**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ**

***Отенко І. П.***
***Мішин О. Ю.***
***Мішина С. В.***

# ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ БАНКІВСЬКИХ УСТАНОВ

**Навчальний посібник**

**Харків. ХНЕУ ім. С. Кузнеця, 2015**

УДК 336.71:005.922.1:33(075)
ББК 65.9-98я7
О-82

Рецензенти: докт. екон. наук, професор, завідувач кафедри економіки і менеджменту Інституту післядипломної освіти Донецького національного університету економіки і торгівлі імені Михайла Туган-Барановського, академік Академії економічних наук України *Лутай Л. А.;* докт. екон. наук, професор, завідувач кафедри менеджменту Харківського національного автомобільно-дорожнього університету *Криворучко О. М.*

**Рекомендовано до видання рішенням вченої ради Харківського національного економічного університету імені Семена Кузнеця.**
Протокол № 3 від 05.11.2012 р.

**Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів (лист № 1/11-9543 від 05.06.2013)**

**Авторський колектив:** докт. екон. наук, професор Отенко І. П. – вступ, теми 3, 4; канд. екон. наук, доцент Мішин О. Ю. – теми 2, 6, 7, глосарій; канд. екон. наук, доцент Мішина С. В. – теми 1, 5, 8 – 10.

**Отенко І. П.**

О-82 Організація та управління фінансово-економічною безпекою банківських установ : навчальний посібник / І. П. Отенко, О. Ю. Мішин, С. В. Мішина. – Х. : ХНЕУ ім. С. Кузнеця, 2015. – 240 с. (Укр. мов.)
ISBN 978-966-676-604-8

Подано лекційні матеріали, тестові та практичні завдання, контрольні запитання, покликані забезпечити знання теоретичних та практичних аспектів і набуття досвіду організації, планування, координації, реалізації та контролю за управлінською діяльністю у сфері фінансово-економічної безпеки банківських установ. Висвітлено питання організації та управління безпекою кредитних, валютних, касових операцій і операцій із цінними паперами.

Рекомендовано для студентів спеціальності 8.18010014 "Управління фінансово-економічною безпекою" всіх форм навчання.

**УДК 336.71:005.922.1:33(075)**
**ББК 65.9-98я7**



ISBN 978-966-676-604-8

# Вступ

Динамічне середовище функціонування суб'єктів господарювання обумовило посилення ролі безпекознавчих дисциплін. Організація та управління фінансово-економічною безпекою банківських установ має свої особливості й тому потребує детального опрацювання.

Об'єктом вивчення дисципліни є процес організації та управління фінансово-економічною безпекою банківських установ.

Предметом вивчення є методи та інструменти ефективного управління фінансово-економічною безпекою банківських установ.

Метою засвоєння дисципліни є вивчення студентами теоретичних основ і набуття практичних навичок в організації та дотриманні фінансово-економічної безпеки в банках.

Завдання навчальної дисципліни: дослідити теоретичні аспекти організації управління фінансово-економічною безпекою банківських установ; розглянути практичні аспекти організації управління фінансово-економічною безпекою банківських установ; вивчити методичне забезпечення оцінювання фінансово-економічної безпеки в банках; розглянути інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою в банківських установах.

Нові підходи, напрями, методи та інструменти управління фінансово-економічною безпекою банківських установ, розширення їх практичного застосування викликають необхідність у підготовці висококваліфікованих спеціалістів із безпеки. Вивчення дисципліни дає можливість набуття досвіду організації, планування, координації, реалізації та контролю за управлінською діяльністю у сфері фінансово-економічної безпеки банківських установ.

У цьому посібнику подано теоретичний матеріал, контрольні запитання, тестові та практичні завдання.

У результаті вивчення дисципліни у студентів має бути сформовано компетентності, тобто здатності виконувати визначені стандартом для магістрів класи професійних завдань (таблиця).

Цифрові дані є умовними й не відображають реальних показників діяльності конкретних банків. Посилання на літературні джерела і джерела інформації, що може бути використано для аналізу, чинні на момент підготовки навчального посібника.

Таблиця

**Опис компетентностей, які набуває та здатен продемонструвати магістр після опанування навчальної дисципліни "Організація та управління фінансово-економічною безпекою банківських установ"**

| Знання | Уміння | Комунікації | Автономність і відповідальність |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Сутність фінансово-економічної безпеки банківських установ;<br>концепція фінансово-економічної безпеки банку;<br>види безпеки і форми її організації;<br>система фінансово-економічної безпеки банку;<br>заходи банку від внутрішніх та зовнішніх загроз;<br>сутність недобросовісної конкуренції та промислового шпигунства, їх вияв у банках; | Визначати політику фінансово-економічної безпеки банків;<br>проектувати систему фінансово-економічної безпеки банківської установи;<br>виконувати функції відділу безпеки банків;<br>розробляти структуру відділу безпеки банку;<br>визначати перелік функцій відділу безпеки банків;<br>розробляти положення про забезпечення фінансово-економічної безпеки банків;<br>формувати механізм управління фінансово-економічною безпекою банку;<br>визначати та передбачати внутрішні й зовнішні загрози банківських установ;<br>розробляти інструкції щодо запобігання шахрайству і зловживанням службовим положенням;<br>уникати ризиків недобросовісного ставлення до виконання службових обов'язків;<br>здійснювати протидію шахрайству та зловживанням | Здійснювати вибір виду нарад, засідань, семінарів із питань фінансово-економічної безпеки банків;<br>розробляти проекти наказів щодо дій в екстремальних умовах;<br>проектувати систему інформаційно-комунікаційних зв'язків банківських установ;<br>організувати дії щодо забезпечення безпеки інформаційно-комунікаційних зв'язків банку;<br>здійснювати організаційні дії з розроблення плану комунікацій | Забезпечити реалізацію механізму управління фінансово-економічною безпекою банків;<br>розробляти пропозиції щодо удосконалення системи управління фінансово-економічною безпекою банків;<br>організувати захист банківської установи від внутрішніх і зовнішніх загроз;<br>розробляти пропозиції щодо використання сучасних технологій зниження загроз та уникнення ризиків |

Продовження таблиці

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| порядок організації охорони та дій банків в екстремальних умовах;<br>організація інформаційної безпеки в банках;<br>забезпечення фінансово-економічної безпеки банків;<br>інформаційно-аналітичне забезпечення діяльності банківських установ;<br>механізм забезпечення безпеки в роботі з персоналом;<br>організація безпеки комп'ютерних технологій і систем у банках | проектувати комплексну систему боротьби з недобросовісною конкуренцією та шпигунством;<br>розробляти плани боротьби з недобросовісною конкуренцією;<br>виявляти факти промислового шпигунства;<br>проектувати систему охорони в банку;<br>організувати забезпечення оптимального режиму охорони в банках;<br>забезпечувати дотримання режиму охорони в банку;<br>здійснювати самоаналіз та коригування особистої діяльності економіста-аналітика як складової частини колективної діяльності установи;<br>приймати рішення за результатами інформаційного аудиту та моніторингу фінансово-економічної безпеки банківських установ;<br>розробляти стратегію фінансово-економічної безпеки банківської установи;<br>організувати роботу щодо забезпечення фінансово-економічної безпеки банківської установи;<br>планувати діяльність банківської установи щодо забезпечення її фінансово-економічної безпеки;<br>забезпечувати фінансово-економічну безпеку виконання банківських операцій та операцій з матеріальними цінностями<br>передбачати виникнення конфліктів та розробляти стратегії їх уникнення; | організувати розробления та виконання заходів щодо захисту інформації та банківської таємниці;<br>визначати потреби в інформації на різних рівнях управління;<br>створювати належні умови для захисту банківських таємниць;<br>розробляти інформаційно-аналітичні документи щодо оцінювання реальних і потенційних загроз фінансово-економічній безпеці банківських установ;<br>організувати систему збирання, відновлення, поширення та зберігання інформації | здійснювати контроль за випадками зловживань і шахрайств;<br>розробляти заходи щодо боротьби із шахрайством і зловживанням;<br>контролювати перебіг недобросовісної конкуренції під час здійснення банківської діяльності;<br>уводити в дію рішення керівництва щодо запобігання шпигунству та недобросовісній конкуренції;<br>здійснювати контроль за дотриманням належного рівня технічного зміцнення банків;<br>надавати рекомендації щодо удосконалення управління охороною в банках;<br>контролювати якість та ефективність організації системи фінансово-економічної безпеки банківської установи; |

Закінчення таблиці

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | створювати належний морально-психологічний клімат у колективі;<br>діагностувати міжособистісні відносини в колективі та їх вплив на стан фінансово-економічної безпеки банківської установи;<br>оцінювати рівень конфліктності членів трудового колективу;<br>розробляти штатний розпис підрозділу фінансово-економічної безпеки банку;<br>проектувати систему безпеки електронних платежів;<br>організувати дії щодо формування та функціонування системи технічного захисту інформації банківських установ;<br>обирати відповідні цілям фінансово-економічної безпеки банківської установи комп'ютерні технології та системи;<br>забезпечувати безпеку використання комп'ютерних технологій і систем у банку;<br>приймати рішення щодо посилення технічного захисту інформації банків;<br>надавати пропозиції щодо накладення на персонал банку, відповідно до законодавства, стягнень за дії, які загрожують безпеці | | здійснювати загальний контроль за діяльністю банківської установи та її структурних підрозділів щодо дотримання фінансово-економічної безпеки;<br>приймати рішення в екстремальних умовах роботи банків;<br>готувати пропозиції щодо розроблення та проведення заходів із посилення фінансово-економічної безпеки банків;<br>розробляти пропозиції щодо вдосконалення управління безпекою банківських операцій;<br>здійснювати загальний контроль за якістю та добросовісністю роботи персоналу банку;<br>контролювати дотримання персоналом банку штатно-фінансової дисципліни та трудового розпорядку |

# 1. Основи безпеки банківської діяльності

**Мета** – дослідити сутність поняття "безпека банку", розглянути види, сили й засоби безпеки банківських установ та діяльність персоналу банку щодо виконання заходів безпеки.

**Ключові поняття:** безпека банку, фінансово-економічна безпека, інформаційна безпека, силова безпека, кадрова безпека, особиста безпека, заходи безпеки банківської діяльності, засоби безпеки банківських установ.

**Основні питання:**

1.1. Сутність безпеки банків, її мета й завдання.

1.2. Види безпеки і форми її організації.

1.3. Сили й засоби безпеки банківських та фінансових установ.

1.4. Діяльність персоналу банку щодо виконання заходів безпеки.

**Література:** [1 – 5; 13; 21; 23; 31; 33].

## 1.1. Сутність безпеки банків, її мета й завдання

Безпека банківської установи є запорукою надійної роботи, плідної співпраці із клієнтами та дотримання банківських нормативів.

У літературних джерелах існують різні підходи до визначення поняття "безпека банку". Так, безпеку розглядають як: стан захищеності; незалежності від негативних дій, впливів; стан ресурсів, потенціалу; стан банку та його відносин; характеристику системи, суб'єкта господарювання; сукупність факторів; міру гармонізації інтересів; здатність досягати мети; процес забезпечення стабільності; комплекс заходів. Найбільш поширеним і, водночас, доцільним є розуміння безпеки як стану захищеності банківських операцій.

**Безпека банківської установи** – стан захищеності банку, за якого забезпечено реалізацію стратегічних цілей і поточних завдань банку, захист від внутрішніх і зовнішніх загроз.

**Економічна безпека банківської установи** – стан захищеності ресурсного забезпечення та інтересів банку, його партнерів і клієнтів, що сприяє уникненню або запобіганню внутрішнім і зовнішнім загрозам та дозволяє забезпечити стабільне функціонування та розширене відтворення з мінімальними втратами для банку.

Теоретичні засади забезпечення банківської безпеки знайшли відображення на рис. 1.1.


Рис. 1.1. **Теоретичні аспекти забезпечення банківської безпеки**

Основними **принципами** банківської безпеки є:

*законність:* заходи, що здійснюють у межах, необхідних для забезпечення безпеки банку, мають ґрунтуватися на чинному нормативному й законодавчому забезпеченні та здійснюватися без його порушення;

*ефективність*: витрати на заходи із забезпечення безпеки мають бути меншими від очікуваних результатів і не мають призводити до погіршення результатів діяльності та стану безпеки банку, перешкоджати реалізації його інтересів;

*компетентності:* реалізація заходів із безпеки має здійснюватися професіоналами, які б не зашкодили гідності й реалізації прав персоналу та клієнтів;

*конфіденційності:* заходи з дотримання безпеки та перевірки дій персоналу повинні мати конфіденційний характер, тобто мати обмежений доступ;

*системності:* управління безпекою має охоплювати всі види банківських операцій, внутрішніх і зовнішніх загроз та діяльність усіх структурних підрозділів;

*цілеспрямованості:* заходи безпеки здійснюють, відповідно до стратегічних цілей та поточних завдань, які вирішує банк, згідно із затвердженою програмою безпеки;

*оперативності:* своєчасності реагування на запобігання загрозам банківській безпеці та їх нейтралізацію;

*гнучкості:* систему управління банківською безпекою має бути побудовано таким чином, щоб реагувати на зміни зовнішнього середовища;

*обізнаності:* персонал банку має бути обізнаним щодо ознак настання загроз безпеці банку.

Надійність та ефективність безпеки визначають шляхом реалізації відповідних вимог [13]:

*Безперервність безпеки.* Забезпечення безпеки має бути постійним. Це безперервний процес, який містить обґрунтування та реалізацію найбільш раціональних форм, методів, способів і шляхів створення, удосконалення і розвитку системи безпеки, безперервне управління нею, контроль за функціонуванням.

*Конкретність безпеки.* Захисту підлягають конкретні об'єкти, загроза яким може завдати шкоди банку.

*Плановість безпеки.* Заходи безпеки не мають бути епізодичними або відставати від фактичних подій. Плановість передбачає запобіжний характер безпеки.

*Активність безпеки.* Постійне прагнення до виявлення загроз банку, своєчасної та ефективної їх нейтралізації.

*Універсальність безпеки.* Заходи безпеки мають перекривати всі можливі напрями виникнення загроз, незалежно від місця їх дії.

*Комплексність безпеки.* Для забезпечення безпеки необхідно застосовувати всі форми й методи захисту та протидії загрозам у повному обсязі.

## 1.2. Види безпеки та форми її організації

Розглядаючи банківську безпеку як багатоступеневу систему слід визначити її види за різними класифікаційними ознаками. Безпеку доцільно класифікувати за ступенем охоплення та змістом (табл. 1.1).

Таблиця 1.1

**Види банківської безпеки**

| Ознаки класифікації | Види безпеки | Характеристики |
|---|---|---|
| 1 | 2 | 3 |
| За ступенем охоплення | особиста | здатність банківського працівника протистояти загрозам власній безпеці, володіючи нормами та правилами безпечної поведінки. Досягають шляхом дотримання персоналом запобіжних заходів, інструкцій із роботи з клієнтами та виконання банківських операцій, правил поведінки персоналу в екстремальних умовах |
| | колективна | здатність підрозділів банку забезпечувати раціональний режим роботи в умовах нестабільності й різноманітних дестабілізаційних факторів. Досягають створенням доброзичливої атмосфери в колективах, виконанням режимних заходів, охороною території, дотриманням правил протипожежної безпеки |
| | корпоративна | безпека єдності функціонування та дотримання корпоративних стандартів і цінностей усім персоналом |
| За змістом | економічна | стан захищеності, за якого забезпечено економічний розвиток і ефективність діяльності банку, захист його фінансових і матеріальних ресурсів, здатність протистояти внутрішнім і зовнішнім загрозам |
| | інформаційна | стан, за якого забезпечено необхідний рівень інформованості керівництва, ефективний захист інформації від зовнішніх і внутрішніх загроз. Забезпечено організацією збирання, опрацювання і зберігання та належного використання інформації |

Закінчення табл. 1.1

| 1 | 2 | 3 |
|---|---|---|
| | правова | забезпечення безпеки банку та захищеності угод і операцій у правовій площині |
| | силова | охорона банківських приміщень, матеріальних цінностей, охоронності грошових коштів та життя персоналу в екстремальних умовах |
| За середовищем дотримання | внутрішня | стан захищеності банку від внутрішніх загроз банківської діяльності |
| | зовнішня | стан захищеності банку від зовнішніх загроз банківської діяльності |
| | комплексна | стан захищеності банку як від внутрішніх, так і від зовнішніх загроз банківської діяльності |

Найбільш важливим видом банківської безпеки є *економічна безпека.* Саме цей вид безпеки забезпечує ефективне функціонування банку та беззбиткову роботу.

Види економічної безпеки:

*фінансова* – стан захищеності банківської установи, який характеризує збалансованість і якість використаних фінансових інструментів, технологій і послуг, що забезпечують достатній рівень ліквідності, платоспроможності та прибутковості банку. У переважній більшості джерел такий вид безпеки називають фінансово-економічною;

*кадрова* – стан захищеності банківської установи, що полягає в забезпеченні безпеки в роботі з персоналом, контролі за дотриманням банківської таємниці, запобіганні промисловому шпигунству, крадіжкам;

*ринкова* – стан банківської установи, який дозволяє реалізувати потенціал банку на ринку банківських послуг за допомогою маркетингових інструментів, спрямованих на забезпечення стійких конкурентних переваг, захист від недобросовісної конкуренції;

*операційна* – стан захищеності банківської установи, що полягає в дотриманні безпечного здійснення банківських операцій, запобіганні витоку інформації про банківські операції.

Заходи безпеки банку реалізують у таких формах [13]:

охорони (фізичної та технічної);

режиму (упровадження відповідної системи захисту інформації банку);

інформаційно-аналітичного забезпечення діяльності банку (комерційної розвідки).

Конкретний перелік заходів із безпеки банківської діяльності наведено в табл. 1.2.

Таблиця 1.2

**Заходи безпеки банківської діяльності**

| Групи заходів | Перелік заходів |
|---|---|
| Проектні | оцінювання кредитоспроможності позичальників;<br>інформаційно-аналітичні дослідження рівня безпеки співпраці із клієнтами;<br>заходи комерційної розвідки |
| Термінові | заходи щодо нейтралізації конкретних випадків промислового шпигунства;<br>протидія недобросовісній конкуренції;<br>припинення витоку комерційної інформації |
| Постійні загального характеру | взаємодія із правоохоронними органами та охоронними агентствами;<br>ретельний підбір персоналу;<br>забезпечення охорони банківських приміщень;<br>захист банківської інформації;<br>формування позитивного іміджу банку |

## 1.3. Сили й засоби безпеки банківських та фінансових установ

Суб'єкти безпеки виконують заходи безпеки з використанням різноманітних засобів.

Виконувати ці заходи банки можуть:

власними силами (підрозділи безпеки банку, персонал банку, охорона банку);

силами сторонніх організацій (спеціалізовані фірми, організації, які надають банкам послуги безпеки, охоронні агентства, правоохоронні органи).

Засоби безпеки містять:

технічні засоби охорони;

програмні й технічні засоби захисту інформації;

спеціальні засоби й техніку;

інженерно-технічні засоби обмеження доступу;

засоби зв'язку, опрацювання і передання інформації;

обладнання для відеоспостереження.

Практичну реалізацію заходів безпеки може бути організовано шляхом створення та забезпечення функціонування системи управління безпекою банку.

Сили й засоби безпеки визначають факторами впливу на банківську безпеку. Їх класифікацію наведено в табл. 1.3.

Таблиця 1.3

**Класифікація факторів, що визначають рівень банківської безпеки**

| Ознаки класифікації | Назви факторів | Характеристики факторів |
|---|---|---|
| За середовищем виникнення | Зовнішні | Дія факторів виявляється за межами банку |
| | Внутрішні | Дія факторів виявляється в банку |
| | Змішані | Дія факторів виявляється як за межами банку, так і в самій установі |
| За характером впливу | Прямі | Наявність причинно-наслідкового зв'язку між впливом факторів і рівнем банківської безпеки |
| | Опосередковані | Не мають прямого впливу на рівень банківської безпеки |
| За змістом | Економічні | Пов'язані з виконанням банківських операцій |
| | Фінансові | Пов'язано з можливістю дотримання ліквідності, банківських нормативів, зростанням прибутковості |
| | Демографічні | Вплив процесів природного й міграційного приросту населення на обсяги діяльності банківських установ |
| | Макроекономічні | Соціально-економічна ситуація у країні |
| | Правові | Законодавче й нормативне забезпечення банківської діяльності |
| | Криміногенні | Криміногенна ситуація у країні, регіоні, районі |
| За часовою ознакою | Реальні | Дія факторів виявляється у звітному періоді |
| | Потенційні | Дія факторів може виявитися в майбутньому |
| За ступенем імовірності | Імовірні | Вплив факторів можливий за будь-яких обставин |
| | Малоймовірні | Вплив факторів можливий за певних обставин |
| | Неймовірні | Вплив факторів швидше за все не виявиться |

## 1.4. Діяльність персоналу банку щодо виконання заходів безпеки

Забезпечення безпеки в банку здійснюють безпосередньо відділ банківської безпеки. Проте керівництво банку має здійснювати визначення пріоритетних засад політики у сфері безпеки підприємства і приймати кінцеві рішення щодо заходів безпеки.

Колектив банку, з одного боку, є об'єктом безпеки, а з іншого – суб'єктом, тобто має сприяти підтримці належного рівня безпеки, сповіщати відділ безпеки про настання внутрішніх чи зовнішніх загроз.

Відповідальність керівного складу банку полягає в такому:

розробленні й затвердженні політики банківської безпеки;

організації безпеки банківської діяльності;

контролі за виконанням заходів із банківської безпеки;

загальному контролі за дотриманням банківської безпеки.

*Відповідальність начальника структурного підрозділу* з управління безпекою полягає в такому:

організації та ефективному виконанні заходів безпеки;

своєчасному інформуванні керівного складу банку про виникнення загрози;

запобіганню недобросовісній конкуренції, промисловому шпигунству.

*Функціональні обов'язки керівника банку* з питань забезпечення безпеки [13]:

визначення мети та основних напрямів забезпечення безпеки банківської діяльності;

формулювання наказів про створення відділу безпеки, склад банківської й комерційної таємниць, уведення режимних заходів у структурних підрозділах банку, формулювання внутрішніх правил трудового розпорядку, а також переліку осіб, допущених до банківської й комерційної таємниці в повному обсязі;

ставлення завдань структурним підрозділам банку щодо підсилення безпеки банківської діяльності, відповідно до впливу різних факторів зовнішнього середовища (політичних, економічних, правових, соціальних) або змін у стратегії й тактиці діяльності банку;

контроль за станом банківської безпеки та оцінювання звітів начальника підрозділу (управління, служби, відділу) безпеки про заходи, що здійснюють задля закриття каналів витоку конфіденційної інформації, виконання встановленого режиму в його підрозділах;

здійснення заходів щодо нематеріального й матеріального стимулювання працівників за ефективне виконання заходів безпеки.

*Посадові обов'язки працівників банку* щодо виконання вимог банківської безпеки [13]:

дотримання встановленого в банку режиму охорони;

зберігання в таємниці всієї інформації, про яку відомо працівникові банку в межах виконання посадових обов'язків, контроль за службовцями щодо розголошення відомостей, які є банківською чи комерційною таємницею або його конфіденційною інформацією;

виконання встановленого порядку і правил документообігу, а також дотримання безпеки із клієнтами, позичальниками, партнерами;

надання для перевірки всіх матеріалів, закріплених за працівником банку, у яких є відомості, що становлять банківську або комерційну таємницю чи конфіденційну інформацію банку;

надання пояснень щодо порушення встановлених правил виконання посадових обов'язків, фактів розголошення таємниці, утрати документів таємного та конфіденційного характеру;

повідомлення безпосереднього керівника й керівника служби безпеки про втрату або нестачу документів, що містять банківську чи комерційну таємницю, посвідчень, перепусток, ключів від режимних приміщень, сховищ, сейфів, особистих печаток, а також про причини та умови можливої втрати закритої інформації;

дотримання встановлених правил і порядку виконання банківських операцій, запобігання завданню збитків або шкоди банку, порушенням, установленим у банку заходам безпеки;

дотримання встановлених банком правил ведення службових переговорів і передання інформації на всіх лініях зв'язку, правил користування копіювальною технікою та програмними засобами;

забезпечення відсутності на робочих місцях та у приміщеннях банку кіно-, відео- і фотоапаратури персоналу;

запобігання використанню технічних засобів банку з корисливою метою та як розважальних засобів;

забезпечення необхідного рівня доступу до інформації як працівника, який відповідає за її збирання, опрацювання і зберігання, так і інших працівників;

повідомлення безпосереднього керівника та керівника служби безпеки в разі спроб несанкціонованого доступу до конфіденційної інформації сторонніх осіб чи організацій.

**Семінарське заняття**

*Мета* – розгляд сутності безпекознавчих понять, засвоєння теоретичних основ організації управління фінансово-економічною безпекою банківських установ.

1. Етимологія поняття "фінансово-економічна безпека банку".

2. Сутність та види економічної безпеки банків.

3. Організація управління фінансово-економічною безпекою діяльності комерційного банку.

4. Безпека діяльності комерційних банків як складова частина безпеки функціонування банківської системи країни.

5. Роль і місце безпеки банківської діяльності в забезпеченні фінансової безпеки держави.

6. Ефективність безпеки банківської діяльності та шляхи досягнення її високого рівня.

7. Діяльність персоналу банку щодо посилення безпеки.

8. Характеристика засобів безпеки.

**Тематика доповідей**

1. Порівняльна характеристика визначень поняття "фінансово-економічна безпека" різних авторів.

2. Роль кадрової безпеки в безпечному функціонуванні банківських і фінансових установ.

3. Місце інформаційної безпеки в системі управління безпекою банку.

4. План заходів із забезпечення фінансово-економічної безпеки банку.

**Практичні завдання для самостійного виконання**

Дати рекомендації щодо вирішення ситуації. Обґрунтувати відповідь:

1. Прийняти й обґрунтувати рішення щодо надання кредиту клієнтові банку. Відомості про клієнта: фірма має добрий фінансовий стан, високі темпи зростання чистої виручки, працює прибутково, має перспективи розширення ринків збуту; продукція, що реалізує фірма, має високу якість. Проте реалізують без сертифікатів якості. Фірму не було викрито жодного разу. Загалом фінансово-економічні показники підприємства стабільні, існують порушення тільки щодо підтвердження належної якості наданих фірмою товарів.

2. Прийняти рішення щодо виправлення похибок у фінансових документах банківської установи. Описати порядок дій. Опис ситуації: ви працюєте на посаді касира в банку і в цей час виконуєте обов'язки завідувача каси. Досвід роботи на цій посаді 18 років. Одного разу до вас звернувся касир щодо нестачі 500 грн у касі, пояснивши, що нестачу

пов'язано з описку у фінансових документах двомісячної давності. Касир пропонував вам зробити виправлення в документах, мотивуючи це тим, що завідувач каси, який перебуває у відпустці, теж робив такі виправлення в касових документах.

3. Пояснити дії начальника відділу розрахунково-касового обслуговування банківської установи в разі, якщо до нього надійшла інформація про те, що один із працівників банку займається списанням грошей із карткових рахунків клієнтів.

## Методичні рекомендації щодо виконання самостійної роботи

Практичні завдання виконують після опрацювання джерела [13] та цього навчального посібника.

Теоретичні питання до семінарського заняття опрацьовують на основі літературних джерел: [1 – 5; 13; 21; 23; 31; 33].

## Контрольні запитання

1. Розкрити сутність безпеки банків, мету й завдання.
2. Охарактеризувати принципи безпеки банків.
3. Розкрити сутність різних видів безпеки банківських установ.
4. Охарактеризувати форми організації банківської безпеки.
5. Дати порівняльну характеристику засобів безпеки банківських установ.
6. У чому полягає діяльність персоналу банку щодо виконання заходів безпеки?
7. Що становлять особиста та колективна безпека банківських установ?
8. Розкрити сутність поняття "економічна безпека банку".
9. Із якими видами банківської безпеки пов'язано інформаційну безпеку?

## Тести

*Тести одиничного вибору*

1. Основна мета забезпечення безпеки банку:

а) виключити можливість завдання збитків або упущення вигоди та забезпечити ефективну діяльність банку і якісну реалізацію всіх операцій та угод;

б) досягнути стабільність функціонування банку;

в) забезпечити беззбитковість діяльності банку;
г) усі варіанти правильні.
2. До функцій безпеки банківської діяльності не включено:
а) інформаційну;
б) аналітичну;
в) соціально-диференційну;
г) застережно-профілактичну;
д) оперативно-інформаційну;
е) організаційно-захисну.
*Тести множинного вибору*
3. Принципи банківської безпеки такі:
а) законність;
б) самостійність і відповідальність;
в) економічна доцільність;
г) компетентність;
д) цілеспрямованість;
е) координація і взаємодія;
є) конфіденційність;
ж) масовість.
4. Заходи безпеки банківської діяльності розподіляють на:
а) загального і спеціального характеру;
б) основні та другорядні;
в) важливі та неважливі;
г) первинні та вторинні.
*Тести на встановлення відповідності*
5.1. Система безпеки банківської діяльності містить:
5.2. Процес управління безпекою банківської діяльності містить:
а) сили безпеки;
б) засоби безпеки;
в) технології безпеки;
г) функції безпеки;
д) етапи управління безпекою.
6.1. Принцип самостійності та відповідальності означає:
6.2. Принцип законності означає:
6.3. Принцип економічної доцільності означає:

6.4. Принцип компетентності означає:

а) заходи, що виконують в межах забезпечення безпеки, мають ґрунтуватися на чинному законодавстві;

б) підрозділи безпеки банку повинні мати у своєму розпорядженні всі необхідні засоби для ефективного вирішення поставлених перед ними завдань у межах повноважень;

в) заходи безпеки мають давати більш суттєвий результат, ніж сума витрат на організацію їх здійснення;

г) заходи безпеки організовувати та здійснювати мають фахівці відповідного професійно-кваліфікаційного рівня.

7. Економічна безпека банку – це:

а) безпека єдності функціонування та дотримання корпоративних стандартів і цінностей усім персоналом;

б) стан захищеності, за якого забезпечено економічний розвиток і ефективність діяльності банку, захист його фінансових і матеріальних ресурсів, здатність протистояти внутрішнім і зовнішнім загрозам;

в) стан захищеності фінансових ресурсів банку;

г) діяльність банку щодо протидії фінансовим загрозам банку.

# 2. Організація управління фінансово-економічною безпекою в банку

**Мета** – вивчити теоретичні засади організації управлінської діяльності у сфері фінансово-економічної безпеки банку.

**Ключові поняття:** об'єкти захисту, система фінансово-економічної безпеки, відділ безпеки, стратегія фінансово-економічної безпеки банку, фактори безпечного функціонування банку.

**Основні питання:**

2.1. Сутність та роль фінансово-економічної безпеки в банку.

2.2. Об'єкти та система фінансово-економічної безпеки.

2.3. Структура відділу безпеки в банку.

2.4. Функції відділу безпеки

**Література:** [6 – 9; 13; 19; 21; 23; 31; 33].

## 2.1. Сутність та роль фінансово-економічної безпеки в банку

Сьогодні не достатньо просто створити відділ фінансово-економічної безпеки (ФЕБ). Слід чітко усвідомлювати його роль у забезпеченні стійкого функціонування підприємства. Вона полягає, перш за все, у нейтралізації та уникненні внутрішніх і зовнішніх загроз підприємства.

У літературі часто мова йде про фінансову безпеку як кількісно і якісно визначений рівень фінансового стану банку, що забезпечує стабільну захищеність його пріоритетних збалансованих фінансових інтересів від реальних і потенційних загроз зовнішнього та внутрішнього характеру. На думку багатьох учених, сутність фінансової безпеки полягає у здатності банку самостійно розробляти та здійснювати фінансову стратегію, відповідно до цілей корпоративної стратегії, в умовах невизначеного й конкурентного середовища.

Щодо фінансової безпеки, то вона є невід'ємною складовою частиною безпеки і, водночас, є нерозривною з економічною складовою. Тому щодо банківських установ доцільним є розгляд бажаного фінансового стану у взаємозв'язку з економічними показниками результативності його функціонування.

Ґрунтуючись на ключових характеристиках фінансової та економічної безпеки, ураховуючи трактування різними науковцями, доцільним є визначення фінансово-економічної безпеки банку як динамічного стану захищеності банківських операцій та фінансових ресурсів, що сприяє уникненню або запобіганню внутрішнім і зовнішнім економічним загрозам і дозволяє забезпечити стабільний фінансовий стан та рентабельну роботу з мінімальними ризиками і втратами для банку.

Проблеми фінансово-економічної безпеки мають два аспекти. З одного боку, необхідно працювати над забезпеченням фінансової безпеки банківської системи загалом, а з іншого – потрібно також досліджувати питання забезпечення фінансової безпеки окремої банківської установи.

Фінансово-економічну безпеку окремого банку тісно пов'язано з безпекою банківської системи загалом. Вони впливають одна на одну. Часто проблеми, що виникли в одному банку, можуть спричинити кризу неплатежів, відплив депозитів, утрату клієнтів і в підсумку недовіру до банківської системи загалом.

Безпечне і стабільне функціонування конкретних банків є запорукою фінансово-економічної безпеки всієї національної банківської системи.

Забезпечення належного рівня фінансово-економічної безпеки банківської установи можливе за таких умов:

1) чіткого визначення мети, завдань та принципів управління фінансово-економічною безпекою;

2) обов'язкового здійснення моніторингу внутрішніх та зовнішніх загроз;

3) формування та постійного оновлення банку даних про внутрішні й зовнішні загрози банку;

4) визначення переліку підсистем управління фінансово-економічною безпекою банку;

5) формування банку методів та інструментів нейтралізації та уникнення загроз;

6) обов'язкового оцінювання результатів роботи відділу фінансово-економічної безпеки.

У ході формування системи управління фінансово-економічною безпекою слід ураховувати її спрямування на забезпечення стану захищеності від загроз та рентабельного функціонування банку.

Під забезпеченням економічної безпеки банку (ЕББ) розуміють діяльність менеджерів і персоналу, спрямовану на запобігання порушенням стабільності функціонування й економічного розвитку банку, унаслідок негативних дій на його корпоративні ресурси з боку зовнішніх і внутрішніх джерел загроз. Джерела загроз – це потенційні антропогенні, техногенні або стихійні носії загрози [13].

До основних корпоративних ресурсів банку, що використовують для забезпечення фінансово-економічної безпеки, загалом можна зарахувати [13]:

майно банку, включаючи засоби технологічного оснащення та інші матеріальні цінності;

фінансові можливості банку за наявної структури капіталу і практики використання основних та оборотних коштів;

кадрові можливості банку, перш за все, компетентність і професіоналізм менеджерів та рівень кваліфікації персоналу;

інформаційні ресурси банку, зокрема матеріальні носії інформації, які містять комерційну, банківську та інші таємниці банку, що охороняють законом;

технології та об'єкти інтелектуальної власності банку.

## 2.2. Об'єкти та система фінансово-економічної безпеки

Для забезпечення правильності застосування та ефективності заходів фінансово-економічної безпеки доцільним є уточнення понятійно-категорійного апарату.

Визначення поняття "система управління фінансово-економічною безпекою банку" сформульовано виходячи зі змісту понять, що його утворюють, а саме таких, як "система", "управління", "фінансово-економічна безпека".

Сутність поняття "система" слід трактувати як сукупність взаємопов'язаних, взаємодійних та взаємообумовлених елементів, що забезпечують формування якісно нової цілісності.

Поняття "управління" є багатогранним і має велику кількість трактувань. Слід зауважити, що управлінська діяльність – це не просто сукупність послідовних дій, а циклічний процес, який повторюється. А, отже,

процес управління – це замкнутий управлінський цикл, який постійно повторюється і має цілеспрямований характер.

Водночас слід зазначити, що вчені по-різному трактують сутність терміна "управління". Управління як циклічний процес такі автори, як Кизим М. О., Забродський В. А., Зінченко В. А., Копчак Ю. С., розглядають із позицій трьох підходів: структури, змісту (функцій) і процесу [15].

Ґрунтуючись на визначенні управління як цілеспрямованого впливу суб'єкта управління (керівної підсистеми) на об'єкт управління (керовану підсистему), що забезпечує зберігання, функціонування і розвиток системи [15] під системою управління фінансово-економічною безпекою банку запропоновано розуміти оптимальну сукупність взаємопов'язаних і взаємодіючих функцій і підсистем, які сприяють уникненню або запобіганню внутрішнім і зовнішнім економічним загрозам і дозволяють забезпечити стабільний фінансовий стан та рентабельну роботу з мінімальними ризиками і втратами для банку.

Забезпечення фінансово-економічної безпеки банку потребує створення на підприємстві власної системи безпеки.

Ефективна система управління фінансово-економічною безпекою банку має ґрунтуватися на:

чітко окреслених бізнес-процесах;

ефективній організаційній структурі;

роботі кваліфікованого та вмотивованого персоналу;

наявній ефективній стратегії розвитку;

чітко визначених тактичних цілях управління.

Головною метою забезпечення фінансово-економічної безпеки банку можна вважати досягнення максимальної стабільності його функціонування та створення умов для подальшого фінансово-економічного розвитку шляхом запобігання внутрішнім і зовнішнім загрозам.

У свою чергу, забезпечення фінансово-економічної безпеки діяльності банку потребує створення власної системи фінансово-економічної безпеки (рис. 2.1).

Система управління фінансово-економічною безпекою має включати керовану, керівну й підсистему забезпечення управління. Кожна підсистема також має свою структуру і складові частини, що забезпечують її належне функціонування.

Так, керована підсистема містить об'єкти управління, внутрішні й зовнішні загрози фінансово-економічній безпеці.

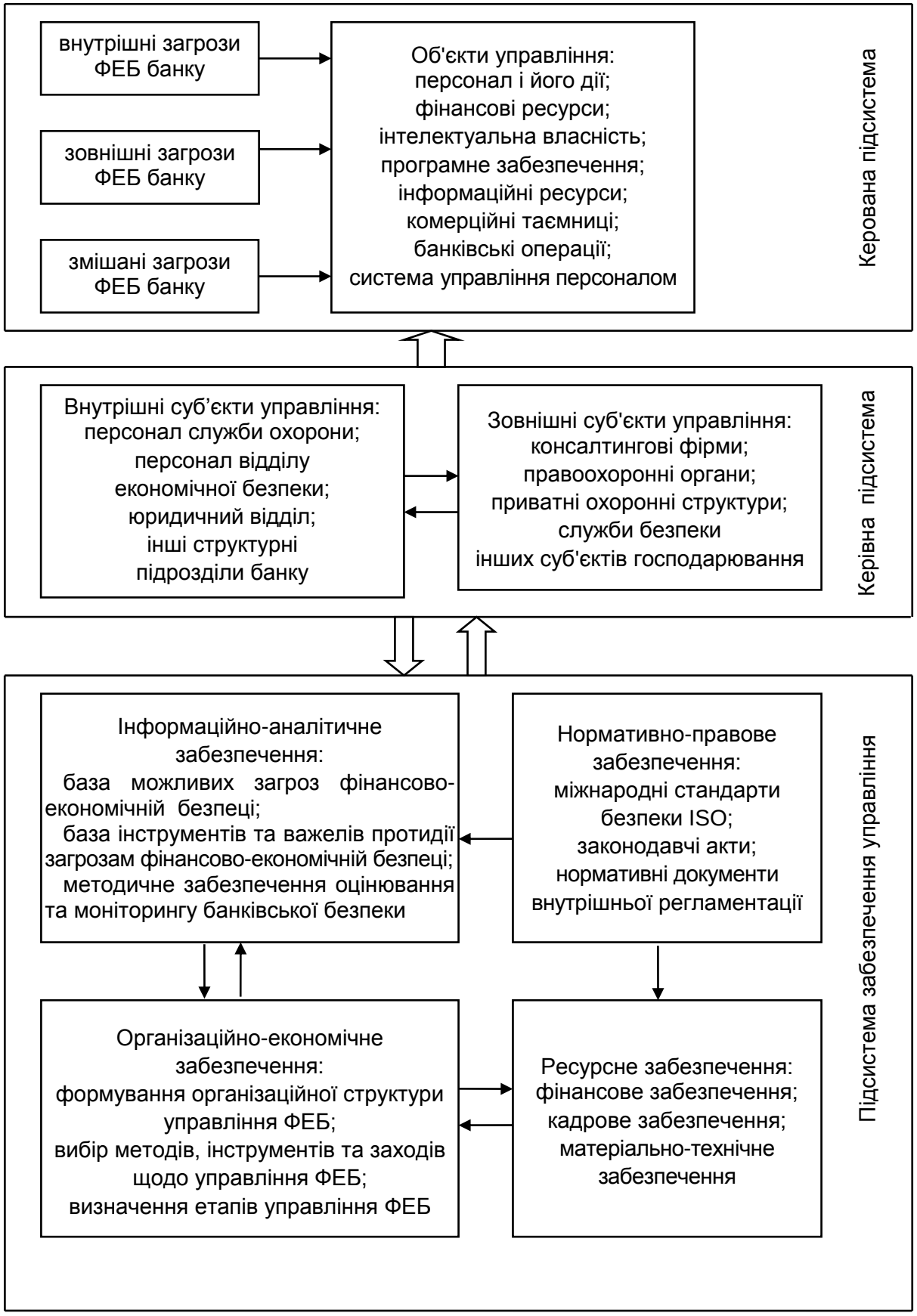


Рис. 2.1. **Структура системи управління фінансово-економічною безпекою банківських установ**

Серед об'єктів виділено: персонал і його дії, фінансові, матеріально-технічні ресурси, банківські операції, інтелектуальну власність, програмне забезпечення, систему управління персоналом та комерційні таємниці.

Керівна підсистема містить внутрішні й зовнішні суб'єкти.

До зовнішніх суб'єктів належать: обслуговчі й консалтингові фірми, правоохоронні органи, приватні охоронні структури, служби безпеки інших суб'єктів господарювання.

До внутрішніх суб'єктів належать: служба охорони, персонал служби економічної безпеки, юридичний відділ та інші структурні підрозділи.

Підсистема забезпечення управління фінансово-економічною безпекою містить інформаційно-аналітичне, нормативно-правове, організаційно-правове та ресурсне забезпечення.

Керівна підсистема має прямий вплив на керовану і водночас впливає на формування елементів підсистеми забезпечення управління фінансово-економічною безпекою. Остання підсистема впливає на характер управлінських дій суб'єктів безпеки. Ця система має універсальний характер і її може бути використано, а в подальшому й адаптовано до специфіки функціонування будь-яких банківських установ.

## 2.3. Структура відділу безпеки в банку

Відділ банківської безпеки створено, відповідно до цілей та видів банківських операцій.

Фактори, що впливають на структуру відділу безпеки банку:

форми та засоби безпеки, які банк має потенційну можливість застосувати;

фінансові можливості банку;

політика банку з питань організації безпеки;

масштаби та обсяги діяльності банку;

організаційна структура банку.

Можлива структура підрозділу (служби, управління, департаменту) безпеки може бути такою:

керівник підрозділу;

сектор фінансового моніторингу, що займається контролем за ключовими фінансовими показниками банку та виявленням фактів тероризму;

сектор оперативного реагування, куди для оперативного вирішення проблем, що раптово виникають, залучають, переважно, фахівців у сфері юриспруденції та банківських технологій;

сектор охорони (може містити такі групи: охорони території й об'єктів, інкасації, особистих охоронців, технічних засобів охорони);

інформаційно-аналітичний сектор (може містити такі групи: збирання інформації, опрацювання інформації, зв'язків із пресою, технічну);

сектор інформаційної безпеки (може містити такі групи: режимну; психологічного контролю; зовнішнього захисту – для взаємодії з правоохоронними органами, підрозділами безпеки інших банків, охоронними та детективними фірмами, органами влади; фінансової безпеки; технічну);

сектор кадрової безпеки здійснює перевірку персоналу щодо зловживань, шахрайств, судимості; сприяє запобіганню витоку інформації та промисловому шпигунству.

## 2.4. Функції відділу безпеки

Відділ безпеки банку здійснює функціонування на основі Положення про відділ безпеки банку та посадових інструкцій працівників цього відділу.

Відділ безпеки банку має виконувати такі **функції** [13]:

*адміністративно-розпорядницьку* – реалізують шляхом розроблення, установлення і підтримання в банку різних режимів безпеки, визначення повноважень, прав, обов'язків і відповідальності службовців банку з питань забезпечення безпеки;

*обліково-контрольну* – забезпечують організацією своєчасного виявлення реальних і потенційних загроз діяльності банку, контролю за джерелами таких загроз та несприятливими для банку ситуаціями та факторами; виявленням критичних напрямів фінансово-комерційної діяльності банку; накопиченням інформації із проблем забезпечення безпеки банку;

*соціально-кадрову* – реалізують шляхом участі підрозділу безпеки в підборі, перевірці та розміщення кадрів; виявлення негативних тенденцій у колективах підрозділів банку, можливих причин та умов виникнення соціальної напруги; запобігання можливим конфліктам і їх локалізації; формування у службовців банку почуття відповідальності за забезпечення безпеки банку;

*організаційно-управлінську* – реалізують за допомогою організаційного, матеріально-технічного і технологічного забезпечення режимів безпеки в банку;

*методичну* – реалізують шляхом виявлення, накопичення і впровадження в банку позитивного досвіду із проблем банківської безпеки; організації навчання працівників банку з питань безпеки; розроблення методик роботи персоналу банку і підрозділу безпеки щодо забезпечення безпеки здійснення банківських операцій;

*інформаційно-аналітичну* – забезпечують шляхом цілеспрямованого збирання, накопичення, опрацювання і розподілу відповідної інформації; створення для цього необхідних технічних і програмних засобів.

## Практичне заняття

*Мета заняття* – формування навичок в організації управління фінансово-економічною безпекою в банку.

**Завдання 2.1.** Прийняття рішення про надання послуг клієнтам банку.

Завдання може виконувати кожен студент як індивідуально, так і у процесі ділової гри. Тривалість виконання завдання 20 – 30 хвилин. Для ділової гри групу розподіляють на команди з 5 – 7 осіб. Кожна з команд отримує вихідні дані про потенційного клієнта. Аналізує їх і обґрунтовує свою точку зору щодо доцільності співпраці із клієнтом. У підсумку обирають команду, що дала найбільш вдалу й обґрунтовану відповідь.

*Вихідні дані для виконання завдання:*

Автотранспортне підприємство "Автотранс" звернулося в банк із клопотанням щодо відкриття зарплатного проекту та договору про розрахунково-касове обслуговування. Підприємство здійснює міські перевезення пасажирів. На трьох кінцевих зупинках міста потрібно здійснювати обідню та вечірню інкасацію коштів, отриманих під час перевезення пасажирів. Кількість персоналу підприємства становить 120 осіб. Виручка від надання транспортних послуг щоденно становить близько 30 тис. грн. Заробітну платню працівникам підприємства сплачують не завжди вчасно. Існує значна заборгованість із заробітної платні. Відсоток за розрахунково-касове обслуговування, прийнятний для підприємства, має бути не більш ніж 0,5 %. Підприємство працює збитково. Проте існує перспектива

розширення обсягів пасажирських перевезень та збільшення кількості обслуговуваних маршрутів.

*Методичні рекомендації щодо виконання завдання*

Завдання виконують поетапно:

1) складання бліц-резюме потенційного клієнта і відображення інформації на аркуші формату А2 за схемою, наведеною на рис. 2.2:

| **Бліц-резюме потенційного клієнта** |
|---|
| Предмет співробітництва з банком: |
| Повна назва клієнта: |
| Вид діяльності: |
| Обсяги діяльності: |
| Кількість персоналу: |
| Перспективи розвитку: |

Рис. 2.2. **Структура бліц-резюме потенційного клієнта банку**

2) аналіз сильних і слабких сторін потенційного клієнта. Здійснено командами з наданням результатів на аркуші паперу за схемою, наведеною на рис. 2.3.

| Можливості й загрози / Сильні та слабкі сторони | **Потенційні можливості** очікувані банком від співпраці із клієнтом | **Загрози** банківській безпеці |
|---|---|---|
| **Сильні сторони** (переваги для банку від співпраці із клієнтом) | | |
| **Слабкі сторони** (ускладнення для банку, що можуть виникнути у процесі співпраці із клієнтом) | | |

Рис. 2.3. **Матриця SWOT-аналізу доцільності співпраці з потенційним клієнтом** (заповнюють студенти у процесі ділової гри)

Команди мають якнайповніше визначити та вказати:

сильні сторони співпраці з потенційним клієнтом, а саме переваги для банку та потенційні можливості очікувані від співпраці;

слабкі сторони співпраці, а саме загрози та ускладнення для банку, що можуть виникнути у процесі співпраці із клієнтом;

3) обговорення бліц-резюме потенційного клієнта та сильних і слабких сторін співпраці з ним для банку;

4) прийняття й обговорення рішення про співпрацю з потенційним клієнтом.

**Завдання 2.2.** Формування організаційної структури відділу фінансово-економічної безпеки.

У головному управлінні банку в Харківській області прийнято рішення про створення відділу безпеки. Цей відділ має обслуговувати 15 філій банку. Кількість персоналу в цих філіях становить 148 осіб. Кількість персоналу в головному управлінні банку – 71 особу. Банк займається кредитуванням як фізичних, так і юридичних осіб, здійснює всі види банківських операцій. Сформувати організаційну структуру відділу безпеки.

*Методичні рекомендації щодо виконання завдання*

Показати схематично місце відділу безпеки у структурі головного управління банку. Зобразити схематично структуру відділу безпеки, взаємозв'язок працівників із іншими структурними підрозділами банку.

**Завдання 2.3.** Ситуаційні вправи, що характеризують дотримання фінансово-економічної безпеки начальниками відділів банківської установи.

1. Підприємство не є клієнтом банку і вперше звернулося за наданням кредиту. Кредитна історія цього клієнта в банку відсутня.

Підприємство є сільгоспвиробником і хотіло б взяти кредит під заставу майбутнього врожаю озимих культур. Сільгоспвиробник має непоганий фінансово-майновий стан. Це підтверджено результатами аудиторської перевірки. Проте в бюро кредитних історій є інформація про непогашені підприємством кредити, узяті в минулому році під майбутній урожай. Які дії кредитного інспектора? Чи може бути надано кредит позичальнику під заставу майбутнього врожаю?

2. Ви працюєте на посаді начальника операційного відділу банківської установи. До вас звернувся колега із проханням виконати операції на вашому комп'ютері з доступом через ваш логін і пароль. Які будуть

ваші дії щодо надання дозволу на виконання такої операції? Чи є цій ситуації ознаки порушення інформаційної безпеки?

3. Ви як начальник кредитного відділу анонімно отримали інформацію про те, що один із кредитних працівників за певну винагороду гарантує клієнтам отримання кредиту, навіть якщо ті не виконують вимоги щодо об'єкта застави. Ваші дії щодо підтвердження отриманої анонімної інформації.

## Тематика доповідей та рефератів

1. Посадові інструкції працівників відділу економічної безпеки фінансових і банківських установ.
2. Етимологія поняття "фінансова безпека".
3. Особливості організації управління фінансово-економічною безпекою банківських установ.
4. Особливості організації управління фінансово-економічною безпекою фінансових установ.
5. Оптимальна структура системи управління фінансово-економічною безпекою банку.

## Практичні завдання для самостійного виконання

Дати рекомендації щодо вирішення ситуації. Обґрунтувати відповідь.

*Ситуаційні вправи:*

1. Начальник відділу безпеки регіонального відділення банку подав на розгляд правління банку проект кошторису витрат, необхідних на посилення інформаційної безпеки у філіях банку та регіональному відділенні. Члени правління дали згоду на закупівлю сучасних програмних засобів. Проте сумнівним стало придбання засобів відеоспостереження для всіх структурних підрозділів регіонального відділення та філій банку. Чому у правління виникли сумніви? Яким чином начальник відділу безпеки регіонального відділення банку міг би обґрунтувати доцільність впровадження засобів відеоспостереження?

2. Ви обіймаєте посаду начальника відділу депозитних операцій. Ваш знайомий – слідчий прокуратури міста – звернувся до вас за допомогою. В усній формі він запросив інформацію про всі депозитні рахунки одного із клієнтів банку. Цей клієнт є доволі відомою в місті особою, що має успішний бізнес, займається благодійністю, є спонсором дитячих будинків міста. Які ваші дії? Чи надасте ви інформацію слідчому і у якій формі (усній чи письмовій)?

3. Ви працюєте на посаді старшого кредитного інспектора в банку і виявили канал витоку інформації про реальних та потенційних клієнтів банку. Витік інформації ініційований начальником відділу кредитної безпеки. Які ваші дії щодо припинення витоку інформації. До кого ви маєте звернутися з підозрами щодо витоку банківської інформації?

