, які можуть виникати у працівників під час роботи в банку.

Зокрема, такими загрозами можуть бути:

- зманювання перспективних працівників банку конкурентами та іншими організаціями;
- вербування працівників банку промисловими шпигунами і залучення їх до роботи, пов'язаної з посяганням та таємниці банку;
- компрометація, шантаж працівників банку з метою примушення їх до здійснення різного роду посадових порушень;
- погрози на адресу працівників банків у зв'язку з невиконанням банком певних зобов'язань, що зумовлені різними економічними причинами;
- замахи на працівників банку, членів їхніх сімей унаслідок особливостей їх професійної діяльності;
- спокуса, що може виникати у працівників банку щодо протиправного заволодіння його власністю.

Досвід показує, що найбільшої небезпеки можуть зазнавати особи керівного складу банку, керівники та працівники касового, кредитного, фінансового, юридичного, операційного, валютного підрозділів, а також підрозділів цінних паперів, безпеки та банківських ризиків, працівники, які мають доступ до таємної інформації банку, пов'язаної з його діяльністю та діяльністю клієнтів. Успіх у реалізації загроз щодо персоналу банку залежатиме, зокрема, і від його стійкості щодо таких загроз, а остання, у свою чергу, буде залежати від умов, у яких здійснюють свою діяльність працівники банку. Звертаючи увагу на потреби й інтереси працівників, під такими умовами слід розуміти рівень та умови оплати праці, наявність соціальних програм, можливість будувати кар'єру, отримати досвід, бути захищеним та перебувати в безпеці при виконанні своїх обов'язків. Крім того, велике значення мають такі супутні фактори, як характер взаємовідносин у банківських колективах та здоровий психологічний клімат, наявність корпоративної культури, хороші побутові та виробничі умови роботи, дотримання санітарних умов і медичне обслуговування тощо.

Важливе місце в протидії загрозам персоналу має формування у нього безпечної поведінки в різних виробничих ситуаціях. Тут банк має застосовувати різні заходи: проведення занять, інструктажі, розроблення різного роду пам'яток, застережень, періодичне інформування персоналу про особливі небезпеки, які виникають у діяльності банку, і захист від них. Основним у поведінці працівника має бути знання та вміння непровокованої до конфлікту поведінки, виявлення ознак підозрілої та небезпечної поведінки в діях колег, клієнтів, відвідувачів банку,

володіння прийомами попередження загроз та захисту себе і банку в умовах їх реалізації.

Найактивніше банк має діяти щодо захисту персоналу від шантажу та замаху на життя та здоров'я працівників. Зокрема, до працівників має бути доведена техніка шантажу, яка з найбільшою імовірністю може бути застосовані до працівників банку за тих чи тих умов, ситуації та типи поведінки працівників, за яких шантаж може ставати неможливим.

Що ж до замахів, то, як показує практика, основними причинами, через які виникають такі явища, можуть бути:

- некоректна поведінка керівництва банку та окремих його працівників до конкурентів і клієнтів, відсутність компромісів та наявність ознак криміналу в їхніх діях;
- невиконання (відмова від виконання) взятих банком зобов'язань;
- непорозуміння в керівництві банку, боротьба за контроль над ним у середовищі акціонерів та тіньових власників;
- рейдерські атаки на банк, що супроводжуються перехопленням влади в банку;
- «ділові» взаємовідносини з кримінальними елементами, пов'язані з діяльністю банку.

Для попередження або мінімізації загрози, пов'язаної із замахами на працівників, банки можуть удаватись до таких дій: усунення об'єкта замаху (працівника банку) з поля зору замовників чи виконавців замаху (переведення на іншу посаду, відрядження, відпустки, лікування тощо), знаходження компромісних варіантів виходу із ситуації, у взаємовідносинах з потенційними замовниками, вжиття заходів захисту щодо осіб, яким може загрожувати замах, у тому числі і технологічного (виробничого) характеру (усунення працівника від одноосібного прийняття рішень, зменшення обсягів коштів, по яких працівник може приймати рішення і т. п.); звернення про допомогу до правоохоронних органів; навчання особливостям поведінки в ситуаціях загрози чи безпосереднього замаху.

Разом з тим слід зазначити, що навички безпечної поведінки персоналу як особиста безпека формуються протягом усієї роботи працівників у банку. Заходи щодо їх формування проводяться в кілька етапів: первинний інструктаж з питань банківської безпеки осіб, що прийняті на роботу в банк (проводиться працівниками служби безпеки); навчання на робочих місцях керівниками підрозділів (заходи безпеки при виконанні обов'язків на

конкретному робочому місці) проводиться з початком роботи і надалі в разі необхідності; періодичне доведення загроз та небезпечних тенденцій, що виникають на ринку банківських послуг, і правил протидії їм.

Головним у такому навчанні є формування у персоналу стійких переконань щодо правил безпечної поведінки на роботі і в побуті.

Водночас дієвим щодо протидії втягуванню персоналу банку в протиправну діяльність є заходи з профілактики порушень трудової та виробничої дисципліни, які має проводити банк (рис. 10.1).

Правове навчання персоналу	Розроблення нормативної бази, яка регламентує діяльність працівників банку щодо виконання заходів безпеки	Перевірка відомостей про співробітників: • доходи яких різко виросли без відомих на те причин; • в оточенні яких з'явилися підозрілі особи
Регулювання розподільних і дозвільних повноважень працівників	Розроблення комплексної системи контролю роботи працівників банку й ефективне її застосування	Розподіл функцій у робочих колективах (у тому числі і при заміщенні посад)
Дотримання принципу «чотирьох» очей (двох підписів)	Періодичне проведення перевірок, інвентаризацій і звірок	Розмежування доступу в приміщення банку
Контроль наявності документів у банку і витоку його інформації з обмеженим доступом	Застосування заходів гарантованого захисту джерел інформації банку з обмеженим доступом	Установлення відповідальності за посягання на інформацію банку

Рис. 10.1. Заходи з профілактики порушень трудової та виробничої дисципліни і протиправної поведінки працівників банку

Зазначені заходи можуть мати очікуваний ефект лише за умов, коли вони проводитимуться в комплексі із заходами, спрямованими на формування банківського патріотизму та відповідальності працівників банку за результати своєї роботи, а також виховної роботи в банку (Додатки 14, 15, 16).

Основними ж напрямами, на яких банк має зосереджувати зусилля щодо захисту свого кадрового складу, можуть бути:

✓ захист персоналу банку від проникнення до його складу нездорових елементів, які своєю поведінкою можуть руйнувати доброзичливі взаємовідносини в банківських колективах; розроблення спеціальних стандартів поведінки персоналу, спрямованих на захист інтересів банку, його клієнтів, партнерів і прийняття працівниками зобов'язань щодо їх дотримання;

✓ здійснення заходів організаційного, соціально-економічного і виховного (дисциплінарного) характеру, спрямованих на підвищення зацікавленості працівників у ефективному розвитку банку, підтриманні необхідного рівня трудової та виробничої дисципліни;

✓ виявлення, попередження і припинення неправомірних дій, спрямованих на спонукання працівників до участі у скоєнні проступків, злочинів, що шкодять інтересам банку;

✓ обмеження негативного впливу на персонал банку осіб, котрі допустили або мали намір заподіяти своїми протиправними, аморальними чи якимись іншими діями шкоду банку, через беззаперечне звільнення їх з роботи.

Таким чином, забезпечення безпеки персоналу банку як об'єкта загроз здійснюється за двома напрямами: створення безпечних умов роботи працівників, у тому числі і таких, що мінімізують спокусу працівників до негативних, неправомірних чи злочинних дій і формування безпечної поведінки самих працівників в умовах загрози або безпосередньої дії небезпечних факторів щодо них.

Розглядаючи ж персонал як суб'єкта загроз банку заходи безпеки мають зосереджуватися також у двох напрямах: ліквідації можливості до формування та реалізації загроз банку з боку його персоналу і ліквідації причин, які спонукали б та сприяли зазначеним діям персонал банку. Слід також звернути увагу, що формування та реалізація загроз від персоналу може здійснюватися умисно або ж унаслідок недостатніх професійних якостей працівників, у першому випадку умови реалізації загроз, як правило, будуть характеризуватись несанкціонованістю, безконтрольністю, безкарністю і таємністю. У другому — некомпетентністю, недисциплінованістю, безгосподарністю. Тобто мінімізація загроз може досягатися через ліквідацію умов, які сприяють їх утворенню та реалізації.

Несанкціоновані дії можуть бути наслідком відсутності в банку чіткої регламентації всіх процедур його діяльності. Важливим стримувальним фактором скоєння будь-якого проступку чи злочину є якраз регламентування всіх внутрішніх

процедур у банківській діяльності, особливо з коштами, інформацією та матеріальними цінностями, у тому числі і право прийняття рішень щодо цих активів. Відсутність регламентації (норм, що регулюють певний вид діяльності, окремий його процес чи конкретну роботу) призводить до того, що, з одного боку, персонал виконує їх на свій розсуд, досконало не навчений виконувати певні процедури, а з другого — працівникам немає чого порушувати, тобто відсутні підстави для притягнення до відповідальності — одного зі стримувальних факторів протиправної та недобросовісної діяльності. Звідси, обов'язковий і правильний опис усіх процедур банківської діяльності, особливо тих із них, неправильне чи свідоме викривлення яких може призвести до негативних для банку наслідків, — одне з головних завдань кадрової безпеки банку.

Другим стримувальним фактором на шляху скоєння працівниками банку проступків і злочинів є наявність і висока ефективність заходів контролю поточного стану всіх систем діяльності банку (фінансової, виробничої, інформаційної, правової і т. д.). Тут слід акцентувати увагу на суті контролю. Просто звичайне спостереження за персоналом і операціями, в яких задіяні певні працівники, як метод забезпечення безпеки від внутрішніх загроз є недієвим. Контроль у даному разі слід розуміти як процес виявлення відхилень від установлених норм, що регулюють режим безпеки в банку та правила застосування технологій захисту банківських операцій. У свою чергу, контроль поділяється на адміністративний і фінансовий. Адміністративний контроль полягає в попередженні відхилень від порядку проведення операцій, які мають здійснюватися лише уповноваженими на те особами в строгій відповідності з визначеними банком повноваженнями і процедурами прийняття рішень.

Фінансовий контроль має попереджувати можливі відхилення від прийнятої і закріпленої в банку його нормативними документами політики надання банківських послуг і їх адекватного відображення в обліку і звітності.

Зазначені види контролю повинні з достатнім ступенем надійності показувати, що доступ працівників банку до його цінностей, виконання банківських операцій здійснюється у строгій відповідності до визначених працівникам повноважень, а самі операції відображаються в обліку відповідно до встановлених у банку вимог і реально показують стан активів і

пасивів банку, а також дають можливість складати об'єктивну звітність.

У процесі контролю відстежується ефективність і дієздатність систем, що контролюють дотримання працівниками встановлених правил здійснення банківських і господарських операцій, надійність процедур і механізмів, що виключають можливість виходу кожного конкретного працівника за межі встановленого обсягу і складу операцій, відповідність умов, за якими проводяться працівниками угоди і операції, загальній політиці залучення і розміщення ресурсів банку. Крім того, під час контролю перевіряється коректність оформлення працівниками первинної документації, здійснення в повному обсязі встановлених у банку процедур звірки, узгодження, візування, а також дотримання процедури формування на базі зазначених документів балансових даних.

Окремо, у процесі контролю, проводиться робота з отримання інформації про можливі порушення порядку здійснення операцій і фінансової політики банку, про зловживання працівників банку своїм службовим становищем.

Безкарність за скоєні порушення є однією з головних причин поширення їх у банківському середовищі. У банку має бути розроблена система реагування на проступки, правопорушення і злочини, які можуть бути скоєні його працівниками, клієнтами чи іншими особами. За всіх умов жодне з порушень правил роботи банку чи режиму його безпеки не може залишатися без відповідного реагування з боку адміністрації банку чи керівників банківських підрозділів. Практично в усіх випадках порушники мають давати письмові пояснення своєї поведінки, а якщо їх діями завдано шкоди банку, має проводитися службове розслідування. За його результатами приймається рішення щодо притягнення порушників до відповідальності. Разом з тим факт притягнення працівника до відповідальності має бути доведено до відома всіх працівників, з тим щоб показати невідворотність відповідальності за скоєні порушення, протиправні дії та злочини щодо банку, клієнтів, партнерів і т. п.

Таємність як умова реалізації внутрішніх загроз є для певного кола осіб досить вагомою підставою, яка обумовлює їх поведінку щодо виконання встановленого в банку режиму безпеки. Для багатьох з них скоїти щось погане на людях є абсолютно неприпустимим, водночас відсутність «зайвих очей» якраз може сприяти неформальній поведінці. Саме таку поведінку банку слід

враховувати створюючи відповідні незручності різними способами колективного та інформаційного впливу.

Додатковими умовами, що мінімізують можливості формування та реалізації загроз з боку персоналу банку, також можуть бути повна зайнятість працівників роботою протягом усього робочого дня відповідно до Правил внутрішнього розпорядку роботи банку, відсутність явних дефектів в обліку і документообороту та удосконалення інженерно-технічного та фізичного захисту матеріальних об'єктів банку.

Реалізація загроз унаслідок недостатніх професійних якостей працівників є більш суттєвим фактором, оскільки мінімізується складніше і протягом тривалого часу. Відсутність або недостатність професійних якостей веде не тільки до неефективного виконання технологічних процедур банківських операцій, а й взагалі до безгосподарності в діяльності банків і, як наслідок, до втрати їх конкурентоспроможності та позицій на ринку.

Прагнучи мінімізувати ризики, пов'язані з недостатнім професіоналізмом персоналу, банки ведуть активний пошук працівників, які відповідають установленим банками вимогам щодо професійної банків компетенції. Водночас нерідко професійна компетенція розуміється суто як здатність професійно й ефективно виконувати певну роботу, з чим погодитись не можна. Фахівці у сфері кадрової безпеки зазначають, що під професійною компетенцією слід розуміти цінності й особистісні якості, а також професійні знання і навички, необхідні для успішного виконання певних посадових обов'язків працівниками підприємства, банку [163, 176]. Для кожного банку, а то і посади набір компетенцій є унікальним і тому якщо певний кандидат з якихось причин не підходить для роботи в одному банку, що це зовсім не означає, що він не може бути прийнятий до іншого.

У переліку компетенцій для працівника банку, який займає управлінську посаду, мають бути чотири групи компетенцій: корпоративні (цінності), менеджерські (управлінські), професійні і компетенції, що забезпечують його особисту ефективність. Для працівника банку виконавчого рівня таких груп компетенцій може бути три: корпоративні, професійні і компетенції особистої ефективності.

Кожна посада має описуватися переліком відповідних компетенцій, з яких будуть складатися критерії конкурсного відбору кандидатів при заміщенні даної посади.

Водночас, виходячи з характеристик вітчизняного ринку праці, банки не можуть задовольнити свої потреби працівниками, які в повному обсязі відповідали б їх вимогам. Звичайно, частина працівників не повною мірою задовольнятиме потреби банків і створюватиме для них додатковий ризик. На мінімізацію такого ризику мають бути спрямовані заходи з додаткової підготовки цих працівників щодо опанування ними специфічними питаннями роботи в конкретному банку, на конкретному робочому місці. Така підготовка може здійснюватися безпосередньо в банку або ж в інших установах і організаціях на замовлення банку, як за кошти останнього, так і за кошти самих кандидатів.

До заходів мінімізації ризиків низької професійної якості працівників можуть бути також віднесені: інструктажі працівників щодо конкретизації методики виконання певних робіт, робота під контролем більш досвідчених працівників, самоудосконалення своїх професійних якостей самими працівниками за програмами, складеними в банках, періодична профатестація працівників.

Зауважимо, що особливістю сьогоднішніх умов кадрового забезпечення банків є якраз необхідність вжиття ними заходів щодо практичного спрямуванню підготовки банківських працівників безпосередньо в банках. Іншого виходу поки що, як показує практика, не існує.

Питання професіоналізму банківських працівників тісно пов’язане з іншими факторами, що стосуються насамперед ліквідації причин, які спонукають персонал банку до дій, якими формуються та реалізуються внутрішні загрози банку. Звичайно, не всі працівники банку є причетними до вказаних загроз. Можна говорити лише про ту частину його працівників, яка має намір заподіяти шкоду, як правило, через прагнення до власного збагачення. Зменшення причин такої поведінки працівників, зниження їх критичності та гостроти — одне із головних завдань кадрової безпеки банку. Можливості до заподіяння шкоди банку у його працівників існують практично завжди і якщо вони відсутні нині, то можуть з’явитись пізніше. І тільки за відсутності у працівників бажання завдати шкоди можна ігнорувати об’єктивне існування вказаних можливостей. Тобто якщо немає причини, що спонукає працівника до заподіяння банку шкоди, він ніколи не буде діяти проти нього.

Аналіз причин протиправної поведінки працівників банків, пов’язаної з заподіянням банкам шкоди, показує, що насправді

більша частина таких причин — поза межами впливу банку і мотивується власними потребами та інтересами працівників. Решта причин породжується в банку і мотивується особливостями взаємовідносин його адміністрації та працівників (недостатня, несправедлива оплата праці, барство керівників і власників, очевидна їх злодійська поведінка щодо банку, недоброзичливі взаємовідносини в колективах, між працівниками і керівництвом, ненадійне зберігання цінностей та нерегламентована внутрішньоофісна діяльність банківських установ тощо).

Очевидно, що зазначені причини пов'язані з особливостями особистих характеристик поведінки, виховання, характеру, потреб самих працівників банку, в основі яких — бажання отримати певні переваги від своєї роботи, у тому числі і через скоєння порушень дисципліни, правопорушень і злочинів. За таких обставин головним у забезпеченні кадрової безпеки має бути мінімізація та ліквідація такого бажання працівників, потягу їх до негативної поведінки. Виконання такого завдання якраз і забезпечить попереджувальний характер кадрової безпеки, а остання не буде зосереджуватися на пошуку порушень і осіб, що їх скоїли. Очевидно також і те, що заходи, яких необхідно вжити з метою мінімізації і ліквідації бажання працівників у будь-який спосіб зашкодити банку, перебувають у площині моралі, доброзичливих, довірливих взаємовідносин та ефективного управління персоналом. Тому свою діяльність із персоналом банк має будувати на основі довіри, визнання, підтримки та розвитку.

За таких умов основу взаємовідносин адміністрації банків і їх персоналу з погляду кадрової безпеки, має становити довіра. Відкриті і чесні взаємовідносини запорука стійкого й успішного бізнесу.

Сьогоднішня позиція банківської безпеки, з якої персонал банку бачиться лише як об'єкт загроз, існувала і в минулому, на даний час вона має бути суттєво доповнена довірою до персоналу. Звичайно, що довіра не може бути безмежною і обов'язковою. Тут має діяти закон — банк довіряє тим, хто довіряє банку, будує відносини з ним на основі чесної, доброзичливої поведінки. Вигода працівників за таких взаємовідносин полягає у конкретних матеріальних і нематеріальних, індивідуальних і колективних надбаннях, які надаються працівникам і банківським колективам як визнання довіри.

В умовах довіри зовсім по іншому будується система відповідальності. Вона має бути:

— однозначною (попередньо обумовленою сторонами);

— прозорою (спосіб її визначення попередньо обговорено);

— публічною (відомості про заходи відповідальності поширюються в оговореному порядку і доводяться до всіх працівників);

— комплексною (можливість одночасного застосування різних видів відповідальності).

Тільки за таких умов довірливі взаємовідносини в системі кадрової безпеки матимуть сенс.

Незважаючи на вагомість довіри до персоналу у забезпеченні кадрової безпеки не менш важливе місце займає визнання здобутків працівників, їх ролі у діяльності банку, причому не декларативне, а реальне. Наприклад, визнанням нелегких умов праці будуть заходи щодо створення комфортних робочих місць, сприятливих побутових умов, а в ролі високої оцінки працівників може бути турбота банку про якість їх життя та здоров'я. Визнанням високих професійних якостей є кар'єрне зростання працівника, пропаганда їхніх здобутків не тільки серед установ банку, а й за його межами, тоді як надання різних пільг, права користуватися соціальним пакетом, активне стимулювання працівників буде визнанням їх лояльності до банку. Головне, щоб заходи з визнання працівників були гласними, впливали на підвищення їх авторитету в колективах, викликали гордість за роботу в банку.

Підтримка працівників з боку банку може здійснюватися через надання правової допомоги силами юридичних підрозділів банку переважно через консультації працівників з правових питань, фінансової допомоги (кредити, матеріальна допомога), допомоги у професійних питаннях (підтримання кваліфікації працівника на належному рівні), інформаційну допомогу (користування інформаційними ресурсами банку), а також моральну підтримку (участь банку у вирішенні конфліктів, що виникли навколо працівника, висловлення підтримки в ситуаціях негараздів, що спіткали працівника тощо). Підтримка працівників — основа поваги з їх боку до банку. Лише не більше 10% осіб у середовищі взаємної поваги здатні до антиморальних, негативних дій стосовно свого оточення [176]. Але за таких умов дії цих осіб зупинить сам колектив, що й буде запорукою для формування в банку високого рівня кадрової безпеки.

Крім перелічених заходів не менш значущим є забезпечення розвитку персоналу. Працівники мають усвідомити, що лише в цьому банку вони можуть розраховувати на саморозвиток і самореалізацію, а не тільки на роботу. Серед сфер, в яких банк має розвивати свій персонал, слід назвати такі:

- розвиток індивідуальних здібностей працівників у різних напрямах їх життєдіяльності (надання можливостей, формування умов, підтримка та допомога);
- розвиток професійних якостей працівників (можливість отримання досвіду, навчання, залучення до розроблення і впровадження нових продуктів, вивчення та узагальнення досвіду банківської діяльності, забезпечення кар'єрного зростання);
- розвиток колективів через заохочення активних форм колективної діяльності (розвиток корпоративності).

Таким чином, концентрація зусиль кадрової безпеки банку на моральній стороні взаємовідносин з персоналом забезпечить створення умов, за яких працівники банку поважатимуть його за відкриті і чесні стосунки з ними, цінувати за підтримку, яку він надає працівникам, будуть вдячні банку за визнання їх як професіоналів і особистостей, захищатимуть банк за можливість забезпечити власну кар'єру та розвиток. Чи можуть виникати у працівників банку за таких умов причини для використання наявних можливостей заподіяння шкоди банку?

Принаймні однозначно можна наголошувати, що таких причин буде значно менше.

Заходи щодо мінімізації ризиків формування негативної поведінки персоналу з погляду моралі та доброзичливих взаємовідносин становлять лише один аспект діяльності кадрової безпеки. Інший утворюють заходи режимного характеру. Ці заходи поширюють свою дію на всі елементи кадрової роботи — від комплектування банку кадрами до звільнення працівників із роботи.

Розглядаючи питання безпеки кадрової роботи, необхідно насамперед забезпечити, щоб заміщення вакантних посад відбувалося тільки на конкурсних засадах. Банк завжди повинен мати вибір фахівців, а не комплектувати посади за вимушеним принципом, погоджуючись на пропозиції будь-кого з претендентів. Конкурсні засади головним чином передбачають такі процедури: підбір, перевірку, оцінку, відбір, розстановку кадрів.

Підбір здійснюється через вивчення ринку праці, публічного оголошення про наявність вакантних посад, отримання заяв

(характеристик-рекомендацій) та формування списку претендентів. У процесі підбору необхідно звернути увагу на відповідність кандидатів загальним критеріям банківського працівника. До таких критеріїв можна було б віднести: відповідний рівень освіти та досвід роботи, вік кандидата, стан здоров'я, кримінальне минуле, перспективність, рівень культури та відповідний менталітет, шкідливі звички тощо.

Сформувавши на основі загальних критеріїв списки кандидатів, банк здійснює їх перевірку, яка виконується за двома напрямами: визначення професійної придатності фахівця для роботи в банку та встановлення його психологічної схильності до такої роботи. Крім того, однією з причин перевірки є визначення ознак, які вказували б на наявність у кандидата шкідливих для роботи в банку вад (азарт, залежність від наркотичних речовин або алкоголю, порочні звички, нездорова заздрість, загострене почуття помсти і т. п.).

Перевірка професійних здібностей кандидатів здійснюється, як правило, фахівцями того підрозділу банку, до якого планується направити того чи того кандидата, та фахівцями кадрового підрозділу. Під час перевірки вивчаються подані кандидатами документи, характеристики та рекомендації на них, проводяться бесіди, а також необхідні випробування. Останні можуть проводитися через розв'язання відповідних тестів, виконання практичних завдань, контролю поведінки в спеціально створених ігрових ситуаціях.

Як правило, інформація, отримана в результаті вивчення кандидата, не буває остаточною для прийняття рішення про зарахування його на роботу, оскільки вона лише дає змогу зробити висновок про характер і професійні якості кандидата. Але для прогнозування майбутньої поведінки тільки таких даних ще не досить. Тому значне місце у відборі кандидатів відводиться перевірці його минулої поведінки. З цією метою отримуються відгуки про кандидатів з тих організацій, де вони попередньо працювали, вивчається їх оточення, взаємовідносини. За необхідності може проводитись опитування окремих осіб.

Визначення схильності кандидатів до роботи в банку та їх негативних рис забезпечується проведенням з ними роботи фахівцями психологічної служби банку (психолога-соціолога). Така перевірка здійснюється через відповідні бесіди та розв'язування спеціальних тестів. Водночас деякі ознаки в поведінці окремих, особливо залежних, осіб можна виявити вже під час співбесіди. Окремі зовнішні ознаки поведінки залежних

осіб подані у Додатку 17. Тут доцільним більш ретельніше вивчення оточення кандидатів на роботу: друзів, партнерів, членів сім'ї. Тривалий взаємний потяг, симпатія, активне співробітництво можливі тільки на основі ідентичних цінностей, які становлять переконання особистості.

Допомогу може надати розширена самооцінка кандидатом своєї особистості. Вона да змогу уточнити його позицію, з'ясувати, наскільки він перейнявся тим, що від нього чекають на роботі, що і як він може зробити. Вивчення висловлювань особистості про свою роль у тій чи тій діяльності допоможе чіткіше зрозуміти природу формування багатьох його вчинків, вад характеру, поглядів, настанов тощо.

При вивченні кандидата слід бути обережним і не допустити порушення його прав. Отримання інформації про кандидата може здійснюватися тільки з його власного дозволу, що необхідно письмово засвідчити.

Наукові джерела повідомляють, що обсяги інформації про людину, отримані в результаті різних методів її перевірки, можуть становити: а) у результаті бесіди — 20%, б) у результаті тестування — 40%, в) у результаті опитування колег, друзів — 35%, г) у результаті спостереження за поведінкою у відповідних ситуаціях — до 60%. Тобто, найбільш повну картину про кандидата на роботу можна отримати лише при використанні комплексного підходу до проведення його перевірки.

Разом з тим слід пам'ятати, що при відборі кандидатів значну роль відіграє так званий кадровий ризик. Справа в тому, що частина кандидатів може мати здібності хорошого, ініціативного, творчого спеціаліста, але тільки на рівні виконавця. У таких фахівців можуть бути відсутні здібності організатора, керівника і такі працівники можуть бути зовсім не здатні до управлінської діяльності. Тому професійний розвиток і кар'єра таких працівників може забезпечуватися тільки по горизонталі: спеціаліст, провідний спеціаліст, головний спеціаліст, консультант, радник, помічник і т. п. Призначення такого фахівця на посаду, пов'язану з керівництвом персоналом, організацією банківського виробництва призведе до дезорганізації роботи відповідного колективу, зниження показників ефективності його діяльності, суттєвих недоліків. Тому у процесі перевірки кандидатів важливо виявити у них не тільки професійні здібності, а й здібності до організаторської, керівної роботи, щоб

у подальшому правильно будувати перспективи їх розвитку і не створювати критичних, ризикових умов роботи.

