**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 існуюча з певною ймовірністю настання можливість нанесення банку будь-якого збитку зловмисниками, конкурентами або обставинами й умовами, що створюють небезпеку для банку, його клієнтів та контрагентів.

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

Згідно з табл. 3.1 загрози діяльності банку діляться на групи за класифікаційними ознаками:

за середовищем виникнення;

за носіями загроз;

за сутнісною характеристикою;

за об’єктами зазіхань;

за тривалістю дії; за характером впливу;

за видами безпеки, на яку впливають загрози.

Таблиця 3.1

**Класифікація загроз банківській безпеці**

|  |  |  |
| --- | --- | --- |
| Ознака класифікації | Види загроз | Характеристика загроз |
| 1 | 2 | 3 |
| За середовищем виникнення (детальний перелік у табл. 3.2) | Внутрішні загрози | Контролюються 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 можуть бути реалізовані шляхом крадіжок, корупційних дій, шахрайства, недобросовісної конкуренції, фізичного тиску на персонал, розголошення банківської інформації |
| Загрози проведенню банківських операцій |
| Загрози інфраструктурі банку |
| Загрози персоналу банку |
| Загрози ліквідності і 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 впиву | 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 в залежності від обставин як у внутрішньому середовищі банку, так і зовнішньому. Важко контрольова­ними загрози стають у випадку їх одночасного виникнення у внутріш­­ньому і зовнішньому середовищах внаслідок змов персоналу із зов­нішніми шахраями.

Таблиця 3.2

**Види загроз за середовищем виникнення**

|  |  |
| --- | --- |
| Вид загроз | Перелік загроз |
| Внутрішні | Фальсифікація і розтрати, змова з конкурентами, контрагентами, халатність, 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 в 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 в цілому банківської безпеки. Найбільш суттєвими і 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 показано в табл. 3.3.

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 оцінки безпеки важливо ідентифікувати можливі загрози.

У першу чергу, в ході забезпечення фінансової безпеки банку здійснюється оцінка загроз економічній безпеці банку, що мають пра­вовий характер. Серед них виділяють:

внутрішні загрози (нераціональне плануван­ня фінансово-економіч­них показників; неправильно обрана ринкова стратегія; помилкова кад­рова, 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.

Таблиця 3.3

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

|  |  |
| --- | --- |
| Зовнішні загрози | Внутрішні загрози |
| 1. Несприятлива соціально-економічна ситуація в країні.  2. Нестійкість та недосконалість нормативно-правової бази.  3. Низький рівень платоспроможного попиту.  4. Нестабільність курсу національної валюти.  5. Недосконала та мінлива політика Національного банку.  6. Високий рівень інфляції.  7. Складна криміногенна ситуація в країні чи регіоні.  8. Відсутність можливостей для розширення ринку банківських послуг.  9. Недобросовісна конкуренція та шахрайство на ринку банківських послуг.  10. Рейдерські атаки та злочинні дії третіх осіб.  11. Недовіра клієнтів до банку | 1. Низька кваліфікація персоналу та менеджменту банку.  2. Низький рівень кваліфікації спеціалістів із забезпечення банківської безпеки.  3. Недостатність ліквідних коштів для погашення зобов’язань.  4. Проблеми з поверненням кредитів.  5. Витік банківської інформації.  6. Недосконалі дії управлінського персоналу.  7. Відсутність або недосконалість маркетингових досліджень ринку банківських послуг.  8. Недосконала кредитна політика банку.  9. Недосконала структура депозитного і кредитного портфелів банку.  10. Низька якість кредитного і депозитного портфелів.  11. Проблемна структура активів банку (значна питома вага низьколіквідних активів, прострочені кредити).  12. Злочинні дії та шахрайство персоналу банку.  13. Погана репутація банку.  14. Підпорядкування цілей банку інтересам власників |

**3.2. Банківське шахрайство і зловживання службовим становищем працівників банків**

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

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

Умови та ознаки шахрайства наведені в табл. 3.4. Якщо в банку створені умови для шахрайських дій, то через деякий час з’являються ознаки шахрайства.

Таблиця 3.4

**Умови та ознаки банківського шахрайства**

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

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

Одним з найбільш поширених способів шахрайства є відмивання грошей. Відмивання грошей – це сукупність дій власника грошей з 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**

|  |  |
| --- | --- |
| Назва | Зміст методу |
| 1. Злиття законних і незаконних фондів | Засновано на використанні в цілях «відмивання» засобів підприємств, в яких значні суми готівки є звичайним і законним явищем (наприклад, ресторани, бари, готелі, компанії та ін.). При цьому застосовуються дві основні схеми: перша - приховування незаконних доходів e масі законних операцій (злиття) реально функціонуючих фірм; друга – створення фіктивної компанії, не провідної реальної діяльності, але що 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 трояка: підтримувати розкішний стиль життя; переводити підозріло крупні суми готівки в однаково цінні, але менш підозрілі форми; купувати майно, яке надалі буде використане в злочинних цілях |
| 3. Незаконний вивіз валюти | Здійснюється в двох основних формах: за допомогою фізичного вивозу і вивозу через фінансові операції. Більшість країн-членів ФАТФ відзначають збільшення об'єму засобів злочинного походження, що поступають контрабандним шляхом для розміщення у фінансовій системі інших держав. Перевозити значні суми грошей злочинцям дозволяє відсутність в багатьох європейських країнах прикордонного контролю за рухом наявних засобів. Так, об'єм кожного перевезення готівки звичайно складає не більше 300 тис. дол., що дає можливість злочинцям обмежити свої втрати у разі крадіжки чи успішної роботи оперативних служб |
| 4. Вивіз грошових коштів | Здійснюється з використанням методів, описаних при характеристиці розміщення через традиційні фінансові установи |

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

1) використання посадових повноважень з корисливою метою;

2) перевищення посадових повноважень з корисливою метою.