## Методичні рекомендації щодо виконання самостійної роботи

Практичні завдання виконують після опрацювання джерела [13].

Теоретичні питання опрацьовують на основі літературних джерел: [6 – 9; 13; 19; 21; 23; 31; 33].

## Контрольні запитання

1. Навести приклад узагальненої структури відділу безпеки банку.
2. Які функції має виконувати відділ безпеки банку?
3. Назвати об'єкти фінансово-економічної безпеки банківської установи.
4. Описати структуру системи фінансово-економічної безпеки банківської установи.
5. Дати визначення та розкрити сутність фінансово-економічної безпеки банківської установи.
6. Проаналізувати зарубіжний досвід формування структури відділу безпеки банку.
7. Охарактеризувати внутрішньополітичні, економічні та правові умови організації безпеки банків.
8. У чому полягає сутність адміністративно-розпорядницької функції відділу безпеки банківських установ?
9. Розкрити сутність соціально-кадрової та методичної функцій відділу безпеки банку.
10. Назвати обов'язки керівника підрозділу безпеки банківської установи.

## Тести

*Тести одиничного вибору*

1. Адміністративно-розпорядницьку функцію відділу безпеки банку:

а) реалізують шляхом розроблення, встановлення і підтримання в банку різних режимів безпеки, визначення повноважень, прав, обов'язків і відповідальності службовців банку з питань забезпечення безпеки;

б) забезпечують організацією своєчасного виявлення реальних і потенційних загроз діяльності банку;

в) полягає у контролі за джерелами загроз;

г) полягає у виявленні критичних напрямів діяльності банку;

д) реалізують шляхом участі підрозділу безпеки в підборі кадрів.

2. До функцій підрозділу безпеки банку не належить:

а) обліково-контрольна;

б) соціально-кадрова;

в) соціально-диференційна;

г) організаційно-управлінська;

д) методична;

е) інформаційно-аналітична.

*Тести множинного вибору*

3. Умови ефективного функціонування системи фінансово-економічної безпеки такі:

а) чітке визначення мети, завдань та принципів управління фінансово-економічною безпекою;

б) обов'язкове здійснення моніторингу внутрішніх та зовнішніх загроз;

в) формування та постійне оновлення банку даних про внутрішні й зовнішні загрози;

г) визначення переліку підсистем управління фінансово-економічною безпекою;

д) правильна відповідь відсутня.

4. Об'єктами захисту є:

а) матеріальні ресурси;

б) фінансові ресурси;

в) персонал;

г) інформаційні ресурси;

д) інформаційні ресурси з обмеженим доступом;

е) усі варіанти правильні.

*Тести на встановлення відповідності*

5.1. До структури відділу фінансово-економічної безпеки входять:

5.2. До структури підрозділу захисту інформації входять:

а) керівник відділу;

б) експертна група для оперативного вирішення проблем;

в) підрозділ охорони;

г) інформаційно-аналітичний підрозділ;

д) підрозділ опрацювання інформації;

е) група психологічного контролю;

є) група зовнішнього захисту інформації;

ж) група збирання інформації.

6.1. Критеріями економічної безпеки банку є:

6.2. Показниками економічної безпеки банку є:

а) ресурсний потенціал банку й можливості його розвитку;

б) рівень ефективності використання ресурсів;

в) рівень можливостей банку протистояти загрозам його економічної безпеки та самостійно ліквідувати їх;

г) конкурентоспроможність банку;

д) цілісність та масштаби структури банку;

е) ефективність кадрової політики банку;

є) структура дебіторської заборгованості банку;

ж) темпи зростання прибутковості;

з) рівень матеріального й соціального забезпечення працівників банку;

и) розмір боргових зобов'язань банку;

і) обсяги використання тіньового капіталу.

# 3. Загрози діяльності банківських установ

**Мета** – вивчити основні види загроз діяльності банківських установ та функції відділу фінансово-економічної безпеки щодо їх нейтралізації.

**Ключові поняття:** загроза, внутрішня загроза, зовнішня загроза, загроза фінансово-економічній безпеці, банківське шахрайство, зловживання службовим становищем.

**Основні питання:**

3.1. Зовнішні та внутрішні загрози, їх характеристика та тенденції розвитку.

3.2. Банківське шахрайство і зловживання службовим становищем працівників банків.

3.3. Заходи банку щодо захисту від зовнішніх та внутрішніх загроз.

**Література:** [10; 11; 13; 21; 30; 33].

## 3.1. Зовнішні та внутрішні загрози, їх характеристика та тенденції розвитку

**Загроза** – це нереалізована, але потенційно чи реально наявна з певною ймовірністю настання можливість завдання банку будь-якого збитку зловмисниками, конкурентами або обставинами й умовами, що створюють небезпеку для банку, його клієнтів та контрагентів.

У системі понять загрози посідають визначене місце. Існує три види небезпек, а саме: невизначеність, ризик та загроза. Як відомо, невизначеність у середовищі функціонування банку може спричинити виникнення банківських ризиків. Імовірність настання цих ризиків збільшується в міру виникнення потенційних загроз та перетворення їх на реальні. Реальні загрози порушують безпеку, тобто спричиняють небезпеку і негативні наслідки.

Згідно з табл. 3.1, загрози діяльності банку розподіляють на такі групи за класифікаційними ознаками:

середовищем виникнення;

носіями загроз;

сутнісною характеристикою;

об'єктами зазіхань;

тривалістю дії;

за характером впливу;

видами безпеки, на яку впливають загрози.

Таблиця 3.1

## Класифікація загроз банківській безпеці

| Ознаки класифікації | Види загроз | Характеристики загроз |
|---|---|---|
| 1 | 2 | 3 |
| За середовищем виникнення (детальний перелік у табл. 3.2) | Внутрішні загрози | Контролюють банком |
| | Зовнішні загрози | Мають неконтрольований (якщо виникають на макро- чи мезорівнях) або частково контрольований банком характер (якщо виникають на мікрорівні) |
| | Змішані загрози | Мають як контрольований, так і неконтрольований характер |
| За носіями загроз | Загрози з боку клієнтів, банку, конкурентів, банків-партнерів, кримінальних структур, державних органів, громадських організацій, стихійних лих | Загрози походять із зовнішнього щодо банку середовища |
| | Загрози з боку власників банку, адміністрації, персоналу, неформальних груп, засобів безпеки й охорони (неналежна робота системи охорони банку) | Загрози походять із внутрішнього середовища банку |
| За сутнісною характеристикою [13] | Економічні загрози | Реалізуються через корупцію, шахрайство, недобросовісну конкуренцію, використання недосконалих технологій захисту банківської таємниці |
| | Фізичні загрози | Реалізуються через крадіжки, пограбування кас, грошових сховищ банку; руйнування, виведення з ладу, неефективну експлуатацію банкоматів, терміналів |
| | Інтелектуальні загрози | Реалізуються через розголошення та неправомірне використання інформації банку і його інтелектуальної власності; соціальні конфлікти в/та навколо банку; психологічні та ідеологічні диверсії |

Закінчення табл. 3.1

| 1 | 2 | 3 |
|---|---|---|
| За об'єктами зазіхань (небезпеки) | Загрози втрати банківських ресурсів | Ці загрози може бути реалізовано шляхом крадіжок, корупційних дій, шахрайства, недобросовісної конкуренції, фізичного тиску на персонал, розголошення банківської інформації |
| | Загрози здійсненню банківських операцій | |
| | Загрози інфраструктурі банку | |
| | Загрози персоналу банку | |
| | Загрози ліквідності та фінансовій стійкості банку | |
| | Загрози втрати майна та матеріальних цінностей | |
| | Загрози інтелектуальній власності банку | |
| | Загрози прибутковості | |
| За тривалістю дії | Періодичні загрози | Виникають час від часу |
| | Постійно діючі загрози | Можуть бути коротко-, середньо- та довгострокової дії |
| За характером впливу | Прямі загрози | Безпосередньо впливають на безпеку банку |
| | Непрямі загрози | Мають вплив на діяльність контрагентів банку |
| За видами безпеки, на яку впливають загрози | Загрози фінансово-економічній безпеці | Загрози економічній безпеці |
| | Загрози інформаційній безпеці | |
| | Загрози кадровій безпеці | |
| | Загрози операційній безпеці | |
| | Загрози ринковій безпеці | |
| | Загрози силовій безпеці | Вторинні в діяльності банку загрози |
| | Загрози правовій безпеці | |

Детальний перелік загроз, залежно від середовища виникнення, наведено в табл. 3.2.

Змішані загрози можуть виникати, залежно від обставин, як у внутрішньому середовищі банку, так і зовнішньому. Важко контрольованими загрози стають у разі їх одночасного виникнення у внутрішньому й зовнішньому середовищах унаслідок змов персоналу із зовнішніми шахраями.

Таблиця 3.2

**Види загроз за середовищем виникнення**

| Види загроз | Перелік загроз |
|---|---|
| Внутрішні | Фальсифікація і розтрати, змова з конкурентами, контрагентами, недобросовісність, невідповідна кваліфікація банківського персоналу, незадоволеність працею та зумисне заподіяння шкоди, неякісний процес відбору персоналу та управління діловою кар'єрою, неефективна система мотивації персоналу, дестабілізація мікроклімату в колективі, низький рівень управління персоналом банку |
| Зовнішні | Тиск на банківський персонал сторонніх структур, конкурентів; банківське шпигунство, недобросовісна конкуренція, протиправні дії конкурентів, несприятлива соціально-економічна ситуація у країні, нестабільність законодавчої бази, зміна політичної ситуації |
| Змішані | Шахрайство, крадіжки, хабарництво, несанкціонований доступ до комп'ютерної мережі банку, витік банківської інформації, співпраця персоналу з конкурентами |

Усі ці види загроз стосуються загалом банківської безпеки. Найбільш суттєвими й різноманітними є загрози фінансово-економічній безпеці. Загрози економічної природи можуть виникати виключно в зовнішньому чи внутрішньому середовищі, змішаними вони не можуть бути. Їх групування за середовищем виникнення наведено в табл. 3.3.

Таблиця 3.3

**Групування загроз економічної природи фінансово-економічній безпеці за середовищем виникнення**

| Зовнішні загрози | Внутрішні загрози |
|---|---|
| 1 | 2 |
| 1. Несприятлива соціально-економічна ситуація у країні.<br>2. Нестійкість та недосконаліть нормативно-правової бази.<br>3. Низький рівень платоспроможного попиту.<br>4. Нестабільність курсу національної валюти.<br>5. Недосконала та мінлива політика Національного банку України. | 1. Низька кваліфікація персоналу та менеджменту банку.<br>2. Низький рівень кваліфікації спеціалістів із забезпечення банківської безпеки.<br>3. Недостатність ліквідних коштів для погашення зобов'язань.<br>4. Проблеми з поверненням кредитів.<br>5. Витік банківської інформації.<br>6. Недосконалі дії управлінського персоналу. |

Закінчення табл. 3.3

| 1 | 2 |
|---|---|
| 6. Високий рівень інфляції.<br>7. Складна криміногенна ситуація у країні чи регіоні.<br>8. Відсутність можливостей для розширення ринку банківських послуг.<br>9. Недобросовісна конкуренція та шахрайство на ринку банківських послуг.<br>10. Рейдерські атаки та злочинні дії третіх осіб.<br>11. Недовіра клієнтів до банку | 7. Відсутність або недосконалість маркетингових досліджень ринку банківських послуг.<br>8. Недосконала кредитна політика банку.<br>9. Недосконала структура депозитного і кредитного портфелів банку.<br>10. Низька якість кредитного і депозитного портфелів.<br>11. Проблемна структура активів банку (значна питома вага низьколіквідних активів, прострочені кредити).<br>12. Злочинні дії та шахрайство персоналу банку.<br>13. Погана репутація банку.<br>14. Підпорядкування цілей банку інтересам власників |

Настання внутрішніх і зовнішніх загроз завжди має ймовірнісний характер, тому деякі автори розглядають безпеку як протилежність ризику. Фінансово-економічна безпека банку залежить від швидкості та адекватності реакції, що забезпечують адаптацію установи до змінних умов зовнішнього середовища. Тому під час оцінювання безпеки важливо ідентифікувати можливі загрози.

У першу чергу, у ході забезпечення фінансової безпеки банку здійснюють оцінювання загроз економічній безпеці банку, що мають правовий характер.

Серед них виділяють:

внутрішні загрози (нераціональне планування фінансово-економічних показників; неправильно обрана ринкова стратегія; помилкова кадрова і кредитна політика);

зовнішні загрози (форми недобросовісної конкуренції, спекулятивні операції на ринку цінних паперів);

загрози форс-мажорного характеру (страйки, стихійні лиха, збройні конфлікти) та загрози, наближені до форс-мажорних.

## 3.2. Банківське шахрайство та зловживання службовим становищем працівників банків

**Банківське шахрайство** – це один із найбільш поширених видів загроз, які можуть виникати як у внутрішньому, так і зовнішньому середовищі.

У Кримінальному кодексі України шахрайство визначено як зловживання довірою, обман із метою введення власника матеріальних цінностей або коштів в оману і на цій основі добровільного передання своєї власності шахраям.

Умови та ознаки шахрайства наведено в табл. 3.4. Якщо в банку створено умови для шахрайських дій, то через деякий час виявляються ознаки шахрайства.

Таблиця 3.4

**Умови та ознаки банківського шахрайства**

| Умови шахрайства | | Ознаки шахрайства | |
|---|---|---|---|
| зловживання довірою | обман | у діяльності банку | у діях персоналу |
| Уведення в оману працівників банку;<br>передача грошових коштів у власність чи тимчасове користування без відповідного документального оформлення;<br>нездійсненні обіцянки та сподівання, надані позичальником кредитним працівникам | Надання неправдивої інформації про позичальника;<br>укриття обставин, фактів;<br>фальсифікація банківських документів;<br>надання в банк фіктивних і підроблених документів;<br>зумисна зміна значень показників діяльності чи суми отриманих доходів | Передача персоналом банку грошей чи відчуження власності без усвідомлення обману;<br>добровільна передача грошей зловмиснику;<br>видача кредитів, що ризикують стати непогашеними | Намагання виокремити від іншого персоналу свою ділянку роботи;<br>відкидання пропозицій щодо переходу на іншу ділянку роботи;<br>відмова від відпусток;<br>виконання роботи інших працівників;<br>часті помилки коригування в документах;<br>хизування придбаннями та туристичними подорожами в соціальних мережах та перед колегами |

Наслідком шахрайства є: розкрадання коштів; наявність нестач матеріальних цінностей, розбіжності, що виявляють у ході зустрічних перевірок.

Одним із найбільш поширених способів шахрайства є "відмивання" грошей. **"Відмивання" грошей** – це сукупність дій власника грошей із приховування їх незаконного походження. Цей процес має небезпечний характер, оскільки він дозволяє злочинцям користуватися своїм прибутком без створення загрози для джерела таких прибутків. Часто використовувані методи відмивання грошей наведено в табл. 3.5.

Таблиця 3.5

**Методи "відмивання" грошей через банки**

| Назви методів | Зміст методів |
|---|---|
| 1. Злиття законних і незаконних фондів | Засновано на використанні з метою "відмивання" засобів підприємств, у яких значні суми готівки є звичайним і законним явищем (наприклад, ресторани, бари, готелі, компанії та ін.). У цьому разі застосовують дві основних схеми: перша – приховування незаконних доходів у масі законних операцій (злиття) фірм, що реально функціонують; друга – створення фіктивної компанії, що не здійснює реальну діяльність, але створює видимість здійснення операцій і показує у фінансовій звітності як дохід легалізовані гроші |
| 2. Придбання майна за готівку | Придбання машин, яхт, літаків, акцій, предметів розкоші або нерухомості за готівковий розрахунок є способом "відмивання" грошей. Мета подібних придбань потрійна: підтримувати розкішний стиль життя; переводити підозріло великі суми готівки в однаково цінні, але менш підозрілі форми; купувати майно, яке надалі буде використано зі злочинною метою |
| 3. Незаконне вивезення валюти | Здійснюють у двох основних формах: за допомогою фізичного вивезення і вивезення шляхом фінансових операцій. Більшість країн-членів ФАТФ зазначають збільшення обсягу засобів злочинного походження, що надходять контрабандним шляхом для розміщення у фінансовій системі інших держав. Перевозити значні суми грошей злочинцям дозволяє відсутність у багатьох європейських країнах прикордонного контролю за рухом наявних засобів. Так, обсяг кожного перевезення готівки звичайно становить не більш ніж 300 тис. дол., що дає можливість злочинцям обмежити свої втрати в разі крадіжки чи успішної роботи оперативних служб |
| 4. Вивезення грошових коштів | Здійснюють із використанням методів, описаних під час характеристики розміщення через традиційні фінансові установи |

Зловживання службовим становищем працівників банків виявляють у двох формах протиправних дій:

1) використання посадових повноважень із корисливою метою;

2) перевищення посадових повноважень із корисливою метою.

Використання посадових повноважень із корисливою метою може здійснюватись шляхом [13]:

штучного 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 завданнями підрозділу або з порушенням установлених правил і технологій;

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

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

Перевищення посадових повноважень із корисливою метою може виражатись у такому [13]:

прийнятті рішень, не притаманних службовому становищу або функціям посадової особи;

виступах, заявах від імені банку без отримання на це необхідних повноважень;

представленні інтересів установи банку без отримання на те відповідних повноважень;

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

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

наданні гарантій, узяття зобов'язань від імені банку без наявності на те відповідних повноважень.

Зловживання службовим становищем є підґрунтям для шахрайства та зловживань. Особливо поширеною є загроза зазіхання на капітал банку через несанкціоновані прийоми використання пластикових платіжних засобів.

Найбільш поширені нині на практиці способи, інструменти та категорії осіб, що здійснюють злочини в банківській сфері, унаочнено в табл. 3.6.

Таблиця 3.6

**Типові способи, інструменти та категорії осіб, які здійснюють злочини в банківській сфері** [30, с. 10]

| Види операцій | Основні способи здійснення злочинів | Засоби здійснення злочинів | Особи, які здійснюють злочини |
|---|---|---|---|
| Розрахункові операції | Підроблення документів; унесення шахрайських змін у документи; розкрадання документів; неправомірне проникнення в комп'ютерну систему банку та в електронні системи банківських рахунків | Розрахунково-платіжні банківські документи (чеки, векселі, тратти); пластикові картки; комп'ютерні віруси; помилкові комп'ютерні команди | Співробітники банку; особи, які не є співробітниками банку |
| Депозитні операції | Неправомірне проникнення в комп'ютерну систему банку; підроблення документів | Депозитні сертифікати; комп'ютерні віруси; помилкові комп'ютерні команди | В основному співробітники банку |
| Кредитні операції | Незаконне отримання кредиту; невиплата відсотків за кредитом; навмисне неповернення кредиту | Надання позичальником підроблених документів про кредитоспроможність або документів, що містять недостовірні дані; фальсифікація надання застави під кредит; навмисне банкрутство | Особи, які не є співробітниками банку; співробітники банку у змові із третіми особами |

Визначальну роль у системі злочинних дій і водночас економічної безпеки банку відіграє кредитна безпека або безпека кредитних операцій, оскільки вони дають 70 % доходу банку.

Злочинні дії персоналу, що здійснюють у змові із клієнтами, полягають у тому, що вони:

сприяють у наданні кредиту чи пільгових умов кредитування шляхом порушення встановлених процедур чи неврахування вимог до позичальників (незважаючи на наявність у матеріалах кредитної справи даних про заборгованість позичальника чи негативні показники його фінансово-господарської діяльності);

відкладають терміни повернення кредиту шляхом безпідставної пролонгації терміну дії кредитного договору;

сприяють неправильному оцінюванню заставного майна, запропонованого як забезпечення кредиту;

використовують засоби підроблення документів або незаконний доступ до комп'ютерних мереж і електронних банків даних.

Отримання кредиту фізичними особами зумовлено заставою та, зазвичай, обмежено порівняно невеликою сумою коштів. Водночас небезпека цього різновиду шахрайства у кредитно-банківській сфері полягає у збільшенні кількості злочинних зазіхань у загальному обсязі неповернутих громадянами позик. Способи шахрайства у сфері споживчого кредитування певною мірою визначають особливості організації цього ринку фінансових послуг. Торговельна організація укладає угоду з банком (кредитною організацією), що пропонує майбутнім покупцям скористатися цільовим споживчим кредитом на придбання товарів у конкретному магазині. У підготовці та реалізації товарів у кредит беруть участь спеціаліст банку в точці продажу та фахівець торговельної точки, який оформлює замовлення. Потенційний позичальник надає фахівцю магазину документи, необхідні для отримання кредиту. Оформлені заявки останній передає спеціалісту банку. За результатами розгляду цих документів банк приймає рішення про надання кредиту. У разі прийняття позитивного рішення, придбаний товар видають позичальникові лише після підтвердження акту зарахування коштів на рахунок магазину. Схема шахрайства передбачає оформлення кредиту на придбання товару без наміру повернення коштів, отримання товару та його продаж із метою виручки готівкових коштів.

*Найбільш поширені схеми шахрайства з банківськими ресурсами, які слід знати власникам грошових коштів:*

1. Заволодіння паролями банківських карток і рахунків. Кіберзлочинці входять у довіру людей, удаючи із себе працівників пенсійних фондів, банків, соціальних служб. Вони пропонують допомогу у знятті грошей

або ж нечесним шляхом дізнаються паролі до карток і знімають гроші. Злочинці як один із варіантів незаконного зняття грошей із карток знаходять в Інтернеті оголошення щодо збирання благодійних коштів, телефонують авторам оголошень як люди, що хочуть надати допомогу, і просять назвати *CVV*-код, розміщений на зворотному боці картки та термін дії карткового рахунку. Ці дані дають змогу шахраям заповнювати дані у "Приват24". Ця система без правильного коду доступу рекомендувала змінити пароль карткового рахунка. На телефон дійсного власника рахунка приходило СМС-повідомлення. Злочинці просили власників картки надати інформацію про зміст СМС для отримання додаткового карткового рахунка для благодійності. Із використанням нового пароля злочинці знімали всі гроші з благодійного карткового рахунка. Ніяка банківська установа не в змозі запобігти такому роду шахрайства.

2. Пропозиція фіктивних банківських послуг. Злочинці розміщують в Інтернеті чи ЗМІ оголошення про можливість отримати кредит без застави за різними банківськими акціями, лотереями. За обслуговування процесу надання кредиту шахраї просять клієнта переказати певну суму на картковий рахунок. Гроші за обслуговування перераховують на підставних або померлих людей, людей із підробленими паспортами.

3. Несанкціонований доступ до системи "клієнт-банк". За допомогою вірусних шкідливих програм шахраї отримують дані із системи і, використовуючи шкідливий програмний код, здійснюють віддалений доступ до комп'ютера користувача.

4. Зчитування інформації із платіжної карти в банкоматі. У банкомат уставляють спеціальний пристрій, що дозволяє зчитати інформацію з банківської картки та зняти гроші.

Основними напрямами протидії Інтернет-шахрайству можуть бути:

1) розроблення нового програмного обладнання та антивірусних програм;

2) удосконалення нормативно-правової бази у сфері боротьби з Інтернет-шахрайством;

3) створення системи автентифікації Інтернет-адреси для перевірки відповідності введеної користувачем адреси дійсному серверу;

4) підвищення загального рівня грамотності Інтернет-користувачів та більш значного поширення інформації про відомі види Інтернет-шахрайства користувачам Інтернету;

5) проведення різного роду науково-практичних конференцій, семінарів, круглих столів за участю теоретиків та практичних працівників.

## 3.3. Заходи банку щодо захисту від зовнішніх та внутрішніх загроз

Заходи банку щодо захисту від внутрішніх і зовнішніх загроз розподіляють на кадрові, іміджеві, локальні та контрольні (табл. 3.7).

Таблиця 3.7

**Заходи банку щодо захисту від внутрішніх і зовнішніх загроз**

| Кадрові заходи | Іміджеві заходи | Контрольні заходи | Локальні заходи |
|---|---|---|---|
| Створення ефективної системи відбору персоналу банку;<br>запобігання конфліктам у колективі;<br>створення дієвої системи мотивації персоналу;<br>формування соціального пакету та системи матеріальної допомоги для малозабезпечених працівників | Формування причетності до корпоративної культури банку;<br>формування в персоналу банківського патріотизму | Перевірки та ревізії банківських операцій;<br>періодичні інформаційно-аналітичні дослідження ринку банківських послуг;<br>контроль за якістю виконуваних заходів безпеки;<br>моніторинг банківської безпеки | Перевірка приміщень на наявність підслухових пристроїв;<br>оснащення приміщень засобами відеоспостереження;<br>захист приміщень від несанкціонованого використання засобів зв'язку;<br>перевірка комп'ютерної техніки |

Частіше за все банки обмежуються локальною автономною системою захисту інформації банку, що охороняють, в окремих приміщеннях. Організація такої системи передбачає здійснення таких заходів:

установлення у приміщеннях кодових замкових пристроїв із метою запобігання несанкціонованому доступу до них банківського персоналу і клієнтів;

перевірку приміщень на відсутність підслухових пристроїв із використанням пошукової апаратури вітчизняного та зарубіжного виробництва;

заходи із захисту приміщень від впливу лазерних мікрофонів, стетоскопів шляхом установлення перешкод на елементах будівель із використанням віброакустичних пристроїв;

забезпечення захисту приміщень від несанкціонованого використання телефонів мобільного зв'язку шляхом дистанційного блокування за допомогою спеціальних технічних засобів;

установлення на абонентні телефонні апарати суміщених із ними технічних засобів захисту мовних повідомлень, що забезпечують шифрування мовного сигналу, який передають телефонною мережею загального користування;

спеціальну перевірку засобів обчислювальної техніки в місцях їх установлення на можливість несанкціонованого доступу до інформації за рахунок побічних електромагнітних випромінювань.

## Семінарське заняття

1. Види внутрішніх загроз у банківських установах.
2. Характеристика зовнішніх загроз банків.
3. Сутність, спільні та відмінні риси банківського шахрайства та зловживання службовим становищем працівників банків.
4. Характеристика заходів банку щодо захисту від зовнішніх та внутрішніх загроз.

## Тематика доповідей

1. Види зловживань.
2. Відмінності між поняттями "шахрайство" і "зловживання".
3. Етимологія поняття "промислове шпигунство".
4. Класифікація кредитних ризиків.

## Питання для самостійного опрацювання

3.1. Найбільш поширені зовнішні та внутрішні загрози на ринку банківських послуг в Україні.

3.2. Відмінності між поняттями банківського шахрайства і зловживання службовим становищем.

3.3. Види банківських ризиків.

## Методичні рекомендації щодо виконання самостійної роботи

Теоретичні питання та тестові завдання опрацьовують на основі літературних джерел: [10; 11; 13; 21; 30; 33].

## Контрольні запитання

1. Назвати та охарактеризувати зовнішні загрози банківських установ.

2. Які внутрішні загрози можуть виникати в діяльності банківських установ?

3. Розкрити сутність банківського шахрайства.

4. Що становить зловживання службовим становищем?

5. Назвати та охарактеризувати можливі заходи банку щодо захисту від зовнішніх та внутрішніх загроз.

6. Розкрити сутність поняття "загроза".

7. Назвати фактори, що утворюють внутрішні й зовнішні загрози банківській діяльності.

8. Дати правову оцінку банківського шахрайства.

9. Назвати особливості шахрайства.

10. Назвати приклади банківського шахрайства.

11. Перелічити ознаки зловживання службовим становищем у банку.

12. Розкрити сутність організаційно-технічних заходів захисту від зловживань службовим становищем у банку.

13. Що становлять заходи захисту від зловживань кадрового характеру?

## Тести

*Тести одиничного вибору*

1. До ознак зловживання службовим становищем не належить:

а) штучне створення посадовцями виключного свого становища в управлінських або технологічних лініях;

б) отримання матеріальної винагороди за послуги, виконання яких передбачено посадовими обов'язками;

в) лобіювання збиткових, безперспективних рішень і проектів, які сприяють створенню вигідних позицій конкурентам, окремим клієнтам або з метою отримання матеріальної винагороди;

г) створення нерівноцінних умов роботи для своїх підлеглих, вимагання від них виконання роботи, не пов'язаної із завданнями підрозділу або з порушенням установлених правил і технологій;

д) усі варіанти правильні.

2. До форм зловживання службовим становищем не належить:

а) використання посадових повноважень із корисливою метою;

б) перевищення посадових повноважень із корисливою метою;

в) виконання посадових обов'язків;

г) усі варіанти правильні.

*Тести множинного вибору*

3. Під час яких операцій у банках здійснюють шахрайство:

а) кредитних;

б) валютних;

в) касових;

г) міжбанківських;

д) усіх видів операцій?

4. Предметом шахрайських зазіхань є:

а) зловживання довірою;

б) обман;

в) гроші;

г) інтелектуальні розробки;

д) товарно-матеріальні цінності.

*Тести на встановлення відповідності*

5.1. Суб'єктами, що створюють зовнішні загрози безпеці банківської установи, є*:*

5.2. Суб'єктами та діями, що створюють зовнішні загрози безпеці банківської установи, є*:*

а) спецслужби іноземних держав;

б) вітчизняні й іноземні кримінальні елементи та структури;

в) конкуренти;

г) засоби масової інформації;

д) колишні працівники банків;

е) клієнти та партнери;

є) працівники банків;

ж) недосконалі технології банківського виробництва з неповним його врегулюванням нормативними актами банків;

з) недосконала система безпеки банків та захисту їх інформації.

6.1. Використання посадових повноважень із корисливою метою здійснено шляхом:

6.2. Перевищення посадових повноважень із корисливою метою здійснено шляхом:

а) штучного створення посадовцями виключного свого становища в управлінських або технологічних лініях;

б) отримання матеріальної винагороди за послуги, виконання яких передбачено посадовими обов'язками;

в) лобіювання збиткових, безперспективних рішень і проектів, які сприяють створенню вигідних позицій конкурентам, окремим клієнтам або з метою отримання матеріальної винагороди;

г) створення нерівноцінних умов роботи для своїх підлеглих, вимагання від них виконання роботи, не пов'язаної із завданнями підрозділу або з порушенням установлених правил і технологій;

д) умисного затягування вирішення службових чи виробничих питань із метою примушення до надання матеріальної винагороди чи акцентування значення власного становища;

е) прийняття рішень, не притаманних службовому становищу або функціям посадової особи;

є) виступів, заяв від імені банку без отримання на це необхідних повноважень;

ж) представлення інтересів установи банку без отримання на те відповідних повноважень;

з) підписання документів, не передбачених функціональними обов'язками або посадовими повноваженнями.

# 4. Недобросовісна конкуренція і промислове шпигунство в банківських установах

**Мета** – дослідити сутність та відмінності між поняттями "недобросовісна конкуренція" та "промислове шпигунство".

**Ключові поняття:** недобросовісна конкуренція, промислове шпигунство, заходи протидії недобросовісній конкуренції, заходи протидії промисловому шпигунству.

**Основні питання:**

4.1. Сутність недобросовісної конкуренції та промислового шпигунства, їх вияв у банках.

4.2. Можливі способи залучення до роботи працівників банку промисловими шпигунами.

**Література:** [1 – 15; 21; 30; 33].

## 4.1. Сутність недобросовісної конкуренції та промислового шпигунства, їх вияв у банках

Розрізняють кілька видів взаємовідносин, які відображають стан відносин суб'єктів ринку у процесі їх комерційної діяльності, серед них [13]:

*співпраця* – тісні ділові взаємовідносини суб'єктів ринку на основі загальних інтересів із метою вдосконалення методів роботи, спрямованої на збільшення прибутків;

*взаємодія* – погоджені дії для досягнення максимального ефекту отримання вигоди та прибутку;

*конкуренція* – змагання між суб'єктами ринку з метою здобуття, завдяки власним досягненням, переваг над іншими суб'єктами ринку;

*суперництво* – антагоністичні дії, побудовані на непримиренності позицій, інтересів і методів роботи щодо здобуття переваг на ринку;

*протиборство* – гостра антагоністична боротьба за заволодіння ринком, під час якої застосовують дуже жорсткі заходи впливу на суперників у такій боротьбі.

**Конкуренція** – це мистецтво приваблювати клієнта, тому недобросовісна конкуренція містить ще й приваблення клієнта на засадах обману та введення в оману.

Засобами конкуренції є банківські продукти, за допомогою яких банки-конкуренти намагаються завоювати визнання та залучити клієнтів. Об'єктом конкуренції в банківському секторі є потреби груп споживачів, які входять до цільового ринку (ринків), що обрали для себе.

Банки є суб'єктами фінансового ринку, що складено з: 1) ринку позичкових капіталів (банки виступають на ньому як покупці або продавці тимчасово вільних фінансових ресурсів); 2) ринку цінних паперів (купівлі-продажу цінних паперів); 3) ринку валют і дорогоцінних металів.

Недобросовісною конкуренцією є незаконне використання ділової репутації банківської установи, створення перешкод банку у процесі конкуренції та досягнення незаконних переваг у конкуренції, неправомірне збирання, використання або розголошення інформації, що є комерційною таємницею.

Метою недобросовісної конкуренції у сфері банківських послуг є прагнення банку-конкурента поліпшити позиції на ринку позичкових капіталів, цінних паперів, валют і цінних металів.

До актів недобросовісної конкуренції в банківській сфері належать: по-перше, незаконне використання ділової репутації банку; по-друге, створення перешкод банкам у процесі конкуренції та здобуття неправомірних переваг у конкуренції; по-третє, неправомірне збирання, розголошення та використання комерційної таємниці.

Економічне суперництво комерційних банків за вигідні ринкові позиції часто здійснено на засадах недобросовісної конкуренції, ознаками якої є:

надання банківських послуг із примусовим асортиментом;

схиляння клієнтів до розірвання взаємовідносин із банками-конкурентами;

схиляння клієнта до дискредитації й підриву репутації банку-конкурента;

антиконкурентні дії, що становлять погоджені дії, наслідком яких є укладання угод щодо обмеження надання банківських послуг, фінансово-економічного розвитку, інвестицій і диференціації банківських послуг для руйнування конкурентних цін;

несанкціоноване збирання інформації щодо діяльності конкурента;

приваблення клієнтів на засадах обману;

викривлення інформації про банківські послуги;

шантаж і компрометація керівництва банку чи персоналу;

зривання угод і договорів через поширення недобросовісної конкуренції;

переманювання клієнтів та персоналу в банків-конкурентів;

використання конфіденційної інформації для заподіяння шкоди конкурентам;

зловживання провідним положенням на ринку банківських послуг;

тиск на клієнтів із метою їх залучення до співпраці;

створення штучних перешкод для діяльності банку;

залякування акціонерів, партнерів, клієнтів банків-конкурентів;

установлення контролю за діяльністю банку-конкурента шляхом уведення до штату своїх людей.

Заходи протидії актам недобросовісної конкуренції наведено в табл. 4.1.

Таблиця 4.1

**Заходи протидії актам недобросовісної конкуренції в банках**

| Аналітичні заходи | Інформаційні заходи | Технічні заходи | Іміджеві заходи |
|---|---|---|---|
| Аналіз можливих утрат банку від недобросовісної конкуренції | Інформування постійних клієнтів щодо результатів діяльності банку | Упровадження технічних засобів захисту банківської інформації | Запрошення постійних клієнтів на банківські свята |
| Визначення найбільш вагомих конкурентів та складання прогнозів розвитку взаємовідносин із ними | Інформування клієнтів про результати порівняння власних банківських продуктів і продуктів конкурентів | Контроль за доступом персоналу до банківської бази та його авторизація | Формування сумісності персоналу з корпоративною культурою банку |
| Вивчення ринків банківських послуг | Інформування клієнтів щодо банківських продуктів | Упровадження конкурентної розвідки | Інформування громадськості про соціальні заходи банку |
| Аналіз утрат у клієнтській базі | | | |

## 4.2. Можливі способи залучення до роботи працівників банку промисловими шпигунами

Промислове шпигунство є невід'ємним елементом недобросовісної конкуренції.

**Промислове шпигунство** – це сукупність заходів щодо забезпечення несанкціонованого доступу до конфіденційної інформації, її знищення, зміни чи використання.

Найбільш повне, із юридичного погляду, визначення дає Міжнародна організація кримінальної поліції (Інтерпол): "… це придбання будь-яким обманним шляхом інтелектуальної власності, яка належить будь-якій юридичній особі та яку було створено або законно придбано цією юридичною особою з метою виробництва, що має або може мати промислову цінність...".

**Конкурентна розвідка** – дослідження відкритих інформаційних джерел, що стосується основних тенденцій банківської діяльності й намірів конкурентів.

Поняття розвідка і промислове шпигунство відрізняються між собою за змістом, але мають спільну мету. Метою як промислового шпигунства, так і конкурентної розвідки є отримання інформації, яка дає змогу здобути конкурентні переваги на ринку. Відмінністю між промисловим шпигунством і конкурентною розвідкою є методи та способи збирання інформації. Здобуття інформації, що використовує розвідник, є законним. Промислове ж шпигунство передбачає нелегальні методи й технології. Служба конкурентної розвідки може користуватися тільки відкритими джерелами інформації, оскільки робота розвідника може бути лише інформаційно-аналітичною, тобто включати збирання й опрацювання різних даних, що впливають на розвиток банківського бізнесу.

Банківське шпигунство полягає в оперативній роботі, а саме: у незаконному проникненні на територію банку-конкурента, викраденні інформації, стеженні, шантажі та підкупі посадових осіб.

*Носії інформації,* що може стати об'єктом промислового шпигунства, такі:

локальна мережа банку;

комп'ютерна техніка;

накопичувачі інформації;

паперові носії інформації;

персонал банку;

записи камер відеоспостереження;

зовнішні суб'єкти промислового шпигунства.

Промислове шпигунство для банку має такі негативні наслідки, як:

утрата конфіденційної інформації;

утрата клієнтів;

утрата ринків збуту банківських продуктів;

утрата довіри клієнтів;

утрата кваліфікованого персоналу;

погіршення фінансових результатів діяльності банку;

зниження ліквідності та платоспроможності банку.

У банківській практиці існує багато різних форм і методів промислового шпигунства. Попри їх численність, їх обумовлено, переважно, самою природою промислового шпигунства як таємною формою конкурентної боротьби (табл. 4.2).

Таблиця 4.2

**Методи промислового шпигунства, що застосовують у банках**

| Характеристики | Агентурні методи | Технічні методи |
|---|---|---|
| Напрями | Вербування, упровадження своєї людини в банк | Несанкціонований доступ до банківської інформації |
| Мета | Знищення конкурента. Розкриття комерційної таємниці банку | |
| Об'єкти розроблення | "другі" або "треті особи" банку-конкурента | Хакери, працівники комп'ютерного відділу, підслухові пристрої |
| Форма оплати послуг промислового шпигуна | Винагородження, передача інтелектуальної власності, перехід на роботу до банку-конкурента | |

Легальні методи збирання інформації, що використовує конкурентна розвідка, такі:

відвідування банків клієнтами, що представляють банк конкурентів;

аналіз відкритих матеріалів про результати діяльності;

установлення приязних взаємовідносин із банківськими установами, клієнтами банків;

укладання угод і договорів із конкурентами;

участь у конференціях та інших форумах, де обговорюють проблеми діяльності банків.

Слід розглянути найбільш поширені способи промислового шпигунства.

*Підкуп* полягає в таких поетапних діях:

з'ясування ступеня обізнаності тих або інших працівників фірми у її справах;

збирання інформації про те, які кошти й кому слід заплатити;

знаходження персоналу, який має необхідну інформацію і згоден її продати за певну суму.

*Переманювання працівників банку.* Метою є подальше оволодіння їх знаннями. На ринку рекрутингових послуг цю послугу називають "хедхантинг".

*Шантаж* здійснюють за двома варіантами:

людину шантажують, загрожуючи розголосом компромату на неї у відповідних колах;

погрожують фізичною розправою (знищити автомобіль, спалити дачу, викрасти дитину).

*"Уливання своїх людей"* до складу персоналу фірми-конкурента здійснюють двома шляхами:

агент виступає під власним прізвищем і працює за професією;

агента працевлаштовують за підробленими документами, під прикриттям "легенди".

*Викрадення інформації,* що можливе такими способами:

викрадення носіїв інформації (магнітних, оптичних дисків, флеш-пристроїв);

копіювання таємної інформації з носіїв;

ознайомлення із залишеними без нагляду роздруками;

знайомство з інформацією з екрана сторонньою особою (під час відображення її користувачем або за його відсутності в місці доступу);

користування спеціальними апаратними засобами, що забезпечують доступ до конфіденційної інформації;

застосування спеціальних технічних засобів для несанкціонованого перехоплення електромагнітних випромінювань;

несанкціонований доступ шкідливих програм до інформації або незаконне розшифровування зашифрованої інформації.

*Спостереження* у вигляді:

копіювання документації, матеріалів кредитних справ;

фотографування, що можна здійснювати на малих і великих відстанях.

*Прослуховування і підслуховування.* Саме цей метод дуже широко використовують через його простоту.

Підслуховування телефонних переговорів найбільш поширене. Його здійснюють:

за рахунок мікрофонного ефекту телефонного апарата;

контактним підключення до лінії зв'язку;

безконтактним підключенням до телефонної лінії;

за допомогою телефонних радіозакладень.

Ознаки спроб *залучення службовців банку до співробітництва з конкурентами або іншими структурами* [13]:

у ході розмов зі службовцями з будь-якої нагоди ставлять запитання, що стосуються різних сторін та способу життя когось із працівників, його ставлення до роботи та керівництва;

спостереження за окремими службовцями: вивчення звичок, улюблених місць проведення свого дозвілля, хобі тощо;

участь однієї й тієї ж особи в позаслужбових зустрічах і заходах, необґрунтовано часта матеріальна і грошова подяка за незначні послуги;

залучення службовця або близьких йому людей до різних сумнівних угод, ризикованих компаній, протизаконних дій, надання грошей у борг, створення інтимних ситуацій;

різноманітні негативні чутки, плітки між службовцями банку, анонімні листи, що надходять до служби безпеки й керівництва банку;

утрата службових документів у підрозділах банку;

оприлюднення або використання конкурентами інформації банку з обмеженим доступом;

залучені працівники ведуть себе більш активно, видають себе за поборників прав своїх колег, мають найбільшу обізнаність у ситуації, прагнуть до позицій лідера в колективі.

Якщо ж промисловим шпигунам удалося залучити когось із службовців до роботи на себе, то цим службовцям вони можуть рекомендувати такі *форми поведінки* [13]:

не давати ніякого приводу, аби звернути на себе увагу керівництва банку або колег;

мати зразкову поведінку, не відмовлятись від позаурочної й додаткової роботи;

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

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

*Заходи захисту банку від недобросовісної конкуренції:*

аналіз інформації у ЗМІ про банк та його діяльність;

використання різних носіїв інформації;

обмеження та авторизація доступу до конфіденційної інформації;

застосування технічних та криптографічних засобів захисту інформації;

захист баз даних від несанкціонованого доступу;

опанування розробок і банківських продуктів;

інструктаж персоналу щодо можливих способів залучення промисловими шпигунами;

забезпечення контролю за ступенем захисту комп'ютерної мережі від несанкціонованого доступу;

здійснення оперативних заходів протидії промисловому шпигунству.

## Практичне заняття

**Завдання 4.1.** Модель поведінки працівників служби фінансово-економічної безпеки в умовах недобросовісної конкуренції.

Вихідні умови: виявлення антирекламної кампанії конкурентного банку.

*Методичні рекомендації щодо побудови моделі*

Структурно модель повинна мати вигляд:

1) дослідження ринку банківських послуг. Ринок банківських послуг слід дослідити в межах Харкова. Визначити основних конкурентів банку. Банк для побудови моделі студент обирає самостійно;

2) ознаки недобросовісної конкуренції. Назвати всі можливі ознаки недобросовісної конкуренції. Визначити притаманні досліджуваному банку;

3) виділення недобросовісних конкурентів. Окреслити перелік банків, що здійснюють недобросовісну конкуренцію на ринку банківських послуг;

4) аналіз дій недобросовісних конкурентів. Скласти перелік дій, що характерні для кожного недобросовісного конкурента;

5) вибір методів поведінки з недобросовісними конкурентами. Його слід здійснювати щодо кожної дії з переліку;

6) створення правил та інструкцій, що регламентують поведінку персоналу з недобросовісними конкурентами. Інструкцію має бути складено, ураховуючи універсальний підхід.

**Завдання 4.2.** Моделювання поведінки персоналу в умовах промислового шпигунства.

Вихідні умови: прийняття на роботу до відділу фінансового моніторингу працівника з банку конкурента.

Модель поведінки формують за такими етапами:

1) виявлення ознак спроб залучення службовців банку до співробітництва з конкурентами або іншими структурами. Указати конкретні ознаки;

2) вибір форми поведінки співробітників банку із промисловими шпигунами:

не давати ніякого приводу, аби звернути на себе увагу керівництва банку або колег;

мати зразкову поведінку, не відмовлятись від спілкування із промисловим шпигуном;

намагатися зібрати інформацію про діяльність промислового шпигуна;

протидіяти збиранню інформації промисловим шпигуном;

доповісти про наявність промислового шпигунства начальнику відділу фінансово-економічної безпеки;

утримуватись від знайомств, які б могли завдати шкоди діяльності такого службовця.

3) визначення засобів і ресурсів, необхідних для боротьби зі шпигунами.

**Завдання 4.3.** Розроблення програми протидії недобросовісній конкуренції та промисловому шпигунству.

Програму складено за формою табл. 4.3. Програму має бути розроблено на квартал. У програмі вказують заходи щодо посилення інформаційної, кадрової та фінансово-економічної безпеки.

Таблиця 4.3

**Програми протидії недобросовісній конкуренції та промисловому шпигунству в банку**

| Заходи протидії | Зміст заходів | Термін виконання | Відповідальні особи | Примітки |
|---|---|---|---|---|
| Перегляд системи підбору та відбору персоналу | | | | |
| | | | | |

## Тематика рефератів

1. Види недобросовісної конкуренції.
2. Види промислового шпигунства.
3. Захист банківських та фінансових установ від промислового шпигунства.
4. Захист банківських та фінансових установ від недобросовісних конкурентів.

## Питання для самостійного опрацювання

4.1. Ознаки недобросовісної конкуренції в банківській діяльності.

4.2. Ознаки промислового шпигунства, його наслідки для банків.

## Методичні рекомендації щодо виконання самостійної роботи

Теоретичні питання та тестові завдання опрацьовують на основі літературних джерел: [1 – 15; 21; 30; 33].

## Контрольні запитання

1. Розкрити сутність недобросовісної конкуренції в банківській сфері.
2. Охарактеризувати вияви промислового шпигунства в банківській сфері.
3. Назвати можливі способи залучення до роботи працівників банку промисловими шпигунами.
4. Розкрити сутність таких видів взаємовідносин, як співпраця, конкуренція, суперництво, протиборство.
5. Назвати перелік дій, які визнають як недобросовісну конкуренцію.
6. Охарактеризувати особливості недобросовісної конкуренції з боку клієнтів та керівництва банків.
7. Назвати історичні приклади промислового шпигунства.
8. Охарактеризувати сучасні форми нелегального збирання інформації.
9. Назвати ознаки спроб залучити персонал банку до промислового шпигунства.

## Тести

*Тести одиничного вибору*

1. Співпраця – це:

а) тісні ділові взаємовідносини суб'єктів ринку на основі загальних інтересів із метою збільшення прибутків;

б) погоджені дії для досягнення максимального ефекту отримання вигоди та прибутку;

в) змагання між суб'єктами ринку з метою здобуття, завдяки власним досягненням, переваг над іншими суб'єктами ринку;

г) антагоністичні дії, побудовані на непримиренності позицій, інтересів і методів роботи щодо здобуття переваг на ринку;

д) власний варіант відповіді.

2. Сукупність заходів, які здійснюють із метою несанкціонованого отримання, зміни, знищення інформації банку з обмеженим доступом, такі:

а) промислове шпигунство;

б) недобросовісна конкуренція;

в) співпраця;

г) протиборство;

д) власний варіант відповіді.

*Тести множинного вибору*

3. Носіями недобросовісної конкуренції є:

а) партнери;

б) клієнти;

в) кримінальні елементи;

г) персонал банку;

д) власний варіант відповіді.

4. Носіями інформації з обмеженим доступом є:

а) персонал;

б) документи;

в) електронні носії інформації;

г) аудіо-, відеоматеріали;

д) усі варіанти правильні.

*Тести на встановлення відповідності*

5.1. Заходи протидії актам недобросовісної конкуренції такі:

5.2. Види недобросовісної конкуренції такі:

а) шантаж і компрометація;

б) зловживання панівним становищем банку;

в) зривання угод;

г) ведення комерційної розвідки;

д) вибір методів і моделей поведінки;

е) заманювання клієнтів.

6.1. Співпраця – це:

6.2. Взаємодія – це:

6.3. Конкуренція – це:

6.4. Протиборство – це:

6.5. Суперництво – це:

а) тісні ділові взаємовідносини суб'єктів ринку на основі загальних інтересів із метою вдосконалення методів роботи, спрямованої на збільшення прибутків;

б) погоджені дії для досягнення максимального ефекту отримання вигоди та прибутку;

в) змагання між суб'єктами ринку з метою здобуття, завдяки власним досягненням, переваг над іншими суб'єктами ринку;

г) антагоністичні дії, побудовані на непримиренності позицій, інтересів і методів роботи щодо здобуття переваг на ринку;

д) гостра антагоністична боротьба за заволодіння ринком, під час якої застосовують дуже жорсткі заходи впливу на суперників у такій боротьбі.

# 5. Організація охорони та дій банківських установ в екстремальних умовах

**Мета** – розглянути теоретичні засади організації охорони та дій банків в екстремальних умовах.

**Ключові поняття:** силова безпека, технічне зміцнення банку, відділ охорони, режим охорони, екстремальні умови.

**Основні питання:**

5.1. Силова безпека та технічне зміцнення банків.

5.2. Організація охорони установ банків.

5.3. Режими охорони.

5.4. Дії установ банків в екстремальних умовах.

**Література:** [10 – 13; 21; 25].

## 5.1. Силова безпека та технічне зміцнення банків

**Силова безпека банківської установи** – це стан захищеності банку від крадіжок власності, утрати іміджу та безпеки персоналу, що досягають шляхом використання комплексу методів протидії сторонньому втручанню і завданню збитків.

*Завдання силової безпеки банку* такі:

організація контрольно-перепусткового режиму в банківській установі;

забезпечення контролю за технікою безпеки праці;

відеоспостереження та контроль за прилеглою до банку територією;

забезпечення захисту комерційної таємниці від розголошення та санкціонованого доступу до неї;

виявлення та локалізація можливих каналів витоку конфіденційної інформації;

коригування поведінки персоналу в екстремальних умовах;

забезпечення охорони приміщень та прилеглої території, матеріальних цінностей у процесі їх транспортування;

забезпечення персонального захисту окремих керівників і фахівців банку на її території та за її межами;

виявлення проникнення сторонніх осіб на територію банку;

охорона заходів (переговорів, нарад, зустрічей);

контроль за станом технічних засобів захисту;

забезпечення дотримання встановленого режиму охорони.

*Заходи силової безпеки банку* містять:

захист активів;

дотримання правил охорони праці;

дотримання правил пожежної безпеки;

заходи цивільної оборони;

охорону приміщення;

захист від стихійних лих.

За вимогою НБУ у сфері силової охорони банки зобов'язують дотримуватися *таких правил:*

забезпечення наявності охорони у стандартних відділеннях, де є касовий вузол і здійснюють операції з готівкою;

забезпечення захисту вікон перших цокольних поверхів металевими ґратами, ударостійким (броньованим) склом;

наявності підтвердження (сертифіката) відповідності на всі матеріали, що застосовують для забезпечення безпеки;

погодження порядку взаємодії керівника банку з територіальним органом Міністерства внутрішніх справ у разі виникнення екстремальних ситуацій.

*Основні вимоги до обладнання входу банку:*

неможливість несанкціонованого проникнення до приміщення банку сторонніх осіб;

забезпечення максимальної зручності входу до банку працівників;

відповідність естетичним нормам.

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

*Варіантами обладнання входу* можуть бути [13]:

установлення одностулкових дверей, що обертаються, із боковими завісами. Такі двері мають бути дерев'яними не менш ніж 40 мм завтовшки; додатково встановлюють ґратчасті металеві двері, що відчиняються всередину будівлі;

установлення дверей, що обертаються, із фіксацією кута повороту. Перевага таких дверей полягає в тому, що їх не можна залишити відчиненими;

обладнання шлюзових входів (установлення 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 зачинено);

установлення на входах "квиткових" турнікетів. У цьому разі документом для проходу до банку може слугувати індивідуальна картка співробітника.