У процесі оцінювання кандидатів визначаються: відповідність їх вимогам робочих місць, на які вони претендують; здатність до аналізу виробничих ситуацій і прийняття самостійних рішень; мотиви прагнення зайняти відповідну посаду в банку; наявність внутрішньої культури, відповідного менталітету; комунікабельність; сприйняття нового, прагнення до навчання (розуміння необхідності додаткового навчання); перспективи розвитку і кар'єри.

Фахівці зазначають, що при відборі кандидатів на роботу та їх подальшому просуванні важливо враховувати п'ять позицій. Кандидат професійно придатний до роботи, якщо він:

— може виконувати роботу (оцінка компетенцій);

— хоче працювати (характер амбіцій, прагнення кар'єри);

— є керованим у роботі (рівень дисципліни, особливо виконавчої);

— сумісний (може працювати в команді, розумітися з керівництвом);

— безпечний (присутні необхідні моральні якості й орієнтація на загальний результат) [163].

Щоб отримати відповідь на зазначені характеристики, оцінка кандидатів має бути комплексною, із застосуванням різних методик (оцінка документів і біографічних фактів, оцінки по віковому і статевому факторах, оцінка психологічних показників, оцінка професійних якостей і т. д.).

Усвідомлюючи провідну роль кадрів у забезпеченні безпеки банку, важливо визначити, які особисті якості людини не можуть сприяти виконанню заходів безпеки, а також хто з персоналу через це потребує особливої уваги або підтримки.

Серед подібних якостей можна назвати: емоційній розлад, неврівноваженість поведінки, розчарування у собі й своїх здібностях, відчуження від колег по роботі, невдоволеність своїм службовим становищем, уразливе самолюбство, украй егоїстичні інтереси, відсутність достатньої розсудливості, небажання виконувати заходи безпеки, нечесність, фінансова безвідповідальність, надмірна балакучість.

Водночас досвід організації банківської безпеки дозволяє виділити основні особисті якості працівника банку, яким надається перевага: чесність, принциповість (суворе додержання основних правил), добросовісність, ретельність і пунктуальність у виконанні своїх обов'язків,

дисциплінованість, емоційна стійкість (самовладання), прагнення до успіху і порядку в роботі, самоконтроль учинків і дій, правильна оцінка особистих можливостей і здібностей, помірна схильність до ризику, обережність, уміння зберігати таємниці, хороша пам'ять і тренована увага.

Відбір і розстановка кандидатів здійснюється за критерієм найбільшої відповідності вимогам робочих місць. Крім цього, ураховуються перспективи подальшого використання прийнятих на роботу працівників, можливості оволодіння ними новими технологіями банківського виробництва та ініціювання таких технологій ними самими, відсутність фактів серйозних порушень банківської безпеки та непорозумінь із законом у минулому.

За певних умов, за наявності відповідних перспектив, але недостатньому досвіді фахівці можуть бути прийняті на роботу за трудовою угодою як помічники, асистенти, дублери відповідних фахівців банку. При набутті ними навичок самостійного виконання виробничих завдань такі фахівці можуть призначатися на посади в порядку, передбаченому штатним розписом.

У деяких випадках може виникати необхідність додаткової підготовки прийнятих на роботу в банк працівників, особливо на посади, пов'язані з виконанням нових видів робіт, освоєнням нових технологій тощо. У таких випадках робота працівника в банку може розпочинатися з його короткострокового навчання.

Важливе місце у формуванні банківського фахівця, скорішого оволодіння ним своїми обов'язками займає правильна організація становлення працівників банку на посаді. Даний період роботи фахівця, як правило, проходить у три етапи: ознайомлювальний, організаційний, адаптаційний. На першому етапі, яким керує безпосередній керівник підрозділу, куди призначено працівника, здійснюється ознайомлення останнього з основними підрозділами банку, їх розміщенням, особливостями і завданнями свого підрозділу, характером його діяльності, посадовими обов'язками працівника і відповідальністю за їх виконання. Тут же здійснюється ознайомлення нового працівника з колективом підрозділу, де він працюватиме. Перший етап виконується протягом першого дня роботи. В цей самий період працівник забезпечується необхідними засобами для виконання роботи.

На цьому етапі з працівником проводяться відповідні інструктажі, у тому числі і з заходів безпеки, отримуються від нього відповідні зобов'язання щодо дотримання в таємниці і нерозголошення інформації банку з обмеженим доступом.

Другий етап призначається для ознайомлення і самостійного виконання всіх виробничих завдань, передбачених посадовими обов'язками працівника, хоча б один раз, визначення ефективності їх виконання і оцінювання безпосереднім керівником. Етап закінчується звітом, який робить працівник за результатами своєї роботи. Тривалість етапу — перший тиждень роботи.

Третій етап призначається для вироблення працівником особистих підходів, стилю роботи і поведінки на робочому місці та в колективі, оволодіння специфікою виконання виробничих функцій, прийнятих у підрозділі, визначення своєї ролі і місця в колективі. Етап триває один місяць.

Контроль роботи працівників банку проводиться з метою виявлення об'єктивного стану справ щодо якості, ефективності виконання ними виробничих завдань і своїх посадових обов'язків, сумлінності та творчості фахівців на своїх робочих місцях, ознак можливого виникнення негативних ситуацій та загроз діяльності банку. Серед заходів контролю можуть застосовуватися різні види перевірок, опитування думки колег, отримання відгуків, вивчення поведінки працівників у колективі і на своїх робочих місцях, періодичне тестування, звіти тощо.

З метою підвищення якості та ефективності контролю роботи працівників, виявлення ознак порушення ними режиму безпеки, недобросовісної та протиправної поведінки підрозділи безпеки банків серед працівників банку виділяють групи ризику. Як показує досвід, до складу таких груп можуть входити: працівники, що мали в минулому судимість або кримінальне переслідування: працівники, в поведінці яких є ознаки залежності; працівники, які відповідно до своїх обов'язків регулярно приймають відвідувачів та клієнтів; особи допоміжного складу (секретарі, водії керівників банку, працівники канцелярії та секретаріату банку, охоронці); працівники, родичі яких працюють у конкурентів чи в правоохоронних органах; працівники, повноваження яких дають змогу приймати остаточні рішення щодо використання коштів банку; особи, що виконують у банку тимчасову роботу; працівники підрозділів матеріально-технічного забезпечення діяльності банку. Відповідно до ступеня ризику за кожною із груп установлюється періодичний, регулярний чи постійний контроль. Щільність контролю визначається підрозділом безпеки. До здійснення контролю залучаються керівники підрозділів, підрозділи безпеки, ревізійний, аудиту

та керівництво банку. Основними формами контролю працівників банку є перевірка їх роботи, спостереження за поведінкою та контроль зв'язків (рис. 10.2).

Велике значення у процесі контролю персоналу має виявлення негативної поведінки працівників щодо банку, скоєння ними протиправних та злочинних дій. З цією метою підрозділи безпеки банків здійснюють заходи внутрішньої безпеки, важливою складовою яких є внутрішньобанківська інформаційна діяльність, спрямована на формування так званого каналу зворотного зв'язку. Відомо, що крім офіційного внутрішнього інформаційного простору банку існує і сфера кулуарної, неофіційної інформації. У цій частині інформаційного простору здійснюють інтенсивний обіг потоки різного роду відомостей про певні, здебільшого латентні для керівництва банку, події, порушення, а то й злочини. Тому формування каналу зворотного зв'язку для безпеки банку, у тому числі й кадрової, є досить актуальним. Цей канал є відкритим і в загальних рисах може прописуватися в Правилах внутрішнього розпорядку роботи банку або ж у Положенні про внутрішньооб'єктовий режим банку. Такий спосіб отримання зворотної інформації буде ефективним, якщо забезпечуватиметься можливість будь-якому працівникові банку в будь-який час надавати свої повідомлення керівництву банку чи підрозділу безпеки, у тому числі й на конфіденційній основі. Це можуть бути поштові скриньки, телефони довіри, пейджери, спеціальна операторська служба тощо. За всіх умов застосування каналу зворотного зв'язку має бути підконтрольним керівництву банку, давати кожному його працівникові комфортно і безболісно надавати повідомлення про відомі йому порушення і злочини, що коються в банку.

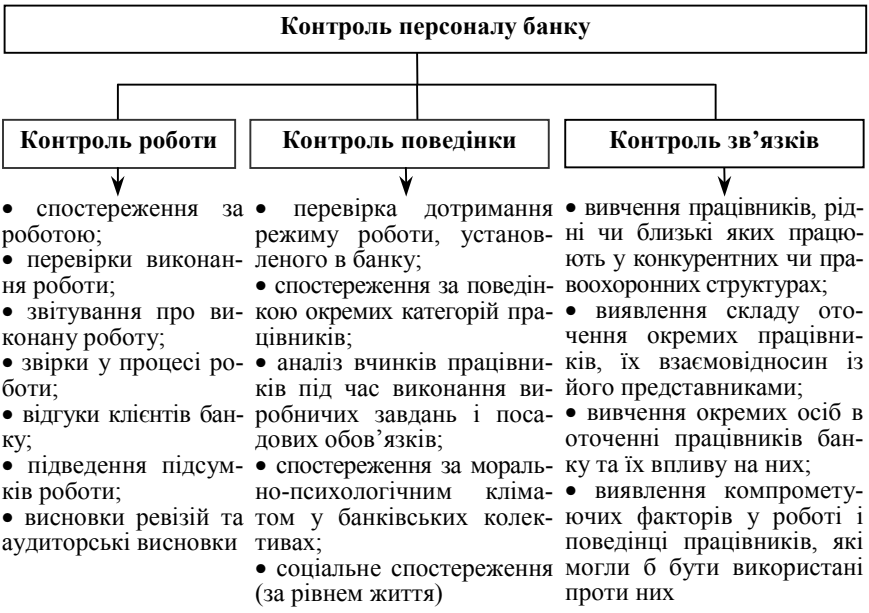

Рис. 10.2. Форми контролю персоналу банку

Узагальнюючи заходи кадрової безпеки, необхідно зазначити, що вони є досить різноманітними, торкання різних сфер взаємовідносин і поведінки працівників банку, але мають одне спрямування — попередження, виявлення та локалізація правопорушень злочинів і недобросовісної поведінки персоналу банку. Основні напрями, за якими кадрова безпека має вживати заходів щодо попередження, виявлення та локалізації правопорушень і злочинів, що можуть бути скоєні працівниками банків наведено на рис. 10.3.

Рис. 10.3. Напрями, за якими кадрова безпека банку має вживати заходів щодо попередження, виявлення та локалізації правопорушень і злочинів, що можуть бути скоєні працівниками банку

10.2. Психологія недобросовісного працівника, клієнта, шахрая

Ученими встановлено, що існує реальна можливість отримувати певну інформацію про стан внутрішнього світу людини за її зовнішніми проявами. Для цього є певні передумови. Взаємодія психіки і тіла людини будується на принципі «психофізичного паралелізму», який виявляється у тому, що психічне відображається у фізичному, і навпаки, фізичні зміни є причиною зміни психічного стану.

Будь-які переживання людини так чи інакше виявляються у її зовнішньому вигляді, міміці, позах, інтонації голосу, жестах та ін. Результати досліджень показують, що досвідчені фахівці понад 65% інформації про людей отримують у процесі спілкування через спостереження за ними. Якщо слово людини частіше за все є результатом її свідомості, оцінки і прогнозування ситуації спілкування, то жести — проекція підсвідомих процесів. Мова і рухи тіла людини можуть говорити про різне. Якщо у мові виражається те, що людина хотіла б сказати, то в жестах і міміці — те, що вона реально відчуває, переживає, чим збуджується і на що сподівається. Неузгодженість між змістом мови і жестами зовнішній спостерігач може побачити по деяких проявах. Насамперед людина може свідомо контролювати (тримати у колі уваги) у середньому 7(±2) об'єктів. Під час контакту зі спеціалістом безпеки злочинець, недобросовісний працівник або клієнт вимушені стежити за словами і обдумувати відповіді на запитання, виконувати вимоги, що ставляться до нього, наприклад, показати документи тощо.

Крім цього, людина одночасно може управляти лише 2—3 елементами свого тіла (наприклад, стежити за виразом обличчя, жестами рук). У будь-якому разі, хвилюючись, порушник буде постійно упускати з-під свідомого контролю окремі «мікросюжети», які будуть свідками розлагодження його мовної і немовної системи комунікацій і, як наслідок, його нещирості. Це

можуть бути ледь помітні мікрорухи м'язів обличчя, більш часте моргання та дихання, почервоніння і збліднення шкіри, звуження зіниць, ковтальні рухи (що свідчить про пересихання в роті), підвищення потовиділення, закриті позиції (схрещування, зжимання, перехоплення рук, перехрещення ніг) тощо.

Більше того, мовою і негативними переживаннями (хвилюванням, страхом, занепокоєнням тощо) управляють різні півкулі кори головного мозку людини. Тому в кризових ситуаціях можуть виявлятися збої в їх синхронному функціонуванні. Права півкуля бере участь в управлінні негативними емоціями і водночас координує діяльність лівої половини тіла людини. Отже, можна спостерігати таке: якщо людина хоче щось показати співрозмовникам, то це відображається на правій половині її тіла, а те, що вона реально переживає, можна спостерігати на лівій. Так, нервові, неадекватні ситуації, рухи лівої руки (вертіння ручки, посилена жестикуляція і т. п.) можуть свідчити про підвищене занепокоєння людини.

Існують й інші характерні психофізичні вади у людини під час посиленого емоційного стану, та вони менш доступні для спостереження, тому й акцентувати увагу на них немає потреби.

Незважаючи на велику кількість сигналів, що дозволяють підозрювати людину в тимчасовому занепокоєнні і хвилюванні, насправді їх вияв може бути настільки незначним і невиразним, що поставити точний «діагноз» дуже важко. Здібностями досконало відчувати подібні зміни в людині можуть володіти не всі фахівці служби безпеки, тому слід організувати пошук та відбір осіб, найбільш підготовлених для цього та створити умови для їх роботи.

Розглядаючи структуру злочину, можна виділити виключно психологічні властивості дій злочинця: мотивацію злочину, обґрунтування злочину, обґрунтування наслідків злочину.

Будь-який злочин мотивується злочинцем якимись особистими потребами і причинами, цим людина, що його здійснює, ніби виправдовує себе і нейтралізує почуття вини.

У переважній більшості банківські працівники і клієнти банку — це люди, які підкоряються визначеним правилам, прийнятим у банку. Але через деякий час дехто з них може дійти висновку, що є можливість присвоїти гроші, викрасти цінності банку або зробити спробу незаконної шахрайської дії з метою отримати нереєстрований прибуток.

Основними факторами мотивації такої ситуації можуть бути:

• привабливість мети: знання того, що бажаний об'єкт є в наявності, і точно відомо, де він міститься, як зберігається й охороняється; знання можливості отримання дарових грошей, матеріальних цінностей за допомогою незначних змін, установлених правил роботи з документами або неоднозначного трактування положень нормативних і законодавчих актів; наявність дуже великих сум грошей;

• об'єктивні й суб'єктивні мотиви, породжені відставанням технологій банківського виробництва від рівня інтелектуального розвитку працівників та високою досконалістю і досвідом роботи окремих із них;

• мотиви, що сприяють рішенню про правопорушення:

а) банк, на думку працівника, настільки багатий, що своїми діями працівник не завдасть йому ніякої шкоди;

б) працівник не відчуває своєї належності до колективу і банку в цілому, вони для нього чужі, робота тут сприймається працівником як засіб збагачення і є тимчасовою;

в) невдоволеність роботою, колективом, керівництвом;

— мотиви, якими намагаються виправдовувати злочин:

а) заперечення відповідальності (якщо ці дії ніким не контролюються, то ніхто не може бути винний у тому, що коїться);

б) заперечення шкоди (розмір отриманих грошей настільки малий, що ніхто від цього не постраждає);

в) осудження дій банку (виконана мною робота така велика, а платня за неї така мала, що не залишається нічого, як піти на такий вчинок);

г) заперечення жертви (банк отримує такий прибуток, що подібний вчинок не зробить його біднішим);

д) звернення до вищої справедливості (дії виправдовуються тим, що отримані гроші, наприклад, будуть використані на лікування близької людини);

е) несприйняття вчинку як правопорушення (навколо всі порушники, злодії, які крадуть у значно більших розмірах).

Багато хто з порушників вважає, що вони самовідданою працею на благо банку заробили право на таке правопорушення.

Обґрунтування злочину складається насамперед з доступності об'єкта злочину та зі здібності працівника його приховати. Працівник знає, що існує відповідна дія або предмет, який є для нього цінністю, знає також, що він за рівнем своєї підготовки, за посадою може легко виконати таку дію без істотних наслідків,

тому в нього виникає готовність до такого вчинку.

Обґрунтування наслідків злочину — це останній психологічний бар'єр у працівника, переступивши який, він стає потенційним злочинцем. Оцінюючи можливість викриття і наступних санкцій, злочинець аналізує: чи буде адекватним покарання скоєному вчинку, можливість доказу, що такий вчинок скоєно саме ним, можливість викриття самого факту вчинку.

Сукупність зазначених вище факторів показує, що мотиви скоєння злочину працівником або клієнтом банку достатньо різноманітні і їх збіг може бути тільки там, де не вживають серйозних заходів безпеки банківської діяльності.

Чи можна звернути увагу на людину, яка ще не скоїла правопорушення, але готова до нього? Відповіддю на це запитання може стати наведений нижче психологічний профіль недобросовісного працівника, клієнта та шахрая. Психологічний профіль — це опис найбільш помітних вад людини (групи людей) і особливостей її поведінки, що вирізняють конкретну людину (групу людей) із загальної маси. Тобто психологічний профіль визначає відмінні характеристики окремої людини або групи людей, об'єднаних загальними психологічними особливостями.

Серед недобросовісних клієнтів і працівників, різного роду шахраїв, порушників і злочинців чітко окреслюються два типи: шахраї за покликанням і шахраї за обставинами.

Шахрай за покликанням сам організовує свої махінації і до певного часу веде їх з успіхом. Він свідомо йде на порушення, його спонукає жадоба грошей. Як правило, у нього високий соціальний статус, збереженню і підвищенню якого він надає велике значення. Для нього мають велике значення матеріальні цінності. Усі людські цінності розглядаються ним через призму вигоди. Така людина має великі здібності до маніпулювання обставинами і людьми, що дає можливість їй створювати хитрі проекти з метою порушення законів і встановлених правил. Вона дуже динамічна, любить контакти, володіє даром переконання, добре орієнтується в соціальній системі. Дуже розумна, але недостатньо культурна й освічена; у прагненні досягти мети діє як нахаба. Цій людині багато чого вдається, і тому вона оптиміст. Шахрай за покликанням — особистість примітивна, агресивна, егоцентрична і самозакохана. Інші люди для нього — це не більше, ніж засіб досягнення особистої мети. Його емоційний світ бідний, глибокі почуття йому недоступні, іншу людину він сприймає як річ, якою можна скористатися. Емоційну порожнечу

він компенсує повною віддачею справі, досягає в цьому великого успіху й отримує у такий спосіб душевну рівновагу. Уявлення такої людини дуже продуктивне і творче, але працює в одному напрямі: знайти нові прийоми, щоб обійти контроль, використати прогалини в законодавстві, її винахідливий розум дає змогу подолати труднощі, якими багате життя ділової людини. Така людина не вдячна тим, хто їй допоміг врятуватися, сама може звинуватити будь-кого. Психологія шахрая за покликанням схожа до психології гравця. Обидва прагнуть до нових перемог не з бажання більшого накопичення, а щоб мати можливість продовжувати таку ризиковану діяльність.

Таким чином, шахрай за покликанням — це людина, що прагне не стільки до багатства, скільки до влади. Як правило, це людина, яка, не отримавши ніякої спадщини, зробила себе сама.

Шахрай за обставинами — людина іншого складу. За природою вона чесна, порушення закону обумовлюється несприятливим збігом обставин. Серед людей цього типу можна зустріти інженерів, науково-технічних працівників, як правило, мало знайомих з фінансовою роботою. Вони отримують не дуже великі доходи і намагаються діяти самостійно, але не можуть оцінити ризику своєї діяльності. Отримавши перший прибуток або зазнавши поразки, втрачають голову і не знаходять інших способів, крім протизаконних. До таких осіб можна віднести дрібних службовців, комерсантів-початківців, секретарів керівників фірм, банків, підприємств. Вони вирізняються безмежною довірливістю, необдуманістю вчинків, непрактичністю. Сукупність таких якостей не дає змогу їм об’єктивно оцінити сумнівну ситуацію, і вони погоджуються або самі йдуть на ризиковані угоди, не вбачаючи небезпеки або недооцінюючи її.

У психологічному плані обидві ці категорії мають одну спільну рису — прагнення до легких грошей, можливості збагатіти без особливих труднощів.

10.3. Конфлікти у банку, їх попередження та вирішення

Конфлікт — це зіткнення протилежних інтересів, думок, оцінок окремих людей або груп людей у процесі їх спільної діяльності чи виконання однієї (близької за змістом) роботи.

Конфлікти в банку можуть бути внутрішніми (між окремими працівниками, групами працівників одного колективу) і зовнішніми — між колективами підрозділів одного банку та колективами банків. Небезпечними для банку є всі конфлікти, але найбільш тяжкі наслідки можуть бути в результаті внутрішніх конфліктів. Як правило, вони відбуваються дуже емоційно і хворобливо, бувають тривалими, їх характер набуває антагоністичних рис.

Характеризуючи наслідки таких конфліктів, необхідно зазначити:

❖ переживання гострого і хронічного несприятливого психічного стану веде до суттєвого зниження ефективності професійної діяльності працівників. Ученими доведено, що сприятливий психічний стан підвищує ефективність дій приблизно на 20%, м'язову силу — до 90%, чутливість зору і слуху — на 35—65%, знижує кількість помилок і неточностей у діях у 5—10 разів. При цьому покращується увага, спостережливість, знижується стомлюваність. Негативні переживання навпаки призводять до розсіювання уваги, перенесення її з об'єктів спостереження на внутрішні процеси і стан, знижують вольову готовність до негайних дій;

❖ довгочасне перебування в умовах негативного емоційного стану (тривоги, невідомості, чекання, злості, незадоволеності тощо), невміння знизити гостроту переживань, несприятливих дій може призводити до порушення діяльності організму людини. Ще в далеку давнину помічено зв'язок між емоціями людини та її фізичним станом. Наприклад, необхідність постійно стримувати емоції порушує роботу серця; заздрість і злість вражають органи травлення; туга і печаль прискорюють старіння; постійний страх приносить шкоду щитовидній залозі; безперервне горе викликає цукровий діабет. Сьогодні вже достеменно відомо, що тривалі нервові перевантаження здатні зруйнувати навіть дуже сильний організм;

❖ неможливість працівника управляти своїми почуттями і настроєм негативно впливає на взаємовідносини з колегами, членами сім'ї, веде до психічної несумісності, конфліктів, ворожнечі.

Конфліктний стан є однією з причин порушення правил безпеки банку. Це не тільки помилки і порушення, які можуть допускати співробітники, що діють у стані негативних емоцій та роздратування, а й вираження незгоди з тими чи іншими правилами та вимогами режиму. Окремі особи можуть

Важко уявити, якою великою буває загроза таких вчинків у тих чи тих конфліктних обставинах.

Отже, конфлікти, створюючи особливу психологічну ситуацію в колективі, можуть завдати значної шкоди інтересам банку, тому попередження та своєчасне вирішення їх має велике значення.

Нормальному психологічному стану в колективі значною мірою сприяють зовнішні фактори:

✓ раціоналізація режиму, інтенсивності, складності, чергування завдань професійної діяльності;

✓ забезпечення ефективними сучасними засобами роботи;

✓ високий соціальний захист;

✓ нормалізація режиму харчування, вітамінотерапія;

✓ ефективна кадрова політика, орієнтована на людину.

✓ До внутрішніх факторів, спрямованих на попередження конфліктів, слід віднести:

✓ повну довіру до співробітників, надання їм максимальної самостійності;

✓ у центрі управління мають бути не плани і робота, а людина та її ініціатива, бо саме вона виконує і плани, і роботу;

✓ максимальне делегування функцій управління співробітникам;

✓ постійний розвиток мотивації працівників;

✓ результат діяльності колективу визначається ступенем його згуртованості.

Розв’язання конфліктів неможливе без виявлення їх причин. Досвід показує, що найчастіше конфлікти обумовлюються особливостями характеру членів колективу та невиправданою кадровою політикою його керівництва.

До першої групи причин можна віднести недостатність спілкування і розуміння колективом окремих працівників, різниця в планах, оцінках та інтересах співробітників, неправильне трактування чиїхось вчинків, дій поглядів, відсутність співчуття бажанням і потребам тощо. Конфлікти цієї групи рідко бувають антагоністичними Як правило, вони відбуваються між окремими співробітниками, рідше — між колективом і співробітником. Вирішують їх через визнання позицій сторін, переведення співробітників на іншу роботу, звільнення їх з роботи, задоволення вимог виконанням тих чи тих дій тощо.

Значно складнішими бувають конфлікти між керівництвом і співробітниками. Вони можуть виникати в результаті відсутності

демократичних основ управління, коли керівник здійснює штучний розподіл складу колективу на близьких йому і далеких від нього працівників, неадекватно оцінює результати роботи членів колективу, необґрунтовано просуває по службі окремих працівників, порушує умови стимулювання праці. Нетактовна поведінка керівника, зневажливе ставлення до своїх підлеглих, ніяк не сприяють здоровому клімату в колективі. Конфлікти, що виникають на такій основі, вирізняються значною тривалістю, антагонізмами, як правило, мають замасковану форму і миром практично ніколи не закінчуються.

При розгляді тих чи тих конфліктних ситуацій керівникові необхідно бути максимально об'єктивним, не підтримувати нічию сторону. Спокійно вислухати кожну сторону і зробити змогу розібратися в ситуації, подивившись на неї з однієї та з другої позиції. У разі необхідності треба порадитися з фахівцями, психологами, працівниками кадрових органів. Можна обговорити ситуацію на зборах колективу, хоча це може бути не завжди виправданим. Якщо виявлено порушення кадрової дисципліни, моральних норм, трудових угод, необхідно вжити всіх заходів до виправлення ситуації і задовольнити всі обґрунтовані претензії. Один з виняткових заходів — заміна керівника колективу або його тимчасове усунення (направлення на навчання, у відрядження тощо).

Щоб запобігти виникненню конфліктів, необхідно правильно формувати колектив. У кожної людини свій рівень сприйняття, темперамент, почуття, які залежно від віку, освіти, фаху можуть розвиватися різними темпами, за різними напрямами. У колективі такі властивості характеру виражаються через сприйняття й оцінки (людини, діяльності, проблеми і т. д.).

У результаті цього виникають різні позиції і погляди відносно того самого об'єкта. За певної відсутності однотипних властивостей характерів членів колективу такі погляди і позиції можуть бути приводом для конфліктів. Тому, формуючи колектив, поряд з професійними вимогами до співробітників необхідно приділяти увагу і їхнім психологічним особливостям, які забезпечували б психологічну сумісність.

При розробленні професійних вимог до фахівців, формуванні їхніх обов'язків рідко хто звертає увагу на те, ким заміщатимуться ті чи ті посади, яким психологічним якостям повинні відповідати фахівці. Мабуть, доцільно нагадати про необхідність розроблення відповідних професіограм, яким мають відповідати працівники банку, що займають ту чи ту посаду.

Професіограма має містити:

— перелік психологічних якостей, найбільш сприятливих для заміщення відповідної посади (спокій, увага, пам'ять, мова, активність, впевненість і т. д.);

— психологічні протипоказання до заміщення посади (дратівливість, готовність до необґрунтованого ризику, неврівноваженість, самозакоханість і т. д.).

Поєднання професійних та психологічних вимог при підборі кандидатів і формуванні колективів дасть змогу зменшити ризик виникнення конфліктних ситуацій.