Використання посадових повноважень з 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 з корисливою метою може виражатись у такому [13]:

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

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

представлення інтересів установи банку без отримання на те відповідних повноважень;

підпис документів, не передбачених функціональними обов’язками або посадовими повноваженнями;

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

надання гарантій, взяття зобов’язань від імені банку без наявності на те відповідних повноважень.

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

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

Таблиця 3.6

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

|  |  |  |  |
| --- | --- | --- | --- |
| Вид операції | Основні способи здійснення злочинів | Засоби здійснення злочинів | Особи, які здійснюють злочини |
| Розрахункові  операції | Підробка документів;  внесення 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; підробка  документів | Депозитні серти­фікати;  комп’ютерні віруси;  помилкові комп’ю­терні команди | В основному співробітники банку |
| Кредитні  операції | Незаконне одержання 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 з 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 здійснюються у змові з 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, що запропоновано як забезпечення кредиту;

використовують засоби підроблення документів або незаконний доступ до комп’ютерних мереж й електронних банків даних.

Одержання кредиту фізичними особами зумовлено заставою та, зазвичай, обмежується порівняно невеликою сумою коштів. Водночас небезпека цього різновиду шахрайства в кредитно-банківській сфері полягає в 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 одержання 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 акта зарахування коштів на рахунок магазину. Схема шахрайства передбачає оформлення кредиту на придбання товару без наміру повернення коштів, одержання товару та його продаж, з метою виручення готівкових коштів.

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

**1. Заволодіння паролями банківських карток і рахунків.** Кібер-злочинці входять в довіру людей, представляючись працівниками пенсійних фондів, банків, соціальних служб. Вони пропонують допомогу в знятті грошей, або ж нечесним шляхом дізнаються паролі до карток і ізнімають гроші. Злочинці, як один з варіантів незаконного зняття грошей з карток знаходять в Інтернеті оголошення щодо збору благодійних коштів, телефонують авторам оголошень як люди, що хочуть надати допомогу і просять назвати CVVкод, розміщений на зворотному боці картки та термін дії карткового рахунку. Ці дані дають змогу шахраям заповнювати дані в «Приват24». Ця система без правильного коду доступу рекомендувала змінити пароль карткового рахунку. На телефон дійсного власника рахунку приходило СМС-повідомлення. Злочинці просили власників картки надати інформацію про зміст СМС для отримання додаткового карткового рахунку для благодійності. З вико­ристанням нового пароля злочинці знімали всі гроші з благодійного карткового рахунку. Ніяка банківська установа не в змозі попередити такого роду шахрайства.

**2. Пропозиція фіктивних банківських послуг.** Злочинці розміщу­ють в Інтернеті чи ЗМІ оголошення про можливість отримати кредит без застави по різним банківським акціях, лотереях. За обслуговування процесу надання кредиту шахраї просять переказати клієнта певну суму на картковий рахунок. Гроші за обслуговування перераховують на підставних або померлих людей, людей з підробленими паспортами.

**3. Несанкціонований доступ до системи “Клієнт-банк”.** За допо­могою вірусних вредоносних програм шахраї отримують дані з системи і використовуючи шкідливий програмний код, здійснюють віддалений доступ до комп’ютера користувача.

**4. Зчитування інформації з платіжної карти в банкоматі.** У бан­комат вставляють спеціальний пристрій, що дозволяє зчитати інфор­мацію з банківської картки і зняти гроші.

Основними напрямками протидії Інтернет-шахрайству можуть бути:

1) розробка нового програмного обладнання та антивірусних програм;

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

3) створення системи аутентифікації інтернет-адрес для перевірки відповідності введеної користувачем адреси дійсному серверу;

4) підвищення загального рівня грамотності інтернет-користувачів та більш широке 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 діляться на кадрові, іміджеві, локальні та контролюючі (табл. 3.7).

Таблиця 3.7

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

|  |  |  |  |
| --- | --- | --- | --- |
| Кадрові заходи | Іміджеві заходи | Контролюючі заходи | Локальні заходи |
| Створення ефе­ктивної системи відбору персоналу банку;  попередження конфліктів у колек­тиві;  створення дієвої системи мотивації персоналу;  формування соціального пакету та системи матері­альної допомоги для малозабезпе­чених працівників | Формування при­четності до корпо­ративної культури банку;  формування у персоналу банків­ського патріотизму; | перевірки та ре­візії банківських операцій;  періодичні ін.­формаційно-аналі­тичні дослідження ринку банківських послуг;  контроль якості виконуваних захо­дів безпеки;  моніторинг банківської безпеки | Перевірка при­міщень на наяв­ність підслухо­вуючих пристроїв;  оснащення при­міщень засобами відеоспостереже­ння;  захист приміщень від несанкціонова­ного використання засобів зв’язку;  перевірка комп’ю­терної техніки |

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

встановлення в приміщеннях кодових замочних пристроїв з метою запобігання несанкціонованому доступу до них банківського персоналу і клієнтів;

перевірка приміщень на відсутність підслуховуючих пристроїв з використанням пошукової апаратури вітчизняного та зарубіжного виробництва;

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

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

встановлення на абонентні телефонні апарати сумісних з ними технічних засобів захисту мовних повідомлень, що забезпечують шифрування мовного сигналу, що передаються телефонною мережею загального користування;

спеціальна перевірка засобів обчислювальної техніки у місцях їх встановлення на можливість несанкціонованого доступу до інформації за рахунок побічних електромагнітних випромінювань.