Широко застосовують автоматизовані системи контролю за доступом. Принцип функціонування такої системи полягає в тому, що кожний працівник отримує індивідуальну картку з нанесеним на неї особистим кодом, на вході встановлюють спеціальні пристрої, які зчитують інформацію з таких карток. Інформація потрапляє до системи, яка на основі аналізу даних про власника картки реагує відповідним чином: відчиняє двері та реєструє присутність власника на робочому місці; умикає сигнал тривоги.

*Особливості обладнання банківського приміщення:*

1) обладнання приміщень спеціальними засобами захисту від підслуховування, стороннього відеоспостереження;

2) підбір такого місця розміщення, яке б дозволяло надати максимум зручностей клієнтам та виключати можливість спостереження клієнтами та сторонніми особами за переміщенням готівки та інших цінностей і роботою з ними персоналу банку;

3) вікна приміщень перших, цокольних, підвальних поверхів банків, касового вузла, виготовлення й оброблення ламінованих карт, служби захисту інформації, архівів, служби безпеки, а також тих покрівель прибудов, що прилягають до пожежних драбин, захищають від несанкціонованого проникнення;

4) захист ґратами від несанкціонованого доступу вентиляційних каналів, водостічних труб, люків, шлюзів та інші комунікаційні отвори розміром понад 150×150 мм;

5) обладнання серверної та приміщень із комп'ютерною технікою генераторами для електропостачання в разі відмикання основного джерела енергозабезпечення;

6) забезпечення аварійного живлення сигналізаційного обладнання;

7) ізоляція та забезпечення належного обладнання внутрішніх касових приміщень, сховищ для зберігання грошей і банківських металів;

8) здійснення захисту серверної, електронного архіву шляхом екранування приміщень;

9) обладнання приміщень та прилеглої території засобами відеоспостереження;

10) установлення захисних  огорож та бар'єрів для недопущення проникнення на територію чи приміщення банку;

11) умикання тривожного освітлення в разі несанкціонованого доступу до приміщення, каси, сховища, що перебувають під сигналізацією.

Для охорони приміщень банки застосовують багаторубіжну систему захисту. *Перший рубіж* охорони захищає будівельні конструкції периметрів приміщень, віконні та дверні отвори, люки, вентиляційні канали, теплові вводи, тонкостінні перегородки та інші елементи приміщень, доступні для проникнення ззовні. *Другий рубіж* охорони контролює простір усередині будинку або приміщень. Сигнал тривоги надходить у разі несанкціонованого проникнення сторонньої особи до приміщення. *Третій рубіж* охорони становлять засоби для блокування підходів до окремих предметів, елементів обладнання приміщень, робочих місць.

## 5.2. Організація охорони установ банків

Метою організації охорони в банках є забезпечення фізичного захисту співробітників, клієнтів, майна і грошових коштів банків від незаконних зазіхань сторонніх осіб.

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

рівень технічного зміцнення банків;

можливість та кількість спроб злочинних зазіхань на майно та інформацію банків;

наявність і якісні характеристики охоронно-пожежної сигналізації;

уразливі місця в технічному зміцненні банку, про які уже відомо банківській охороні;

режим роботи банку, кількість і суми грошових та матеріальних цінностей, що знаходяться у приміщенні банку;

обраний режим охорони установи банку;

особливості та характеристики місцевості, де розташовано банківську установу;

якісні й кількісні характеристики відділу охорони;

технічна оснащеність працівників охорони.

*Основні принципи організації охорони в банку:*

безперервність охоронних дій у часі. Спостереження мають здійснювати в режимі реального часу;

дієвість охоронних заходів. Охоронні заходи мають бути результативними, дії персоналу служби охорони зваженими й точними;

запобіжний характер охорони. Систему охорони має бути організовано таким чином, щоб забезпечувати своєчасне уникнення несанкціонованого доступу до банківських приміщень третіх осіб;

оперативність реагування на несанкціонований доступ до інформації та приміщень;

належна, відповідно до рівня доступу, інформованість персоналу служби охорони про події, що відбуваються в банку;

своєчасна й доцільна співпраця служби охорони із правоохоронними органами.

Охорону можна здійснювати службою охорони банку, підрозділами внутрішніх справ або охоронними агентствами.

Організація охорони містить комплекс заходів із:

фізичної охорони, що здійснюють шляхом установлення стаціонарних постів, виділення груп для охорони грошових сховищ, супроводження цінностей, патрульних груп та груп охорони посадових осіб банківської установи;

технічної охорони, що полягає у встановленні в необхідних місцях технічних засобів охорони, які може бути надано засобами затримання, спостереження за територією і приміщеннями банківської установи, охоронної та пожежної сигналізацій, обладнанням для виявлення за внесення чи винесення заборонених матеріалів, зброї.

Керівник банку або уповноважена ним особа в ході організації охорони визначає [13]:

організацію перепусткового та внутрішньооб'єктового режиму;

місця встановлення технічних засобів охорони та їх кількість;

технічні засоби охорони для забезпечення відповідного реагування на їх сигнали сил охорони;

конкретні (мінімально можливі) терміни оперативного реагування сил охорони на сигнали технічних засобів охорони;

дії працівників банку і сил охорони в разі спрацювання технічних засобів охорони, а також їхні дії в непередбачених ситуаціях;

взаємодію між різними суб'єктами охорони, якщо має місце залучення до виконання завдань охорони різних суб'єктів;

інші заходи, необхідні для забезпечення надійного збереження цінностей і належного рівня охорони відповідної установи банку.

*Вимоги до працівників банківської охорони:*

а) керівників підрозділів охорони: вища юридична освіта або досвід роботи не менше від трьох років в охоронних, оперативних, слідчих підрозділах органів МВС, СБУ або досвід несення служби не менш ніж п'ять років на командних посадах військових частин і навчальних підрозділів

Збройних сил України чи досвід роботи не менш ніж п'ять років за останні 10 років в охоронних фірмах та структурах;

б) працівників підрозділів охорони: вік не менш ніж 18 років, позитивний висновок лікарської комісії про відсутність заборони виконувати функції, пов'язані із охоронною діяльністю; належна початкова підготовка до виконання посадових обов'язків із охорони громадян і об'єктів; відсутність притягнень за організацію чи участь у громадських безпорядках; відсутність наркозалежності та захворювання на алкоголізм; відсутність судимості чи звинувачень у скоєнні злочинів, непогашеної судимості; відсутність рішення суду про позбавлення права займатись охоронною діяльністю; наявність постійного місця проживання.

## 5.3. Режими охорони

Залежно від розміру банку, наявних грошових і матеріальних цінностей та за рішенням керівника установи банку може обиратись один із перелічених режимів охорони:

1) за характером спостережних дій:

цілодобова фізична охорона із залученням відповідних технічних засобів охорони та відеоспостереження;

фізична охорона із залученням відповідних технічних засобів охорони для спостереження в робочий час, а в неробочий – використання тільки технічних засобів;

цілодобова охорона тільки за допомогою відповідних технічних засобів охорони, що залучають для спостереження сил охорони;

2) залежно від завдань охорони [13]:

*внутрішньооб'єктовий режим*, що передбачає створення відповідної системи заходів і правил, спрямованих на забезпечення схоронності матеріальних цінностей банку його інформаційних ресурсів, особистої безпеки працівників банку, його клієнтів, аварійної та пожежної безпеки;

розроблення та введення в дію внутрішньооб'єктового розпорядку роботи установи банку;

порядок допуску працівників банку до режимних приміщень;

порядок відкривання, закривання і здавання під охорону робочих приміщень;

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

порядок використання індивідуальних карток, призначених для проходження в банк через автоматизовані системи доступу;

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

порядок дій сил охорони і персоналу банку в позаштатних ситуаціях (під час пожеж, стихійних лих, нападів на установи банку та ін.);

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

обов'язки працівників банку щодо дотримання вимог внутрішньооб'єктового режиму та відповідальність за його порушення;

*перепустковий режим*, що передбачає встановлення відповідного порядку доступу до банку, який усував би можливість безконтрольного входу (виходу) на територію установи банку, у його приміщення та до персоналу сторонніх осіб, клієнтів. Він містить:

порядок приймання відвідувачів і видачі перепусток;

порядок пропускання осіб;

порядок пропускання транспортних засобів і матеріальних цінностей;

порядок документування порушень перепусткового режиму.

Види перепусток, що використовуються банком:

*постійні* – видають персоналу банку, що перебуває у штаті. Термін дії таких перепусток указано на бланку самої перепустки. Перепустка дійсна без подання інших документів, що засвідчують особу, оскільки містять фотографію, засвідчену печаткою;

*тимчасові* – зазвичай, для штатних працівників на період терміну випробування; осіб, що працюють за трудовою угодою або у складі тимчасових колективів. Термін дії таких перепусток до півроку;

*разові* – для всіх клієнтів (крім клієнтів операційних підрозділів), партнерів, гостей. Видають одноразово. Така перепустка дійсна протягом робочого дня. Після завершення роботи в банку перепустку підписує особа, яка її замовляла, у цьому разі вказують 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, яких обслуговують у цій установі банку;

*матеріальні* перепустки дають право винесення (вивезення) із банку вказаних у них матеріальних цінностей.

Разові та матеріальні перепустки видають на підставі заявок або розпоряджень керівництва, його заступників, головного бухгалтера. Заявки й розпорядження фіксують у книзі приймання відвідувачів.

Стан безпеки банку визначено рівнем оснащеності системи охорони (табл. 5.1).

Таблиця 5.1

**Стан безпеки банку,**
**залежно від рівня оснащеності системи охорони**

| Рівні оснащеності системи охорони | Характеристики | Стани банку |
|---|---|---|
| Елементарний | Використовують тільки такі засоби технічного захисту: замки, засувки, огорожі, освітлення території банку | Внутрішні й зовнішні небезпеки |
| Задовільний | Використовують засоби технічного захисту: сучасні системи охорони з дистанційним управлінням; сучасні огорожі, розташовані по периметру банку; система відеоконтролю. Фізичний захист реалізує охоронець із засобами зв'язку | Реальні як внутрішні, так і зовнішні загрози |
| Достатній | Засоби захисту: система охорони банку по периметру, спеціально підготовлена охорона із засобами зв'язку, система контролю за доступом до об'єкта, система зв'язку із правоохоронними органами, план охорони банку за непередбачених обставин | Потенційні внутрішні загрози |
| Високотехнологічний | Наявність підрозділу швидкого реагування, високотехнологічна система охорони | Відносна безпека |

Лише високотехнологічний рівень оснащеності забезпечує відносну безпеку банківських операцій.

## 5.4. Дії установ банків в екстремальних умовах

**Екстремальні ситуації** – це ситуації, за яких банки та їх персонал піддаються серйозному впливу напружених, майже критичних, обставин, що характеризуються високим рівнем загрози їхньому здоров'ю, життю та ефективності діяльності.

Причини екстремальних ситуацій мають здебільшого зовнішнє походження. До них належать: недобросовісні дії конкурентів, протиправна діяльність злочинців, різкі зміни правових умов, невиконання зобов'язань партнерами, сили природи, техногенні процеси виробничої діяльності підприємств, небезпечна поведінка окремих осіб.

Види екстремальних ситуацій за походженням наведено в табл. 5.2.

Таблиця 5.2

**Види екстремальних ситуацій у банках за походженням**

| Характери екстремальних ситуацій | Перелік екстремальних ситуацій |
|---|---|
| Соціально-психологічний | шантаж, використання психотропних речовин та спеціальних психотехнічних комунікацій, дискредитація, наклеп, поширення негативних чуток щодо персоналу банку |
| Фізичний | терористичні акти, розбійні напади, захоплення заручників серед клієнтів та персоналу банку |
| Стихійний | землетруси, повені, бурі |
| Техногенний | радіаційні або хімічні аварії та атаки, пожежі |

Правила поведінки банківського працівника в екстремальній ситуації:

оволодіти собою, заспокоїтися, привести себе до стану, який дозволить нормально думати й діяти;

проаналізувати ситуацію та зрозуміти свою роль у ній;

визначити й оцінити джерело небезпеки, що створило екстремальну ситуацію;

визначити тактику поведінки й дій в екстремальній ситуації.

Екстремальні ситуації мають невизначений характер, непередбачуваність у часі та наслідках їх настання. Проте для правильного реагування на них і запобігання людським утратам і втратам матеріальних цінностей банківські установи мають планувати свої дії.

План поведінки банку в екстремальній ситуації зазвичай містить:

1. Перелік профілактичних заходів щодо запобігання екстремальним ситуаціям.

2. Перелік заходів щодо гарантування безпеки персоналу та майна.

3. Заходи щодо обмеження доступу сторонніх осіб до банку.

4. Заходи щодо запобігання скоєнню будь-яких протизаконних дій, якими може бути створено загрозу настання екстремальної ситуації.

5. Перелік заходів щодо ліквідації негативних наслідків екстремальних ситуацій.

**Екстремальна ситуація в роботі інкасації** – це дії техногенного характеру чи сторонніх осіб, пов'язані зі втратою життя, здоров'я інкасаторів, із викраденням грошових коштів, цінностей, зброї або ж пошкодженням інкасаторського автомобіля.

Порядок дій банківських працівників відрізняється, залежно від виду екстремальної ситуації. Види та характеристики екстремальних ситуацій, що виникають у роботі інкасаторів, наведено в табл. 5.3.

Таблиця 5.3

**Види та характеристики екстремальних ситуацій, що виникають у роботі інкасаторів**

| Ознаки розгляду | Характеристики |
|---|---|
| 1 | 2 |
| Види екстремальних ситуацій | Поломка транспортного засобу; напад на інкасаторів; напад на спецавтомобіль; утрата (крадіжка) готівки й цінностей; утрата (крадіжка) зброї й патронів; неприбуття бригади інкасаторів до пункту призначення на маршруті у встановлений час (за відсутності з нею зв'язку); дорожньо-транспортна пригода з тяжкими наслідками (наявність постраждалих, утрата готівки, цінностей або зброї та ін.); виявлення в/на спецавтомобілі невідомих предметів, що є потенційним джерелом небезпеки; пожежа в салоні спецавтомобіля; форс-мажорні обставини: повінь, пожежа, землетрус та інші стихійні лиха; війна або військові дії |
| Порядок дій в екстремальній ситуації | 1) швидко і правильно оцінити сформовану обстановку (характер зовнішнього впливу, ступінь небезпеки);<br>2) визначити варіанти подальшого розвитку подій;<br>3) прийняти рішення про порядок своїх дій;<br>4) посилити спостереження за навколишнім середовищем;<br>5) за потреби надати першу медичну допомогу потерпілим;<br>6) викликати швидку допомогу та міліцію |

Закінчення табл. 5.3

| 1 | 2 |
|---|---|
| Правила поведінки в екстремальній ситуації | У всіх випадках нападу на бригаду інкасаторів або на спецавтомобіль водій-інкасатор умикає звукову та світлову сигналізацію |
| | Зброю застосовувати, не допускаючи захоплення автомобіля |
| | Старший бригади (інший член бригади) інкасаторів негайно повідомляє за допомогою засобів зв'язку черговому про необхідність у наданні допомоги бригаді інкасаторів |
| | Черговий негайно передає інформацію в найближче відділення МВС і станцію швидкої допомоги |
| | Черговий інкасатор дає також указівку резервній бригаді підготуватися до виїзду і, за вказівкою керівника підрозділу інкасації (заступника) або самостійно за їх відсутності, відправляє на місце події |
| | Черговий інкасатор: виконує вказівки керівника підрозділу інкасації (заступника); постійно підтримує зв'язок із бригадою інкасаторів, уточнює інформацію про розвиток подій і реагує на нові повідомлення з метою надання сприяння бригаді; повідомляє клієнтам про затримку або скасування заїзду інкасаторів |
| | Керівник підрозділу інкасації, отримавши повідомлення про надзвичайну ситуацію на маршруті: негайно доповідає про подію керівнику банку (заступнику керівника банку, який курирує діяльність підрозділу інкасації) та інформує керівника підрозділу безпеки з метою надання сприяння бригаді інкасаторів, що опинилася в надзвичайній ситуації; за потреби дає вказівку черговому інкасатору про відправлення резервної бригади (резервного спецавтомобіля) до місця події або виїжджає на місце події на чолі резервної бригади |
| | У разі застосування нападниками хімічних засобів (ОВ) члени бригади надягають протигази |
| | Бригаді категорично заборонено переслідувати нападників.<br>Не намагатися відірватися від переслідувачів, використовуючи рельєф місцевості та велику швидкість |
| | У разі блокування автомобіля і неможливості продовження руху члени бригади готують для використання протигази, перевіряють надійність запорів усіх дверей і люків автомобіля |

Існують різні види нападів на інкасаторські автомобілі. Їх перелік наведено в табл. 5.4.

Таблиця 5.4

**Види нападів на інкасаторські автомобілі**

| Види нападів | Характеристики |
|---|---|
| Стаціонарна засідка | Організовано з метою зупинки або блокування автомобіля інкасації в ході його руху. Злочинці можуть створити імітацію аварійної ситуації, ремонту дороги тощо. Для цього використовують легкові та вантажні автомобілі, будь-який транспорт, колоди, сміттєві баки, контейнери, ящики та інші предмети. Намагайтеся уникнути пасток, об'їжджаючи перешкоди. Слід ураховувати особливості місцевості, швидкість руху автомобіля, стан дорожнього покриття, відстань до перешкоди, інтенсивність руху, можливість тарана, кліматичні умови. Може бути зроблено спробу проникнення в автомобіль методом "автостопу", коли один із злочинців (частіше жінка; особа, яка видає себе за співробітника міліції або військовослужбовця), голосуючи, зупиняє автомобіль із проханням підвезти або надати сприяння в ремонті або буксируванні автомашини. У разі спроби співробітника міліції зупинити спецавтомобіль, старший бригади інкасаторів через зачинене вікно автомобіля подає службове посвідчення інкасатора й повідомляє про те, що бригада виконує завдання з доставки цінностей. Пропонує співробітнику міліції пройти на стаціонарний пост для з'ясування причин зупинки. Не можна наближатися до місць аварії, перешкод на маршруті, виходити з автомобіля |
| Завіса як різновид стаціонарної засідки | Використовують бандгрупами, коли їм відомі "реперні" пункти регулярних маршрутів інкасації. Напад відбувається в момент посадки чи висадки з автомобіля або виходу з об'єкта інкасації |
| Рухома засідка | Бандити "ведуть" автомашину від воріт банку, спостерігають за її відходом і повідомляють сигналом по рації про її рух своїм спільникам. Місцем нападу, зазвичай, вибирають малолюдні вулиці та провулки, заміські дороги, залізничні переїзди (із шлагбаумом), темні й захаращені під'їзди до об'єктів, що інкасують, місця здавання вантажу, які мають прохідні двори, під'їзди, сходові клітки |
| Комбінована засідка | Автомобіль інкасації, маршрут якого відомий, "веде" автомобіль злочинців до місця, де розміщено стаціонарну засідку. У цьому місці розворот автомашини інкасації у зворотному напрямку виявляється неможливим, оскільки ззаду її вже "заблокувала" автомашина злочинців |

У процесі руху інкасаторської машини можуть виникати й нестандартні ситуації на маршруті, що можуть бути початком надзвичайних ситуацій або призвести до надзвичайних ситуацій. **Нестандартні ситуації на маршруті інкасації** – це ситуації, пов'язані з непередбаченою зміною умов роботи бригади інкасаторів на маршруті, які можуть мати негативний вплив на здійснення операцій із інкасації та доставки готівки й цінностей, забезпечення безпеки бригади та схоронність перевезених нею готівки та цінностей. Нестандартні ситуації наведено на рис. 5.1.

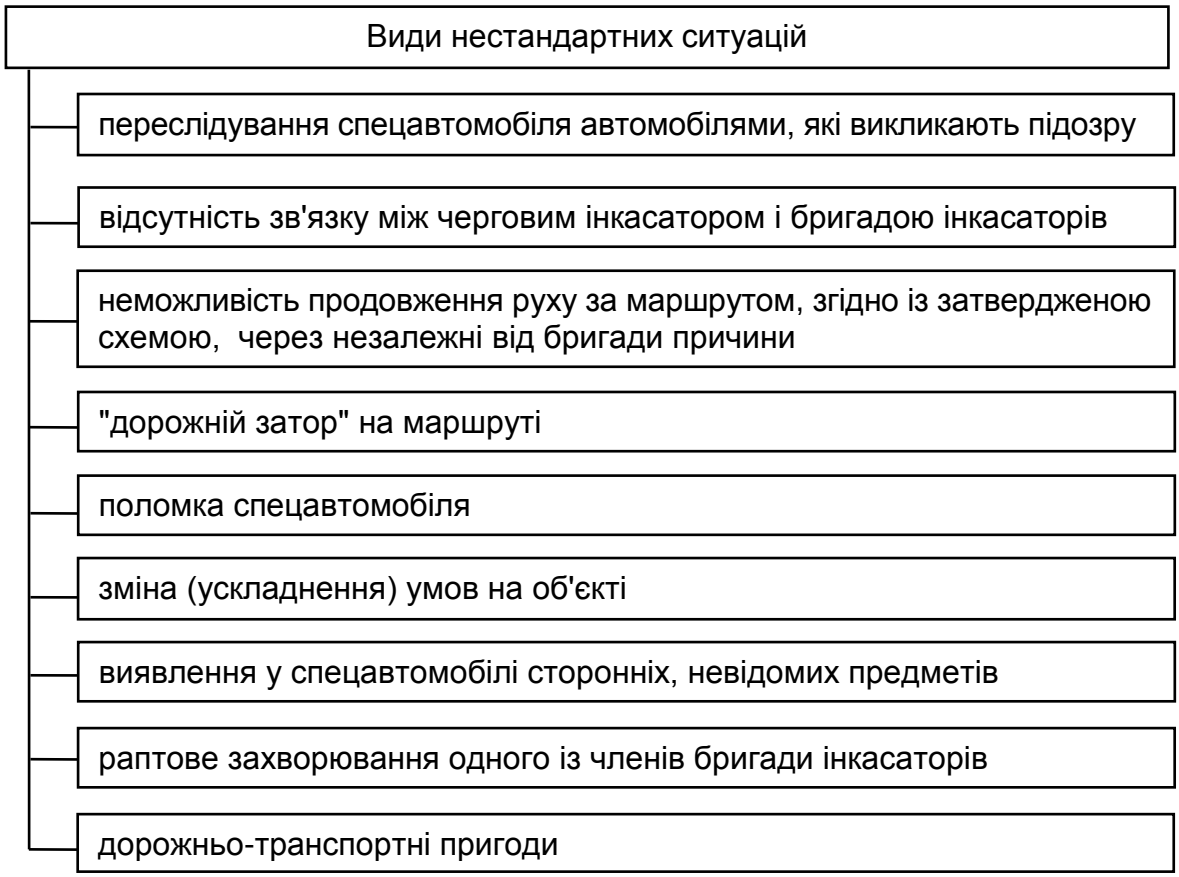


Рис. 5.1. **Види нестандартних ситуацій у роботі інкасаторів**

У разі виникнення нестандартної ситуації старший бригади інкасаторів зобов'язаний: оцінити сформовану обстановку; прийняти рішення про порядок дій бригади й дати вказівки членам бригади на дотримання запобіжних заходів щодо зберігання життя членів бригади, охорони та захисту перевезеної готівки, цінностей і зброї. Про виникнення нестандартної ситуації старший бригади (інший член бригади) негайно повідомляє черговому інкасатору і згодом підтримує з ним зв'язок, періодично повідомляє про зміну обстановки, виконує отримані від нього вказівки. Особливості поведінки інкасаторів у нестандартних ситуаціях наведено в табл. 5.5.

Таблиця 5.5

## Особливості поведінки інкасаторів у нестандартних ситуаціях

| Види нестандартних ситуацій | Дії інкасаторів |
|---|---|
| 1 | 2 |
| Виявлені несправності автомобіля на маршруті інкасації | Водій зупиняє автомобіль у безпечному місці, умикає сигнал аварійної зупинки, виставляє знак аварійної зупинки. Усі двері має бути закрито зсередини салону автомобіля. Старший бригади повідомляє черговому по підрозділу інкасації про те, що трапилося. До прибуття резервного автомобіля старший бригади організовує кругове спостереження й охорону цінностей, інформуючи чергового про всі зміни, що відбуваються на прилеглій до шляху руху автомобіля території. Із прибуттям резервного автомобіля бригада переносить до нього цінності під охороною резервної бригади. Автомашини розташовують у протилежному напрямку на найменшій відстані одна від одної з увімкненими аварійними сигналами. Через відкриті бічні двері (які є додатковим захистом) цінності перевантажують із салону до салону. У цьому разі один або кілька членів бригади інкасаторів здійснюють охоронні функції. Першими закривають броньовані двері навантаженого автомобіля. Після доповіді старшим бригади інкасаторів черговому по підрозділу інкасації про перевантаження цінностей бригада на резервному автомобілі продовжує інкасацію (доставку цінностей). Начальник підрозділу (черговий) уживає заходів щодо буксирування несправного автомобіля на ремонтну базу. Черговий по підрозділу (начальник інкасації) повідомляє в організації про затримання заїзду інкасаторів, уживаючи заходів щодо забезпечення безпечного продовження операцій на маршруті |
| Дорожньо-транспортна пригода | Спецавтомобіль залишають на місці ДТП, умикають аварійний сигнал і виставляють знак аварійної зупинки. Усі члени бригади інкасації перебувають у машині. Старший бригади або один з членів бригади повідомляє черговому по підрозділу про подію. Постраждалим членам бригади надають першу долікарську допомогу. Якщо в результаті ДТП постраждав один із членів бригади і він потребує термінової госпіталізації, старший бригади тимчасово вилучає в нього зброю і боєприпаси для подальшого здавання черговому по підрозділу, складаючи акт у довільній формі. Надалі бригада діє за рішенням начальника інкасації. Начальник інкасації повідомляє про затримання інкасації та заміну бригади клієнтам і організовує продовження маршруту резервною бригадою |

Закінчення табл. 5.5

| 1 | 2 |
|---|---|
| Загоряння в салоні спецавтомобіля | Водій зупиняє машину і відмикає живлення. Старший бригади вживає заходів щодо гасіння вогнища загоряння, доповідає про це черговому по підрозділу (начальникові інкасації). За неможливості ліквідувати займання бригада інкасаторів організовує евакуацію цінностей у безпечне місце, їх охорону, надає допомогу постраждалим і чекає прибуття пожежних розрахунків і резервної бригади. Надалі бригада діє за рішенням начальника інкасації (чергового). Начальник інкасації (черговий) повідомляє клієнтам про затримання інкасації та вживає заходів до евакуації цінностей і відновлення руху за маршрутом |
| Виявлення у спецавтомобілі вибухового пристрою | Старший бригади повідомляє про це черговому по підрозділу, уживає заходів щодо евакуації бригади й цінностей у безпечне місце (краще за все в найближчий касовий вузол чи підприємство, що інкасують), організовує охорону цінностей до прибуття резервного автомобіля із бригадою інкасаторів. Черговий по підрозділу інкасації повідомляє про подію в міліцію і відправляє до місця події резервну бригаду, далі повідомляє в організації клієнтів про затримання заїзду інкасації |
| Переслідування бригади інкасації | Слід використовувати можливість руху за іншими (резервними) маршрутами. Необхідно створити умови для маневрування автомашиною на швидкості в обмеженому просторі. До місця укриття або міліції треба їхати добре відомими вулицями, використовуючи особливості маршруту руху, намагатися вибирати резервний маршрут, що виключає блокування автомобіля |

Правильна поведінка персоналу має неабияке значення і в разі техногенних аварій, тобто не керованих людиною ситуацій. Персонал має знати та виконувати ряд правил поведінки в таких ситуаціях (табл. 5.6).

Таблиця 5.6

## Правила поведінки банківського персоналу під час техногенних аварій

| Види нестандартних ситуацій | Дії інкасаторів |
|---|---|
| 1 | 2 |
| Затоплення приміщень банку | виявити джерело затоплення та вжити заходів щодо його перекриття; евакуювати персонал, цінності та документи із затоплених або тих, яким загрожує затоплення, приміщень; |

Закінчення табл. 5.6

| 1 | 2 |
|---|---|
| | вимкнути електропостачання;<br>якщо вода зійшла, перевірити справність та стан будинку банку, приміщень, каналізації, електромереж та мереж зв'язку;<br>ужити заходів щодо ліквідації наслідків затоплення |
| Землетрус | персонал, який перебуває на першому поверсі, має змогу залишити будівлю банку;<br>у разі перебування на другому і вищих поверхах потрібно зайняти найбільш безпечне місце;<br>заборонено користуватись ліфтами, спускатись сходами, ховатись у кутових приміщеннях;<br>за можливості відімкнути електроживлення, загасити будь-який вогонь;<br>якщо поштовхи припинились, негайно залишити будівлю;<br>у разі заблокування персоналу у приміщеннях слід подати голос; постукати у стіни, щоб установити контакт;<br>після закінчення землетрусу вжити всіх заходів щодо пошуку і звільнення з-під завалів людей, надання їм медичної допомоги;<br>визначити місцезнаходження сховищ, архівів серед руїн банку; організувати спостереження за ними до завершення ліквідаційних робіт, а за можливості й евакуацію цінностей |
| Виявлення вибухових пристроїв та підозрілих предметів | здійснити невідкладні заходи щодо організації особистої безпеки та присутніх;<br>повідомити керівника банку та керівника підрозділу безпеки про виявлений вибуховий пристрій чи підозрілий предмет;<br>заборонити користуватись мобільним телефоном поблизу місця знаходження вибухового пристрою;<br>у подальшому діяти за вказівками керівництва установи |

Під час отримання поштових надходжень, кур'єрських доставок слід звернути увагу на наявність позначки "Особисто в руки", надмірну поштову оплату, вагу, ретельне або нетрадиційне пакування, незвичайний запах.

## Семінарське заняття

1. Найбільш поширені проблеми захисту таємниць комерційних банків в Україні.

2. Профілактика розголошення таємниць банку та запобігання йому.

3. Законодавче забезпечення захисту банківської та комерційної таємниці й конфіденційної інформації.

4. Види відповідальності за зазіхання на інформацію банку.

5. Організація захисту комерційних таємниць банків.

6. Критерії визнання інформації комерційною таємницею.

7. Профілактика розголошення комерційних таємниць банківських установ та запобігання йому.

### Тематика доповідей

1. Поняття про силову безпеку.
2. Організації охорони в банку.
3. Вимоги до працівників охорони.
4. Дії групи управління банком в екстремальних умовах.

### Теоретичні питання для самостійного опрацювання

5.1. Технічні аспекти забезпечення належного режиму охорони банківських установ.

5.2. Положення про відділ охорони в банківських установах.

5.3. Види екстремальних умов роботи в банківських установах.

5.4. Ознаки настання екстремальних умов.

### Методичні рекомендації щодо виконання самостійної роботи

Теоретичні питання опрацьовують на основі літературних джерел: [10 – 13; 21; 25].

### Контрольні запитання

1. Назвати необхідне обладнання для забезпечення безпеки банківської установи.
2. Визначити поняття технічного зміцнення банків.
3. Розкрити порядок організації охорони в установах банків.
4. Що становлять режими охорони в банках?
5. Охарактеризувати дії установ банків в екстремальних умовах.
6. Назвати основні вимоги до обладнання входу банку.
7. Розкрити порядок обладнання каси в банку.
8. Охарактеризувати фактори, що впливають на вибір форм і методів охорони.
9. Назвати види охорони.
10. Що таке "перепустковий режим"?
11. Які види перепусток можуть застосовуватися?

## Тести

*Тести одиничного вибору*

1. Комплекс організаційних та спеціальних заходів, спрямованих на обмеження доступу до установ банку, захист його території, приміщень, об'єктів та персоналу від протиправних зазіхань, – це:

а) охорона банку;

б) недобросовісна конкуренція;

в) промислове шпигунство;

г) власний варіант відповіді.

2. Порядок допуску працівників банку до режимних приміщень, порядок відкривання, закривання і здавання під охорону робочих приміщень, порядок видачі та зберігання ключів від робочих приміщень, металевих печаток для опечатування дверей приміщень становить:

а) систему внутрішньооб'єктового режиму;

б) систему зовнішньооб'єктового режиму;

в) систему охорони;

г) систему безпеки банку;

д) власний варіант відповіді.

*Тести множинного вибору*

3. Основні вимоги до обладнання входу такі:

а) усунення можливості несанкціонованого проникнення до банку сторонніх осіб;

б) забезпечення зручності проходу в банк його службовців;

в) відповідність естетичним нормам;

г) відсутність перешкод;

д) відеообладнання.

4. Можливі джерела злочинних зазіхань на банки такі:

а) характеристика технічного зміцнення установ банків;

б) наявність і характеристики охоронно-пожежної сигналізації;

в) наявність уразливих місць у технічному зміцненні банку;

г) умови розташування установи, її конструктивні особливості;

д) технічна оснащеність сил охорони.

*Тести на встановлення відповідності*

5.1. Види охорони такі:

5.2. Види перепусткового режиму такі:

а) цілодобова фізична охорона;

б) у робочий час фізична охорона із залученням відповідних технічних засобів охорони для спостереження сил охорони, у неробочий –

охорона тільки за допомогою відповідних технічних засобів охорони, залучених для спостереження сил охорони;

в) цілодобова охорона тільки за допомогою відповідних технічних засобів охорони;

г) відсутність охорони;

д) охоронний режим;

е) порядок приймання відвідувачів і видачі перепусток;

є) порядок пропускання осіб;

ж) порядок пропускання транспортних засобів і матеріальних цінностей;

з) порядок документування порушень перепусткового режиму;

и) тимчасовий режим;

і) постійний режим.

6.1. Постійні перепустки:

6.2. Тимчасові перепустки:

6.3. Разові перепустки:

6.4. Перепустки для клієнтів операційних підрозділів:

6.5. Матеріальні перепустки:

а) видають особам, які перебувають у штаті банку, працівникам охорони та особам, яких обслуговують ТЗО;

б) зазвичай, для штатних працівників на період терміну випробування; осіб, що працюють за трудовою угодою або у складі тимчасових колективів;

в) для всіх відвідувачів, вона є одноразовою і дійсною протягом робочого дня;

г) для представників підприємств, яких обслуговують у банку;

д) дають право винесення (вивезення) із банку вказаних у них матеріальних цінностей.

# 6. Інформаційна безпека банківських установ

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

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

**Основні питання:**

6.1. Сутність інформаційної безпеки банку.

6.2. Неправомірне розголошення інформації та захист від нього.

6.3. Правове регулювання захисту таємниць банків.

6.4. Нормативна база банку із забезпечення інформаційної безпеки.

**Література:** [13; 17; 24; 28; 29].

## 6.1. Сутність інформаційної безпеки банку

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

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

Інформаційна безпека у практичному аспекті означає комплекс засобів, застосування яких дозволяє забезпечити належний доступ до інформації та її захист від витоку й неправомірного використання з шахрайською метою шпигунами або недобросовісними конкурентами.

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

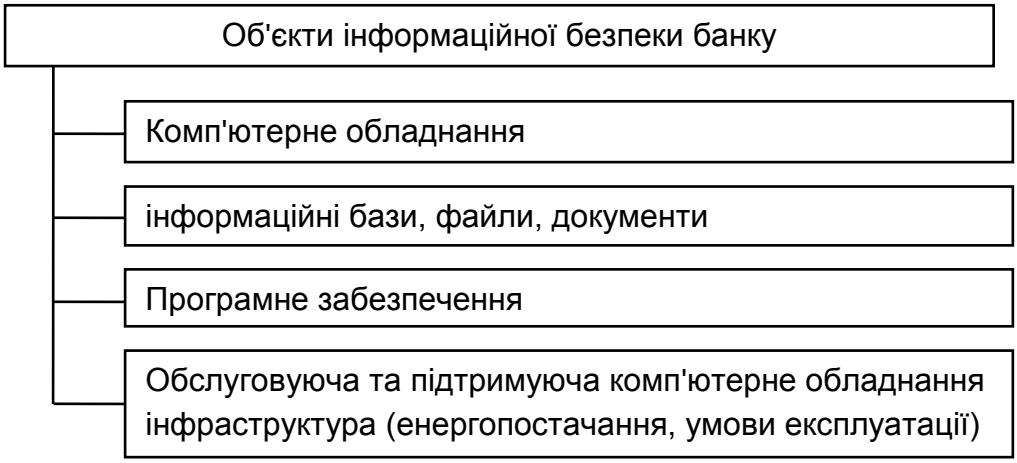


Рис. 6.1. **Об'єкти інформаційної безпеки банку**

*Принципи інформаційної безпеки банківських установ*:

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

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

3) адекватність – означає розроблення і впровадження заходів захисту, адекватних характеру виявлених загроз, ураховуючи витрати на їх реалізацію і сумісність цих заходів із діючим банківським технологічним процесом. Ці заходи не мають суперечити стратегічним цілям банку;

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

5) контрольованість – усі операції з доступом до банківської інформації повинні мати контрольований характер;

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

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

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

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

недотримання банківської таємниці банківським персоналом;

прагнення персоналу заробити додаткові гроші;

ненадійна система захисту банківської інформації;

незадоволеність персоналу роботою в банку;

звичка персоналу поділитися чутками, плітками, здогадками;

конфліктні ситуації;

безконтрольний доступ до банківської інформації.

*Загрози інформаційній безпеці банківської установи* містять:

саботаж;

крадіжку програмного забезпечення та інформаційних ресурсів;

шахрайські дії;

несанкціонований доступ до інформаційної системи банку;

розголошення комерційних таємниць банку;

знищення інформації;

підміну інформації, її викривлення;

знищення або викрадення носіїв банківської інформації;

організацію перебоїв у функціонуванні банківської інформаційної системи.

## 6.2. Неправомірне розголошення інформації та захист від нього

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

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

Способи витоку інформації наведено в табл. 6.1.

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

Таблиця 6.1

## Способи витоку інформації в банківській системі

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

Найчастіше несанкціонований доступ здійснюють щодо такої інформації:

платіжні документи;

внутрішні платіжні документи;

кредитні документи;

документи на грошові перекази;

персональні дані клієнтів та працівників банку;

статистичні звіти;

інші документи, які містять інформацію з обмеженим доступом.

Отримувачами цієї конфіденційної інформації є:

спецслужби конкурентів;

кримінальні елементи;

ЗМІ;

різні інформаційні, детективні агентства;

промислові шпигуни.

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

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

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

Існує багато каналів витоку інформації, а саме: акустичні та акустико-перероблювальні, електромагнітні (у тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії та ін.).

Ці канали передачі інформації використовують як за мимовільного витоку інформації, так і під час зумисного розголосу.

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

Таблиця 6.2

## Характеристики каналів витоку банківської інформації

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

Заходи захисту інформації в засобах і мережах передачі інформації містять такі:

апаратні;

програмні;

криптографічні.

Крім того, існують фізичні, законодавчі та профілактичні заходи.

Загальну характеристику засобів захисту наведено в табл. 6.3.

Таблиця 6.3

**Характеристика засобів захисту банківської інформації**

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

Закінчення табл. 6.3

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

Вибір засобів захисту інформації в банківських установах є надто складним завданням, оскільки банк уважає за потрібне досягти абсолютного захисту і водночас обрати зі значної різноманітності технічних і програмних засобів найбільш ефективні й дієві для умов функціонування конкретного банку.

## 6.3. Правове регулювання захисту таємниць банків

Згідно із Законом України "Про банки і банківську діяльність", *банківською таємницею* є будь-яка інформація, що стосується клієнта, якою банк володіє на законних підставах (за винятком, якщо така інформація становить державну таємницю), тобто інформація про діяльність і фінансовий

стан клієнта, що стала відома банку у процесі його обслуговування і взаємовідносин із ним або третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди клієнту [24].

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

Структурно всю банківську інформацію розподіляють на відкриту та інформацію з обмеженим доступом (рис. 6.2) [13].

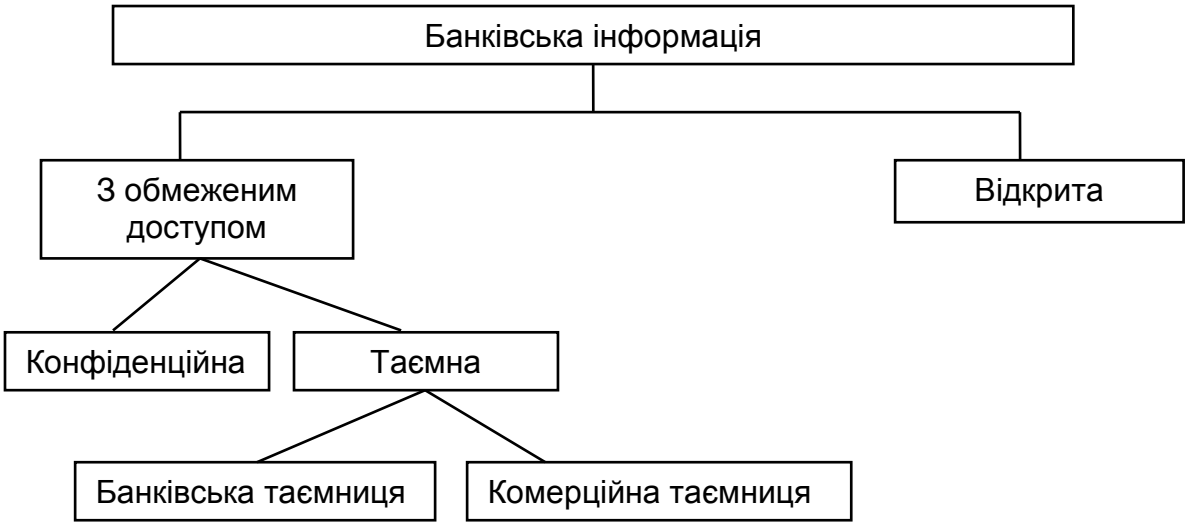


Рис. 6.2. **Структура банківської інформації**

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

Правовий режим доступу до банківської таємниці встановлено Законом України "Про банки і банківську діяльність". Інформацію, що становить

банківську таємницю фізичних осіб – клієнтів банку, розкриває банк на письмовий запит або з письмового дозволу власника інформації, а також на письмову вимогу або за рішенням суду. Водночас банківську таємницю юридичних осіб – клієнтів банку, крім зазначених умов, розкривають у таких випадках:

банкам заборонено надавати інформацію про клієнтів іншого банку, навіть якщо їхні імена вказують в документах, угодах і операціях клієнта;

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

Комерційною таємницею не можуть бути [13]:

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

інформація за всіма формами державної звітності;

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

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

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

інформація про забруднення навколишнього середовища, порушення умов безпеки праці;

відомості, які, відповідно до чинного законодавства, підлягають опублікуванню.

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

## 6.4. Нормативна база банку із забезпечення інформаційної безпеки

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

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

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

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

Положення про забезпечення безпеки під час надання послуг за міжнародними банківськими платіжними картками;

Інструкція про порядок надання доступу користувачам до автоматизованих банківських систем;

Інструкція про проведення службових розслідувань в установах банку;

Положення про порядок підготовки, надсилання, опрацювання та зберігання електронних документів під час використання електронної пошти;

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

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

Положення про технічний захист інформації в банку;

Технологічна інструкція служби фінансової безпеки;

Положення про порядок одержання доступу до локальної обчислювальної мережі та ресурсів систем електронного опрацювання інформації;

Положення про режимні приміщення банку;

угоди про конфіденційність із клієнтами, партнерами та іншими суб'єктами, із якими банк вступає у правовідносини, різного характеру пам'ятки, інструкції, заяви;

список осіб, до відома яких у повному обсязі може доводитись інформація, що становить банківську і комерційну таємницю та є конфіденційною.

Слід розглянути основні нормативні документи банку з інформаційної безпеки.

Положення про комерційну таємницю і конфіденційну інформацію містить [13]:

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

порядок захисту конфіденційної інформації в установах банку;

відповідальність за організацію заходів захисту;

відповідальність за розголошення конфіденційних відомостей.

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

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

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

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

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

загальні обов'язки персоналу банку щодо зберігання його таємниць;

порядок доступу на засідання і наради, де обговорюють питання, у яких наявна інформація з обмеженим доступом;

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

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

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

## Семінарське заняття

1. Види неправомірного отримання інформації та захист від нього.
2. Законодавче регулювання захисту таємниць банків.
3. Відповідальність за зазіхання на таємниці банків.
4. Нормативна та інформаційна база банку щодо управління інформаційною безпекою.
5. Поняття про інформаційний моніторинг у банківській установі.

## Тематика доповідей

1. Матеріально-речові та акустичні канали інформації.
2. Фактори, що створюють умови для витоку інформації.
3. Засоби посилення інформаційної безпеки в банківських та фінансових установах.

## Питання для самостійного опрацювання

6.1. Сутність поняття "комерційна таємниця".

6.2. Види відповідальності за порушення банківської таємниці.

6.3. Сутність поняття "інформаційна безпека".

## Методичні рекомендації щодо виконання самостійної роботи

Теоретичні питання та тестові завдання опрацьовують на основі літературних джерел: [13; 17; 24; 28; 29].

## Контрольні запитання

1. Назвати види неправомірного отримання інформації.
2. Охарактеризувати сутність несанкціонованого доступу до інформації.
3. Назвати способи захисту від неправомірного отримання інформації.
4. Охарактеризувати правове регулювання захисту таємниць банків.
5. Назвати види відповідальності за порушення комерційної таємниці.
6. Охарактеризувати нормативну базу банківських установ з інформаційної безпеки.
7. Назвати фактори, що створюють умови для витоку інформації.
8. Назвати завдання захисту від несанкціонованого доступу до інформації.
9. Охарактеризувати організаційні, організаційно-технічні та технічні заходи захисту інформації.
10. Розкрити сутність структури банківської інформації.
11. Охарактеризувати види інформації, документації, що не може бути комерційною таємницею.
12. Визначити поняття цивільної відповідальності за розголошення комерційної таємниці.
13. Дати перелік нормативних актів українських банків щодо захисту їх інформації з обмеженим доступом.

## Тести

*Тести одиничного вибору*

1. Витік інформації – це:

а) мимовільне поширення інформації за рахунок технічних або експлуатаційних особливостей певного обладнання, утрати, пошкодження,

знищення документальних та програмних носіїв інформації в результаті дії стихійного лиха, поширення інформації через потрапляння в інформаційні мережі комп'ютерних вірусів, інші випадки, які не мають навмисного характеру;

б) розголошення інформації, що має навмисний характер;

в) оголошення, передання, надання для ознайомлення інформації;

г) доступ до інформації, який здійснено з порушенням установлених правил розмежування доступу.

2. Організаційні заходи апаратного захисту – це:

а) заходи обмежувального характеру, які передбачають регламентацію доступу і використання технічних засобів передавання й опрацювання інформації;

б) заходи, що забезпечують блокування можливих каналів витоку інформації;

в) заходи, які забезпечують використання спеціальних, захищених від побічних випромінювань технічних засобів;

г) власний варіант відповіді.

*Тести множинного вибору*

3. За призначенням апаратні засоби захисту інформації розподіляють на:

а) засоби виявлення несанкціонованого доступу;

б) засоби захисту від несанкціонованого доступу;

в) абсолютні засоби захисту;

г) відносні засоби захисту;

д) універсальні засоби захисту;

е) специфічні засоби захисту.

4. Каналами отримання інформації є такі:

а) візуально-оптичні;

б) акустичні;

в) електромагнітні;

г) змішані;

д) комбіновані.

5. Апаратні засоби захисту банківської інформації містять:

а) організаційні;

б) організаційно-технічні;

в) технічні;

г) програмні;

д) криптографічні.

*Тести на встановлення відповідності*

6.1. Акустичні канали:

6.2. Візуально-оптичні канали:

6.3. Електромагнітні канали:

а) створюють як оптичний шлях від об'єкта інформації до її отримувача;

б) джерелом створення такого каналу є тіла та механізми, які здійснюють вібрацію або коливання;

в) канали, що створюються через наявність у технічних засобах, які використовують у виробництві, джерел небезпечних сигналів.

7.1. Джерелами створення акустичних каналів є:

7.2. Факторами, що створюють умови для витоку інформації є:

а) поширення акустичних (механічних) коливань у вільному повітряному просторі;

б) вплив звукових коливань на елементи й конструкції будівель;

в) дія звукових коливань на технічні засоби опрацювання інформації;

г) надмірна балакучість персоналу;

д) мікрофонний ефект, акустична модуляція тощо;

е) наявність передумов для виникнення конфліктів.

# 7. Інформаційно-аналітичне забезпечення діяльності банківських установ

**Мета** – розглянути теоретичні засади та практичні аспекти організації інформаційно-аналітичної роботи в банках у межах управління банківською безпекою.

**Ключові поняття:** інформаційно-аналітична робота, економіст-аналітик, інформаційний аудит, моніторинг банківської діяльності.

**Основні питання:**

7.1. Зміст інформаційно-аналітичної роботи в банках.

7.2. Функції економіста-аналітика в банках.

7.3. Сутність інформаційного аудиту та моніторингу в банках.

7.3.1. Сутність та завдання внутрішнього банківського аудиту.

7.3.2. Сутність та види банківського моніторингу.

**Література:** [13; 16; 18; 20; 22; 25; 32].

## 7.1. Зміст інформаційно-аналітичної роботи в банках

**Інформаційно-аналітичне забезпечення безпеки банківської діяльності (ІАЗББД)** – це вид інформаційно-аналітичного забезпечення, що полягає у збиранні, опрацюванні, зберіганні й наданні необхідної інформації щодо стану безпеки відповідним користувачам.

**Головна мета ІАЗББД** – це своєчасне виявлення й забезпечення загроз банківській безпеці.

Керівництво ІАЗББД здійснює начальник служби безпеки. ІАЗББД формує служба безпеки на основі власної інформації та інформації інших структурних спецпідрозділів: кредитного відділу, відділу валютних операцій, розрахунково-касового обслуговування, охорони та ін.

**Основним змістом управління ІАЗББД** є збирання та аналіз даних щодо вірогідних загроз та засобів протидії їх негативному впливу з метою прийняття рішень щодо всебічного забезпечення банківської безпеки. ІАЗББД має забезпечувати потреби керівництва та служби безпеки в інформації щодо загроз діяльності банківської установи чи особистій безпеці персоналу.

**Організація ІАЗББД** – це комплекс організаційних і практичних заходів щодо розроблення змісту, способів дій, термінів та послідовності

виконання силами й засобами служби банківської безпеки інформаційно-аналітичних завдань.

Елементи організації ІАЗББД наведено на рис. 7.1.

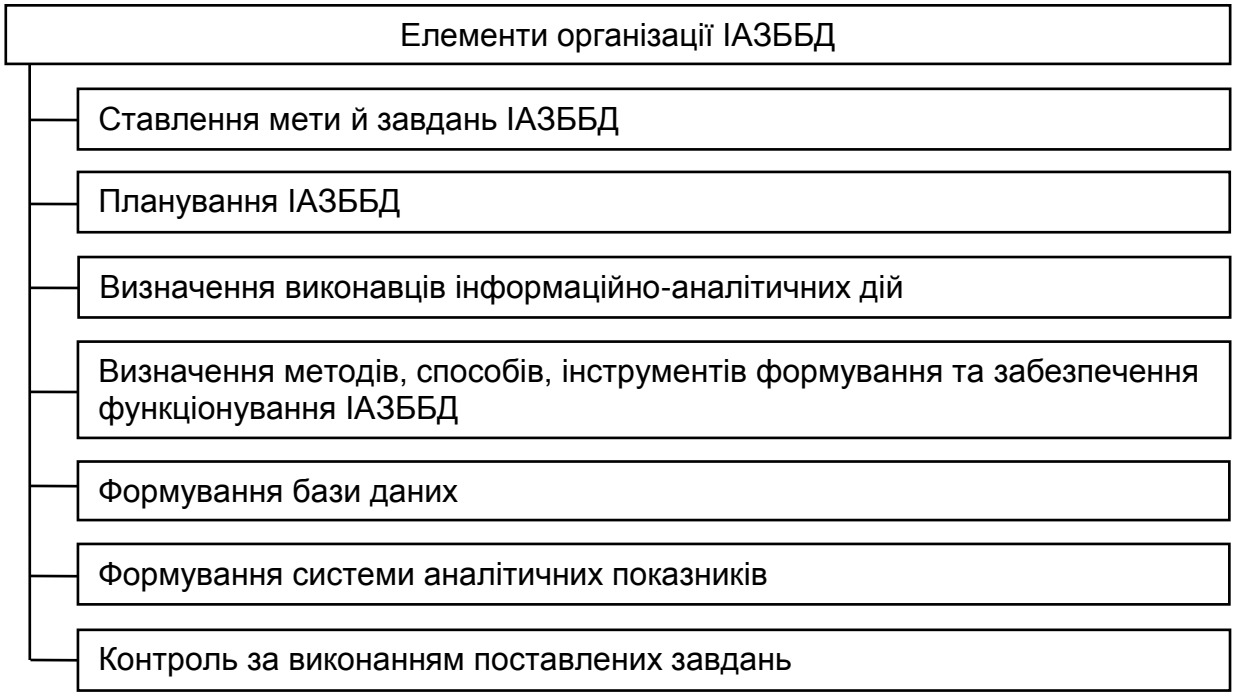


Рис. 7.1. **Елементи організації ІАЗББД**

**Інформаційно-аналітична робота банку із забезпечення безпеки –** це комплекс заходів, які здійснює відділ безпеки банку з метою збирання та опрацювання інформації про загрози і стан безпеки та розроблення відповідних інформаційно-аналітичних документів для керівництва банку.