Аналізуючи досвід кадрової роботи комерційних підприємств, у тому числі і банків, можна дати кілька рекомендацій та зауважень щодо формування виробничого колективу:

- збільшення терміну сумісної роботи керівника з підлеглими призводить до того, що дистанція в офіційних (ділових) відносинах між ними зменшується і керівник не може використовувати у повному обсязі свої посадові права. Тому на кожному рівні керівництва має існувати оптимальний період роботи керівника в тому самому колективі. Якщо адміністрація не має можливості підвищувати на посаді керівника, то ефективним може стати його переведення через відповідний термін на ту саму посаду в інший колектив;
- працівника, який тривалий час працював в одному колективі і підвищується на посаді, доцільно направляти працювати в інший колектив, щоб старі шляхи неформальних взаємовідносин не зв'язували ініціативу і заповзятість у його діяльності;
- для кожного рівня керівництва є своя домінуюча категорія підлеглих, на яку доцільно переважно орієнтуватися керівникові при прийнятті рішення;
- при створенні колективу доцільно мати на увазі, що оптимальний склад групи, сектору — три—чотири працівники, відділу — п'ять—шість, управління — 25—35 працівників;
- колективи доцільно створювати різностатеві з різницею у віці 8—10 років.

Слід зазначити, що тривогу викликають не тільки конфлікти, а й їх відсутність. Останнє свідчить, що обстановка в колективі не зовсім здорова. Якщо немає конфліктів, то можна вбачати, що в таких колективах існує або повний диктат, або ж про колектив не може йти мова взагалі, там кожен сам собі колектив.

10.4. Управління кадровою безпекою банку

Велике значення для ефективного забезпечення кадрової безпеки в банку має ефективне управління її функціями, які поширюють свій вплив, з одного боку, на персонал банку, а з другого — на всю його діяльність та стан безпеки. Причому зазначений вплив має здійснюватись як загальноприйнятими методами кадрової роботи, так і специфічними — режимними, що є прерогативою безпеки. За таких умов можна зробити висновок, що під управлінням кадровою безпекою банку можна розуміти цілеспрямований вплив органів управління банку на його стан та діяльність за допомогою заходів кадрової роботи і режиму з метою формування і підтримання високого рівня його безпеки на ринку банківських послуг. Управлінський вплив має бути цілком усвідомленим, тобто обґрунтованим і контролюючим, базуватися на виважених рішеннях керівництва банку. Крім того, такий вплив має здійснюватись як на систему в цілому, так і на окремі її елементи.

Базовими принципами управління, крім загальновідомих (законність, цілеспрямованість, відповідальність і т. д.), мають бути забезпечення розвитку та безпеки. Тут ми маємо виходити із загальноприйнятих законів суспільного розвитку, згідно з якими рівень розвитку будь-якої організації визначається рівнем розвитку її потреб та інтересів, а рівень безпеки — рівнем задоволення цих потреб і інтересів. Тобто управління має забезпечити збалансованість цих рівнів. Розвиток, задоволення і захист потреб і інтересів формують вимоги до управління, яке якраз і має забезпечити оптимальне співвідношення розвитку і безпеки як безпосередньо банку, так і суб'єктів, які забезпечують діяльність банку та формують умови для його функціонування, тобто персоналу, клієнтів та держави. За такого підходу управління кадровою безпекою банку з погляду розвитку, задоволення і захисту його інтересів матиме корпоративний характер (рис. 10.4).

Рис. 10.4. Корпоративний характер управління кадровою безпекою банку

Таким чином, особливість управління кадровою безпекою банку полягає в тому, що воно здійснюється через інтереси як самого банку, так і його персоналу, клієнтів і держави, у сфері безпеки.

Формування інтересів передбачає визначення потреб у безпеці всіх суб'єктів, на яких спрямовано управлінський вплив (рис. 10.5). Крім того, потреби в безпеці мають бути адекватні сучасним умовам та можливостям кожного із суб'єктів та забезпечувати їх розвиток у галузі безпеки, тому тут мають бути встановлені відповідні нормативи та рівні. Більше того, управління у своєму плануванні має орієнтуватися на такі нормативи, а також забезпечувати контроль відповідності потреб зазначеним нормативам. До основних таких показників у формуванні потреб безпеки можна було б віднести: рівень знань про небезпеки і загрози та шляхи їх подолання; психологічну, соціальну та професійну стійкість персоналу банку до загроз; автономність та живучість персоналу (здатність підтримувати певний час на необхідному рівні свої можливості); здатність до відтворення (термін приведення себе в робочий стан); національну незалежність і т. п.

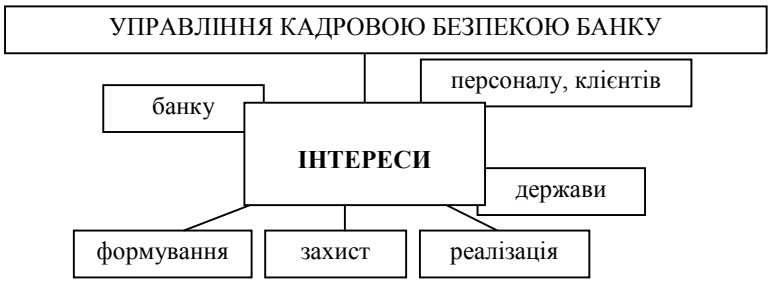

Рис. 10.5. Управління кадровою безпекою банку через інтереси її суб'єктів

Реалізація інтересів передбачає практичну діяльність щодо задоволення потреб безпеки як складову інтересу певного суб'єкта в конкретних умовах. Тобто управління кадровою безпекою банку має передбачати визначення та планування комплексу заходів, адекватних існуючим загрозам суб'єкта, своєчасне й ефективне їх проведення та ліквідацію наслідків. Тут важливим буде забезпечення моніторингу стану захищеності інтересів відповідних суб'єктів як складової комплексної системи економічної безпеки. Реалізація інтересів як потреб безпеки

здійснюється всіма суб'єктами, стосовно яких забезпечується управлінський вплив як самостійно, так і в сукупності.

Захист інтересів у сфері безпеки з погляду управління процесом передбачає утримання на необхідному рівні захисних можливостей суб'єктів за рахунок формування їх економічного, інтелектуального, фізичного та іншого потенціалу відповідно до потреб безпеки та умов, в яких вона реалізує свої функції.

Оскільки інтереси мають суб'єктивну (можливості суб'єкта щодо формування потреб безпеки та їх внутрішня структура) та об'єктивну (діяльність суб'єкта з реалізації заходів щодо задоволення зазначених потреб), процес управління має впливати на обидві ці складові інтересів та їх суб'єктів. При цьому, забезпечуючи вплив на суб'єктивну сторону, процес управління має бути спрямований на формування відповідного менталітету щодо формування, реалізації та захисту інтересів безпеки. А здійснюючи вплив на об'єктивну сторону, процес управління має спрямовуватися на формування умов діяльності суб'єктів щодо задоволення своїх потреб та розвитку інтересів з питань безпеки. Оскільки інтереси є достатньо стійкими і мають, як правило, довгостроковий характер, процес управління, впливаючи на їх формування, реалізацію та захист забезпечуватиме формування відповідної ідеології, усвідомленого переконання в безпечній поведінці банку, персоналу, клієнтів, державних органів на ринку банківських послуг, адекватній умовам функціонування даного ринку.

З огляду на те, що управління є самостійною сферою діяльності, його предметом є взаємовідносини, що складаються між суб'єктами, які, з одного боку, забезпечують вплив, а з другого — сприймають його, тобто в управлінні існують свій суб'єкт і об'єкт. Водночас управління кадровою безпекою банку не може бути абсолютно самостійним видом діяльності. Спрямовуючи свій вплив на забезпечення відповідного стану банку, управління кадровою безпекою є лише елементом загальної системи управління банком і спирається на ті самі ресурси, що й остання. Тобто, говорячи про суб'єкти управління, можна зазначити, що ними будуть органи управління діяльністю банку: загальні збори, рада акціонерів, правління банку, голова правління, дорадчі органи, які формуються у банку.

Об'єктом управління кадровою безпекою банку можна вважати діяльність підрозділів, установ, окремих осіб щодо забезпечення його розвитку та безпеки.

Методи управління залежатимуть від того, який рівень

режиму має бути сформовано в банку. Останній же залежатиме від потреб та інтересів відповідних суб'єктів і може формуватися як потреба захисту від загроз або потреба протидії їм, тобто формувати пасивну чи активну форму режиму безпеки.

Пасивний режим або режим захисту банку від загроз буде формуватися через такі фактори впливу:

— формування нормативно-правової бази банку з питань його безпеки;

— запровадження елементів безпеки в технологіях кадрової роботи;

— створення дієвої системи контролю та регламентування роботи і поведінки персоналу, банку, установлення відповідальності за порушення режиму його безпеки;

— формування адекватної політики поведінки банку на ринку та у взаємовідносинах з державними органами;

— формування банківського патріотизму у персоналу банку та банківських династій;

— установлення адекватного режиму охорони установ банку.

У свою чергу, активного режиму або режиму протидії загрозам банку у процесі управління кадровою безпекою може бути досягнуто через застосування таких методів впливу:

- упровадження моніторингу загроз персоналу банку, вироблення і проведення заходів щодо їх своєчасного виявлення, усунення і нейтралізації;
- виявлення правопорушень і злочинів у діяльності працівників банку та притягнення їх до відповідальності;
- проведення заходів з протидії впливу на персонал банку пропаганди конкурентів, залученню працівників до роботи на промислових шпигунів;
- притягнення працівників банку до матеріальної відповідальності щодо відшкодування завданих банку із їх вини збитків.

Реалізація цих та інших методів впливу в цілому має сформувати в банку відповідний режим кадрової безпеки, рівень якого має буде адекватним ситуації, яка утворюється навколо нього. Водночас зазначені методи впливу повинні враховувати потреби й інтереси з питань безпеки як самого банку, так і його персоналу, клієнтів та держави. Якщо інтереси безпеки банку, визначені в самому понятті його безпеки, то інтереси інших суб'єктів мають бути сформовані насамперед виходячи із їх ролі в системі безпеки банку.

Основними інтересами персоналу банку з питань безпеки можуть бути:

• отримання гарантій роботи та соціального захисту;
• забезпечення безпечних умов праці, формування особистої незалежності та впевненості в собі;
• формування професійного досвіду та кар'єри;
• створення умов для забезпечення власних потреб персоналу.

Водночас інтереси безпеки держави в системі безпеки банку передбачають:
• забезпечення гарантій стійкості фінансової системи країни та соціального захисту населення через надійну роботу банків;
• розвиток економічної могутності країни на основі розвиненої системи інвестиційної діяльності банків;
• зменшення ризику впливу тіньової складової фінансів на розвиток економіки країни за допомогою встановлення в банках відповідного режиму їх безпеки.

Зазначені інтереси можуть бути забезпечені лише через роботу персоналу банків.

Інтереси клієнтів банку полягають насамперед у доступності банківських послуг, їх якості та гарантіях рівних взаємовідносин.

За таких умов управління кадровою безпекою банку можна вважати як управління інтересами суб'єктів, що є учасниками управлінського процесу.

Підсумовуючи розглянуті питання можна зазначити, що під кадровою безпекою банку слід розуміти такий стан його кадрових ресурсів, за якого забезпечується мінімальний ризик формування загроз банку від його персоналу та ефективний вплив працівників банку на його прибуткову діяльність.

РЕЗЮМЕ

Безпека банку в роботі з персоналом забезпечується у двох напрямах: формування банківського патріотизму та лояльності персоналу через забезпечення його потреб та інтересів, у тому числі й у сфері безпеки; створення у банку відповідного режиму комплектування кадрами та поведінки персоналу. У першому випадку в основу формування кадрової безпеки має бути покладено довіру до персоналу, у другому ж — відповідні правила роботи працівників банку. поєднання цих двох напрямів і має забезпечувати відповідний рівень кадрової безпеки в банку.

Разом з тим кожен з працівників банку має взяти на себе обов'язок протидії недобросовісній та протиправній поведінці своїх колег, утримання їх від дій, які суперечать чесним звичаям

та традиціям, що склались у банку. Водночас банк має утворити відповідні умови чесної поведінки, а саме: урегулювати взаємовідносини з персоналом, розробити відповідні технології забезпечення безпеки, яких мають дотримуватися працівники, ввести відповідні заборони на певні дії працівників і вжити заходів мотивації їх безпечної поведінки. Якраз такі умови і забезпечуватимуть очікуваний рівень кадрової безпеки у банку.

Терміни і поняття

Вирішення конфліктних ситуацій
Комплектування банку персоналом
Контроль персоналу
Конфлікт
Персонал банку
Попередження конфліктів у банку
Психологія недобросовісного працівника, клієнта, шахрая
Становлення працівника банку на посаді
Управління кадровою безпекою банку

Питання для перевірки знань

1. Яких заходів слід вжити банку для попередження або мінімізації загроз щодо персоналу банку?
2. Чому правове навчання персоналу вважається одним із заходів профілактики правопорушень та злочинів у банку?
3. На що мають бути спрямовані заходи безпеки, щоб мінімізувати загрози банку від його персоналу?
4. Якими принципами слід керуватися при побудові системи відповідальності в умовах довіри?
5. Чому заміщення вакантних посад має здійснюватися на конкурсних засадах?
6. За якими напрямами здійснюється перевірка кандидатів на роботу в банк?
7. Чи можуть впливати особистісні якості кандидата на роботу в банк на рішення про прийняття його на роботу?
8. Чи може бути прийняте позитивне рішення про прийняття на роботу фахівця, якому необхідна додаткова підготовка?

9. Що передбачає такий елемент кадрової роботи, як становлення працівника на посаді?

10. У чому полягає мета контролю роботи і поведінки працівників банку?

11. Яких заходів слід вжити банку для попередження, виявлення та локалізації правопорушень і злочинів, що можуть бути скоєні працівниками банку?

12. Чим обумовлюється виникнення конфліктних ситуацій у колективах підрозділів банку?

13. Що є основою вирішення конфліктних ситуацій?

14. Які рекомендації слід використовувати банкам при формуванні виробничих колективів?

15. У чому полягає особливість управління кадровою безпекою банку?

Завдання для індивідуальної роботи

1. Ви — фахівець банківської справи, тимчасово не працюєте, активно здійснюєте пошук роботи. Одного разу вас запросили на співбесіду до одного із провідних банків. Після співбесіди особа, яка її проводила, звернулася до вас із запитанням, чи не заперечуєте ви стосовно подальшої перевірки вас фахівцями банку. Ви не заперечували, але яких дій з перевірки вашої кандидатури вам слід чекати?

2. Ви — керівник підрозділу з роботи з проблемними кредитами. До вас на співбесіду прийшла молода жінка, яка бажала зайняти вакантне місце економіста у вашому підрозділі. На цій посаді ви хотіли бачити чоловіка, а не жінку. Але рівень її кваліфікації значно вищий, ніж у чоловіків, які також претендували на цю посаду. Яке рішення ви приймете в цій ситуації і чому?

3. Ви — заступник головного бухгалтера, усі працівники бухгалтерії жінки. Через ваш характер або з якихось інших причин ви не подобаєтеся нікому з колективу, в якому працюєте. Головний бухгалтер пропонує вам перейти в окремий кабінет, але це негативно впливатиме на вашу роботу, оскільки вам необхідна інформація, яку повідомляють вам працівники бухгалтерії. Як ви будете діяти за таких обставин?

Література для поглибленого вивчення

1. *Алавердов А. Р.* Управление кадровой безопасностью организации : ученик / Алавердов А. Р. — М. : ООО «Маркет ДС Корпорейшн», 2010. — 176 с.

2. *Гордієнко К. Д.* Прийняття на роботу: співбесіда, анкетування : практ. посіб. / Гордієнко К. Д. — К. : КНТ, 2006. — 184 с.

3. *Демин Ю. М.* Управление кадрами в кризисных ситуациях / Демин Ю. М. — СПб. : Питер, 2004. — 219 с.

4. Економіка праці та соціально-трудові відносини : підручник / [А. М. Колот, О. А. Грішнова, О. О. Герасименко та ін.] ; за наук. ред. д-ра екон. наук, проф. Колота А. М. — К. : КНЕУ, 2009. — 711 [1] с.

5. *Самоукина Н. В.* Незаменимый сотрудник и кадровая безопасность / Самоукина Н. В. — М. : Вершина, 2008. — 176 с.

6. *Сулейманов У. И.* Правила охоты на «крыс» или как бороться с внутрикорпоративными хищениями / Сулейманов У. И. — М. : Ось-89, 2008. — 144 с.

7. *Шейнов В. П.* Конфликты в нашей жизни и их разрешение / Шейнов В. П. — Минск : Амалфея, 1996. — 288 с.

Розділ 11

ДІЇ УСТАНОВ БАНКІВ В ЕКСТРЕМАЛЬНИХ УМОВАХ

*Вивчивши матеріал цього розділу, ви будете **знати**:*

- ✓ *суть і види екстремальних ситуацій, що можуть утворюватися в/навколо банку;*
- ✓ *організацію дій банку на випадок виникнення екстремальних ситуацій;*
- ✓ *дії банку в умовах виникнення психологічних чи ідеологічних диверсій, терористичних актів, техногенних аварій та катастроф, стихійного лиха, масових протестів і безладдя;*
- ✓ *правила ліквідації наслідків впливу екстремальних ситуацій і відновлення режиму безпеки банку,*

*а також **уміти**:*

- ✓ *забезпечувати безпечну поведінку в умовах дії уражаючих факторів екстремальних ситуацій;*
- ✓ *грамотно діяти у складі евакуаційних команд та команд рятівників у разі виникнення екстремальних ситуацій;*
- ✓ *забезпечувати роботу банку в умовах дії уражаючих факторів екстремальних ситуацій.*

11.1. Організація дій банку на випадок виникнення екстремальних ситуацій

Окрім загроз економічного, інформаційного та кадрового характеру сучасний бізнес може стикатися з різними непередбачуваними обставинами, результати негативної дії яких можуть завдавати масової шкоди засобам виробництва, персоналу, виробничим технологіям і бізнесу взагалі. Через дію таких обставин суб'єкти господарювання змушені займатись аварійно-рятівними роботами, вживати заходів для збереження здоров'я постраждалих працівників, зменшенню матеріальної шкоди, відновленню свого бізнесу.

Крім того, характерною особливістю сьогодення є високе фізичне та психологічне напруження при вирішенні всіх життєвих завдань, у тому числі і в процесі виробництва. Таке напруження, зокрема, створюють умови навколишнього середовища, інформаційна насиченість нашого буття, підвищена емоційність взаємовідносин та сприйняття різноманітних ситуацій підприємницької діяльності. Усе вищезазначене у сукупності може обумовлювати ситуації за яких підприємства, банки, установи та їх працівники піддаються серйозному впливу досить напружених, майже критичних ситуацій, які характеризуються високим рівнем загроз їх здоров'ю, життю та діяльності.

Характеризуючи суть поняття екстремальної ситуації слід зазначити, що під екстремальними ситуаціями в бізнесі можна розуміти події, явища природного, економічного, соціального чи якогось іншого походження або результат діяльності суб'єктів чи певних процесів, які за своєю інтенсивністю, масштабами поширення, тривалістю, складністю та небезпечністю виходять за межі звичайних умов існування, можуть уражати людей, об'єкти та суб'єкти економіки або довкілля та вимагають для їх подолання найвищої концентрації фізичних, духовних, фінансових, матеріальних та інших зусиль і ресурсів.

За своїм походженням екстремальні ситуації бувають *психологічного (ідеологічного) характеру*, пов'язані з дією різного роду (шантаж, використання психотропних (наркотичних) речовин і спеціальних психотехнічних комунікацій, зомбіювання, дискредитація, наклеп, поширення

негативних чуток тощо) факторів психологічного (ідеологічного) впливу; *фізичного характеру*, пов'язані з загрозою застосування сили у будь-якому вигляді (терористичні акти, розбійні напади, захват заручників і т. і.); *стихійного характеру* (землетруси, повені, бурі і т. і.); *техногенного характеру* (радіаційні або хімічні аварії та атаки, виробничі аварії, пожежі).

Класифікуючи екстремальні ситуації відповідно до характеру їхнього впливу на банк та його працівників, можна виділити такі:

— ситуації, що виникають навколо банку і стосуються тільки його;

— ситуації, що виникають навколо працівників банку і мають суттєвий вплив на банк;

— ситуації, що виникають у колективах банку або навколо них і створюють напружені умови їх роботи;

— ситуації, в які банк або його працівники потрапляють випадково.

Дії екстремальних ситуацій, як правило, спрямовані на заподіяння банку матеріальної або моральної шкоди та шкоди його працівникам. Так, матеріальна шкода банку може виникати через фінансові збитки, які він може нести через змушення окремих працівників банку приймати неефективні рішення; втрату майна, обладнання, техніки банку через їх пошкодження та знищення в результаті терористичних актів, пожеж, дії стихійного лиха або техногенних аварій і катастроф; упущення вигоди або збитки від несанкціонованого витоку інформації банку, з обмеженим доступом; витрат банку понесених з метою ліквідації наслідків дії екстремальних ситуацій.

У свою чергу, моральна шкода банку може виражатись у пониженні іміджу банку, його позицій на ринку і рівня конкурентоспроможності. Моральна шкода, завдана працівникам банку, може виявлятися через різноманітні стреси, психологічний розлад у роботі і поведінці, пониженні психологічної стійкості до різних загроз (страх, невпевненість у собі тощо), порушенні загальноприйнятих принципів моралі.

Крім того, працівники банку можуть зазнавати фізичної шкоди від дій екстремальних ситуацій. Насамперед це може бути пов'язано з послабленням їх здоров'я, хворобами, каліцтвом, загибеллю та ін.

Усе це вказує на те, що в процесі здійснення підприємницької діяльності обов'язково необхідно враховувати можливість виникнення і негативного впливу таких ситуацій.

Основними причинами та джерелами екстремальних ситуацій можуть бути недобросовісні дії конкурентів, протиправна діяльність злочинців, різкі зміни правових умов, невиконання зобов'язань партнерами, сили природи, техногенні процеси виробничої діяльності підприємств, безпечна поведінка окремих осіб. Екстремальні ситуації, як правило, настають раптово, унаслідок чого банк та його працівники не мають можливості заздалегідь підготуватися до дій у тих чи тих ситуаціях і не завжди можуть правильно реагувати на перші ознаки та прояви таких ситуацій. Водночас саме перші хвилини (години) мають вирішальне значення для подальшого розвитку ситуацій. Тому банки та інші підприємства повинні прогнозувати можливості створення навколо їх установ різних видів екстремальних ситуацій, розроблювати плани своїх дій і формувати відповідні органи на випадок виникнення таких ситуацій. Такі плани мають передбачати порядок дій установ банку в період загрози та наступу екстремальних ситуацій, а також дії щодо ліквідації їх наслідків. Крім того, у цих планах можуть передбачатись заходи забезпечення безпеки персоналу та майна банків, їх ресурсів, а також заходи щодо забезпечення комерційної діяльності в умовах дії екстремальних ситуацій.

Варіант структури плану дій банку на випадок загрози та виникнення екстремальних ситуацій подано на рис. 11.1.

Для управління діяльністю банку і виконання специфічних завдань з протидії уражаючим факторам екстремальних ситуацій, а також захисту об'єктів і працівників банку в умовах дії екстремальних ситуацій у банку можуть утворюватися відповідні органи: група управління діяльністю банку в екстремальних умовах, евакуаційні команди та команди рятівників.

Основними функціями групи управління є організація захисту об'єктів і персоналу банку від уражаючих факторів екстремальних ситуацій, забезпечення роботи банку (у тому числі і обмеженими силами і засобами) під впливом уражаючих факторів екстремальних ситуацій, ліквідація наслідків дії уражаючих факторів та відновлення функціонування елементів структури банку. Очолює групу управління керівник банку (установи банку). До складу групи управління можуть входити керівники юридичного, адміністративно-господарського, фінансового підрозділів, а також підрозділів безпеки, кадрів, по зв'язках з громадськістю та інших за рішенням керівника банку (установи банку). За погодженням до складу зазначеної групи можуть входити представники органів МНС та МВС.

Основні функції керівника та членів групи наведено в Додатках 18, 19.

Рис. 11.1. Структура плану дій банку на випадок загрози та виникнення екстремальних ситуацій

Евакуаційні команди призначені для організованого проведення евакуації, цінностей та персоналу банку в період безпосередньої загрози виникнення екстремальної ситуації. Склад команди визначається із розрахунку по дві особи для евакуації кожного з банківських підрозділів та від 10 до 30 осіб для евакуації цінностей і документів.

Особи, які задіяні у таких командах, проходять відповідну підготовку та інструктажі щодо їх дій у період виникнення загроз настання екстремальних ситуацій та при настанні таких ситуацій. Зокрема, евакуаційні команди вивчають правила та процедуру евакуації, можливі небезпеки, які можуть виникати під час екстремальних ситуацій, способи протидії та виходу з них, основні та запасні маршрути евакуації, правила попередження паніки, місця збору персоналу і матеріальних цінностей після евакуації.

Команди рятівників призначені для пошуку, надання допомоги та евакуації з осередків ураження та небезпечних місць, осіб, що постраждали від дії уражаючих факторів у екстремальних ситуаціях. В установі банку можуть створюватися одна—дві команди у складі 10—15 осіб кожна.

Персонал зазначених команд вивчає найбільш вірогідні місця, у яких можуть переховуватися люди під час дії вражаючих факторів екстремальної ситуації, правила поведінки з людьми, які перебувають у стресовому стані, стані найвищого емоційного напруження або психологічного розладу, правила надання першої медичної допомоги і транспортування поранених, травмованих, уражених осіб та правила гасіння пожеж і поведінки в приміщеннях, які горять. Усі команди (евакуаційні і рятівників) комплектуються за рахунок працівників банку. До складу цих команд підбираються фізично здорові, треновані працівники банку, здатні за своїми психологічними, моральними та фізичними даними виконувати роботи в умовах суттєвого ризику й емоційного напруження.

Основними заходами з попередження та уникнення екстремальних ситуацій у банку можуть бути:

- використання безпечних і надійних технологій виробництва, дотримання їх у діяльності банку;
- дотримання правил техніки безпеки в повсякденній діяльності банку;
- виконання вимог трудової та виробничої дисципліни всім персоналом банку;

• вироблення компромісної політики у взаємовідносинах з конкурентами;
• створення системи безпеки в банку;
• технічне укріплення території банку та його об'єктів;
• прогнозування та планування дій банку на випадок виникнення екстремальних ситуацій;
• упровадження системи сповіщення персоналу, його підготовки на випадок дій в екстремальних умовах;
• протипожежне обладнання території та приміщень банку;
• дотримання встановленого законом порядку здійснення банківської діяльності;
• пропаганда та реклама ефективної діяльності банку;
• створення безпечних умов праці в банку;
• організація взаємодії з органами МНС і МВС на випадок виникнення в банку екстремальних ситуацій;
• створення в банку обстановки, яка б виключала конфлікти і конфронтацію у взаємовідносинах з іншими суб'єктами;
• оприлюднення спроб негативного інформаційного впливу на банки та умисних дій щодо заподіяння йому шкоди, формування вигідної банку громадської думки щодо таких спроб.