Етапи функціонування інформаційно-аналітичного забезпечення безпеки банку повторюються циклічно і містять: збирання та пошук інформації (головний, найважчий і визначальний); облік, попереднє вивчення, інформаційно-аналітичне опрацювання, формулювання висновків; підготовка інформаційно-аналітичних документів.

ІАЗББД має будуватися на таких *принципах:*

1) достовірність інформації. Інформація має відображувати реальні процеси та показники, що мають місце на підприємстві;

2) вичерпність інформації. Інформація корисна тільки в тому разі, коли вона є повною, а не частковою, оскільки це може призвести до викривлення результатів інформаційно-аналітичної роботи;

3) зіставність інформації. Інформація з різних джерел щодо одного й того ж процесу чи явища має бути ідентичною;

4) оперативність отримання інформації. Інформація має цінність тільки якщо є актуальною;

5) ефективність інформації. Інформаційно-аналітичне опрацювання інформації має бути доцільним, тобто ефект від такого опрацювання має перевищувати витрати на її здійснення;

6) зручність інформації. Інформацію має бути подано у зручному для користування вигляді;

7) доцільність інформації. Інформація має бути корисною, тобто необхідною для здійснення аналітичних розрахунків. Не має відбуватися перевантаження системи ІАЗББД побічною інформацією, що не має відношення до банківської безпеки чи загроз їй.

ІАЗББД сформовано для потреб конкретного банку, залежно від умов його функціонування та можливих загроз його діяльності як із внутрішнього, так і зовнішнього середовища.

ІАЗББД сформовано з використанням автоматизованої банківської системи. Вона містить такі підсистеми:

операційний день банку (ОДБ);

управління кредитними ресурсами банку;

управління валютними операціями;

управління депозитами;

управління цінними паперами;

управління касою;

внутрішньобанківський облік;

управління розрахунками з використанням пластикових карток;

звітність банку;

аналіз діяльності банку.

Кожна із цих підсистем є джерелом інформації, що використовують у процесі формування ІАЗББД.

До банку даних щодо загроз безпеці банківської діяльності має автоматично потрапляти інформація з підсистем автоматизованої банківської системи.

## 7.2. Функції економіста-аналітика в банках

Аналітичні операції виконуються інформаційно-аналітичним підрозділом банку.

Основними завданнями інформаційно-аналітичного підрозділу є:

формування інформаційного забезпечення аналізу діяльності банку;

створення автоматизованих інформаційних баз даних;

організація інформаційно-аналітичного дослідження вітчизняного ринку банківських послуг;

організація та здійснення інформаційного аудиту та інформаційного моніторингу;

інформаційно-аналітичне дослідження клієнтської бази банку.

**Функції економістів-аналітиків** підрозділів установ банку такі:

аналіз ефективності технологій здійснення банківських операцій;

проведення інформаційного аудиту;

участь в аналітичних дослідженнях, що здійснюються клієнтами, партнерами та іншими суб'єктами ринку банківських послуг;

розроблення пропозицій щодо оптимізації та вдосконалення банківських продуктів та перспектив їх розвитку;

оцінювання ефективності депозитних, кредитних та розрахунково-касових операцій;

прогнозування основних показників діяльності банку;

оцінювання фінансових результатів банку.

Аналіз безпеки банківської діяльності здійснює відділ безпеки банківської діяльності. Аналітичну роботу виконують аналітики з питань фінансово-економічної безпеки. Їх функції відображують у посадовій інструкції, що складено на основі Довідника кваліфікаційних характеристик професій працівників "Безпека господарської діяльності підприємства, установи, організації". Цей довідник розроблено Державною установою "Науково-дослідний інститут соціально-трудових відносин" Міністерства соціальної політики України за участю фахівців Всеукраїнської організації "Український союз промисловців і підприємців", Університету економіки та права "КРОК", Київського національного економічного університету імені Вадима Гетьмана, Національної академії Служби безпеки України, Інституту стандартів безпеки, Інституту Управління державної служби охорони України Київського національного університету імені Тараса Шевченка та ТОВ "ДТЕК".

У Довіднику кваліфікаційних характеристик професій працівників "Безпека господарської діяльності підприємства, установи, організації" зазначено завдання, обов'язки, знання та кваліфікаційні вимоги до економіста з питань фінансово-економічної безпеки.

На основі довідника визначають:

*1. Завдання та обов'язки аналітика з питань фінансово-економічної безпеки банку.* Організовує аналітичні та методичні практики впровадження заходів із фінансово-економічної безпеки. Бере участь у розробленні, удосконаленні та реалізації теоретико-практичних методів забезпечення необхідною інформацією у сфері фінансово-економічної безпеки. Визначає перспективність та ефективність інноваційної діяльності з використанням інформаційних, облікових та аналітичних методів для вдосконалення процесів фінансово-економічної безпеки в межах установлених стандартів і норм. Визначає індикатори економічної безпеки. Забезпечує підготовку документів, необхідних для прийняття управлінських рішень щодо діяльності банку в умовах реальних і потенційних загроз та небезпек, функціонування системи економічної безпеки, ефективної діяльності суб'єктів її забезпечення. Розроблює проекти наказів, положень, інструкцій щодо організації діяльності аналітиків із питань фінансово-економічної безпеки, їх взаємодії з іншими суб'єктами безпеки та інформаційно-аналітичного забезпечення функціонування системи економічної безпеки. Визначає та оцінює стан і рівень фінансово-економічної безпеки банку, партнерів (контрагентів) та конкурентів. Забезпечує визначення зовнішніх і внутрішніх ризиків та загроз у сфері фінансово-економічної безпеки банку. Забезпечує зберігання та примноження матеріальної та фінансової бази банку, раціонального та ефективного використання його ресурсів, надання інформації, необхідної для прийняття управлінських рішень щодо доцільності діяльності банку, ураховуючи виявлені загрози й небезпеки, захист отриманої інформації, яка належить до комерційної таємниці банку, вивчає вплив внутрішніх і зовнішніх загроз на фінансовий результат банківської установи. Сприяє здійсненню стратегічного управління банком і його фінансово-економічною безпекою. Здійснює всі види інформаційного, аналітичного та обліково-аналітичного забезпечення функціонування системи економічної безпеки банків. Бере участь у проведенні діагностики фінансового стану банку з метою запобігання його банкрутству. Організовує проведення моніторингу оцінювання стану безпеки, надійності та рівня: економічного стану підприємства, потенційних партнерів підприємства, стратегії діяльності на ринку конкурентів, максимально повного інформаційного забезпечення функціонування системи економічної безпеки підприємства з метою мінімізації

внутрішніх і зовнішніх загроз. Бере участь у розробленні заходів щодо мінімізації їх впливу на діяльність банку, розробленні стратегічної орієнтації підприємства, ураховуючи вимоги до забезпечення фінансово-економічної безпеки. Бере участь у плануванні заходів із забезпечення фінансово-економічної безпеки, удосконалення інформаційно-аналітичного процесу функціонування системи фінансово-економічної безпеки та плануванні окремих спеціальних заходів щодо оперативного реагування на загрози, ризики, небезпеки в діяльності банку. Розробляє аналітичні документи, за якими здійснюють оцінювання стану та надають пропозиції щодо діяльності банку в умовах загроз і небезпек, рекомендації щодо їх зниження. Надає визначеним керівництвом банку особам аналітичну інформацію щодо фінансово-економічної безпеки. Бере участь у проведенні експертного оцінювання отриманої інформації, визначає рівень її достовірності. Надає пропозиції щодо здійснення заходів безпеки. Розробляє всі види аналітичних документів, які стосуються забезпечення фінансово-економічної безпеки банку. Бере участь у підвищенні кваліфікації працівників свого структурного підрозділу.

*2. Аналітик із питань фінансово-економічної безпеки банку має знати*: Конституцію України, Господарський, Адміністративний, Кримінальний кодекси України, закони й постанови Верховної Ради України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, НБУ та інші нормативно-правові документи, що стосуються сфери фінансово-економічної безпеки; функції, загальні принципи побудови та організації діяльності комплексної системи забезпечення фінансово-економічної безпеки банку; методи проведення аналітичних досліджень; організацію та особливості здійснення інформаційно-аналітичного забезпечення діяльності працівників, які є суб'єктами системи забезпечення фінансово-економічної безпеки; захист інформації та комерційної таємниці в банку; технології, форми та методи діагностування небезпек, загроз і ризиків, їх оцінювання та мінімізації, рівня та стану економічної безпеки, критеріїв її оцінювання в банку; технічні засоби пошуку, отримання, аналізу інформації та її захисту; державну та недержавну системи безпеки; порядок розроблення та ведення аналітичної документації, що регламентує діяльність аналітиків із питань фінансово-економічної безпеки банку; порядок розроблення та впровадження інновацій у систему забезпечення фінансово-економічної безпеки; механізми інформаційно-

аналітичного забезпечення управління системою фінансово-економічної безпеки; порядок організації, здійснення контролю за рівнем фінансово-економічної безпеки та його оцінювання; методи та технології роботи фінансових підрозділів банку, передовий вітчизняний і зарубіжний досвід організації та здійснення інформаційно-аналітичного забезпечення функціонування системи фінансово-економічної безпеки; правила ділового етикету; правила та норми охорони праці та протипожежного захисту; основні принципи роботи з комп'ютером та відповідні програмні засоби; державну мову.

*3. Кваліфікаційні вимоги до аналітиків із питань фінансово-економічної безпеки банків* (табл. 7.1).

Таблиця 7.1

**Кваліфікаційні вимоги до аналітиків із питань фінансово-економічної безпеки банків**

| Посади | Кваліфікаційні вимоги |
|---|---|
| Провідний аналітик із питань фінансово-економічної безпеки | повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра. Стаж роботи за професією аналітика з питань фінансово-економічної безпеки I категорії – не менше від 2 років |
| Аналітик із питань фінансово-економічної безпеки I категорії | повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Стаж роботи за професією аналітика з питань фінансово-економічної безпеки II категорії для магістра – не менше від 1 року, спеціаліста – не менше від 2 років |
| Аналітик із питань фінансово-економічної безпеки II категорії | повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Стаж роботи за професією аналітика з питань фінансово-економічної безпеки для магістра – не менше від 1 року, спеціаліста – не менше від 2 років |
| Аналітик із питань фінансово-економічної безпеки | повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Без вимог до стажу роботи |

## 7.3. Сутність інформаційного аудиту та моніторингу в банках

### 7.3.1. Сутність та завдання внутрішнього банківського аудиту

Положення про організацію внутрішнього аудиту в комерційних банках України містить таке визначення: "Аудит банку – це процес оцінювання стану банку на основі перевірки правильності складання та підтвердження достовірності балансу, обліку прибутків та збитків, аналізу стану обліку, відповідність обліку та дій банку вимогам чинного законодавства, дотримання рівності прав акціонерів (учасників) у ході розподілу дивідендів, голосування, надання прав на придбання нових акцій тощо та підготовки висновків для надання інформації керівництву, акціонерам (учасникам) банку та іншим користувачам".

Внутрішній аудит у банку здійснює служба внутрішнього аудиту банківської установи, яка становить самостійний структурний підрозділ, сформований за рішенням виконавчого органу установи та підпорядкований безпосередньо Правлінню банку.

На службу внутрішнього аудиту банку покладено такі *завдання у сфері дотримання банківської безпеки:*

сприяння адекватності системи внутрішнього контролю за законністю операційних процедур;

здійснення професійного та об'єктивного оцінювання фінансової, операційної та інших систем, а також процедур контролю в банку;

контроль за законністю ведення бухгалтерського обліку;

контроль за якістю функціонування інформаційних систем управління задля своєчасного виявлення та усунення недоліків і порушень у ході здійснення банківських операцій;

оперативне виявлення недоліків та порушень у діяльності банківських структурних підрозділів, прийняття і реалізація оптимальних рішень щодо їх ліквідації, а також усунення причин виникнення недоліків у діяльності банку;

розслідування в межах повноважень охорони банку вчинених порушень та запобігання їм у системі внутрішнього контролю і випадкам виявів будь-яких ризиків;

виявлення та оцінювання сфер потенційних збитків для банку, діагностика сприятливих умов для зловживань, шахрайства і незаконного присвоєння грошових коштів та дорогоцінних металів;

налагодження і підтримання взаємодії із зовнішніми аудиторами, державними органами контролю та службою банківського нагляду Національного банку України.

Внутрішньому аудиту банківської діяльності має передувати тестування системи внутрішнього контролю. За результатами такого тестування складають програми внутрішнього аудиту.

Приклад програми внутрішнього аудиту безпеки кредитних операцій наведено в табл. 7.2.

Таблиця 7.2

Суб'єкт перевірки – внутрішні аудитори.
Період перевірки – 01.04.2015 р. – 31.06.2015 р.
Термін перевірки – 01.08.2015 р. – 05.08.2015 р.

**Програма внутрішнього аудиту безпеки кредитних операцій банку**

| Перелік аудиторських процедур | Виконавці | Терміни перевірки | Примітки |
|---|---|---|---|
| Перевірка рівня навантаження працівників кредитного відділу | Петров О. А. | 01.08.2015 р. | |
| Перевірка усунення порушень та недоліків, виявлених попередніми перевірками | Іванова С. В. | 01.08.2015 р. | |
| Перевірка стану кредитного моніторингу | Петров О. А. | 02.08.2015 р. | |
| Перевірка якості роботи з погашення прострочених кредитів | Іванова С. В. | 02.08.2015 р. | |
| Перевірка обліку кредитних операцій щодо відповідності законодавству | Петров О. А. | 03.08.2015 р. | |
| Перевірка дотримання правил кредитування працівниками кредитного відділу | Іванова С. В. | 03.08.2015 р., 04.08.2015 р. | 10 % вибірка справ |
| Перевірка роботи секторів кредитування у філіях | Петров О. А. | 04.08.2015 р. | |
| Складання переліку виявлених помилок та порушень | Іванова С. В. | 05.08.2015 р. | |

Склав
Перевірив
Ознайомився

### 7.3.2. Сутність та види банківського моніторингу

Існують різні види банківського моніторингу. Із точки зору безпеки банківської діяльності здійснюють фінансовий моніторинг та експрес-моніторинг банківської безпеки.

Обов'язковий фінансовий моніторинг здійснює Державний комітет фінансового моніторингу України (Держфінмоніторинг). Він є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовує і координує Кабінет Міністрів України. Відповідно до законодавства, Державний комітет фінансового моніторингу має здійснювати збирання, опрацювання та аналіз інформації про фінансові операції, що підлягають обов'язковому фінансовому моніторингу або ж інші операції, пов'язані з відмиванням доходів.

Згідно із Законом України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму", **фінансовий моніторинг** – це комплекс заходів у сфері запобігання та протидії легалізації (відмиванню) доходів, отриманих злочинним шляхом, або фінансуванню тероризму [25].

Систему фінансового моніторингу складено із двох рівнів – первинного та державного.

*Фінансові операції, що підлягають обов'язковому фінансовому моніторингу* [25]:

фінансова операція підлягає обов'язковому фінансовому моніторингу в разі, якщо сума, на яку її здійснюють, дорівнює чи перевищує 150 000 грн або дорівнює сумі в іноземній валюті, еквівалентній 150 000 грн, чи перевищує її, та має одну або більше таких ознак:

1) переказ грошових коштів на анонімний (номерний) рахунок за кордон і надходження грошових коштів із анонімного (номерного) рахунка з-за кордону, а також переказ коштів на рахунок, відкритий у фінансовій установі у країні, зарахованій Кабінетом Міністрів України до переліку офшорних зон;

2) зарахування або переказ коштів, надання або отримання кредиту (позички), здійснення інших фінансових операцій у разі, якщо хоча б одна зі сторін-учасників фінансової операції є фізичною або юридичною особою, що має відповідну реєстрацію, місце проживання чи місцезнаходження у країні (на території), що не виконують чи неналежним чином виконують рекомендації міжнародних, міжурядових організацій, що здійснюють

діяльність у сфері боротьби з легалізацією (відмиванням) доходів, отриманих злочинним шляхом, або фінансуванням тероризму, або однією зі сторін є особа, яка має рахунок у банку, зареєстрованому в терористичній країні (території);

3) зарахування на рахунок коштів у готівковій формі з їх подальшим переказом того самого або наступного операційного дня іншій особі;

4) зарахування коштів на поточний рахунок юридичної або фізичної особи-підприємця чи списання коштів із поточного рахунка юридичної або фізичної особи-підприємця, період діяльності якої не перевищує трьох місяців із дня реєстрації, або зарахування коштів на поточний рахунок чи списання готівки з поточного рахунка юридичної або фізичної особи-підприємця в разі, якщо операції на зазначеному рахунку не здійснювали із дня його відкриття;

5) переказ особою коштів за кордон за відсутності зовнішньоекономічного договору (контракту);

6) обмін банкнот, особливо іноземної валюти, на банкноти іншого номіналу;

7) здійснення фінансових операцій із векселями із бланковим індосаментом або індосаментом на подавця;

8) здійснення розрахунку за фінансовою операцією в готівковій формі;

9) здійснення розрахунків за зовнішньоекономічним контрактом, що не передбачає фактичного постачання на митну територію України товарів, робіт і послуг.

*Фінансові операції, що підлягають внутрішньому фінансовому моніторингу:*

1. Фінансова операція підлягає внутрішньому фінансовому моніторингу, якщо вона має одну або більше ознак, визначених цим законом, або містить інші ризики:

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 здійснення фінансових операцій, характер яких дає підстави вважати, що метою їх здійснення є уникнення процедур обов'язкового фінансового моніторингу або ідентифікації, передбачених цим законом.

2. У разі якщо в суб'єкта первинного фінансового моніторингу виникають підстави вважати, що фінансову операцію пов'язано з легалізацією ("відмиванням") доходів, отриманих злочинним шляхом, або фінансуванням тероризму, внутрішній фінансовий моніторинг проводять також щодо інших фінансових операцій, в уточненні яких виникла необхідність.

3. Внутрішньому фінансовому моніторингу підлягають операції, відповідно до типологій міжнародних організацій, що здійснюють діяльність у сфері протидії легалізації ("відмиванню") доходів, отриманих злочинним шляхом, або фінансуванню тероризму.

Метою внутрішньобанківського фінансового моніторингу є протидія фінансуванню тероризму та легалізації отриманих злочинним шляхом доходів через банківську систему.

Відділ фінансового моніторингу виконує такі завдання щодо внутрішнього фінансового моніторингу:

координацію дій банку з діями суб'єктів державного фінансового моніторингу та правоохоронними органами;

прийняття і постійне оновлення програм внутрішнього фінансового моніторингу;

організацію управління фінансовими ризиками;

виявлення фінансових операцій, що підлягають внутрішньому фінансовому моніторингу;

ідентифікацію, вивчення та класифікацію клієнтів, ураховуючи їх минулий досвід у співпраці з банками.

**Експрес-моніторинг банківської безпеки** – це безперервний процес збирання інформації та оцінювання динаміки ключових показників стану банківської безпеки з метою своєчасного виявлення внутрішніх і зовнішніх загроз.

Експрес-моніторинг банківської безпеки здійснюють за відповідного інформаційного, технічного, організаційного та методичного забезпечення. У процесі формування моделі системи експрес-моніторингу банківської безпеки слід виділити чотири основних блоки, у межах яких вирішують питання: а) цільових настанов і завдань експрес-моніторингу; б) організаційно-інформаційного забезпечення процесу експрес-моніторингу; в) методичного забезпечення експрес-моніторингу; г) аналітичного забезпечення (рис. 7.2).

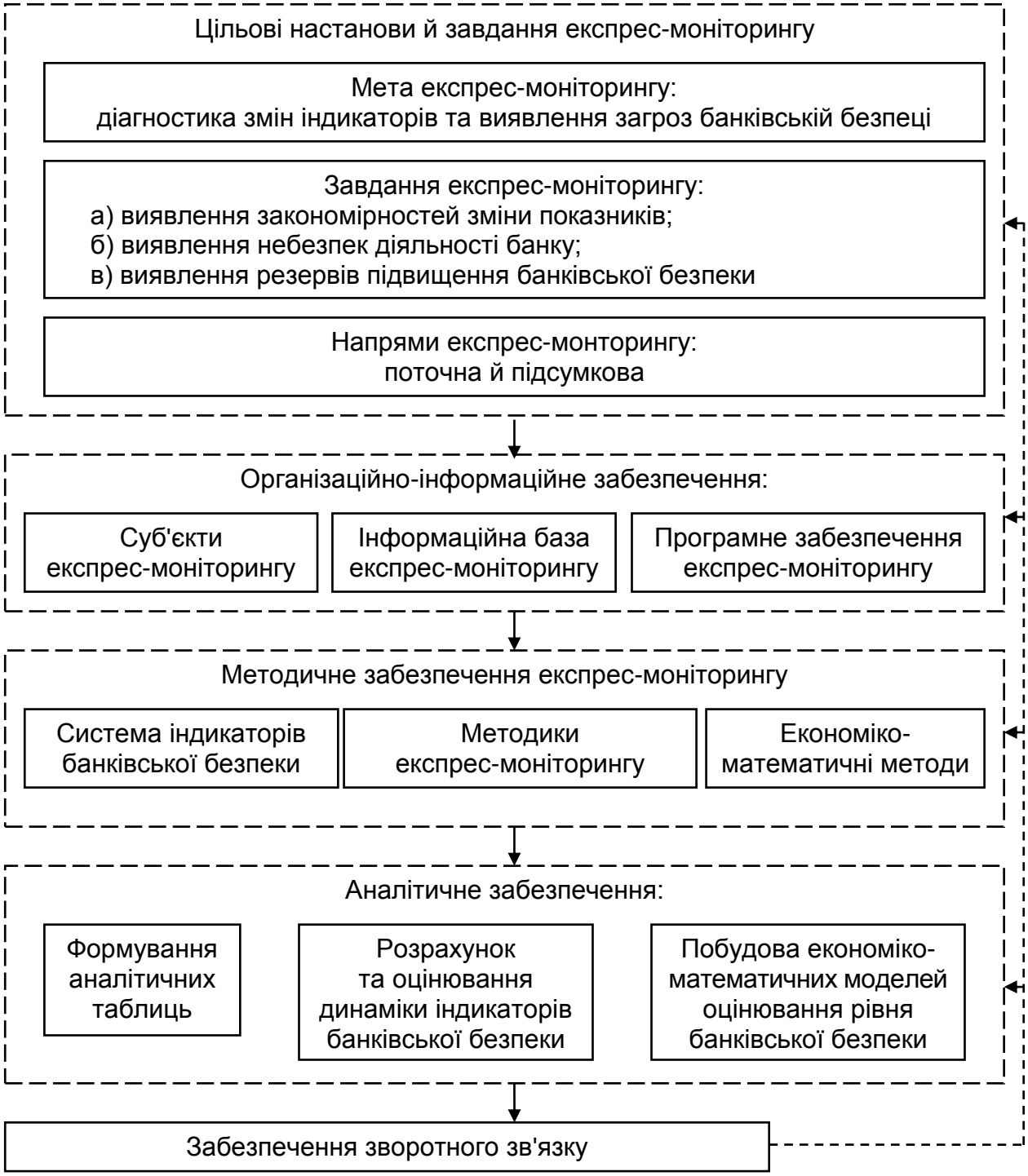


Рис. 7.2. **Модель системи експрес-моніторингу банківської безпеки**

Обґрунтування цільових настанов і завдань є важливим із точки зору формалізації об'єкта оцінювання. Метою експрес-моніторингу є діагностика змін індикаторів та виявлення загроз банківській безпеці. Подана цільова настанова має загальний характер та є підґрунтям для конкретизації завдань оцінювання. Основний етап формування системи експрес-моніторингу пов'язаний із вирішенням питань методичного, організаційно-інформаційного та аналітичного характеру.

Під час конкретизації системи експрес-моніторингу банківської безпеки важливим також є врахування методичних засад її реалізації. Об'єктом щомісячного експрес-моніторингу стають не абсолютні, а відносні показники, показники динаміки, структури та відхилень.

Система показників експрес-моніторингу містить набір груп показників за такими видами безпеки, як: ринкова (табл. 7.3); фінансово-економічна (табл. 7.4); правова, силова та інформаційна (табл. 7.5); кадрова (табл. 7.6).

Таблиця 7.3

**Показники експрес-моніторингу ринкової безпеки банку**

| Показники | Порядок розрахунків | Ознаки настання загрози ринковій безпеці |
|---|---|---|
| Показник цінової конкурентоспроможності банківської послуги | Відношення ціни банківської послуги банку до середньоринкової ціни цієї банківської послуги | Значення більше за 1 |
| Коефіцієнт ритмічності здійснення кредитних операцій | Відношення фактичної суми кредитного портфеля за певний період, зарахованої у виконання плану, до планової суми кредитного портфеля | Значення менше за 1 |
| Коефіцієнт ритмічності здійснення депозитних операцій | Відношення фактичної суми кредитного портфеля за певний період, зарахованої у виконання плану, до планової суми депозитного портфеля | Значення менше за 1 |
| Відносна ринкова частка банку | Відношення частки банку на ринку до частки найсильнішого конкурента | Значення менше за 1 |
| Показник витрат на рекламу | Відношення витрат на рекламу до чистого прибутку банку | Тенденція до значного зменшення |
| Темпи зростання кількості клієнтів | Відношення кількості клієнтів звітного періоду до кількості клієнтів минулого періоду | Значення менше за 1 |

Таблиця 7.4

## Показники експрес-моніторингу фінансово-економічної безпеки банку

| Показники | Порядок розрахунків | Ознаки настання загрози фінансово-економічній безпеці |
|---|---|---|
| Темпи зростання кредитного портфеля | Відношення суми кредитного портфеля у звітному та попередньому періоді | Значне зменшення або необґрунтоване зростання |
| Коефіцієнт погашення кредитів | Відношення погашених позичок до суми їх залишку на початок року та щойно виданих кредитів у звітному році | Значне зниження показника |
| Прибутковість кредитних операцій | Відношення прибутку від кредитних операцій до середніх активів | Зниження показника |
| Коефіцієнт кредитної активності | Відношення кредитних укладень до загальної суми активів | Недотримання оптимального значення (65 – 70 %) |
| Коефіцієнт інвестиційної активності | Відношення суми інвестицій у цінні папери до загальної суми активів | Недотримання оптимального значення (30 %) |
| Чиста рентабельність активів | Відношення чистого прибутку до середніх активів | Від'ємне значення або значне зниження |
| Доходи на 1 грн активів | Відношення доходів банку до загальної суми активів | Значне зниження, порівняно з попереднім періодом |
| Доходи на одного працівника банку | Відношення суми доходів банку до середньооблікової кількості працівників | Зниження, порівняно з попереднім періодом |
| Коефіцієнт розвитку клієнтської бази | Відношення суми коштів на поточних рахунках клієнтів та коррахунках до суми зобов'язань | Недотримання оптимального значення (15 – 40 %) |
| Коефіцієнт концентрації власного капіталу | Відношення балансового капіталу (брутто-капіталу) до суми пасивів | Недотримання оптимального значення (15 – 20 %) |
| Коефіцієнт надійності | Відношення брутто-капіталу до суми зобов'язань | Недотримання оптимального значення (25 – 30 %) |

Таблиця 7.5

## Показники експрес-моніторингу інформаційної, правової та силової безпеки банку

| Показники | Порядок розрахунків | Ознаки настання загрози безпеці |
|---|---|---|
| Показники експрес-моніторингу інформаційної безпеки банку | | |
| Індекс дохідності інформаційного забезпечення | Відношення додаткових економічних вигід чи економії до суми витрат на придбання програмного забезпечення | Тенденція до зменшення |
| Коефіцієнт інформаційної озброєності | Відношення витрат на придбання програмного забезпечення та засобів захисту інформації до середньооблікової чисельності персоналу | |
| Рівень витратності захисту банківської інформації | Відношення вартості засобів захисту інформаційних ресурсів до вартості програмного забезпечення | |
| Показники експрес-моніторингу правової безпеки банку | | |
| Рівень платіжної дисципліни банку | Відношення суми відсоткових доходів банку за мінусом штрафів і санкцій до суми відсоткових доходів | Значення менше за 1 |
| Коефіцієнт якості юридичного обслуговування | Відношення кількості виграних банком судових позовів до загальної кількості позовів за участю банку | Значення менше за 0,9 |
| Коефіцієнт ефективності юридичного менеджменту | Відношення доходу від відшкодованих банку штрафних санкцій до сплачених банком штрафних санкцій | Значення менше за 1 |
| Показники експрес-моніторингу силової безпеки банку | | |
| Коефіцієнт транспортних утрат | Відношення вартості викрадених цінностей у ході транспортування до суми транспортних витрат банку, помножене на 100 | Тенденція до збільшення |
| Рівень витрат на забезпечення силової безпеки | Відношення суми витрат на охорону банку до суми чистого прибутку банку, помножене на 100 | Тенденція до зменшення |
| Середньомісячна кількість крадіжок та протиправних зазіхань | Відношення загальної кількості крадіжок і протиправних посягань до кількості місяців у звітному періоді | Тенденція до збільшення |

Таблиця 7.6

**Показники експрес-моніторингу кадрової безпеки банку**

| Показники | Порядок розрахунків | Ознаки настання загрози кадровій безпеці |
|---|---|---|
| Коефіцієнт плинності кадрів | Відношення кількості персоналу, звільненого за власним бажанням та порушення трудової дисципліни, до середньооблікової чисельності персоналу | Більше за 0,1 |
| Кількість скарг у розрахунку на одного працівника | Відношення кількості скарг до середньооблікової чисельності персоналу | Більше за 0,05 |
| Коефіцієнт плинності персоналу зі стажем роботи до 1 року | Відношення кількості персоналу зі стажем роботи до 1 року, звільненого за власним бажанням та порушення трудової дисципліни, до середньооблікової чисельності персоналу | Більше за 0,03 |
| Відсоток персоналу, задоволеного перебігом атестації чи оцінювання | Відношення кількості персоналу, задоволеного об'єктивністю результатів атестації до загальної кількості атестованого персоналу, помножене на 100 | Значення менше за 70 % |
| Середній термін перебування працівника на посаді | Відношення суми років роботи працівників на останній посаді в банку до середньооблікової чисельності персоналу | Значення більше за 7 років |
| Рівень задоволеності персоналу роботою в банку | Відношення кількості персоналу, загалом задоволеного роботою в банку, до загальної чисельності персоналу, помножене на 100 | Значення менше за 70 % |

Таким чином, експрес-моніторинг здійснено з метою загального швидкого оцінювання стану безпеки банку. Сутність експрес-моніторингу полягає у швидкому отриманні та постійному відстежуванні невеликої кількості ключових інформативних показників, що комплексно характеризують безпеку банку. Показники експрес-моніторингу, розглянуті в динаміці є індикатором безпеки банківської діяльності.

## Практичне заняття

**Завдання 7.1.** Складання програми інформаційно-аналітичної роботи в банках.

*Методичні рекомендації щодо виконання завдання*

Програма має містити такі обов'язкові елементи, як: етапи інформаційно-аналітичної роботи, її зміст, виконавці та термін проведення. Форму програми наведено в табл. 7.7.

Таблиця 7.7

**Програма інформаційно-аналітичної роботи банку**

| Етапи інформаційно-аналітичної роботи | Зміст інформаційно-аналітичної роботи | Виконавці | Терміни проведення |
|---|---|---|---|
| 1. Створення та постійне оновлення інформаційної бази для аналізу банківської діяльності | | | |
| ….. | | | |
| Узагальнення результатів аналізу | | | |
| Коригування структури аналітичного забезпечення | | | |

**Завдання 7.2.** Розроблення програми внутрішнього інформаційного аудиту в банках.

*Методичні рекомендації щодо виконання завдання*

Форму програми внутрішнього інформаційного аудиту в банках наведено в табл. 7.8.

Таблиця 7.8

Суб'єкт перевірки _____

Період перевірки _____

Термін перевірки _____

**Програма внутрішнього інформаційного аудиту**

| Перелік аудиторських процедур | Виконавці | Терміни перевірки | Примітки |
|---|---|---|---|
| Перевірка наявності та якісного розвитку інформаційної бази | | | |
| …… | | | |
| Складання переліку виявлених помилок та порушень | | | |

Склав _____

Перевірив _____

Ознайомився _____

**Завдання 7.3.** Складання та опрацювання тесту внутрішнього інформаційного аудиту банку.

*Методичні рекомендації щодо виконання завдання*

Тест внутрішнього інформаційного аудиту має містити 10 – 15 запитань, варіанти відповіді та примітки. У примітках зазначають, для яких респондентів призначено запитання, яка мета запитань, відомості, які слід урахувати під час відповіді на конкретно поставлене запитання.

Результати опитування опрацьовують і за кожним запитанням щодо різних варіантів відповіді подають результат у відсотковому виразі. Цей результат характеризує відсоток респондентів, що дають певний варіант відповіді на певне запитання. Форму програми внутрішнього інформаційного аудиту в банках наведено в табл. 7.9.

Таблиця 7.9

**Тест внутрішнього інформаційного аудиту**

Об'єкт перевірки _____

Респонденти _____

| Зміст запитань | Варіанти відповідей | | | Примітки |
|---|---|---|---|---|
| | так | ні | інформація відсутня | |
| 1. Чи є у вашому розпорядженні вся інформація, необхідна для виконання трудових функцій | | | | |
| … | | | | |
| 10. Чи маєте ви доступ до інформації, не використовуваної вами в роботі | | | | |

Виконав _____

Перевірив _____

Ознайомився _____

**Тематика доповідей**

1. Аналітична робота в банківській установі.
2. Сутність, мета та завдання інформаційного аудиту.
3. Сутність, мета та завдання моніторингу економічної безпеки банку.
4. Показники моніторингу економічної безпеки банку.

## Питання для самостійного опрацювання

7.1. Організація аналітичної роботи в банках.

7.2. Відмінності між інформаційним аудитом та моніторингом у банках.

7.3. Посадова інструкція економіста-аналітика банківської установи.

## Практичні завдання для самостійного виконання

**Завдання 7.1.** Банк має намір здійснити дві операції. Якому виду моніторингу вони підлягають?

1. Банківська операція підлягає фінансовому моніторингу. За результатами його проведення встановлено, що юридичною особою здійснено переказ страхового платежу в сумі 2 000 100 грн на поточний рахунок страхової компанії, відкритий в іншій банківській установі. Протягом тижня цією страховою організацією на рахунки громадянина та громадянки Іванових переказано кошти на суму 700 000 грн із указанням призначення платежу – "страхова винагорода за укладені агентські угоди". Цього ж дня за рахунок цих коштів було погашено заборгованість за кредитом в іншому банку.

2. Фізична особа звернулася до банку з метою реалізації золотого зливка вагою 100,0 г. Оскільки операцію здійснено в сумі до 50 000 грн без відкриття рахунка, ідентифікацію клієнта не має здійснювати банк. Працівник банку після виконання операцій із банківськими металами виявив, що цією фізичною особою протягом двох тижнів здійснено ще десять операцій із продажу золотих і срібних зливків вагою 100 – 250 г. У банківського працівника виникли підозри щодо навмисного уникнення клієнтом – фізичною особою процедур фінансового моніторингу. Клієнт надав для підтвердження особи ксерокопію паспорта, що міститься в базі даних про втрачені паспорти.

**Завдання 7.2.** Проаналізувати можливий вплив показників руху персоналу на стан кадрової безпеки банківської установи. Вихідні дані наведено в табл. 7.10.

Таблиця 7.10

### Вихідні дані для аналізу

| Роки / Показники | 2013 | 2014 | 2015 |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Прийнято персоналу | 150 | 163 | 110 |
| Вибуло персоналу | 275 | 358 | 187 |

Закінчення табл. 7.10

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| у тому числі:<br>на навчання | 5 | 6 | 3 |
| у збройні сили | 22 | 18 | 15 |
| на пенсію та з інших причин, передбачених законом | 20 | 30 | 27 |
| за власним бажанням | 215 | 260 | 115 |
| за порушення трудової дисципліни | 13 | 44 | 27 |
| Середньооблікова кількість працівників | 1 700 | 1 758 | 1 140 |

## Методичні рекомендації щодо виконання самостійної роботи

Теоретичні питання опрацьовують на основі літературних джерел [13; 16; 18; 20; 22; 25; 32]. Практичні завдання для самостійного виконання виконують із використанням формул, наведених у підрозділі 7.3.2 цього навчального посібника.

## Контрольні запитання

1. Охарактеризувати зміст інформаційно-аналітичної роботи в банках.
2. Які функції має виконувати економіст-аналітик у банках?
3. Розкрити сутність інформаційного аудиту та моніторингу в банках.
4. Порівняти поняття інформаційного аудиту та моніторингу в банках.
5. Дати визначення поняття "комерційна розвідка".
6. Розкрити сутність поняття "інформаційний ресурс".
7. Охарактеризувати сутність інформаційно-аналітичної роботи.
8. Які існують канали отримання інформації?
9. Назвати завдання інформаційно-аналітичного підрозділу.
10. Перелічити інформаційно-аналітичні документи банківських установ.

## Тести

*Тести одиничного вибору*

1. Обстеження підрозділів банку з метою вивчення й оцінювання наявної в них інформації – це:

а) інформаційний аудит;

б) інформаційний моніторинг;

в) інформаційний контролінг;

г) інформаційно-аналітичне забезпечення;

д) власний варіант відповіді.

2. Контроль за надходженням інформації з метою визначення її важливості й можливості використання в інтегрованих базах даних – це:

а) інформаційний аудит;

б) інформаційний моніторинг;

в) інформаційний контролінг;

г) інформаційно-аналітичне забезпечення;

д) власний варіант відповіді.

3. Надання надзвичайно важливої інформації в будь-якій формі – це:

а) повідомлення;

б) доповідь;

в) довідка;

г) огляд;

д) прогноз.

4. Доповідь – це:

а) комплексне й різнобічне викладення проблеми з використанням усієї наявної інформації;

б) надання надзвичайно важливої інформації в будь-якій формі;

в) опис окремих характеристик конкретних подій або об'єктів;

г) опис основних інформаційних повідомлень за певний період;

д) опис загальної картини подій, що відбуваються.

*Тести множинного вибору*

5. Інформаційно-аналітична робота щодо дослідження конкретного об'єкта містить такі аспекти:

а) вивчення наявного стану об'єкта;

б) вивчення можливостей об'єкта;

в) вивчення (визначення) намірів об'єкта;

г) власний варіант відповіді.

6. Носіями джерел інформації для діяльності комерційної розвідки банківської установи є:

а) персонал банку;

б) звільнені працівники банку;

в) матеріали засобів масової інформації;

г) неофіційні джерела інформації;

д) матеріали періодичних видань;

е) статистичні збірники;

є) усі варіанти правильні.

*Тести на встановлення відповідності*

7.1. Інформаційний аудит полягає в:

7.2. Інформаційний моніторинг полягає в:

а) обстеженні підрозділів банку з метою вивчення й оцінювання наявної в них інформації;

б) контролі за надходженням інформації з метою визначення її важливості, цінності й можливості використання в інтегрованих базах даних.

8.1. Організація інформаційно-аналітичної роботи в банку полягає у:

8.2. Збирання інформації в межах формування інформаційно-аналітичного забезпечення банку полягає в такому:

а) визначенні сфер і об'єктів інформаційної уваги;

б) визначенні мети й завдань інформаційної безпеки;

в) ставленні завдань із інформаційної безпеки;

г) плануванні роботи інформаційно-аналітичного відділу;

д) організації роботи інформаційних каналів;

е) відборі об'єктів інформації;

є) збиранні та опрацюванні інформації.

# 8. Фінансово-економічна безпека банківських установ

**Мета** – розглянути теоретичні засади та практичні аспекти організації управління фінансово-економічною безпекою банківських установ і методичне забезпечення її аналізу.

**Ключові поняття:** безпека банківських операцій, безпека кредитних операцій, безпека валютних операцій, безпека касових операцій, легалізація незаконно отриманих грошей.

**Основні питання:**

8.1. Захист матеріальних цінностей, обладнання та технічних засобів від протиправних зазіхань.

8.2. Забезпечення безпеки банківських операцій.

8.2.1. Забезпечення безпеки кредитних операцій банків.

8.2.2. Забезпечення безпеки роботи банків на фондовому ринку.

8.2.3. Забезпечення безпеки здійснення в банках касових операцій.

8.2.4. Забезпечення безпеки валютних операцій банків.

8.2.5. Боротьба з легалізацією (відмиванням) незаконно отриманих грошей.

**Література:** [13; 16; 18; 20; 26; 27; 32].

## 8.1. Захист матеріальних цінностей, обладнання та технічних засобів від протиправних зазіхань

Наслідком загроз схоронності матеріальних цінностей є збитки, пов'язані зі втратою власності чи витратами на відновлення матеріальних цінностей.

Види загроз безпеці банківських матеріальних цінностей за середовищем виникнення розподіляють на:

1) внутрішні:

неправомірне або непрофесійне використання матеріальних цінностей;

порушення правил обслуговування матеріальних цінностей;

крадіжки;

пошкодження та зумисне знищення матеріальних цінностей;

недобросовісність;

2) зовнішні:

злочинні напади;

тероризм;

стихійні лиха;

крадіжки та псування цінностей персоналом.

Система безпеки матеріальних цінностей банку містять ряд запобіжних заходів:

контроль за обліком матеріальних цінностей;

посилення відповідальності посадових та матеріально відповідальних осіб за правильне зберігання, технічний стан, грамотну експлуатацію, а також за шкоду, завдану банку втратою, пошкодженням чи виведенням із ладу його обладнання, технічних засобів та інших цінностей;

організацію належної охорони матеріальних цінностей, яка б унеможливлювала їх псування, знищення і крадіжки, умови їх ненадійного зберігання;

проведення інвентаризацій матеріальних цінностей та постійний контроль за їх станом та умовами зберігання;

контроль за дотриманням правил зберігання матеріальних цінностей;

забезпечення цілодобового відеоспостереження за матеріальними цінностями й порядком їх використання.

## 8.2. Забезпечення безпеки банківських операцій

### 8.2.1. Забезпечення безпеки кредитних операцій банків

Кредитна безпека банку є головною складовою частиною фінансово-економічної безпеки банку, оскільки вона визначає як рівень прибутків, так і збитків банку.

*Загрози кредитній безпеці банку:*

непрофесійне здійснення кредитного моніторингу;

неповне збирання інформації про позичальника;

непрофесійні дії працівників банку щодо супроводу кредиту;

недосконале вивчення кредитної історії позичальника;

злочинні дії персоналу щодо надання наперед безнадійних кредитів;

недобросовісна поведінка або кримінальний характер діяльності позичальників;

погіршення фінансового стану позичальника;

суттєве погіршення соціально-економічної ситуації у країні;

форс-мажорні обставини.

Ознаками, які можуть указувати на можливість виникнення проблем із повернення кредитів і бути виявлені в ході кредитного моніторингу, є [13]:

істотні зміни у структурі підприємства-позичальника, раптове створення дочірніх підприємств або ж заснування інших підприємств для передання у їх власність частки активів основного позичальника, істотні зміни в кадровому забезпеченні, раптові звільнення провідних фахівців, посадових осіб керівного складу;

наявність конфліктних ситуацій у колективах підприємства-позичальника, його керівному апараті, у відносинах із клієнтами;

припинення дії договорів оренди на невизначений термін;

припинення позичальником співпраці із клієнтами та партнерами, розпродаж майнових цінностей, закриття філій;

від'їзд керівників підприємства-позичальника та членів їх сімей за межі країни, реалізація ними особистого майна;

призупинення робіт із реалізації бізнес-проектів;

наявність доказів щодо порушення законодавства позичальником або його зв'язків із кримінальним світом;

здійснення виплат зі щойно відкритих нових рахунків, цілковита відсутність коштів на рахунках позичальника протягом певного часу, погіршення фінансових показників позичальника (зменшення суми прибутку, обсягів реалізації товарів та послуг, зростання залежності від позичкових коштів, зменшення суми обігових коштів);

затримки позичальника в наданні до банку фінансової звітності, невчасне погашення основних платежів банку, погіршення відносин із банком (відмова від зустрічей, телефонних розмов, уникнення зустрічей із персоналом банку);

запити від інших банків щодо намірів позичальника отримати нові кредити;

наявність сімейних проблем у посадових осіб чи керівництва підприємства-позичальника (розлучення, виконання судових рішень, серйозні хвороби близьких, пов'язані з додатковими витратами).

Процес повернення боргів за безнадійними кредитами здійснюють поетапно різні структурні підрозділи банку (рис. 8.1).


Рис. 8.1. **Процес повернення боргів за безнадійними кредитами**

Слід розглянути **перелік заходів щодо забезпечення безпеки кредитних операцій банку:**

*1. Заходи, що здійснює підрозділ безпеки:*

1.1. Перевірка достовірності, законності документів, наявності всіх реквізитів, відповідності підписів посадових осіб їх повноваженням; наявності фіктивних документів, підписів, виправлень у тексті документа.

1.2. Перевірка кредитної історії позичальника.

1.3. Оцінювання ризику помилок у прийнятті рішень щодо кредитування.

1.4. Перевірка наявності та відповідності вказаним у кредитній справі фактичних об'єктів застави. Визначення вартості, ліквідності,

можливих змін об'єкта застави на момент повернення кредиту. Перевірка застави щодо перебування у заставі інших кредиторів.

1.5. Перевірка достовірності довідок про доходи фізичних осіб.

1.6. Перевірка можливостей поручителів, їх платоспроможності та повноважень осіб, що підписують документи про надання гарантії (поручительства).

1.7. Вивчення можливостей та платоспроможності страховиків, їх повноважень та умов страхування.

*2. Заходи, що здійснює юридичний підрозділ:*

2.1. Перевірка законності існування та діяльності позичальника;

2.2. Перевірка правомірності та правильності складання кредитних договорів.

*3. Заходи, що здійснює кредитний відділ:*

3.1. Оцінювання бізнес-планів позичальника.

3.2. Визначення цільового призначення кредиту.

3.3. Складання графіка погашення кредитів і прогнозів, необхідних для цього коштів позичальнику.

3.4. Оцінювання достатності джерел погашення кредитів.

3.5. Оцінювання кредитоспроможності позичальника.

3.6. Підготовка кредитної справи для прийняття кредитним комітетом рішення про кредитування (із указанням висновків щодо слабких і сильних сторін позичальника, ступеня ризику співпраці та результатів оцінювання кредитоспроможності).

3.7. Здійснення кредитного моніторингу, у ході якого здійснюють контроль за виконанням умов кредитної угоди сторонами.

Метою кредитного моніторингу є виявлення ознак і обставин, які вказують на зміни умов виконання кредитної угоди й реалізації проекту позичальника, своєчасне вжиття заходів щодо повернення позичкових коштів. Досвід роботи банків показує, що до кредитного моніторингу належать такі заходи контролю [13]:

контроль за цільовим використанням кредиту, платоспроможністю позичальника;

контроль за виконанням графіка погашення кредиту і відсотків за нього;

контроль за наявністю і станом предмета застави, поведінкою та станом гарантів (поручителів) і страховиків;

контроль за діяльністю партнерів (контрагентів) позичальника, поведінкою його керівників;

контроль за ситуацією на ринку позичальника, змінами його кон'юнктури, господарської діяльності та ділової активності позичальника, його поведінки на ринку;

контроль за зв'язками позичальника.

**Функції структурних підрозділів банку у сфері кредитного моніторингу** [13]:

*1) кредитні підрозділи* банків контролюють виконання графіка погашення кредиту та сплати відсотків, його цільове використання, фіксують наявність затримок у наданні банку відомостей і звітів, здійснюють аналіз поточної фінансової документації. Крім того, кредитними підрозділами періодично проводять перевірки безпосередньо на підприємстві позичальника, зокрема перевіряють надходження матеріальних цінностей, придбаних за позичкові кошти, реальність виробничої діяльності щодо реалізації бізнес-проекту;

*2) підрозділи безпеки* в ході кредитного моніторингу здійснюють контроль за поведінкою позичальника, його діловою активністю, появою нових комерційних зв'язків, загальним режимом діяльності підприємства (кадровими змінами, конфліктними ситуаціями, змінами в організації виробництва тощо), наявністю негативних відгуків про діяльність підприємства чи його власників або керівництва в засобах масової інформації, поведінкою керівників і засновників (власників) підприємства, їх ставленням до стану і перспектив діяльності підприємства. Підрозділи безпеки також тримають у полі зору соціальну ситуацію на підприємстві, його взаємовідносини із правоохоронними органами й особливо податковою службою;

*3) юридичні підрозділи* здійснюють контроль за правовою ситуацією з питань кредитування та вживають заходів щодо захисту інтересів банку в разі її змін. Крім того, вони забезпечують контроль за дотриманням позичальником обумовлених у договорах умов виконання зобов'язань та, відповідно до рішень керівних органів банку, здійснюють юридичне оформлення змін виконання сторонами своїх зобов'язань або умов їх забезпечення;

*4) підрозділи банківських ризиків* (за відсутності відділ безпеки) насамперед здійснюють вивчення ситуації щодо стану забезпечення повернення кредиту. Зокрема, із питань, що стосуються застави: чи не перезаставлено предмет застави, умови зберігання та стан предмета застави, чи не реалізовано (замінено), украдено предмет застави, дотримання передбачених договорами умов використання (експлуатації,

оновлення) предметів застави. Щодо гарантів (поручителів), страховиків підрозділи банківських ризиків здійснюють контроль за їхнім фінансовим станом та можливостями щодо виконання своїх зобов'язань;

*5) 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.

Найбільш вирішальним етапом безпеки кредитних операцій є оцінювання кредитоспроможності позичальника.

Із 01.01.2013 р. набув чинності Закон України "Про затвердження Положення про порядок формування та використання банками України резервів для відшкодування можливих втрат за активними банківськими операціями" № 23 [27] від 25.01.2012 р., розроблений на підставі міжнародних стандартів. Особливістю цієї методики оцінювання кредитоспроможності підприємства є зведення фінансових показників до єдиного інтегрального показника.

Послідовність оцінювання кредитоспроможності позичальника юридичної особи наведено на рис. 8.2.

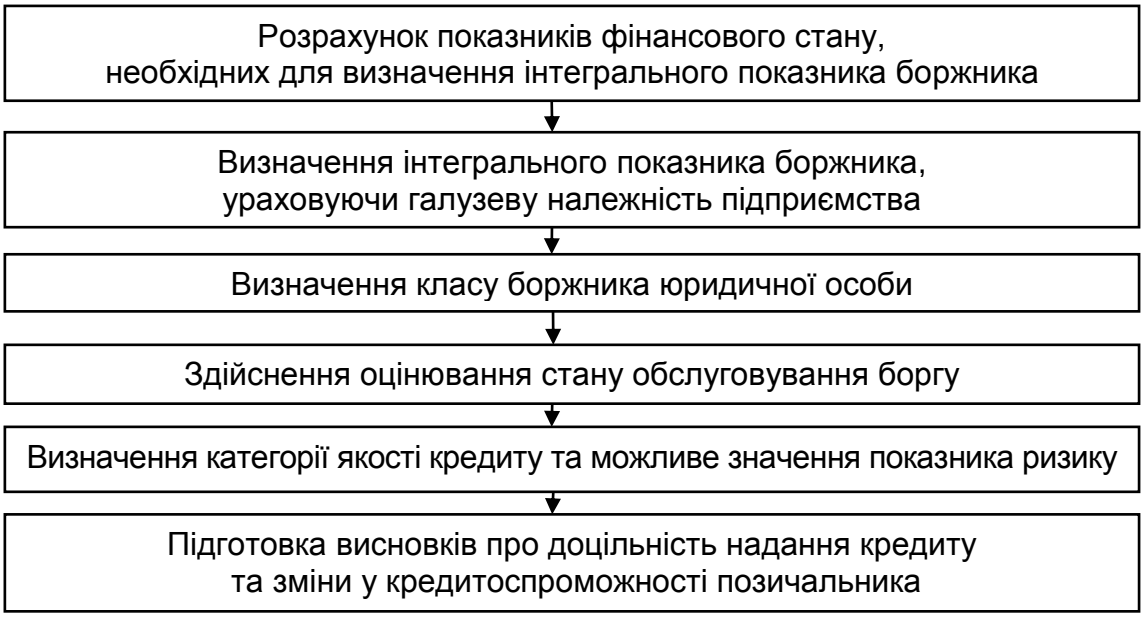


Рис. 8.2. **Послідовність оцінювання кредитоспроможності позичальника юридичної особи**

1. Розрахунок показників фінансового стану, необхідних для визначення інтегрального показника боржника.