11.2. Забезпечення діяльності банку під впливом уражаючих факторів екстремальних ситуацій

Найбільш поширеними ситуаціями, які виникають у діяльності банків, можуть бути ситуації, пов'язані з ідеологічними диверсіями проти них. Під екстремальною ситуацією, створеною в результаті ідеологічної диверсії, розуміють нагнітання моральної і психологічної обстановки навколо банку або в його колективах з метою створення високого емоційного напруження в роботі і поведінці персоналу, пониження довіри клієнтів і партнерів до банку, провокування його керівництва до непродуманих рішень і дій. Серед дій, які спрямовані на проведення ідеологічних диверсій можуть бути:

♦ тиск на банк з використанням засобів масової інформації через передання або публікацію інформації, яка ганьбить банк чи його керівництво, перекручення об'єктивних відомостей, оприлюднення неправдивих відомостей чи таких,

♦ тиск на банк з використанням можливостей органів державного управління, контролю і нагляду безпідставним проведенням численних перевірок і ревізій, вимог надання різноманітних довідок, прийняття рішень, які суттєво обмежують діяльність банку;

♦ поширення негативних чуток навколо банку;

♦ підбурювання до агресивної поведінки щодо банку його клієнтів, партнерів, акціонерів та персоналу;

♦ поширення інформації, яка сприяє виникненню конфліктних ситуацій у колективах банку.

Основними видами ідеологічних диверсій можуть бути провокації, дискредитація, а також поширення негативних чуток про банк.

У процесі провокацій здійснюються дії, спрямовані на підбурювання клієнтів, акціонерів, працівників банку до колективних чи масових виступів, демонстрацій, мітингів, спрямованих проти власників, керівників або взагалі діяльності банку. Тут же можуть мати місце заклики до недовіри банку чи його керівництву, необґрунтовані звинувачення, масова відмова від його послуг. В окремих випадках можна бачити провокаційну поведінку, виступи в ЗМІ лідерів певних соціальних груп, окремих особистостей чи окремих його працівників, по різних каналах поширюється інформація, що викликає страх, недовіру, депресію особливо у клієнтів, конфлікти у колективах банку.

У процесі дискредитації банку в ЗМІ та через неформальне спілкування поширюється інформація, що ганьбить банк чи його власників або керівництво, з'являються відомості про кримінальну їх поведінку, зв'язок із сумнівними суб'єктами чи організаціями. У такій ситуації можуть активно поширюватися відомості, що компрометують окремих працівників банку, у ЗМІ з'являються різного роду прогнози розвитку ситуації навколо банку, як правило, з негативними наслідками. В інформаційному середовищі досить часто мають місце відомості, які самостійно чи в сукупності з уже відомими вводять його суб'єктів в оману щодо об'єктивності ситуації навколо банку. Як правило, такі відомості подаються викривлено, неповно, під вигідним для суб'єктів диверсій кутом зору, хоча зазначені відомості і можуть базуватися на дійсних фактах але об'єктивний характер їх є іншим.

За певних умов ідеологічні диверсії можуть створювати для банків досить суттєві та тривалі екстремальні ситуації, вихід із яких, як правило, здійснюється болісно, із втратою іміджу, а інколи і з матеріальними втратами. Тому основними заходами захисту банку від ідеологічних диверсій будуть заходи упереджувального характеру. Враховуючи таке, банками напрацьовано відповідний досвід щодо протидії ідеологічним диверсіям. Такі заходи умовно можна розділити на заходи організаційного та заходи спеціального характеру. До першої групи відносять:

— періодичні публікації, виступи представників банку про його стан і діяльність у засобах масової інформації. Звикнувши до отримання об'єктивної інформації про банк клієнти, інші громадяни можуть з недовірою поставитися до появи іншої інформації, яка характеризує банк або керівництво у негативному плані;

— періодичні зустрічі керівництва банку з представниками засобів масової інформації. Такі зустрічі дадуть змогу мати більш тісні стосунки з журналістами, які за певних умов з метою перевірки можуть звернутися до банку у разі надходження до них негативної для банку інформації. Більше того, у банку завжди буде змога більш ефективно впливати на інформаційне оточення банку, формувати у нього позитивний імідж, знаходити порозуміння з представниками «мас-медіа»;

— контроль публікацій, виступів у засобах масової інформації, в яких згадується банк за будь-яких підстав, визначення причин появи таких публікацій (виступів) і відповідна реакція на них. Причому реакція має бути як щодо засобів масової інформації, так і стосовно авторів публікацій, виступів, незалежно від того, позитивно чи негативно згадується банк у них;

— підтримка в колективах банку доброзичливої обстановки, заснованої на засадах взаємної довіри і нормах службової етики, контроль морального стану колективів установи банку;

— постійний аналіз сфери діяльності банку, своєчасне виявлення появи загроз йому, у тому числі й ідеологічного характеру, вжиття заходів щодо недопущення їх реалізації та нейтралізації наслідків;

— періодичне проведення перевірок роботи персоналу, його атестації, виявлення та облік факторів, які сприяють створенню конфліктних або яки

— хось інших негативних ситуацій у колективах банку;

— установлення і підтримання порозуміння та добросусідських взаємовідносин із місцевими органами влади та правопорядку;

— постійне проведення роботи щодо недопущення створення умов, за яких можуть бути скоєні порушення встановлених правил роботи, зловживання або злочинні дії персоналом банку;

— активне відстоювання інтересів банку і захист своїх працівників у всіх інстанціях незалежно від характеру протидії.

Заходи спеціального характеру, у свою чергу, поділяються на заходи активного характеру — протидії і заходи пасивного характеру — захисту.

Активними заходами є:

- установлення авторства і замовників негативних і неправдивих публікацій, виступів (надання інформації), організація та проведення компанії антидиверсій щодо них;
- збір фактів недобросовісної поведінки щодо банку з боку джерел ідеологічних загроз (диверсій), доведення до них вимог про припинення негативних дій проти банку та спростування неправдивої інформації з одночасною загрозою оприлюднити такі факти;
- організація надання позитивної для банку інформації від імені третіх осіб, особливо тих, які користуються авторитетом у споживачів інформації або таких, що є керівниками відповідних державних і недержавних установ і органів;
- проведення роботи з представниками засобів масової інформації та організація протидії виходу у світ неправдивих про банк відомостей;
- оприлюднення інформації про наявність (появу) у банку суттєвого супротивника (на ринку банківських послуг або в іншій сфері), дії якого направлено на заподіяння банку моральної та матеріальної шкоди, пониження його іміджу і використання такої ситуації з певною метою.

До пасивних заходів відносять:

— викриття вигаданого і неправдивого характеру негативної інформації про банк або окремих його працівників, яка з'явилася в його інформаційному просторі;

— звернення до суду щодо дій окремих осіб та організацій, установ, які поширюють негативну, наклепницьку інформацію про банк;

— звернення до відповідних державних структур з вимогою перетинання свавілля, яке коїться навколо банку, особливо, коли встановлено, що до таких дій причетні державні службовці;

— вжиття заходів щодо обмеження каналів подання негативної інформації, впливу її на персонал і клієнтів банку, недопущення доступу такої інформації в банк;

— вжиття заходів щодо зміни об'єкта ідеологічних диверсій, модифікації інформації, яка створює негативну ситуацію навколо банку, доведення такої інформації додатковими чутками, виступами, публікаціями до зовсім безглуздої і на цій основі демонстрація безпідставності відомостей, які подаються в інформаційне середовище банку.

Важливе місце у протидії ідеологічним диверсіям займає робота з нейтралізації чуток, що негативно впливають на банк. У загальному вигляді під чутками розуміють усну інформацію з невизначеним ступенем достовірності, яка стихійно поширюється учасниками комунікаційної системи (членами колективів банку) і відповідає направленості їхніх потреб.

Ознаками чуток вважаються: невизначена достовірність інформації, чутки спрямовані на задоволення якої-небудь потреби людей, незадоволеної іншим способом, колективне авторство та анонімність чуток, усний характер чуток, яскравість чуток. Як правило, чутки є відповіддю на громадське бажання, уявлення щодо тих чи тих характеристик стану діяльності банку або їх змін. З цих позицій несприйняття чуток або ігнорування їх системою безпеки є невиправданим.

Основними причинами виникнення чуток можуть бути невизначеність ситуації, в якій опинився банк чи колектив за певних умов його діяльності. Саме така ситуація може викликати невпевненість і тривогу людей і породжувати різноманітні чутки.

Близькою до цієї причини є недостатня інформованість людей про відповідні події та рішення, які приймаються керівництвом банку. Важливою психологічною закономірністю, що сприяє поширенню чуток є те, що вони є відповідною компенсацією емоційної недостатності в процесі сприйняття і відображення подій і фактів, які мають місце в банку та навколо нього. Людина, яка передає чутки, отримує задоволення від реакції слухачів на її повідомлення, а останні — від сприйняття нової, раніше невідомої інформації.

Причинами чуток також можуть бути необхідність в утвердженні особистості в колективі, бажання людей попередити про небезпеку на основі передання неповної (невідомої) інформації, вороже ставлення стосовно членів колективу один до одного, бездіяльність, одноманітність, нудьга в організації

роботи, недоліки управління колективами і людьми (деяка затримка в прийнятті рішень, недостатня координація дій виконавців, наявність конфліктів і т. і.).

Чутки небезпечні тим, що можуть впливати на ефективність роботи персоналу банку, поведінку його клієнтів, партнерів. Особливо небезпечними є чутки, пов'язані з негативними характеристиками діяльності банку та його керівництва, саме поширення таких чуток може сприйматися як ідеологічна диверсія проти банку.

Важливим елементом боротьби з чутками є профілактика та протидія їх поширенню. Серед заходів щодо профілактики чуток слід виділити такі:

- попередження зростання високого рівня невизначеності і тривоги в колективах банку та його клієнтів;
- створення і підтримка на необхідному рівні системи інформування, яка володіє відповідним іміджем, високою надійністю і достовірністю;
- створення стійкого зворотного зв'язку від колективів, клієнтів, партнерів до джерел інформації, своєчасне реагування на потреби і запити людей;
- формування емоційного середовища, яке виключало б можливість поширення чуток.

У протидії чуткам можуть бути використані такі заходи:

- подавлення чуток фактами, без прямого спростування самих чуток;
- виступи офіційних осіб зі спростуванням чуток;
- зустрічне поширення протилежної інформації;
- дискредитація відомого «автора» чуток фактами його причетності до поширення таких чуток.

Водночас за певних умов одним із методів протидії чуткам є їх підтвердження. Тут слід зауважити, що переважна кількість чуток містить, по суті, об'єктивну, хоч і дещо змінену інформацію. Якщо це так, то спростовувати правду не треба. Підтвердження чуток є умовою їх припинення.

Отже, чутки є відображенням відповідних змін в інформаційному просторі. Тому неуважне ставлення до них сил безпеки може залишити непомітним появу загроз банку і в наступному значно ускладнити ситуацію як у банку, так і навколо нього. Чутки не будуть небезпечними, якщо є знання їх природи, причин і вжито відповідних дій щодо профілактики їх поширення в банку, протидії їм та нейтралізації наслідків їх появи.

На межі ідеологічних і економічних диверсій існує ще одна небезпека, яка, як правило, є непомітною і тому неперевершеною за своєю підступністю і безжалісністю. Ім'я їй — саботаж. Екстремальні ситуації, створені в результаті саботажу, є найбільш негативними для іміджу та економічної безпеки банку.

Під саботажем слід розуміти всілякі усвідомлені дії, які явно призводять до порушення і дезорганізації встановленого порядку, норм і правил роботи банку. На даний час саботаж є одним з так званих «м'яких» методів конкурентної боротьби суб'єктів підприємницької діяльності. У своїй спрямованості він найчастіше орієнтується на руйнування зв'язків і взаємодії між суб'єктами банківської діяльності, тобто клієнтами, партнерами, акціонерами, персоналом. Тут використовуються непомітні на перший погляд методи, які маскуються під звичайний розвиток подій.

Саботаж — досить складна діяльність, яка потребує знання або розроблення спеціальних методик, значної кваліфікації його організаторів і виконавців, серйозної підготовчої роботи та залучення великих ресурсів. Тому його проведення здійснюється тільки в особливі періоди загострення конкуренції, виході банків на нові ринки, залученні ресурсних клієнтів та в інших ситуаціях посилення агресивної поведінки суб'єктів ринку.

Виходячи з критеріїв походження саботажу його можна розділити на:

— стихійний — виникає спонтанно, без підготовки, не ставить перед собою конкретної мети, як правило, виходить з самого банку (банківської системи), некерований, випадковий у проявах. Частіше за все він є реакцією на відповідну напруженість, яка виникає у самому банку (банківській системі). Такий саботаж також може спонтанно і припинитися;

— організований — виникає штучно, готується заздалегідь, має конкретну мету, виходить як із самого банку, так і з його оточення. У таких випадках явища, які виникають у рамках саботажу, пов'язані між собою та з іншими видами негативних дій щодо банку.

По видах дій, які застосовуються при проведені саботажу, його акції можна розділити на: а) організаційні — спрямовані на прийняття помилкових управлінських рішень; б) морально-психологічні — спрямовані на погіршення загального морально-психологічного стану в колективах банку або в окремих його працівників; в) технічні — спрямовані на організацію збоїв у роботі обладнання та технічних засобів, які використовуються у

банку; г) технологічні — спрямовані на погіршення якості послуг банку та неефективне проведення банківських операцій.

На жаль, як показує досвід, саботаж складно або ж взагалі неможливо попередити. Але за таких умов, необхідно бути готовим до застосування його проти банку і вжити заходів щодо зменшення втрат від нього. Тут, важливим є виявлення ознак настання саботажу. Серед таких ознак можуть бути: зростання збоїв у роботі банку (неефективне проведення операцій, втрата важливих для банку клієнтів, звільнення з роботи провідних фахівців та ін.), яка до останнього часу була стабільною; штучне обмеження сфери діяльності банку нормативними актами місцевих органів влади, поява негативних чуток про банк, підвищений інтерес до банку органів нагляду та контролю і т. п. Наявність деякої сукупності таких ознак, періодичне повторення та послідовність їх настання може говорити, що проти банку проводяться акти саботажу. Тут слід докласти зусиль щодо встановлення джерел та причин саботажу і одночасно вжити протисаботажних заходів загального характеру:

- перекривається несанкціонований доступ до колективів, технологій, інформації банку, у тому числі і для осіб, які працюють у банку, але безпосередньо не причетні до конкретних видів робіт, технологій, інформації;
- визначаються та приводяться в дію засоби за допомогою яких здійснюються дублюючі функції окремих технологій, операцій, послуг і систем комунікації;
- посилюються методи контролю за станом діяльності банку і окремими його установами та підрозділами, збільшується кількість показників стану та характеристик діяльності установ і підрозділів банку, зменшуються терміни між контрольними заходами.

Після встановлення джерел та причин саботажу може виникнути можливість з'ясувати кінцеву його мету. Це дозволить конкретизувати і посилити протисаботажні заходи, зокрема:

- організувати удавані об'єкти саботажу для розпорошення сил і ресурсів його ініціаторів;
- за відповідних умов блокувати чи нейтралізувати діяльність виконавців саботажних акцій або перенацілити їх діяльність проти удаваних об'єктів;
- створити уявлення про досягнення ініціатором саботажу своєї мети.

Слід зазначити, що практика українських банків та інших комерційних підприємств з боротьби з саботажем ще досить

незначна і вони тільки набувають такого досвіду. Тому виникнення екстремальних ситуацій, створених у результаті акцій саботажу, переживаються ними дуже важко, зі значними матеріальними і моральними втратами.

Поряд з ідеологічними диверсіями, спрямованими проти банку, достатньо поширеним є психологічний вплив на конкретних працівників банку, особливо керівного складу та провідних менеджерів. В окремих випадках такий вплив може здійснюватись у формі психологічних диверсій. Під останніми розуміють активне використання засобів комунікації, механізмів соціально-психологічного впливу, медичних препаратів та інших засобів з метою підпорядкування дій людини суб'єктам зазначених диверсій або створення сприятливих умов для реалізації їх задумів і рішень. Основними видами психологічних диверсій є:

✓ шантаж — залякування через загрозу оприлюднення компрометуючих фактів чи матеріалів, які ганьблять певну особу з метою примушування її до відповідних дій чи поведінки;

✓ застосування психотехнічних комунікацій — вплив на людину через використання її переконань, звичок, слабких рис характеру, особливостей психохарактеристик колективу для формування необхідної позиції чи поведінки (людини, колективу);

✓ зомбіювання — штучне введення людини у стан трансу і програмування її поведінки в інтересах досягнення відповідної мети, яку ставлять перед собою суб'єкти психологічної диверсії;

✓ застосування психотропних речовин — штучне (на хімічному чи біологічному рівні) обмеження інтелектуальних можливостей людини з метою примушення її до несвідомого виконання необхідних суб'єктам психологічних диверсій дій;

✓ поширення чуток — поширення в інформаційному середовищі певної особи відомостей, достовірність яких невідома, про саму особу або її оточення (виробничий колектив, сім'ю, близьких) з метою приведення їх до напруженого емоційного стану.

Ознаки екстремальної ситуації, зумовленої психологічним тиском (психологічною диверсією), наведено на рис. 11.2.

Рис. 11.2. Ознаки наступу екстремальної ситуації, викликаної психологічним тиском (психологічною диверсією)

У системі захисту від уражаючих факторів психологічних диверсій важливим є грамотна поведінка особи. Так, у разі спроби шантажу компрометуючою інформацією чи матеріалами слід показати шантажисту, що компромат, який ним використовується, зовсім не сприймається таким, не треба проявляти зацікавленість щодо походження такого компромату. Водночас, коли компрометуюча інформація (матеріали) дійсно небезпечна або ж вона подається в агресивній формі доцільно буде вимагати ознайомитися (побачити, прочитати, прослухати) з нею, отримати конкретну відповідь, перед ким шантажист хоче скомпрометувати, яким способом та коли. У процесі оцінювання факту компрометації слід пригадати, чи відбувалися події, випадки, дії, факти, якими чи через які шантажист хоче скомпрометувати, визначитися, наскільки реальною може бути компрометація і якими можуть бути її наслідки. Тут також доцільно визначитися, кому може бути вигідно компрометувати саме у такий спосіб, а також, як може сприйняти компрометуючий матеріал особа, перед якою шантажист прагне скомпрометувати. У процесі спроби шантажу необхідно також

визначити обсяг часу, який є для нейтралізації ситуації до моменту надання компромату, і порядок дій щодо захисту від негативних наслідків шантажу. Щодо змісту цих дій, то вони можуть бути такими:

- категорично відмовитися від подальшого спілкування з шантажистом і сприйняття повідомлення як компрометуючого у разі, якщо подій, фактів, якими прагнуть компрометувати, не було і є змога це довести;
- вжити заходів щодо недопущення передання компрометуючих матеріалів особі, перед якою хочуть скомпрометувати;
- вжити заходів щодо попередження шкідливих наслідків передання компрометуючих матеріалів, інформації;
- довести ситуацію до особи, перед якою хочуть скомпрометувати, подавши себе як жертву;
- тимчасово вийти із ситуації (виїхати у відрядження, піти у відпустку, лягти в лікарню і т. п.);
- у разі, якщо відомо особу шантажиста, вдатися до компромату проти неї і т. п.

За всіх умов в ситуації шантажу як і за інших видів психологічного впливу, необхідно залишатися, наскільки це можливо, урівноваженим, тримати себе у стані, який дає змогу нормально думати і діяти. Опинившись в такій ситуації, завжди доцільно зробити її аналіз та визначити своє місце в ній (ситуація створена проти вас, проти колег, рідних, близьких, потрапили в ситуацію випадково). Важливим тут буде оцінка ситуації, чим і наскільки вона небезпечна, кому може бути вигідне її створення і яку мету ставлять особи, якими створено ситуацію. Після аналізу та оцінювання ситуації необхідно визначити тактику своєї поведінки в ситуації психологічної диверсії.

Значне емоційне напруження та скрутне становище виникає, коли екстремальні ситуації створюються в результаті терористичних актів (загроза підриву або підрив вибухового пристрою, захват заручників, погроза насильством та насильницькі дії аж до знищення окремих фізичних осіб).

Ураховуючи особливу небезпеку терористичних актів, банки повинні вживати додаткових заходів безпеки у разі отримання інформації або виявлення ознак загрози терористичного акту, зокрема:

- посилити охорону об’єктів;
- установити оперативний зв’язок з правоохоронними органами і доповісти про виниклі підозри;

- уточнити заходи плану кризових дій;
- створити резерв автотранспорту на випадок проведення евакуаційних робіт;
- вжити заходів щодо захисту персоналу банку, попередити працівників про можливість роботи банку в умовах загрози або настання екстремальної ситуації;
- привести в готовність до негайних дій евакуаційні команди та команди рятівників;
- перевірити роботу резервних засобів зв'язку;
- привести в готовність до негайної роботи групу управління діяльністю банку в екстремальних ситуаціях.

Найбільш поширеними з терористичних актів проти банківських установ, як показує досвід іноземних банків, є загроза підриву або підрив вибухового пристрою в установах чи на території банків. Такі загрози створюють обстановку страху, невпевненості, посиленого емоційного напруження, стресу як для працівників банку, так і для їх клієнтів. Цим злочинці добиваються своєї основної мети — залякують не тільки персонал банку, а й членів їхніх сімей, партнерів і клієнтів банку.

Крім того, метою такого терористичного акту може бути демонстрація серйозності намірів конкурентів, злочинців, шантаж керівників банку, заподіяння моральної і матеріальної шкоди, помста, знищення конкурентів та ін.

Загроза підриву вибухового пристрою може визначатися через повідомлення про таке, а також рядом інших ознак, серед яких: посилення безкомпромісної конфронтації конкурентів; спроби застосування сили щодо банку та його працівників в інших формах; попередження про наступне застосування більш серйозних заходів; спроби несанкціонованого проникнення до банку; посилення негативів криміногенної ситуації та наявність зазначених вище умов нестабільності.

За таких умов до банку можуть надходити підозрілі (без зворотної адреси або від невідомих відправників) посилки, бандеролі, листи, передачі. Можуть зустрічатися підозрілі пакунки, як правило, у приміщеннях загального користування або в коридорах, несподівано з'являтись сліди ремонтних робіт, там, де їх не планувалося, чужі сумки, портфелі, коробки, інші предмети.

Вибухові пристрої можуть маскуватися в дитячих візках, транспортних засобах, інвалідних візках, телефонних апаратах, фото- та відеоапаратурі. Особливу небезпеку становлять так звані міни-сюрпризи, які комуфлюються під привабливі речі: гаманці,

авторучки, запальнички, плеєри, радіоприймачі тощо. Такі вибухові пристрої спрацьовують при торканні чи використанні їх.

Кожен працівник банку обов'язково повинен звертати увагу на такі явища та предмети, повідомляти про них підрозділ безпеки. Ніхто не має права чіпати такі предмети, переміщувати або якимось чином розкривати їх, не можна використовувати засоби радіозв'язку, у тому числі й мобільні телефони, поблизу таких предметів. Представники підрозділу безпеки, отримавши повідомлення про підозрілий предмет, ізолюють його від можливої дії щодо нього працівників банку, обмежують рух навколо предмета, візуально обстежують його, у разі необхідності забезпечують охорону підозрілих предметів до прибуття відповідних фахівців та доповідають керівникові банку. За його рішенням, викликають фахівців щодо знешкодження вибухових пристроїв, які опитують особу, котра першою знайшла даний предмет. За рішенням керівника банку або фахівців, які прибули для знешкодження можливого вибухового пристрою, проводиться евакуація персоналу установи банку (усього або його частини). У приміщенні, де містяться підозрілі предмети, відкривають вікна і двері для зниження ефекту вибухової хвилі та небезпеки ураження осколками конструкцій будівель, скла, предметів інтер'єру.

Про виявлений предмет та загрозу підриву вибухового пристрою до відповідного рішення керівника банку нікого з осіб, котрі перебувають у його приміщеннях, не повідомляють, аби не викликати паніки.

Таблиця 11.1

НЕБЕЗПЕЧНІ ВІДСТАНІ ПРИ ВИБУХУ РІЗНИХ ВИДІВ ВИБУХОВИХ ПРИСТРОЇВ

Вид вибухового пристрою	Відстань
Граната РГД-5	50 м
Граната Ф-1	200 м
Тротилова шашка масою 200 г.	50 м
Пивна банка 0,33 л.	60 м
Кейс	250 м
Дорожній чемодан	350 м
Автомобіль (легковик)	450—600 м

У разі підриву вибухового пристрою всі працівники банку незалежно від того де вони перебувають (у місці підриву чи в іншому місці), повинні за можливості зберігати самовладання, уточнити, чи є можливість самостійно покинути установу банку. Якщо це неможливо, то вжити заходів щодо подання сигналів про своє місцезнаходження.

Підрозділ безпеки у таких випадках повинен:

- зафіксувати час і місце вибуху;
- разом з командами рятівників вжити заходів щодо надання першої медичної допомоги пораненим, ураженим та особам, які перебувають у стані психічного розладу, евакуації працівників банку з небезпечної зони;
- зібрати осіб, які спостерігали вибух, для опитування працівниками правоохоронних органів;
- виставити додаткові пости охорони в усіх входах до банку, місцях найбільшої концентрації людей, зосередження цінностей і грошей;
- заборонити всім присутнім торкатись предметів, які перебувають у зоні вибуху, виключити можливість перебування там сторонніх осіб;
- вжити заходів щодо фіксації слідів і охорони місця події, після закінчення огляду місця вибуху правоохоронними органами взяти участь у ліквідації наслідків підриву вибухового пристрою;
- у разі виникнення пожежі вжити заходів щодо її гасіння.

Крім того, існують певні рекомендації щодо поведінки персоналу та інших осіб, які опинилися в зоні вибуху або поблизу нього. Насамперед не слід допускати скупчення людей у місці вибуху, оскільки може спрацювати інший вибуховий пристрій. Через небезпеку вибуху газової суміші, яка може накопичитись у зруйнованих і пошкоджених приміщеннях, не слід користуватися відкритим полум'ям (сірниками, запальничками, свічками, факелами і т. п.). Пересуватися слід обережно, не торкаючись пошкоджених конструкцій будівлі і будь-яких дротів. У задимленому приміщенні треба прикрити органи дихання мокрою тканиною. У разі ізоляції в окремих приміщеннях голосом або стукотом привертати увагу до себе інших людей.

З метою попередження терористичних актів з підривом вибухового пристрою необхідно в підвальних приміщеннях та на горищах банківських будівель установити міцні двері та надійні

замки, установити огорожу будівлі, що виключає легкий в'їзд автомобіля-бомби в будівлю банку, постійно перевіряти всі порожні приміщення. Періодично проводити огляд і по можливості віддаляти підозрілі автомобілі, що перебувають поблизу банку. Місця паркування автомобілів повинні бути якомога подалі від будівлі банку. Працівникам банку даються рекомендації звертати увагу на підозрілих людей, незвичну їх поведінку, необхідність ідентифікувати їх особистість.

Усі службові приміщення, приміщення, в яких розташовані технічні установки, сходові площадки мають бути вільними від зайвих предметів. У банку має бути запроваджено щоденне винесення сміття з приміщень та його території, сміттєві контейнери мають бути встановлені за межами будівель банку.

Для фіксування анонімних телефонних дзвінків передбачити спеціальні контрольні прилади для виявлення телефонного апарату, з якого може телефонувати зловмисник. Усі телефони, зазначені в офіційних довідниках, доцільно обладнати автоматичними пристроями для визначення номера телефона абонента та звукозаписуючими пристроями. Обов'язково слід провести інструктаж персоналу банку щодо дій у разі отримання повідомлення про загрозу підриву вибухового пристрою.

Підвищену увагу необхідно проявляти у разі доставки:

- пакетів, посилок, листів з помилками в адресі, назві банку, прізвищі адресата, з відсутньою зворотною адресою;
- листів у незвичних товстих (більше 3 мм) і важких конвертах, при згинанні вони схожі на резину;
- листів і посилок, доставлених не працівниками пошти чи кур'єрами, а невідомими особами;
- незвично легких або досить важких посилок і посилок зі зміщеним центром тяжіння;
- підозрілих мішків, ємностей, контейнерів.

Досить небезпечними є дії терористів, пов'язані із замахами на життя та здоров'я працівників банку. Відповідно до мети, яку ставлять перед собою терористи, замахи можуть бути демонстративні (для створення психологічного ефекту), замасковані, коли подається фальсифікована версія замаху, скриті (факт замаху приховується). Основними об'єктами замахів можуть бути власники, керівники, провідні менеджери установ банків, особи, які володіють компрометуючими матеріалами або інформацією на інших осіб, а також ті, що не бажають виконувати своїх зобов'язань перед кредиторами і не шукають компромісних рішень у взаємовідносинах з ними.

Ознаками, що вказують на формування загрози замаху, можуть бути:

- погрози, які висловлюються на адресу особи, щодо якої може бути скоєно замах;
- виявлення випадків спостереження за особою;
- пошкодження, виведення з ладу систем життєзабезпечення та комунікації в місцях, де перебуває особа;
- пошкодження дверей запасних входів, входів на горище, у підвали, у приміщення, де перебуває чи може перебувати особа, на яку готується замах;
- нав'язування знайомств з особою або її оточенням;
- часті спроби несанкціонованого доступу на об'єкт, де працює особа;
- різні і несподівані зміни в поведінці партнерів чи близького оточення особи;
- наполегливі спроби влаштуватися на роботу, пов'язану з обслуговуванням особи;
- незаплановані ремонтні роботи поблизу місць, де перебуває особа;
- наявність фактів щодо збору інформації про особу.

Поява сукупності таких та інших ознак має викликати у сил безпеки банку відповідну реакцію, насамперед пов'язану з установленням достовірності підготовки замаху та вжиття заходів щодо захисту особи. У цьому разі проводиться відповідний інструктаж особи щодо її поведінки, здійснюються заходи контролю за її пересуванням та перебуванням у місцях, пов'язаних з її роботою, а за необхідності вживаються заходи щодо охорони особи. Якщо ступінь загрози досить великий чи невідомий або існує велика імовірність замаху особа може бути на певний час виведена за межі небезпечної ситуації (поїхати у відпустку, відрядження, перебувати вдома тощо). Рекомендації щодо особистої поведінки людини в умовах загрози щодо неї терористичного акту (у тому числі й замаху) наведено в Додатку 20.

Досить поширеним актом терористичних дій є захоплення заручників. У наш час будь-який об'єкт може бути місцем захоплення й утримання заручників (у тому числі й банківські установи). Метою захоплення заручників, як правило, буває отримання викупу або примушення до виконання певних дій чи прийняття необхідних злочинцям рішень відповідними посадовими особами. При цьому зловмисники можуть добиватися досягнення своєї мети різними способами. Зазвичай у

ролі посередника в переговорах злочинці використовують керівників об'єктів (у даному разі банків). У всіх випадках життя людей, захоплених у заручники, стає предметом торгівлі.

При захопленні заручників у банку необхідно негайно повідомити правоохоронні органи, ініціативно не вступати в переговори з терористами, вжити заходів до перешкодного проходу в банк (до місця утримання заручників) представників правоохоронних органів та надати їм необхідну інформацію. У разі вимог терористів, що знаходяться в компетенції керівництва банку, виконувати їх, якщо це не пов'язано із заподіянням шкоди персоналу банку чи іншим особам, не суперечити терористам і не ризикувати життям оточуючих, не допускати дій, які можуть спровокувати злочинців до застосування зброї, підриву вибухових пристроїв чи інших небажаних дій.

Особливості поведінки осіб, що опинилися в заручниках подано в Додатках 21, 22.

В умовах загрози чи виникнення екстремальної ситуації в банку, у тому числі і обумовленої терористичними актами, особливо важливим є збереження діяльності банку відповідно до його призначення. Для утримання діяльності банку в межах, що дають змогу виконувати покладені на нього функції, під впливом уражаючих факторів терористичного акту керівництво банку періодично проводить аналіз можливостей щодо виконання своїх зобов'язань перед клієнтами і кредиторами, визначає найбільш важливі, критичні напрями зосередження своїх зусиль. У разі порушення режиму роботи банку, пошкодження його об'єктів визначаються можливості, терміни та порядок відновлення їх функціонування, проводяться відповідні заходи щодо залучення коштів для виконання таких завдань. Тут керівництво банку має бути готовим до реструктуризації банку, а то і його реорганізації, забезпечення діяльності банку обмеженими силами і засобами. В окремих випадках може бути доцільним перетворення (реінжиніринг) бізнес-процесів банку відповідно до умов, що склалися.

У разі великих обсягів відновлювальних робіт управління діяльністю банку може забезпечуватись по двох напрямках одночасно: звичайному — виконання завдань, безпосередньо пов'язаних з банківською діяльністю, і відновлювальному — ліквідація наслідків дії уражаючих факторів терористичного акту.

Деякі особливості щодо дій банку існують у разі загрози нападу на банк. Вони обумовлюються тим, що мета нападу має здебільшого матеріальний характер. І тому напади, як правило,

здійснюються злочинними елементами, тактика яких у загальному плані відома. Виходячи з цього банками вироблено ряд рекомендацій щодо дій:

а) у разі виявлення загрози нападу на банк:

— посилити охорону банку, його керівництва, перевірити роботу технічних засобів охорони. З метою підвищення ефективності роботи технічних засобів охорони слід урахувати досвід іноземних банків. Як виявилося, ефективність технічних засобів охорони у разі нападу на банк, як правило, не забезпечує очікуваних результатів. Так, технічні засоби охорони спрацьовують при нападі лише у 55% випадках. Телевізійні пристрої на 26% об'єктів виявлялися несправними, а лише 68% із числа справних незалежно реагували на напад. Тому посилення охорони слід забезпечувати насамперед за рахунок додаткового залучення сил фізичної охорони;

— вжити заходів щодо зменшення обсягу цінностей і сум грошей, які зберігаються у сховищі установи банку;

— сповістити правоохоронні органи про наявність загрози нападу та відпрацювати порядок сумісних дій у разі реалізації даної загрози;

— уточнити план дій у кризових ситуаціях;

— зменшити інтенсивність переміщення транспортних засобів банку і його керівництва;

— забезпечити контроль (вранці та ввечері) приміщень, які найбільш відвідуються сторонніми особами;

— упорядкувати за місцем і в часі потоки відвідувачів і персоналу банку, активно використовувати технічні засоби контролю людей та особистих речей, які вони проносять у банк, забезпечити візуальний і технічний контроль потоків осіб, які відвідують банк, періодично фіксувати їх за допомогою відео- і фотоапаратури;

— забезпечити проведення роботи щодо виявлення джерел і причин появи загроз, їх характеристик (місця, об'єкта, способу виконання і т. п.);

б) у разі нападу на банк:

— провести оповіщення персоналу банку та вжити заходів до його евакуації або переміщення в безпечне місце;

— змінити місцезнаходження і маршрути переміщення керівництва банку, у разі необхідності вжити заходів щодо легендування поведінки окремих осіб керівного складу;

— уточнити місце і час нападу, у разі, якщо нападники перебувають у банку, вжити заходів щодо встановлення їх місцезнаходження;

— заблокувати місце перебування та можливі маршрути переміщення зловмисників, сформувати групи, які контролюватимуть територію банку;

— у разі затримання нападників вилучити в них зброю і підозрілі предмети, провести особистий огляд, кожного з затриманих помістити в окреме приміщення і виставити надійну охорону до прибуття працівників правоохоронних органів.

Одним із уражаючих факторів терористичних актів є страх, який виникає у людей як стан сильної тривоги, неспокою, душевного збентеження перед небезпекою, яку несуть у собі терористичні дії. Негативність стану страху обумовлюється ще й тим, що він залишається у людини і після того, як небезпека минула, та може тривати довгий час, а то викликати суттєві зміни у психіці та поведінці людини. Тому важливо вжити заходів насамперед підрозділу безпеки щодо подолання працівниками банку страху, який виникнув у результаті скоєння терористичного акту. Тут було б доцільно об'єктивно розкрити ситуацію, що виникла внаслідок терористичного акту чи нападу на банк злочинців, довести рішення керівництва банку стосовно дій в умовах, які склалися та заходів захисту персоналу. Крім того, слід вжити заходів психологічного та медичного характеру щодо осіб, які зазнали психічних травм. Важливим є і демонстрація заходів, спрямованих на посилення режиму безпеки в банку. В окремих випадках доцільним буде проведення ротації працівників між підрозділами банку та створення їм нових умов роботи.

Суттєву небезпеку та екстремальну ситуацію можуть спричинити для банку техногенні аварії та катастрофи на підприємствах, що розташовані поблизу нього. Техногенні аварії та катастрофи здебільшого пов'язані з неконтрольованим викидом різного роду речовин і енергії. Мимовільне вивільнення енергії призводить до промислових вибухів, а мимовільне вивільнення речовин — до вибухів, пожеж і хімічного чи радіаційного забруднення території. В останньому випадку виникають тривалі, досить небезпечні ситуації для будь-якої діяльності, у тому числі і для банківської на забрудненій території. Заходи щодо захисту банку від уражаючих факторів техногенних аварій і катастроф, а також при забрудненні навколишнього середовища

отруйними та радіаційними речовинами подано в Додатках 23, 24, 25, 26.

Природні явища також є джерелом формування екстремальних ситуацій і справляють украй негативний вплив на діяльність суб'єктів господарювання, у тому числі і банків. У разі, якщо вони призводять до аварій, катастроф на виробництві та елементах інфраструктури або ж іншим явищам, спрямованим проти життєдіяльності людини, їх розглядають як стихійні лиха. В Україні це можуть бути землетруси та повені.

Землетруси найбільш характерні для сейсмічно активних зон. Такі зони оточують Україну на південному заході і півдні: Закарпатська, гори Вранча, Кримсько-чорноморська та Південно-Азовська. У сейсмічному відношенні найбільш небезпечними областями в Україні є Закарпатська, Івано-Франківська, Чернівецька, Одеська та Автономна Республіка Крим. На Закарпатті визначаються осередки землетрусів до 6—7 балів, на Буковині — до 6 балів, у Кримсько-чорноморській зоні землетруси можуть виникати до 8—9 балів. У Південно-Азовській зоні зафіксовані землетруси до 5—6 балів.

У разі отримання попередження про можливість землетрусу або ж перших його ознак банк має бути готовим зупинити виробничий процес, відключити подачу електроенергії, води, газу до його об'єктів, попередити персонал про загрозу землетрусу. Після закінчення поштовхів здійснити обстеження банківських об'єктів, визначити наявність пошкоджень та загальний їх стан. У разі руйнування об'єктів забезпечити пошук людей та евакуацію їх із небезпечних зон і надання допомоги. Відповідно до масштабів руйнувань необхідно встановити об'єкти, які можуть продовжувати свою діяльність, об'єкти, яким необхідно провести мінімальні відновлювальні роботи, об'єкти, щодо яких необхідно виконати відновлювальні роботи у значних обсягах, об'єкти, які не підлягають відновленню. Дії персоналу банку під час землетрусу викладено в Додатку 27.

Повені визначаються як значне затоплення місцевості внаслідок підвищення рівня води в річках, озерах, водосховищах, спричинене зливами, таненням снігу, руйнуванням грабель і т. п. Найбільш вірогідними зонами повеней в Україні є:

— у північних регіонах — басейни річок Прип'ять, Десна. За деякими даними площа повені в басейні р. Прип'ять може досягати 600—800 тис. га;

— у західних регіонах — басейни верхнього Дністра, річок Тиса, Прут, Західний Буг (площа можливих затоплень — від 20 до 130 тис. га);

— у східних регіонах — басейни р. Сіверський Донець з притоками, річки Псьол, Ворскла, Сула та інших приток Дніпра;

— у південному і південно-західному регіонах — басейн приток нижнього Дунаю та р. Південний Буг.

У разі загрози повені банк має вжити певних заходів щодо захисту своєї діяльності, цінностей і документів. Зокрема, доцільно всі документи, апаратуру, робоче знаряддя зосередити на верхніх поверхах, за можливості всі предмети, які під час повені можуть бути змиті, слід було б прив'язати щонайвище до міцних предметів. Практика показує, що варто зробити запаси питної води, а то і їжі, найбільш необхідних медичних препаратів. Використання електроенергії та газу здійснюється тільки з дозволу комунальних служб. Найбільш уразливі об'єкти слід укріпити мішками з піском, загородити вікна перших поверхів та двері. Окремі види майна необхідно заздалегідь евакуювати. Обов'язковим є проведення інструктажу працівників банку щодо їх роботи і поведінки в умовах загрози повені і затоплення приміщень банку.

Суттєву загрозу створення екстремальних ситуацій становлять пожежі.

За статистикою, понад 90% пожеж виникають унаслідок діяльності людини. З цього приводу великого значення набуває протипожежна безпека банку, заходи якої мають базуватись на вимогах Закону України «Про пожежну безпеку» (рис. 11.3).

З метою попередження пожеж в установах банку доцільно:

- обладнати всі робочі, виробничі приміщення та ділянки засобами пожежної сигналізації;
- установити в доступних місцях засоби гасіння пожежі, забезпечити періодичну перевірку їх працездатності;
- розробити Правила пожежної безпеки в установах банку, довести їх до персоналу та забезпечити контроль дотримання їх вимог;
- забезпечити щоденне прибирання та вивіз побутового сміття, не накопичувати легкозаймисті матеріали в одних місцях, вжити заходів щодо дотримання протипожежного порядку їх зберігання;
- обладнати та утримувати в робочому стані запасні виходи та виїзди з території банку;

• призначити особу, відповідальну за організацію пожежної безпеки в банку;

• усі проходи, виходи в будівлях банку утримувати в стані, який забезпечує швидку евакуацію людей, розробити план евакуації цінностей та персоналу;

• створити пожежну команду та забезпечити її підготовку до дій на випадок пожежі;

• не накопичувати і не складувати майно, застаріле обладнання на горищах, у підвалах, на території поблизу будівель банку;

• обладнати місця для паління.

Рис. 11.3. Забезпечення пожежної безпеки в банку (відповідно до Закону України «Про пожежну безпеку»)

Важливе місце в оперативному інформуванні персоналу про виникнення загрози, зумовленої екстремальною ситуацією, має формування системи сповіщення. У банку має розроблюватися план

сповіщення, в якому міститься схема оперативного доведення інформації до групи управління банком в екстремальних ситуаціях, схема виклику евакуаційних команд і команд рятівників, схема сповіщення персоналу і система її сигналів. Система сповіщення має забезпечувати подання звукових і/або світлових сигналів у будівлях і приміщеннях банку, а також на його території, трансляцію мовної інформації про характер небезпеки, необхідність евакуації чи інших дій відповідно до ситуації. Крім того, система сповіщення має передбачати включення в будівлі банку аварійного освітлення, світлових дороговказів напрямів і шляхів евакуації та періодичну трансляцію спеціально підготовлених текстів, спрямованих на попередження паніки. Система також повинна забезпечувати дистанційне відкриття дверей запасних входів в банку або інших додаткових виходів. Сигнали сповіщення мають відрізнятися від сигналів іншого призначення. Кількість пристроїв сповіщення та їх потужність повинні забезпечувати одночасне доведення сигналів до всіх працівників установи банку. Управління системою сповіщення повинно здійснюватися з приміщення охорони.

Отже, можна зазначити, що сьогоднішня діяльність суб'єктів господарювання, у тому числі і банків, а також життєдіяльність громадян здійснюється в умовах існування досить великого різноманіття негативних факторів, небезпек і загроз, зумовлених природними, кліматичними, соціальними, економічними, інформаційними, політичними особливостями нашого буття. Урахування таких особливостей, вжиття заходів щодо захисту від їх негативного впливу буде однією з передумов успіху в будь-якій діяльності. За таких умов у працівників банку необхідно виховувати безпечну поведінку, психологічну готовність зустріти небезпеку і вміння грамотно діяти в таких умовах. А самому банку слід розроблювати ефективні заходи захисту свого іміджу, матеріальних цінностей та персоналу не тільки для ефективного проведення банківських операцій, а й для забезпечення виживання в умовах дій несприятливих факторів.

РЕЗЮМЕ

Забезпечення банківської діяльності під впливом екстремальних ситуацій є досить актуальним, оскільки походження цих ситуацій є досить різноманітним. Така різноманітність обумовлюється різними

сферами їх утворення, що, у свою чергу, вказує на несподіваний характер виникнення екстремальних ситуацій, без попередніх ознак, які діють дуже активно, завдають чутливого впливу на банк. Як показує досвід, суб'єкти господарювання, у тому числі і банки, не завжди бувають готові до такого впливу і зазнають суттєвих збитків.

Мінімізувати негативні наслідки екстремальних ситуацій можна було б попереднього вжиття заходів щодо дій банку в умовах екстремальних ситуацій, підготовки персоналу та об'єктів банку, а також прогнозування можливості підтримання роботи банку обмеженими силами та засобами. Важливим тут буде вивчення дій персоналу банку щодо забезпечення власної безпеки та банківської діяльності в різних видах екстремальних ситуацій.

Терміни і поняття

Види екстремальних ситуацій
Група управління діяльністю банку в екстремальних умовах
Евакуаційні команди
Екстремальні ситуації
Загроза підриву або підрив вибухового пристрою в установах або на території банків
Замахи на життя та здоров'я працівників банку
Застосування психотехнічних комунікацій
Застосування психотропних речовин
Заходи з попередження та уникнення екстремальних ситуацій у банку
Захоплення заручників
Землетруси
Зомбіювання
Ідеологічні диверсії
Команди рятівників
План дій банку на випадок загрози та виникнення екстремальних ситуацій
Повені
Пожежі
Психологічні диверсії
Саботаж
Система сповіщення
Терористичний акт
Техногенні аварії
Чутки

Шантаж

Питання для перевірки знань

1. Чим зумовлюються екстремальні ситуації, що виникають у банку?
2. Які органи створюються у банку на випадок виникнення екстремальної ситуації?
3. У яких випадках під час дії екстремальних ситуацій управління діяльністю банку переноситься до однієї з його філій?
4. Що ви маєте засвоїти передусім у разі, якщо вас призначено до складу евакуаційної команди?
5. Яка різниця між командами рятівників та евакуаційними командами?
6. Які дії банківських працівників ви можете вважати правильними під час евакуації з банку?
7. На що насамперед спрямовані ідеологічні диверсії?
8. За яких умов найбільш імовірне виникнення чуток у банку?
9. Що покладається в основу ситуації шантажу?
10. Якою має бути поведінка людини у разі ситуації шантажу, коли вона точно знає, що факту, яким її компрометують, не було, але у неї не має можливості це довести?
11. Чи можуть терористичні акти мати економічне підґрунтя?
12. Які дії працівника банку будуть найбільш виправданими у разі виявлення ним у робочому приміщені незнайомого предмета, поява якого в даному приміщенні нічим не обґрунтована?
13. У чому полягають обов'язки працівника банку щодо протидії екстремальним ситуаціям, пов'язаним із виникненням пожеж?
14. За яких умов у банку може виникати загроза екстремальної ситуації, пов'язаної з хімічними чи радіаційними уражаючими факторами?
15. Яка поведінка людини, котра потрапила в заручники, може бути найбільш виправданою?

Завдання для індивідуальної роботи

1. Ви — керівник установи банку. Одного разу по радіо і телебаченню оголосили про те, що в регіоні, де розташований ваш банк, передбачаються сильні зливи, і тому існує загроза затоплення значної частини території. Як ви гадаєте, чи слід

звертати увагу на це попередження і яких дій слід вам вжити, щоб захистити майно банку у разі настання екстремальної ситуації від повені?

2. Ви — керівник установи банку. Одного разу на банк було здійснено напад трьох осіб, які захопили в заручники працівників каси та клієнтів, які на той час перебували в касі. Терористи вимагали 1 млн грн готівкою, у разі, якщо їх вимоги не будуть задоволені обіцяли стратити заручників та підірвати приміщення банку. Зразу ж після цього повідомлення ви віддали розпорядження про евакуацію персоналу банку та намагалися провести переговори з нападниками, але у вас нічого не вийшло ви ще більше їх розлютили. Як ви гадаєте, чи правильно ви діяли в даній ситуації? Що ви будете робити далі, щоб звільнити заручників і не допустити підриву приміщення банку?

3. Вас призначено до складу команди рятівників на випадок виникнення у банку екстремальної ситуації. Одного разу керівник підрозділу безпеки зробив спробу провести тренування вашої команди. Але всі працівники, які входили до складу команди, зазначили, що вони досить добре знають свої обов'язки і порядок дій у разі настання екстремальної ситуації. Керівник підрозділу безпеки погодився з такою пропозицією, а вам як новому члену команди запропонував вивчити свої обов'язки і порядок дій самостійно. Що вам необхідно у цьому зв'язку засвоїти і як ви будете здійснювати опанування своїх обов'язків?

Література для поглибленого вивчення

1. *Белоножкин В. И.* Информационные аспекты противодействия терроризму / Белоножкин В. И., Остапенко Г. А. — М. : Горячая линия — Телеком, 2009. — 112 с.

2. *Вишняков Я. Д.* Основы противодействия терроризму / Я. Д. Вишняков, Г. А. Бондаренко — М. : Академия, 2006. — 240 с.

3. *Зубок М. І.* Бізнес в екстремальних умовах : навч.-метод. посіб. / Зубок М. І. — К. : КНТЕУ, 2008. — 183 с.

4. *Ильин А. А.* Школа выживания в условиях экономического кризиса / Ильин А. А. — М. : Эксмо-Пресс, 2001. — 384 с.

5. *Ильин А. А.* Школа выживания при авариях и стихийных бедствиях / Ильин А. А. — М. : Эксмо-Пресс, 2001. — 194 с.

Висновки

Організація банківської безпеки — трудомісткий, багатогранний процес, який торкається практично всіх сторін діяльності банку. Ефективність заходів безпеки досягається лише тоді, коли вони проводяться в комплексі з маркетинговою діяльністю, відповідними кадровою політикою та методами управління. Рекомендації з безпеки повинні враховуватися при розробленні банківських технологій та методик проведення операцій. Персонал банку має з довірою ставитися до заходів безпеки, сприяти їх проведенню та особисто виконувати всі норми і правила, установлені в банку.

Водночас безпека банку — це завдання не тільки підрозділу безпеки. Кожен підрозділ і працівник банку, реалізуючи відповідні технології та виконуючи свої обов'язки відповідно до вимог законодавчих та нормативних актів, є гарантом безпеки банку. Більше того, заходи безпеки – це не тимчасові вимоги, не чергова кампанія. В умовах ринку і конкуренції це один із способів існування комерційної структури. З першими успіхами і невдачами рано чи пізно до кожного бізнесмена приходить розуміння необхідності самостійного забезпечення захисту своїх прав, інтересів, власності, своєї діяльності.

Разом з тим технології безпеки не можуть бути стандартними як для кожного виду бізнесу, так і безпосередньо в кожному конкретному бізнесі. Вони мають розвиватися, удосконалюватися разом із розвитком технологій виробництва і комерційної діяльності, завжди бути адекватними умовам, в яких здійснює свою діяльність той чи той суб'єкт.

Виходячи з цього і сьогоднішні наші знання — це вже історія для завтра, ми маємо постійно шукати нові форми та прийоми забезпечення безпеки підприємницької діяльності. А враховуючи, що основними тенденціями в бізнесі XI ст. буде широка його інформатизація та активний вплив на нього людського фактору, можна передбачати, що основні зусилля безпеки мають бути зосереджені якраз на розвитку інформаційних технологій безпеки та удосконаленні систем

кадрової безпеки. У зв'язку з наведеним виникає гостра потреба в теоретичних розробках і практичних напрацюваннях нових підходів забезпечення безпеки бізнесу взагалі і банківського зокрема, підготовці професійних кадрів, здатних на високому рівні з необхідним рівнем якості забезпечувати безпеку підприємств і банків. Знання теоретичних закономірностей, вітчизняного та іноземного досвіду організації безпеки бізнесу, методик її забезпечення безпосередньо у структурах підприємництва є необхідною умовою формування сучасного фахівця — професіонала будь-якої сфери діяльності.

Словник основних термінів

Банківська таємниця — це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам під час надання 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 — лише її утримувачі та суб'єкт, зобов'язаний обмежувати доступ до неї.

Безпека банківської діяльності — стан стійкої життєдіяльності, за якого забезпечується реалізація мети банку та основних його інтересів, захист від внутрішніх і зовнішніх дестабілізувальних факторів незалежно від умов функціонування.

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

Внутрішньооб'єктовий режим банку — установлений у певній установі банку порядок виконання правил внутрішнього розпорядку роботи, спрямований на забезпечення безпеки банківського виробництва, схоронності матеріальних цінностей і інформаційних ресурсів, захист персоналу і відвідувачів банку.

Дезінформація — поширення в інформаційному середовищі викривлених або неправдивих відомостей з метою введення в оману конкурентів, кримінальних елементів, інших суб'єктів, що загрожують банку, стосовно істинних намірів діяльності банку.

Дестабілізувальні фактори — певні процеси, явища, поведінка, які своєю дією здатні змінювати ситуацію, формуючи несприятливі умови для певної діяльності (у даному разі банківської), визначаючи її характер або окремі риси і зумовлюючи відповідні відхилення від планових нормативів та стандартів.

Евакуаційні команди — спеціально сформовані з працівників банку групи, призначені для організованого проведення евакуації цінностей та персоналу банку в період безпосередньої загрози виникнення екстремальної ситуації. Склад команди визначається з розрахунку по дві особи для

евакуації кожного з банківських підрозділів та від 10 до 30 осіб — для евакуації цінностей та документів.

Економічна безпека банку — стан, за якого забезпечується економічний розвиток і стабільність діяльності банку, гарантований захист його ресурсів, здатність адекватно і без суттєвих втрат реагувати на зміни внутрішньої і зовнішньої ситуації.

Екстремальні ситуації в бізнесі — події, явища природного, економічного, соціального чи якогось іншого походження або результат діяльності суб'єктів чи певних процесів, які за своєю інтенсивністю, масштабами поширення, тривалістю, складністю і небезпечністю виходять за межі звичайних умов існування, можуть уражати людей, об'єкти та суб'єктів економіки або довкілля і вимагають для їх подолання найвищої концентрації фізичних, духовних, фінансових, матеріальних та інших зусиль і ресурсів.

Забезпечення фінансової безпеки банку — сукупність заходів, спрямованих на формування фінансових ресурсів, запобігання збитків та ефективне використання коштів у його фінансово-господарській діяльності.

Загроза банківській діяльності — потенційні чи реальні дії певних суб'єктів, здатні завдати конкретному банку матеріальної або моральної (шкодити іміджу банку) шкоди.

Застосування психотехнічних комунікацій — вплив на людину через використання її переконань, звичок, слабких рис характеру, особливостей психохарактеристик колективу для формування необхідної позиції чи поведінки (людини, колективу).

Застосування психотропних речовин — штучне (на хімічному чи біологічному рівні) обмеження інтелектуальних можливостей людини з метою примушення її до несвідомого виконання необхідних суб'єктам психологічних диверсій дій.

Знищення інформації — приведення носіїв інформації (документів, електронних носіїв, аудіо-, відеозаписів та інших носіїв, що мають матеріальний характер) у стан, непридатний для їх подальшого використання або ж неможливості використання інформації, яка на них зберігалась.

Зомбіювання — штучне введення людини у стан трансу і програмування її поведінки в інтересах досягнення відповідної мети, яку ставлять собі суб'єкти психологічної диверсії.

Ідеологічні диверсії — нагнітання моральної і психологічної обстановки навколо банку або в його колективах з метою

створення високого емоційного напруження в роботі і поведінці персоналу, зниження довіри клієнтів і партнерів до банку, провокування його керівництва до непродуманих рішень і дій.

Інформаційна безпека банку — стан, за якого здійснюється ефективне інформаційне забезпечення його діяльності, гарантований захист інформаційного ресурсу та належна протидія негативному інформаційному впливу.