Серед цих показників:

коефіцієнт покриття;

проміжний коефіцієнт покриття;

коефіцієнт фінансової незалежності;

коефіцієнт покриття необоротних активів власним капіталом;

коефіцієнт рентабельності власного капіталу;

коефіцієнт рентабельності продажу за фінансовими результатами від операційної діяльності;

коефіцієнт рентабельності продажу за фінансовими результатами від звичайної діяльності;

коефіцієнт рентабельності активів за чистим прибутком;

коефіцієнт оборотності оборотних активів;

коефіцієнт оборотності позичкового капіталу за фінансовими результатами від звичайної діяльності.

Порядок визначення згаданих показників наведено в додатку А.

2. Визначення інтегрального показника боржника, ураховуючи галузеву належність підприємства. Банк визначає клас боржника – юридичної особи, залежно від значення інтегрального показника, ураховуючи величину підприємства (велике, середнє або мале), згідно з даними додатка Б.

3. Визначення класу боржника – юридичної особи. Цю процедуру здійснюють на основі додатка В.

Банк визначає клас боржника – юридичної особи не вищим за 8, якщо:

у договорах немає письмової згоди боржника – юридичної особи – на збирання, зберігання, використання та поширення через бюро кредитних історій інформації про боржника – юридичну особу;

банк не надав після 01.01.2014 р. до бюро кредитних історій відомості про боржника – юридичну особу – за наявності в договорі відповідної згоди;

немає фінансової звітності боржника – юридичної особи – за останній звітний період або фінансова звітність не відповідає вимогам;

проти боржника – юридичної особи – порушено справу про банкрутство;

кредит в іноземній валюті надано боржнику – юридичній особі, у якого немає документально підтверджених очікуваних надходжень валютної виручки в обсязі, достатньому для погашення боргу протягом дії договору.

Надходження валютної виручки вважають достатніми за одночасного дотримання таких умов:

обсяг очікуваних надходжень позичальника на дату розрахунку резерву перевищує обсяг його зобов'язань, ураховуючи терміни їх виконання та ризик перерахунку однієї валюти в іншу;

банк здійснює контроль за станом надходжень валютної виручки позичальника, згідно з укладеними договорами, за якими визначалася достатність надходжень валютної виручки, та має документально підтверджені результати такого контролю;

банк має документально підтверджену інформацію щодо позитивного досвіду (за останні 12 місяців, що передують даті визначення достатності валютної виручки) надходжень валютної виручки на рахунки позичальника в цьому банку та/або в інших банках.

Банк визначає клас боржника – юридичної особи – не вищим за 9, якщо боржника визнано банкрутом у встановленому законодавством України порядку.

Банк визначає клас боржника – юридичної особи, що є нерезидентом, за класом, нижчим із двох, визначених на підставі оцінювання його фінансового стану та ризику країни місцезнаходження.

Банк визначає клас боржника – юридичної особи, що є нерезидентом, згідно з табл. 8.1.

Таблиця 8.1

**Трансформація групи ризику у клас боржника – юридичної особи**

| Номери груп | Класи боржників – юридичних осіб |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |
| 8 | 8, 9 |

4. Здійснення оцінювання стану обслуговування боргу. Банк здійснює оцінювання стану обслуговування боргу боржником – юридичною особою – на підставі кількості календарних днів прострочення погашення боргу станом на перше число місяця, наступного за звітним, згідно з табл. 8.2. Кількість календарних днів прострочення погашення боргу визначено на звітну дату, починаючи з наступного робочого дня за днем, коли не відбулося погашення боргу в термін, передбачений договором. Якщо кількість календарних днів прострочення за основною сумою боргу

та нарахованими доходами відрізняється, то беруть більшу за значенням кількість календарних днів прострочення [27].

Таблиця 8.2

**Визначення стану обслуговування боргу боржником – юридичною особою**

| Кількість календарних днів прострочення (включно) | Стани обслуговування боргу |
|---|---|
| від 0 до 7 | "високий" |
| від 8 до 30 | "добрий" |
| від 31 до 90 | "задовільний" |
| від 91 до 180 | "слабкий" |
| понад 180 | "незадовільний" |

Банк визначає стан обслуговування боргу як "високий" за умови, що сплату боржником – юридичною особою – відсотків, відповідно до умов договору, передбачено не рідше ніж один раз на три місяці.

5. Визначення категорії якості кредиту та можливого значення показника ризику. Банк класифікує кредит, наданий боржнику – юридичній особі – за категоріями якості на підставі визначеного класу боржника – юридичної особи – та стану обслуговування ним боргу, згідно з табл. 8.3 [27].

Таблиця 8.3

**Класифікація кредиту, наданого боржнику – юридичній особі – за категоріями якості**

| Класи боржників – юридичних осіб | Стани обслуговування боргу | | | | |
|---|---|---|---|---|---|
| | "високий" | "добрий" | "задовільний" | "слабкий" | "незадовільний" |
| 1 | I | I | III | IV | V |
| 2 | I | I | III | IV | V |
| 3 | I | II | III | IV | V |
| 4 | I | II | III | IV | V |
| 5 | II | II | III | IV | V |
| 6 | II | III | IV | IV | V |
| 7 | II | III | IV | IV | V |
| 8 | II | III | IV | IV | V |
| 9 | II | III | IV | V | V |

Банк визначає показник ризику кредиту, наданого боржнику – юридичній особі, залежно від категорії якості в межах діапазонів, зазначених у табл. 8.4 [27].

Банк визначає показник ризику за кредитом, наданим боржнику – юридичній особі – у межах установленого діапазону, ураховуючи динаміку фактичних значень інтегрального показника, коефіцієнта покриття боргу, якості менеджменту боржника – юридичної особи, ринків збуту продукції, наявності бізнес-планів, визначених рейтингів боржника – юридичної особи – (за наявності) та інших подій та обставин, що можуть вплинути на своєчасність і повноту погашення боргу [27].

Таблиця 8.4

**Визначення показника ризику кредиту, наданого боржнику – юридичній особі**

| Категорії якості за кредитом | Значення показників ризику кредиту |
|---|---|
| I – найвища | 0,01 – 0,06 |
| II | 0,07 – 0,20 |
| III | 0,21 – 0,50 |
| IV | 0,51 – 0,99 |
| V – найнижча | 1,00 |

Підготовка висновків про доцільність надання такого кредиту та зміни у кредитоспроможності позичальника.

Оцінювання кредитоспроможності позичальника фізичної особи здійснюють у послідовності, наведеній на рис. 8.3.


Рис. 8.3. **Методика оцінювання кредитоспроможності боржника – фізичної особи**

1. Оцінювання кількісних та якісних показників фінансового стану боржника – фізичної особи.

**Кількісні показники,** згідно з постановою № 23 [27], містять:

сукупний чистий дохід (щомісячні сукупні доходи, зменшені на сукупні витрати та зобов'язання, крім зобов'язань перед банком, що здійснює оцінювання фінансового стану боржника – фізичної особи – із метою формування резерву;

накопичення на рахунках у банку (інформацію надають на бажання боржника – фізичної особи);

коефіцієнти, що характеризують поточну платоспроможність боржника – фізичної особи – та його фінансові можливості виконати зобов'язання за кредитом (зокрема співвідношення сукупних доходів і витрат/зобов'язань боржника – фізичної особи; співвідношення обсягу боргу за кредитом до вартості об'єкта кредитування/застави; співвідношення щомісячних витрат боржника на обслуговування боргу до обсягу його щомісячних доходів тощо). Оптимальні значення цих коефіцієнтів банк установлює самостійно, ураховуючи види кредитів, залежно від форми їх надання, цільового призначення, терміну користування, наявності забезпечення, способу сплати тощо.

Банк для розрахунку кількісних показників ураховує доходи, факт отримання яких протягом дії договору підтверджено достовірними документами, виданими третьою особою (довідка з місця роботи, довідка про доходи, виписка (довідка) банку з рахунка про рух коштів) або банком-кредитором, який є працедавцем боржника – фізичної особи – або здійснює обслуговування його рахунка.

До **якісних показників** належать такі [27]:

загальний матеріальний стан клієнта (наявність у власності майна, крім майна, переданого в заставу);

соціальна стабільність клієнта (тобто наявність постійної роботи, ділова репутація, сімейний стан тощо);

вік клієнта.

Банк оцінює якісні показники на підставі достовірних документів, у тому числі відповідних копій документів, засвідчених в установленому законодавством порядку.

Оцінювання фінансового стану боржника – фізичної особи, який є суб'єктом господарювання, має здійснювати банк, також ураховуючи аналіз фінансової звітності, що подається ним як суб'єктом господарювання за встановленими законодавством України формами. Аналіз фінансової звітності боржника – фізичної особи, який є суб'єктом господарювання,

має враховувати дослідження динаміки показників його діяльності. Питома вага кількісних показників у загальній оцінці фінансового стану боржника – фізичної особи – має становити не менш ніж 70 %.

Банк визначає періодичність здійснення оцінювання поточного фінансового стану боржника – фізичної особи – самостійно, ураховуючи стан обслуговування боргу, але не рідше ніж один раз на рік (або за результатами фінансового року).

2. Визначення класу боржника – фізичної особи, що здійснюють на підставі результатів оцінювання його фінансового стану, відповідно до наведених характеристик (табл. 8.5).

Таблиця 8.5

**Характеристика класів боржника – фізичної особи**

| Класи боржників | Визначення |
|---|---|
| 1 | 2 |
| Клас А – фінансовий стан "добрий" | Сукупний чистий дохід боржника – фізичної особи перевищує внески на погашення боргу за всіма активами банку щодо цього боржника за відповідний період; наявність у власності майна, крім майна, переданого в заставу; коефіцієнти, що характеризують поточну платоспроможність боржника – фізичної особи – та його фінансові можливості виконати зобов'язання за кредитом, перевищують їх оптимальні значення |
| Клас Б – фінансовий стан "задовільний" | Сукупний чистий дохід боржника – фізичної особи є не меншим, ніж сума внесків на погашення боргу за всіма активами банку щодо цього боржника за відповідний період, простежують негативну тенденцію (зміну місця роботи з погіршенням умов, зростання обсягу зобов'язань боржника – фізичної особи, що свідчить про підвищення ймовірності несвоєчасного та/або в неповній сумі погашення боргу); коефіцієнти, що характеризують поточну платоспроможність боржника – фізичної особи – та його фінансові можливості виконати зобов'язання за кредитом, не нижчі, ніж їх оптимальні значення |
| Клас В – фінансовий стан "незадовільний" | Сукупний чистий дохід боржника – фізичної особи – є нижчим, ніж сума внесків на погашення боргу за всіма активами банку щодо цього боржника за відповідний період, наявні негативні зміни щодо загального матеріального стану клієнта та/або його соціальної стабільності; зростання обсягу зобов'язань боржника – фізичної особи – свідчить про високу ймовірність несвоєчасного та/або в неповній сумі погашення боргу; коефіцієнти, що характеризують поточну платоспроможність боржника – фізичної особи – та його фінансові можливості виконати зобов'язання за кредитом, є несуттєво нижчими, ніж їх оптимальні значення |

Закінчення табл. 8.5

| 1 | 2 |
|---|---|
| Клас Г – фінансовий стан "критичний" | Сукупний чистий дохід боржника – фізичної особи – є недостатнім для своєчасних та в повному обсязі внесків на погашення боргу за всіма активами банку щодо цього боржника за відповідний період; коефіцієнти, що характеризують поточну платоспроможність боржника – фізичної особи – та його фінансові можливості виконати зобов'язання за кредитом, нижчі, ніж їх оптимальні значення |

Банк у разі наявності в боржника – фізичної особи – характеристик, які відповідають різним класам, має зарахувати такого боржника до нижчого класу.

Банк зараховує боржника – фізичну особу – до класу Г у разі [27]:

відсутності в договорах письмової згоди боржника – фізичної особи – на збирання, зберігання, використання та поширення через бюро кредитних історій інформації про боржника – фізичну особу;

ненадання банком після 01.01.2014 р. до бюро кредитних історій інформації про боржника – фізичну особу – за наявності в договорі відповідної згоди;

відсутності документів, що підтверджують отримання боржником – фізичною особою – постійних доходів;

порушення проти боржника – фізичної особи, яка є суб'єктом господарювання, справи про банкрутство або визнання банкрутом у встановленому законодавством України порядку;

відсутності в боржника – фізичної особи, якому надано кредит в іноземній валюті, документально підтверджених очікуваних надходжень виручки/доходів в іноземній валюті в обсязі, достатньому для погашення боргу протягом дії договору.

Банк визначає клас боржника – фізичної особи, що є нерезидентом, за класом, нижчим із двох, визначених на підставі оцінювання його фінансового стану та ризику країни місцезнаходження. Банк визначає клас боржника – фізичної особи, що є нерезидентом, згідно з табл. 8.6 [27].

Таблиця 8.6

**Трансформація групи ризику у клас боржника – фізичної особи**

| Номери груп | Класи боржників – фізичних осіб |
|---|---|
| 1 | 2 |
| 1 | А |
| 2 | |

Закінчення табл. 8.6

| 1 | 2 |
|---|---|
| 3 | Б |
| 4 | |
| 5 | |
| 6 | В |
| 7 | |
| 8 | Г |

3. Оцінювання стану обслуговування боргу боржником – фізичною особою, що здійснюють на підставі кількості календарних днів прострочення погашення боргу станом на перше число місяця, наступного за звітним, згідно з табл. 8.7.

Таблиця 8.7

**Визначення стану обслуговування боргу боржником – фізичною особою**

| Кількість календарних днів прострочення (включно) | Стани обслуговування боргу |
|---|---|
| від 0 до 7 | "високий" |
| від 8 до 30 | "добрий" |
| від 31 до 90 | "задовільний" |
| від 91 до 180 | "слабкий" |
| понад 180 | "незадовільний" |

Банк визначає стан обслуговування боргу як "високий" за умови, що сплату відсотків боржником – фізичною особою, відповідно до умов договору, передбачено не рідше ніж один раз на три місяці.

Банк визначає стан обслуговування боргу не вищим, ніж "слабкий", якщо його сплату боржником – фізичною особою, відповідно до умов договору, передбачено в кінці терміну дії договору, термін дії якого становить один рік або більше. Цю вимогу не поширено на кредити, забезпечені майновими правами на грошові кошти заставодавця, що розміщено на вкладному (депозитному) рахунку в банку-кредиторі на термін, не менший, ніж термін користування кредитом, за умови

повного покриття боргу депозитом, ураховуючи ризик перерахунку однієї валюти в іншу, та забезпечення безперечного контролю за коштами й доступу банку-кредитора до них у разі невиконання боржником зобов'язань за кредитною операцією, що обумовлено договором [27].

4. Класифікація кредиту, наданого боржнику – фізичній особі, за категоріями якості. Банк класифікує кредит, наданий боржнику – фізичній особі, за категоріями якості на підставі визначеного класу боржника – фізичної особи – та стану обслуговування ним боргу, згідно з табл. 8.8.

Таблиця 8.8

**Класифікація кредиту, наданого боржнику – фізичній особі, за категоріями якості**

| Фінансові стани боржника – фізичної особи (клас) | Стани обслуговування боргу | | | | |
|---|---|---|---|---|---|
| | "високий" | "добрий" | "задовільний" | "слабкий" | "незадовільний" |
| А | I | II | III | IV | V |
| Б | I | II | III | IV | V |
| В | II | III | IV | IV | V |
| Г | II | III | IV | V | V |

5. Визначення показника ризику кредиту, наданого боржнику – фізичній особі, що здійснюють, залежно від категорії якості, у межах діапазонів, зазначених у табл. 8.9.

Таблиця 8.9

**Визначення показника ризику кредиту, наданого боржнику – фізичній особі**

| Категорії якості кредиту | Значення показників ризику кредиту |
|---|---|
| I – найвища | 0,01 – 0,06 |
| II | 0,07 – 0,20 |
| III | 0,21 – 0,50 |
| IV | 0,51 – 0,99 |
| V – найнижча | 1,00 |

Рішення про надання кредиту приймає кредитний комітет, який є оперативним і постійно діючим органом банку.

**Кредитний комітет** – колегіальний орган банку, який уповноважений визначати кредитну політику, приймати рішення щодо можливості та умов здійснення кредитних операцій на основі оцінювання кредитних ризиків, а також забезпечувати розвиток кредитних зв'язків із позичальниками.

У банку створюють кредитний комітет (у головному банку) або кредитну комісію (у філіях банку). **Кредитна комісія** – колегіальний орган філії банку, який уповноважений приймати рішення щодо можливості та умов здійснення кредитних операцій у межах наданих йому повноважень. Кредитний комітет (комісію) банку формують у складі не менш ніж 5 членів та секретаря кредитного комітету. Склад кредитного комітету призначають і затверджують за рішенням правління банку.

Основні функції кредитного комітету банку перелічено в табл. 8.10.

Таблиця 8.10

**Функції кредитного комітету банку**

| Групи функцій | Перелік функцій |
|---|---|
| 1 | 2 |
| Функції кредитного комітету щодо контролю за роботою кредитних комісій | установлення кредитним комісіям підпорядкованих філій ліміту надання кредитів одному позичальникові |
| | розгляд клопотання філій на здійснення активних операцій у національній та іноземній валюті понад повноваження, які їм надано |
| | розгляд та затвердження лімітів кредитування: загальних за філіями, індивідуальних за позичальниками та лімітів із окремих видів кредиту |
| | постійний розгляд і аналіз (не рідше ніж один раз на місяць) стану кредитного портфеля філії, правильність зарахування позичальників до відповідної групи ризику та розрахунку резерву під кредитні ризики |
| | прийняття самостійного рішення про надання кредитів понад установлені підпорядкованим філіям ліміти |
| | заслуховування керівників відповідних підрозділів банку та підпорядкованих філій із питань структури кредитного портфеля та розгляд ефективності вжитих заходів щодо її поліпшення |
| Функції кредитного комітету в межах власних повноважень | прийняття самостійного рішення про здійснення кредитних операцій |
| | прийняття рішення щодо можливості зміни умов кредитування |
| | визначення кредитної політики банку |
| | розгляд та аналіз стану кредитного портфеля банку (не рідше ніж один раз на місяць) |
| | розгляд результатів роботи із кредитною заборгованістю |

Закінчення табл. 8.10

| 1 | 2 |
|---|---|
| | розгляд і визнання боргів безнадійними та пошук джерел їх покриття |
| | визначення стратегічних напрямів інвестування та кредитування, а також основних видів прийнятного забезпечення |
| | контроль за якістю та достатністю сформованих резервів |
| | розроблення нових кредитних продуктів |
| | затвердження переліків елітних і системних клієнтів, інсайдерів |
| Функції кредитної комісії | самостійне прийняття рішень про здійснення кредитних операцій філії |
| | вирішення питання щодо можливості зміни умов здійснення кредитних операцій, пролонгації кредиту на встановлений головним банком термін |
| | визначення пріоритетних для філії напрямів кредитування |
| | розгляд та аналіз стану кредитного портфеля філії |

*Особливості роботи кредитного комітету:*

1) усі члени кредитного комітету беруть на себе відповідальність за прийняття рішень щодо надання кредиту;

2) секретар кредитного комітету є відповідальним за підготовку засідань кредитного комітету; оформлення, зберігання протоколів засідань та матеріалів до них; своєчасне доведення рішень та пропозицій до відома відповідних структурних підрозділів банку та філій; конфіденційність інформації, що стала йому відома в ході виконання обов'язків секретаря;

3) засідання кредитного комітету проводять у міру необхідності (щотижня, два рази на тиждень), але не рідше ніж один раз на місяць. Позитивне вирішення питання в робочому порядку може бути здійснено за одностайної підтримки його всіма членами кредитного комітету;

4) засідання кредитного комітету зазвичай уважають таким, що відбулося, якщо на ньому присутні не менш ніж 2/3 його кількісного складу;

5) секретар кредитного комітету не пізніше як за день до проведення засідання отримує питання до порядку денного від підрозділів, які ініціюють кредитну операцію. Секретар кредитного комітету надає його членам матеріали кредитних справ;

6) якщо відсутні голова кредитного комітету та його заступник, засідання не проводять;

7) рішення кредитного комітету вважають прийнятим, якщо за нього проголосувало більшість присутніх на засіданні членів кредитного комітету. Якщо голоси розподілилися порівну, приймають рішення, за яке проголосував головуючий на засіданні кредитного комітету. Внутрішнім

положенням банку про кредитний комітет може бути встановлено іншу необхідну кількість присутніх;

8) за тимчасової відсутності секретаря його обов'язки може виконувати інший співробітник за розпорядженням голови кредитного комітету;

9) доповідачем із чергового питання порядку денного засідання кредитного комітету є керівник підрозділу, що ініціював розгляд питання;

10) у разі необхідності на засідання можна запрошувати фахівця, що працює з первинними документами та готує картку кредитної справи позичальника;

11) протокол засідання кредитного комітету підписують голова та секретар, результат голосування з кожного питання підписує кожен член кредитного комітету, що брав участь у голосуванні. **Протокол кредитного комітету** – документ, що містить перелік питань, які подають на розгляд кредитного комітету; результати голосування з кожного питання, формулювання підсумкових рішень;

12) рішення, зазначене у протоколі, доводять до відома відповідних структурних підрозділів та філій банку у формі витягу із протоколу не пізніше наступного робочого дня після підписання, воно є обов'язковим для виконання відповідними підрозділами банку;

13) протоколи засідань кредитного комітету, матеріали та висновки підрозділів зберігають у секретаря, а витяги із протоколів доводять до відома кредитних підрозділів банку та філій і зберігають у кредитних справах.

### 8.2.2. Забезпечення безпеки роботи банків на фондовому ринку

Операції банку на фондовому ринку посідають друге місце за ступенем ризику.

*Головні загрози безпеці банку в ході роботи на фондовому ринку*:

купівля цінних паперів недійсних або фіктивних фірм;

придбання наперед неліквідних цінних паперів;

зміна в бік погіршення ринкової ситуації на фондовому ринку;

необізнаність банку щодо стану фондового ринку;

злочинні дії банківського персоналу та суб'єктів фондового ринку.

На протидію загрозам безпеці банківських операцій на фондовому ринку мають застосовуватися такі *заходи системного характеру:*

якісну перевірку достовірності угод та відповідності стану емітентів заявленим умовам;

перевірку прав власності на цінні папери власника;

контроль за дотриманням законності операцій із цінними паперами;

контроль за правильністю і своєчасністю переходу права власності на цінні папери;

налагодження тісної співпраці банку із суб'єктами національної депозитарної системи, насамперед із реєстраторами та зберігачами акцій;

отримання банком дозволу на депозитарну діяльність, тобто зберігання власних цінних паперів;

детальне вивчення фінансового стану, перспектив розвитку, конкурентоспроможності, термінів діяльності, основних власників акцій підприємств-емітентів цінних паперів, що співпрацюють із банком;

здійснення фінансової експертизи векселів;

створення інформаційних баз даних щодо основних емітентів.

Превентивні заходи безпеки банку щодо операцій із цінними паперами (ЦП) наведено в табл. 8.11.

Таблиця 8.11

**Превентивні заходи щодо забезпечення безпеки банківських операцій із цінними паперами**

(на основі опрацювання джерела [13])

| Види ЦП | Перелік превентивних заходів безпеки |
|---|---|
| 1 | 2 |
| Акції | розмежування функцій працівників банку щодо обліку акцій і торгівлі ними |
| | проведення емісії акцій за вартістю, не нижчою за номінальну |
| | здійснення конвертації інших цінних паперів в акції тільки тоді, коли це обумовлено у проспекті емісії |
| | прийняття до обліку тільки оригіналів акцій та сертифікатів, а не ксероксів |
| | продаж акцій може починатись не раніше ніж через 30 днів після публікації про їх випуск |
| | здійснення придбання акцій на основі договору купівлі-продажу |
| | забезпечення відповідної кількості ступенів захисту акцій та всіх необхідних реквізитів |
| | сплата вартості акцій у національній валюті |
| | здійснення періодичних запитів до реєстратора (депозитарія) щодо стану реєстру (облікового реєстру) акцій емітента |
| | передбачення в разі застави акцій та непогашення кредиту позичальником передання банку права власності на певну кількість акцій |

Закінчення табл. 8.11

| 1 | 2 |
|---|---|
| | прийняття як застави від фізичних осіб, переважно, іменних акцій |
| | прийняття в заставу від юридичних осіб тільки тих акцій, які перебувають на балансі підприємства |
| | обов'язкове здійснення моніторингу стану вторинного ринку обігу акцій, взаємодія з операторами вторинного ринку |
| | забезпечення однакової номінальної вартості акцій, що перебувають в обігу |
| Векселі | обов'язкова перевірка платоспроможності векселедавців (термін роботи з векселями, репутація, фінансовий стан, перспективи розвитку); |
| | здійснення інкасування векселів тільки в установах банків |
| | прийняття до обліку тільки векселів із їх реєстрами |
| | заборона приймати опротестовані векселі |
| | наявність перекладу тексту, завіреного нотаріально, якщо вексель оформлено іноземною мовою |
| | прийняття до обліку, під заставу і рефінансування векселів, виданих тільки юридичними особами на підставі здійснення реальних товарних і комерційних угод |
| | забезпечення перевірки безперервного ряду індосаментів. Найбільш надійними вважають векселі, які мають багато передавальних написів, частковий індосамент є недійсним; індосамент має бути простим і нічим не обумовленим, будь-які обмежуючі його умови вважають ненаписаними |
| | здійснення протесту в неплатежі за векселем, який підлягає оплаті на певну дату або у визначений термін від дати складання чи подання, має бути того дня, коли вексель підлягає оплаті, або одного із двох наступних робочих днів |
| | здійснення вексельного забезпечення кредиту з розрахунку 200 % номінальної вартості векселів від суми кредиту |
| | надання переваги короткостроковим векселям, які менше залежать від змін економічної ситуації |
| | наявність за вексельних кредитів у векселях іменного індосаменту на користь банку |
| | контроль за поданням векселедавцем під час передавання векселя довідки про сплату державного мита |
| | здійснення платежу за векселем на території України тільки в безготівковій формі |

Служба безпеки банку має вимагати від подавця належних доказів, які підтверджують дієздатність і справжність підписів векселедавців (трасантів) і акцептантів, а також підстави для отримання векселя подавцем,

попередньо здійснивши фінансову експертизу векселя. У ході експертизи служба безпеки встановлює можливість сплати векселя вчасно, аналізує фінансовий стан подавця векселя. Для виконання цих функцій банк може залучати аудиторські, консалтингові, рейтингові агенції.

### 8.2.3. Забезпечення безпеки здійснення в банках касових операцій

Безпека касових операцій банку може бути під впливом таких *загроз зовнішнього та внутрішнього походження,* як:

незаконні дії персоналу з метою зумисних крадіжок цінностей та грошових коштів;

крадіжки, напади та інші незаконні дії, що походять із зовнішнього середовища;

недобросовість працівників банку;

непрофесійність касирів;

неналежна охорона приміщень, сховищ, де зберігають готівку та інші цінності;

неналежне обладнання приміщень банку засобами відеоспостереження, захисту, сповіщення.

*Складові частини безпеки касових операцій банків:*

1) належне обладнання приміщень банків та робочих місць, де здійснюють касові операції. **Сховище цінностей** – спеціально обладнане приміщення банку (філії, відділення), сейф, депозитна система та АТМ-сейфи, що використовують для зберігання готівки та інших цінностей, технічний стан яких відповідає нормативно-правовим актам. Приміщення має бути обладнано й технічними засобами для роботи з готівкою. До них належать: машини, пристрої; прилади для оброблення банкнот (монет), за допомогою яких виконують кілька або окремі операції з перераховування банкнот (монет), контролю за захисними ознаками банкнот (монет), обандеролюванням корінців банкнот, упаковуванням банкнот (монет) [26].

**Автоматична касова машина** (АТМ) – машина, що обслуговує клієнтів в автоматичному або частково автоматичному режимі. До АТМ належать термінали та банкомати, депозитні системи, пристрої з видачі/приймання готівки та інших цінностей [26].

На робочих місцях касирів має знаходитися таке обладнання: сейфи, прилад для визначення справжності грошей, лічильна машина,

комп'ютер, засоби тривожної сигналізації, телефонного чи радіозв'язку. Територіально відокремлені робочі місця касирів слід розташовувати всередині будинків організацій, установ, магазинів, а їх конструктивна будова має виключати можливість несанкціонованого проникнення в них. Огороджувальні конструкції кабін мають бути непрозорими. Працівники каси в разі спроби нападу або крадіжки цінностей із боку клієнтів або інших осіб мають подати за встановленим порядком сигнал "Тривога";

2) належна поведінка персоналу під час здійснення касового обслуговування. Поведінку персоналу та виконання функцій регламентовано Інструкцією про ведення касових операцій банками в Україні [26].

Касири мають забезпечувати, згідно з Інструкцією про ведення касових операцій банками в Україні [26]:

правильність розрахунків із клієнтами;

належне документальне оформлення касових операцій;

роботу з виявлення фальшивих та зношених банкнот;

роботи із приймання, видачі, зберігання готівки та інших цінностей в операційній касі, у тому числі із застосуванням АТМ;

виконання роботи з перерахування готівки;

зведення залишків готівки в операційній касі;

роботи із застосуванням електронних платіжних засобів через операційну касу;

виконання роботи із платіжними пристроями.

У межах розрахунково-касової роботи відділ безпеки має здійснювати:

контроль за касовими операціями;

контроль за організацією роботи відповідальних осіб сховища цінностей (їх кількість та посади);

перевірку порядку відкривання і закривання сховищ цінностей;

контроль за здаванням під охорону та прийняттям із-під охорони сховищ цінностей і депозитних систем, а також зберігання ключів (дублікатів ключів) до них та здійснення ревізії цінностей.

Щодо кадрового забезпечення, то служба безпеки має приділяти особливу увагу підбору відповідного персоналу, зокрема на перебіг роботи на попередніх місцях, надійність майбутніх працівників, відсутність у них небажаних звичок та пристрастей, випадків зловживання службовим становищем та порушень законів. Головний бухгалтер має зібрати

і зберігати зразки підписів усіх касирів та договори про матеріальну відповідальність.

У межах запобігання загрозам утрати готівки працівники мають виконувати такі *правила безпечного здійснення касових операцій* [13]:

не приймати претензії щодо неправильної видачі грошей чи решти, якщо клієнт відійшов від банківської каси;

не обмінювати банкноти одного номіналу на інший;

перевірити на відповідність підписи посадових осіб, які мають право дозволу на видачу грошей, установленим зразкам;

перевірити наявність підпису клієнта на документі про отримання грошей;

порівняти суму, проставлену цифрами, із сумою, зазначеною на документі літерами;

викликати отримувача грошей за номером видаткового документа і запитати про суму грошей, яку він отримує;

перевірити наявність даних про подання паспорта або іншого документа, який засвідчує особу, котра отримує гроші, за винятком здійснення валютно-обмінних операцій та реалізації ювілейних, пам'ятних, інвестиційних монет та іншої нумізматичної продукції;

підготувати суму грошей, зіставити цю суму із сумою, указаною в чеку, відбити на лічильній машині, видати їх отримувачу й підписати видатковий касовий ордер;

приймати та видавати гроші, якщо клієнт здійснює операції за кількома видатковими або прибутковими документами з різних рахунків, за кожним документом окремо;

перевірити наявність та відповідність підписів операційних працівників із наявними в нього зразками;

звірити відповідність указаних у документах сум цифрами й літерами;

прийняти від клієнтів гроші з обов'язковим перерахунком банкнот;

звірити номер контрольної марки або талона в касі з номером на видатковому документі й наклеїти контрольну марку або талон, відповідно, до чека або ордера;

усі прийняті раніше гроші мають зберігати в шухлядах стола або металевих шафах, сейфах, які мають замикати.

обладнання робочого місця має бути таким, щоб клієнт міг безперешкодно спостерігати за прийманням грошей;

на столі касира не можна тримати ніяких інших грошей, крім тих, що приймають від особи, із якою працює касир;

не можна виконувати операцію, а документ і готівку слід повернути платнику, якщо бодай один із реквізитів, передбачених формою прибуткового документа, не заповнено чи заповнено з помилками, порушенням вимог, або якщо сума коштів, що є в розпорядженні клієнта, менша, ніж сума платежу;

не допускати часткових виплат (приймання) сум коштів, указаних у прибуткових чи видаткових документах;

обов'язково вилучати фальшиві та зношені монети, банкноти;

заборонено передавати іншим касирам та інкасаторам виконання дорученої роботи з матеріальними цінностями, а також виконувати роботу, яка не входить до кола їхніх обов'язків;

заборонено здійснювати касові операції, оминаючи бухгалтерію;

касиру заборонено зберігати власні гроші із грошима й цінностями банку;

у разі тимчасової відсутності на робочому місці касири не повинні у відкритому вигляді зберігати печатки, цінності, гроші, ключі від сховищ, сейфів, теки із грошима;

касири зобов'язані стежити за відповідністю грошей зразкам, виявляти фальшиві банкноти;

не дозволено зберігати в касі їжу, верхній одяг, інші предмети, що не стосуються роботи касира.

*Правила безпеки під час роботи з непридатними до обігу монетами й банкнотами:*

касири зобов'язані приймати до обміну зношені та значно зношені монети й банкноти, якщо відсутні дані щодо номіналу банкноти та ознаки фальшування;

заборонено видавати клієнтам непридатні до обігу банкноти й монети;

фальшиві або перероблені банкноти в 10-денний термін передають на експертизу до НБУ;

на виявлені працівниками кас неплатіжні, фальшиві та перероблені грошові білети й монети обов'язково складають акт із зазначенням серії, номера та номіналу кожного білета, сум монет;

фальшиві та перероблені монети й банкноти банки вилучають і передають до НБУ для висновку, а НБУ, залежно від результатів експертизи, передає фальшиві гроші органам внутрішніх справ.

Класифікацію та характеристику банкнот і монет за ступенем придатності до обігу наведено в табл. 8.12.

Таблиця 8.12

**Характеристика банкнот і монет за ступенем придатності до обігу**

| Види банкнот | Характеристики |
|---|---|
| 1 | 2 |
| 1. Придатні до обігу | Монети й банкноти, що не мають пошкоджень, зношеності чи дефектів, а також не є фальшивими |
| 2. Непридатні до обігу | Монети й банкноти з дефектами виробника або ті, що є фальшивими, набули ознак зношення і пошкодження та зберегли всі ознаки платіжності або втратили чи змінили окремі з них |
| 2.1. Зношені | Банкноти й монети, що мають незначні ознаки зношення та пошкодження, а саме [13]:<br>банкноти без пошкоджень, але потерті із загальним та локальним забрудненням, що псують естетичний вигляд банкноти;<br>банкноти, у будь-якому місці яких є плями, написи (включаючи видимі в ультрафіолетових або інфрачервоних променях), відбитки штампів (крім штампів про погашення);<br>надірвані та надрізані банкноти, незалежно від розміру надриву, надрізу, зі склеєними надривами й надрізами;<br>банкноти із проколами й дірками, відірваними краями та кутами;<br>монети з подряпинами та зміненим початковим кольором, якщо вони зберегли зображення малого Герба України та номіналу, а також рельєфний гурт, якщо він є на затвердженому зразку |
| 2.2. Значно зношені | Банкноти й монети, що мають суттєві ознаки зношення чи (і) пошкоджень [13]:<br>банкноти з утраченими частинами, якщо збереглось не менш ніж 55 % початкової площі банкноти;<br>банкноти, розірвані й розрізані на дві або більше частин, крім розрізаних на вузькі смуги, та склеєні (склеєна ділянка не має заважати визначенню справжності та склеюватись із іншими банкнотами), у тому числі з утраченими частинами, якщо не менш ніж 55 % загальної площі частин, що залишились, безумовно, належать одній банкноті;<br>банкноти, розірвані на вузькі смуги та склеєні, якщо всі смуги збереглися;<br>банкноти, пошкоджені вогнем, водою, різними рідинами та хімікатами; |

Закінчення табл. 8.12

| 1 | 2 |
|---|---|
| | банкноти, склеєні із двох половинок різних банкнот одного номіналу й дизайну, якщо ці половинки (частини) у місці склеювання за дизайном доповнюють одна одну, а їх сумарна площа не менш ніж 75 % початкової площі банкноти;<br>монети деформовано, але без дірок і надломів, якщо на цих монетах збереглися зображення малого Герба України та номіналу |
| 2.3. Із дефектами виробника | Банкноти й монети, що не відповідають затвердженому зразку, проте не є фальшивими |
| 2.4. Фальшиві банкноти й монети | Банкноти й монети, виготовлені будь-яким способом, включаючи промисловий, усупереч установленому законодавством порядку, які імітують (фальсифікують) платіжні банкноти й монети, виготовлені на замовлення НБУ і введені ним в обіг |
| 2.5. Перероблені банкноти | Банкноти й монети, на яких змінено шляхом наклеювання, малювання, друкування тексту і (або) цифр зображення, що визначають номінал, рік зразка (емісії), банк-емітент, інші реквізити, та які за зовнішнім виглядом може бути сприйнято як справжні вищого номіналу або іншого року зразка |

*Правила безпечної роботи касирів із інкасаторами* (на основі опрацювання джерела [13]):

перевірка сумок із готівкою щодо зовнішніх пошкоджень, дефектів (зовнішніх швів, латок, дірок у тканині, пошкоджених пломб, розривів шпагату або вузлів на ньому);

перевірка відбитків пломбірів на чіткість і відповідність завіреним зразкам;

перевірка відповідності номерів сумок номерам, указаним у накладних;

перевірка відповідності кількості мішків із монетами, а також загальної суми, що приймають, записам у накладних;

установлення відповідності кількості сумок, зданих інкасаторами до каси, даним довідки про видачу сумок та даним явочних карток;

перерахування грошей у разі виявлення дефектних сумок, розбіжностей у записах про суму грошей. Про це та результати перевірки складають відповідний акт посадові особи, відповідальні за схоронність грошей та цінностей, якими є керівник (заступник керівника), головний бухгалтер (заступник головного бухгалтера) та завідувач каси установи банку.

*Правила безпеки під час видачі грошей зі сховищ* [13]:

здійснювати під розписку у Книзі обліку видачу зі сховищ грошей і матеріальних цінностей;

перед закриттям сховищ обов'язково перевіряти щодо того, чи всі цінності, книги, документи, які мають зберігати у сховищах, занесено у сховище; чи відповідає фактична наявність готівки та цінностей операційної каси даним бухгалтерського обліку і залишкам, зазначеним у книзі обліку готівки операційної каси й інших цінностей; чи всі шафи зачинено, а електроприлади та світло вимкнено;

здійснювати запис у контрольному журналі про здавання під охорону замкнених та опечатаних сховищ;

розмежувати доступ до грошового сховища посадових осіб, відповідальних за схоронність цінностей. Інші працівники можуть входити до грошового сховища тільки з дозволу керуючого банку або його заступника, який відповідальний за операції з матеріальними цінностями, обов'язково у присутності посадових осіб, відповідальних за схоронність цінностей;

обов'язково відкривати грошові сховища в робочі дні з метою огляду й перевірки посадовими особами, відповідальними за схоронність цінностей, незалежно від факту здійснення операцій із цінностями;

складати акт до відкриття сховища в разі, якщо виявлено пошкодження дверей, замків або печаток, є підозри у спробі проникнення у сховище. Акт підписують посадові особи, що є відповідальними за схоронність цінностей, та представник охорони. Потім повідомляють керуючого банку. У разі порушення цілісності приміщення сховища слід скласти акт про наявність цінностей;

обов'язково змінювати ключі від грошового сховища, сейфів у разі їх утрати. Про факт утрати ключів або печаток, якими опечатують сховища, зміни ключів та кодів до замків складають відповідний акт, потім в обов'язковому порядку проводять службові розслідування. За результатами розслідування осіб, винних у втраті ключів та печаток, притягують до дисциплінарної або кримінальної відповідальності в разі їх сприяння крадіжкам;

3) дотримання порядку обліку, видачі, використання та зберігання ключів від грошових сховищ, сейфів, шаф, приміщень, що здають під охорону. У банках на основі чинної нормативно-правової бази розроблено порядок обліку, видачі, використання та зберігання ключів від грошових сховищ, сейфів, шаф, приміщень, що здають під охорону, та приміщень господарського призначення банку.

Порядок обліку, видачі та зберігання ключів наведено в табл. 8.13.

Таблиця 8.13

**Правила безпеки зберігання, обліку та видачі ключів від приміщень банку**

| Види приміщень | Особливості зберігання ключів |
|---|---|
| 1 | 2 |
| Сховища, сейфи, шафи, приміщення касового вузла | Ключі обліковує у "Книзі обліку ключів від грошових сховищ, сейфів та шаф" відповідальний працівник відділу безпеки, на якого покладено обов'язок вести облік. Ключі від основного грошового сховища видають під підпис у книзі обліку трьом матеріально відповідальним особам банку, які, згідно з наказом голови правління, мають право відкривати та закривати грошове сховище. Ключі від сейфів та шаф, що знаходяться у грошових сховищах та на робочих місцях касових працівників, видають під підпис у книзі обліку касовим працівникам, які користуються конкретними сейфами та шафами. Дублікати ключів передають на зберігання до відділу безпеки в мішку, запечатаному сургучними печатками трьох матеріально відповідальних осіб, що відкривають та закривають грошове сховище. У мішку разом із ключами обов'язково залишено опис укладених ключів. Мішок із дублікатами ключів від грошового сховища, сейфів та шаф видає відділ безпеки лише за службовою запискою з письмовою вимогою трьох матеріально відповідальних осіб та їх підписами. Після закінчення робочого дня ключі від вхідних дверей касового вузла касир, який останнім залишає роботу в касах, здає співробітнику охорони в опечатаних тубусах під підпис у "Контрольному журналі здавання-прийняття" під охорону касового вузла банку. Усі ключі від дверей приміщень касового вузла відповідальна особа відділу безпеки передає керівнику касового підрозділу. Під час використання грошових сховищ, сейфів або шаф кількома працівниками, передачу ключів між ними здійснюють через відповідального працівника відділу безпеки із записами у книзі обліку ключів |
| Вхідні двері банку, запасні виходи та приміщення господарського призначення | Ключі в одному примірнику зберігають у шафі, що зачиняють, у кімнаті охорони банку, їх видає охоронець працівникам банку, причетним до конкретних приміщень, під підпис у спеціально заведеному для цього відділом безпеки "Журналі обліку приймання-видавання ключів на посту охорони". Усі інші примірники ключів зберігають у сейфі працівника відділу безпеки, що відповідає |

Закінчення табл. 8.13

| 1 | 2 |
|---|---|
| | за організацію охорони банку. Ключі від приміщень, де розміщено технологічне обладнання систем забезпечення життєдіяльності банку (газова котельня, електрощитова) надають під підпис у названому журналі лише працівникам банку, погодженим із відділом безпеки за службовою запискою адміністративно-господарського управління, а також представникам орендодавця, список яких погоджено з керівництвом банку |
| Приміщення, де розміщені сервери банку | Працівників банку, що виконують обов'язки операціоністів та операторів автоматизованих робочих місць (АРМ) і користуються таємними ключами електронного підпису платіжних документів банку в Системі електронних платежів НБУ, забезпечують сейфами або секціями в загальній шафі для зберігання таємних ключів та металевою печаткою для їх опечатування. За умов змінної роботи адміністраторів АРМ НБУ передачу ключів за змінами здійснюють одночасно з передачею апаратури криптозахисту інформації НБУ та сейфа, де її зберігають. Передавання фіксують у "Журналі приймання-передавання засобів захисту інформації". По одному примірнику кожного ключа від приміщення АРМ НБУ і сейфа надають адміністратору АРМ НБУ під підпис у книзі обліку, а від приміщення, де розміщено сервери банку, надають під підпис у книзі обліку ключів працівнику управління інформаційних технологій, якому дозволено вхід до цих приміщень і здавання їх під охоронну сигналізацію. Після закінчення робочого дня ключі від вхідних дверей АРМ НБУ та серверної працівники банку здають на пост охорони в опечатаних тубусах під підпис у "Журналі обліку приймання-видавання тубусів із ключами на посту охорони" |
| Сейфи працівників банку, де зберігають таємні ключі електронних підписів банківських документів | Один примірник кожного ключа від сейфа надають працівнику банку під підпис у книзі обліку, а дублікати ключів зберігають у відділі безпеки в опечатаних працівниками банку конвертах і видають у тимчасове користування працівнику в разі втрати ним основного ключа або залишенні ключа вдома. У разі втрати ключа відділ безпеки здійснює службову перевірку і вживає негайних заходів щодо заміни замка або надання працівнику іншого сейфа |

Утрата ключів є прямою загрозою безпеці касових операцій. Тому дії персоналу мають бути оперативними та зваженими.

*Дії банківського персоналу в разі втрати ключів:*

працівник банку зобов'язаний доповісти про цей випадок відділу безпеки банку та вживати всіх необхідних заходів щодо розшуку ключа;

відділ безпеки здійснює службову перевірку факту втрати ключа для з'ясування обставин його втрати та надає допомогу з розшуку втраченого ключа. Про результати службової перевірки доповідають керівництву банку. У разі неможливості знайти ключ або за підозри, що його можуть використати для завдання шкоди банку, відділ безпеки вносить пропозицію щодо заміни замка або сейфа чи шафи;

про втрату ключів від грошових сховищ або приміщення й сейфа АРМ НБУ, сейфів операторів АРМ та операціоністів, де зберігають засоби захисту інформації НБУ, керівництво банку доповідає Національному банку України.

### 8.2.4. Забезпечення безпеки валютних операцій банків

**Валютні операції банку** – це одна з найбільш ризикових сфер його діяльності, оскільки аналіз співпраці з іноземними партнерами часто характеризується браком інформації про їх діяльність та фінансову стійкість.

*Загрози безпеці валютних операцій банку*:

коливання курсу валют;

неправомірні дії персоналу банку;

умисні злочинні дії клієнтів;

утрата валюти під час перерахування із-за кордону;

неправомірні дії з готівковою іноземною валютою;

недотримання валютними обмінними пунктами правил продажу валюти;

ненадійні іноземні банки-кореспонденти;

відсутність документального оформлення обмінних операцій;

неретельна перевірка банкнот із метою виявлення фальшивих.

Пункти обміну валют у межах безпеки валютних операцій мають дотримуватися певних правил перевірки банкнот (табл. 8.14).

Таблиця 8.14

**Ознаки виявлення фальшивої валюти**

| Ознаки | Характеристики |
|---|---|
| 1 | 2 |
| Папір | Папір для грошей виготовляють із високоякісної сировини, вона має якісну проклейку, що надає їй жорсткості, тому, зминаючи гроші, можна чути характерний хрускіт |

Закінчення табл. 8.14

| 1 | 2 |
|---|---|
| Водяні знаки | Водяні знаки містяться практично в усіх валютах. Якщо розглядати їх на світло, вони будуть більш темними (іноді більш світлими), ніж основний фон купюри, причому перехід кольору майже не помітний |
| Захисні нитки | У папір багатьох валют уставляють металізовані, профарбовані тоненькі смужки, які містять мікродрук |
| Мікротекст | На деяких частинах малюнків грошових знаків має бути мікротекст |
| Волокна | На грошових знаках мають бути волокна, які у процесі виробництва паперу для грошей додають до нього. Переважно, вони світяться під дією ультрафіолетових променів і можуть бути кольоровими чи безкольоровими. Волокна можна підчепити голкою, тоді як на фальшивих грошових знаках такі волокна можна стерти |
| Конфеті | У папір деяких грошових знаків під час його виготовлення вводять маленькі кружечки – безкольорові та флуоресцентні під дією ультрафіолетових променів. Вони мають мікродрук або блідо-кольорові нитки і створюють відповідний рельєф, якого не буває на фальшивих грошових знаках |
| Тиснені сітки | Сітки помітні лише тоді, якщо розглядати гроші під відповідним кутом зору |
| Друк | На банкнотах використано офсетний, глибокий, металографічний друк та спеціальні номератори. На грошових знаках виконано особливий "райдужний" друк, чим забезпечено плавний кольоровий перехід фарб, який практично неможливо зімітувати |
| Малюнок | На банкнотах має бути філігранний малюнок портретів провідних політичних діячів, учених, представників культури. Портрети, сітки для фону, малюнки складено з тонких чітких ліній. Повторити чітко такі малюнки частіш за все неможливо. На обох сторонах грошових знаків існують малюнки, які під час розгляду на світлі мають створювати малюнок, що збігається. Подібну точність фальшивовалютники не завжди можуть відтворити |
| Оптичний ефект | Під різним кутом зору кольори грошових знаків деяких валют змінюють свій відтінок. Переважно, підробок грошових знаків таких валют немає |
| Фарба | Має містити різноманітні елементи, що світяться в ультрафіолетових променях. Крім того, мають місце домішки, які мають феромагнітні властивості |
| Голограми | Голограми, кінограми хоч і є дорогим засобом захисту грошей, але на знаках великих номіналів вони можуть бути |
| Пластикове покриття | Пластикове покриття деяких грошових знаків створює добре помітний захисний блиск і до того ж більше зберігає "працездатність" таких знаків |

*Функції банку щодо забезпечення безпеки валютних операцій:*

контроль за роботою обмінних кас щодо дотримання вимог зберігання валюти;

перевірка обмінних кас щодо своєчасності та правильності оформлення виконаних операцій;

контроль за законністю здійснюваних обмінними пунктами операцій;

здійснення перевірки пункту обміну, відповідно до вимог НБУ;

перевірка фінансового стану та надійності іноземних банків-кореспондентів за результатами рейтингового оцінювання їх діяльності міжнародними агенціями;

уникнення платежів за кордон за підробленими документами;

боротьба з відмиванням "брудних" грошей, що використовують для оплати товарів і послуг українських суб'єктів господарювання.

ознайомлення з договорами та митними деклараціями клієнтів із метою уникнення незаконних операцій;

здійснення банком купівлі валюти без участі посередників;

детальний аналіз динаміки валютних курсів на міжбанківському ринку.

### 8.2.5. Боротьба з легалізацією ("відмиванням") незаконно отриманих грошей

**Легалізація ("відмивання") грошей** – це процес, спрямований на приховування чи маскування незаконного походження, місця знаходження чи переміщення грошових коштів і володіння ними.

Небезпечний характер "відмивання" грошей обумовлений тим, що дозволяє злочинцям користуватися грошима без загрози виявлення їх незаконного походження.

Визначення терміна "легалізація ("відмивання") грошей" уперше використано в Директиві Європейського Економічного Союзу "Про запобігання використанню фінансової системи для "відмивання" грошей (91/308/ЄЕС)" від 19 червня 1991 р. У цьому документі вказано, що "відмиванням" грошей є такі злочинні дії в міжнародному масштабі:

перетворення та передача майна, знаючи, що це майно отримано в результаті злочинної діяльності або співучасті в такій діяльності з метою приховування чи маскування незаконного походження коштів, або надання допомоги будь-якій особі, залученій у таку діяльність, із метою уникнення юридичних наслідків цієї діяльності;

маскування або покриття дійсних джерел доходів, місцезнаходження, переміщення власності чи майна, знаючи, що таке майно отримано в результаті злочинної діяльності або співучасті в такій діяльності;

придбання майна, володіння або користування ним, знаючи, що таке майно отримано в результаті злочинної діяльності або співучасті в такій діяльності;

надання допомоги, співучасть, здійснення спроби "відмивання" грошей, сприяння в наданні порад щодо здійснення дій, пов'язаних із приховуванням доходів.

*Види нелегальних доходів:*

доходи від наркобізнесу;

доходи від торгівлі зброєю;

контрабандні доходи;

доходи від торгівлі людьми, викрадання людей;

доходи від несплати податків та інших незаконних джерел.