Інформаційний аудит — інформаційне обстеження сфери інформаційної уваги чи певних об'єктів (об'єкта) з метою отримання, вивчення й оцінювання необхідної суб'єкту аудиту (у даному разі банку) інформації. Основними технологіями інформаційного аудиту є: пошук та вивчення інформації про конкретний об'єкт безпосередньо на самому об'єкті; пошук та вивчення інформації про конкретний об'єкт через його зв'язки (ділові, комерційні, організаційні та ін.); пошук та вивчення інформації про конкретний об'єкт через спеціальне обстеження відповідної сфери інформаційної уваги банку.

Інформаційний вплив — 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.

Інформаційний канал — сукупність джерел інформації, засобів та методів їх подання до споживачів інформаційних продуктів.

Інформаційний моніторинг — контроль надходження інформації в інформаційне середовище з метою виявлення важливої та цінної інформації і її використання для забезпечення діяльності банку. Технологіями, які використовуються у процесі інформаційного моніторингу, є: контроль інформації, що надходить в інформаційне середовище банку за визначеними ознаками та індикаторами; контроль інформації, яка надходить в інформаційне середовище банку з певних джерел; суцільний контроль інформації, що з'являється в інформаційному середовищі банку.

Інформаційний ресурс банку — сукупність інформації, яка перебуває у власності чи розпорядженні банку і використовується ним для забезпечення його діяльності.

Інформаційні загрози — потенційно можливі або реальні дії суб'єктів загроз, пов'язані з використанням інформаційних

технологій для забезпечення впливу на певних суб'єктів чи конкретних осіб.

Інформаційні ризики — 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, а також можливість поширення в інформаційному середовищі невигідної, негативної чи небезпечної для суб'єкта господарювання інформації, що в кінцевому підсумку може завдавати йому збитків, матеріальної або моральної шкоди.

Інформаційно-аналітична робота — діяльність, пов'язана зі збором і обробкою відкритої інформації, формуванням відповідних інформаційних документів та наданням їх керівництву банку.

Інформація банку — документовані чи оголошені відомості, які можуть міститися на різноманітних носіях, та перебувають у розпорядженні банку і відтворюють (характеризують) події та явища (діяльність), що відбуваються в банку.

Команди рятівників — спеціально сформовані з працівників банку групи, призначені для пошуку, надання допомоги та евакуації з осередків ураження чи інших небезпечних місць осіб, які постраждали від дії уражаючих факторів екстремальних ситуацій. В установі банку можуть утворюватись одна—дві команди у складі 10—15 осіб кожна.

Комерційна таємниця — 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 і 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.

Контрпропаганда — інформаційна реакція банку на комунікативні дії конкурентів чи інших суб'єктів, якими вони прагнуть забезпечити свій вплив на інформаційне середовище ринку банківських послуг усупереч інтересам банку;

Конфіденційна інформація — 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.

Конфлікт — зіткнення протилежних інтересів, думок, оцінок окремих людей або груп людей у процесі їх спільної діяльності чи виконання однієї (близької за змістом) роботи.

Критерій економічної безпеки — оцінка економічного стану банку. Критеріальна оцінка економічної безпеки базується на оцінках: ресурсного потенціалу банку і можливостей його розвитку; рівня ефективності використання ресурсів; рівня можливостей банку протистояти загрозам його економічній безпеці та самостійно ліквідовувати їх; конкурентоспроможності банку; цілісності та масштабів структури банку; ефективності кадрової політики банку.

Модифікація інформації — 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 вимагає суттєвого уточнення та аналізу.

Недобросовісна конкуренція — будь-які дії у конкуренції, що суперечать торговельним та іншим чесним звичаям у господарській діяльності.

Незаконне використання інформації — 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 їх службовою чи іншою діяльністю.

Об'єкт інформації — установа, організація, виробництво, захід, у яких зосереджена необхідна банку інформація.

Охорона банків — комплекс організаційних та спеціальних заходів, направлених на обмеження доступу, захист території, приміщень і об'єктів банку від протиправних посягань.

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 і програмно-технічних засобів, які визначають архітектуру системи захисту, та 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.

Проблемний кредит — заборгованість за банківськими

кредитами, за якими своєчасно не проведено одного чи більше платежів та внаслідок інших обставин виникають підстави для сумніву щодо повернення кредиту взагалі.

Промислове шпигунство — діяльність, в основу якої покладено сукупність спеціальних заходів, спрямованих на отримання інформації з обмеженим доступом, яка охороняється певним суб'єктом.

Пропаганда — активне поширення в інформаційному середовищі інформації про досягнення, переваги, масштаби діяльності банку, вигідність взаємовідносин з ним у різних напрямах його діяльності.

Пропускний режим — установлений у банку відповідний порядок допуску працівників, клієнтів і відвідувачів банку на його територію, переміщення за межі банку матеріальних цінностей.

Психологічні диверсії — активне використання засобів комунікації, механізмів соціально-психологічного впливу, медичних препаратів та інших засобів з метою підпорядкування дій людини суб'єктам зазначених диверсій або створення сприятливих умов для реалізації їхніх задумів і рішень.

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

Саботаж — усілякі усвідомлені дії, які явно призводять до порушення і дезорганізації встановленого порядку, норм і правил роботи банку.

Система безпеки банку — сукупність заходів, технологій їх виконання, сил і засобів безпеки, спрямованих на формування здатності банку протистояти різноманітним загрозам його діяльності.

Система захисту інформації банку — 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.

Спеціальні інформаційні операції — комплекс спеціальних інформаційних заходів, які проводяться протягом конкретно визначеного часу в інформаційному середовищі банку з метою

формування (підтримання, відновлення) його позитивного іміджу, захисту від негативного інформаційного впливу та дезорієнтації конкурентів і кримінальних елементів, які є суб'єктами загроз банку.

Сфера інформаційної уваги банку — сегмент інформаційного середовища банку, в якому він забезпечує стратегічні, тактичні та оперативні інформаційні інтереси і завдання.

Таємна інформація — відомості, що становлять державну та іншу передбачену законом таємницю (банківську, комерційну, військову, лікарську та ін.), розголошення якої завдає шкоди особі, суспільству, державі.

Територія банку — у відповідний спосіб обладнана ділянка місцевості з розташованими на ній спорудами, сховищами, іншими будівлями, необхідними для забезпечення його роботи.

Терористичний акт — загроза підриву або підрив вибухового пристрою, захоплення заручників, руйнування споруд та об'єктів інфраструктури, погроза насильством і насильницькі дії аж до знищення окремих фізичних осіб.

Технічна укріпленість — спеціальне конструювання, обладнання і оснащення споруд, приміщень і території банківських об'єктів, спрямовані на забезпечення їх захисту від несанкціонованого проникнення і злому.

Управління кадровою безпекою банку — цілеспрямований вплив органів управління банку на його стан та діяльність за допомогою заходів кадрової роботи і режиму з метою формування і підтримання високого рівня його безпеки на ринку банківських послуг.

Фінансова безпека банку — стан фінансових ресурсів банку, за якого забезпечується його ефективна (прибуткова) діяльність, захист фінансових інтересів та здатність зберігати свої фінансові можливості під впливом різного роду небезпек і загроз.

Чутки — усна інформація з невизначеним ступенем достовірності, що стихійно поширюється в інформаційному середовищі банку з метою захисту його інтересів.

Шантаж — залякування через загрози оприлюднення компрометуючих фактів чи матеріалів, які ганьблять певну особу з метою примушення її до відповідних дій чи поведінки.

Шахрайство — зловживання довірою, обман з метою введення власника матеріальних цінностей або коштів в оману і на тій основі добровільне передання ним своєї власності шахраям.

Список використаних джерел

Основні

1. *Адамик Б. П.* Інформаційні технології у банківській сфері : навч. посіб. / Адамик Б. П., Литвин І. С., Ткачук В. О. — К. : Знання, 2008. — 351 с.

2. *Бєгун В. І.* Інформаційна безпека : навч. посіб. / Бегун В. І. — К.: КНЕУ, 2008. — 280 с.

3. *Вишняков Я. Д.* Основы противодействия терроризму / Я. Д. Вишняков, Г. А. Бондаренко. — М. : Академия, 2006. — 240 с.

4. Господарський Кодекс України від 16.01.2003 р. — № 436-IV із змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

5. Действия при угрозах и осуществлении террористических актов : памятка для руководителей и работников организаций и производственных объектов / авт.-сост. С. В. Петров ; ред. А. М. Меламед. — М. : Изд-во НЦ ЭНАС, 2006. — 32 с.

6. *Диба М. І.* Тимчасова адміністрація та ліквідація банків : навч. посібник / Диба М. І., Раєвський К. Є., Зубок М. І. — К. : КНЕУ, 2008. — 192 с.

7. *Зубок М.* Державний реєстр як джерело інформації про суб'єкта господарювання / М. Зубок, Р. Двикалюк // Бизнес и безопасность. — 2010. — № 3. — С. 24—25.

8. *Зубок М. І.* Безпека банків : навч. посіб. / Зубок М. І. — К. : КНТЕУ, 2002. — 306 с.

9. *Зубок М. І.* Безпека банківської діяльності : навч. посіб. / Зубок М. І. — К. : КНЕУ, 2002. — 190 с.

10. *Зубок М. І.* Безпека бізнесу : навчальний посібник у схемах і таблицях / Зубок М. І., Позднишев Є. В., Яременко С. М. — К. : КНЕУ, 2008. — 480 с.

11. *Зубок М. І.* Бізнес в екстремальних умовах : навч.-метод. посіб. / Зубок М. І. — К. : КНТЕУ, 2008. — 183 с.

12. *Зубок М. І.* Захист підприємницької діяльності від недобросовісної конкуренції і промислового шпигунства : навч.-метод. посіб. / Зубок М. І. — К. : КНТЕУ, 2005. —

13. *Зубок М. І.* Інформаційна безпека : навч. посіб. для студ. вищ. навч. закл. / Зубок М. І. — К. : КНТЕУ, 2005. — 133 с.

14. *Зубок М. І.* Інформаційно-аналітичне забезпечення підприємницької діяльності : навч. посіб. для студ. вищ. навч. закл. / Зубок М. І. — К. : КНТЕУ, 2007. — 156 с.

15. *Зубок М. І.* Основи безпеки комерційної діяльності підприємств та банків : навч.-метод. посіб. / Зубок М. І. — К. : КНТЕУ, 2005. — 201 с.

16. *Зубок М. І.* Охорона та охоронна діяльність : навч. посіб. для студ. вищ. навч. закл. / Зубок М. І. — К. : КНТЕУ, 2006. — 172 с.

17. Информационно-психологическая безопасность в эпоху глобализации : учеб. пособ. / В. М. Петрик, В. В. Остроухов, А. А. Штоквиш [и др.]; под ред. В.В. Остроухова — К. : ГУИКТ, 2008. — 544 с.

18. Інструкція з організації перевезення валютних цінностей та інкасації коштів у банківських установах в Україні // Постанова Національного банку України від 14.02.2007 р. № 45 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

19. Інструкція про касові операції в банках України // Постанова Національного банку України від 14.08.2003 р. № 337 із змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

20. Інструкція про порядок організації та здійснення валютно-обмінних операцій на території України // Постанова Національного банку України від 12.12.2002 р. № 502 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

21. Інструкція про порядок регулювання діяльності банків в Україні // Постанова Національного банку України від 28.08.2001 р. № 368 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

22. Кодекс законів про працю України від 10.12.1971 р. № 322-VIII / Верховна Рада України // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

23. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8073-X із змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

24. Конституція України // Закон України від від 28.06. 1996 р. № 254к/96-ВР із змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

25. Концепція економічної безпеки. — К. : Логос, 1999. — 56 с.

26. *Кормич Б. А.* Інформаційна безпека: організаційно-правові основи / Кормич Б. А. — К. : Кондор, 2004. — 384 с.

27. Кримінальний кодекс України від 05.04.2001 р. № 2341-III із змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

28. *Курило В. І.* Правові засади охоронної діяльності : навч. посіб. / Курило В. І. — К. : Кондор, 2005. — 182 с.

29. Ліцензійні умови провадження господарської діяльності з надання послуг, пов'язаних з охороною державної та іншої власності, надання послуг з охорони громадян // Наказ Міністерства внутрішніх

справ України від 01.12.2009 р. № 505 // [Електронний ресурс]. — Режим доступу: http://www.mvs.gov.ua.

30. *Минаев Г. А.* Безопасность организации / Минаев Г.А. — М. : Логос, 2008. — 368 с.

31. *Міщенко В. І.* Банківські операції / Міщенко В. І., Словянська Н. Г., Коренєва О. Г. — К. : Знання, 2007. — 796 с.

32. *Павлов А. В.* Основы организации безопасности банков : учеб. пособие / Павлов А. В. — М. : Академия, 2010. — 128 с.

33. *Палюк В. І.* Особливості розкриття банківської таємниці судами / В. І. Палюк — К.: Юстініан, 2009. — 384 с.

34. Паризька конвенція про охорону промислової власності від 20 березня 1883 р. (переглянута у Брюсселі 14 грудня 1900 р., у Вашингтоні 2 червня 1911 р., у Гаазі 6 листопада 1925 р., у Лондоні 2 червня 1934 р., у Лісабоні 31 жовтня 1958 р., у Стокгольмі 14 липня 1967 р., змінена 2 жовтня 1979 р., підтверджена у 1992 р.

35. Положення про вимоги щодо технічного стану та організації охорони приміщень банків України // Постанова Національного банку України від 29.12.2007 р. № 493 // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

36. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем // Постанова Національного банку України від 25.09.2007 р. № 348 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

37. Положення про застосування Національним банком України заходів впливу за порушення банківського законодавства // Постанова Національного банку України від 28.08.2001 р. № 369 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

38. Положення про здійснення банками фінансового моніторингу // Постанова Національного банку України від 14.05.2003 р. № 189 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

39. Положення про здійснення уповноваженими банками операцій з банківськими металами // Постанова Національного банку України від 06.08.2003 р. № 325 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

40. Положення про порядок здійснення банками операцій з векселями в національній валюті на території України // Постанова Національного банку України від 16.12.2002 р. № 508 із змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

41. Положення про порядок здійснення операцій з чеками в іноземній валюті на території України // Постанова Національного банку України від 29.12.2000 р. № 520 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua

42. Положення про порядок здійснення уповноваженими банками операцій за документарними акредитивами в розрахунках за

зовнішньоекономічними операціями // Постанова Національного банку України від 03.12.2003 р. № 514 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

43. Положення про порядок реєстрації випуску акцій // Рішення Державної комісії з цінних паперів та фондового ринку від 26.04.2007 р. № 942 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

44. Положення про порядок формування та використання резерву для відшкодування можливих втрат за кредитними операціями банків // Постанова Національного банку України від 06.07.2000 р. № 279 із змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

45. Правила визначення платіжності та обміну банкнот і монет Національного банку України // Постанова Національного банку України від 17.11.2004 р. № 547 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

46. Правила зберігання, захисту, використання та розкриття банківської таємниці // Постанова Національного банку України від 14.07.2006 р. № 267 // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

47. *Примостка Л. О.* Фінансовий менеджмент у банку : підручник. — 2-ге вид., доп. перероб. / Примостка Л. О. — К.: КНЕУ, 2004. — 468 с.

48. Про акціонерні товариства // Закон України від 17.092008 р. № 514-VI зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

49. Про банки і банківську діяльність // Закон України від 07.12.2000 р. — № 2121-III зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

50. Про встановлення мінімального розміру регулятивного капіталу банків у гривнях на 2009 рік // Постанова Правління Національного банку України від 04.03.2009 р. № 116 // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

51. Про господарські товариства України // Закон України від 19.09.1991 р. — № 1576-XII зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

52. Про забезпечення вимог кредиторів та реєстрацію обтяжень // Закон України від 18.11.2003 р. № 1255-IV зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

53. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму із змінами і доповненнями // Закон України від 28.11.02 р. № 249–IV із змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

54. Про заставу // Закон України від 02.10.1992 р. 2654-XII // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

55. Про затвердження Випуску 1 «Професії працівників, що є загальними для всіх видів економічної діяльності» Довідника кваліфікаційних характеристик професій працівників // Наказ Міністерства праці та соціальної політики України від 29.12.2004 р. № 336.
56. Про захист від недобросовісної конкуренції // Закон України від 07.06.1996 р. № 236/96-ВР зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
57. Про захист економічної конкуренції // Закон України від 11.01.2001 р. № 2210-III зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
58. Про захист інформації в автоматизованих системах // Закон України від 31.05.2005 р. 2594-IV // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
59. Про здійснення операцій з використанням спеціальних платіжних засобів // Постанова Правління Національного банку України від 30.04.2010 р. № 223 зі змінами та доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
60. Про інформацію // Закон України від 02.10.1992 р. № 2657-XII зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
61. Про Національний банк України // Закон України від 20.05.1999 р. 679-XIV // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
62. Про Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні // Закон України від 10.12.97 р. — № 710/97-ВР зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua
63. Про оподаткування прибутку підприємств // Закон України від 28.12.1994 р. № 334/94-ВР зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
64. Про організацію формування та обігу кредитних історій // Закон України від 23.06.2005 р. 2704-IV зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
65. Про основи національної безпеки України // Закон України від 19.06.2003 р. № 964-IV зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
66. Про систему валютного регулювання і валютного контролю // Декрет Кабінету Міністрів України від 19.02.1993 р. № 15-93 зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
67. Про цінні операції та фондовий ринок // Закон України від 23.02.2006 р. 3480-IV зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
68. Цивільний кодекс України від 16.01.2003 р. № 435-IV / Верховна Рада України // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

69. *Яременко С. М.* Безпека банківської діяльності. Збірник тестів, ситуаційних та комплексних кваліфікаційних завдань : навч. посіб. / С. М. Яременко. — К. : КНЕУ, 2008. — 192 с.
70. *Яременко С. М.* Забезпечення економічної безпеки діяльності банків: дис. … канд. економ. наук : 08.00.08 / С. Яременко. — К., 2010. — 247 с.

Додаткові

71. Актуальні проблеми забезпечення економічної безпеки України: зб. тез доповідей ІІ наук.-практ. семінару з міжнародною участю, 16–18 грудня 2008 р. / Терноп. нац. екон. ун-т. — Тернопіль : Вектор, 2008. — 276 с.
72. *Ареф'єва О. В.* Планування економічної безпеки підприємств / О. В. Ареф'єва, Т. Б. Кузенко. — К. : Вид-во Європ. ун-ту, 2004. — 170 с.
73. Банк выдал бизнесмену почти полтора миллиона фальшивых гривен [Електронний ресурс]. — Режим доступу: http://www.4post.com.ua/criminal/138426.htm/.
74. *Баяндин Н. И.* Технологии безопасности бизнеса / Баяндин Н. И. — М. : Юристъ, 2002. — 320 с.
75. *Берлач А. І.* Безпека бізнесу: навч. посіб. / Берлач А. І. — К. : Університет «Україна», 2007. — 280 с.
76. *Боган К.* Бизнес-разведка / К. Боган, М. Инглиш. — М. : Вершина, 2006. — 368 с.
77. *Богомолов В. А.* Экономическая безопасность: учебное пособие для студентов ВУЗов, обучающихся по специальностям экономики и управления / Богомолов В. А. — М. : ЮНИТИ-ДАНА, 2009 — 295 с.
78. *Бондарчук Ю. В.* Безпека бізнесу: організаційно-правові основи. : наук.-практ. посіб. / Ю. В. Бондарчук, А. І. Марущак. — К. : Скіф, 2008. — 369 с.
79. В Киеве снова грабят банки [Електронний ресурс]. — Режим доступу: http://www.utro.ua/ru/proisshestviya/v_kieve_snova_grabyat_banki1246976260.
80. В Украине участились махинации с кредитами [Електронний ресурс]. — Режим доступу: www.vecherniy.kharkov.ua.
81. *Ваків В.* «Проблемні» кредити. Обрій піб. № 40(98), 2002.
82. *Вахненко Т. П.* Кредитно-боргова експансія банків та методи її стимулювання / Вахненко Т.П. — К. : ІЕП НАНУ, 2008.
83. Великий тлумачний словник сучасної української мови (з дод. і допов.) / [уклад. В. Бусел]. — К. : Ірпінь, 2005. — 1728 с.
84. *Гамза В. А.* Безопасность банковской деятельности / В. А. Гамза, И. Б. Ткачук. — М. : Маркет, 2010. — 408 с.
85. *Гапоненко В. Ф.* Экономическая безопасность предприятий / Гапоненко В.Ф., Беспалько А. А., Власков А. С. — М. : Издательство «Ось-89», 2007. — 208 с.

86. *Гордієнко К. Д.* Прийняття на роботу: співбесіда, анкетування : практ. посіб. / Гордієнко К. Д. — К. : КНТ, 2006. — 184 с.

87. *Гришина Н. В.* Комплексная система защиты информации на предприятии : учеб. пособ. / Гришина Н. В. — М. : ФОРУМ, 2009. — 240 с.

88. *Демин Ю. М.* Управление кадрами в кризисных ситуациях / Демин Ю. М. — СПб. : Питер, 2004. — 219 с.

89. *Деревицкий А. А.* Коммерческая разведка / Деревицкий А. А. — СПб. : Питер, 2006. — 208 с.

90. *Дзлиев М. И.* Предпринимателю. Как избежать опасности / Дзлиев М. И. — М. : Экономика, 2006. — 349 с.

91. *Доля Л.* Стан боротьби зі злочинністю у банківській системі України: шляхи нейтралізації та протидії [Електронний ресурс]. — Режим доступу: http://mndc.naiau.kiev.ua.

92. *Донець Л. І.* Економічна безпека підприємства. / Л. Донець, Н. Ващенко. — К. : Центр учбової літератури, 2008. — 240 с.

93. *Доронин А. И.* Бизнес-разведка / Доронин А. И. — М. : Ось-89, 2007. — 528 с.

94. *Дудихин В. В.* Конкурентная разведка в Интернете / В. В. Дудихин, О. В. Дудихина. — М. : NT Press, 2004. — 229 с.

95. Економічна безпека / [Мельник П., Терангул Л. та ін.] ; за ред. З. С. Варналія. — К. : Знання, 2009. — 647 с.

96. *Зайцев И.* Рейдерство в Украине. Как защитить предприятие / И. Зайцев, В. Кульпинов. — К. : Тандем, 2008. — 160 с.

97. *Захаров О. Ю.* Обеспечение комплексной безопасности предпринимательской деятельности / Захаров О. Ю. — М. : АСТ «Астрель», 2008. — 320 с.

98. *Зацеркляний М. М.* Основи економічної безпеки : навч. посіб. / М. Зацеркляний, О. Мельников. — К. : КНТ, 2009. — 337 с.

99. Звіт Національного банку України за 2008 р. / Національний банк України [Електронний ресурс]. — Режим доступу до звіту: http://bank.gov.ua/Publication/an_rep.htm.

100. *Зубок М.* Борги підприємств, банків і протидія їм // Бизнес и безопасность. — 2004. — № 2.

101. *Зубок М. І.* Безпека підприємницької діяльності / М. І. Зубок, Р. М. Зубок. — К. : Істина, 2004. —

102. *Зубок М. І.* Забезпечення безпеки кредитних операцій банків // Бизнес и безопасность. — 2003. — № 3.

103. *Зубок М. І.* Правове регулювання безпеки підприємницької діяльності : навч.-метод. посіб. / Зубок М. І. — К. : КНТЕУ, 2005. — 140 с.

104. *Зубок М. І.* Управління проблемним кредитом / М. І. Зубок, С. М. Яременко // Фінанси, облік і аудит : зб. наук. пр. — К. : КНЕУ, 2007. — № 10. — С. 38—48.

105. *Зубок Н. И.* О бедной охране замолвите слово / Н. И. Зубок, С. Н. Яременко // Бизнес и безопасность. — 2004. — № 4. — С. 8—9.

106. *Зубок Н. И.* Охрана в предпринимательской деятельности / Н. И. Зубок, С. Н. Яременко // Бизнес и безопасность. — 2005. — № 1. — С. 2—3.
107. *Иванов М.* Кадровая безопасность / М. Иванов // Бизнес и безопасность. — 2009. — № 1 (69) — С. 30—38.
108. *Іванюта Т. М.* Економічна безпека підприємства : навч. посіб. для студ. вищ. навч. закл. / Т. М. Іванюта, А. О. Заїнчковський. — К. : Центр учб. л-ри, 2009. — 254 с.
109. *Камлик М. І.* Економічна безпека підприємницької діяльності. Економіко-правовий аспект / М. І. Камлик — К. : Атіка, 2005. — 431 с.
110. *Кириченко О.* Банківський менеджмент / О. Кириченко — К. : Знання–Прес, 2002.
111. Кількість шахрайства з банківськими картками росте // Економічна правда. — 2010. — 14 трав.
112. *Кован С.* Практикум по финансовому оздоровлению неплатежеспособных предприятий / С. Кован, В. Мерзлова — М. : Финансы и статистика, 2005. — 208 с.
113. *Ковров А. В.* Предатели: «пятая колона» в организации / Ковров А. В. — М. : Арсин, 1999. — 120 с.
114. *Коноплева И. А.* Управление безопасностью и безопасность бизнеса: учеб. пособ. для вузов / И. Коноплева, И. Богданов. — М. : ИНФРА-М, 2008. — 448 с. — (Высшее образование).
115. *Корнеев И. К.* Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов. — М. : Проспект, 2008. — 336 с.
116. Криза збільшить тіньову економіку до рівня ВВП? [Електронний ресурс]. — Режим доступу: http://www.epravda.com.ua/publications/ 499bd4b24a43f/.
117. *Кузнецов И. Н.* Бизнес-безопасность / Кузнецов И. Н. — М. : Дашков и К, 2010. — 416 с.
118. *Кузнецов Н. И.* Учебник по информационно-аналитической работе / Кузнецов Н. И. — М. : Яуза, 2001. — 320 с.
119. *Магура М. И.* Поиск и отбор персонала / М. И. Магура. — М. : Интелсинтез, 1997. — 79 с.
120. МВС: Міліція викрила майже півтора тисячі злочинів безпосередньо в банках [Електронний ресурс]. — Режим доступу: http://news.yurist-online.com/news/.... /2809/.
121. МВС: Через кризу в Україні збільшується кількість економічних злочинів [Електронний ресурс]. — Режим доступу: http://novynar.com.ua/politics/46020.
122. Моніторинг геоекономічних змін та індикаторів економічної безпеки. Національний інститут проблем міжнародної безпеки [Електронний ресурс] / А. І. Сухоруков, Т. П. Крушельницька, В. О. Шевчук, В. Г. Савченко. — Режим доступу: http://www.niisp.gov.ua/monitoring/economy/ monitor-geoeconomic-0803.pdf.

123. *Мэй А.* Скрытое управление сознанием человека / Мэй А. — СПб. : Прайм-Еврознак, 2007. — 96 с.
124. На рынке ценных бумаг в 2008 г. выявлено 34 преступления [Електронний ресурс]. — Режим доступу: www.rba.ua.
125. НБУ рассказал как работать с заемщиками // Сегодня. — 2009. — 13 авг.
126. *Нежданов И. Ю.* Аналитическая разведка для бизнеса / Нежданов И. Ю. — М. : Ось-89, 2008. — 336 с.

127. *Нездоля А. И.* Украина третьего тысячелетия: Союз демократических сил / Нездоля А. И. — Донецк : Каштан, 2005. — 459 с.
128. *Низенко, Е. І.* Забезпечення інформаційної безпеки підприємництва : навч. посібник / Е. І. Низенко, В. П. Каленяк — К. : МАУП, 2006. — 134 с.
129. *Ніколаюк С. І.* Безпека суб'єктів підприємницької діяльності : Курс лекцій / С. І. Ніколаюк, Д. Й. Никифорчук. — К. : КНТ, 2005. — 317 с.
130. *Новак Б. В.* Бизнес в России — руководство по технике безопасности. — СПб. : Питер, 2008. — 240 с.
131. *Одинцов А. А.* Экономическая и информационная безопасность предпринимательства : учеб. пособие для вузов / Одинцов А. А. — М. : Академия, 2006. — 336 с.
132. *Орлов П. І.* Основи економічної безпеки фірми : навч. посіб. / П. І. Орлов, В. Є. Духов — Х. : Прометей-Прес, 2004. — 284 с.
133. *Ортинський В. Л.* Економічна безпека підприємств, організацій та установ : навч. посіб. / Ортинський В. Л., Керницький І. С., Живко З. Б. — К.: Правова єдність, 2009. — 544 с.
134. Офіційний сайт Асоціації українських банків [Електронний ресурс]. — Режим доступу: aub.org.ua.
135. Офіційний сайт Державного комітету статистики України [Електронний ресурс]. — Режим доступу: www.ukrstat.gov.ua.
136. Офіційний сайт Міністерства внутрішніх справ України [Електронний ресурс]. — Режим доступу: http://www.mvs.gov.ua.
137. Офіційний сайт Міністерства економіки України [Електронний ресурс]. — Режим доступу: www.me.gov.ua.
138. Офіційний сайт Міністерства фінансів України [Електронний ресурс]. — Режим доступу: www.minfin.gov.ua.
139. Офіційний сайт Національного банку України [Електронний ресурс]. — Режим доступу: www.bank.gov.ua.
140. Офіційний сайт Рахункової палати України [Електронний ресурс]. — Режим доступу: www.ac-rada.gov.ua
141. *Панарин И. Н.* Первая мировая информационная война. Развал СССР / Панарин И. Н. — М. : Питер, 2010. — 256 с.
142. *Перерва П. Г.* Трудоустройство без проблем (искусство самомаркетинга) / Перерва П. Г. — Харьков : Фактор, 2009. — 473 с.

143. Повідомлення прес-служби МВС [Електронний ресурс]. — Режим доступу: http://www.kmu.gov.ua.
144. Повідомлення прес-служби МВС [Електронний ресурс]. — Режим доступу: http://news.if.ua.
145. *Поздняков Е. Н.* Защита объектов / Поздняков Е. Н. — М. : Концерн «Банковский Деловой Центр», 1997. — 224 с.
146. *Потапов Б.* Рівень захисту банків загрозливий / Б. Потапов // Газета плюс. — 2008. № 45 (185) — С. 18—31.
147. *Почепцов Г. Г.* Информация и дезинформация / Почепцов Г. Г. — К. : Эльга, 2001. — 252 с.
148. *Прескотт Д. Е.* Конкурентная разведка: уроки из окопов / Д. Е. Прескотт, С. Х. Миллер. — М. : Альпина Бизнес Букс, 2004. — 335 с.
149. Прес-реліз Адвокатської компанії «Агеев, Бережной и партнеры» від 21.03.02 р. «Дело Бориса Фельдмана и банка «Славянский».
150. *Прибутько П. С.* Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П. С. Прибутько, І. Б. Лук'янець — К. : Вид. ПАЛИВОДА А. В., 2007. — 252 с.
151. Про захист персональних даних // Закон України від 01.06.2010 р. № 2297-VI зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
152. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними // Закон України від 15.02.95 р. № 62/95-ВР зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
153. Про ліцензування певних видів господарської діяльності // Закон України від 01.06.2000 р. № 1775-III зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
154. Про платіжні системи та переказ коштів в Україні // Закон України від 05.04.2001 р. № 2346-III зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
155. Про пожежну безпеку // Закон України від 17.12.1993 р. № 3745-XII // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
156. Про порядок продажу, придбання, реєстрації, обліку і застосування спеціальних засобів самооборони, затверджених речовинами сльозоточивої і дратівливої дії // Постанова Кабінету Міністрів України від 07.09.1993 р. № 706 // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
157. Про Стратегію національної безпеки України // Указ Президента України від 12.02.2007 р. № 105/2007 // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
158. Про страхування // Закон України від 07.03.1996 р. 85/96-ВР зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.

159. Про фінансовий лізинг // Закон України від 16.12.1997 р. 723/97-ВР зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
160. Про фінансові послуги та державне регулювання ринків фінансових послуг // Закон України від 12.07.2001 № 2664-III зі змінами і доповненнями // [Електронний ресурс]. — Режим доступу: www.rada.kiev.ua.
161. Протидія відмиванню доходів, здобутих злочинним шляхом : [зб. нормативно-правових актів, міжнародних документів, коментарі]. — К. : «Атіка», 2003. — 256 с.
162. *Рыков А.* Аналитики — кабинетные рыцари шпионских войн / А. Рыков // Разведка. — 2010. — № 2 — С. 50—55.
163. *Самоукина Н. В.* Незаменимый сотрудник и кадровая безопасность / Самоукина Н. В. — М. : Вершина, 2008. — 176 с.
164. *Семененко І.* Банк «Україна»: справа честі: монографія / І. Семененко, С. Іванченко — К. : Міжрегіон. акад. упр. персоналом, 2006. — 31 с.
165. *Станкин М. И.* Психология общения. Курс лекций / Станкин М. И. — М. : МПСИ, 2000. — 301 с.
166. *Степанов Е. А.* Информационная безопасность и защита информации / Е. А. Степанов, И. К. Корнеев. — М. : Инфра-М, 2001. — 304 с.
167. *Стрельбицька Л. М.* Банківське безпекознавство: навч. посібник / Стрельбицька Л. М., Стрельбицький М. П., Гіжевський В. К. — К. : Кондор, 2007. — 601 с. — (Юридична книга).
168. *Сулейманов У. И.* Правила охоты на «крыс» или как бороться с внутрикорпоративными хищениями / Сулейманов У. И. — М. : Ось-89, 2008. — 144 с.
169. Торік у сфері банківської діяльності [Електронний ресурс]. — Режим доступу: http://news.if.ua/print.php?id=3124.
170. *Тумар М. Б.* Основи економічної безпеки підприємства / Тумар М. Б. — К.: Хай-Тек Прес, 2008. — 232 с.
171. *Туник И. Ю.* Антирейдер. Пособие по противодействию корпоративным захватам /И. Ю. Туник, В. А. Поляков. — СПб. : Питер, 2007. — 208 с.
172. Удосконалення податкової системи України — потужний фактор зменшення обсягів тіньової економіки [Електронний ресурс]. — Режим доступу: http://www.refine.org.ua.
173. Украина: экономические преступления в период кризиса. ИТ-Бизнес CRN № 1 [Електронний ресурс]. — Режим доступу: http://crn.com.ua.
174. Управление проблемными кредитами [Електронний ресурс]. — Режим доступу: http://probusiness.in.ua/kb/management/practiec/finance/bank/opera

175. *Цыганов В. В*. Информационные войны в бизнесе и политике: Теория и методология / В. В. Цыганов, С. Н. Бухарин. — М. : Академический Проект, 2007. — 336 с.

176. *Чумарин И. Г*. Предотвращение потерь в розничной торговле. Проверенные способы / И. Г. Чумарин. — М. : Питер Пресс, 2007. — 192 с.

177. *Шейнов В. П*. Конфликты в нашей жизни и их разрешение / В. П. Шейнов. — Минск : Амалфея, 1996. — 288 с.

178. *Шейнов В. П*. Скрытое управление человеком (психология манипулирования) / В. П. Шейнов. — М. : АСТ, 2001. — 848 с.

179. *Яременко С. М*. Безпека кредитних операцій / С. М. Яременко // Економіка та підприємництво : зб. наук. праць. — Випуск № 17. — К. : КНЕУ, 2006. — С. 130—137.

180. *Яременко С. М*. Економічна безпека банків та способи її забезпечення / С. М. Яременко // Фінанси, облік і аудит: зб. наук. пр. — К. : КНЕУ, 2009. — № 13. — С. 136—145.

181. *Яременко С. М*. Забезпечення безпеки проведення в банках касових операцій / С. М. Яременко // Бизнес и безопасность. — 2004. — № 2. — С. 8—10.

182. *Яременко С. Н*. Обеспечение экономической безопасности банков / С. Н. Яременко // Бизнес и безопасность. — 2005. — № 3. — С. 20—21.

183. *Ярочкин В. И*. Безопасность банковских систем / Ярочкин В. И. — М. : Ось-89, 2004. — 416 с.

184. *Ярочкин В. И*. Корпоративная разведка / В. И. Ярочкин, Я. В. Бузанова. — М. : Ось-89, 2004. — 228 с.

185. *Яскевич В. В*. Секьюрити. Организационные основы безопасности фирмы / Яскевич В. В. — М. : Ось-89, 2005. — 368 с.

Додатки

Додаток 1

ОЗНАКИ ЗАГРОЗИ ПРОВЕДЕННЯ АБО ПРОВЕДЕННЯ АКТІВ НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ ЩОДО БАНКУ

Незвична поведінка партнерів та клієнтів	Непрогнозовані зміни в діяльності банку	Зміни в інформаційному середовищі діяльності
• уникнення зустрічей із представниками банку; • неконкретні зобов'язання під час переговорів і при укладанні угод; • збільшення випадків обману з боку клієнтів і партнерів; • порушення договірних зобов'язань; • залучення партнерами і клієнтами до сумісних дій впливових осіб, відомих фірм, компаній, підприємств, банків; • необґрунтовані звинувачення банку	• безпідставний зрив угод укладених банком; • раптові і непередбачені зміни зовнішнього середовища діяльності банку (відключення електроенергії, раптові поломки засобів комунікації, збої в комунальному забезпеченні, підвищення тарифів, організацій, які обслуговують банк тощо); • різке зниження попиту на послуги банку; • збільшення випадків виходу із ладу техніки, обладнання, виявлення випадків крадіжок матеріальних цінностей; • наявність безпідставних скарг на роботу персоналу і установ банку	• поява негативних чуток про банк, оприлюднення небажаних для нього відомостей; • наявність випадків порівняльної реклами щодо послуг банку; • різке збільшення позитивних виступів, публікацій про конкурентів; • зникнення документів, виявлення випадків витоку інформації банку з обмеженим доступом; • отримання електронної інформації, ураженої вірусами; • різке збільшення виступів та публікацій різного спрямування та змісту про банк у ЗМІ; • несподівані публічні заяви, коментарі посадових осіб державних органів щодо діяльності банку

Зміни у взаємовідносинах з органами влади і правоохоронними органами	Зміни у поведінці персоналу банку
• поява нормативних документів, які у той чи той спосіб безпідставно обмежують діяльність банку; • наявність інформації про лобіювання інтересів конкурентів окремими посадовими особами державних установ; • зниження активності зустрічей з керівництвом державних органів і установ, участі в роботі органів державного управління і самоврядування; • різке і необґрунтоване збільшення перевірок, вимог надання звітів з боку органів фінансового контролю та інших контрольних і наглядових органів	• раптове звільнення з роботи провідних фахівців, збільшення плинності кадрів; • поява неодноразових випадків неправдивого приймання на роботу іншими суб'єктами працівників банку; • збільшення випадків міжособистих та міжколективних конфліктів, невдоволення працівників умовами роботи; • поява випадків завищених вимог працівників до банку (особливо тих, хто займає провідні посади в організації діяльності банку) до оплати праці; • збільшення випадків порушення встановлених правил і порядку роботи

Додаток 2

ПОТЕНЦІЙНІ ОБЄКТИ ДЛЯ ЗАЛУЧЕННЯ ДО РОБОТИ НА ПРОМИСЛОВИХ ШПИГУНІВ

Додаток 3

ЗМІСТ ЗАВДАНЬ ЗАХИСТУ ІНФОРМАЦІЇ БАНКУ

Правового характеру

- регулювання доступу до інформаційних ресурсів банку представників державних органів і установ;
- регулювання доступу персоналу до інформаційних ресурсів банку;
- установлення відповідальності за посягання на інформаційні ресурси банку

Криптографічного характеру

- шифрування інформації при переданні її через незахищені засоби зв'язку;
- регламентація доступу до баз даних та електронних документів

Організаційного характеру

- категоріювання інформації банку;
- установлення відповідного режиму роботи банку;
- організація спеціального діловодства в банку;
- підбір персоналу для роботи з інформацією, що має обмежений доступ;
- профілактична та виховна робота з персоналом;
- здійснення заходів захисту інформації під час зустрічей, ділових переговорів, конференцій тощо;
- планування дій банку при стихійних лихах, пожежах, терористичних актах, у тому числі і щодо захисту інформації

Інженерно-технічного характеру

- спеціальне інженерно-технічне обладнання місць зберігання інформації;
- застосування спеціальних технічних засобів для перекриття різних видів каналів витоку інформації;
- застосування технічних засобів охорони та технічна укріпленість об'єктів

Програмно-апаратного характеру

- застосування спеціальних програмних засобів захисту комп'ютерної інформації;
- застосування антивірусних програм;
- забезпечення безперебійної роботи комп'ютерних систем при аварійних ситуаціях;
- виключення можливості перехоплення електромагнітних випромінювань і наводок;
- створення системи страхового копіювання комп'ютерної інформації

Додаток 4

ЗАХИСТ ІНТЕРЕСІВ БАНКУ У ВЗАЄМОВІДНОСИНАХ З ПЕРСОНАЛОМ, ДОПУЩЕНИМ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

Зобов'язання про нерозголошення інформації банку з обмеженим доступом	***Трудовий договір (контракт)***
Правовий документ, в якому працівник банку добровільно письмово дає згоду на обмеження його прав щодо використання інформації банку з обмеженим доступом. Одночасно працівник попереджується про відповідальність за розголошення такої інформації	Наявність у договорі: • зобов'язань працівника не розголошувати відомості, які становлять таємну або конфіденційну інформацію банку; • зобов'язань працівника дотримуватися правил захисту інформації з обмеженим доступом, установлених у банку; • зобов'язань працівника повідомляти безпосереднього керівника і службу безпеки банку про втрату носіїв інформації з обмеженим доступом; • видів відповідальності працівника за недотримання ним правил захисту інформації

Наказ про призначення на посаду

• визначається ступінь допуску до відомостей, які становлять таємну та конфіденційну інформацію банку;

• визначаються обов'язки працівника та заходи, які повинні ним вживатися для захисту інформації банку

Посадова інструкція

• обов'язок працівника дотримувати у таємниці відомості, які йому стали відомі у зв'язку з його роботою в банку;

• відповідальність працівника за порушення правил зберігання банківської інформації

Додаток 5

РОЗРОБЛЕННЯ ТАЄМНИХ ДОКУМЕНТІВ У БАНКУ

Облік документів таємного та конфіденційного характеру

Облік виготовлених, отриманих документів розробником (виконавцем)	Облік наявності та руху документів спецчастиною	Облік користування документами в спецчастині та у користувачів	Облік знищення документів та передання на зберігання

Додаток 6

ОФОРМЛЕННЯ ДОКУМЕНТІВ ТАЄМНОГО ТА КОНФІДЕНЦІЙНОГО ХАРАКТЕРУ В БАНКУ

На всіх документах вказується гриф документа: «КТ» Ї комерційна таємниця; «БТ» Ї банківська таємниця; «КІ» Ї конфіденційна інформація	На всіх документах вказується поряд з грифом номер примірника	На звороті останньої сторінки документу вказується кількість примірників, їх місцезнаходження, прізвище виконавця документа та дата його розроблення
Усі документи пересилають тільки в щільних конвертах, на яких вказується гриф документа та його індекс	Документи візуються виконавцем і підписуються посадовою особою, яка має підписувати такі документи	На всіх документах проставляється дата та індекс реєстрації документів за обліком спецчастини

Додаток 7

РЕЄСТРАЦІЯ ТАЄМНИХ ТА КОНФІДЕНЦІЙНИХ ДОКУМЕНТІВ У БАНКУ

Реєстрація документа Ї фіксування факту створення або надходження документа проставленням на ньому умовного позначення — реєстраційного індексу з подальшим записом у реєстраційних формах необхідних відомостей про документ

Реєстрація таємних та конфіденційних документів в установі банку проводиться централізовано	Кожний документ реєструється лише один раз, вхідні — у день надходження, створювані — у день підписання та затвердження	Реєстраційний індекс складається з порядкового номера в межах групи документів, що реєструються і доповнюються індексами за номенклатурою справ, питаннями діяльності, кореспондентами тощо

Реєстрація документів здійснюється у відповідних журналах (окремо таємні та конфіденційні документи)	Запис про реєстрацію має містити назву документа, короткий зміст, адресата (виконавця), дату реєстрації, кількість сторінок, реєстраційний індекс (власний та банку для вхідних документів) гриф документа та номер примірника

Додаток 8

РОБОТА З ДОКУМЕНТАМИ ТАЄМНОГО ТА КОНФІДЕНЦІЙНОГО ХАРАКТЕРУ В БАНКУ

Роботу з документами здійснюють тільки ті працівники, яких допущено до відповідних відомостей таємного та конфіденційного характеру	Робота здійснюється на своїх робочих місцях за умови неможливості ознайомлення з ними інших осіб або у спеціально виділених приміщеннях	Робота з документами здійснюється тільки у визначений час, як правило, з обов'язковим їх поверненням до спецчастини в кінці робочого дня
Надання документів для роботи здійснюється з обов'язковим записом у відповідному журналі (реєстрі) під підпис особи, яка отримала зазначений документ	У разі тривалої роботи з таємними та конфіденційними документами (більше одного робочого дня) виконавець ураховує документ у відповідному індивідуальному описі таємних та конфіденційних документів та зберігає його в особистому сейфі	Перевірка наявності документів таємного та конфіденційного характеру здійснюється виконавцем щоденно, керівником підрозділу щонеділі з відповідним записом у індивідуальному описі документів

Додаток 9

ЗБЕРІГАННЯ ДОКУМЕНТІВ ТАЄМНОГО ТА КОНФІДЕНЦІЙНОГО ХАРАКТЕРУ В БАНКУ

Зберігання документів працівниками	**Зберігання документів у спецчастині**	**Зберігання документів у архівах**
— в індивідуальних сейфах; — у металевих шафах за умови призначення відповідальної особи в підрозділі за доступ до таких шаф; — кімнати, в яких знаходяться сейфи (металеві шафи), зачиняються на замок, опечатуються і передаються під охорону	— у металевих шафах за справами; — кімнати спецчастин повинні мати спеціальне обладнання і відповідне технічне укріплення, зачинятися на замок, опечатуватися і здаватися під охорону; — доступ до спецчастини має обмежене коло осіб	— у металевих шафах за справами; — приміщення архіву повинне мати спеціальне обладнання та технічне укріплення, зачинятися на замок, опечатуватися та здаватися під охорону; — доступ до архіву мають тільки працівники архіву

Зберігання документів таємного
та конфіденційного характеру здійснюється окремо від інших документів

Додаток 10

ТЕХНОЛОГІЇ ПРОВЕДЕННЯ ІНФОРМАЦІЙНОГО АУДИТУ

Обстеження інформації на об'єкті	**Обстеження інформації про об'єкт**	**Спеціальне обстеження сфери інформаційної уваги**
— визначення належності інформації, яку необхідно виявити під час обстеження; — визначення об'єкта обстеження; — визначення переліку джерел інформації, які підлягають обов'язковому обстеженню; — пошук ознак наявності необхідної інформації; виявлення умов появи необхідної інформації на об'єкті та її повного обсягу; — виявлення зв'язку необхідної інформації з іншою, яка є на об'єкті; — відбір необхідної інформації під час обстеження	— визначення основних інформаційних характеристик та ознак об'єкта; — прогнозування місць зосередження інформації про об'єкт, її можливих джерел; — обстеження інформаційних масивів з метою виявлення орієнтуючої інформації про об'єкт; — виявлення зв'язків орієнтуючої інформації, умов її появи в інформаційному середовищі; — пошук інформації, яка будь-яким чином пов'язана з об'єктом; — замовлення спеціальних досліджень, подання запитів з метою отримання інформації про об'єкт; — пошук джерел первинної інформації про об'єкт	— вибір сфери інформаційної уваги; — обстеження всіх об'єктів та джерел сфери інформаційної уваги з метою виявлення ознак важливої та цінної для банку інформації; — пошук додаткової інформації, що підтверджує попередню інформацію або суперечить їй; — виявлення обставин появи важливої для банку інформації; — установлення зв'язків важливої інформації з іншою

Додаток 11

ТЕХНОЛОГІЇ ПРОВЕДЕННЯ ІНФОРМАЦІЙНОГО МОНІТОРИНГУ

Контроль інформації за певними ознаками та індикаторами	**Контроль інформації за певними джерелами**	**Суцільний контроль інформації, що з'являється в інформаційному середовищі**
— визначення ознак інформації, які характеризують необхідні банку знання; — визначення інформаційних характеристик ознак; — контроль наявності ознак у складі інформації, яка подається різними джерелами; — виявлення зв'язків між ознаками у складі інформації різних джерел; — фіксація ознак і змісту важливих інформаційних повідомлень	— визначення джерел інформації відповідно до: — можливості появи необхідної інформації; — об'єктивності та вартості інформації; — доступності джерел; — постійний контроль інформації, яка подається певними джерелами; — фіксація важливих інформаційних повідомлень	— розподіл сил і засобів за групами джерел інформації; — визначення інформації, яка має бути виявлена під час контролю інформаційного середовища; — визначення порядку (графіка) та видів (постійного, періодичного, вибіркового) контролю; — фіксація певної інформації під час контролю

Додаток 12

МЕТОДИКА ПЕРЕВІРКИ ОКРЕМИХ ВИДІВ ДОКУМЕНТІВ ПРИ ВИДАЧІ КРЕДИТУ

1. **Перевірка паспорта громадянина України.** Паспорт подається в оригіналі. Основними реквізитами паспорта є:

- наявність єдиного встановленого бланку паспорта;
- наявність у паспорті 16 сторінок;
- наявність серії з двох літер і номера з шести цифр. Серія і номер паспорта вказується шляхом наскрізного вибиття у верхній частині кожної із сторінок паспорту, в тому числі і на обкладинках;
- на останній сторінці паспорта (обкладинці) має бути інформація про паспорт громадянина України (витяг з Наказу про паспорт громадянина України, затвердженого Постановою Верховної Ради України від 02.09.1993 р.;
- на першій, третій і п'ятій сторінках паспорта відповідно до віку мають бути фотографії власника паспорта, завірені печатками. Фотографії не повинні виходити за рамки встановлених ліній і чотирьох кутів, а також мати строгий розмір 35х45 мм. Вони мають бути наклеєні по всій площині рівномірно і не повинні відклеюватись. Лінії обрізування фотографій мають бути рівними. Обрізування фотографій до необхідного розміру здійснюється у паспортній службі спеціальним приладом. Лінії зрізу фотографій мають бути досить чіткими;
- наявність рельєфної гербової печатки у правому верхньому куті фотографії на першій сторінці і на всіх фотографіях внесених відповідно до віку;
- усі графи першої, другої, четвертої і шостої сторінок паспорта мають бути заповнені у відповідних органах МВС;
- паспорт заповнюється друкарським способом чи від руки, чорнилами чорного кольору, без скорочень і виправлень;
- наявність гербової печатки у лівому нижньому куті на другій сторінці паспорта, а також на четвертій і шостій сторінках після вклеювання фотографій відповідного віку;
- звернути увагу на чотири цифри, зображені попарно через дефіс на рельєфній гербовій печатці, і цифри, зображені попарно на гербовій печатці, вони мають бути однаковими;
- гербові печатки мають спеціальну нумерацію: перші дві цифри означають індекси, що закріплені за областями, містами Києвом і Севастополем і Республікою Крим; дві наступні — індекси, закріплені за відповідним органом МВС у певному регіоні. Відбитки печаток мають бути чіткими і розбірливими. У середині малюнка печатки обов'язково має бути присутнім малий герб України;
- на всіх сторінках, де є фото, має бути підпис власника паспорту;

- перший запис про прописку / реєстрацію вноситься на 11-ту сторінку;
- у штампі про прописку / реєстрацію обов'язково має бути вказана така інформація: адреса прописки / реєстрації (місто, вулиця, № будинку, № квартири), а також дата прописки / реєстрації і підпис відповідального працівника МВС;
- відмітка про реєстрацію, розірвання шлюбу, здійснюється органами реєстрації громадського стану на 10-й сторінці «Сімейний стан».

2. **Перевірка довідки про присвоєння ідентифікаційного номера.** Довідка обов'язково надається в оригіналі. Основними реквізитами довідки є:
- ідентифікаційний номер має складатися з 10 цифр;
- якщо перші п'ять цифр номера розділити на 365, то перші дві цифри будуть означати рік народження власника довідки;
- ідентифікаційний номер не може бути видано раніше 1996 р.;
- «Картка фізичної особи — платника податків» почала видаватись органами ДПІ з 20 грудня 2001 р. У разі втрати «Довідки про присвоєння ідентифікаційного номера» видається дублікат Картки, а не дублікат Довідки, при цьому у верхньому правому куту Картки вказується «Дублікат»;
- на довідці про присвоєння ідентифікаційного номера обов'язково мають бути: підпис відповідального працівника і чітка «мокра» печатка ДПІ;
- якщо людина через свої релігійні переконання відмовилась від присвоєння ідентифікаційного номера, то в її паспорті обов'язково має бути про це відповідна відмітка.

3. **Перевірка довідки про доходи з місця роботи.** Довідка про доходи має надаватися в оригіналі:
- наявність прізвища, ім'я і по-батькові. Дані про власника довідки, вказані в ній, та ідентифікаційний номер мають збігатися з даними паспорта і Картки фізичної особи — платника податків / Довідки про присвоєння ідентифікаційного номера;
- наявність даних про період нарахування заробітної плати (розбивка сум помісячно із зазначенням року);
- наявність підписів керівника і головного бухгалтера на довідці з організації, де працює особа із зазначенням юридичної адреси;
- наявність чіткої «мокрої» печатки (виключно круглої форми) і штампу (прямокутної форми), на яких чітко видно назву організації і код ЄДРПОУ;
- довідка про доходи дійсна 1 місяць і 20 днів з останньої дати нарахування заробітної плати.

Додаток 13

СХВАЛЕНОпостановою Правління Національного банку Українивід 6 серпня 2009 р. № 461

НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

ПАМ'ЯТКА ПОЗИЧАЛЬНИКА, ЯКИЙ МАЄ ЗАБОРГОВАНІСТЬ ПЕРЕД БАНКОМ ЗА СПОЖИВЧИМ КРЕДИТОМ І ПОТРАПИВ У СКРУТНЕ ФІНАНСОВЕ СТАНОВИЩЕ

Чи варто ігнорувати умови кредитного договору?

Отримавши кредит, Ви як позичальник банку зобов'язані повернути банку основну суму боргу, сплатити проценти за користування ним у розмірах і в строки, установлені умовами кредитного договору.

Крім того, умовами кредитного договору часто передбачається необхідність здійснення позичальником інших платежів, пов'язаних з отриманням, обслуговуванням та погашенням кредиту як на користь банку (комісії з відкриття поточного/карткового рахунку, здійснення розрахунково-касового обслуговування, забезпечення обслуговування кредитної заборгованості, що, наприклад, пов'язано з бажанням позичальника отримувати виписки за кредитним/картковим рахунком, здійснення валютно-обмінних операцій, надання консультаційних, у тому числі юридичних, послуг тощо), так і на користь третіх осіб (страхові платежі, платежі за послуги нотаріусів, інших осіб, біржові збори тощо).

Національний банк України з метою захисту прав позичальників під час укладення ними кредитних договорів запровадив Правила надання банками України інформації споживачеві про умови кредитування та сукупну вартість кредиту, затверджені постановою Правління Національного банку України від 10 травня 2007 №168, зареєстровані в Міністерстві юстиції України 25 травня 2007 за №541/13808 (далі — Правила №168), і підготував детальну інформацію для громадян, які вирішили отримати кредит у банку, викладену в Пам'ятці позичальника банку за споживчим кредитом, що розміщена на інтернет-сторінці Національного банку України в підрозділі «Інформаційна допомога позичальнику» розділу «Інформаційні матеріали» за адресою: www.bank.gov.ua/Inf_mat.