Боротьбу банку з незаконним "відмиванням" грошей мають здійснюватися на всіх етапах відмивання грошей, виділених FATF:

1) розміщення. Нелегально отримані гроші розміщують у фінансових інструментах банківських та небанківських фінансових установ шляхом розподілу внесків, незаконного використання винятків із законодавства, використання кореспондентських відносин із банками, переказу грошей незаконним шляхом, використання "колективних" та транзитних рахунків, обміну дрібних банкнот на купюри іншої вартості або іншу валюту; злиття законних і незаконних засобів;

2) шарування, що становить відокремлення незаконних доходів від джерел їх отримання шляхом створення багатоланкового ланцюга фінансових операцій, спрямованих на маскування походження цих доходів. Для шарування використовують такі методи: переказ наявних грошей у грошові інструменти, придбання і продаж майна, електронний переказ коштів, множинний переказ грошей на рахунки інших фірм, переказ грошей в офшорні зони;

3) інтеграція – створення видимості легальності отриманих злочинним шляхом грошових коштів. На цьому етапі нелегальних грошам знаходять легальне джерело походження, а потім їх інвестують у цілком легальну економіку. У ході інтеграції "відмиті" гроші повертають до банківської системи під виглядом чесно зароблених доходів. Методи, використовувані у процесі інтеграції: продаж нерухомості; викривлення цін

за зовнішньоторговельними операціями (через завищення в документах сум, що надходять до країни, задля виправдання вкладень відповідних сум у банки або завищення обсягів експорту з метою обґрунтування легальності отримання відповідних сум (із-за кордону); трансферпрайсинг (складають два договори: реальний і фіктивний (із завищеною сумою операції). Згідно з фіктивним договором, гроші переказують фірмі-посереднику, зазвичай зареєстрованій в офшорній зоні. Різниця між реальною та фіктивною ціною і є доходом фірми, що залишається на її рахунку); користування банківськими рахунками іноземної або спільної фірми; унесення готівки на поточний рахунок фірми задля надання грошовим коштам видимості доходів від продажів; використання підставних компаній та помилкових кредитів.

*У межах запобігання "відмиванню" і легалізації тіньових доходів банки мають виконувати такі запобіжні заходи:*

не вести анонімні рахунки клієнтів;

не відкривати рахунки на фіктивні прізвища;

ідентифікувати клієнтів у разі сумнівних операцій;

виявляти операції, що здійснюють за незвичних або невиправдано заплутаних умов;

виявляти операції, що є економічно недоцільними або суперечать чинному законодавству;

здійснювати не тільки обов'язковий, а і внутрішній фінансовий моніторинг;

звертати увагу на операції, що здійснюють за незвичайними схемами або з незрозумілою кінцевою метою таких операцій;

не вступати в договірні відносини із клієнтами, яких підозрюють у здійсненні сумнівних операцій;

звертати увагу на виявлення компаній, що працюють в офшорних зонах;

розробляти програми протидії "відмиванню" грошових коштів.

*Ідентифікацію юридичних та фізичних осіб, що ймовірно здійснюють сумнівні операції, мають здійснювати в такий спосіб:*

щодо юридичних осіб – шляхом перевірки та отримання підтвердження юридичного факту і юридичної форми існування особи, адреси, прізвища керівників та їхніх повноважень;

щодо фізичних осіб – шляхом установлення особистості на підставі документа, що посвідчує особу власника, та фіксації в письмовій формі прізвища та імені, дати народження, адреси особи, яка здійснює угоду,

а також назви, номера й дати видачі документа, назви установи, що його видала;

щодо третіх осіб – шляхом перевірки повноважень діяти від імені клієнта з індентифікацією як юридичної чи фізичної особи.

*Характерними особливостями існування компаній, заснованих в офшорних зонах,* є [13]:

засновниками компаній можуть бути особи – не громадяни цієї 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 та вести рахунки не тільки у країні, де їх зареєстровано, а й інших країнах;

компанії офшорних зон не платять податків за місцем реєстрації, сплачують тільки щорічний збір, необхідний для підтримання юридичного статусу компаній;

за місцем реєстрації компанії подають фінансову звітність у спрощеній формі, що значною мірою скорочує обсяг публічної інформації про них;

компанії можуть мати номінальних директорів, які виконують тільки функції підтримання взаємовідносин компанії з державними органами країни.

Програми протидії "відмиванню" (легалізації) грошових коштів мають містити розроблення внутрішньої політики, методик внутрішнього фінансового моніторингу, програми підготовки кадрів.

## Практичне заняття

**Завдання 8.1.** Оцінювання кредитоспроможності позичальника.

*1. Оцінювання кредитоспроможності позичальника – юридичної особи (середнє підприємство).*

Узагальнену інформацію, де зазначено відомості про боржників за кредитами, має бути наведено в табл. 8.15.

Таблиця 8.15

**Дані про боржників за наданими кредитам**и

| № п/п | Відомості про боржників за наданими кредитами |
|---|---|
| 1 | 2 |
| 1 | Назва (для юридичних осіб), прізвище, ім'я та по батькові (для фізичних осіб) боржника і характер його відносин із банком (клієнт, інсайдер) |

Закінчення табл. 8.15

| 1 | 2 |
|---|---|
| 2 | Тип підприємства (вид господарського товариства, галузь промисловості, статутна діяльність), його власники (для юридичних осіб) |
| 3 | Номери аналітичних рахунків у банку (поточних, із обліку кредитів, депозитів, нарахованих доходів, позабалансових) |
| 4 | Інформація про наявність джерел надходження валютної виручки (за кредитами в іноземній валюті) |
| 5 | Інформація про включення суми боргу до групи фінансових активів (для фізичних осіб) |
| 6 | Номер договору про надання кредиту, дата видачі та кінцева дата погашення кредиту |
| 7 | Графік погашення кредиту |
| 8 | Сума (ліміт) та валюта кредиту |
| 9 | Фактична сума боргу за кредитом |
| 10 | Розмір відсоткової ставки та комісії (на дату видачі кредиту, поточної, за потреби – ставки пені), порядок сплати відсотків |
| 11 | Аналіз виконання бізнес-плану (для кредитів під інвестиційний проект) |
| 12 | Інформація про результати оцінювання фінансового стану боржника |
| 13 | Класифікація кредиту (клас боржника, стан обслуговування боргу, категорія кредиту) |
| 14 | Форма забезпечення кредиту (вид, назва, опис, місцезнаходження, ринкова вартість) |
| 15 | Інформація про перевірку заставленого майна (дата, результат перевірки, висновок фахівця банку щодо необхідності в переоцінюванні заставленого майна) |
| 16 | Сума забезпечення, яку беруть до розрахунку резерву |
| 17 | Розрахункова сума резерву за кредитом |
| 18 | Сума фактично сформованого резерву за кредитом |

Здійснити оцінювання кредитоспроможності підприємства переробної промисловості за даними балансу (додаток Д) та звіту про фінансові результати (додаток Е). Підприємство є середнім за розміром.

*Методичні рекомендації щодо виконання завдання:*

1. Розрахувати показники фінансового стану, необхідні для визначення інтегрального показника боржника та внести їх у табл. 8.16.

Таблиця 8.16

**Результати розрахунку фінансових коефіцієнтів із метою визначення інтегрального показника фінансового стану**

| Фінансові коефіцієнти | Значення для середнього підприємства | Значення для малого підприємства |
|---|---|---|
| 1) К1, МК1 – коефіцієнт покриття (ліквідність третього ступеня) | | |
| 2) К2, МК2 – проміжний коефіцієнт покриття | | |
| 3) К3, МК3 – коефіцієнт фінансової незалежності | | |
| 4) К4, МК4 – коефіцієнт покриття необоротних активів власним капіталом | | |
| 5) К5 – коефіцієнт рентабельності власного капіталу | | |
| 6) МК5 – коефіцієнт оборотності кредиторської заборгованості | | |
| 7) К6, МК6 – коефіцієнт рентабельності продажу за фінансовими результатами від операційної діяльності (EBIT) | | |
| 8) К7 – коефіцієнт рентабельності продажу за фінансовими результатами від звичайної діяльності | | |
| 9) МК7 – коефіцієнт рентабельності продажу за фінансовими результатами до оподаткування | | |
| 10) К8, МК8 – коефіцієнт рентабельності активів за чистим прибутком | | |
| 11) К9, МК9 – коефіцієнт оборотності оборотних активів | | |
| 12) К10 – коефіцієнт оборотності позичкового капіталу за фінансовими результатами від звичайної діяльності (EBITDA) | | |
| 13) МК10 – коефіцієнт оборотності позичкового капіталу за фінансовими результатами до оподаткування | | |

2. Здійснити оцінювання стану обслуговування боргу, якщо відомо, що прострочення платежів за кредитом відсутні.

3. Визначити інтегральний показник боржника за даними додатка Б та ураховуючи галузеву належність підприємства.

4. Визначити клас боржника юридичної особи за даними додатка В.

5. Визначити категорію якості кредиту та можливе значення показника ризику на основі табл. 8.4.

6. Зробити висновки про доцільність надання такого кредиту та зміни у кредитоспроможності позичальника.

*2. Оцінювання кредитоспроможності позичальника – юридичної особи (мале підприємство).*

Здійснити оцінювання кредитоспроможності суб'єкта малого підприємництва, основним видом діяльності якого є здавання в оренду нерухомості, за даними балансу (додаток Ж) та звіту про фінансові результати (додаток З).

Методичні рекомендації до виконання завдання 2 аналогічні рекомендаціям до виконання завдання 1.

**Завдання 8.2.** Рольова гра *"Робота кредитного комітету".*

У рольовій грі обирають склад кредитного комітету. Усі студенти можуть узяти участь у грі, якщо їх розподілити на групи з восьми осіб, які по черзі будуть виконувати роль кредитного комітету. Вихідні дані для роботи кредитного комітету беруть із попереднього завдання. Завдання (кредитні справи) у кредитних комітетів можуть бути як однакові, так і різні. Роботу комітетів можна оцінювати за аргументованістю висновків, злагодженістю та взаємопогодженістю рішень, виконанням окремих функцій, правильністю прийнятого рішення про кредитування. Бажану для створення структуру кредитного комітету наведено на рис. 8.4.


Рис. 8.4. **Структура кредитного комітету банку**

*Хід рольової гри:*

**1-й етап.** Визначення ролей у кредитному комітеті.

**2-й етап.** Обговорення функцій кожного члена кредитного комітету.

Голова кредитного комітету (голова правління банку) головує на його засіданнях. За його відсутності така функція переходить до обов'язків заступника голови (першого заступника голови правління банку).

Секретар кредитного комітету – особа, яку призначає голова кредитного комітету та яка готує проект порядку денного, веде протокол засідання, надає виписки із протоколу засідання кредитного комітету. До складу кредитного комітету головного банку може бути введено керівників підрозділу управління ресурсами, управління ризиками, відділу з питань роботи із проблемною заборгованістю; начальника департаменту планування та аналізу; фахівців із-поміж співробітників банку, кваліфікація та досвід яких дають можливість їм якісно виконувати функції, покладені на членів кредитного комітету.

До складу кредитного комітету, за можливості, не мають входити фахівці, які безпосередньо беруть участь у вивченні документів, наданих клієнтом для кредитування, та працівники з підготовки висновків щодо можливості здійснення кредитної операції.

**3-й етап.** Розгляд кредитної справи.

Для початку кредитний комітет має назвати необхідну кредитну документацію. Кількість правильно названих позицій кредитної документації враховують у процесі оцінювання роботи команд.

Кредитну документацію (справа) формують на паперових носіях, вона має містити:

1) письмове клопотання (заяву) боржника про надання кредиту;

2) бізнес-план, техніко-економічне обґрунтування потреби у кредиті на відповідні цілі (для юридичних осіб);

3) контракти та/або договори про купівлю-продаж (за наявності);

4) фінансову звітність (для юридичних осіб), інформацію про доходи (для фізичних осіб) боржника;

5) фінансову та бюджетну звітність (для бюджетної установи);

6) інформацію про надходження коштів на поточні рахунки в банку та інших банках щонайменше за останні шість повних місяців (боржник – фізична особа – надає за бажанням);

7) інформацію, надану боржником та документально підтверджену іншими банками, про:

а) заборгованість боржника з визначенням основних умов договору про надання кредиту (сума за договором, термін, залишок заборгованості, вид забезпечення за кредитом тощо);

б) наявність простроченої заборгованості;

8) інформацію про стан виконання зобов'язань боржника перед банком за попередніми договорами, кредитну історію (за наявності);

9) інформацію про перевірку цільового використання кредиту;

10) підтвердні документи (виписки за балансовими та позабалансовими рахунками, платіжні доручення тощо), що свідчать про надання та погашення кредиту, наявні фінансові зобов'язання, оприбуткування заставленого майна тощо;

11) аудиторський висновок про фінансовий стан боржника (за наявності);

12) висновок уповноважених фахівців банку щодо оцінювання кредитоспроможності боржника;

13) установчі та реєстраційні документи (для юридичних осіб), копії відповідних сторінок паспорта та довідки про присвоєння реєстраційного номера облікової картки платника податків (для фізичних осіб) або серії та номера паспорта для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків і повідомили про це відповідний орган Державної податкової служби та мають позначку в паспорті;

14) рішення колегіальних органів банку про можливість надання кредиту або рішення колегіальних органів щодо надання повноважень визначеній особі банку приймати рішення про можливість надання кредитів, запровадження змін до чинних умов договору про надання кредиту;

15) договір про надання кредиту і додаткові договори до нього;

16) договори застави (іпотеки) та додаткові договори до них, гарантійні листи;

17) документи, що підтверджують повноваження особи підписувати договір про надання кредиту, договори застави (іпотеки) та додаткові договори до них від імені контрагента банку;

18) копії правоустановчих документів на майно (майнові права), що передають у забезпечення;

19) документи, що підтверджують ринкову вартість заставленого майна (майнових прав) під час видачі кредиту;

20) документи, що свідчать про наявність та якість зберігання заставленого майна (акти, довідки, матеріали перевірок);

21) документи, що свідчать про обтяження майна та його державну реєстрацію, відповідно до вимог законодавства України;

22) договори страхування заставленого майна та документи, що підтверджують сплату страхового платежу (за наявності);

23) інформацію про вжиті банком заходи для погашення боргу (документи, що засвідчують процедуру повернення або стягнення боргу).

**4-й етап.** Створення бізнес-моделі позичальника за схемою, показаною на рис. 8.5.

| Назва підприємства |
|---|
| Вид діяльності |
| Цінність продуктів і послуг |
| Сегменти ринку, цільовий ринок |
| Партнери |
| Основні вхідні грошові потоки |
| Основні вихідні грошові потоки |
| Кредитна історія |
| Об'єкти застави, гарантії погашення кредиту |
| Перспективи розвитку діяльності позичальника |
| Клас позичальника |

Рис. 8.5. **Карта бізнес-моделі позичальника**

**5-й етап.** Оцінювання загроз та переваг співробітництва з позичальником, що здійснюють за схемою, наведеною в табл. 8.17. Усі переваги та недоліки має бути обґрунтовано.

Таблиця 8.17

**Систематизація переваг співробітництва з позичальником та загроз непогашення ним кредиту**

| Переваги та гарантії успішного співробітництва | Загрози непогашення кредиту |
|---|---|
| | |

**6-й етап.** Обговорення інформації про позичальника.

Виступи учасників кредитного комітету в межах своїх повноважень.

**7-й етап.** Прийняття рішення шляхом відкритого голосування.

Оцінювання роботи команд здійснюють, залежно від якості й аргументованості рішення та кількості правильно названої кредитної документації.

## Тематика доповідей та рефератів

1. Організація управління безпекою кредитних операцій.
2. Засоби забезпечення безпеки валютних операцій.
3. Фактори, що визначають рівень безпеки касових операцій.
4. Оцінювання кредитоспроможності позичальника.

## Практичні завдання для самостійного виконання

**Завдання 8.1.** Здійснити аналіз структури кредитного портфеля банку на основі даних, наведених у табл. 8.18. Зробити висновки.

Таблиця 8.18

### Аналіз структури кредитного портфеля банку

| Категорії якості кредитів | Суми, тис. грн | Структура, % | Коефіцієнти ризику, % | Суми резерву, тис. грн |
|---|---|---|---|---|
| I – найвища | 12 169,50 | ? | ? | ? |
| II | 17 100,00 | ? | ? | ? |
| III | 25 458,30 | ? | ? | ? |
| IV | 6 406,03 | ? | ? | ? |
| V – найнижча | 5 094,20 | ? | ? | ? |
| Усього | ? | 100 | – | ? |

**Завдання 8.2.** Визначити та проаналізувати динаміку показників погашення кредитів. Зробити висновки про їх вплив на економічну безпеку банку. Вихідні дані наведено в табл. 8.19.

Таблиця 8.19

**Вихідні дані для аналізу погашення кредитів,** тис. грн

| Показники | Минулий рік | Звітний рік |
|---|---|---|
| Сума кредитного портфеля | 1 200,0 | 1 500,5 |
| Позички із простроченою сплатою відсотків і основного боргу | 100,1 | 120,5 |
| Збитки за позичками, отриманими за період | 50,2 | 30,9 |
| Середній залишок позичкової заборгованості за кредитами | 987,1 | 1 130,5 |
| Сума виданих кредитів за період | 212,9 | 370,0 |
| Сума погашених кредитів за період | 345,6 | 564,9 |

**Завдання 8.3.** Здійснити коефіцієнтний аналіз якості розрахунково-касового обслуговування клієнтів банку. Вихідні дані наведено в табл. 8.20.

Таблиця 8.20

**Вихідні дані для аналізу розрахунково-касового обслуговування,** тис. грн

| Показники | Минулий рік | Звітний рік |
|---|---|---|
| Дебіторська заборгованість банку за розрахунками із клієнтами | 120,0 | 150,5 |
| Кредиторська заборгованість банку за розрахунками із клієнтами | 100,1 | 120,5 |
| Оборот за надходженням коштів | 345,5 | 430,5 |
| Оборот за видатками (платежами) | 212,9 | 370,0 |
| Середні залишки на поточних рахунках клієнтів | 445,6 | 565,5 |

**Завдання 8.4.** Здійснити коефіцієнтний аналіз валютних розрахунків банку. Визначені за минулий і звітний період показники порівняти, зробити висновки про їх динаміку та ефективність роботи валютного відділу банку. Вихідні дані наведено в табл. 8.21.

Таблиця 8.21

**Вихідні дані для аналізу валютних розрахунків банку**

| Показники | Минулий рік | Звітний рік |
|---|---|---|
| Доходи від валютних операцій, тис. грн | 220,0 | 150,5 |
| Середні валютні активи, тис. грн | 500,1 | 620,5 |
| Середня сума активів, тис. грн | 1 345,5 | 1 430,5 |
| Загальна сума доходів банку, тис. грн | 712,9 | 770,0 |
| Кількість персоналу валютного відділу, осіб | 7,0 | 10,0 |
| Витрати на здійснення валютних операцій, тис. грн | 150,1 | 170,5 |

**Завдання 8.5.** Розрахувати значення таких банківських нормативів: нормативу адекватності регулятивного капіталу та нормативу співвідношення регулятивного капіталу до сукупних активів.

Вихідні дані для аналізу:

регулятивний капітал банку – 1 200,0 тис. грн;

активи та позабалансові інструменти, зважені на ризик – 22 000,0 тис. грн;

сума резервів за активними операціями – 6 000,0 тис. грн;

сума сукупних активів – 18 000,0 тис. грн.

Установити відповідність значень нормативу адекватності регулятивного капіталу та нормативу адекватності власного капіталу їх нормативним значенням, установленим, згідно із чинним законодавством України. Проаналізувати в разі невиконання нормативів наслідки для банківської установи. Розробити рекомендації щодо забезпечення дотримання цих нормативів.

**Завдання 8.6.** Визначити нормативи ліквідності банку. Проаналізувати відповідність їх значень установленим нормативам. Зробити припущення про наслідки для банку в разі невиконання нормативів. Запропонувати за потреби заходи щодо забезпечення дотримання нормативів ліквідності.

Вихідні дані для аналізу:

кошти в касі банку – 10,2 тис. грн;

кошти на коррахунку в НБУ – 40,9 тис. грн;

кошти на коррахунках в інших банках – відсутні;

зобов'язання за поточними рахунками – 650,5 тис. грн;

боргові цінні папери – 30,0 тис. грн;

надані кредити з терміном погашення в межах місяця – 100,0 тис. грн;

зобов'язання з терміном погашення до 30 днів – 340,6 тис. грн;

сума ліквідних активів – 250,0 тис. грн;

короткострокові зобов'язання з початковим терміном погашення до одного року – 350,0 тис. грн.

**Завдання 8.7.** Запропонувати власний варіант вирішення кожної із трьох поставлених проблем. Відповідь обґрунтувати.

1. До кредитного відділу банківської установи звернулося відоме підприємство із клопотанням про відкриття кредитної лінії. Банку стало відомо, що на підприємстві добігає кінця аудиторська перевірка. Банк висловив побажання отримати результати аудиторської фірми. Проте підприємство поспішає з відкриттям кредитної лінії й отриманням першого кредиту.

Який висновок (позитивний чи негативний) ви зробите щодо можливості надання кредиту цьому підприємству?

2. Клієнт банку надав для отримання кредиту фінансову звітність, що не містить ніяких проблемних статей. За результатами оцінювання кредитоспроможності позичальника – юридичної особи – фінансовий стан визначено як стійкий. Перевірка застави пройшла на належному рівні та встановила відповідність фактичного об'єкта та його грошової вартості заявленому. Банк є членом Бюро кредитних історій. Служба безпеки виявила, що позичальник є фігурантом цього бюро. Яким має бути ймовірне рішення про надання кредиту? Чому?

3. Ви займаєте посаду начальника відділу кредитних операцій і є членом кредитного комітету. Одного разу на голосуванні за надання кредиту одному з позичальників голоси членів кредитного комітету розподілилися порівну. Якими мають бути дії начальника відділу кредитних операцій? Хто приймає остаточне рішення про надання кредиту позичальнику?

**Завдання 8.8.** Здійснити аналіз структури кредитного портфеля за своєчасністю погашення кредитів. Зробити висновки щодо впливу такої структури кредитного портфеля на фінансово-економічну безпеку банку. Вихідні дані наведено в табл. 8.22.

Таблиця 8.22

## Вихідні дані для аналізу структури кредитного портфеля за видами кредитів та якістю їх погашення

| Рядки | Назви статей | Кредити юридичним особам | Кредити фізичним особам-підприємцям | Іпотечні кредити фізичних осіб | Споживчі кредити фізичним особам | Інші кредити фізичним особам | Усього |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Непрострочені та незнецінені | 446 569 | 26 292 | 2 904 | 66 079 | 117 | 541 961 |
| 1.1 | великі позичальники із кредитною історією більшою від 2 років | 73 955 | 0 | 0 | 0 | 0 | 73 955 |
| 1.2 | нові великі позичальники | 13 966 | 0 | 0 | 0 | 0 | 13 966 |
| 1.3 | кредити середнім компаніям | 299 661 | 0 | 0 | 0 | 0 | 299 661 |
| 1.4 | кредити малим компаніям | 58 987 | 0 | 0 | 0 | 0 | 58 987 |
| 1.5 | інші кредити фізичним особам | 0 | 26 292 | 2 904 | 66 079 | 117 | 95 392 |
| 2 | Прострочені, але не знецінені | 287 | 5 | 0 | 143 | 0 | 435 |
| 2.1 | із затримкою платежу до 31 дня | 0 | 5 | 0 | 0 | 0 | 5 |
| 2.2 | із затримкою платежу від 32 до 92 днів | 0 | 0 | 0 | 15 | 0 | 15 |
| 2.3 | із затримкою платежу від 93 до 183 днів | 96 | 0 | 0 | 0 | 0 | 96 |
| 2.4 | із затримкою платежу від 184 до 365 (366) днів | 0 | 0 | 0 | 0 | 0 | 0 |
| 2.5 | із затримкою платежу більш ніж 366 (367) днів | 191 | 0 | 0 | 128 | 0 | 319 |
| 3 | Знецінені кредити, оцінені на індивідуальній основі: | 0 | 0 | 0 | 0 | 0 | 0 |
| 3.1 | із затримкою платежу до 31 дня | 0 | 0 | 0 | 0 | 0 | 0 |

Закінчення табл. 8.22

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 3.2 | із затримкою платежу більш ніж 366 (367) днів | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | Загальна сума кредитів до вирахування резервів | 446 856 | 26 297 | 2 904 | 66 222 | 117 | 542 396 |
| 5 | Резерв під знецінення за кредитами | (3 970) | (6) | (4) | (2 425) | (1) | (6 406) |
| 6 | Усього кредитів за мінусом резервів | 442 886 | 26 291 | 2 900 | 63 797 | 116 | 535 990 |

## Методичні рекомендації щодо виконання практичних завдань:

*До завдання 8.1*

Аналіз структури кредитного портфеля здійснюють шляхом визначення питомої ваги кредитів різної якості. Резерв визначити за верхньою межею показника ризику (табл. 8.23).

Таблиця 8.23

### Визначення показника ризику кредиту, наданого боржнику – фізичній особі

| Категорії якості кредиту | Значення показників ризику кредиту |
|---|---|
| I – найвища | 0,01 – 0,06 |
| II | 0,07 – 0,20 |
| III | 0,21 – 0,50 |
| IV | 0,51 – 0,99 |
| V – найнижча | 1,00 |

*До завдань 8.2 і 8.3*

Оцінювання видачі та погашення кредитів здійснюють шляхом коефіцієнтного аналізу. Формули для його здійснення наведено в табл. 8.24.

Таблиця 8.24

## Показники аналізу видачі та погашення кредитів

| Показники | Формули для розрахунку | Сутність показників |
|---|---|---|
| *Показники аналізу видачі кредитів* | | |
| Коефіцієнт забезпеченості позичок | $К1 = \frac{\text{сума забезпечення кредитів}}{\text{сума кредитного портфеля}}$ | Характеризує захищеність банку від утрат за рахунок гарантій, застави майна, поручительства |
| Коефіцієнт захищеності позичок | $К2 = \frac{\text{сума резерву на покриття збитків за позичками}}{\text{сума кредитного портфеля}}$ | Характеризує рівень внутрішньої захищеності банку від збитків за рахунок формування резервів |
| Темпи зростання кредитного портфеля | $К3 = \frac{\text{сума кредитного потрфеля на кінець періоду}}{\text{сума кредитного портфеля на початок періоду}}$ | Характеризує кредитну активність банку |
| Коефіцієнт покриття позичок власним капіталом | $К4 = \frac{\text{власний капітал банку}}{\text{сума кредитного портфеля}}$ | Показує, яку частину кредитного портфеля фінансують за рахунок власних коштів |
| *Показники аналізу погашення кредитів* | | |
| Коефіцієнт несплачених позичок | $К5 = \frac{\text{позички із простроченою сплатою відсотків та основного боргу}}{\text{сума кредитного портфеля}}$ | Показує відсоток проблемних кредитів. Банки мають сприяти його зменшенню |
| Коефіцієнт збитковості позичок | $К6 = \frac{\text{збитки за позичками, отриманими за період}}{\text{середній залишок заборгованості за кредитами}}$ | Визначає частину позичок за певний період, що призвели до збитків |
| Коефіцієнт погашення позичок | $К7 = \frac{\text{сума погашених позичок}}{\text{сума виданих позичок}}$ | Показує відсоток погашення виданих кредитів |
| Коефіцієнт оборотності кредитів | $К8 = \frac{\text{сума погашених позичок за період}}{\text{середній залишок позичкової заборгованості}}$ | Характеризує кількість оборотів, що здійснюють кредитні ресурси за період |
| Тривалість обороту у днях | $К9 = \frac{\text{тривалість періоду}}{К8}$ | Бажаним є зменшення К9 і збільшення К8 |

*До завдання 8.4*

Коефіцієнтний аналіз валютних розрахунків містить [17]:

1) коефіцієнт дохідності валютних операцій (відношення доходів від валютних операцій до середніх валютних активів);

2) валютний дохід на 1 грн активів (відношення доходів від валютних операцій до середніх активів);

3) питому вагу доходів від валютних операцій у загальних доходах;

4) продуктивність праці одного працівника валютного відділу (відношення доходів від валютних операцій до чисельності працівників валютного відділу);

5) рентабельність валютних операцій (відношення доходів від валютних операцій до витрат на здійснення валютних операцій).

*До завдання 8.5*

**Норматив Н2** – норматив адекватності регулятивного капіталу (платоспроможності) – відображає здатність банку в повному обсязі та своєчасно розраховуватися за зобов'язаннями, що випливають із торговельних і кредитних операцій. Чим більше значення Н2, тим більша частка ризику, що її беруть власники банку, і навпаки. Його визначають так:

$$Н2 = \frac{Н1}{Ар - Р} \cdot 100, \qquad (8.1)$$

де Н1 – регулятивний капітал банку;

Ар – активи та позабалансові інструменти, зважені на ризик;

Р – сума резервів за активними операціями.

Нормативне значення коефіцієнта Н2 для діючих банків має бути не меншим за 10 %.

Норматив співвідношення регулятивного капіталу до сукупних активів Н3: значення має бути не меншим за 9 % співвідношення регулятивного капіталу до сукупних активів.

*До завдання 8.6*

**Норматив миттєвої ліквідності (Н4)** визначають для контролю за здатністю банку забезпечити своєчасне виконання своїх грошових зобов'язань за рахунок високоліквідних активів. Формула для розрахунку нормативу Н4 має такий вигляд:

$$Н4 = \frac{Кк + Кн + Кі}{З}, \qquad (8.2)$$

де Кк – кошти в касі банку;

Кн – кошти на коррахунку в НБУ;

Кі – кошти на коррахунках в інших банках;

З – зобов'язання за поточними рахунками.

Н4 має бути не меншим за 20 %. Якщо фактичне значення Н4 значно більше від нормативного і цю тенденцію спостерігають декілька днів, то банк накопичує ліквідність для фінансування кредитів чи інвестування або в нього неприпустимо великою є частка зобов'язань до вимоги в сукупних зобов'язаннях, або мають місце тимчасові труднощі із прибуткового розміщення залучених коштів. Якщо ситуація вказує на непокриття нормативу впродовж деякого часу, то банк має проблеми з виконанням зобов'язань перед клієнтами, покриває відплив коштів із депозитів або допускає несвоєчасну сплату їх рахунків.

**Норматив поточної ліквідності (Н5)** установлено для визначення збалансованості термінів і сум ліквідних активів та зобов'язань банку. Для його розрахунку беруть вимоги й зобов'язання банку з кінцевим терміном погашення до 30 днів включно. Н5 має становити не менш ніж 40 %. Формула для розрахунку має такий вигляд:

$$Н5 = \frac{Ап + Ав}{Зт}, \qquad (8.3)$$

де Ап – активи первинної ліквідності (це кошти в касі та на коррахунках банку в НБУ та інших банках);

Ав – активи вторинної ліквідності (боргові цінні папери та надані кредити з терміном погашення в межах місяця);

Зт – зобов'язання з терміном погашення до 30 днів.

**Норматив короткострокової ліквідності (Н6)** установлено для контролю за здатністю банку виконувати взяті ним короткострокові зобов'язання за рахунок ліквідних активів. Н6 має бути не меншим за 20 %. Формула для розрахунку має такий вигляд:

$$Н6 = \frac{ЛА}{КЗ}, \qquad (8.4)$$

де ЛА – ліквідні активи;

КЗ – короткострокові зобов'язання з початковим терміном погашення до одного року.

*До завдання 8.8*

Структуру кредитного портфеля аналізують шляхом визначення питомої ваги різних видів кредитів.

## Методичні рекомендації щодо виконання самостійної роботи

Опрацювання доповідей, рефератів та підготовку до занять здійснюють на основі літературних джерел: [13; 16; 18; 20; 26; 27; 32].

## Контрольні запитання

1. Описати порядок захисту матеріальних цінностей, обладнання та технічних засобів від протиправних зазіхань.
2. Яким чином мають забезпечувати безпеку банківських операцій?
3. Які існують види банківських операцій?
4. Описати механізм забезпечення безпеки кредитних операцій банків.
5. Як забезпечують безпеку роботи банків на фондовому ринку?
6. Охарактеризувати процес забезпечення безпеки здійснення в банках касових операцій.
7. Яким чином забезпечують безпеку роботи банків із пластиковими платіжними засобами?
8. Назвати особливості забезпечення безпеки валютних операцій банківських установ.
9. Описати порядок здійснення боротьби з легалізацією ("відмиванням") незаконно отриманих грошей.
10. Що таке "фінансово-економічна безпека банківських установ"?
11. Розкрити поняття про повну та обмежену матеріальну відповідальність.
12. Назвати ризики неправильного вибору позичальника.
13. Розкрити сутність кредитного моніторингу.
14. Назвати ознаки виникнення проблем із поверненням кредиту.
15. Охарактеризувати роботу банку із простроченими кредитами.
16. Назвати наявні види цінних паперів.
17. Описати порядок визнання грошей зношеними та значно зношеними.
18. Охарактеризувати порядок прийняття банком грошей від інкасаторів.
19. Розкрити сутність сумнівних фінансових операцій.

## Тести

*Тести одиничного вибору*

1. Загальний розділ характеристики позичальника не містить відомості про:

а) форму власності, організаційно-правову форму;

б) кількість працівників;

в) місце розташування підприємства;

г) номери службових, домашніх та мобільних телефонів керівників;

д) участь підприємства в державних програмах, наявність пільгових умов для ведення своєї діяльності в межах конкретних програм;

е) наявність на підприємстві служби безпеки, хто її очолює;

є) види продукції.

2. Характеристика позичальника містить такі розділи:

а) загальний і спеціальний;

б) основний і додатковий;

в) первинний і вторинний;

г) аналітичний і загальну характеристику;

д) власний варіант відповіді.

*Тести множинного вибору*

3. Які структурні підрозділи банку беруть участь у кредитному моніторингу:

а) кредитний відділ;

б) відділ маркетингу;

в) відділ безпеки;

г) юридичний відділ;

д) відділ банківських ризиків;

е) усі варіанти правильні?

4. Заходи кредитного моніторингу такі:

а) контроль за цільовим використанням кредиту;

б) контроль за виконанням графіка погашення кредиту і відсотків;

в) контроль за наявністю і станом предмета застави, поведінкою та станом гарантів (поручителів) і страховиків;

г) контроль за діяльністю партнерів (контрагентів) позичальника;

д) контроль за зв'язками позичальника;

е) усі варіанти правильні.

*Тести на встановлення відповідності*

5.1. Ознаки зношених банкнот такі:

5.2. Ознаки значно зношених банкнот такі:

а) банкноти без пошкоджень, але потерті;

б) банкноти, у будь-якому місці яких є плями, написи;

в) надірвані та надрізані банкноти, незалежно від розміру надриву;

г) банкноти із проколами й дірками, відірваними краями та кутами;

д) банкноти, розірвані й розрізані на дві частини або більше, крім розрізаних на вузькі смуги, та склеєні;

е) банкноти з утраченими частинами, якщо збереглось не менш ніж 55 % початкової площі;

є) банкноти, пошкоджені вогнем, водою, різними рідинами та хімікатами;

ж) банкноти, склеєні із двох половинок різних банкнот одного номіналу й дизайну.

6.1. Фальшиві банкноти й монети – це:

6.2. Перероблені банкноти – це:

а) банкноти, виготовлені будь-яким способом, включаючи промисловий, усупереч установленому законодавством порядку, які імітують (фальсифікують) платіжні банкноти й монети, виготовлені на замовлення НБУ і введені ним в обіг;

б) банкноти, на яких змінено шляхом наклеювання, малювання, друкування тексту і (або) цифр зображення, що визначають номінал, рік зразка (емісії), банк-емітент, інші реквізити, та їх за зовнішнім виглядом може бути сприйнято як справжні вищого номіналу або іншого року зразка.

# 9. Забезпечення безпеки в роботі з персоналом банківських установ

**Мета** – розглянути теоретичні засади та практичні аспекти забезпечення кадрової безпеки в банках.

**Ключові поняття:** електронні платежі, конфлікти, система технічного захисту інформації, недобросовісний клієнт, шахрай.

**Основні питання:**

9.1. Сутність кадрової безпеки банку та заходи щодо її забезпечення.

9.2. Психологія недобросовісного працівника, клієнта, шахрая.

9.3. Конфлікти, запобігання їм та вирішення їх.

**Література:** [8; 10; 11; 13; 21; 25].

## 9.1. Сутність кадрової безпеки банку та заходи щодо її забезпечення

**Кадрова безпека банку** – стан захищеності банку, що полягає в забезпеченні безпеки в роботі з персоналом, контролі за дотриманням банківської таємниці, запобіганні промисловому шпигунству, крадіжкам.

Функції щодо забезпечення кадрової безпеки виконує відділ безпеки спільно з відділом кадрів. Щодо питань відбору персоналу здійснює його, переважно, відділ кадрів. Проте особисті дані, їх достовірність перевіряє відділ безпеки.

*Принципи забезпечення кадрової безпеки:*

ефективність;

цілеспрямованість;

оперативність;

гнучкість;

індивідуальний підхід;

соціальна спрямованість.

У банківській сфері кадрові загрози є найбільш суттєвою причиною витоку інформації, промислового шпигунства. Виникнення кадрових ризиків у середовищі функціонування банку може спричинити й невизначеність. Імовірність настання цих ризиків збільшується у міру виникнення потенційних загроз та перетворення їх на реальні. Реальні загрози порушують безпеку, тобто спричиняють небезпеки й негативні наслідки (рис. 9.1).


Рис. 9.1. **Алгоритм причинно-наслідкових зв'язків виникнення загроз кадровій безпеці банку та їх негативних наслідків**

Виходячи зі згаданого алгоритму (див. рис. 9.1), обґрунтовано необхідність у створенні класифікації невизначеності, ризиків, загроз та негативних наслідків у сфері кадрової безпеки.

Класифікацію має бути побудовано з дотриманням найбільш важливих вимог. Серед них: багатокритеріальність, ієрархічність, повнота, чіткість, можливість практичного використання, зрозумілість. В основу побудови багатокритеріальної ієрархічної класифікації загроз кадровій безпеці покладено види невизначеності. **Невизначеність** – досить широке поняття, яке відображає об'єктивну неможливість здобуття абсолютного знання про внутрішні та зовнішні умови їх функціонування, неоднозначність параметрів.

Кадрову безпеку спрямовано, з одного боку, на мінімізацію загроз від персоналу, а з іншого – на сприяння високопродуктивній праці, про що і свідчить табл. 9.1.

Таблиця 9.1

## Багатокритеріальна ієрархічна класифікація кадрових ризиків та загроз кадровій безпеці банку

| Види невизначеності | Види кадрових ризиків та загроз за середовищем виникнення | Ознаки класифікації загроз кадровій безпеці | | | | | | Негативні наслідки кадрових загроз |
|---|---|---|---|---|---|---|---|---|
| | | за можливістю прогнозування | за ступенем об'єктивності | за рівнем керованості | за ймовірністю настання | за об'єктами виникнення | за змістом | |
| Недостовірність | внутрішні (виникають на індивідуальному та мікрорівні) | передбачувані | об'єктивні; суб'єктивні | керовані | потенційні | загрози пов'язані з: діями персоналу; утратою фінансових, матеріально-технічних, інформаційних ресурсів, інтелектуальної власності, програмного забезпечення, розголошенням банківських таємниць; перебоями у функціонуванні системи управління персоналом | шахрайство, фальсифікація і розтрати; змова з конкурентами, контрагентами; недобросовісність, невідповідна кваліфікація персоналу банку, незадоволеність працею та зумисне заподіяння шкоди, неякісний процес відбору персоналу та управління діловою кар'єрою, неефективна система мотивації, несприятливий мікроклімат у колективі, низький рівень управління персоналом банку | прямі збитки для банку, неналежне виконання посадових обов'язків, зниження прибутків банку, висока плинність кадрів |
| Невідомість | змішані (виникають на будь-якому рівні) | непередбачувані | | керовані | реальні | | крадіжки, хабарництво, несанкціонований доступ до інформації, витік інформації, співпраця персоналу з конкурентами | рейдерство, збитки, утрата власності, ресурсів, клієнтської бази, зниження рівня доходів |
| Неоднозначність | зовнішні (виникають на мезо-, макро- та мегарівнях) | непередбачувані | об'єктивні | некеровані | | | тиск на персонал сторонніх структур, конкурентів, банківське шпигунство; недобросовісна конкуренція; протиправні дії конкурентів; несприятлива соціально-економічна ситуація; нестабільність законодавчої бази, політичної ситуації | |

Напрями забезпечення кадрової безпеки розглядають в аспекті видів кадрової роботи (табл. 9.2).

Таблиця 9.2

**Напрями забезпечення кадрової безпеки банку**

| Напрями кадрової роботи | Напрями забезпечення кадрової безпеки |
|---|---|
| Відбір і найм персоналу | Недопущення проникнення в банк осіб, які є недобросовісними працівниками, промисловими шпигунами, мали судимість |
| Розміщення та ротація кадрів | Правильне формування колективів, урахування типів особистості персоналу |
| Соціальний контроль | Виявлення протиправних дій працівників через періодичну перевірку рівня життя окремих працівників банку, виявлення необґрунтованих змін у поведінці персоналу |
| Звільнення персоналу | З'ясування істинних мотивів звільнення; оформлення підписки про нерозголошення інформації з обмеженим доступом, із якою обізнана особа, що звільняється; забезпечення передачі справ |
| Мотивація персоналу | Забезпечення нормальних умов праці, сприяння вдосконаленню кваліфікації, забезпечення нормального рівня доходів, формування дієвої системи стимулювання персоналу, уведення валентної системи оплати праці в банку |
| Адаптація персоналу | Формування банківського патріотизму, причетності до корпоративної культури як сукупності методів впливу на свідомість, почуття, волю і характер працівників із метою формування в них усвідомленого бажання якісно і в мінімальні терміни виконувати свої функціональні обов'язки та працювати на користь банку |

За суб'єктами злочинних дій злочини банківського персоналу розподілено на вчинені: топ-менеджментом, працівниками бухгалтерії банків, іншими категоріями банківських працівників (табл. 9.3).

*Системні засоби протидії кадровим загрозам у банку:*

формування високого рівня інтелекту банківських працівників;

розвиток ефективної системи мотивації праці;

формування в персоналу корпоративної причетності та патріотизму;

профілактика конфліктів;

підвищення рівня задоволеності персоналу роботою в банку;

упровадження нематеріальної мотивації;

забезпечення відносно високого ступеня самостійності у виконанні роботи персоналом у поєднанні з дієвою системою контролю.

Таблиця 9.3

## Злочини, що здійснює банківський персонал у змові із клієнтами

| Види шахрайств | Характеристики шахрайств персоналу |
|---|---|
| Злочини топ-менеджменту банку | Використання фіктивного підприємництва, тобто реєстрація шляхом обману фіктивного підприємства без наміру здійснювати статутну діяльність із метою отримання банківських кредитів і позик для фінансування діяльності, не передбаченої статутом підприємства, звільнення від податків або іншого незаконного використання зазначених кредитів і позик |
| | Зловживання депозитним капіталом банку, тобто шахрайське отримання грошових коштів, залучених на банківські рахунки. Способи скоєння цих злочинів мають різний характер. Особливо небезпечними вони стають у тому разі, коли до них залучено велику кількість людей, а шкоду заподіяно зі згоди керуючого банку |
| Злочини працівників кредитного і вексельного відділів | Фіктивні кредити, незабезпечені позики підприємствам за фінансової зацікавленості керівників і службовців банку, позички під неадекватне або малоліквідне забезпечення; заниження сум грошових зборів, позичкових відсотків, знижок та збільшення сум виплати відсотків; заниження кредитових і завищення дебетових проведень за контрольним рахунком у загальній бухгалтерській книзі, продовження терміну платежу і збільшення комісійних зборів без відома клієнтів, несанкціоноване звільнення застави, незаконне привласнення облікових векселів, незаконне привласнення платежів за векселями; використання з корисливою метою векселів, на яких боржник проставляє бланковий індосамент і залишає для пролонгації терміну погашення кредиту; використання непоінформованості позичальника, що вже заплатив частину суми векселя, для того щоб примусити його оплатити повністю вексель; незаконне привласнення чекових сум, залишених боржником для сплати векселів після закінчення терміну. Підміна векселів, підписаних векселедавцями, що неспроможні забезпечити цей вексель та не мають векселя посадової особи; фіктивні проведення залишків банків-кореспондентів; завищення сум за документами, порівняно з фактично виконаними проведеннями; створення фіктивних рахунків у банках-кореспондентах |
| Злочини бухгалтерських співробітників | Показ неправильної суми проведень за дебетом і кредитом; нерівномірне списання з рахунків, коли працівник діє як особа, що має доручення; фіктивні вклади, рахунки на фіктивних осіб, фіктивні проведення за рахунками клієнтів, зарахування чеків працівників на рахунки клієнтів, вилучення і знищення чеків працівників до їх перенесення до бухгалтерської книги; нерівномірне зняття грошових сум із рахунків клієнтів, які тимчасово не використовують; незаконне присвоєння комісійних зборів, незаконне присвоєння вкладів, маніпуляції із відсотками за ощадними рахунками |

Ці заходи застосовують у процесі управління кадровою безпекою банку. Проте управління мають здійснювати на основі чіткої послідовності дій.

Під **управлінням кадровою безпекою банків** слід розуміти вибір і застосування інструментів, методів, засобів ефективного впливу та протидії загрозам кадрової безпеки в такому поєднанні, яке б забезпечувало максимальний результат за мінімальних витрат.

**Процес управління кадровою безпекою** – послідовність дій, що має бути виконано для формування управлінського впливу, який би забезпечував кадрову безпеку в банку.

Будь-який процес управління, у тому числі й кадровою безпекою, має будуватися на підставі системного підходу, що враховує всі аспекти й підсистеми кадрової безпеки. Водночас виникнення загроз кадрової безпеки має ситуаційний характер.

Ураховуючи ці фактори, доцільним буде побудова процесу управління кадровою безпекою банку на підставі раціонального поєднання системно й ситуаційно орієнтованого управління (рис. 9.2).

Етап визначення, перегляду елементів системи управління кадрової безпекою та забезпечення її функціонування відіграє концептуальну роль в організації управлінського процесу.

Під **системою управління кадровою безпекою банку** слід розуміти сукупність взаємопов'язаних і взаємодіючих підсистем, необхідних для виявлення, протидії кадровим загрозам і забезпечення ефективного перебігу трудових процесів.

Кожна підсистема управління кадровою безпекою забезпечує проходження певних етапів управління. Усі підсистеми взаємопов'язані між собою. Між ними існують як прямі, так і зворотні взаємозв'язки. Провідну роль відіграють організаційна підсистема і підсистема планування та контролю. Функціонування підсистем і сам процес управління повинні мати безперервний характер і відповідати вимогам ефективності.

До структури системи управління кадровою безпекою входять такі підсистеми:

організаційна;

оцінювання стану кадрової безпеки;

моніторингу та протидії загрозам кадровій безпеці банківської установи;

планування й контролю.

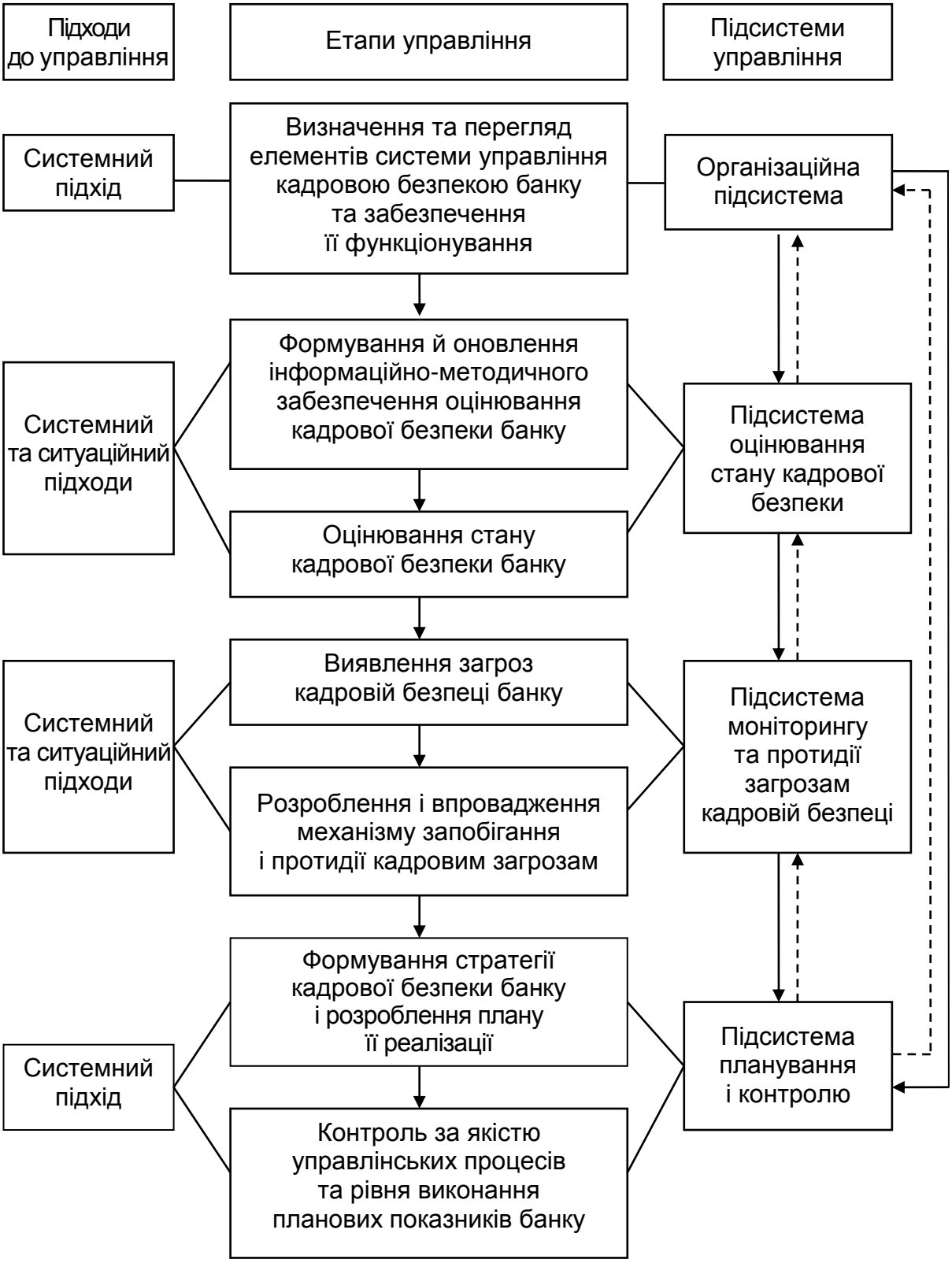


Рис. 9.2. **Процес управління кадровою безпекою банку**

Таким чином, кадрова безпека банку є передумовою забезпечення протидії загрозам усім іншим видам безпеки, а саме: фінансово-економічній, інформаційній, ринковій, силовій і правовій безпеці.

## 9.2. Психологія недобросовісного працівника, клієнта, шахрая

Першочерговим завданням безпеки банківської діяльності є запобігання неправомірним діям недобросовісних працівників, клієнтів чи взагалі шахраїв. Для вирішення цих завдань використовують виховну та профілактичну діяльність, яка містить сукупність методів впливу на свідомість, почуття, волю, характер працівників банку з метою формування в них уміння зберігати комерційну та банківську таємницю й точно дотримуватись установлених правил роботи в банку.

Особливу увагу має бути приділено відбору банківського персоналу з метою недопущення до роботи недобросовісних працівників.

*Етапи відбору банківського персоналу:*

1) визначення вимог для кожної категорії працівників до займаної посади. Вимоги до освіти та стажу роботи містяться у внутрішніх банківських посадових інструкціях. Основні критерії, якщо вони є, щодо віку, статі, сімейного стану, стажу роботи встановлює керівник, який приймає рішення про майбутнє зарахування працівника;

2) підбір персоналу. Кадрова служба, використовуючи різні способи пошуку персоналу (ЗМІ, Інтернет, рекрутингові агентства, служба зайнятості, знайомі) збирає резюме кандидатів на вакантну посаду. Із великої кількості резюме, що надішли до банку, відбирають ті, які відповідають сформульованим вимогам;

3) відбір персоналу. Етап полягає у проведенні співбесіди й перевірці службою безпеки даних про потенційного кандидата на вакантні посади. Цей етап погодження кандидатури умовно розподіляють на п'ять частин:

співбесіду з менеджером із персоналу (якщо банк має можливість, одночасно здійснюють психологічне оцінювання претендента);

співбесіду з особою, що перевіряє кваліфікацію претендента;

перевірку службою безпеки відомостей, наданих претендентом;

погодження кандидатури з відповідальним керівником банківської установи;

перевірку кандидата на наявність психічних захворювань шляхом обговорення економічних публікацій, роботи НБУ.

*Правила проведення ефективної співбесіди на заміщення вакантних посад у банку* такі:

недопустимість будь-якого вияву суб'єктивного ставлення до кандидата;

ретельне спостереження за поведінкою, хвилюваннями кандидата;

обов'язкова перевірка здатності кандидата працювати в команді;

обов'язкове оцінювання комунікабельності кандидата на вакантну посаду;

виявлення причин зміни місця роботи кандидатом;

перевірка інформації, викладеної в резюме;

оцінювання мотивації кандидата до отримання посади;

отримання письмової згоди кандидата на перевірку його особистої інформації, відеознімання співбесіди;

ретельна перевірка рівня кваліфікації кандидата шляхом формулювання тестових та практичних завдань;

оцінювання загального культурного та професійного рівня;

отримання відомостей про здатність кандидата на вакантну посаду зберігати комерційні таємниці;

повідомлення претендента на посаду про відмову йому у прийнятті на роботу. Формулювання та обґрунтування мають бути максимально нейтральними та вмотивованими.

*Функції відділу безпеки щодо виявлення недобросовісних кандидатів на вакантні посади:*

1) перевірка інформації, викладеної в резюме. У разі наведення претендентом на вакантну посаду відомостей, які свідчать про особливі досягнення під час навчання (наявність диплома з відзнакою, участь у конференціях, перемоги в конкурсах) або про інші успіхи кандидата, які не можуть бути підтверджені документально, цю інформацію перевіряють у відповідних установах та закладах. Відомості, наведені в резюме, звіряють із записами у трудовій книжці;

2) перевірка рекомендацій. Служба безпеки телефонує в організації, що надали рекомендації, і перевіряє їх справжність. У ході контакту з особою, що надала рекомендації, необхідно перевірити, яку посаду обіймає ця особа, скільки часу вона знайома з кандидатом, якого рекомендує. Це необхідно для перевірки правдивості та повноти відомостей, наведених у рекомендаціях чи резюме, а також перевірки повноважень особи надавати таку рекомендацію. Усю інформацію, отриману працівником служби безпеки під час перевірки рекомендацій, фіксують письмово. Якщо наданих відомостей недостатньо або вони не піддаються перевірці, треба зажадати додаткових рекомендацій від кандидата на посаду;

3) перевірка достовірності документів про освіту. Працівник служби безпеки перевіряє справжність наданих документів, фактично здійснює їх експертизу. У разі, коли виникають сумніви, він може зробити запит про справжність документа до органу, який його видав;

4) перевірка кандидата на вакантну посаду на наявність кримінального минулого. Ці відомості можна дізнатись від колишніх співробітників, сусідів, дільничних інспекторів міліції, друзів претендента;

5) перевірка інформації про причини звільнення кандидата на вакантну посаду. Служба безпеки має зателефонувати керівникам підприємств, на яких працював претендент, та перевірити правильність наданої інформації, уточнити причини звільнення з минулого місця роботи. Якщо особа претендує на відповідальну посаду, необхідно зустрітися з її колишніми керівниками та співробітниками, вислухати їхні думки про роботу цього працівника. Банк зацікавлений у нормальних відносинах та лояльності майбутнього працівника, тому має перевірити, наскільки коректно людина звільнялася з місць попередньої роботи, наскільки сумлінно виконувала зобов'язання щодо вирішення поточних справ та їх передавання. Недоцільно брати на роботу людину, що під час звільнення не закінчила справи чи забрала клієнтську базу, переманивши клієнтів;

6) збирання інформації про претендента на вакантну посаду як про особистість, яка має якісь слабкості, що можуть заважати успішному виконанню обов'язків та спонукати до правопорушень (схильність до азартних ігор, пияцтва, фінансових афер);

7) застосування "детектора брехні" (поліграфа) під час прийняття на роботу працівника, що можливе за згоди кандидата на вакантну посаду. Деякі банки мають таке обладнання та використовують його. Перевірку можна здійснювати в разі добровільної згоди кандидата. Поліграф тільки реєструє інформацію про стан людини в момент відповіді на поставлене запитання. Поліграф не може розрізняти, чим саме викликано хвилювання: неправильною відповіддю респондента чи негативними асоціаціями, які викликає запитання. За умови використання поліграфа треба мати кваліфікованого спеціаліста щодо роботи з ним.

*Заходи щодо забезпечення поточної боротьби з недобросовісними працівниками:*

1) організація "гарячої лінії". Гаряча лінія проти шахрайства дозволить збирати інформацію про факти правопорушень, що здійснює банківський персонал, як від їх колег, так і від клієнтів банку. Це ресурс, що є конфіденційним і нейтральним: приймання та опрацювання інформації здійснюють фахівці, які не працюють у банку й не пов'язані з його співробітниками;

2) періодичне використання поліграфа ("детектора брехні") щодо окремих працівників, яких підозрюють у промисловому шпигунстві чи крадіжках;

3) періодичне використання тестування *Midot* для виявлення серед співробітників банківської установи, які працюють і яких приймають на роботу, потенційної "зони ризику". В основі системи тесту рішень *Midot System* лежить алгоритм оцінювання не професійних, а етичних цінностей і моральних суджень особистості, що дає підстави прогнозувати тенденції в поведінці. *Midot System* дозволяє підвищити достовірність оцінювання кандидата на вакантну посаду та суттєво скоротити час та витрати на здійснення цього оцінювання. Якщо за результатами оцінювання кандидат порядний, чесний і надійний, є сенс продовжувати оцінювання його професійних і ділових якостей та співбесіду. Для застосування *Midot System* потрібно мати комп'ютер та Інтернет. Використовуючи індивідуальні паролі, працівник здобуває доступ до системи тестування в будь-якому місці. Це не забере багато часу: протягом 20 хвилин кандидатові буде поставлено 120 – 150 запитань, які формулюють індивідуально для кожного, кого тестують, виходячи з характеру та швидкості відповідей.

Контроль за лояльністю та якістю виконання функцій фахівців банку здійснюють із метою протидії їх співпраці з недобросовісними клієнтами та виявлення об'єктивного стану справ щодо якості, ефективності виконання ними функціональних завдань і своїх посадових обов'язків. Серед заходів контролю можуть застосовувати: перевірки відділу банківського нагляду, спостереження, тестування, опитування, застосування процедури "таємний клієнт".

## 9.3. Конфлікти, запобігання їм та вирішення їх

**Конфлікт у банківській сфері** – це зіткнення у процесі виконання трудових функцій протилежних інтересів, дій, думок, оцінок окремих працівників або їх груп виключно між собою чи за участю клієнтів та партнерів.

Конфлікт може мати місце в разі наявності конфліктної ситуації, яка в разі супроводу її інцидентами переходить у той чи інший вид конфлікту.

**Конфліктна ситуація в банківській сфері** – це накопичені суперечності, пов'язані із трудовою діяльністю персоналу чи поведінкою і вподобаннями клієнтів та контрагентів банку.

Переростання цієї суперечності в конфліктну ситуацію може відбутися за умови виникнення інциденту.

**Інцидент** – активізація діяльності одного із суб'єктів конфліктної ситуації або дії третьої сторони, що сприяють загостренню конфліктної ситуації.

*Суб'єктами конфлікту* виступає частина учасників конфліктної взаємодії, інтереси яких зачеплено. Це, наприклад, окремі особи (керівники, співробітники), групи, підрозділи, банку, що захищають свої особисті інтереси.

*Об'єкт конфлікту* – це те, на що претендує кожна з конфліктних сторін і спричиняє їхню протидію. Наприклад, ресурси, право власності, право приймати рішення, нова посада.

*Ознаки конфлікту:*

наявність конфліктної ситуації;

наявність та неподільність об'єкта конфлікту;

наявність причин і бажання в суб'єктів продовжувати конфліктне протистояння.

Функції конфліктів у банківській сфері наведено в табл. 9.4.

Таблиця 9.4

**Функції конфліктів у банківській сфері**

| Назви функцій | Характеристики |
|---|---|
| Виявлення недоліків у системі управління персоналом банку | Функція дозволяє окреслити напрями посилення кадрової безпеки в банку |
| Зняття напруженості | Унаслідок інцидентів у процесі конфлікту відбувається конфліктна взаємодія, що супроводжується бурхливими реакціями, які знімають в учасників емоційне напруження, приводять до зниження інтенсивності негативних емоцій |
| Розвиток соціальної та інноваційної активності банківського колективу | Конфлікти підтримують соціальну активність людей, сприяють запобіганню застою, слугують джерелом інновацій, формують мобільну структуру колективу |
| Згуртування колективу банку щодо боротьби із зовнішніми загрозами | Конфлікти допомагають визначити можливі осередки зовнішньої загрози (конкурентів, фінансово-кредитні організації, природні явища та ін.) і вчасно дати їм спільну відсіч |
| Активізація громадської свідомості персоналу банку | Дії конфліктних сторін стають предметом спостереження, обговорення значної частини колективу і, відповідно, сприяють виявленню об'єктивних причин конфлікту та прозорості громадської думки |
| Оцінювання та передбачення поведінки учасників конфлікту | Спостереження за перебігом конфлікту дозволяє прогнозувати дії суб'єктів та передбачати зміни в поведінці та структурі неформальних груп банківського персоналу |

*Причини конфліктів у банківській сфері:*

1) суб'єктивного характеру:

кар'єризм;

конфліктний характер у провідних фахівців;

розбіжності в інтересах, поглядах і сподіваннях персоналу;

неоднозначне трактування подій;

брак спілкування;

агресивність окремих членів колективу;

конфліктність та агресивність клієнтів;

підтримка керівництвом виявів заздрості та інтриг;

2) об'єктивного характеру:

непродумана кадрова політика;

авторитарний стиль управління;

необ'єктивне оцінювання результатів праці банківського персоналу;

непрозора кадрова політика з питань просування кадрів по службі;

необізнаність персоналу щодо загального стану справ у банку;

порушення правил ділової етики.

*Наслідки конфліктів у контексті забезпечення банківської безпеки:*

1) позитивні наслідки, що сприяють зміцненню банківської безпеки:

зняття напруги між суб'єктами конфлікту;

розуміння й передбачення можливостей і поведінки;

джерело інновацій, прогресу;

зростання співробітництва між частинами колективу;

виявлення проблем в організації управління та взаємодії персоналу;

2) негативні наслідки, що сприяють послабленню банківської безпеки:

емоційні, матеріальні втрати, утрати часу;

зростання плинності кадрів;

імовірність розголошення комерційної таємниці банку;

зростання незадоволеності персоналу роботою в банку;

погіршення соціально-психологічного клімату в колективі;

утрати робочого часу внаслідок захоплення конфліктами;

напружене ставлення до ідейних противників;

довготривале відновлення ділових відносин і рівноваги в колективі.

Методи запобігання конфліктам обирають, залежно від виду та характеру перебігу конфлікту.

*Класифікація конфліктів у банківській сфері:*

1) за ступенем охоплення:

внутрішньоособистісні;

міжособистісні;

міжгрупові;

комбіновані (між особистістю і групою персоналу);

2) за рівнем вияву:

відкриті (супроводжуються інцидентами);

приховані (характеризуються тільки наявністю конфлікної ситуації, яка ще не має зовнішнього вияву);

3) за середовищем виникнення:

внутрішні;

зовнішні;

змішані (виникають як у банку, так і поза його межами);

4) за суб'єктами:

трудові конфлікти;

управлінські конфлікти;

конфлікти персоналу із клієнтами;

конфлікти банку з партнерами й контрагентами;

5) за ступенем суб'єктивності:

об'єктивного характеру (такі, що мають об'єктивне підгрунтя, причину виникнення);

суб'єктивного характеру (виникають через незадоволеність окремих осіб, що грунтується лише на їх здогадках);

6) за ієрархією:

вертикальні (між керівництвом і підлеглими);

горизонтальні (між колегами);

змішані.

Вибір конкретних методів вирішення конфліктів залежить від ситуації, перебігу конфлікту та природи його виникнення. Методи управління конфліктами охарактеризовано в табл. 9.5.

Таблиця 9.5

**Методи вирішення конфліктів у банківських установах**

| Методи | Характеристики |
|---|---|
| 1 | 2 |
| Методи вирішення конфліктів (спільна діяльність учасників конфлікту, спрямована на припинення протидії та вирішення проблеми, яка призвела до зіткнення) | |

Закінчення табл. 9.2

| 1 | 2 |
|---|---|
| Загасання конфлікту | Тимчасове припинення протидії в разі збереження основних ознак конфлікту: суперечностей і напружених відносин. Загасання звичайно відбувається в результаті: утрати мотивації до протиборства (об'єкт конфлікту втратив свою актуальність); переорієнтації мотиву, перемикання на невідкладні справи; виснаження ресурсів, сил і можливостей для боротьби |
| Переростання в інший конфлікт | У відносинах сторін виникає нова, більш значуща суперечність і відбувається зміна об'єкта конфлікту |
| Міжособистісні методи | *Конкуренція.* Одна зі сторін конфлікту намагається задовольнити власні інтереси, не зважаючи на інтереси іншої сторони та змушуючи її приймати запропоновані рішення |
| | *Ухиляння.* Використовують тоді, коли одна зі сторін уважає, що проблема не має для неї важливого значення, а вирішення її потребує значних зусиль |
| | *Пристосування.* Означає, що одна зі сторін конфлікту не намагається відстоювати власні інтереси та взаємодіє з іншою стороною, оскільки для останньої ці інтереси важливіші або вона має більшу владу |
| | *Компроміс.* Обидві сторони конфлікту трохи поступаються власними інтересами, щоб частково їх задовольнити та спільно вирішити |
| | *Співробітництво.* Кожна зі сторін конфлікту, відстоюючи власні інтереси, намагається враховувати інтереси опонента. Спільні рішення виробляють у ході переговорів |
| Методи врегулювання конфліктів (усунення конфліктної ситуації за участю третьої сторони) | |
| Припинення конфліктної взаємодії | Зміна посади чи схеми взаємодії між персоналом, що перебувають у стані конфлікту. Такі заходи дозволяють відволікти персонал від предмета конфлікту |
| Усунення конфлікту | Ліквідація структурних елементів конфліктів шляхом: вилучення із протиборства одного з опонентів (переведення до іншого відділу, філії; звільнення з роботи); виключення взаємодії опонентів на тривалий час (відправлення у відрядження одного або обох та ін.); усунення об'єкта конфлікту (позбавлення тих, хто конфліктує, можливості мати доступ до об'єкта конфлікту) |
| Переростання в інший конфлікт | У відносинах сторін виникає нова, більш значуща суперечність і відбувається зміна об'єкта конфлікту |

*Заходи щодо запобігання конфліктам у банківській сфері:*

поліпшення умов праці;

оцінювання морально-психологічного клімату в колективі;

удосконалення організації оплати праці;

контроль за дотриманням правил ділової етики;

урахування очікувань і сподівань персоналу;

урахування типів особистості персоналу;

індивідуальний підхід до формування колективів;

діагностика сумісності персоналу з корпоративною культурою банку;

переформатування колективів на стадії зародження конфліктів;

поважне, шанобливе ставлення керівництва до підлеглих.

**Практичне заняття**

Ділова гра *"Вирішення конфліктних ситуацій у системі фінансово-економічної безпеки банківських установ".*

Гра полягає у вирішенні конфліктної ситуації. Для цього студентів розподіляють на групи з кількістю учасників, згідно з умовами гри. Кожна група отримує умови конфліктної ситуації, обговорює ситуацію та розробляє рекомендації щодо її вирішення.

**Ситуація 1.** У грі беруть участь 1 керівник і 1 підлеглий.

*Керівник кредитного відділу.* Підлеглий не вийшов учора на роботу, він зателефонував уранці секретареві та сказав, що в нього раптово заболів зуб і він пішов до стоматолога. У вас невеликий підрозділ із шести осіб, ви працюєте всі разом близько року. Начальником ви стали близько трьох тижнів тому. *Мета керівника* – вирішити дисциплінарне питання, щоб у подальшому не виникало подібних прецедентів, а також чітко визначити свою позицію та статус.

*Підлеглий.* У вас вчора зламалася коронка, ви подзвонили на роботу й повідомили секретареві, що не прийдете. Сьогодні, прийшовши на роботу, ви отримали поштою повідомлення із проханням зайти до начальника. Ви пропрацювали разом із вашим новим начальником близько року, у підрозділі шість осіб. Він став начальником близько трьох тижнів тому і поки що його співробітники сприймають просто номінально.

**Ситуація 2.** У грі беруть участь 1 керівник і 5 підлеглих.

*Керівник.* Це ваш перший день роботи в банку на посаді керівника. У відділі фінансового моніторингу у вас п'ять підлеглих, ви припускаєте, що хтось із них може претендувати на вашу позицію, але не знаєте, хто саме. *Мета керівника* – відрекомендуватися, визначити свою позицію та статус.

**Ситуація 3.** У грі беруть участь 1 керівник і 4 підлеглих.

*Керівник.* Вас призначено управляти новим сектором у банку, вам підпорядковано четверо осіб. Із двома підлеглими ви пропрацювали разом на рівнозначних позиціях близько півроку, із третім – разом навчалися в інституті, четвертого – ніколи не бачили. Сьогодні ви призначили нараду, щоб обговорити найбільш загальні питання роботи. *Мета керівника* – відрекомендуватися, визначити свою позицію та статус.

**Ситуація 4.** У грі беруть участь 1 керівник і 5 підлеглих.

*Керівник.* Ви начальник відділу, у якому три підрозділи. Ви сприймаєте свій відділ як ефективний і дружній колектив. Ви зібрали один із підрозділів із п'яти осіб, начальник якого раптово для всіх перейшов на роботу до іншого банку, для того щоб повідомити їх, що ви прийняли рішення запросити на роль нового начальника підрозділу нового співробітника і завтра він виходить на роботу. Ви розумієте, що деякі співробітники могли претендувати на те, щоб посісти це місце, і всі співробітники чекали, що ви приймете рішення, радячись із ними. *Мета керівника* – призначити нового начальника підрозділу.

**Ситуація 5.** *Керівник.* Ви зібрали всіх співробітників, щоб повідомити їх про те, що вводиться нова форма одягу. Надалі ви хотіли б використовувати цю зустріч для розмови про зовнішній вигляд співробітників, щодо якого було дуже багато нарікань із боку вашого начальства, і ви самі не цілком задоволені тим, який вигляд мають ваші співробітники. Для вас це одна з найбільш болючих тем, оскільки на будь-які ваші спроби сказати що-небудь щодо пом'ятої спідниці, розпущеного волосся або банних капців, ви завжди отримували розгорнені пояснення про несправні праски, шпильки, що ламаються, хворі ноги та в результаті про мізерну зарплату, яку отримують офіціанти. У таких ситуаціях ви й не намагаєтеся заперечити, і цілий день потім переживаєте. *Мета керівника* – увійти в контакт, визначити свою позицію та статус.

**Ситуація 6.** *Керівник.* Ви зібрали співробітників для того, щоб поговорити про час приходу на роботу. Робочий день у банку починається о 9:00, і, відповідно, співробітникам необхідно приходити мінімум за 15 хвилин до початку робочого дня. Сьогодні в банк на 9:00 приходить зазвичай одна людина, а на 9:30 – 10:00 приходить решта всіх співробітників. За будь-яких ваших спробах почати розмову на цю тему співробітники завжди вам пояснюють, що перші відвідувачі, переважно, з'являються не раніше від 10 ранку. А якщо хто і прийде о 9:00, то, з одного боку, й один

співробітник із цим упорається, а з іншого – відвідувач розуміє, що банк тільки відчинився і йому, можливо, доведеться почекати. *Мета керівника* – увійти в контакт, визначити свою позицію та статус [13].

*Ситуаційні вправи з вивчення психології недобросовісного працівника, клієнта та шахрая:*

1. У відділі обслуговування карткових рахунків клієнтів старший економіст Петров І. І. завжди завантажений роботою. Він постійно розробляє нові банківські продукти. Протягом трьох років не був у відпустці. Нікого не допускає до своєї роботи, посилаючись на те, що клієнти так активно можуть працювати тільки з ним. Співробітники банку підозрюють, що Петров живе не тільки на заробітну плату. Яким чином можна перевірити інформацію про співробітника банку, уникнувши розголосу серед клієнтів?

2. Ви новачок у банку. Керівництво призначило вам наставника. Проте ви не знаходите спільної мови з наставником. Розуміючи, що він не хоче ділитися знаннями й досвідом, ви нервуєте та приймаєте рішення звільнитися. Оскільки, імовірніше за все, ви як молодий фахівець банку, випробувальний термін не пройдете. Як будете діяти в такій ситуації? Яким чином можна запобігти звільненню і як поводитися молодому фахівцю, щоб успішно пройти випробувальний термін?

3. Ви працюєте на посаді керівника структурного підрозділу банку. Один із ваших підлеглих постійно спізнюється на роботу. Ви як керівник призначили дисциплінарну бесіду. Проте, маючи намір серйозно поговорити з підлеглим, ви самі спізнилися. Яким чином слід побудувати бесіду, аби досягти бажаного результату й не скомпрометувати себе як керівника?

## Тематика доповідей

1. Засоби боротьби із шахрайством клієнтів.
2. Засоби протидії конфліктам.
3. Призначення та переваги користування послугами Бюро кредитних історій.

## Методичні рекомендації щодо виконання самостійної роботи

Теоретичні питання та тестові завдання опрацьовують на основі літературних джерел: [8; 10; 11; 13; 21; 25].

## Контрольні запитання

1. Яким чином здійснюють підбір персоналу на вакантні посади в банках?

2. Що становить психологія недобросовісного працівника, клієнта, шахрая?

3. Які існують види конфліктів?

4. Назвати способи запобігання конфліктам у банках.

5. Охарактеризувати можливі шляхи вирішення конфліктів у банках.

6. Назвати етапи додаткової підготовки прийнятих на роботу нових працівників банку.

7. Перелічити правила роботи з банківським персоналом.

8. Що таке "обґрунтування злочину"?

9. Пояснити сутність обґрунтування наслідків злочину.

10. Назвати та охарактеризувати типи шахраїв.

## Тести

*Тести одиничного вибору*

1. До причин конфліктів, обумовлених непродуманою кадровою політикою, не належить:

а) відсутність демократичних засад у колективах;

б) неадекватне оцінювання роботи працівників;

в) необґрунтоване просування по службі;

г) значна собівартість продукції;

д) відсутність гласності;

е) несприятливі умови праці, недоліки в її організації.

2. Назвати метод, що не належить до методів перевірки кандидатів на вакантну посаду:

а) перевірка минулого досвіду та досягнень;

б) самооцінювання;

в) оцінювання професійних якостей;

г) психологічне та професійне тестування;

д) анкетування;

е) власний варіант відповіді.

*Тести множинного вибору*

3. Причини конфліктів, обумовлені особливостями характеру людей:

а) брак спілкування;

б) різниця у планах, оцінках, інтересах;

в) різниця в поглядах;

г) неоднозначне трактування вчинків і поглядів;

д) егоїзм, відсутність почуття співпереживання, заздрість;

е) прагнення до переваг.

4. Заходи щодо створення організаційної причетності до банку такі:

а) створення сприятливих умов праці, просування по службі;

б) уведення валентної системи оплати праці;

в) уведення розвинутої системи стимулювання праці;

г) заохочення банківських династій, забезпечення довгостроковою роботою кожного працівника;

д) підтримка високого морального й ділового клімату в колективах установ банку;

е) надання необхідно можливого ступеня самостійності й довіри працівникам банку;

є) усі варіанти правильні.

*Тести на встановлення відповідності*

5.1. Джерела підбору персоналу такі:

5.2. Критерії підбору персоналу такі:

а) вищі навчальні заклади;

б) служба зайнятості;

в) кадровий резерв;

г) ринок праці;

д) освіта;

е) кримінальне минуле;

є) досвід роботи.

6.1. Спостереження – це:

6.2. Самооцінка – це:

6.3. Психологічне тестування – це:

а) особистий опис кандидатом на вакантну посаду своїх досягнень і невдач;

б) оцінювання рівня конфліктності, комунікабельності, схильності до правопорушень;

в) контроль за якістю виконання своїх обов'язків у період проходження випробувального терміну.

# 10. Безпека комп'ютерних технологій і систем у банківських установах

**Мета** – проаналізувати досвід організації комп'ютерних технологій і систем у банківських установах.

**Ключові поняття:** інформація, технічний захист інформації, система технічного захисту інформації, безпека електронних платежів.

**Основні питання:**

10.1. Система технічного захисту інформації банків.

10.2. Забезпечення безпеки електронних платежів.

**Література:** [10; 13; 17; 21; 28; 29].

## 10.1. Система технічного захисту інформації банків

В умовах динамічного середовища функціонування банківських установ особливого значення набувають системи технічного захисту інформації.

**Технічні заходи банківської безпеки** – це спрямовані на захист інформації заходи, здійснення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень у сфері банківської безпеки.

*До структури системи технічного захисту інформації* входять:

об'єкти захисту;

криптографічна підсистема захисту;

підсистема захисту від несанкціонованого доступу.

*Основними об'єктами захисту інформації* є:

технічні та комп'ютерні засоби збирання, опрацювання та зберігання інформації;

програмні засоби та бази даних, що використовують у процесі збирання, опрацювання та використання інформації;

інформація з обмеженим доступом, тобто інформаційні ресурси, зокрема, ті, що містять відомості, які належать або до таємної, або конфіденційної інформації;

допоміжні технічні засоби та прилади (засоби зв'язку, звукосупровід, переговорні й телевізійні пристрої, копіювальна техніка, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, енергопобутові прилади тощо, а також самі приміщення, де циркулює інформація.

Підсистему захисту від несанкціонованого доступу будують на засадах підбору системи технічних заходів, призначених для закриття каналів витоку інформації. Серед них виділяють:

1) технічні заходи з використанням таких пасивних методів, як:

контроль за доступом на об'єкти й у приміщення і його обмеження;

локалізація випромінювання через екранування, заземлення, звукоізоляцію;

блокування сигналів, що можуть виходити за межі банку через системи опалення, водозабезпечення і каналізації;

установлення автономних або стабілізованих пристроїв електроживлення;

2) технічні заходи з використанням таких активних методів, як:

просторове зашумлення з використанням генераторів шуму, акустичних і вібраційних завад, шумотронів;

лінійне зашумлення мереж електроживлення та кіл заземлення сторонніх дротів та з'єднувальних ліній, що виходять за межі банку;

знешкодження під'єднаних до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів "жучків").

**Криптографічна підсистема захисту** полягає в контролі за інформаційними потоками шляхом шифрування інформації.

Криптосистеми вирішують такі завдання у сфері інформаційної безпеки:

забезпечення конфіденційності, цілісності даних;

автентифікацію даних і їх джерел.

Криптографічні методи захисту є гарантією безпечних інформаційних систем. Особливого значення криптографічні методи набули з розвитком розподілених відкритих мереж, у яких немає можливості забезпечити фізичний захист каналів зв'язку. Найнадійніший технічний метод захисту інформації заснований на використанні криптосистем.

Криптографічна система містить:

алгоритм шифрування;

набір ключів (послідовність двійкових чисел), використовуваних для шифрування;

система управління ключами.

Схема роботи криптосистеми полягає в перетворенні тексту на шифротекст за допомогою алгоритму шифрування та ключів і у зворотному напрямі після передачі зашифрованої інформації.

Класифікацію систем шифрування наведено в табл. 10.1.

Таблиця 10.1

**Класифікація систем шифрування банківської інформації**

| Системи шифрування | Характеристики |
|---|---|
| Спосіб шифрування | |
| Системи "прозорого" шифрування | Криптографічні перетворення здійснюють у режимі реального часу, непомітно для користувача |
| Спеціальні системи для шифрування | Програми, які необхідно спеціально викликати для виконання шифрування банківської інформації |
| Ступінь охоплення інформації | |
| Канальне шифрування | Захищають всю інформацію, що передають по каналу зв'язку, включаючи службову. Цей спосіб дозволяє досягти вбудовування процедур шифрування на канальний рівень і дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи захисту банківської інформації |
| Кінцеве (абонентське) шифрування | Дозволяє забезпечити конфіденційність даних, переданих між двома абонентами. У цьому разі захищають тільки зміст повідомлень, усю службову банківську інформацію залишають відкритою |
| Кількість використовуваних ключів | |
| Симетричні системи | Використовують один і той же секретний ключ як шифратор і дешифратор інформації банку. Недолік цього методу полягає в тому, що ключ має бути відомий і відправнику, і отримувачу |
| Асиметричні системи | Використовують два взаємопов'язаних ключі: для шифрування й розшифрування. Один ключ є закритим і відомим лише отримувачу. Другий ключ є відкритим, тобто він може бути загальнодоступним для мережі й опублікованим разом із адресою користувача |

Для контролю за електронними платежами використовують асиметричні системи захисту інформації у вигляді електронного цифрового підпису (ЕПЦ). Його реалізують із використанням методу шифрування з відкритим ключем. Відправник формує цифровий підпис, використовуючи секретний ключ відправника. Отримувач перевіряє підпис, використовуючи відкритий ключ відправника.

Сутність технології електронного підпису полягає в такому: 1) відправник передає два примірники одного повідомлення: відкрите й розшифроване його закритим ключем (тобто зворотне шифрування); 2) отримувач шифрує за допомогою відкритого ключа відправника розшифрований екземпляр; 3) якщо він збігається з відкритим варіантом, то особистість і підпис відправника вважають установленими. У процесі використання ЕЦП шифрують не всі повідомлення, а лише спеціальну контрольну суму (хеш), що захищає послання від нелегальної зміни. ЕЦП використовують із метою перевірки цілісності повідомлення, він засвідчує особу відправника.

Схоронність криптографічних ключів є запорукою безпеки електронних ключів. У разі витоку інформації про криптографічні ключі зловмисник може заволодіти ключовою інформацією та здобути повний доступ до всієї інформації в системі або мережі. Розрізняють такі функції управління ключами: генерацію, зберігання й розподіл ключів (табл. 10.2).

Таблиця 10.2

**Функції управління криптографічними ключами**

| Функції | Характеристики |
|---|---|
| Генерація ключів | Для генерації ключів симетричних криптосистем використовують апаратні та програмні засоби генерації випадкових чисел. Генерація ключів для асиметричних криптосистем більш складна, оскільки ключі мають певні математичні властивості |
| Зберігання ключів | Організація безпечного зберігання, обліку та видалення інформації про криптографічні ключі. Для цього застосовують їх додаткове шифрування за допомогою інших ключів |
| Розподіл ключів | Виконують на основі принципів оперативності, точності, конфіденційності. Між користувачами мережі ключі розподіляють двома способами: за допомогою прямого обміну сеансовими ключами; використовуючи один або декілька центрів розподілу ключів |

В Україні існує затверджений перелік сертифікованих засобів криптографічного захисту інформації. Серед цих засобів:

програмний виріб *NovaLib* (Бібліотеки функцій криптографічних перетворень);

програмний виріб "Шифр" (Бібліотеки функцій криптографічних перетворень. Версія 1.0);

програмний виріб "Шифр+" (Бібліотеки функцій криптографічних перетворень. Версія 1.0);

програмне забезпечення апаратно-програмних засобів електронного цифрового підпису "Основа";

засіб апаратно-програмний криптографічного захисту інформації "Старт".

## 10.2. Забезпечення безпеки електронних платежів

Для запобігання загрозам безпеці електронних платежів можна використовувати програмне забезпечення, що належить до категорії засобів пошуку "зламування" мереж, а саме:

*Internet Security Scanner* (фірма *Internet Security Systems*).

*NetRecon* (фірма *Axent*).

*NetProbe* (фірма *Qualix*).

*Ballista* (фірма *Secure Networks*).

*NetGuard* (фірма *Network Guardians*).

*NetSonar* (фірма *WheelGroup*).

У межах забезпечення інформаційної безпеки вітчизняні комерційні банки України виступають, переважно, споживачами спеціального банківського програмного забезпечення іноземного виробництва:

1) комплексну безпеку корпоративних мереж забезпечують програмні продукти VPN ЗАСТАВА 3.3, створені компанією "ЭЛВИС-ПЛЮС";

2) криптографічний захист "Крипто Про CSP", розроблена компанією "Крипто Про", допомагає ефективно перевіряти електронний цифровий підпис;

3) фінансову безпеку кредиторів забезпечує система A2 AGRUS APPLICATION, створена компанією "Агрус MGS";

4) комплекс "Банк – Доступ" забезпечує централізоване управління, розподіляючи доступ до інформаційних ресурсів;

5) комплекс "Банк – Активний Захист", розроблений фірмою "Андек", використовують для ліквідації наслідків атак хакерів, якщо їм таки вдалося прорвати інформаційний захист.

Забезпечення безпеки електронних платежів здійснюють перш за все щодо учасників карткових операцій та електронних платежів.

Система захисту має містити захист абсолютно всіх учасників карткових операцій: власників карток, банків, платіжних організацій.

*Етапи забезпечення безпеки карткових операцій* містять:

налагодження взаємодії із правоохоронними органами Українською міжбанківською асоціацією членів *EuroPay International* (ЕМА), банківськими установами з питань ризиків, які виникають у картковому бізнесі, іншими організаціями щодо безпеки карткових проектів;

ставлення завдань захисту карткових проектів;

організацію ідентифікації клієнтів карткових проектів;

упровадження програм протидії шахрайству;

моніторинг карткових операцій у режимі реального часу;

забезпечення конфіденційності операцій на карткових рахунках;

контроль за роботою персоналу задля оперативного виявлення чи недопущення шахрайства;

участь у проведенні розслідувань банківських шахрайств із картковими рахунками.

Найбільш поширені *види шахрайств із картковими рахунками такі:*

виготовлення та використання фальшивих банківських карток;

користування вкраденими картками;

злочинні дії персоналу банку щодо списання коштів із карткових рахунків клієнтів;

підроблення платіжних документів установами-отримувачами платежу.

Інформаційна безпека систем Інтернет-банкінг містить два основних *напрями інформаційної безпеки:*

безпеку в системі дистанційного банківського обслуговування (ДБО);

загальну інформаційну безпеку банку.

*Захист систем ДБО* має містити:

однозначну ідентифікацію суб'єктів, що взаємодіють із системою (клієнта й банку);

шифрування переданої фінансової інформації;

безпеку каналів передачі інформації, захист носіїв інформації.

Часто в системі Інтернет-банкінг самі клієнти допускають суттєві помилки, а саме:

1) небажане списання коштів через Інтернет-банкінг, що може статися, якщо користувач сам неправильно ввів дані для відправлення грошей;

2) якщо клієнт під час відправлення переказу через Інтернет-банкінг допустив помилку в номері рахунка, то процедура повернення платежу нічим не відрізняється від відправлення під час відвідування банку;

3) технічні перебої під час виконання операції з переказу грошей;

4) пересилання паролів на неправильний номер телефона.

Вирішення цих проблем забезпечено професійними засобами захисту, які використовують як у західних, так і вітчизняних системах ДБО. Заходи забезпечення безпеки в системі Інтернет-банкінгу наведено в табл. 10.3.

Таблиця 10.3

**Заходи забезпечення безпеки в системі Інтернет-банкінгу**

| Заходи | Характеристики |
|---|---|
| 1 | 2 |
| Створення безпечного середовища функціонування ДБО на боці клієнтів | Ніякі зміни в робочому коді середовища і його налаштуваннях, що виникли у процесі функціонування системи, не мають зберігати під час вимикання системи. У цьому разі, навіть якщо зловмисник і отримає якимось чином віддалений доступ до цього середовища у процесі його функціонування, він не зможе оволодіти ним на постійній основі |
| Створення захищеного від несанкціонованого доступу каналу передачі інформації між клієнтом і банком | Використовують механізм криптографічної автентифікації сторін – для забезпечення захищеної взаємодії через *Internet.* Забезпечення криптографічної автентифікації сторін досягають унаслідок використання захищеного протоколу під час установлення з'єднання між *Web*-сервером банку і клієнтом. Для підтвердження справжності *Web*-сервера здійснюють порівняння доменного імені сайта банку, що завантажують, із указаним у сертифікаті *Web*-сервера |
| Забезпечення безпеки банківських серверів, що обслуговують | Сервери системи Інтернет-банкінгу, переважно, розміщують в окремому мережному сегменті з доступом із мережі *Internet*, що контролюють на міжмережному екрані *(Firewall),* із внутрішньої захищеної мережі банку |
| Забезпечення умов, що не допускають розкрадання ключів і паролів, застосовуваних для роботи в системі ДБО | Цю умову має виконувати як банк, так і клієнти. Повернення коштів у разі користування паролями шахраїв майже неможливе |

Закінчення табл. 10.3

| 1 | 2 |
|---|---|
| Використання електронного цифрового підпису (ЕЦП) | Електронний цифровий підпис під електронними документами слід використовувати для забезпечення цілісності та автентичності (підтвердження авторства) інформації. ЕЦП клієнта використовують як аналог особистого підпису. Банки мають вести контрольні архіви, у яких зберігають усі електронні документи з ЕЦП для вирішення конфліктів |
| Шифрування даних | Слід використовувати для забезпечення конфіденційності інформації, що передають через *Internet.* Шифрування інформації здійснюють за допомогою сесійних ключів, що генерують на етапі встановлення з'єднання між клієнтом і сервером застосувань |

В Інтернет-банкінгу ведуть історію документів: ким і коли документ був створений, відредагований, підписаний, виконаний або відхилений, також журнали обліку доступу клієнтів до всіх сервісів, у яких зберігають інформацію про IP-адресу клієнта, час доступу, ідентифікатор ключа ЕЦП, що був використаний, виконані операції тощо. Під час упровадження системи в банку здійснюють ретельне налагодження операційних систем на серверах Інтернет-банкінгу, вилучають підтримку протоколів, що не використовують, мережних сервісів та служб. Повністю виключено мережний доступ до файлової системи, залучено вбудовані в ОС механізми аудиту.

Для захисту системи Інтернет-банкінгу провідні вітчизняні банки використовують: одноразові СМС-паролі; зовнішні електронні ключі; одноразові паролі, що отримують у банкоматі; віртуальну клавіатуру; електронний цифровий підпис.

## Семінарське заняття

1. Структура системи технічного захисту інформації банків.
2. Механізм забезпечення безпеки електронних платежів.
3. Організація безпеки комп'ютерних технологій.

## Тематика доповідей

1. Методи перевірки кандидатів на вакантну посаду.
2. Види захисту інформації.
3. Програмне забезпечення, що використовують в обліку банківських установ.

## Практичні завдання для самостійного виконання

1. Ви працюєте в операційному підрозділі банку, здійснюєте обслуговування рахунків працівників великої корпорації. Ваш колега говорить, що знає всіх цих працівників і впевнений у тому, що свої рахунки вони не контролюють. Тому можна впевнено списувати невеликими сумами кошти із цих карткових рахунків на фіктивний рахунок. Але для цього ви маєте дозволити йому заходити до банківської мережі в операційний день під вашим іменем. Які ваші дії в такій ситуації? Як запобігти незаконним діям працівника?

2. Вийшовши з кабінету за викликом керівника, ви залишили свій телефон. Коли ви повернулися, то ваш колега телефонував комусь із вашого телефона. До того ж ви помітили, що ваш колега заходив із вашого комп'ютера до облікової програми банку. Проте ніяких операцій не здійснював. Після цього випадку ви помітили, що ваш телефон прослуховують. Чи винні ви в тому, що сталося? Як ви будете протидіяти колезі? Чи можливим буде уникнення неправомірного прослуховування вашого телефонного апарата?

3. Під час здійснення банківської операції ви помітили, що до банківської інформації здійснено несанкціонований доступ. Ви не розумієте, чим це може закінчитися для банку і вас особисто. Які ваші дії в цій ситуації? До кого слід звернутися? І яким чином можна запобігти незаконному доступу до інформації?

## Методичні рекомендації щодо виконання самостійної роботи

Практичні завдання виконують після опрацювання джерела [13].

Теоретичні питання опрацьовують на основі літературних джерел: [10; 13; 17; 21; 28; 29].

## Контрольні запитання

1. Охарактеризувати комплекс заходів щодо забезпечення безпеки електронних платежів.

2. Що таке "система технічного захисту інформації банків"?

3. Описати структуру системи технічного захисту інформації банків.

4. Що таке "підсистема захисту від несанкціонованого доступу до інформації"?

5. Дати визначення поняття "система забезпечення безпеки даних".

## Тести

*Тести одиничного вибору*

1. До функцій підсистеми захисту від несанкціонованого доступу до інформації не належить такий:

а) ідентифікація користувачів;

б) автентифікація ресурсів інформаційної системи;

в) розмежування доступу до інформаційних ресурсів;

г) опрацювання інформації;

д) власний варіант відповіді.

2. До правил грамотної експлуатації засобів комп'ютерної техніки не належить таке твердження:

а) дотримуватись технологічного процесу роботи у прийнятій банком системі електронних платежів, згідно з відповідними технологічними інструкціями;

б) не розголошувати та не передавати свого пароля в системах іншим службовцям банку або стороннім особам;

в) не допускати до роботи в системах інших осіб під своїм паролем;

г) терміново повідомляти керівника підрозділу та підрозділ безпеки банківської діяльності про допущені чи виявлені порушення технологічного процесу, що виникли з вини службовця або через незалежні від нього причини;

д) не обговорювати ні з ким та не розкривати зміст інформації, що передають у системі електронних платежів;

е) обговорювати особливості використання комп'ютерних технологій у банку із друзями та родичами.

*Тести множинного вибору*

3. Заходи щодо забезпечення безпеки електронних платежів такі:

а) управління ключовою системою;

б) електронний підпис документів;

в) шифрування повідомлень у разі передавання по каналах зв'язку;

г) розмежування повноважень під час роботи з електронними документами;

д) захист на рівні протоколів зв'язку;

е) захист архівів від руйнування;

є) організаційні заходи.

4. Структурою підсистеми нормативно-правового забезпечення є:

а) комплекс організаційних заходів;

б) комплект документів, які визначають порядок роботи із засобами захисту інформації та регулюють інформаційні процеси банківського виробництва;

в) комплект документів, які визначають права та відповідальність посадових осіб під час роботи із засобами інформатизації;

г) власний варіант відповіді.

*Тести на встановлення відповідності*

5.1. Підсистемами технічного захисту інформації є:

5.2. Криптографічною підсистемою захисту інформації є:

а) криптографічна;

б) підсистема захисту від несанкціонованого доступу до інформації;

в) управлінська;

г) організаційна;

д) нормативно-правова;

е) підсистема, що забезпечує захист інформації на прикладному й мережному рівнях.

6.1. Підсистемою захисту інформації від несанкціонованого доступу є:

6.2. Підсистемою управління технічним захистом інформації є:

а) розмежування повноважень, контролю за доступом до інформації та комп'ютерних програм і технологій;

б) управління ключовими даними криптографічної підсистеми, контроль за системами захисту та їх діагностика.

.

# Глосарій

**Актив банку –** це будь-який об'єкт бухгалтерського обліку, право контролю за яким закріплено за банком і який дає дохід банківській установі або може бути обміняний на інший об'єкт, котрий, у свою чергу, даватиме дохід банківській установі.

**Активні операції банків** – це операції з розміщення коштів із метою отримання доходу.

**Аудит банку** – це визначення стану банку на основі перевірки правильності складання та підтвердження достовірності балансу, обліку прибутків та збитків, аналізу стану обліку, відповідність обліку та дій банку вимогам чинного законодавства, дотримання рівності прав акціонерів (учасників) під час розподілу дивідендів, голосування, надання прав на придбання нових акцій тощо та підготовка висновків для надання інформації керівництву, акціонерам (учасникам) банку та іншим користувачам.

**Банківська таємниця** – будь-яка інформація, що стосується клієнта, якою банк володіє на законних підставах (за винятком, якщо така інформація становить державну таємницю), тобто інформація про діяльність і фінансовий стан клієнта, що стала відома банку у процесі його обслуговування та взаємовідносин із ним або із третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

**Безпека банківської установи** – стан захищеності банку, за якого забезпечено реалізацію стратегічних цілей і поточних завдань банку, захист від внутрішніх і зовнішніх загроз.

**Взаємодія** – погоджені дії для досягнення максимального ефекту отримання вигоди та прибутку.

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

**Відсоткові витрати банку** – це витрати за коштами, отриманими від банків і клієнтів, за випуском цінних паперів як боргових зобов'язань.

**Відсоткові доходи банку** – це доходи від коштів, розміщених в інших банках, плати за надані кредити, доходи від інвестиційних цінних паперів.

**Внутрішньооб'єктовий режим охорони** – режим, що передбачає створення відповідної системи заходів і правил, спрямованих на забезпечення схоронності матеріальних цінностей банку, його інформаційних ресурсів, особистої безпеки працівників банку, його клієнтів, аварійної та пожежної безпеки.

**Економічна безпека банківської установи** – стан захищеності ресурсного забезпечення та інтересів банку, його партнерів і клієнтів, що сприяє уникненню або запобіганню внутрішніх і зовнішніх загроз та дозволяє забезпечити стабільне функціонування й розширене відтворення з мінімальними втратами для банку.

**Експрес-моніторинг банківської безпеки** – це безперервний процес збирання інформації та оцінювання динаміки ключових показників стану банківської безпеки з метою своєчасного виявлення внутрішніх і зовнішніх загроз.

**Екстремальні ситуації** – це ситуації, за яких банки та їх персонал піддаються серйозному впливу напружених, майже критичних, обставин, що характеризуються високим рівнем загрози їхньому здоров'ю, життю та ефективності діяльності.

**Загроза** – це нереалізована, але потенційно чи реально наявна з певною ймовірністю настання можливість завдання банку будь-якого збитку зловмисниками, конкурентами або обставинами й умовами, що створюють небезпеку для банку, його клієнтів та контрагентів.

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

**Інформаційно-аналітична робота банку із забезпечення безпеки –** це комплекс заходів, які здійснює відділ безпеки банку з метою збирання та опрацювання інформації про загрози та стан безпеки й розроблення відповідних інформаційно-аналітичних документів для керівництва банку.

**Інформаційно-аналітичне забезпечення безпеки банківської діяльності** – це вид інформаційно-аналітичного забезпечення, що полягає у збиранні, опрацюванні, зберіганні й наданні необхідної інформації щодо стану безпеки відповідним користувачам.

**Інцидент** – активізація діяльності одного із суб'єктів конфліктної ситуації або дії третьої сторони, що сприяють загостренню конфліктної ситуації.

**Кадрова безпека банку –** стан захищеності банку, що полягає в забезпеченні безпеки в роботі з персоналом, контролі за дотриманням банківської таємниці, запобіганні промисловому шпигунству, крадіжкам.

**Конкуренція** – змагання між суб'єктами ринку з метою здобуття, завдяки власним досягненням, переваг над іншими суб'єктами ринку.

**Конфіденційна інформація** – це відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням, відповідно до передбачених ними умов. Ця інформація належить до інформації з обмеженим доступом.

**Конфліктна ситуація в банківській сфері** – це накопичені суперечності, пов'язані із трудовою діяльністю персоналу чи поведінкою і вподобаннями клієнтів та контрагентів банку.

**Конфлікт у банківській сфері** – це зіткнення у процесі виконання трудових функцій протилежних інтересів, дій, думок, оцінок окремих працівників або їх груп, виключно між собою чи за участю клієнтів та партнерів.

**Криптографічна підсистема захисту інформації** – це система захисту, що полягає в контролі за інформаційними потоками шляхом шифрування інформації.

**Легалізація ("відмивання") грошей** – це процес, спрямований на приховування чи маскування незаконного походження, володіння, місця знаходження чи переміщення грошових коштів.

**Матеріальні банківські перепустки** – це перепустки, що дають право на винесення (вивезення) із банку вказаних у них матеріальних цінностей.

**Недобросовісна конкуренція –** неправомірне використання ділової репутації суб'єкта господарювання, створення перешкод суб'єктам господарювання у процесі конкуренції та досягнення неправомірних переваг у конкуренції, неправомірне збирання, розголошення та використання комерційної таємниці.

**Несанкціонований доступ до інформації** – це доступ до інформації, який здійснюють із порушенням установлених правил розмежування доступу.

**Нестандартні ситуації на маршруті інкасації** – це ситуації, пов'язані з непередбаченою зміною умов роботи бригади інкасаторів на маршруті, які можуть мати негативний вплив на здійснення операцій із інкасації та доставки готівки й цінностей, забезпечення безпеки бригади та схоронність перевезених нею готівки й цінностей.

**Операції із цінними паперами** – це закінчена дія чи ряд дій із цінними паперами і/чи грошовими коштами на фондовому ринку, що здійснюють для досягнення поставлених цілей і потребують забезпечення фінансовими ресурсами суб'єкта господарювання, формування та збільшення його статутного капіталу, залучення позичкового капіталу або ресурсів в обіг.

**Операційна безпека банку** – це стан захищеності банку, що полягає в дотриманні безпечного здійснення банківських операцій, запобіганні витоку інформації про банківські операції.

**Організація інформаційно-аналітичного забезпечення безпеки банківської діяльності** – це комплекс організаційних і практичних заходів щодо розроблення змісту, способів дій, термінів і послідовності виконання силами й засобами служби банківської безпеки інформаційно-аналітичних завдань.

**Перепустки для клієнтів операційних підрозділів банку** – це перепустки, що видають для представників підприємств, яких обслуговують у цій установі банку.

**Перепустковий режим охорони** – це режим, що передбачає установлення відповідного порядку доступу в банк, який виключав би можливість безконтрольного входу (виходу) на територію установи банку, у його приміщення та до персоналу сторонніх осіб, клієнтів.

**Платоспроможність банку** – це здатність банку в належні терміни забезпечувати повною мірою погашення своїх зобов'язань.

**Постійні банківські перепустки** – це перепустки, що видають персоналу банку, який перебуває у штаті. Термін дії таких перепусток указано на бланку самої перепустки. Перепустка дійсна без подання інших документів, що засвідчують особу, оскільки містить фотографію, засвідчену печаткою.

**Промислове шпигунство** – це заходи щодо забезпечення несанкціонованого доступу до конфіденційної інформації, її знищення, зміни чи використання.

**Протиборство** – гостра антагоністична боротьба за заволодіння ринком, під час якої застосовують дуже жорсткі заходи впливу на суперників у такій боротьбі.

**Разові банківські перепустки** – це перепустки, що видають для всіх клієнтів (крім клієнтів операційних підрозділів), партнерів, гостей. Видають одноразово. Така перепустка дійсна протягом робочого дня. Після завершення

роботи в банку перепустку підписує особа, яка її замовляла, де вказано час вибуття відвідувача, потім її здають на пропускному пункті. Черговий фіксує час вибуття відвідувача у відповідному журналі.

**Ринкова безпека банку** – це такий стан банку, який характеризується реалізацією потенціалу банку на ринку банківських послуг за допомогою маркетингових інструментів, спрямованих на забезпечення стійких конкурентних переваг, захист від недобросовісної конкуренції.

**Робочі активи** – це активи, що дають банку дохід, тобто кошти на коррахунках, у касі, вклади в майно, цінні папери, розміщені в банках, видані кредити.

**Силова безпека банківської установи** – це стан захищеності банку від крадіжок власності, утрати іміджу та безпеки персоналу, що досягають шляхом використання комплексу методів протидії сторонньому втручанню і завданню збитків.

**Система управління фінансово-економічною безпекою банку** – оптимальна сукупність взаємопов'язаних і взаємодійних функцій та підсистем, які сприяють уникненню або запобіганню внутрішнім і зовнішнім загрозам та дозволяють забезпечити стабільний фінансовий стан і рентабельну роботу з мінімальними ризиками та втратами для банку.

**Співпраця** – тісні ділові взаємовідносини суб'єктів ринку на основі загальних інтересів із метою вдосконалення методів роботи, спрямованої на збільшення прибутків.

**Суперництво** – антагоністичні дії, побудовані на непримиренності позицій, інтересів і методів роботи щодо здобуття переваг на ринку.

**Сховище цінностей** – спеціально обладнане приміщення банку (філії, відділення), сейф, депозитна система та АТМ-сейфи, що використовують для зберігання готівки та інших цінностей, технічний стан яких відповідає нормативно-правовим актам. Приміщення має бути обладнано й технічними засобами для роботи з готівкою. До них належать: машини, пристрої, прилади для оброблення банкнот (монет), за допомогою яких виконують кілька або окремі операції з перераховування банкнот (монет), контролю за захисними ознаками банкнот (монет), обандеролювання корінців банкнот, упаковування банкнот (монет).