У разі невиконання або неналежного виконання обов'язків, передбачених кредитним договором щодо забезпечення повернення кредиту, а також у разі втрати або суттєвого погіршення стану наданого в заставу майна, яке залишається у Вашому користуванні, банк має право вимагати від Вас дострокового повернення кредиту та сплати фактично нарахованих процентів. Право банку пред'явити таку вимогу також, як правило, зазначено в кредитному договорі.

Крім того, банки накопичують інформацію про стан обслуговування кредитів позичальником, у результаті чого формується його кредитна історія. Усі Ваші дії або бездіяльність, що призведуть до неналежного погашення кредиту, можуть вплинути на якість Вашої кредитної історії. Надаючи кредити, банки, як правило, перевіряють кредитну історію позичальника. Наявність у позичальника негативної кредитної історії може стати в майбутньому підставою для надання банком кредиту за більш високою процентною ставкою або взагалі для відмови в наданні кредиту.

УВАГА! Прагнучи забезпечити дотримання позичальником графіка платежів за кредитом, установленого умовами кредитного договору, за неналежного його виконання банки застосовуватимуть штрафні санкції (неустойки, штрафи, пені). Унаслідок цього сума боргу разом з нарахованими штрафними санкціями може стати настільки великою, що її вже неможливо буде погасити навіть через продаж майна, яке було надане в заставу за кредитом. У такому разі погашається лише частина боргу і позичальник за рішенням суду продовжує нести відповідальність перед банком уже іншими своїми активами (заробітною платою, іншим майном тощо).

Позичальникові також недопустимо приймати необачні рішення щодо способів повернення кредиту, особливо в скрутні для нього часи. Наприклад, недопустимо самовільно залишити автомобіль, що був у заставі за кредитом, біля будівлі банку, вважаючи, що цим забезпечено повний розрахунок за кредитом. Адже це лише особиста думка позичальника. Відповідно до статті 1 Закону України «Про заставу» банк має законні підстави вважати інакше. Ураховуючи постійну зміну цін на нерухомість та автомобілі, амортизацію та інші обставини, банк здійснюватиме реалізацію заставленого майна за ринковою вартістю. Тож і в цьому разі може виникнути ситуація, коли погашеною буде лише частина заборгованості позичальника за кредитом.

У зв’язку з цим для позичальника дуже важливо повністю контролювати ситуацію, у якій він опинився з тих чи тих причин, та намагатися разом з банком знайти прийнятний для обох сторін вихід з неї.

Чи може банк допомогти Вам?

Банки з розумінням ставляться до того, що Ви можете наразитися на непередбачені обставини, які можуть негативно вплинути на Ваш фінансовий стан і здатність своєчасно та в повному обсязі погашати кредит.

Непередбаченими обставинами, що спричинили негативний вплив на Ваше фінансове становище і здатність своєчасно та в повному обсязі погашати кредит, можуть бути: зменшення заробітної плати та/або інших надходжень; втрата пільг, роботи; тяжке захворювання та/або отримання інвалідності; розлучення; смерть членів сім’ї або інше, якщо

ці обставини спричинили втрату доходів або їх зниження до рівня, за яким щомісячні сукупні платежі за кредитом перевищують 30% Вашого місячного доходу.

За наявності підтвердження достовірними документами (довідка з місця роботи, довідка з державної служби зайнятості тощо) об'єктивних та беззаперечних доказів того, що Ви не в змозі своєчасно та в повному обсязі погашати кредит у зв'язку з настанням непередбачених обставин, а також ураховуючи інші обставини (наприклад, стан обслуговування кредиту до настання подій, які спричинили погіршення фінансового становища, причини настання таких подій, поточний фінансовий стан, перспективи відновлення платоспроможності тощо), банк може надати Вам можливість погашати кредит на нових умовах, прийнятних як для Вас, так і для банку.

Що Ви можете зробити, потрапивши у фінансову скруту?

Передусім не ігноруйте листи та дзвінки від тих, перед ким у Вас є фінансові (грошові) зобов'язання. Борг сам по собі не зникне, тому Вам потрібно зустрітися з представниками банку для конструктивного вирішення Ваших боргових проблем. І чим швидше Ви це зробите, тим меншими будуть штрафи за несвоєчасне погашення кредиту та більш вигідними для Вас нові умови погашення кредиту.

Разом з тим Ви не повинні покладатися лише на банк. Зі свого боку Ви повинні виважено оцінити ситуацію, у якій Ви опинилися. Ви маєте усвідомлювати, що Вам необхідно повернути взяті в кредит гроші. Адже банк, як установа, яка по суті виконує функцію фінансового посередника, не тільки надає кредити, а й залучає депозити (вклади), які є джерелом коштів для надання кредитів. Залучені депозити банку необхідно повернути у визначені депозитними договорами строки, сплативши проценти за користування ними. Ураховуючи це, кошти, що повертаються позичальниками під час погашення кредитів, є джерелом для повернення депозитів. З метою забезпечення стабільності своєї роботи банк узгоджує графіки виплат за депозитами та надходжень за виданими кредитами. Тому Ви, у свою чергу, повинні докладати максимальних зусиль щодо забезпечення повернення кредиту.

Як банк повинен обходитися з позичальником, який потрапив у скрутне фінансове становище?

Якщо Ви потрапили у скрутне фінансове становище, як Ви, так і банк зацікавлені в знаходженні оптимального рішення щодо забезпечення повернення кредиту. Реалізація майна, наданого в заставу за кредитом, є вимушеним заходом з боку банку, до якого він вдається, коли немає впевненості в забезпеченні повернення кредиту відновленням платежів з боку позичальника.

Національний банк України постановою Правління від 06 серпня 2009 №461 схвалив Рекомендації щодо роботи банків з позичальниками — фізичними особами, які мають заборгованість за споживчими кредитами та потрапили в скрутне фінансове становище (далі — Рекомендації №461).

Відповідно до цих Рекомендацій банки повинні:

✓ підтримувати зв'язок з позичальником у зручний для нього час і спосіб (зустрічі, листування, телефон, факс тощо);

✓ надати позичальникові повну і доступну інформацію щодо загального розміру його заборгованості, уключаючи всі платежі, передбачені умовами кредитного договору, та проінформувати позичальника про заходи, які можуть бути застосовані в разі невиконання позичальником умов кредитного договору, у тому числі повідомити, що неналежне виконання умов кредитного договору може негативно вплинути на кредитну історію позичальника і в майбутньому призвести до погіршення доступу до кредитів;

✓ обговорити з позичальником усі обставини його скрутного фінансового становища для того, щоб визначити можливі шляхи повернення кредиту;

✓ разом з позичальником розробити прийнятну як для позичальника, так і для банку програму погашення кредиту, зокрема, це може бути реструктуризація кредиту позичальника, зміна валюти кредиту тощо.

Які існують основні шляхи забезпечення повернення кредиту?

Банк може:

- здійснити реструктуризацію кредиту;
- здійснити зміну валюти кредиту;
- продати кредит іншому банку;
- передати право вимоги за кредитним договором;
- звернутися до третіх осіб за послугами з повернення кредиту;
- здійснити звернення-стягнення на майно.

Реструктуризація кредиту означає внесення змін до раніше укладеного з банком кредитного договору через укладення додаткового договору про продовження строку дії договору, зміни графіка платежів, зміни процентних ставок тощо. Реструктуризація кредиту дасть змогу Вам на інших умовах погашати кредит. Умови реструктуризації кредиту визначаються банком для кожного позичальника індивідуально на підставі об'єктивних та беззаперечних доказів неможливості виконувати умови раніше укладеного кредитного договору, що підтверджені достовірними документами.

Укладаючи договір з банком, у тому числі і додатковий, переконайтеся, що всі умови договору Вам зрозумілі, Вам надана вичерпна інформація про сукупну вартість послуг банку відповідно до

Правил №168 і Ви повністю усвідомлюєте всі наслідки підписання договору.

Уклавши з банком договір, дотримуйтесь усіх його умов

Якщо ж Ви не здійснюєте платежі за кредитом відповідно до умов договору, ігноруєте нагадування, не відповідаєте на листи та телефонні дзвінки банку, а також Вами не досягнуто згоди щодо укладення договору про реструктуризацію кредиту, банк може звернутися до суду або до третіх осіб — суб'єктів господарювання за послугами з повернення заборгованості за кредитом, іншого банку з метою продажу Вашого боргу або передання права вимоги за Вашим кредитним договором.

Додаток 14

ВИХОВНА ТА ПРОФІЛАКТИЧНА РОБОТА З КАДРАМИ В БАНКУ

Сукупність методів впливу на свідомість, почуття, волю і характер працівників банку в інтересах формування у них банківського патріотизму, вміння зберігати таємниці банку, суворо дотримуватись установлених правил роботи і вимог законодавства

Навчання правилам поведінки з інформацією з обмеженим доступом і способам протидії її витоку	Навчання правилам дотримання заходів безпеки під час виконання своїх посадових обов'язків	Створення обстановки негативного ставлення до фактів порушення встановлених правил і норм законів у колективах банку
Пропаганда іміджу банку	Застосування диференційованої системи оплати і стимулювання праці	Дотримання принципу рівних можливостей під час просування по службі
Висока вимогливість до працівників, контроль їх роботи і неухильна відповідальність за порушення	Матеріальне і моральне заохочення в роботі щодо виконання заходів безпеки	Забезпечення довготривалою роботою працівників банку

Створення сприятливих умов для роботи

Додаток 15

СИСТЕМА ЗАХОДІВ, СПРЯМОВАНИХ НА ФОРМУВАННЯ ВІДПОВІДАЛЬНОСТІ ПРАЦІВНИКІВ БАНКУ ЗА РЕЗУЛЬТАТИ ЇХ РОБОТИ

1. Формування моральних і професійних норм поведінки працівників банку.

2. Правильне засвоєння посадових обов'язків працівниками, персональне попередження їх про необхідність дотримання встановлених у банку порядку і правил роботи.

3. Постійний контроль якості роботи і дотримання працівниками встановлених норм і правил.

4. Упровадження розвинутої системи заходів дисциплінарного впливу за допущені працівниками порушення і проступки.

5. Неухильна відповідальність за допущені порушення і проступки.

6. Залежність системи оплати праці від її результатів.

7. Розроблення і впровадження Положення про трудову дисципліну в установах банку.

8. Розроблення і прийняття конкретних зобов'язань сторін у трудових договорах і контрактах.

9. Періодичне доведення до працівників рішень керівництва банку і судової практики щодо осіб, які допустили порушення встановлених правил роботи і норм чинного законодавства

Додаток 16

СИСТЕМА ЗАХОДІВ, СПРЯМОВАНИХ НА ФОРМУВАННЯ БАНКІВСЬКОГО ПАТРІОТИЗМУ ПРАЦІВНИКІВ

1. Створення сприятливих умов праці та просування по службі.

2. Введення валентної системи оплати праці.

3. Створення в банку системи удосконалення професійної підготовки працівників.

4. Заохочення банківських династій, забезпечення довгостроковою роботою кожного працівника.

5. Підтримка високого морального і ділового клімату в колективах установ банку.

6. Упровадження жорсткої системи відповідальності персоналу банку за результати своєї праці, дотримання встановлених правил і законності.

7. Мотивація і заохочення творчої ініціативи працівників, створення дійової системи матеріальних і моральних стимулів.

8. Упровадження у банку атрибутів відомчих відзнак.

9. Пропаганда досягнень банку, його іміджу і переваг на ринку.

10. Розроблення і пропаганда власного стилю банківської діяльності.

11. Упровадження заходів соціального і правового захисту працівників.

12. Надання необхідно-можливого ступеня самостійності і довіри працівникам.

13. Використання гнучкої, нетравмуючої системи звільнення з роботи.

Додаток 17

ДЕЯКІ ОЗНАКИ ПОВЕДІНКИ ЗАЛЕЖНИХ ОСІБ

На даний час залежними є особи, які перебувають чи потенційно можуть перебувати під впливом певних факторів. Залежна поведінка пов'язана з бажанням людини усунути себе від реальності подій (ситуацій) через зміну стану своєї свідомості. Усунення від реальності завжди супроводжується емоційними переживаннями. Останні ж якраз і є складовою залежності.

Залежно від того, що використовується для усунення людини від реальності, розрізняють залежності — від наркотиків, алкоголю, токсинів, куріння, субстанціональні залежності (комп'ютерні, ігрові, сексуальні і т. п.).

Ознаки залежності

1. Члени релігійних організацій:

- ✓ одинокі люди;
- ✓ постійно мають при собі фотографії духовних наставників;
- ✓ мають особливий режим харчування (визначений час, свої харчі, певні ритуали);
- ✓ наявність у паспорті відміток про відмову від ідентифікаційного коду, групи крові;
- ✓ небажання давати власні фото, у тому числі і до кадрових органів;
- ✓ характерні особливості одягу, манери розмовляти, наявність специфічних аксесуарів.

2. Алкоголіки:

- ✓ небажання надавати власні фото, у тому числі і до кадрових органів;
- ✓ швидка мова, підвищена моторика, неоднозначні тягучі відповіді на запитання, безпричинний сміх;
- ✓ метушливість, потирання рук при згадуванні епізодів вживання алкогольних напоїв;
- ✓ погана пам'ять, довго згадує певні епізоди свого життя, відомих йому раніше осіб;
- ✓ стан обличчя (набряклість, почервоніння носа);
- ✓ часта похвала себе (хвастовство).

3. Наркомани:

- ✓ як правило, молоді особи;
- ✓ довгі рукава одягу незалежно від погоди і обставин;
- ✓ набряклі кисті рук, звалене волосся;
- ✓ сутула постава;
- ✓ невиразна, розтягнута мова;
- ✓ затримані, незграбні рухи;
- ✓ ознаки втрати контролю над собою;
- ✓ дратівливість, різкість, неповага у розмові з іншими особами;

✓ наявність у розмові певного сленгу.

4. Ігромани:

✓ демонстрація клубних карток казино;
✓ хороша обізнаність з предметами, об'єктами й умовами гри;
✓ наявність нестатусної атрибутики (каблучки, ланцюги);
✓ постійне нарікання на відсутність грошей при рідкісних випадках аристократичної поведінки.

Додаток 18

ЗМІСТ РОБОТИ КЕРІВНИКА ГРУПИ УПРАВЛІННЯ ДІЯЛЬНІСТЮ БАНКУ НА ВИПАДОК ЗАГРОЗИ АБО ВИНИКНЕННЯ ЕКСТРЕМАЛЬНИХ СИТУАЦІЙ

1. Доповідає членам групи ситуацію, що склалась, або залучає для цього працівника, якому стало відомо про загрозу банку.

2. Організовує проведення аналізу ситуації, що склалась, та її оцінку.

3. У разі необхідності залучає для участі в роботі групи необхідних фахівців.

4. Приймає рішення про введення в дію плану дій банку на випадок виникнення екстремальних ситуацій.

5. Приймає рішення про сповіщення правоохоронних та інших органів, установ і організацій про екстремальну ситуацію.

6. Організовує взаємодію банку з представниками залучених органів, установ та організацій.

7. Керує діяльністю групи під час виконання заходів плану.

8. Визначає порядок діяльності банку в умовах дії екстремальної ситуації, вводить відповідні обмеження й заборони, установлює обсяг операцій і термін операційного дня, приймає рішення про зміни повноважень філій і встановлює режим їх діяльності.

9. Приймає рішення про заходи щодо ліквідації наслідків екстремальної ситуації.

Додаток 19

ФУНКЦІЇ ЧЛЕНІВ ГРУПИ УПРАВЛІННЯ ДІЯЛЬНІСТЮ БАНКУ НА ВИПАДОК ЗАГРОЗИ АБО ВИНИКНЕННЯ ЕКСТРЕМАЛЬНИХ СИТУАЦІЙ

Керівник юридичного підрозділу

- Дає правову оцінку ситуації, що склалася.
- Розробляє рекомендації щодо правового розв'язання ситуації.
- Вживає заходів щодо збереження особливо важливих документів банку (договорів, угод, архіву правових документів)

Керівник фінансового (бухгалтерського) підрозділу

- Оцінює розмір можливих втрат, фінансові і матеріальні можливості банку щодо задоволення злочинних вимог зловмисників, обсяги коштів для ліквідації наслідків екстремальної ситуації.
- Розробляє рекомендації щодо оптимізації витрат на проведення заходів, пов'язаних із виходом із екстремальної ситуації.
- Вживає заходів щодо збереження або евакуації основних фінансових документів, у разі необхідності формує фонд їх дублікатів

Керівник підрозділу кадрів

- На вимогу керівника групи готує характеристики на окремих працівників банку.
- Інформує членів групи про моральний стан персоналу і характер взаємовідносин у колективах підрозділів банку.
- Проводить роботу, спрямовану на недопущення паніки, припинення нездорових чуток, роз'яснення обстановки серед персоналу банку.
- Керує евакуацією персоналу банку

Керівник підрозділу безпеки

- Вживає заходів щодо посилення охорони і режиму в банку.
- Контролює ситуацію й інформує членів групи про її зміни.
- За певних умов бере участь у проведенні переговорів зі злочинцями.
- Підтримує взаємозв'язок з правоохоронними органами та іншими установами.
- Керує виконанням спеціальних заходів кризового плану

Додаток 20

ЗАХОДИ ОСОБИСТОЇ БЕЗПЕКИ В УМОВАХ ЗАГРОЗИ ТЕРОРИСТИЧНОГО АКТУ

Уникати самостійного пересування, виходити з роботи, з дому, пересуватись у справах чи за особистою необхідністю доцільно у складі групи	Уникати постійних маршрутів, безлюдних вулиць, пересуватись по жвавих дорогах. У разі пересування на автомобілі займати місце в середньому ряду, щоб не дати можливості притиснути автомобіль до узбіччя	При переміщенні в автомобілі закривати вікна і двері на замок, якщо хтось зупинив ваш автомобіль, не слід виходити з нього, особливо на безлюдній дорозі чи в темряві
Залишати автомобіль слід у місцях, за якими є можливість спостерігати або на стоянках, що охороняються	Підійшовши до автомобіля, слід оглянути його, упевнитись, що в ньому нікого немає, чи немає під автомобілем або поблизу підозрілих предметів чи людей	Пересування дітей до школи має бути під наглядом дорослих. Попередити вчителів, що дітей ні в якому разі не можуть забирати будь-які сторонні особи
Попередити родичів, щоб не пускали нікого до помешкання, нікому не повідомляли відомості про вашу діяльність, місцезнаходження на даний час, не приймали ніяких передач, пакунків, листів	З обережністю слід ставитися до осіб, що видають себе за працівників комунальних, ремонтних служб, роздрібних торговців	Завжди доцільно підтримувати дружні стосунки з сусідами, особливо літніми
Необхідно обговорити у сім'ї порядок дій у разі нападу на помешкання, несанкціонованого проникнення до неї, у разі тривалої відсутності вас з роботи чи інших місць	У робочих кабінетах слід установити тривожні кнопки для негайного виклику охорони	З обережністю слід ставитися до поштових листів, які мають товщину понад 3 мм, та таких, що надійшли від невідомих кореспондентів
На роботі вся пошта має отримуватися через секретаря у відкритому вигляді	Робочі та житлові приміщення обов'язково мають перебувати під сигналізацією	Завжди слід мати осіб, яким можна зателефонувати у разі безпосередньої загрози вам

Додаток 21

ОСОБЛИВОСТІ ПОВЕДІНКИ ОСІБ, ЩО ОПИНИЛИСЯ В ЗАРУЧНИКАХ

З моменту захоплення в заручники необхідно особливо контролювати свої дії і фіксувати все, що коїться навколо

У разі наявності знайомих осіб серед терористів не слід показувати, що впізнали їх, не звертатися до них як до знайомих

Не ставити зайвих питань терористам, не дивитись їм в очі, не привертати до себе уваги, зняти яскраві прикраси, не вставати і не ходити без дозволу

При можливості слід повідомити про себе інформацію, яка отримана в ході захоплення і утримання особі, що веде переговори з терористами

При контакті з близькими та родичами необхідно намагатись їх заспокоїти та пояснити, як вони мають діяти, ретельно виконувати все те, що сказано вами

При спробах здійснити фізичний вплив на заручників не слід відбиватись, необхідно прийняти позу, за якої такий вплив може бути зменшений чи не так відчутний

Доцільними будуть спроби пом'якшити ворожість зловмисників стосовно заручників, пошук способів установлення індивідуальних контактів з особами, що їх утримують

Обов'язково підтримувати особисту гігієну, стежити за часом, виконувати можливі фізичні вправи

Слід продумано підходити до питань терористів, по можливості передбачати їхню реакцію і поведінку, а також поведінку інших заручників на дії терористів, особливо, коли їх примушувати виконувати певні дії

Додаток 22

ДІЇ ЗАРУЧНИКІВ ПРИ ЇХ ЗВІЛЬНЕННІ ПРАВООХОРОННИМИ ОРГАНАМИ

Ні в якому разі не привертати до себе увагу, зайняти безпечне місце і укритись від куль та осколків	У разі задимлення чи газової атаки зробити пов'язку, змочити її і дихати через неї	У разі загрози пожежі й отримання опіків доцільно звільнитися від синтетичного одягу
Не брати в руки зброю вбитих терористів, не намагатися допомогти правоохоронцям	При виявленні заручників правоохоронцями і виходу їх із приміщення, в якому вони утримувалися, чітко виконувати всі команди правоохоронців, не робити різких рухів і заяв	Про звільнення заручники терміново повідомляють своїх близьких і безпосередніх керівників на роботі

Додаток 23

ЗАХИСТ ВІД УРАЖАЮЧИХ ФАКТОРІВ АВАРІЙ ІЗ ВИКИДОМ ОТРУЙНИХ РЕЧОВИН У ПОБУТІ

Негайно покинути місце аварії або осередку, де виявлено сильнодіючі отруйні речовини	У разі отримання сигналу тривоги негайно включити радіоприймачі, телевізори, настроївши їх на місцеві станції	Виконувати всі рекомендації і команди місцевого органу МНС
У разі, якщо загроза отруйних речовин наявна, а команди чи повідомлення відсутні дії щодо захисту необхідно здійснювати самостійно	Зібрати в одному місці всіх членів сім'ї, визначивши місце і час збору	У приміщенні закрити всі вікна та двері і загерметизувати їх, а також загерметизувати всі вентиляційні отвори
Дітям повісити на шию пенали із записками, указавши прізвище, ім'я, по батькові, рік та місце народження, адресу, контактні телефони батьків, родичів та друзів, що знають дітей	Доцільно взути гумові чоботи, прорезинові куртку та штани або плащ чи поліетиленові накидки, на голову капюшон (поліетиленовий пакет), гумові рукавиці. За необхідності зробити ватно-марлеву пов'язку на лице	Залишаючи квартиру, перекрити воду, газ, подання електроенергії. Із собою взяти тільки ті речі, які забезпечують життєдіяльність, документи та цінності
Виходити із зони ураження слід у бік, перпендикулярний напрямку вітру	Уникати розташування в підвалах, балках, підземних переходах, ярах тощо	

Додаток 24

ЗАХИСТ ВІД УРАЖАЮЧИХ ФАКТОРІВ РАДІАЦІЇ

Організація і проведення інструктажу персоналу про правила поведінки в умовах загрози підвищеного фону іонізуючих випромінювань	Пересікати розповсюдження чуток і неправдивих суджень про підвищену небезпеку радіоактивного ураження	Обмеження куріння
Обов'язкове миття рук перед кожним прийомом їжі	Організація періодичного контролю рівня доз радіації на території і в приміщеннях банку	У разі отримання команди або виявлення підвищених рівнів радіоактивного випромінювання негайно вживати заходів для евакуації персоналу
Періодичне поливання (помивка) території банку під'їздів, входів, коридорів і сходових маршів	Забезпечення персоналу респіраторами	Щоденне вологе прибирання робочих приміщень. На входах у них покласти вологі килимки, при вході ретельно витирати взуття
Організація своєчасного інформування персоналу про зміну радіаційної обстановки	При проведенні евакуації вживати заходів щодо недопущення паніки, команди, які подаються, мають бути чіткими, ясними, стислими і зрозумілими, вимагати конкретних і простих дій	Періодичне проведення медичного обстеження персоналу щодо отримання підвищених доз радіації

Додаток 25

ЗАХОДИ ЗАХИСТУ ВІД УРАЖАЮЧИХ ФАКТОРІВ АВАРІЙ ТА КАТАСТРОФ НА ОБ'ЄКТАХ ВИРОБНИЦТВА

А. Попередження аварій і катастроф

Строге дотримання правил та технологій експлуатації виробничих мереж та обладнання	Протиаварійне обладнання об'єктів виробництва	Дотримання заходів техніки безпеки у виробничому процесі
Підготовка персоналу з питань техніки безпеки та на випадок виникнення аварій і катастроф	Своєчасне обслуговування, ремонт виробничого обладнання та проведення профілактичних робіт	Вжиття заходів щодо заміни обладнання, яке відпрацювало встановлений термін

Б. Дії у разі виникнення аварій

Сповіщення персоналу про виникнення аварії та евакуація працівників з небезпечних зон	Вжиття заходів щодо ліквідації пожеж, розчищення завалів, витоку води та ін.	Перекриття подання електроенергії, газу, води на об'єкти де виникла аварія
Сповіщення аварійних служб району про місце та масштаби аварії	Очищення території від непридатних предметів та іншого майна, яке втратило можливість його подальшого використання	

Додаток 26

ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ БАНКУ В УМОВАХ ЕКСТРЕМАЛЬНОЇ СИТУАЦІЇ, ВИКЛИКАНОЇ ТЕХНОГЕННИМИ АВАРІЯМИ І КАТАСТРОФАМИ

Концентрація діяльності на об'єктах, яким не загрожує небезпека, перенесення частини роботи на зазначені об'єкти	Аналіз ушкоджень на об'єктах, які зазнали впливу вражаючих факторів, визначення перспектив відновлення їх роботи	Проведення розрахунків витрат коштів та часу для відновлення роботи об'єктів, які зазнали впливу вражаючих факторів аварії
Формування робочих груп, які будуть задіяні на відновлювальних роботах	Виділення робіт, пов'язаних із відновленням функціонування об'єктів, які зазнали впливу уражаючих факторів аварії в окремий напрям і забезпечення діяльності банку на двох напрямах: основному та відновлювальному	Забезпечення послідовного або паралельного виконання робіт з відновлення виробничих потужностей і будівництва приміщень для їх розташування
Оренда приміщень, обладнання для підтримання необхідних обсягів банківського виробництва	Тимчасове надання лише окремих послуг, з подальшим їх розширенням	Використання можливостей виробничих потужностей, що залишилися неушкодженими у виробництві банківських послуг

Додаток 27

ДІЇ ЛЮДИНИ ПІД ЧАС ЗЕМЛЕТРУСУ

Перебуваючи на першому поверсі, негайно покинути будинок	На другу та інших поверхах зайняти безпечне місце у приміщенні	Не бігати по приміщенню (будинку) під час землетрусу, не бігти по сходах і не користуватися ліфтом
Не виходити на балкони, якщо з нього не можна безпечно вистрибнути на землю	Негайно залишити будівлю після першої серії поштовхів	Залишати будівлю в чому є, похапцем взявши речі, які під рукою
Вибігаючи з будинку, обов'язково прикривати голову від можливого падіння уламків	Якщо ви керівник чи здійснюєте евакуацію людей, команди віддавайте гучним, рівним і спокійним голосом, однозначно зрозумілими разами	При переміщенні в будівлі триматися ближче до стін
Перш ніж здійснити переміщення чи кудись увійти уважно оглянути відповідну зону і впевнитися, що нічого не може загрожувати	Якщо є можливість, слід надати першу медичну допомогу потерпілим	Опинившись у завалі, слід з'ясувати, чи немає когось поряд, подавати сигнали про допомогу; якщо притиснуті якісь частини тіла, слід зробити спроби звільнити їх, але при цьому не вибивати чи розштовхувати уламки. Притиснуті частини слід підкопувати знизу і збоку