**Технічні заходи банківської безпеки** – це спрямовані на захист інформації заходи, здійснення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень у сфері банківської безпеки.

**Тимчасові банківські перепустки** – це перепустки, що видають, зазвичай, для штатних працівників на період терміну випробування; осіб, що працюють за трудовою угодою або у складі тимчасових колективів. Термін дії таких перепусток до півроку.

**Фінансова безпека банку** – стан захищеності банку, який характеризується збалансованістю та якістю використаних фінансових інструментів, технологій і послуг, які забезпечать достатній рівень ліквідності, платоспроможності та прибутковості банку.

**Фінансовий моніторинг** – це комплекс заходів у сфері запобігання та протидії легалізації ("відмиванню") доходів, отриманих злочинним шляхом, або фінансуванню тероризму.

**Фінансово-економічна безпека банку** – динамічний стан захищеності банківських операцій та фінансових ресурсів, що сприяє уникненню або запобіганню внутрішнім і зовнішнім загрозам та дозволяє забезпечити стабільний фінансовий стан і рентабельну роботу з мінімальними ризиками та втратами для банку.

**Цінні папери** – це грошові документи, які затверджують право власності або позики власника документа щодо особи, яка випустила такий документ (емітента).

**Шахрайство** – зловживання довірою, обман із метою введення власника матеріальних цінностей або коштів в оману й на цій основі добровільного передання своєї власності шахраям.

# Використана література


1. Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны / Г. А. Андрощук, П. П. Крайнев. – К. : ВД "Ін Юре", 2000. – 398 с.
2. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : монографія. – К. : Київ. нац. торг.-екон. ун-т, 2004. – 759 с.
3. Веретенникова Г. Б. Економічна безпека підприємства: планування й організація : конспект лекцій / Г. Б. Веретенникова. – Х. : ХНЕУ, 2008. – 84 с.
4. Вечканов Г. С. Экономическая безопасность : учеб. пособ. / Г. С. Вечканов. – СПб. : Вектор, 2005. – 251 с.
5. Гамза В. А. Безопасность банковской деятельности : учеб. / В. А. Гамза, И. Б. Ткачук. – М. : Маркет ДС, 2006. – 424 с.
6. Герасимчук З. В. Економічна безпека регіону: діагностика та механізм забезпечення / З. В. Герасимчук, Н. С. Вавдіюк. – Луцьк : Надстир'я, 2006. – 244 с.
7. Головко В. І. Фінансово-економічна діяльність підприємства: контроль, аналіз та безпека : навч. посіб. для студ. вищ. навч. закл. / В. І. Головко, А. В. Мінченко, В. М. Шаманська ; Київський національний ун-т імені Тараса Шевченка. – К. : Центр навчальної літератури, 2006. – 444 с.
8. Грунин О. А. Экономическая безопасность организации / О. А. Грунин, С. О. Грунин. – СПб. ; М. ; Х. ; Мн. : Питер, 2002. – 160 с.
9. Губарєв О. О. Економічна безпека: конспект лекцій / О. О. Губарєв. – Х. : ХНЕУ, 2007. – 60 с.
10. Економічна безпека : навч. посіб. / З. С. Варналій, П. В. Мельник, Л. Л. Тарангул [та ін.] ; за ред. д-ра екон. наук, проф. З. С. Варналія. – К. : Знання, 2009. – 647 с.
11. Єпіфанов А. О. Фінансова безпека підприємств і банківських установ : монографія / А. О. Єпіфанов, О. Л. Пластун, В. С. Домбровський. – Суми : ДВНЗ "УАБС НБУ", 2009. – 295 с.
12. Захарченко В. И. Экономическая безопасность бизнеса : учеб. пособ. для студ.-магистров экон. спец. / В. И. Захарченко, Н. Н. Меркулов, Н. В. Халикян ; Одес. нац. политехн. ун-т ; Одес. нац. ун-т им. И. Мечникова. – Одеса : Наука и техника, 2009. – 176 с.

13. Зубок М. І. Безпека банківської діяльності : навч.-метод. посіб. для самост. вивч. дисц. / М. І. Зубок. – К. : КНЕУ, 2003. – 156 с.

14. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. / М. І. Калмик. – К. : Атіка, 2005. – 432 с.

15. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения / А. В. Козаченко, В. П. Пономарев, А. Н. Ляшенко. – К. : Либра, 2003. – 280 с.

16. Кочетков В. М. Забезпечення фінансової стійкості сучасного комерційного банку: теоретико-методологічні аспекти / В. М. Кочетков. – К. : КНЕУ, 2002. – 256 с.

17. Кузнецов О. О. Захист інформації та економічна безпека підприємства : монографія / О. О. Кузнецов, С. П. Євсеев, С. В. Кавун. – Х. : ХНЕУ, 2008. – 360 с.

18. Отенко І. П. Аналіз у бюджетних та банківських установах : навч. посіб. / І. П. Отенко, О. Ю. Мішин, С. В. Мішина. – Х. : Вид-во ХНЕУ, 2010. – 240 с.

19. Оцінка і діагностика фінансової стійкості підприємства : монографія / М. О. Кизим, В. А. Забродський, В. А. Зінченко та ін. – Х. : ВД "ІНЖЕК", 2003. – 144 с.

20. Парасій-Вергуненко І. М. Аналіз банківської діяльності : навч.-метод. посіб. для самост. вивч. дисц. / І. М. Парасій-Вергуненко. – К. : КНЕУ, 2003. – 348 с.

21. Побережний С. М. Фінансова безпека банківської діяльності : навч. посіб. для самост. вивч. дисц. "Безпека банків" / С. М. Побережний, О. Л. Пластун, Т. М. Болгар. – Суми : ДВНЗ "УАБС НБУ", 2010. – 112 с.

22. Понікаров В. Д. Аудит : навч. посіб. / В. Д. Понікаров, Т. М. Сєрікова. – Х. : ВД "Інжек", 2006. – 224 с.

23. Пономаренко В. С. Экономическая безопасность региона: анализ, оценка, прогнозирование / В. С. Пономаренко, Т. С. Клебанова, Н. Л. Чернова. – Х. : ИД "ИНЖЭК", 2004. – 144 с.

24. Про банки і банківську діяльність : Закон України № 2121-III від 07.12.2000 р. Поточна редакція від 02.08.2014 р. [Електронний ресурс]. – Режим доступу : http://www. zakon4rada.gov.ua.

25. Про запобігання та протидію легалізації ("відмиванню") доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України № 1702-VII

від 14.10.2014 р. [Електронний ресурс]. – Режим доступу : http://www.zakon.rada.gov.ua.

26. Про затвердження Інструкції про ведення касових операцій банками в Україні : Постанова Правління НБУ від 01.06.2011 р. № 174. Поточна редакція від 07.06.2014 р. [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua.

27. Про затвердження Положення про порядок формування та використання банками України резервів для відшкодування можливих втрат за активними банківськими операціями : Постанова Правління НБУ від 25.01.2012 р. № 23. Поточна редакція від 22.11.2014 р. [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua.

28. Про інформацію : Закон України № 2657-XII від 02.10.1992 р. Поточна редакція від 02.03.2014 р. [Електронний ресурс]. – Режим доступу : http://www.zakon4rada.gov.ua.

29. СОУН НБУ 65.1 СУІБ 2.0:2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO/IES 27002:2005, MOD) [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua.

30. Шахрайство на фінансовому ринку. Практичний посібник з протидії / [за ред. В. Фещенка]. – К. : Українське агентство фінансового розвитку, 2011. – 424 с.

31. Шкарлет С. М. Економічна безпека підприємства: інноваційний аспект : монографія / С. М. Шкарлет. – К. : Книжкове видавництво Національного авіаційного ун-ту, 2007. – 436 с.

32. Щибиволок З. І. Аналіз банківської діяльності : навч. посіб. / З. І. Щибиволок. – К. : Знання, 2006. – 312 с.

33. Экономическая безопасность : энциклопедия / А. Г. Шаваев (пред. ред. кол.), А. Т. Багаутдинов (авт.-сост.). – М. : ИД "Правовое просвещение", 2001. – 511 с.

# Додатки

Додаток А

Таблиця А.1

## Формули для розрахунку фінансових коефіцієнтів із метою визначення інтегрального показника фінансового стану

| Фінансові коефіцієнти | Характеристики | Формули розрахунку | Алгоритми розрахунку для: | |
|---|---|---|---|---|
| | | | великого або середнього підприємства | малого підприємства |
| 1 | 2 | 3 | 4 | 5 |
| 1) К1, МК1 – коефіцієнт покриття (ліквідність третього ступеня) | Здатність підприємства покривати поточні зобов'язання оборотними активами | Оборотні активи / Поточні зобов'язання | ф. 1 р. 1195 гр. 4 / ф. 1 р. 1695 гр. 4 | ф. 1-м (1-мс) р. 260 гр. 4 / ф. 1-м (1-мс) р. 620 гр. 4 |
| 2) К2, МК2 – проміжний коефіцієнт покриття | Здатність підприємства розраховуватися за своїми поточними зобов'язаннями монетарними оборотними активами. Характеризує очікувану платоспроможність боржника в короткостроковому періоді | Монетарні оборотні активи / Поточні зобов'язання | (ф. 1 р. 1125 + р. 1160 + р. 1165 гр. 4) / ф. 1 р. 1695 гр. 4 | ф. 1-м р. 160 + р. 220 + + р. 230 + р. 240 гр. 4 / ф. 1-м р. 620 гр. 4 або ф. 1-мс р. 210 + р. 230 + + р. 240 гр. 4 / ф. 1-м (1-мс) р. 620 гр. 4 |
| 3) К3, МК3 – коефіцієнт фінансової незалежності | Питома вага власного капіталу в загальному обсязі джерел фінансування. Характеризує ступінь залежності підприємства від позичкових джерел | Власний капітал / Валюта балансу | ф. 1 р. 1495 гр. 4 / ф. 1 р. 1900 гр. 4 | ф. 1-м (1-мс) р. 380 гр. 4 / ф. 1-м (1-мс) р. 640 гр. 4 |

Продовження табл. А.1

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 4) К4, МК4 – коефіцієнт покриття необоротних активів власним капіталом | Рівень фінансування необоротних (довгострокових) активів за рахунок власного капіталу підприємства | Власний капітал / Необоротні активи | ф. 1 р. 1495 гр. 4 / ф. 1 р. 1095 гр. 4 | ф. 1-м (1-мс) р. 380 гр. 4 / ф. 1-м (1-мс) р. 080 гр. 4 |
| 5) К5 – коефіцієнт рентабельності власного капіталу | Ефективність використання капіталу підприємства, інвестованого власниками | Чистий прибуток/збиток / Інвестований власний капітал | ф. 2 р. 2350 – – р. 2355 гр. 3 / ф. 1 [(р. 1400 + р. 1405 + + р. 1410 – р. 1425 – – р. 1430 гр. 3) + + (р. 1400 + р. 1405 + + р. 1410 – р. 1425 – – р. 1430 гр. 4)] : 2 | – |
| 6) МК5 – коефіцієнт оборотності кредиторської заборгованості | Здатність розраховуватися за кредиторською заборгованістю за товари, роботи, послуги виручкою від реалізації | Чиста виручка від реалізації / Кредиторська заборгованість | – | ф. 2-м (2-мс) р. 030 гр. 3 / ф.1-м (1-мс) р. 530 (гр. 3 + гр. 4) : 2 |
| 7) К6, МК6 – коефіцієнт рентабельності продажу за фінансовими результатами від операційної діяльності (EBIT) | Характеризує рентабельність продажу за фінансовими результатами від операційної діяльності до оподаткування та здійснення витрат, пов'язаних із запозиченнями | Фінансові результати від операційної діяльності (EBIT) / Чиста виручка від реалізації | ф. 2 р. 2190 – – р. 2195 гр. 3 / ф. 2 р. 2000 гр. 3 | ф. 2-м (2-мс) р. 030 – – р. 080 гр. 3 / ф. 2-м (2-мс) р. 030 гр. 3 |

Продовження табл. А.1

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 8) К7 – коефіцієнт рентабельності продажу за фінансовими результатами від звичайної діяльності (EBITDA) | Характеризує рентабельність продажу за фінансовими результатами від звичайної діяльності до оподаткування, здійснення фінансових витрат та нарахування амортизації | Фінансові результати від звичайної діяльності до оподаткування фінансових витрат та нарахування амортизації / Чиста виручка + + інші операційні доходи | ф. 2 р. 2350 – – р. 2355 + р. 2315 + + р. 2300 + р. 2250 гр. 3 / ф. 2 р. 2000 + + р. 2120 гр. 3 | – |
| 9) МК7 – коефіцієнт рентабельності продажу за фінансовими результатами до оподаткування | Характеризує рентабельність продажу за фінансовими результатами до оподаткування | Фінансовий результат до оподаткування / Разом чисті доходи | – | ф. 2-м (2-мс) р. 070 – – р. 120 гр. 3 / ф. 2-м (2-мс) р. 070 гр. 3 |
| 10) К8, МК8 – коефіцієнт рентабельності активів за чистим прибутком | Характеризує ефективність використання (рентабельність) активів підприємства | Чистий прибуток (збиток) / Валюта балансу | ф. 2 р. 2350 – – р. 2355 гр. 3 / ф. 1 р. 1300 (гр. 3 + гр. 4) : 2 | ф. 2-м (2-мс) р. 070 – – р. 120 – р. 140 – р. 145 гр. 3 / ф. 1-м (1-мс) р. 280 (гр. 3 + гр. 4) : 2 |
| 11) К9, МК9 – коефіцієнт оборотності оборотних активів | Характеризує ефективність використання оборотних активів | Чиста виручка від реалізації / Оборотні активи | ф. 2 р. 2000 гр. 3 / ф. 1 р. 1195 (гр. 3 + + гр. 4) : 2 | ф. 2-м (2-мс) р. 030 гр. 3 / ф. 1-м (1-мс) р. 260 (гр. 3 + + гр. 4) : 2 |

Закінчення табл. А.1

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 12) К10 – коефіцієнт оборотності позичкового капіталу за фінансовими результатами від звичайної діяльності (EBITDA) | Здатність підприємства розраховуватися з боргами за рахунок внутрішніх фінансових джерел | Фінансові результати від звичайної діяльності до оподаткування фінансових витрат та нарахування амортизації) / Довгострокові та поточні зобов'язання | ф. 2 р. 2350 – р. 2355 + + р. 2315 + + р. 2300 + р. 2250 гр. 3 / ф. 1 р. 1595 + + р. 1695 гр. 4 | – |
| 13) МК10 – коефіцієнт оборотності позичкового капіталу за фінансовими результатами до оподаткування | Здатність підприємства розраховуватися з боргами за рахунок фінансового результату | Фінансовий результат до оподаткування / Довгострокові та поточні зобов'язання | – | ф. 2-м (2-мс) р. 070 – – р. 120 гр. 3 / ф. 1-м (1-мс) р. 480 + + р. 620 гр. 4 |

Додаток Б

Таблиця Б.1

## Моделі розрахунку інтегрального показника боржника – юридичної особи – для великого або середнього підприємства

| № п/п | Групи видів економічної діяльності | Моделі |
|---|---|---|
| 1 | Сільське господарство, лісове господарство та рибне господарство: секція A | $Z = 1{,}3 \cdot К_3 + 0{,}03 \cdot К_4 + 0{,}001 \cdot К_5 + 0{,}61 \cdot К_6 + 0{,}75 \cdot К_7 + 2{,}5 \cdot К_8 + 0{,}04 \cdot К_9 - 0{,}2$ |
| 2 | Виробництво харчових продуктів, напоїв та тютюнових виробів: секція C | $Z = 0{,}035 \cdot К_1 + 0{,}04 \cdot К_2 + 2{,}7 \cdot К_3 + 0{,}1 \cdot К_6 + 1{,}1 \cdot К_7 + 1{,}2 \cdot К_8 + 0{,}05 \cdot К_9 - 0{,}8$ |
| 3 | Переробна промисловість: секція C | $Z = 0{,}95 \cdot К_3 + 0{,}03 \cdot К_4 + 1{,}1 \cdot К_6 + 1{,}4 \cdot К_7 + 3{,}1 \cdot К_8 + 0{,}04 \cdot К_9 + 0{,}03 \cdot К_{10} - 0{,}45$ |
| 4 | Добувна промисловість і розроблення кар'єрів: секція B; переробна промисловість: секція C; постачання електроенергії, газу: секція D; водопостачання, каналізація: секція E | $Z = 0{,}025 \cdot К_1 + 1{,}9 \cdot К_3 + 0{,}45 \cdot К_6 + 1{,}5 \cdot К_8 + 0{,}03 \cdot К_9 - 0{,}5$ |
| 5 | Будівництво: секція F | $Z = 0{,}02 \cdot К_1 + 1{,}7 \cdot К_3 + 0{,}01 \cdot К_4 + 0{,}3 \cdot К_6 + 0{,}4 \cdot К_7 + 2{,}9 \cdot К_8 - 0{,}1$ |
| 6 | Оптова та роздрібна торгівля, ремонт автотранспортних засобів: секція G; тимчасове розміщування й організація харчування: секція I | $Z = 1{,}03 \cdot К_3 + 0{,}001 \cdot К_4 + 0{,}16 \cdot К_6 + 0{,}6 \cdot К_7 + 2{,}9 \cdot К_8 + 0{,}08 \cdot К_9 - 0{,}14$ |
| 7 | Транспорт, складське господарство, поштова та кур'єрська діяльність: секція H; електрозв'язок: секція J | $Z = 0{,}07 \cdot К_2 + 1{,}27 \cdot К_3 + 0{,}32 \cdot К_6 + 1{,}98 \cdot К_8 + 0{,}04 \cdot К_9 + 0{,}04 \cdot К_{10} - 0{,}15$ |
| 8 | Фінансова та страхова діяльність (крім банків): секція K | $Z = 0{,}025 \cdot К_1 + 2{,}7 \cdot К_3 + 0{,}005 \cdot К_4 + 0{,}13 \cdot К_7 + 2{,}4 \cdot К_8 - 0{,}93$ |
| 9 | Інформація та телекомунікації: секція J; інші операції та послуги: секції L – U | $Z = 0{,}03 \cdot К_1 + 0{,}9 \cdot К_3 + 0{,}01 \cdot К_4 + 0{,}002 \cdot К_5 + 0{,}15 \cdot К_6 + 0{,}5 \cdot К_7 + 2{,}9 \cdot К_8 - 0{,}05$ |

Таблиця Б.2

**Моделі розрахунку інтегрального показника боржника – юридичної особи – для малого підприємства**

| № п/п | Групи видів економічної діяльності | Моделі |
|---|---|---|
| 1 | Сільське, лісове та рибне господарство: секція A | $Z = 0{,}02 \cdot МК_1 + 0{,}02 \cdot МК_2 + 1{,}5 \cdot МК_3 + 0{,}6 \cdot МК_7 + 2{,}6 \cdot МК_8 + 0{,}008 \cdot МК_9 – 1{,}1$ |
| 2 | Виробництво харчових продуктів, напоїв та тютюнових виробів: секція C | $Z = 0{,}01 \cdot МК_1 + 0{,}03 \cdot МК_2 + 2{,}2 \cdot МК_3 + 0{,}03 \cdot МК_4 + 0{,}95 \cdot МК_7 + 1{,}3 \cdot МК_8 + + 0{,}06 \cdot МК_9 + 0{,}2 \cdot МК_{10} - 0{,}7$ |
| 3 | Переробна промисловість: секція C | $Z = 0{,}03 \cdot МК_2 + 1{,}95 \cdot МК_3 + 0{,}01 \cdot МК_4 + 0{,}002 \cdot МК_6 + 2{,}5 \cdot МК_7 + 0{,}8 \cdot МК_8 + 0{,}05 \cdot МК_9 – 0{,}9$ |
| 4 | Добувна промисловість і розроблення кар'єрів: секція B; переробна промисловість: секція C; постачання електроенергії, газу: секція D; водопостачання, каналізація: секція E | $Z = 0{,}01 \cdot МК_1 + 2{,}42 \cdot МК_3 + 0{,}01 \cdot МК_4 + 0{,}05 \cdot МК_7 + 1{,}35 \cdot МК_8 + 0{,}05 \cdot МК_9 – 0{,}7$ |
| 5 | Будівництво: секція F | $Z = 0{,}02 \cdot МК_1 + 2{,}2 \cdot МК_3 + 0{,}001 \cdot МК_5 + 0{,}01 \cdot МК_6 + 0{,}009 \cdot МК_7 + 1{,}4 \cdot МК_8 + 0{,}2 \cdot МК_{10} – 0{,}27$ |
| 6 | Оптова та роздрібна торгівля, ремонт автотранспортних засобів: секція G; тимчасове розміщування й організація харчування: секція I | $Z = 0{,}03 \cdot МК_1 + 1{,}85 \cdot МК_3 + 0{,}004 \cdot МК_4 + 0{,}001 \cdot МК_5 + 0{,}1 \cdot МК_6 + 0{,}2 \cdot МК_7 + + 2{,}2 \cdot МК_8 + 0{,}009 \cdot МК_9 – 0{,}35$ |
| 7 | Транспорт, складське господарство, поштова та кур'єрська діяльність: секція H; електрозв'язок: секція J | $Z = 0{,}04 \cdot МК_1 + 0{,}01 \cdot МК_2 + 1{,}8 \cdot МК_3 + 0{,}002 \cdot МК_5 + 0{,}6 \cdot МК_6 + 0{,}85 \cdot МК_7 + + 1{,}7 \cdot МК_8 + 0{,}03 \cdot МК_9 – 0{,}8$ |
| 8 | Фінансова та страхова діяльність (крім банків): секція K | $Z = 0{,}02 \cdot МК_1 + 1{,}7 \cdot МК_3 + 0{,}001 \cdot МК_4 + 0{,}001 \cdot МК_5 + 0{,}15 \cdot МК_6 + 3{,}1 \cdot МК_8 + + 0{,}02 \cdot МК_9 - 0{,}4$ |
| 9 | Інформація та телекомунікації: секція J; інші операції та послуги: секції L – U | $Z = 0{,}01 \cdot МК_1 + 1{,}92 \cdot МК_3 + 0{,}01 \cdot МК_6 + 0{,}02 \cdot МК_7 + 1{,}2 \cdot МК_8 + 0{,}01 \cdot МК_9 – 0{,}35$ |

Додаток В

Таблиця В.1

**Класи боржника – юридичної особи – для великого або середнього підприємства**

| № п/п | Види економічної діяльності | Класи | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | клас 1 | клас 2 | клас 3 | клас 4 | клас 5 | клас 6 | клас 7 | клас 8 | клас 9 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | Сільське господарство, лісове господарство та рибне господарство: секція А | Більше ніж +1,25 | Від +1,25 до +0,81 | Від +0,80 до +0,60 | Від +0,59 до +0,35 | Від +0,34 до +0,05 | Від +0,04 до -0,25 | Від -0,26 до -0,70 | Від -0,71 до -3,20 | Менше ніж -3,20 |
| 2 | Виробництво харчових продуктів, напоїв та тютюнових виробів: секція С | Більше ніж +1,35 | Від +1,35 до +0,71 | Від +0,70 до +0,35 | Від +0,34 до 0,00 | Від -0,01 до -0,36 | Від -0,37 до -0,70 | Від -0,71 до -1,20 | Від -1,21 до -3,50 | Менше ніж -3,50 |
| 3 | Переробна промисловість: секція С | Більше ніж +1,35 | Від +1,35 до +0,81 | Від +0,80 до +0,51 | Від +0,50 до +0,17 | Від +0,16 до -0,20 | Від -0,21 до -0,50 | Від -0,51 до -1,04 | Від -1,05 до -3,70 | Менше ніж -3,70 |
| 4 | Добувна промисловість і розроблення кар'єрів: секція В; переробна промисловість: секція С; постачання електроенергії, газу: секція D; водопостачання, каналізація: секція Е | Більше ніж +1,35 | Від +1,35 до +0,80 | Від +0,79 до +0,51 | Від +0,50 до +0,04 | Від +0,03 до -0,40 | Від -0,41 до -0,75 | Від -0,76 до -1,34 | Від -1,35 до -4,70 | Менше ніж -4,70 |
| 5 | Будівництво: секція F | Більше ніж +0,60 | Від +0,60 до +0,07 | Від +0,06 до -0,15 | Від -0,16 до -0,40 | Від -0,41 до -0,67 | Від -0,68 до -0,90 | Від -0,91 до -1,30 | Від -1,31 до -3,80 | Менше ніж -3,80 |

Закінчення табл. В.1

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | Оптова та роздрібна торгівля, ремонт автотранспортних засобів: секція G; тимчасове розміщування й організація харчування: секція I | Більше ніж +1,50 | Від +1,50 до +0,91 | Від +0,90 до +0,62 | Від +0,61 до +0,16 | Від +0,15 до -0,27 | Від -0,28 до -0,60 | Від -0,61 до -1,20 | Від -1,21 до -4,70 | Менше ніж -4,70 |
| 7 | Транспорт, складське господарство, поштова та кур'єрська діяльність: секція H; електрозв'язок: секція J | Більше ніж +1,55 | Від +1,55 до +1,01 | Від +1,00 до +0,76 | Від +0,75 до +0,35 | Від +0,34 до -0,05 | Від -0,06 до -0,37 | Від -0,38 до -0,95 | Від -0,96 до -3,50 | Менше ніж -3,50 |
| 8 | Фінансова та страхова діяльність (крім банків): секція K | Більше ніж +2,00 | Від +2,00 до +1,20 | Від +1,19 до +0,95 | Від +0,94 до +0,52 | Від +0,51 до +0,10 | Від +0,09 до -0,25 | Від -0,26 до -0,83 | Від -0,84 до -4,20 | Менше ніж -4,20 |
| 9 | Інформація та телекомунікації: секція J; інші операції та послуги: секції L – U | Більше ніж +1,15 | Від +1,15 до +0,70 | Від +0,69 до +0,45 | Від +0,44 до +0,09 | Від +0,08 до -0,26 | Від -0,27 до -0,55 | Від -0,56 до -1,10 | Від -1,11 до -3,30 | Менше ніж -3,30 |

Таблиця В.2

## Класи боржника – юридичної особи – для малого підприємства

| № п/п | Види економічної діяльності | Класи | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | клас 1 | клас 2 | клас 3 | клас 4 | клас 5 | клас 6 | клас 7 | клас 8 | клас 9 |
| 1 | Сільське господарство, лісове господарство та рибне господарство: секція А | Більше ніж +1,00 | Від +1,00 до +0,50 | Від +0,49 до +0,28 | Від +0,27 до -0,10 | Від -0,11 до -0,45 | Від -0,46 до -0,75 | Від -0,76 до -1,26 | Від -1,27 до -4,20 | Менше ніж -4,20 |
| 2 | Виробництво харчових продуктів, напоїв та тютюнових виробів: секція С | Більше ніж +2,00 | Від +2,00 до +1,40 | Від +1,39 до +1,05 | Від +1,04 до +0,55 | Від +0,54 до +0,01 | Від 0,00 до -0,40 | Від -0,41 до -1,10 | Від -1,11 до -4,40 | Менше ніж -4,40 |
| 3 | Переробна промисловість: секція С | Більше ніж +1,70 | Від +1,70 до +1,11 | Від +1,10 до +0,81 | Від +0,80 до +0,35 | Від +0,34 до -0,10 | Від -0,11 до -0,50 | Від -0,51 до -1,14 | Від -1,15 до -4,10 | Менше ніж -4,10 |
| 4 | Добувна промисловість і розроблення кар'єрів: секція В; переробна промисловість: секція С; постачання електроенергії, газу: секція D; водопостачання, каналізація: секція Е | Більше ніж +2,20 | Від +2,20 до +1,25 | Від +1,24 до +0,90 | Від +0,89 до +0,42 | Від +0,41 до -0,05 | Від -0,06 до -0,50 | Від -0,51 до -1,20 | Від -1,21 до -4,90 | Менше ніж -4,90 |
| 5 | Будівництво: секція F | Більше ніж +2,10 | Від +2,10 до +1,40 | Від +1,39 до +0,81 | Від +0,80 до +0,53 | Від +0,52 до +0,04 | Від +0,03 до -0,35 | Від -0,36 до -1,10 | Від -1,11 до -4,20 | Менше ніж -4,20 |

Закінчення табл. В.2

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | Оптова та роздрібна торгівля, ремонт автотранспортних засобів: секція G; тимчасове розміщування й організація харчування: секція I | Більше ніж +1,60 | Від +1,60 до +0,96 | Від +0,95 до +0,71 | Від +0,70 до +0,20 | Від +0,19 до -0,24 | Від -0,25 до -0,59 | Від -0,60 до -1,25 | Від -1,26 до -5,20 | Менше ніж -5,20 |
| 7 | Транспорт, складське господарство, поштова та кур'єрська діяльність: секція H; електрозв'язок: секція J | Більше ніж +1,40 | Від +1,40 до +0,86 | Від +0,85 до +0,61 | Від +0,60 до +0,20 | Від +0,19 до -0,19 | Від -0,20 до -0,50 | Від -0,51 до -1,10 | Від -1,11 до -4,40 | Менше ніж -4,40 |
| 8 | Фінансова та страхова діяльність (крім банків): секція K | Більше ніж +2,50 | Від +2,50 до +1,51 | Від +1,50 до +1,20 | Від +1,19 до +0,75 | Від +0,74 до +0,32 | Від +0,31 до -0,10 | Від -0,11 до - 0,75 | Від -0,76 до -3,40 | Менше ніж -3,40 |
| 9 | Інформація та телекомунікації: секція J; інші операції та послуги: секції L – U | Більше ніж +1,60 | Від +1,60 до +0,98 | Від +0,97 до +0,62 | Від +0,61 до +0,23 | Від +0,22 до -0,20 | Від -0,21 до -0,55 | Від -0,56 до -1,19 | Від -1,20 до -4,20 | Менше ніж -4,20 |

Додаток Д

# Баланс (Звіт про фінансовий стан) на 31.12. 2014 р.

Форма № 1 Код за ДКУД 1801001

| Актив | Код рядка | На початок звітного періоду | На кінець звітного періоду |
|---|---|---|---|
| **I. Необоротні активи** | | | |
| Нематеріальні активи | 1000 | 1 | 1 |
| первісна вартість | 1001 | 22 | 23 |
| накопичена амортизація | 1002 | (21) | (22) |
| Незавершені капітальні інвестиції | 1005 | | |
| Основні засоби | 1010 | 62597 | 76731 |
| первісна вартість | 1011 | 142445 | 163320 |
| знос | 1012 | (79848) | (86589) |
| Інвестиційна нерухомість | 1015 | | |
| Довгострокові біологічні активи | 1020 | | |
| Довгострокові фінансові інвестиції: які обліковують за методом участі в капіталі інших підприємств | 1030 | | |
| інші фінансові інвестиції | 1035 | 2 | 2 |
| Довгострокова дебіторська заборгованість | 1040 | | |
| Відстрочені податкові активи | 1045 | | |
| Інші необоротні активи | 1090 | | |
| **Усього за розділом I** | **1095** | **62600** | **76734** |
| **II. Оборотні активи** | | | |
| Запаси | 1100 | 11612 | 12464 |
| Поточні біологічні активи | 1110 | | |
| Дебіторська заборгованість за продукцію, товари, роботи, послуги | 1125 | 5000 | 11910 |
| Дебіторська заборгованість за розрахунками: за виданими авансами | 1130 | 294 | 14 |
| із бюджетом | 1135 | 1040 | 1081 |
| у тому числі з податку на прибуток | 1136 | | |
| Інша поточна дебіторська заборгованість | 1155 | 61 | 66 |
| Поточні фінансові інвестиції | 1160 | | |
| Гроші та їх еквіваленти | 1165 | 294 | 389 |
| Витрати майбутніх періодів | 1170 | 3 | 2 |
| Інші оборотні активи | 1190 | 250 | 3 |
| **Усього за розділом II** | **1195** | **18304** | **25926** |
| **III. Необоротні активи, утримувані для продажу, та групи вибуття** | **1200** | | |
| **Баланс** | **1300** | **80904** | **102660** |

| Пасив | Код рядка | На початок звітного періоду | На кінець звітного періоду |
|---|---|---|---|
| **I. Власний капітал** | | | |
| Зареєстрований капітал | 1400 | 67416 | 67416 |
| Капітал у дооцінках | 1405 | | |
| Додатковий капітал | 1410 | 26202 | 24284 |
| Резервний капітал | 1415 | | |
| Нерозподілений прибуток (непокритий збиток) | 1420 | (30408) | (27765) |
| Неоплачений капітал | 1425 | | |
| Вилучений капітал | 1430 | | |
| **Усього за розділом I** | **1495** | **63210** | **63935** |
| **II. Довгострокові зобов'язання і забезпечення** | | | |
| Відстрочені податкові зобов'язання | 1500 | 1796 | 419 |
| Довгострокові кредити банків | 1510 | 8075 | 8326 |
| Інші довгострокові зобов'язання | 1515 | | 17629 |
| Довгострокові забезпечення | 1520 | | |
| Цільове фінансування | 1525 | | |
| **Усього за розділом II** | **1595** | **9871** | **24642** |
| **III. Поточні зобов'язання і забезпечення** | | | |
| Короткострокові кредити банків | 1600 | | |
| Поточна кредиторська заборгованість за: довгостроковими зобов'язаннями | 1610 | | |
| товари, роботи, послуги | 1615 | 6115 | 5583 |
| розрахунками з бюджетом | 1620 | 616 | 1868 |
| у тому числі з податку на прибуток | 1621 | | |
| розрахунками зі страхування | 1625 | 46 | 87 |
| розрахунками з оплати праці | 1630 | 107 | 270 |
| Поточні забезпечення | 1660 | | 4332 |
| Доходи майбутніх періодів | 1665 | | |
| Інші поточні зобов'язання | 1690 | 939 | 189 |
| **Усього за розділом III** | **1695** | **7823** | **12351** |
| **IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття** | **1700** | | |
| **Баланс** | **1900** | **80904** | **102660** |

Додаток Е

## Звіт про фінансові результати (Звіт про сукупний дохід) за 12 місяців 2014 р.

Форма № 2 Код за ДКУД 1801003

## І. Фінансові результати

| Стаття | Код рядка | За звітний період | За аналогічний період попереднього року |
|---|---|---|---|
| Чистий дохід від реалізації продукції (товарів, робіт, послуг) | 2000 | 77795 | 41314 |
| Собівартість реалізованої продукції (товарів, робіт, послуг) | 2050 | 61560 | 34776 |
| **Валовий:** прибуток | 2090 | 16235 | 6538 |
| збиток | 2095 | | |
| Інші операційні доходи | 2120 | 28274 | 3014 |
| Адміністративні витрати | 2130 | 6415 | 4525 |
| Витрати на збут | 2150 | 9330 | 5453 |
| Інші операційні витрати | 2180 | 27144 | 5896 |
| **Фінансовий результат від операційної діяльності:** прибуток | 2190 | 1620 | |
| збиток | 2195 | | 6322 |
| Дохід від участі в капіталі | 2200 | | |
| Інші фінансові доходи | 2220 | | |
| Інші доходи | 2240 | 71 | 33 |
| Фінансові витрати | 2250 | 1484 | 999 |
| Втрати від участі в капіталі | 2255 | | |
| Інші витрати | 2270 | 154 | 133 |
| **Фінансовий результат до оподаткування:** прибуток | 2290 | 53 | |
| збиток | 2295 | | 7421 |
| Витрати (дохід) з податку на прибуток | 2300 | | |
| Прибуток (збиток) від припиненої діяльності після оподаткування | 2305 | | |
| **Чистий фінансовий результат:** прибуток | 2350 | 53 | |
| збиток | 2355 | | 7421 |

## II. Сукупний дохід

| Стаття | Код рядка | За звітний період | За аналогічний період попереднього року |
|---|---|---|---|
| Дооцінка (уцінка) необоротних активів | 2400 | | |
| Дооцінка (уцінка) фінансових інструментів | 2405 | | |
| Накопичені курсові різниці | 2410 | | |
| Частка іншого сукупного доходу асоційованих та спільних підприємств | 2415 | | |
| Інший сукупний дохід | 2445 | | |
| **Інший сукупний дохід до оподаткування** | **2450** | | |
| Податок на прибуток, пов'язаний з іншим сукупним доходом | 2455 | | |
| **Інший сукупний дохід після оподаткування** | **2460** | | |
| **Сукупний дохід (сума рядків 2350, 2355 та 2460)** | **2465** | | |

## III. Елементи операційних витрат

| Назва статті | Код рядка | За звітний період | За аналогічний період попереднього року |
|---|---|---|---|
| Матеріальні затрати | 2500 | 47324 | 25990 |
| Витрати на оплату праці | 2505 | 11649 | 7116 |
| Відрахування на соціальні заходи | 2510 | 4193 | 2559 |
| Амортизація | 2515 | 6812 | 6923 |
| Інші операційні витрати | 2520 | 8506 | 6476 |
| **Разом** | **2550** | 78484 | 49064 |

## IV. Розрахунок показників прибутковості акцій

| Назва статті | Код рядка | За звітний період | За аналогічний період попереднього року |
|---|---|---|---|
| Середньорічна кількість простих акцій | 2600 | | |
| Скоригована середньорічна кількість простих акцій | 2605 | | |
| Чистий прибуток (збиток) на одну просту акцію | 2610 | | |
| Скоригований чистий прибуток (збиток) на одну просту акцію | 2615 | | |
| Дивіденди на одну просту акцію | 2650 | | |

Додаток Ж

## Фінансовий звіт
## суб'єкта малого підприємництва

Форма № 1-м

Код за ДКУД 1801006

**Баланс на 31 грудня 2014 р.**

| Актив | Код рядка | На початок звітного року | На кінець звітного періоду |
|---|---|---|---|
| **I. Необоротні активи** | | | |
| Незавершені капітальні інвестиції | 1005 | | |
| Основні засоби | 1010 | 405,2 | 399,4 |
| первісна вартість | 1011 | 575,7 | 575,7 |
| знос | 1012 | (170,5) | (76,3) |
| Довгострокові біологічні активи | 1020 | | |
| Довгострокові фінансові інвестиції | 1030 | | |
| Інші необоротні активи | 1090 | | |
| **Усього за розділом I** | **1095** | 405,2 | 399,4 |
| **II. Оборотні активи** | | | |
| Запаси | 1100 | | |
| у тому числі готова продукція | 1103 | | |
| Поточні біологічні активи | 1110 | | |
| Дебіторська заборгованість за товари, роботи, послуги | 1125 | 49,7 | 54,2 |
| Дебіторська заборгованість за розрахунками з бюджетом | 1135 | | |
| у тому числі з податку на прибуток | 1136 | | |
| Інша поточна дебіторська заборгованість | 1155 | | |
| Поточні фінансові інвестиції | 1160 | | |
| Гроші та їх еквіваленти | 1165 | 17,6 | 6,2 |
| Витрати майбутніх періодів | 1170 | | |
| Інші оборотні активи | 1190 | | |
| **Усього за розділом II** | **1195** | 67,3 | 60,4 |
| **III. Необоротні активи, утримувані для продажу, та групи вибуття** | **1200** | | |
| **Баланс** | **1300** | 472,5 | 459,8 |

| Пасив | Код рядка | На початок звітного року | На кінець звітного періоду |
|---|---|---|---|
| **I. Власний капітал** | | | |
| Зареєстрований (пайовий) капітал | 1400 | 1100,0 | 1100,0 |
| Додатковий капітал | 1410 | | |
| Резервний капітал | 1415 | | |
| Нерозподілений прибуток (непокритий збиток) | 1420 | 18,6 | 24,9 |
| Неоплачений капітал | 1425 | (685,0 ) | (685,0 ) |
| **Усього за розділом I** | **1495** | 433,6 | 439,9 |
| **II. Довгострокові зобов'язання, цільове фінансування та забезпечення** | **1595** | | |
| **III. Поточні зобов'язання** | | | |
| Короткострокові кредити банків | 1600 | | |
| Поточна кредиторська заборгованість за: | | | |
| довгостроковими зобов'язаннями | 1610 | | |
| товари, роботи, послуги | 1615 | 9,2 | 3,5 |
| розрахунками з бюджетом | 1620 | 12,3 | 9,5 |
| у тому числі з податку на прибуток | 1621 | | |
| розрахунками зі страхування | 1625 | | |
| розрахунками з оплати праці | 1630 | 17,4 | 6,9 |
| Доходи майбутніх періодів | 1665 | | |
| Інші поточні зобов'язання | 1690 | | |
| **Усього за розділом III** | **1695** | 38,9 | 19,9 |
| **IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття** | **1700** | | |
| **Баланс** | **1900** | 472,5 | 459,8 |

Додаток 3

## Звіт про фінансові результати за рік 2014 р.

Форма № 2-м

Код за ДКУД 1801007

| Стаття | Код рядка | За звітний період | За аналогічний період попереднього року |
|---|---|---|---|
| Чистий дохід від реалізації продукції (товарів, робіт, послуг) | 2000 | 513,0 | 598,1 |
| Інші операційні доходи | 2120 | | |
| Інші доходи | 2240 | 57,2 | 67,2 |
| **Разом доходи** (2000 + 2120 + 2240) | **2280** | **570,2** | **665,3** |
| Собівартість реалізованої продукції (товарів, робіт, послуг) | 2050 | (498,2) | (597,2) |
| Інші операційні витрати | 2180 | (67,7) | (68,1) |
| Інші витрати | 2270 | ( ) | ( ) |
| **Разом витрати** (2050 + 2180 + 2270) | **2285** | (**565,9**) | (619,1) |
| Фінансовий результат до оподаткування (2280 – 2285) | 2290 | **4,3** | **46,2** |
| Податок на прибуток | 2300 | ( ) | ( ) |
| **Чистий прибуток (збиток)** (2290 – 2300) | **2350** | **4,3** | **46,2** |

Додаток И

## Кваліфікаційні характеристики посади керівника (директора) підрозділу (служби, управління, департаменту) із безпеки (фінансово-економічної, інформаційної)

**Завдання та обов'язки.** Керує фінансово-економічним та інформаційним напрямами забезпечення безпеки підрозділу (служби, управління, департаменту), відповідає за наслідки прийнятих рішень, ефективне використання інформації. Контролює та координує напрями робіт із розроблення, запровадження та реалізації заходів із забезпечення фінансово-економічної та інформаційної безпеки. Відповідає за дотримання підрозділом (службою, управлінням, департаментом) усіх зобов'язань із фінансово-економічної секретності перед державними та приватними юридичними особами. Затверджує (візує) керівні документи, які стосуються організації діяльності системи фінансово-економічної та інформаційної безпеки підрозділу (служби, управління, департаменту), механізмів управління та взаємодії. Організовує роботу та ефективну взаємодію всіх структурних підрозділів, пов'язаних із дотриманням норм фінансово-економічної секретності. Забезпечує виконання підрозділом (службою, управлінням, департаментом) програм, планів щодо впровадження новітніх технологій у сфері фінансово-економічної та інформаційної безпеки, оновлення відповідних програмних забезпечень. Уживає заходів щодо забезпечення підрозділу (служби, управління, департаменту) працівниками з питань фінансово-економічної та інформаційної безпеки, найкращого використання їх знань і досвіду. Під час виявлення зовнішніх і внутрішніх загроз і ризиків у сфері фінансово-економічної безпеки підрозділу (служби, управління, департаменту) координує та контролює хід виконання відповідних процедур щодо їх усунення та зменшення. Вирішує питання щодо фінансово-економічної та інформаційної безпеки в межах наданих йому повноважень, доручає виконання окремих функцій іншим працівникам: своїм заступникам, керівникам відповідних структурних підрозділів. Затверджує правовий статус структури підрозділів фінансово-економічної та інформаційної безпеки. Координує роботи зі створення та впровадження нових технологій щодо зниження загроз і ризиків діяльності підрозділу (служби, управління, департаменту), забезпечення фінансово-економічної та інформаційної безпеки. У межах наданих йому повноважень надає всім категоріям посадових осіб інформацію, яка стосується діяльності із забезпечення фінансово-економічної та інформаційної безпеки. Установлює

межі взаємодії інших керівників підрозділу (служби, управління, департаменту), підрозділу фінансово-економічної безпеки з органами державної влади, іншими державними органами, підприємствами, установами та організаціями, громадськими об'єднаннями та громадянами в ході здійснення заходів щодо забезпечення безпеки. Контролює організацію підвищення кваліфікації працівників структурних підрозділів у галузі фінансово-економічної та інформаційної безпеки. Сприяє захисту фінансово-економічних та інформаційних інтересів підрозділу (служби, управління, департаменту) у суді, органах державної влади й управління, приватних і юридичних осіб. Забезпечує дотримання законності, активне використання правових засобів удосконалення управління та функціонування в ринкових умовах, зміцнення договірної, економічної та фінансової дисципліни.

**Повинен знати:** Конституцію України, Господарський, Адміністративний, Кримінальний кодекси України, закони та постанови Верховної Ради України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, інші нормативно-правові документи, що стосуються сфери фінансово-економічної безпеки; функції, загальні принципи побудови та організації діяльності комплексної системи забезпечення фінансово-економічної безпеки підрозділу (служби, управління, департаменту); перспективи, вітчизняні та світові тенденції технологічного, технічного, фінансово-економічного розвитку підрозділу (служби, управління, департаменту); методику розроблення концепції та планування діяльності системи фінансово-економічної та інформаційної безпеки; організацію та особливості здійснення інформаційно-аналітичного забезпечення діяльності системи фінансово-економічної безпеки; можливості ефективного використання виробничих потужностей, наявних технологічних процесів, їх реструктуризації або заміни; захист інформації та комерційної таємниці; технології, форми, методи та методики протидії небезпекам, загрозам і ризикам; технічні засоби спостереження, охорони та захисту; державну та недержавну системи безпеки; порядок розроблення та ведення документації, що регламентує діяльність системи фінансово-економічної безпеки; порядок розроблення та впровадження інновацій у систему забезпечення фінансово-економічної та інформаційної безпеки; механізми управління системою забезпечення фінансово-економічної та інформаційної безпеки; кадрові ресурси підрозділу (служби,

управління, департаменту); порядок організації, здійснення контролю за рівнем фінансово-економічної та інформаційної безпеки та їх оцінювання; передовий вітчизняний і зарубіжний досвід у сфері забезпечення фінансово-економічної безпеки; порядок укладання та виконання фінансово-економічних договорів; правила ділового етикету; правила та норми охорони праці та протипожежного захисту; основні принципи роботи з комп'ютером та відповідні програмні засоби; державну мову.

**Кваліфікаційні вимоги.** Повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра. Підвищення кваліфікації в галузі знань фінансово-економічної безпеки. Стаж роботи на керівних посадах – не менш ніж 5 років.

Додаток К

## Кваліфікаційні характеристики посади професіонала з фінансово-економічної безпеки

**Завдання та обов'язки.** Розробляє, запроваджує та реалізує на практиці заходи із забезпечення фінансово-економічної безпеки. Визначає перспективність та ефективність інноваційної діяльності в галузі фінансово-економічної безпеки підприємства, відповідно до встановлених стандартів (норм). Застосовує техніку й технології із забезпечення фінансово-економічної безпеки. Забезпечує підготовку керівних документів, які стосуються організації діяльності системи фінансово-економічної безпеки підприємства, механізмів управління та взаємодії. Розробляє проекти положень, наказів та інструкцій, що регламентують функціонування системи безпеки, а також діяльність підрозділу економічної безпеки підприємства та його взаємодію з іншими структурними підрозділами. Визначає зовнішні та внутрішні загрози й ризики у сфері фінансово-економічної безпеки підприємства. Сприяє здійсненню інформаційно-аналітичного забезпечення щодо оцінювання рівня реальних і потенційних загроз фінансово-економічній безпеці підприємства. Проектує систему підготовки керівного складу та персоналу підприємства щодо здійснення ефективних заходів із зниження рівня небезпек, загроз та ризиків. Розробляє плани щодо забезпечення фінансово-економічної безпеки та її вдосконалення, здійснення окремих спеціальних заходів щодо оперативного реагування на загрози, ризики, небезпеки діяльності підприємства. Надає пропозиції щодо визначення правового статусу, структури підрозділу економічної безпеки підприємства та визначення його основних функцій. Бере участь у створенні та використанні нових технологій щодо зниження загроз і ризиків діяльності підприємства, забезпечення фінансово-економічної безпеки. Бере участь у розробленні стратегічної орієнтації підприємства, ураховуючи вимоги до забезпечення фінансово-економічної безпеки. Розробляє документи, що визначають стандарти безпеки, повноваження структурних підрозділів підприємства, види та напрями їх діяльності щодо запобігання загрозам, ризикам, небезпеці та забезпечення фінансово-економічної безпеки. У межах наданих йому повноважень надає всім категоріям працівників підприємства інформацію, яка стосується діяльності із забезпечення фінансово-економічної безпеки. Здійснює загальний

контроль за діяльністю структурних підрозділів підприємства щодо забезпечення фінансово-економічної безпеки. Готує пропозиції щодо організації взаємодії керівників підприємства, підрозділу економічної безпеки з органами державної влади, іншими державними органами, підприємствами, установами та організаціями, громадськими об'єднаннями та громадянами під час здійснення заходів щодо забезпечення безпеки діяльності підприємства. Готує пропозиції та надає рекомендації із взаємовідносин із партнерами підприємства щодо розроблення антикризових заходів і забезпечення безпеки. Бере участь в апробації заходів із фінансово-економічної безпеки підприємства шляхом розроблення моделі економічної безпеки підприємства. Забезпечує підвищення кваліфікації працівників підпорядкованого структурного підрозділу в галузі фінансово-економічної безпеки.

**Повинен знати:** Конституцію України, Господарський, Адміністративний, Кримінальний кодекси України, закони й постанови Верховної Ради України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, інші нормативно-правові документи, що стосуються сфери фінансово-економічної безпеки; функції, загальні принципи побудови та організації діяльності комплексної системи забезпечення фінансово-економічної безпеки підприємства; методику розроблення концепції та планування діяльності системи фінансово-економічної безпеки; організацію та особливості здійснення інформаційно-аналітичного забезпечення діяльності системи фінансово-економічної безпеки; особливості захисту інформації та комерційної таємниці на підприємстві; технології, форми, методи та методики протидії небезпекам, загрозам і ризикам; технічні засоби спостереження, охорони та захисту; державну та недержавну системи безпеки; порядок розроблення та ведення документації, що регламентує діяльність системи фінансово-економічної безпеки; порядок розроблення та впровадження інновацій у систему забезпечення фінансово-економічної безпеки; механізми управління системою забезпечення фінансово-економічної безпеки; порядок організації, здійснення контролю за рівнем фінансово-економічної безпеки та його оцінювання; передовий вітчизняний і зарубіжний досвід у сфері забезпечення фінансово-економічної безпеки; правила ділового етикету; правила та норми охорони праці та протипожежного захисту; основні принципи роботи з комп'ютером та відповідні програмні засоби; державну мову.

**Кваліфікаційні вимоги**

*Провідний професіонал із фінансово-економічної безпеки:* повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра. Стаж роботи за професією професіонала з фінансово-економічної безпеки I категорії – не менш ніж 2 роки.

*Професіонал із фінансово-економічної безпеки I категорії:* повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Стаж роботи за професією професіонала з фінансово-економічної безпеки II категорії для магістра – не менш ніж 1 рік, спеціаліста – не менш ніж 2 роки.

*Професіонал із фінансово-економічної безпеки II категорії:* повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Стаж роботи за професією професіонала з фінансово-економічної безпеки для магістра – не менш ніж 1 рік, спеціаліста – не менш ніж 2 роки.

*Професіонал із фінансово-економічної безпеки:* повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Без вимог до стажу роботи.

# Зміст

НАВЧАЛЬНЕ ВИДАННЯ

**Отенко** Ірина Павлівна
**Мішин** Олександр Юрійович
**Мішина** Світлана Володимирівна

# ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ БАНКІВСЬКИХ УСТАНОВ

**Навчальний посібник**

Відповідальний за випуск *Отенко І. П.*

Відповідальний редактор *Оленич М. М.*

Редактор *Лященко О. Г.*

Коректор *Доценко О. Г.*

План 2015 р. Поз. № 19-П.
Підп. до друку 24.11.2015 р. Формат 60×90 1/16. Папір офсетний. Друк цифровий.
Ум. друк. арк. 15,0. Обл.-вид. арк. 18,75. Тираж 400 пр. Зам. № 214.

Видавець і виготівник – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Леніна, 9-А

*Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру*
***ДК № 4853 від 20.02.2015 р.***